Network Architectures
and Services
NET 2011-07-2

FI & IITM
SS 2011

Proceedings of the Seminars
Future Internet (FI) and
Innovative Internet Technologies and Mobile Communications (IITM)

Summer Semester 2011

Munich, Germany, 18.04.-29.07.2011

Editors

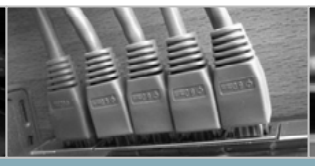
Georg Carle, Corinna Schmitt

Organisation

Chair for Network Architectures and Services
Department of Computer Science, Technische Universität München

Technische Universität München




Network Architectures
and Services
NET 2011-07-2

FI & IITM

SS 2011

Proceedings zu den Seminaren
Future Internet (FI) und
Innovative Internettechnologien und Mobilkommunikation (IITM)

Sommersemester 2011

München, 18.04.-29.07.2011

Editoren: Georg Carle, Corinna Schmitt

Organisiert durch den Lehrstuhl Netzarchitekturen und Netzdienste (I8),
Fakultät für Informatik, Technische Universität München

Technische Universität München

Proceedings of the Seminars
Future Internet (FI) and Innovative Internet Technologies and Mobile Communications (IITM)
Summer Semester 2011

Editors:

Georg Carle
Lehrstuhl Netzarchitekturen und Netzdienste (I8)
Technische Universität München
D-85748 Garching b. München, Germany
E-mail: carle@net.in.tum.de
Internet: http://www.net.in.tum.de/~carle/

Corinna Schmitt
Lehrstuhl Netzarchitekturen und Netzdienste (I8)
Technische Universität München
D-85748 Garching b. München, Germany
E-mail: schmitt@net.in.tum.de
Internet: http://www.net.in.tum.de/~schmitt/

Cataloging-in-Publication Data

Seminars FI & IITM SS2011
Proceedings zu den Seminaren „Future Internet“ (FI) und „Innovative Internettechnologien und Mobilkommunikation“ (IITM)
München, Germany, 18.04.-29.07.2011
Georg Carle, Corinna Schmitt
ISBN: 3-937201-22-X

ISSN: 1868-2634 (print)
ISSN: 1868-2642 (electronic)
DOI: 10.2313/NET-2011-07-2
Lehrstuhl Netzarchitekturen und Netzdienste (I8) NET 2011-07-2
Series Editor: Georg Carle, Technische Universität München, Germany

Vorwort

Wir präsentieren Ihnen hiermit die Proceedings zu den Seminaren „Future Internet“ (FI) und “Innovative Internettechnologien und Mobilkommunikation” (IITM), die im Sommersemester 2011 an der Fakultät Informatik der Technischen Universität München stattfanden.
Im Seminar FI wurden Beiträge zu unterschiedlichen Fragestellungen aus den Gebieten Internettechnologien und Mobilkommunikation vorgestellt. Die folgenden Themenbereiche wurden abgedeckt:

- Einführung in das Patentrecht
- Patentrecherche und Bewertung
- DNSSEC im Vergleich zu DNSCurve für Sicherheit im Netz
- Erkennung „bösartiger“ Domänen
- Locator/Identifier Split
- Der neue, elektronische Personalausweis
- Dienstgüte-Unterstützung für zukünftige Netze
- Strategien zur Paketverarbeitung bei Dienstgüte-Unterstützung
- Standards zur Gerätevernetzung
- Wie sicher sind „Secure Interdomain Routing“ Protokolle?
- Benutzerschnittstellen für intelligente Gebäude

Im Seminar IITM wurden Vorträge zu verschiedenen Themen im Forschungsbereich Innovative Internettechnologien und Mobilkommunikation vorgestellt. Die folgenden Themenbereiche wurden abgedeckt:

- Smart Grids
- Correlated Network Flows Detection
- Patente: Von der Erfindung zum Patent
- „Side-Channel Leaks“ in Internetapplikationen
- Netzwerkvirtualisation
- Übertragungsprotokolle für „Delay-Tolerant“-Networks
- Verkehrsmenge und Caching von Videos
- Probleme beim Einsatz von DTNs
- Vergessene DTNs: Mailbox-Netze und UUCP
- Einführung in die Dualität von konvexer Optimierung

Wir hoffen, dass Sie den Beiträgen dieser Seminare wertvolle Anregungen entnehmen können. Falls Sie weiteres Interesse an unseren Arbeiten habe, so finden Sie weitere Informationen auf unserer Homepage http://www.net.in.tum.de.

München, Juli 2011

Georg Carle

Corinna Schmitt

Preface

We are very pleased to present you the interesting program of our main seminars on “Future Internet” (FI) and “Innovative Internet Technologies and Mobil Communication” (IITM) which took place in the summer semester 2011.

In the seminar FI we deal with issues of Future Internet. The seminar language was German, and the majority of the seminar papers are also in German. The following topics are covered by this seminar:

- Introduction to Patent Law
- Patent research and Evaluation
- DNSSEC vs. DNSCurve for Securing the Net
- Recognition of malicious domains
- Locator/Identifier Split
- The new electronical passport
- QoS Support for Future Networks
- Strategies for Paket Processing with QoS Support
- Standards for Device Connectivities
- How Secure are Secure Interdomain Routing Protocols?
- User Interface for Smart Ambiences – A State of the Art Analysis

In the seminar IITM talks to different topics in innovativ internet technologies and mobile communications were presented. The seminar language was German, and also the seminar papers. The following topics are covered by this seminar:

- Smart Grids
- Correlated Network Flows Detection
- Patent: From Invention to Patent Announcement
- Side-Channel Leaks in Web-Applications
- Network Virtualization
- Transmission Protocols for Delay-Tolerant Networks
- Traffice occurance and Caching of Videos
- Problems with DTNs
- Forgotten DTNs: Mailbox-Networks and UUCP
- An Introduction to Duality in Convex Optimization

We hope that you appreciate the contributions of these seminars. If you are interested in further information about our work, please visit our homepage http://www.net.in.tum.de.

Munich, July 2011

Seminarveranstalter

Lehrstuhlinhaber

Georg Carle, Technische Universität München, Germany

Seminarleitung

Corinna Schmitt, Technische Universität München, Germany

Betreuer

Tobias Bandh, *Technische Universität München, Wiss. Mitarbeiter I8*
Lothar Braun, *Technische Universität München, Wiss. Mitarbeiter I8*
Ali Fessi, *Technische Universität München, Wiss. Mitarbeiter I8*
Stephan Günther, *Technische Universität München, Wiss. Mitarbeiter I8*
Michael Herrmann, *Technische Universität München, Wiss. Mitarbeiter I8*
Ralph Holz, *Technische Universität München, Wiss. Mitarbeiter I8*
Nils Kammenhuber, *Technische Universität München, Wiss. Mitarbeiter I8*
Holger Kinkelin, *Technische Universität München, Wiss. Mitarbeiter I8*
Alexander Klein, *Technische Universität München, Wiss. Mitarbeiter I8*
Andreas Müller, *Technische Universität München, Wiss. Mitarbeiter I8*
Heiko Niedermayer, Technische Universität München, Wiss. Mitarbeiter I8
Marc-Oliver Pahl, *Technische Universität München, Wiss. Mitarbeiter I8*
Corinna Schmitt, *Technische Universität München, Wiss. Mitarbeiterin I8*

Kontakt:

{carle,schmitt,bandh,braun,fessi,guenther,herrmann,holz,hirvi,kinkelin,klein,
mueller,niedermayer,pahl}@net.in.tum.de

Seminarhomepage

http://www.net.in.tum.de/de/lehre/ss11/seminare/

Inhaltsverzeichnis

Seminar Future Internet

Session 1: Patente

Session 2: Dienstgüte

Session 3: Anwendungen und Innovationen

Session 4: Protokolle und Sicherheit

Seminar Innovative Internettechnologien und Mobilkommunikation

Session 1: Netwerke

Session 2: Delay-Tolerant Networks (DTN)

Session 3: Anwendungen und Optimierungen

Einführung in das Patentrecht

Philip Schieber
Betreuer: Andreas Müller, Tobias Bandh
Seminar Future Internet SS2011
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: schieber@in.tum.de

KURZFASSUNG

Der Patentschutz ist heute ein unentbehrliches Mittel zur Förderung des innovativen Entwicklungsdrangs unserer Gesellschaft. Statistiken des Deutschen Patent- und Markenamtes zufolge wird etwa alle neun Minuten eine Erfindung in Deutschland unter gesetzlichen Schutz gestellt. Das Patent als Schutzrecht für technische Innovationen belohnt seinen Urheber durch ein wirtschaftliches Verwertungsmonopol. Gerade für Unternehmen sind derartige gesetzliche Möglichkeiten nicht nur wegen ihrer wirtschaftlichen Relevanz wichtig. Patentanmelder gelten als innovativ, intellektuell und kreativ. Doch wie wird ein Patent genau definiert und was sind die Voraussetzungen, die erfüllt werden müssen, um eine Innovation unter gesetzlichen Schutz stellen zu lassen? Bezugnehmend auf derartige Fragestellungen wird im Folgenden eine Einführung in die Thematik des Patentrechts gegeben. Darüber hinaus werden deutsche und international geltende juristischen Grundlagen des Patentwesens analysiert und dargestellt.

Schlüsselworte

Patent, Patentrecht, Erfindung, Schutzgegenstand, DPMA

1. EINLEITUNG

„[...] Es ist jedem Dritten für die Dauer von 10 Jahren verboten, ohne die Zustimmung des Urhebers eine weitere Vorrichtung zu bauen, die mit besagter Vorrichtung übereinstimmend oder ähnlich ist.“ [13]

Dieser Auszug eines venezianischen Gesetzestextes aus dem Jahre 1474 ist das erste historisch fundierte Dokument, das den gesetzlichen Schutz einer Erfindung festhält. Abstammend von der lateinischen Beschreibung „littera patens“, was frei übersetzt „offener Brief“ bedeutet, wird dieses Schutzrecht auf eine technische Innovation heute „Patent" genannt.
Durch das Patentrecht erhält ein Erfinder für seine schöpferische Leistung eine Rechtsstellung, die ausschließlich ihn für eine bestimmte Zeit zur Verwertung der Erfindung berechtigt.
Die heutige Relevanz des Themas Patentrecht wird unter anderem durch die Analyse von Daten und Statistiken des Deutschen Patent- und Markenamt (DPMA) ersichtlich. Alleine im Jahr 2009 wurden laut dem Jahresbericht des DPMA [5] fast 60.000 neue Patente in Deutschland angemeldet. Hierbei lohnt es sich nunmehr die juristischen Hintergründe des Patentrechts zu analysieren und die internationalen Zusammenhänge dieses Rechtsgebiets darzustellen. Im Folgenden werden, ausgehend von der deutschen Rechtsprechung als Referenzsystem, allgemeine Charakteristika des Patentwesens herausgearbeitet.
So wird das Patentrecht in Abschnitt 2 in einen Kontext mit der deutschen Rechtsprechung gesetzt, woraufhin in Abschnitt 3 international geltende materiell-rechtliche Grundlagen zur Patentfähigkeit einer Erfindung dargelegt werden. In Abschnitt 4 werden das deutsche Patentrecht sowie Grundlagen des Patenterteilungsverfahrens dargestellt und außerdem internationale Bestrebungen zur Harmonisierung des Patentwesens beleuchtet. Zuletzt werden Besonderheiten des amerikanischen Patentrechts vorgestellt und mit den deutschen Rechtsgrundlagen verglichen.

2. Einordnung des Patentrechts in einen juristischen Kontext

„Das deutsche Patentrecht ist eine zentrale Norm des gewerblichen Rechtsschutzes“ [12]. Der Rechtsschutz verpflichtet sich wiederum, als Teil des Privatrechts, dem Schutz des geistig gewerblichen Schaffens. Die relevanten Bereiche des gewerblichen Rechtsschutzes werden in Abbildung 1 dargestellt.

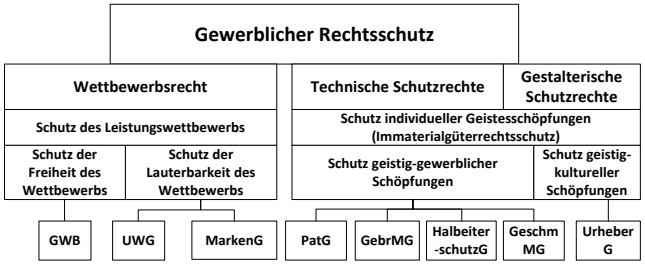


Abbildung 1: Systematisierung der Rechtsmaterie des gewerblichen Rechtsschutzes (In Anlehnung an [17], S.33)

Wie Abbildung 1 zeigt, lässt sich der gewerbliche Rechtsschutz in zwei Teilbereiche gliedern.

So kann man die technischen und gestalterischen Schutzrechte als eine Unterteilung auffassen. Diese Rechte befassen sich mit dem Schutz von individuellen Geistesschöpfungen, welche das Gebiet des Immaterialgüterrechtsschutzes begründen. Ein wichtiges Charakteristikum des Immaterialguts ist, dass es einer bestimmten Person zugeordnet werden kann. Der Immaterialgüterrechtsschutz besteht daher, wie in Abbildung 1 dargestellt, vor allem aus dem Schutz von geistig-gewerblichen Schöpfungen. Hierunter stellen das Patentgesetz, das Gebrauchsmustergesetz und das Halbleiterschutzgesetz die technischen Schutzrechte dar. Das Patentgesetz schützt technische Erfindungen, die aus geistigen Leistungen entstanden sind. Das Gebrauchsmusterrecht ist in

doi: 10.2313/NET-2011-07-2_01

seinem Wesen ähnlich zum Patentrecht. Es beinhaltet ebenfalls Schutzrechte für technische Innovationen, grenzt sich allerdings durch eine weniger strenge Prüfung auf Neuheit und Existenz erfinderischer Schritte vom Patentrecht ab. Umgangssprachlich wird das Gebrauchsmuster deshalb oft auch „kleines Patent“ genannt. Das Halbleiterschutzgesetz bildet eine Sonderform der technischen Schutzrechte für den Bereich der mikroelektronischen Halbleitererzeugnisse. Gemäß dem Gesetzestext erstreckt sich nach §1 Abs.4 des Halbleiterschutzgesetz [3] der Schutz nicht auf die „der Topographie zugrunde liegenden Entwürfe, Verfahren, Systeme, Techniken oder auf die in einem mikroelektronischen Halbleitererzeugnis gespeicherte Information, sondern nur auf die Topographie als solche.“ Das Geschmackmustergesetz unterscheidet sich von den technischen Schutzrechten zufolge dahingehend, dass es nicht technischen Handlungsanweisungen Schutz vor Nachahmung gewährt, sondern neuen, individuellen sowie ästhetischen Gestaltungsformen gewerblicher Leistungen, wie beispielsweise Stoffmustern. Der Erfinder kann hierbei das subjektive Recht an seinem Formgedanken beim Patent- und Markenamt erwerben. Dagegen umfasst das Urhebergesetz den Schutz von kulturellen Schöpfungen, wie beispielsweise literarischen Werken oder Musikstücken.

Neben den technischen und gestalterischen Schutzrechten existiert das Wettbewerbsrecht, als weitere Unterteilung des gewerblichen Rechtsschutzes. Dessen Intention ist der Schutz des Leistungswettbewerbs. Hier kann man den Schutz der Freiheit des Wettbewerbs als einen Unterpunkt auffassen. Juristisch festgeschrieben sind derartige Schutzrechte im Gesetz gegen Wettbewerbsbeschränkungen (GWB). Darüber hinaus existieren Gesetze zum Schutz der Lauterbarkeit des Wettbewerbs. Hierzu gehört unter anderem das im Markengesetz (MarkenG) verankerte Kennzeichenrecht. Dieses regelt neben Markennamen auch geschäftliche Bezeichnungen eines Unternehmens. Folglich wird durch dieses Gesetz vor allem die Werbeleistung eines Markensymbols geschützt.

Somit bleibt festzuhalten, dass das Patentgesetz im Umfeld des gewerblichen Rechtsschutzes ein Teilgebiet des Schutzes geistig gewerblicher Schöpfungen mit technischem Hintergrund abdeckt.

3. Materiell-rechtliche Grundlagen des Patentrechts

Nach der Einordnung des Patentrechts in einen Rechtskontext, gilt es nun die materiell-rechtlichen Grundlagen des Patentwesens zu erläutern. Diese stellen die juristische Basis dar, welche die sachlichen Grundvoraussetzungen zur Erteilung eines Patents festlegt. Die materiell-rechtlichen Grundlagen lassen sich in fünf zentrale Säulen gliedern. Abbildung 2 stellt diese grafisch dar.

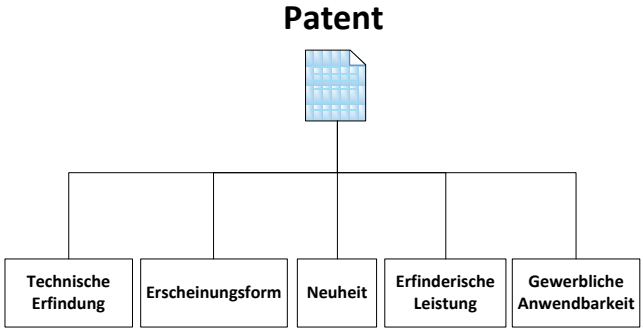


Abbildung 2: Materiell-Rechtliche Säulen eines Patents

Im Folgenden gilt es zu klären, ob ein Schutzgegenstand die Eigenschaften einer technischen Erfindung erfüllt. Ferner muss man unterscheiden, welche Patenterscheinungsform vorliegt, da man zwischen Sach- und Verfahrenspatenten differenziert. Nach Klärung dieser Sachverhalte muss der Schutzgegenstand noch unter weiteren drei Gesichtspunkten, welche die sachlichen Schutzvoraussetzungen darstellen, beleuchtet werden. Ein zu analysierender Aspekt ist der Grad der Neuheit einer Erfindung. Darüber hinaus bilden die erfinderische Leistung und gewerbliche Anwendbarkeit des Schutzgegenstandes zwei weitere Prüfungsgrundsätze zur Patentfähigkeit.

Ausgehend von der deutschen Rechtsprechung werden die beschriebenen Patenterteilungsvoraussetzungen genauer beleuchtet. Als juristische Grundlage des deutschen Patentrechts dient das Patentgesetz (PatG) [4]. Dieses trat erstmals 1877 in Kraft und wurde zwischen 1970 und 1980 grundlegend überarbeitet.

3.1 Die Erfindung als Schutzgegenstand

Gemäß §1 PatG werden Patente ausschließlich für Erfindungen auf allen Gebieten der Technik erteilt. Allerdings existiert für den Begriff der „Erfindung“ keine juristische Definition. Ann [2] beschreibt, dass man sich zudem auch in der Rechtswissenschaft auf keine allgemeine Definition einigen konnte. Allerdings haben sich im Laufe der Zeit feste Kriterien durchgesetzt, anhand derer das Vorliegen einer Erfindung im Einzelfall ermittelt werden kann. So gilt heute der Grundsatz: „Eine Erfindung ist eine Lehre zum planmäßigen Handeln unter Einsatz beherrschbarer Naturkräfte zur unmittelbaren Erreichung eines kausal übersehbaren Erfolgs“ [2]. Hierbei sind jedoch einzelne Definitionen der im Satz auftretenden Begriffe von zentraler Bedeutung. Eine „Lehre“ ist ein vom Menschen erschaffenes Gut. Es ist hierbei jedoch wichtig, dass etwas Neues hervorgebracht wird, was über die Auffindung von etwas Gegebenem hinaus geht. Bei dem Begriff „Naturkräfte“ ist zu beachten, dass diese ohne Zwischenschaltung menschlicher Verstandtätigkeit existieren. Ein „kausal übersehbarer Erfolg“ ist eine beabsichtigte, realisierbare und wiederholbare Lösung eines technischen Problems.
Auch für den Begriff der „Technik“ fehlt im Gesetz eine juristische Legaldefinition. Zu beachten ist, dass der Technikbegriff nicht von zeitloser Gültigkeit, sondern anpassungsfähig an die technologischen Veränderungen und die daraus resultierenden Schutzbedürfnissen ist. Der Technikbegriff ist daher in seinem Wesen dynamisch und von Veränderungen seiner Umgebung abhängig. Dadurch wird ein Vorgang dargestellt, welcher der „Welt der Dinge“ [2] zuordenbar ist. Reine Anweisungen an den Geist sind allerdings nicht technisch, infolgedessen können sie auch nicht durch ein Patent geschützt werden.

Eine Erfindung ist freilich gemäß §1 Abs.3 Nr.1 PatG von einer Entdeckung abzugrenzen, welche für sich genommen, mangels Technizität, nicht patentierbar ist. Eine Entdeckung beschreibt definitionsgemäß das bloße Auffinden von bereits existierenden Kenntnissen, bei der die Anweisungen zum neuartigen Handeln fehlen. Ferner wird im selben Paragraphen die Patentfähigkeit von wissenschaftlichen Theorien und mathematischen Methoden negiert, da diese ebenfalls keine Lehre zum Handeln darstellen und somit eher einer Entdeckung als einer Erfindung zurechenbar sind. §1 Abs.3 Nr.3 PatG schließt Pläne, Regeln und Verfahren für gedankliche Tätigkeiten, Spiele oder geschäftliche Tätigkeiten sowie Programme oder Datenverarbeitungsanlagen aus. Vor allem das Verbot der Patentierung von Datenverarbeitungsanlagen,

doi: 10.2313/NET-2011-07-2_01

welche umgangssprachlich auch als „Softwarepatente“ bezeichnet werden, wird aktuell kontrovers diskutiert.

Zusammenfassend ist anzumerken, dass der Begriff der technischen Erfindung juristisch nicht eindeutig geklärt ist und die Ermittlung der Patentfähigkeit eines Schutzgegenstandes oft subjektiven Auffassungen unterliegt.

3.2 Erscheinungsformen eines Patents

Gemäß §9 PatG verleiht ein Patent seinem Inhaber das ausschließliche Benutzungsrecht an der geschützten Erfindung. Darüber hinaus schreibt das Gesetz zudem ein Verbietungsrecht fest, dass Dritten die Verwendung der geschützten Erfindung ohne Erlaubnis des Patentinhabers untersagt. Nun gilt es jedoch zu unterscheiden, welche Erscheinungsform eines Patents vorliegt, da die rechtlichen Benutzungseinschränkungen je nach Patentform verschieden sind.

3.2.1 Erzeugnispatent

In §9 Satz 2 Nr.1 PatG ist festgehalten, dass es jedem Dritten untersagt ist, ohne die Zustimmung des Patentinhabers ein Erzeugnis, das Gegenstand eines Patents ist, herzustellen, anzubieten, in Verkehr zu bringen oder zu gebrauchen. Aus dieser Formulierung lässt sich der Begriff des „Erzeugnispatents“ ableiten. Dieser ist allerdings an keiner Stelle im Gesetzestext genauer definiert. Jedoch haben sich in der Vergangenheit aus Literatur und Rechtsprechung verschiedene Arten des Erzeugnispatents herausgebildet.

Zum einen kann man „[…] Vorrichtungs- oder Einrichtungspatente, deren Schutzgegenstand Arbeitsmittel sind“ [11], den Erzeugnispatenten zuordnen. Diese erfüllen einen bestimmten Funktionszweck und bestehen im Regelfall aus körperlichen Elementen, die bestimmte Arbeitsschritte ausführen. Als Beispiel für Vorrichtungs- oder Einrichtungspatent dienen Maschinen oder Geräte. Ferner gelten Anordnungen als Erzeugnispatente. Jene bestehen aus Mitteln mit vorwiegend körperlicher Natur, die durch funktionelles Zusammenwirken einen Mehrwert bringen. Oftmals wird auch die Anordnung als Sonderfall des Einrichtungspatents angesehen. Die auf Stoffe erteilten Patente werden ebenfalls den Erzeugnispatenten zugeordnet. Anwendung in der Praxis finden derartige Patente meistens auf dem Gebiet der Chemie. In Abgrenzung zu den Vorrichtungs- und Einrichtungspatenten basiert hierbei der Schutz auf der inneren Beschaffenheit eines Erzeugnisses.

3.2.2 Verfahrenspatent

§ 9 Satz 2 Nr.2 PatG besagt, dass es jedem Dritten verboten ist, ein Verfahren, das Gegenstand eines Patents ist, anzuwenden. Bei derartigen Verfahrenspatenten differenziert man zwischen zwei Arten. Auf der einen Seite werden Prozesse betrachtet, deren Hauptfunktionalität in der Herstellung von Gütern liegen. Die Charakteristik eines Herstellungsverfahrens ist aus einem bestimmten Ausgangsprodukt mit Hilfe von festgelegten Verfahrensschritten ein Endprodukt zu produzieren. Wichtig ist hierbei, dass das Produkt während des Vorgangs einer Transformation unterliegt. Derartige Herstellungsverfahren können mechanische, physikalische, biologische oder chemische Prozesse enthalten. Auf der anderen Seite stehen die Verfahren, welche sich auf die Veränderung von Erzeugnissen beziehen. Diese werden ebenfalls den Verfahrenspatenten zugeordnet.

3.3 Sachliche Schutzvoraussetzungen

Nach §1 Abs.1 PatG ist eine Erfindung nur dann patentfähig, wenn sie folgende drei sachliche Schutzvoraussetzungen erfüllt. Diese sind „Neuheit“, „erfinderische Tätigkeit“ und „gewerbliche Anwendbarkeit“.

3.3.1 Neuheit

Die sachliche Schutzvoraussetzung „Neuheit“ beruht auf dem eigentlichen Zweck des Patents. Demzufolge hat die Förderung des technischen Fortschritts höchste Priorität. Das Patent als Ausschließungsrecht ist daher für den Erfinder eine Art Belohnung dafür, dass er die technische Entwicklung vorangetrieben hat. Der im Gesetz verankerte Neuheitsbegriff wurde 1978 in das PatG eingebracht. Seitdem hat er die Anforderungen an eine erfinderische Leistung durch den zusätzlich zu überprüfenden Aspekt der Neuheit nochmals verschärft.

§3 Abs.1 PatG definiert den Neuheitsbegriff: Eine Erfindung gilt dem Gesetzestext zufolge als neu, wenn sie nicht zum Stand der Technik gehört. Der Stand der Technik wird im Gesetz definiert als die Kenntnisse, die vor dem für den Zeitrang der Anmeldung maßgeblichen Tag durch schriftliche oder mündliche Beschreibung, durch Benutzung oder in sonstiger Weise der Öffentlichkeit zugänglich gemacht worden sind.

Ensthaler [7] spricht unter Beachtung des Gesetzestexts von einem absoluten Neuheitsbegriff. Er verwendet das Adjektiv „absolut“, da eine ältere Veröffentlichung, die unter Umständen nie zur Ausführung kam, neuheitsschädlich sein kann. Neuheitsschädlich ist somit alles, was dem Stand der Technik zuordenbar ist. Dies umfasst insbesondere die Kenntnisse, die der Öffentlichkeit vor dem Anmeldetag zugänglich waren. Die Öffentlichkeit und der damit bezeichnete Personenkreis als solcher ist ein mengenmäßig schwer zu definierender Bereich. Die Publikation einer Information erfordert daher eine Unkalkulierbarkeit der Empfängerzahl sowie die Auffindbarkeit der Informationen durch einen Durchschnittsfachmann. Im juristischen Sinne ist ein Durchschnittsfachmann „[...] ein Experte, der auf seinem Gebiet über das übliche Fachwissen und durchschnittliche Fähigkeiten verfügt“ [14].

Wie in §3 Abs.1 PatG beschrieben, gibt es verschiedene Arten der Veröffentlichung von Informationen. Ist nun eine öffentlich zugägnliche Quelle einer Erfindung ähnlich, so ist die Schutzvoraussetzung der Neuheit verletzt. Infolgedessen ist eine solche Erfindung nicht patentfähig. Die Quellen, aus welchen sich der aktuelle Stand der Technik ableitet, sind jedoch unterschiedlich und differenzierbar. Es besteht die Möglichkeit, dass schriftliche Publikationen existieren, die für die Öffentlichkeit erreichbar sind. Gleicht eine solche Quelle der Erfindung, die auf Patentfähigkeit geprüft wird, so spricht man im juristischen Sinne von einer neuheitsschädlichen Vorveröffentlichung. Ferner ist es möglich, mündlich Informationen zugänglich zu machen. Dies bezeichnet den Vorgang der Publikation von Informationen durch das gesprochene Wort in der Öffentlichkeit. Im Gesetzestext wird darüber hinaus die Variante der Veröffentlichung von Informationen durch Benutzung einer Erfindung festgeschrieben. Allerdings muss hier der Kern der Innovation für die Öffentlichkeit klar erkenntlich sein. Juristisch läge hier, sofern eine solche Quelle einer Erfindung gleicht, ein Fall der neuheitsschädlichen Vorbenutzung vor. Auch jegliche sonstige Art und Weise der Veröffentlichung kann neuheitsschädlich sein. Das heißt, dass jedes Medium, das Träger relevanter Informationen ist, zum aktuellen Stand der Technik beiträgt.

Abschließend bleibt festzuhalten, dass die Rechtsprechung auf die Kenntnisse und Fähigkeiten eines Durchschnittsfachmanns abzielt. In diesem Fall würde keine neuheitsschädliche Vorbeschreibung vorliegen, wenn der Durchschnittsfachmann eine vorbeschriebene Lehre nicht nachvollziehen oder die Lehre

doi: 10.2313/NET-2011-07-2_01

mit Hilfe einer Vorbeschreibung nicht ausführen kann.

3.3.2 Erfinderische Tätigkeit

Gemäß §4 Satz 1 PatG ist eine Erfindung auf einer erfinderischen Tätigkeit beruhend, wenn sie sich für einen Fachmann nicht in naheliegender Weise aus dem Stand der Technik ergibt. Zweck dieses Gesetzes ist es die technologische Weiterentwicklung zu fördern. Der Erfinder muss somit ein erforderliches Mindestmaß an geistiger und schöpferischer Anstrengung nachweisen, um eine erfinderische Leistung zu erzielen. Oftmals wird diese Voraussetzung vereinfachend „Erfindungshöhe" genannt. Dem Gesetzestext zufolge sind zur Beurteilung der Erfindungshöhe zwei Aspekte heranzuziehen. Einerseits ist das Urteil eines Durchschnittsfachmanns (siehe Definition in Abschnitt 3.3.1) und andererseits der Stand der Technik von zentraler Bedeutung. Hierdurch wird versucht eine möglichst objektive Bewertung der erfinderischen Tätigkeit zu wahren.

Nichtsdestotrotz bleibt die Bewertung der erfinderischen Tätigkeit ein eher subjektiver Vorgang. In vielen Patentverfahren ist diese Schutzvoraussetzung Teil von juristischen Auseinandersetzungen, da hier das Gesetz keine eindeutigen Vorgaben, sondern allenfalls Richtlinien vorgibt. Meistens bleibt daher ein Spielraum zur subjektiven Bewertung der Erfindungshöhe.

3.3.3 Gewerbliche Anwendbarkeit

Die dritte sachliche Schutzvoraussetzung zur Patenterteilung ist die gewerbliche Anwendbarkeit einer Erfindung. Diese gilt nach §5 PatG als gewerblich anwendbar, wenn ihr Gegenstand auf irgendeinem gewerblichen Gebiet, einschließlich der Landwirtschaft, hergestellt oder benutzt werden kann. Beachtet wird hierbei allerdings nur die Möglichkeit der tatsächlichen Anwendbarkeit einer Erfindung. Ob diese wirtschaftlich rentabel realisiert werden kann ist rechtlich nicht von Bedeutung. Somit ist der Grundgedanke dieser Schutzvoraussetzung vor allem die Förderung der praktischen Umsetzbarkeit von technischen Innovationen.
Die Formulierung im Gesetzestext wirft jedoch nach Anns [2] Meinung Probleme hinsichtlich der deutschen Definition des Gewerbebegriffs auf. Dieser schließt zwar alle Bereiche auf den Gebieten der Industrie, des Handwerks, des Bergbaus und der Landwirtschaft mit ein, vernachlässigt jedoch die freien Berufe, wie Anwälte oder Ärzte. Hierbei gilt es allerdings zu beachten, dass nach §2 Abs.1 Nr.2 PatG alle chirurgischen oder therapeutischen Verfahren zur Behandlung des menschlichen oder tierischen Körpers von der Patentfähigkeit ausgenommen sind.

4. Patentsysteme

„Die Gründe zur Legitimation eines Patentsystems liegen in der Schutz- und Informationsfunktion von Patenten" [16]. Daraus folgt, dass die Schutzfunktion die Aussicht auf Patentschutz die Erfindungs- und Innovationstätigkeit anregt. Der Informationsfunktion von Patenten liegt die Offenbarungstheorie zugrunde. Demnach wird ein Vertrag zwischen Erfinder und der Allgemeinheit abgeschlossen, bei dem der Erfinder sein geheimes Wissen zugunsten eines Ausschließlichkeitsschutzes für die gewerbliche Verwertung aufgibt.

Eine weitere wichtige Säule eines Patentsystems ist die Tatsache, dass eine Erfindung durch die Erteilung eines Patents zu einem handelbaren und transferierbaren Gut wird.

Die Bedingungen und Funktionen von Patenten sind zwar weltweit durchaus ähnlich, jedoch unterscheiden sich Patentanmeldungsverfahren und Wirkungsrechte zwischen den einzelnen Staaten zum Teil erheblich. Grundsätzlich besitzt jedes Land ein eigenes Patentamt, welches sich um Belange der Patenterteilung und um Verletzungen des Patentrechts kümmert. Im Folgenden werden nunmehr das deutsche Patentrecht und der Prozess des deutschen Patenterteilungsverfahrens dargestellt. Daneben wird auch das europäische Patentrecht vor allem hinsichtlich dessen territorialer Wirkung analysiert. Abschließend wird das amerikanische Patentsystem, im Hinblick auf Unterschiede zum deutschen und europäischen Patentrecht, untersucht.

4.1 Das deutsche Patentrecht

Nach §34 Abs.1 PatG ist eine Erfindung zur Erteilung eines Patents beim DPMA anzumelden. Über den Anspruch des Anmelders auf Erteilung eines Patents wird in einem Verfahren vor dem Patentamt verhandelt. Beschwerdefälle werden vor dem Patentgericht und Rechtsbeschwerdeverfahren vor dem Bundesgerichtshof entschieden.

Zunächst ist festzustellen, dass ein Patentrecht „[…] in seiner Wirkung räumlich auf das Gebiet des Staates, in dem das Patent erteilt wurde, beschränkt ist" [9]. Diese Regelung bezeichnet man als „Territorialitätsgrundsatz". Das bedeutet, wenn beim DPMA ein Patent angemeldet wird, ist dieses nur auf dem Staatsgebiet der Bundesrepublik Deutschland gültig. Hintergrund dieser Tatsache ist die Souveränität der einzelnen Staaten, die als elementarer Grundsatz im Völkerrecht verankert ist.

Darüber hinaus treten bei der Patenterteilung gesetzliche Wirkungen in Kraft, welche sich vor allem in Form von Rechten für den Patentanmelder äußern. So gilt unter anderem nach §9 Satz 1 PatG, dass alleine der Patentinhaber befugt ist, die patentierte Erfindung im Rahmen des geltenden Rechts zu benutzen. Das geltende Recht ist allerdings an den Schutzbereich des Patents gebunden. Dieser wird nach §14 Satz 1 PatG bei der Patentanmeldung durch die Patentansprüche bestimmt. Das Gesetz besagt, dass zur Auslegung der Patentansprüche Beschreibungen und Zeichnungen herangezogen werden sollen. Diese sind §32 Abs.3 Satz 1 PatG zufolge in der Patentschrift enthalten. Die Wirkung des Patents erstreckt sich gemäß §11 PatG nicht auf Handlungen, die im privaten Bereich zu nichtgewerblichen Zwecken vorgenommen werden.

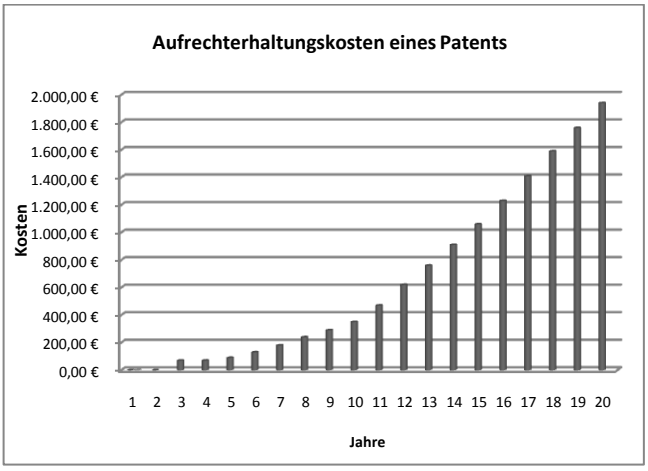


Abbildung 3: Aufrechterhaltungskosten eines Patents

Beginnend mit dem Tag, der auf die Anmeldung folgt, dauert das Patent, gemäß §16 Abs.1 PatG, 20 Jahre. Ferner gilt es zu beachten, dass ab dem dritten Jahr progressiv steigende Aufrechterhaltungskosten für ein Patent anfallen. Abbildung 2 veranschaulicht diese Kostenentwicklung, basierend auf dem Kostenmerkblatt des DPMA [6], grafisch.

doi: 10.2313/NET-2011-07-2_01

4.1.1 Das deutsche Patenterteilungsverfahren

Nachdem die rechtlichen Grundlagen des deutschen Patentwesens dargelegt wurden, gilt es nun das deutsche Patenterteilungsverfahren zu analysieren.

Gemäß §34 Abs.1 PatG ist eine Erfindung zur Erteilung eines Patents beim DPMA anzumelden. Diese Anmeldung muss den Namen des Anmelders und einen Antrag auf Erteilung eines Patents enthalten. Darüber hinaus müssen ein oder mehrere Patentansprüche, in denen angegeben ist, was als patentfähig unter Schutz gestellt werden soll, klar ersichtlich sein. Zusätzlich ist es erforderlich eine Beschreibung der Erfindung, sowie Zeichnungen, auf die sich die Patentansprüche beziehen, der Anmeldung beizufügen. Nach §34 Abs.4 PatG ist eine Erfindung so deutlich zu offenbaren, dass ein Durchschnittsfachmann (siehe Definition in Abschnitt 3.3.1) sie ausführen kann.
Im Anschluss an die Anmeldung erfolgt zunächst eine Offensichtlichkeitsprüfung, bei der die Einhaltung formaler Vorschriften überwacht wird und die Erfindung in die „Internationale Patentklassifikation“ [17] eingeordnet wird. Die Prüfung auf die materiell-rechtlichen Schutzvoraussetzungen erfolgt gemäß §44 Abs.1 PatG nur auf Antrag durch den Patentanmelder oder durch jeden Dritten, der nicht am Prüfungsverfahren beteiligt ist. Hierbei ist eine gesetzlich festgelegte Anmeldefrist von sieben Jahren nach Einreichung der Anmeldung zu beachten. Erfolgt innerhalb dieses Zeitraums kein Prüfungsantrag, so gilt die Patentanmeldung als nichtig. Neben dieser Prüfung existiert die Möglichkeit eine Recherche durch das DPMA in Auftrag zu geben. Hier bietet die Behörde die Möglichkeit an, den Stand der Technik, das heißt die Voraussetzungen, anhand derer Neuheit und Erfindungshöhe des Patents beurteilt werden, zu ermitteln. In der Praxis werden beim DMPA häufig derartige Anträge gestellt, da deren Arbeit als gründlich und vollständig gilt. Gemäß §31 Abs.2 Nr.2 PatG stehen, sofern seit dem Anmeldezeitpunkt 18 Monate verstrichen sind, die Akten der Patentanmeldung jedermann zur Einsicht frei. Nach §49 Abs.1 PatG kann schlussendlich die Prüfungsstelle das Patents nach vollständiger Kontrolle aller Anmeldungserfordernisse, sowie Schutzvoraussetzungen erteilen. Genügt eine Erfindung den Anforderungen des Gesetzes nicht, wird der Patentantrag gemäß §48 PatG durch die Prüfungsstelle zurückgewiesen.

Im Falle der Erteilung eines Patents wird die Patentschrift veröffentlicht. In dieser sind die Patentansprüche, Beschreibungen, Zeichnungen und Verweise enthalten. Zudem wird die neu patentierte Erfindung im Patentblatt aufgeführt. Danach treten die gesetzlichen Wirkungen des Patents in Kraft. Nach Art.30 Abs.1 PatG führt das Patentamt ein Register, welches alle Patentanmeldungen datentechnisch erfasst. Das Patentblatt ist eine regelmäßig erscheinende Veröffentlichung des DPMA und beinhaltet gemäß §32 Abs.5 PatG Übersichten über die Eintragungen ins Register.

§59 Abs.1 PatG schreibt fest, dass innerhalb von drei Monaten nach Veröffentlichung der Patenterteilung Einspruch gegen diesen Beschluss erhoben werden kann.

4.2 Internationales Patentrecht

Der gesetzliche Rechtschutz war „[…] von Anbeginn seiner Entstehung dadurch geprägt, dass dieser auch grenzüberschreitend beachtet werden sollte“ [1]. Aufgrund der lediglich territorialen Wirkungskraft von Patenten galt es frühzeitig schon rechtliche Rahmenbedingungen zu schaffen, um Patente staatenübergreifend anmelden zu können. Heute basiert der internationale Patentschutz auf zwei Säulen. Zum einen existieren die nationalen Rechtssysteme der Mitgliedsstaaten und zum anderen wurden auf zwischenstaatlicher Ebene Rechtsverträge sowie Vereinbarungen abgeschlossen. Im Folgenden werden die drei wichtigsten zwischenstaatlichen Übereinkommen zur Vereinfachung von staatenübergreifenden Patentanmeldungen näher betrachtet.

4.2.1 Pariser Verbandsübereinkunft (PVÜ)

Im Laufe des 19. Jahrhunderts traten die ersten Bestrebungen auf, welche sich als Ziel gesetzt hatten die auf staatlicher Ebene geltenden Gesetze beziehungsweise Normen im Bereich der gewerblichen Schutzrechte international zu vereinheitlichen. Eine Reihe von Staaten unterzeichnete daher am 20. März 1883 die Pariser Verbandsübereinkunft (PVÜ) zum Schutz des gewerblichen Eigentums. Dieser Vertrag ist einer der ersten international geltenden Übereinkommen im Bereich des gewerblichen Rechtsschutzes. Die Prinzipien der PVÜ basieren vor allem auf dem „Inländerbehandlungsprinzip“. Dieses schreibt vor, dass die Mitglieder der PVÜ jedem Bürger, der aus einem Mitgliedsstaat stammt, die gleichen rechtlichen Vorteile bezüglich des Schutzes des geistigen Eigentums einräumen müssen. Hierdurch wird vermieden, dass ein Land seine eigenen Bürger rechtlich zu Ungunsten von ausländischen Bürgern bevorteilt. Darüber hinaus ist das Prinzip der „Unionspriorität“ von großer Bedeutung. Die Intention hierbei ist es Konflikte, die sich bei zwei oder mehr Erfindungen zur selben Sache ergeben könnten, zu verhindern. Es wurde beschlossen, dass jeder Antragssteller für ein Patent in einem Mitgliedsstaat der PVÜ demnach eine Prioritätsfrist von derzeit 12 Monaten für die Hinterlegung des Antrags in jedem anderen Land, das der PVÜ angehört, hat. Während dieser Frist kann kein Patent, das Ähnlichkeiten zu der durch die Prioritätsfrist geschützten Erfindung aufweist, in einem anderen Mitgliedsstaat angemeldet werden. Eine Gruppe von Patentanmeldungen in verschiedenen Ländern, die direkt oder indirekt durch eine gemeinsame Priorität miteinander in Verbindung stehen, wird Patentfamilie genannt.

Die PVÜ als älteste Vereinbarung auf dem Gebiet des gewerblichen Rechtsschutzes gilt als „[…] die Basis des internationalen Patentsystems“ [17]. Heute umfasst die Vereinigung 173 Mitgliedsstaaten.

4.2.2 Patent Cooperation Treaty (PCT)

1978 wurde in Washington ein Vertrag zur Vereinbarung besserer zwischenstaatlicher Zusammenarbeit im Hinblick auf den Patentschutz von mehreren Staaten unterzeichnet. Intention dieser Vereinigung war es „[…] die Ebene rein territorialen Denkens zu verlassen“ [18]. Nach der PVÜ wurden zwar Fortschritte im Zuge der internationalen Vereinheitlichung des Patentschutzes erreicht, es war aber immer noch notwendig in jedem Land einen Patentantrag in dessen Sprache unter Beachtung der verschiedenen Anmeldeformalia zu stellen.
Im Zuge der PCT ist es nunmehr möglich eine international geltende Anmeldung eines Patents zu erreichen. Dazu meldet man eine Erfindung bei einem nationalen Patentamt oder beim Europäischen Patentamt an und kann verschiedene Bestimmungsstaaten angeben, auf die sich der Patentschutz ausweiten soll. „Das PCT-Verfahren lässt sich in eine internationale und nationale Phase gliedern“ [17].
Die internationale Phase wird mit der Einreichung der Patentanmeldung initialisiert. Darauf folgen die Erstellung des internationalen Rechercheberichts sowie die Veröffentlichung der internationalen Anmeldung. Diesem Prozess schließt sich nun ein Prüfungsverfahren durch die nationalen Patentämter der Bestimmungsländer an. An dieser Stelle werden die materiellen Schutzvoraussetzungen sowie länderspezifische Voraussetzungen zur Patenterteilung überprüft.

doi: 10.2313/NET-2011-07-2_01

Neuhäusler [15] zufolge hat das PCT-Verfahren zwei große Vorteile. Der erste besteht darin, dass die Anmeldung eines Patents in der eigenen Sprache erfolgen kann und nicht in der Sprache des Bestimmungslandes formuliert werden muss. Der zweite Vorteil liegt in einer vorläufigen internationalen Prüfung, die eine zeitliche Verschiebung des Eintritts in die nationale Phase zur Folge hat. Infolgedessen entstehen Kosten erst 12 Monate später, also zu einem Zeitpunkt, zu dem der Patentanmelder bereits nähere Erkenntnisse über die wirtschaftlichen Erfolgsaussichten eines Patents hat. Den Vorteilen stehen allerdings auch Nachteile des PCT-Verfahrens in der Praxis gegenüber. So erkennen einige nationale Patentämter die vorläufige internationale Prüfung oftmals nicht an. Infolgedessen muss eine derartige Prüfung, die außerdem zusätzliche Kosten für den Patentanmelder verursacht, auf nationaler Ebene wiederholt werden.

Aktuell gibt es 142 PCT-Mitgliedsstaaten, wie unter anderem die USA und Deutschland. Die Bedeutung der PCT-Anmeldungen nimmt heutzutage immer mehr zu. So gab es alleine 2010 nahezu 163.000 PCT-Anmeldungen [20], was gegenüber den Anmeldezahlen von 2009 eine Steigerung von etwa 5 % entspricht.

4.2.3 Europäisches Patentübereinkommen (EPÜ)

Im Jahre 1978 trat das Europäische Patentübereinkommen (EPÜ), ein multilateraler Staatsvertrag über die Erteilung europäischer Patente, in Kraft. Dieser Vertrag führt die Errungenschaften der PVÜ und PCT zu einem einheitlichen europäischen Erteilungsverfahren fort. Die Besonderheit in diesem Prozess liegt jedoch darin, dass die beteiligten Staaten einen Teil ihrer Souveränität aufgeben. Das Übereinkommen sieht vor, dass vom Europäischen Patentamt als zentrale Behörde ein europäisches Patent mit rechtlicher Wirkung für die beteiligten Staaten erteilt werden kann. Der Erteilung eines europäischen Patents geschieht ohne Bestätigung der nationalen Behörden.

Die materiellen Schutzvoraussetzungen eines Patents auf europäischer Ebene entsprechen weitestgehend dem deutschen PatG. Wird nun durch das Europäische Patentamt ein Patent mit unmittelbarer Schutzwirkung für alle vom Anmelder benannten Staaten erteilt, so zerfällt dieses in ein Bündel nationaler Patente, von denen unter Umständen jedes an die lokalen rechtlichen Begebenheiten angepasst werden muss.

Patentanmeldungen beim Europäischen Patentamt können nicht nur von Staatsangehörigen der Mitgliedsstaaten eingereicht werden, sondern von allen Staatsbürgern der Erde. Laut der Statistik des Europäischen Patentamts [8] stammen die meisten Patentanmeldungen des Jahres 2009 aus den USA.Neben allen 27 Mitgliedsstaaten der Europäischen Union gehören heute elf weitere Staaten, wie die Türkei oder die Schweiz zur Europäischen Patentorganisation.

4.2.4 Vergleich der Patenterteilungsverfahren

Wie im bisherigen Verlauf geschildert, existieren verschiedene Varianten einer Patentanmeldung. Abbildung 4 visualisiert die Möglichkeiten einer nationalen oder internationalen Patentanmeldung grafisch.

Es gilt festzuhalten, dass es zum einen die Möglichkeit gibt, ein Patent direkt beim national zuständigen Patentamt anzumelden. Nachteile hierbei sind, dass eine Patentanmeldung in der jeweiligen Landessprache verfasst werden muss. Darüber hinaus verfügt jeder Staat und somit jedes Patentamt über spezifisch geltende Gesetze und Normen, die man im Einzelfall beachten muss.

Eine weitere Möglichkeit stellt die PCT-Anmeldung dar. Vorteile hierbei sind, dass man eine international geltende Anmeldung bei lediglich einem Patentamt anmelden muss. Ein entscheidender Nachteil ist die Tatsache, dass diese Anmeldung durch alle Patentämter der Bestimmungsstaaten geprüft, übersetzt und gegebenenfalls an die national geltenden Gesetze angepasst werden muss. Im Zuge dessen entstehen Kosten für den Patentanmelder.

Eine europäische Patentanmeldung hat den Vorzug, dass die zentrale Patentanmeldung beim Europäischen Patentamt nicht mehr durch die einzelnen Bestimmungsstaaten geprüft werden muss. Dies erspart dem Patentanmelder zusätzliche Kosten, die bei den Prüfverfahren durch die jeweiligen nationalen Patentämter angefallen wären.

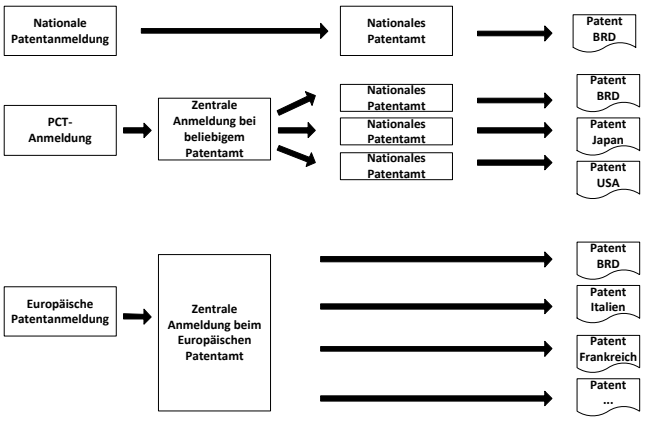


Abbildung 4: Möglichkeiten der nationalen und internationalen Patentanmeldung

4.3 Das US-Patentrecht

Das amerikanische Patentrecht grenzt sich erheblich von der deutschen und internationalen Gesetzgebung ab.

Der wohl bedeutsamste Unterschied ist das prioritätsbegründete Erfinderprinzip. Ann [2] schildert, dass überall auf der Welt der Erstanmelder das Patent erhält, welches dem Grundsatz des „first to file“ entspricht. In den USA hingegen hat der Ersterfinder, nach dem Prinzip „first to invent“, den Anspruch auf das Patent. Dies ist unter Umständen zwar gerechter, lässt sich aber schwerer handhaben als das sonst überall geltende Erstanmelderprinzip. Eine Anmeldung lässt sich einfach und eindeutig rekonstruieren, wohingegen der Zeitpunkt einer Erfindung rechtlich nur schwer definierbar ist. In der Praxis hat dies in den USA zur Folge, dass in den Forschungs- und Entwicklungsabteilungen von Unternehmen Aufzeichnungen, zum Beispiel in Form von Laborberichten existieren, um später im Falle eines Rechtsstreit beweisen zu können, die Erfindung als Erster getätigt zu haben. Die Schutzdauer eines Patents beträgt, wie auch im deutschen Patentrecht, 20 Jahre.

Weitere Unterschiede zum deutschen und europäischen Patentrecht werden anhand der Patentarten und Gegenständen, die patentiert werden können, ersichtlich. So existieren „[…] in den USA drei Arten von Patenten“ [15]. Die „utility patents“ werden an denjenigen vergeben, der einen neuen und nützlichen Prozess, eine Maschine, einen herstellbaren Gegenstand oder eine Materialzusammensetzung erfindet beziehungsweise entdeckt. Die „design patents“ werden für neue, originale und verzierende Designs für einen herstellbaren Gegenstand an den Erfinder vergeben. Darüber hinaus können „plant patents“ an jeden erteilt

doi: 10.2313/NET-2011-07-2_01

werden, der eine neue Varietät einer Pflanze erfindet oder entdeckt und asexuell reproduziert.

2009 wurden in den USA 482.871 Patente [19] durch das „United States Patent and Trademark Office“ erteilt.

5. Zusammenfassung

Abschließend bleibt anzumerken, dass das deutsche und internationale Patentrecht ein weites Gebiet darstellt, welches in Auszügen dargelegt wurde. Alleine die Tatsache, dass sich in Deutschland eine Vielzahl von Patentanwälten um die Belange des gewerblichen Rechtsschutzes kümmern, verdeutlicht den Umfang und die Komplexität dieses Rechtsgebietes. Festzuhalten bleibt, dass sich einige Aspekte des nationalen und internationalen Patentrechts nur wenig unterscheiden. So kann man unter anderem die materiellen Patententerteilungsvoraussetzungen aufführen, die international weitgehend einheitlich im Gesetzestext formuliert sind. Andere Aspekte, wie beispielsweise die Patenterteilungsverfahren einzelner Staaten sind jedoch auf nationaler und zwischenstaatlicher Ebene zu differenzieren. Hierzu wurden Bestrebungen zur Harmonisierung des internationalen Patentrechts skizziert. So existieren heutzutage Beschlüsse, wie die PVÜ, das PCT oder das EPÜ, deren Intention die Vereinheitlichung und Vereinfachung von international geltenden Patentanmeldungen ist.

Zusammenfassend gilt es zu unterstreichen, dass das Patentrecht wirtschaftlich und gesellschaftlich heute eine äußerst wichtige Stellung inne hat. Der ehemalige Präsident des DPMA Erich Otto Häußer (1930-1990) bringt die Bedeutung des Patentrechts pointiert mit folgendem Zitat auf den Punkt:

> „Wer nicht erfindet, verschwindet.
> Wer nicht patentiert, verliert.“ [10]

6. Literatur

[1] Ahrens, C. (2008), „Gewerblicher Rechtsschutz“, Mohr Siebeck Tübingen, 2008.

[2] Ann, C. (2008), „Patente und Marken“, http://www.jura.wi.tum.de/fileadmin/w00bcz/www/Materialien_PatMa/PatMa_WS_2010_11_PatR.pdf, zugegriffen am 21.03.2011.

[3] Bundesministerium der Justiz, „Gesetz über den Schutz der Topographien von mikroelektronischen Halbleitererzeugnissen“, http://www.gesetze-im-internet.de/bundesrecht/halblschg/gesamt.pdf, zugegriffen am 10.03.2011.

[4] Bundesministerium der Justiz, „Patentgesetz“, http://www.gesetze-im-internet.de/bundesrecht/patg/gesamt.pdf, zugegriffen am 10.03.2011.

[5] Deutsches Patent- und Markenamt, „Jahresbericht 2009“, Juni 2010.

[6] Deutsches Patent- und Markenamt, „Kostenmerkblatt“, http://www.dpma.de/docs/service/formulare/allgemein/a9510.pdf, zugegriffen am 17.03.2011

[7] Ensthaler, J. (2009), „Gewerblicher Rechtsschutz und Urheberrecht“, Springer-Verlag, 3.Auflage, Januar 2009.

[8] EPO, „Europäische Patentanmeldungen von 2000-2009 nach Sitz bzw. Wohnstaat“, http://documents.epo.org/projects/babylon/eponet.nsf/0/57439235539A0D63C125755B005CAFC1/$File/applications_2000-2009_per_residence_en.pdf, zugegriffen am 18.03.2011.

[9] Götting, H.-P., Schwipps, K. (2004), „Grundlagen des Patentrechts“, B.G.Teubner Verlag, 1.Auflage, Januar 2004.

[10] Häußer, E., „Zitate zum Thema Patent“, http://www.zitate.de/kategorie/Patent/, zugegriffen am 18.03.2011

[11] Hofmann, A. (2000), „Der Schutz von Verfahrenserfindungen im Vergleich zu Erzeugniserfindungen“, Dissertation an der Technischen Universität München ((Fakultät für Wirtschafts- und Sozialwissenschaften), 2000.

[12] Ilzhöfer, V., Engels, R. (2009), „Patent-, Marken- und Urheberrecht“, Franz Vahlen GmbH, 7.Auflage, Januar 2010

[13] Kostylo, J., Translation of “Venetian Statute on Industrial Brevets, Venice (1474)”, http://www.copyrighthistory.org/cgi-bin/kleioc/0010/exec/showTranslation/%22i_1474%22/start/%22yes%22, zugegriffen am: 08.03.2011.

[14] Kraßer, R. (2004), „Patentrecht – Ein Lehrbuch zum deutschen Patent- und Gebrauchsmusterrecht, Europäischen und Internationalen Patentrecht“, 5.Auflage, 2004.

[15] Neuhäusler, P. (2008), „Patente in Europa und den USA“, Fraunhofer IS Discussion Paper.

[16] Nirk, R., Ullmann, E. (2007), “Patent-, Gebrauchsmuster- und Sortenschutzrecht (Start ins Rechtsgebiet)“, C.F.Müller, 3.Auflage, November 2006.

[17] Spranger, H. C. (2006), „Die Bewertung von Patenten“, Dissertation an der Universität Würzburg (Fakultät für Wirtschaftswissenschaften), 2006.

[18] Thum, B., “Die Territorialität gewerblicher Schutzrechte und ihre Bedeutung für Sachverhalte mit Auslandsbezug” http://www.wuesthoff.de/fileadmin/site/documents/news/de/Aufsatz_zu_Territorialitaetsprinzip_-_Thum.pdf, zugegriffen am 18.03.2011

[19] United States patent and trademark office, “U.S. patent statistic report”, http://www.uspto.gov/web/offices/ac/ido/oeip/taf/us_stat.pdf, zugegriffen am 18.03.2011

[20] WIPO, „International Patent Filings Recover in 2010“,http://www.wipo.int/pressroom/en/articles/2011/article_0004.html, zugegriffen am 18.03.2011.

doi: 10.2313/NET-2011-07-2_01

Patentrecherche und Bewertung

Matthias Kastner
Betreuer: Tobias Bandh, Andreas Müller
Seminar Future Internet SS2011
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: kastner@in.tum.de

KURZFASSUNG

Gewerbliche Schutzrechte wie Patente spielen im zunehmenden Maße eine bedeutende Rolle für den wirtschaftlichen Erfolg von Unternehmen, da hiermit ein entscheidender Wettbewerbsvorteil geschaffen werden kann. Um sicherzustellen gegen keine andere Patente zu verstoßen, ist vor einer Patentanmeldung eine Recherche obligatorisch. Doch auch in weiteren Bereichen sollte einer Patentrecherche Beachtung geschenkt werden. Sind bereits eigene Patente angemeldet, so können hiermit Verstoße von Dritten identifiziert und anschließend rechtlich dagegen vorgegangen werden. Darüber hinaus kann die Patentliteratur als mächtige Informationsquelle genutzt werden. In dieser Arbeit wird beschrieben wie eine Analyse von Patentschriften zusammen mit einer Patentrecherche durchgeführt werden kann. Dabei werden verschiedene Möglichkeiten einer Patentrecherche vorgestellt und der Umgang mit Patentdatenbanken erklärt.

Schlüsselworte

Patentrecherche, Patentbewertung, Patentanalyse, Patentfamilien, Patentdatenbanken, Patentklassifikation

1. EINLEITUNG

Im schnelllebigem Informationszeitalter sind Unternehmen einem immer stärker anwachsenden Konkurrenz- und somit auch Innovationsdruck ausgesetzt. Mithilfe von technischen Schutzrechten wie Patenten ist es möglich, sowohl die eigene Unternehmensposition als auch die Aktivitäten von anderen Unternehmen maßgeblich zu beeinflussen [1].

Wie in [2] beschrieben, sollte die Patentrecherche besonders in Unternehmen, welche sich mit technischen Entwicklungen beschäftigen einen sehr hohen Stellenwert einnehmen. Dies wird dabei durch Studien belegt, welche besagen, dass durch eine umfangreiche Patentrecherche die Entwicklungskosten um bis zu 30 % gesenkt und die Entwicklungszeiten um bis zu 25 % verringert werden können. Aus diesen Gründen ist es äußerst überraschend, dass weniger als 10 % der mittelständischen Unternehmen Patentrecherchen durchführen.

Den Kern dieser Arbeit bildet die Patentrecherche zusammen mit einer Bewertung von Patenten. Um eine Patentrecherche erfolgreich durchführen zu können, ist ein grundlegendes Verständnis von Patenten erforderlich. Dieses wird zunächst vermittelt. Dabei werden insbesonders die für die Patentrecherche relevanten Bereiche wie Patentfamilien, der Aufbau von Patentschriften und die Patentklassifikation beschrieben. Aufgrund der Masse an Patentdokumenten sollte eine tiefergehende Recherche immer in Verbindung mit einer Analyse von Patentdokumenten durchgeführt werden. Daher wird gezeigt wie mittels Indikatoren eine Bewertung von Patentschriften erfolgen kann. Darauf folgend werden die verschiedenen Typen einer Recherche erläutert. Im Anschluss dazu werden die verschiedenen Möglichkeiten einer Patentrecherche vorgestellt. Da eine erste Recherche heutzutage meist mittels Patentdatenbanken über das Internet geschieht, wird der Umgang mit den bedeutendsten Patentdatenbanken erklärt. Eine umfangreiche Patentrecherche ist komplex und mit zahlreichen Herausforderungen verbunden. Diese werden abschließend beschrieben und dabei Tipps für eine zielführende Patentrecherche gegeben.

Inhalt dieser Arbeit sind lediglich Patente. Andere Schutzrechte wie Gebrauchsmuster, Geschmacksmuster oder Marken werden hierbei nicht behandelt. Im Folgenden wird sowohl das deutsche als auch das europäische Patentrecht berücksichtigt. Weiteren Patentgesetzen aus anderen Ländern wird keine Beachtung geschenkt.

2. PATENTE

Die Zielsetzung des Patentsystems ist die Förderung technischer Innovationen, das Verbreiten von Informationen und die Steigerung von Technologietransfers [3]. Den rechtlichen Rahmen des Patentsystems bildet das Patentgesetz (PatG) [4].

Im Folgenden wird nach [5] eine Definition für Patente gegeben. Ein Patent ermöglicht den Schutz von technischen Erfindungen, die weltweit neu sind, auf einer erfinderischen Tätigkeit beruhen und gewerblich anwendbar sind. Das Patent gibt dem Inhaber ein staatlich garantieres Recht für einen bestimmten Zeitraum exklusiv über die Erfindung zu verfügen. Dabei kann der Patentinhaber andere von der kommerziellen Nutzung ausschließen. Patente dürfen prinzipiell für Erfindungen aus allen Bereichen der Technik erteilt werden.

Ausgeschlossen sind dabei jedoch unter anderem folgende Teilgebiete:

- bloße Entdeckungen
- wissenschaftliche Theorien
- mathematische Methoden
- Pläne, Regeln und Verfahren für gedankliche Tätigkeiten

doi: 10.2313/NET-2011-07-2_02

- geschäftliche Tätigkeiten wie beispielsweise Organisationsmodelle
- EDV-Programme als solche

Neben dem Schutzrecht entstehen zahlreiche weitere Vorteile durch eine Patentanmeldung. Nach [3] bietet eine Patentanmeldung unter anderem folgende Funktionen:

- Technische Dokumentation
- Hindernis für Anmeldungen von Konkurrenten
- Portfoliobildung durch Eigenverwertung, Lizenztausch, Verkauf
- Werbung/Firmenimage

Ein Patent ist in seiner Wirkung begrenzt in räumlicher Hinsicht durch das Gebiet für das es erteilt und in Kraft ist, in zeitlicher Hinsicht durch seine Laufzeit, welche normalerweise 20 Jahre beträgt und in Ausnahmefällen fünf Jahre verlängert werden kann und in sachlicher Hinsicht durch seinen rechtlichen Schutzbereich mit Patentansprüchen [3].

2.1 Patentansprüche

An dieser Stelle werden die Patentansprüche nach [6] erläutert. Der rechtliche Schutzbereich wird durch die jeweiligen Patentansprüche eingegrenzt. Nach Definition beschreiben Patentansprüche den wesentlichen Gegenstand der Erfindung für den Schutz begehrt wird. Patentansprüche können ein- oder zweiteilig in der Patentschrift beschrieben werden. Bei einer zweiteiligen Formulierung, welche vorrangig in deutschen Patentschriften verwendet wird, ist der Patentanspruch in einen Oberbegriff und einen kennzeichnenden Bereich geteilt. Im Oberbegriff sind dabei die durch den Stand der Technik bekannten Merkmale der Erfindung beschrieben, während im kennzeichnenden Teil die Merkmale der Erfindung erläutert werden, für welche in Verbindung mit den Merkmalen des Oberbegriffs Schutz begehrt wird.

2.2 Patenterteilungsverfahren

Ein Patent entsteht nicht bereits mit der Fertigstellung einer Erfindung, sondern erst nach Durchlaufen eines Erteilungsverfahrens vor einem Patentamt durch einen Erteilungsakt. Für detaillierte Informationen zum Erteilungsverfahren sei auf [7] und [8] verwiesen.

Ab dem Anmeldezeitpunkt entsteht ein einjähriges Prioritätsrecht. Innerhalb dieses Zeitraumes kann der Patentinhaber das Patent in sämtlichen Ländern, welche der Pariser Verbandsübereinkuft angehören, nachträglich anmelden [3]. Eine Auflistung dieser derzeit insgesamt 173 Länder liefert [9].

2.3 Patentfamilien

Bei einer Patentfamilie handelt es sich nach [2] in der Regel um sämtliche Dokumente, die mindestens auf eine gemeinsame Erstanmeldung zurückgehen. Wird ein Patent innerhalb der Prioritätsfrist in weiteren Ländern nachträglich angemeldet, so entsteht für jedes Land zwar ein nationales Patent, jedoch sind diese Patente über eine gemeinsame Priorität miteinander verbunden und gehören somit immer derselben Patentfamilie an.

2.4 Patentklassifikation

Die Internationale Patentklassifikation (IPC) kategorisiert Patente in unterschiedliche Klassen. Jedes Patent wird dabei in eine von 70.000 technischen Untergliederungen eingeordnet. Mit der Deutschen Feinklassifikation (DEKLA) kann die Selektion auf insgesamt 110.000 und mit der europäischen Klassifikation (ECLA) auf 135000 Klassen detailliert werden [10]. Die Klassifikation erfolgt (ohne DEKLA/ECLA) mittels fünf Ebenen, wobei mit jeder Ebene die Einordnung verfeinert wird.

Zuerst muss eine Sektion, anschließend eine Klasse, eine Unterklasse, eine Gruppe und abschließend eine Untergruppe ausgewählt werden.

Es existieren nach [11] die folgenden acht Sektionen:

- Sektion A - Täglicher Lebensbedarf
- Sektion B - Arbeitsverfahren, Transportieren
- Sektion C - Chemie, Hüttenwesen
- Sektion D - Textilien, Papier
- Sektion E - Bauwesen, Bergbau
- Sektion F - Maschinenbau
- Sektion G - Physik
- Sektion H - Elektrotechnik

In Tabelle 1 wird die IPC-Einordnung am Beispiel eines Skateboardes mit Bremse dargestellt. Die oberen fünf Zeilen beinhalten die Ebenen, welche bereits beschrieben wurden. Die beiden letzten Zeilen beschreiben die Verfeinerung mit ECLA, womit in diesem Fall eine Unterscheidung zwischen Bremsen, die auf den Rollen und Bremsen, welche auf den Boden wirken getroffen werden kann.

Tabelle 1: IPC-Einordnung: Skateboard mit Bremse

Wert	Ebene	Bezeichnung
A	Sektion	Täglicher Lebensbedarf
A 63	Klasse	Sport, Spiele etc.
A 63 C	Unterklasse	Schlittschuhe, Rollschuhe, Ski
A 63 C 17	Gruppe	Rollschuhe, Rollbretter
A 63 C 17/04	Untergruppe	mit Bremse
A 63 C 17/14 B	ECLA	auf die Rollen wirkende Bremsen
A 63 C 17/14 C	ECLA	auf den Boden wirkende Bremsen

2.5 Inhalt einer Patentschrift

In dieser Arbeit wird nur ein kurzer Überblick über die Patentschrift (auch Offenlegungsschrift genannt) mit den für die Recherche und Bewertung relevanten Punkten gegeben. Für ein tiefergehendes Verständnis sei auf §§34 - 41 in [4] und auf [10] verwiesen.

Die Offenbarung stellt einen wesentlichen Bestandteil des Patentrechts dar und ist eine der zwingenden Voraussetzungen zur Erlangung des Patentschutzes.

doi: 10.2313/NET-2011-07-2_02

Die Erfindung muss in dieser Schrift so deutlich und vollständig beschrieben sein, dass ein Fachmann sie ausführen kann. Für die Recherche von Patentschriften zur Analyse ist besonders die erste Seite von Bedeutung. Ein Beispiel für eine deutsche Patentschrift ist in Abbildung 1 dargestellt.

(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 10 2004 054 762 A1** 2005.06.23

(12) **Offenlegungsschrift**

(21) Aktenzeichen: **10 2004 054 762.9**
(22) Anmeldetag: **12.11.2004**
(43) Offenlegungstag: **23.06.2005**

(51) Int Cl.[7]: **B60C 23/00**
G08B 21/02

(30) Unionspriorität:
2003/383302 13.11.2003 JP

(74) Vertreter:
HOFFMANN & EITLE, 81925 München

(71) Anmelder:
THE YOKOHAMA RUBBER CO., LTD., Tokio/Tokyo, JP

(72) Erfinder:
Tozawa, Yukio, Hiratsuka, Kanagawa, JP; Kuramori, Akira, Hiratsuka, Kanagawa, JP

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Warnvorrichtung für Reifen und pneumatischer Reifen**

(57) Zusammenfassung: Diese Erfindung bezieht sich auf eine Reifen-Warnvorrichtung, die Zugkräfte zumindest eines Verstärkungs-Kords einer Gewebeunterbau-Lage oder einer Gurt-Lage eines pneumatischen Reifens detektiert und eine Warnung auf Basis der detektierten Zugkräfte zur Verfügung stellt. Die Reifen-Warnvorrichtung beinhaltet einen Belastungssensor, der an zumindest einem Verstärkungs-Kord angebracht ist, zum Abtasten einer Belastung des zumindest einem Verstärkungs-Kords, Übermittlungsmittel zum Übermitteln eines durch den Belastungssensor abgetasteten Signals, Empfangsmittel zum Empfangen eines abgetasteten Signals von dem Übermittlungsmitteln, Verarbeitungsmitteln, die die Zugkräfte des zumindest einen Verstärkungs-Kords auf Basis des abgetasteten Signalinputs von den Empfangsmitteln berechnet und bestimmt, ob die Warnung auf Basis der berechneten Zugkräfte zur Verfügung gestellt wird oder nicht, und Warnmittel zum zur Verfügungstellen der Warnung auf Basis der Bestimmung der Verarbeitungsmittel.

Abbildung 1: Deutsche Patentschrift [12]

Im Folgenden werden nach [10] die wichtigsten Inhalte der ersten Seite einer Patentschrift genannt. Die jeweiligen Nummerierungen beziehen sich dabei auf Abbildung 1. Es befinden sich auf dieser Seite unter anderem Informationen über den Anmeldetag (22), den Offenlegungstag (43), das Aktenzeichen (21), die Patentklassifikation (10), den Anmelder/Patentinhaber (71), den Erfinder (72), den Titel der Erfindung (54), eine Zusammenfassung (57) und (optional) eine Skizze. Bei europäischen Patenten müssen zusätzlich die Staaten, für welche das Patent in Kraft ist, angegeben werden.

Dem Titelblatt folgt nach [7] die Patentbeschreibung worin der Stand der Technik, dessen Problem, die Lösung des Problems durch die Erfindung, die Vorteile der gewählten Lösung und Ausführungsbeispiele beschrieben sind. Anschließend werden die Patentansprüche formuliert, welche den Schutzumfang des Patents bilden. Abschließend befinden sich noch Zeichnungen/Skizzen zu den Ausführungsbeispielen.

3. PATENTANALYSE

Unter einer Patentanalyse versteht man die Untersuchung von Technologie-Output anhand von Patentdokumenten [13]. Es ist von größter Bedeutung, Patentschriften und Patentansprüche zu bewerten, um relevante Patente und wichtige Informationen von Patentschriften zu filtern. Wie bereits eingangs erwähnt, sollte eine Patentrecherche zusammen mit einer Patentanalyse durchgeführt werden. In welcher Reihenfolge dabei vorgegangen werden sollte, kann nicht generalisiert werden. Weitere Informationen hierzu finden sich in Kapitel fünf.

Wie auch in [13] beschrieben, ist eine qualitative Untersuchung, bei welcher gesamte Patentschriften gelesen und bewertet werden müssen, aufgrund der Masse an verschiedenen Patentdokumenten, in den meisten Fällen nicht praktikabel. Aus diesem Grund ist eine quantitative Patentanalyse zu bevorzugen. Bei einer Patentanalyse wird Gebrauch von bibliometrischen Methoden und Indikatoren gemacht. Bei bibliometrischen Methoden handelt es sich um die statistische Auswertung von bibliografischen Daten, bei Indikatoren um Messgrößen, die Aussagen über Situationen oder Entwicklungen treffen können. Das Ziel einer Patentanalyse ist die Bewertung von Relevanz, Wichtigkeit und Qualität der Patentschriften durch statistische Verfahren.

Mit dieser Analyse können Fragen wie „Wie verlaufen die Entwicklungstrends innerhalb bestimmter Bereiche?“, „Welche Unternehmen sind die Technologieführer?“ oder „Was sind die typischen Absatzmärkte für bestimmte technische Lösungen?“ beantwortet werden. Dabei wird die Suche meist auf bestimmte Untergruppen eingeschränkt, was mittels der Patentklassifikation geschehen kann.

Es sei darauf hingewiesen, dass mit einer (quantitativen) Patentanalyse lediglich ein Überblick und keine Detailanalyse erfolgt. Diese kann anschließend durch eine qualitative Analyse für bestimmte Patentschriften geschehen.

Die Anwendung der Bibliometrie ist mit einigen technischen und methodologischen Problemen verbunden. Zum einen kann grundsätzlich nicht unterschieden werden ob eine Lösung in einer Publikation von hoher oder niedriger Qualität ist. Dies ist problematisch, da somit die „schwächeren“ Patente den besseren Patenten gleichgestellt sind. Zudem existieren Inkonsistenzen und Fehler (beispielsweise Schreibfehler oder fehlende Daten) in Patentschriften. Solche Patente bleiben womöglich unberücksichtigt. Unterschiedliche Schreibweisen (beispielsweise Personen- und Firmennamen) erschweren die Patentanalyse zusätzlich. Ein weiteres Problem stellt das Format des Volltextes dar. Während inzwischen zwar die meisten Patente teilweise recherchierbar sind, existieren immer noch Patente, welche in einem unrecherchierbaren Format gespeichert sind.

3.1 Indikatoren

Indikatoren stellen nach [13] den Kern einer Patentanalyse dar. Prinzipiell kann zwischen einfachen Indikatoren (Reihenfolgen) und Indikatoren, die anhand von mehreren Feldwerten berechnet werden, unterschieden werden. Bei letzterem bedient sich die Patentanalyse auch komplexerer Methoden zur Datenverarbeitung und -visualisierung wie beispielsweise dem Textmining oder der Clusteranalyse.

Bei einfachen Indikatoren handelt es sich um eine Aufzäh-

doi: 10.2313/NET-2011-07-2_02

lung von Werten eines bestimmten Datenbankfeldes. Im Folgenden werden die meistgenutzten einfachen Indikatoren aufgelistet und mögliche Anwendungsbereiche beschrieben.

- **Anzahl der Patente**
  Dieser Indikator wird zur Einschätzung der Stärke (Aktivität, Produktivität) eines Akteurs (Erfinder, Unternehmen) genutzt
- **Anzahl der Zitierungen**
  Die Anzahl der Zitierungen stellt ein wichtiges Qualitätsmaß dar. Wird eine Patentschrift (oder auch Publikationen des Autors) häufiger zitiert, so ist das Patent mit großer Wahrscheinlichkeit von höherer Wichtigkeit als eine Patentschrift, welche nicht oder nur kaum zitiert wird.
- **Patentfamiliengröße**
  Ein Patent, welches in vielen Ländern angemeldet ist, wird vom Akteur bedeutsamer eingeschätzt als ein Patent welches nur in einem Land angemeldet ist. Mit der Patentfamiliengröße lässt sich ermitteln, für wie relevant ein Patent angesehen wird. Es ist hierbei jedoch zu beachten, dass dies kein objektives Maß, sondern nur die Sicht des Entwicklers wiedergibt.
- **Verteilung der Patente über Fachgebiete**
  Die Anzahl der Patente in einem Fachgebiet verdeutlicht, im Vergleich mit anderen Anmeldegebieten, die Interessen des Unternehmens (Entwicklungsschwerpunkte).
- **Laufzeit des Patents**
  Für ein Patent fallen progressive Aufrechterhaltungskosten an. Ist ein Patent über einen sehr langen Zeitraum angemeldet, so ist dies ein Indiz dafür, dass der Anmelder das Patent für sehr bedeutend hält. Ansonsten würde dieser vermutlich den Patentschutz erlischen lassen indem die Gebühren nicht entrichtet werden.

Es existieren verschiedene Verfahren um Indikatoren, die anhand von mehreren Feldwerten berechnet werden, zu bestimmen. In dieser Arbeit werden diese Indikatoren jedoch nicht betrachtet, da sie meist auf komplexen statistischen Verfahren beruhen und eine Werkzeugunterstützung notwendig ist. Es sei dafür empfohlen, eigens für diesen Zweck entwickelte Programme wie beispielsweise STN Easy [14] oder Delphion [15] zu verwenden. Als Einführung bietet sich hierzu [13] an.

3.2 Analyse von Patentansprüchen

Patentansprüche bilden nach [6] den Kern einer jeden Patentschrift. Da sie den Schutzumfang einer Erfindung beschreiben, ist es elementar, sie zu bewerten. Wurden Patentschriften als relevant identifiziert, so sollten die Patentansprüche auf jeden Fall analysiert werden.

Üblicherweise sind Patentansprüche zweiteilig formuliert. In einem solchen Fall ist der kennzeichnende Teil, welcher die Patentansprüche beschreibt, mit „dadurch gekennzeichnet, dass“, „gekennzeichnet durch“ oder einer sinngemäßen Wendung eingeleitet.

Eine weitere Hilfe bei der Bewertung von Patentansprüchen bietet, dass bei einer Zusammenfassung mehrerer Merkmale jedes Merkmal mit einer neuen Zeile beginnen muss.

Zum besseren Verständnis können dazugehörige Zeichnungen beitragen, welche Patentansprüche oftmals deutlicher darstellen.

4. PATENTRECHERCHE

Eine umfangreiche Patentrecherche ist in vielen Situationen obligatorisch. So muss vor einer Anmeldung eines Patents sichergestellt werden, dass gegen kein anderes Patent verstoßen wird. Sollten bereits eigene Patente angemeldet sein, so kann mit einer Recherche geprüft werden ob andere Patente gegen eigene verstoßen. Im Weiteren bietet die Patentrecherche eine wertvolle Informationsquelle, da schätzungsweise 85-90 % des gesamten veröffentlichten technischen Wissens in Patentliteratur enthalten ist [7]. Lediglich 5 - 10 % dieses Wissens ist auch in anderer Literatur publiziert [11]. Mit einer Patentrecherche kann die Konkurrenz beobachtet und abgelaufene Schutzrechte bzw. Patente, welche nicht im jeweiligen Land angemeldet sind, frei genutzt werden. Mit der Nutzung dieser Patente können massive Einsparungen erzielt werden. Es wird geschätzt, dass in Europa durch die konsequente Nutzung der Patentliteratur Kosten für Doppelentwicklung in Höhe von 20 Milliarden Euro jährlich eingespart werden könnten [2].

4.1 Recherchetypen

Die Patentrecherche kann eine Vielzahl von Fragen beantworten und verschiedene Funktionen übernehmen. Um sicherzustellen, dass ein Rechercheergebnis bei der Beantwortung der gestellten Fragen hilfreich ist, haben sich verschiedene Recherchetypen für verschiedene Anfragen herausgebildet. Generell unterscheidet man zwischen Formal- und Sachrecherchen, welche im Folgenden nach [2] erläutert und voneinander abgegrenzt werden.

4.1.1 Formalrecherchen

Bei Formalrecherchen werden die Formalangaben (bibliografische Daten) genutzt. Dabei kann eine Unterscheidung zwischen Namens-, Familien- und Rechtsstandsrecherchen gemacht werden.

Mittels einer *Namensrecherche* werden Patentanmeldungen einer Person oder eines Unternehmens ermittelt. Das Ziel dabei ist, zu überprüfen, welche Verfahren bzw. Produkte von einem bestimmten Unternehmen geschützt sind. Eine Namensrecherche dient vorrangig zur Überwachung der Patentanmeldungen eines Unternehmens, da sich die Recherche auf einzelne Unternehmen beschränkt.

Eine *Familienrecherche* stellt eine weitere Möglichkeit einer Formalrecherche dar. Mit einer Familienrecherche können zu einem Patent Anmeldungen in anderen Ländern ermittelt werden. Mit einer Patentfamilienrecherche lässt sich gewissermaßen die Bedeutung eines Patents für die jeweilige Firma ableiten. Zudem können hiermit unter Umständen sprachliche Barrieren umgangen werden, da vermutlich ein Patent, welches in mehreren Ländern angemeldet ist, zumindest auch in Englisch verfügbar ist.

Mit einer *Rechtsstandsrecherche* kann der rechtliche Status einer Patentanmeldung eingesehen werden. Dadurch kann geklärt werden ob ein Schutzrecht bereits erteilt bzw. noch in Kraft ist. Darüber hinaus kann in Erfahrung gebracht

doi: 10.2313/NET-2011-07-2_02

werden ob gegen ein Patent Einspruch erhoben worden ist. Diese Art der Recherche wird vorrangig als erster Schritt bei vermutlichen Patentverstößen durchgeführt.

4.1.2 Sachrecherchen

Sachrecherchen beziehen sich auf den technisch-inhaltlichen Charakter der Schutzrechte. Dabei erfolgt die Suche in den Datenbanken nicht nach einem formalen Eintrag sondern nach technologischen Inhalten. Dabei wird der Volltext oder ein bestimmter Teil einer Patentschrift durchsucht.

Eine *Übersichtsrecherche* (auch Technologierecherche genannt) ist eine Ausprägung einer Sachrecherche. Das Ziel einer Übersichtsrecherche ist das Finden verschiedener Lösungsansätze zu einem bestimmten Problem. Es wird dazu die Patentliteratur betrachtet Dabei steht nicht im Vordergrund, die Lösungsansätze im Detail zu betrachten, sondern lediglich das Verschaffen eines Überblicks.

Bei einer *Stand der Technik-Recherche* werden alle Beschreibungen in Betracht gezogen, die vor dem Anmeldedatum der Öffentlichkeit zugänglich gemacht wurden. Im Gegensatz zu einer Übersichtsrecherche ist es bei einer Stand der Technik-Recherche von keinerlei Bedeutung, ob es sich bei den Publikationen um Patentliteratur oder andere Literatur handelt.

Mittels einer *Neuheitsrecherche* wird versucht, Patentschriften mit einer Kombination von bestimmten technischen Merkmalen zu identifizieren. Diese Recherche wird vor der Patentanmeldung durchgeführt, um sicherzustellen, gegen keine bereits erteilten Patente zu verstoßen.

Das Ziel einer *Einspruchsrecherche* ist es, bereits erteilten Patenten den Neuheitscharakter abzusprechen. Diese Art der Recherche wird vorrangig dann verwendet, wenn der Verdacht besteht, dass ein anderes Patent gegen das eigene verstößt. Der Einspruch muss dabei während der Einspruchsfrist, welche neun Monate beträgt, erfolgen.

4.1.3 Welche Recherche?

Welche Art der Recherche erfolgen sollte, ist nach [2] von der Fragestellung, den Ausgangsinformationen und dem Ergebnisziel abhängig. Beispielsweise sollte bei der Fragestellung „Welche Veröffentlichungen lassen sich einem bestimmten Erfinder zuordnen?“ eine Namensrecherche durchgeführt werden. Ist das Ziel hingegen, ein Patent anzumelden, bietet es sich an, mit einer Neuheitsrecherche zu prüfen, ob bereits ähnliche Patente angemeldet sind. Einen sehr umfangreichen Überblick darüber liefert.

4.2 Recherchemöglichkeiten

Es existieren verschiedene Möglichkeiten, eine Patentrecherche durchzuführen. Welche Recherche zu bevorzugen ist, ist vom Anwendungsbereich abhängig.

Um sich einen kurzen Überblick zu verschaffen, einfache Fragen zu beantworten und Einzeldokumente herunterzuladen, bietet sich das Internet als erste Anlaufstelle an [1]. In [11] wird jedoch darauf hingewiesen, dass die Recherche im Internet keineswegs die professionelle Patentrecherche ersetzt.

Eine tiefergehende Patentrecherche kann kostenlos in einem Recherchesaal in einem Patentamt durchgeführt werden. Dabei steht sowohl eine umfangreiche Fachbibliothek, als auch eine kostenlose sachkundige Unterstützung bei der Recherche zur Verfügung [5].

Außerdem bieten eigens dafür spezialisierte Institute gegen Gebühr an, Recherchetätigkeiten auszuführen [7].

4.3 Patentdatenbanken

In [16] wird ein Überblick für Patentdatenbanken gegeben. Mittels Patentdatenbanken kann (meist kostenlos) auf Patentschriften und bibliographische Daten zugegriffen werden. Eine Patentrecherche startet meist mit der Nutzung von Patentdatenbanken, da der Zugang weitestgehend über das Internet erfolgt und somit mit vergleichsweise geringem Aufwand und wenig Kosten verbunden ist. Gegenwärtig existieren weltweit mehr als 100 Datenbanken, welche für eine Patentrecherche genutzt werden können.

Im Folgenden soll ein Überblick über die beiden bedeutendsten Patentdatenbanken (esp@cenet für europäische Patente und depatisnet vorrangig für deutsche Patente) gegeben und diese Datenbanken bewertet werden. Weitere Datenbanken werden aufgelistet, jedoch nicht beschrieben.

4.3.1 esp@cenet

Bei esp@cenet handelt es sich um die weltweit umfangreichste Patentdatenbank [1]. Sie ist unter [17] abrufbar und bietet einen kostenlosen Zugriff auf über 60 Millionen Patentdokumente aus aller Welt [18].

Wie unter [18] beschrieben, werden im Folgenden die fünf verschiedenen Suchmodi skizziert. Der *SmartSearch*-Modus ermöglicht eine Ein- oder Mehrwortsuche sowie komplexe Abfragen auf Basis von logischen Verknüpfungen. Mit der *Kurzsuche* kann eine einfache Suche anhand eines Schlagwortes, eines Erfinders oder einer Firma durchgeführt werden. Die *erweiterte Suchfunktion* ermöglicht das Verknüpfen von verschiedenen Begriffen. Beispielsweise kann nach Patentdokumenten aus einem bestimmten Jahr gesucht werden, welche im Titel gewisse Wörter enthalten. Mit der *Nummernsuche* lassen sich Patente, von denen die Anmelde- oder Veröffentlichungsnummer bekannt ist, schnell finden. Mit der *Klassifikationssuche* können sämtliche Patentdokumente eines bestimmten Gebietes durchsucht werden. Letztere Suche erfordert eine verhältnismäßig lange Einarbeitungszeit.

In Abbildung 2 ist ein Beispiel eines Suchergebnisses dargestellt. Dabei wurde die SmartSearch-Suche benutzt und nach dem Begriff „Reifen“ gesucht. Das zweite Suchergebnis lieferte das abgebildete Patent. Als „Startseite“ werden sämtliche biographischen Daten angezeigt. Die komplette Patentschrift kann als Portable Document Format (PDF)-Datei heruntergeladen werden.

In [1] wird die Patentdatenbank esp@cenet folgendermaßen bewertet:
Neben der hohen Anzahl an verfügbaren Patenten besteht ein weiterer Vorteil von esp@cenet darin, dass sich nicht nur erteilte Patente, sondern auch Patentanmeldungen einsehen

doi: 10.2313/NET-2011-07-2_02

Abbildung 2: Beispiel Suchergebnis esp@cenet [17]

lassen. Die Dokumente sind im Normalfall bereits 14 Tage nach ihrer Publikation verfügbar. Aus diesem Grund eignet sich esp@cenet besonders gut für die Überwachung von Schutzrechten.

Als Schwachstellen von esp@cenet können die eingeschränkte Stichwortsuche (einige Patentschriften können nur über den Titel oder die IPC-Nummer gefunden werden) und das Fehlen von statistischen Auswertungen angesehen werden. Im Weiteren lassen sich mit esp@cenet lediglich 500 Suchergebnisse anzeigen.

4.3.2 Depatisnet

Die Datenbank depatisnet ist unter [12] abrufbar. Im Folgenden wird die Vorgehensweise nach [19] beschrieben. Bei depatisnet handelt es sich um die weltweit zweitgrößte Patentdatenbank mit ca. 41 Millionen Einträgen. Da depatisnet vom Deutschen Patent- und Markenamt entwickelt wurde, sollte sie als erste Anlaufstelle für deutsche Patente genutzt werden. Darüber hinaus existieren in dieser Datenbank viele Einträge aus anderen Ländern.

Depatisnet ermöglicht die Nutzung von fünf verschiedenen Suchmodi mit den Namen Einsteiger, Experte, IKOFax, Familie und PIZ (Patentinformationszentrum)-Unterstützung zur Formulierung von Suchanfragen. Mit dem *Einsteigermodus* kann nach Veröffentlichungsnummer, Titel, Anmelder, Erfinder, Veröffentlichungsdatum, Internationaler Patentklassifkation oder im Volltext gesucht werden. Im *Expertenmodus* können Suchanfragen, die mit logischen Operatoren verknüpft sind, erstellt werden. Der *IKOFax*-Modus verwendet eine eigene Syntax zur Formulierung von Suchanfragen. Dieser Modus ist besonders flexibel, erfordert allerdings eine gewisse Einarbeitungszeit. In Listing 1 und Listing 2 werden beispielhafte Anfragen dargestellt.

Listing 1: einfache IKOFax-Abfrage

```
[Auto](5W)[Reifen]
```

Listing 1 liefert sämtliche Suchergebnisse, worin die Patentschrift die Begriffe „Auto“ und „Reifen“ enthalten sind mit der zusätzlichen Bedingung, dass zwischen Auto und Reifen maximal fünf Wörter stehen .

Listing 2: komplexe IKOFax-Abfrage

```
CH/PC
AND 2001 >= /PY >= 1999
AND B23H? /ICM
```

Die Anfrage in Listing 2 ist etwas komplexer. In der ersten Zeile wird das Suchergebnis auf sämtliche schweizer Dokumente eingeschränkt (Syntax: Länderkürzel/PC) und zudem werden nur Veröffentlichungen von den Jahren 1999, 2000 und 2001 betrachtet (Syntax: bis_Jahr >/>= /PY >/>= von_Jahr). Mit der letzten Zeile wird die Suche weiter eingeschränkt, indem nur Patente aus der IPC-Hauptklasse B23H betrachtet werden (Syntax: Hauptklasse? /ICM). Das ? dient dabei als Wildcard. Es werden also sämtliche Unterklassen der Hauptklasse B23H betrachtet. Die einzelnen Suchanfragen werden mit einer logischen UND-Verknüpfung (AND) verbunden, womit nur Ergebnisse aufgelistet werden, die sämtliche Bedingungen erfüllen. Eine ausführliche Referenz zum IKOFax-Modus ist unter [20] zu finden. Mittels einer *Patentfamilienrecherche* können sämtliche Patente, die zur selben Familie gehören, ermittelt werden. Dafür ist es notwendig, die Veröffentlichungsnummer zu kennen. Sollte ein User Probleme bei der Erstellung von Anfragen haben, so kann mithilfe der *PIZ-Unterstützung* eine (syntax)freie Anfrage gestellt werden. Ein Mitarbeiter des Patent- und Markenamtes hilft im Rahmen einer Erstunterstützung dem User kostenlos. Anfragen, deren Bearbeitung über die Erstunterstützung hinausgehen, sind allerdings kostenpflichtig.

Die Stärken und Schwächen können nach [1] folgendermaßen zusammengefasst werden.
Eine Stärke von depatisnet ist, dass die (deutschen) Dokumente sehr schnell nach der Publikation erhältlich sind. Als weiterer Vorteil kann die IKOFax-Syntax angesehen werden mit welcher sehr mächtige Anfragen erstellt werden können. Auch mit depatisnet lassen sich Patente im PDF-Format herunterladen.

Als Schwachpunkt kann die Anzahl an Patenten, welche sich in der depatisnet-Datenbank befinden, betrachtet werden. Es sind, verglichen mit esp@cenet, deutlich weniger. Zudem sind Vorkenntnisse in IKOFax notwendig, um die Suche effizient zu gestalten.

4.3.3 Weitere Datenbanken

Generell empfiehlt es sich (besonders aufgrund des Prioritätsrechtes), Datenbanken von verschiedenen Ländern zu

doi: 10.2313/NET-2011-07-2_02

durchsuchen. In Tabelle 2 werden einige weitere Patentdatenbanken aufgelistet.

Tabelle 2: Übersicht Patentdatenbanken [1]

Beschreibung	Internetadresse
Schweizer Patente	http://www.swissreg.ch
Österreichische Patente	http://at.esp@cenet.com
US Patente	http://patft.uspto.gov
WIPO (World Intellectual Property Organisation) - weltweit, jedoch nur Bibliographien, Zeichnungen und Abstracts	http://www.wipo.int/pctdb/en

4.4 Herausforderungen

In dieser Arbeit wurde verdeutlicht, dass eine Patentrecherche keineswegs unterschätzt werden sollte. Dabei muss mit zahlreichen Herausforderungen umgegangen werden, welche im Folgenden beschrieben werden.

Bereits im Jahre 2005 umfasste die internationale Patentliteratur mehr als 40 Millionen Dokumente. Das Wachstum wurde damals mit 800.000 Dokumenten pro Jahr geschätzt [2]. Das tatsächliche Wachstum wurde damit stark unterschätzt, da sich 2009 bereits 60 Millionen Dokumente in der esp@cenet-Datenbank befanden [18]. Aus diesem Grund stellt es eine große Herausforderung dar, in diesen Unmengen von Literatur die relevanten Schriften zu filtern. Eine Hilfestellung kann dabei die Einschränkung der Suche auf bestimmte Kategorien bewirken.

Patentdatenbanken liefern zudem als Suchergebnis sämtliche Wörter, worin sich das Schlüsselwort befindet. Gibt man beispielsweise als Schlüsselwort „Auto“ ein, so werden auch Ergebnisse, die „automatisch“ oder „Autokorrektur“ beinhalten, angezeigt. Auch diesem Problem kann mit einer Beschränkung der Suche auf bestimmte Gruppen und/oder der Nutzung einer mächtigen Abfragesprache wie IKOFax Abhilfe geschaffen werden.

Generell wurde die Patentrecherche zwar durch die zunehmende Digitalisierung vereinfacht, jedoch sind noch nicht alle Patente in einem recherchierbaren Format wie XML (Extensible Markup Language) oder PDF abgespeichert. Patente, welche in einem nicht-recherchierbaren Format abgespeichert sind, sind nur mit einem großen Aufwand zu analysieren. Dabei ist anzumerken, dass dieses Problem zwar derzeit noch relevant ist, jedoch zunehmend an Bedeutung verliert, da sämtliche neu ausgestellte Patente digitalisiert werden.

Ein weiteres Problem stellt nach [7] die Sprache dar. Ein Patent kann in der jeweiligen Landessprache angemeldet werden. Sollte in der Patentabteilung jedoch niemand dieser Sprache mächtig sein, so kann diesem Patent keine Beachtung geschenkt werden, da unter anderem die relevanten Suchbegriffe unbekannt sind. Innerhalb der Prioritätsfrist kann dieses Patent jedoch in anderen Ländern nachträglich angemeldet werden und in der jeweiligen Sprache innerhalb von 3 Monaten nachgereicht werden. Diese Problematik ist besonders bei sehr schnelllebigen Entwicklungen zu berücksichtigen.

Neben einem Fachverständnis für das jeweilige Gebiet, welches recherchiert werden soll, erfordert eine Patentrecherche auch ein Verständnis über die sprachliche Eigenart von Patentschriften. So existieren in der Patentliteraturen unübliche Konstruktionen, um etwa eine Generalisierung eines Patentanspruches zu erreichen. Es kann beispielsweise eine „Mausefalle“ mit „Vorrichtung zur Festsetzung von Nagern“ umschrieben werden. Dabei sagt letztere Umschreibung nichts über die Gattung der Nager aus. Daher sollte nach [2] eine Suchanfrage immer auf verschiedene Arten beschrieben und mit logischen Operatoren verknüpft werden.

Darüber hinaus erfordert eine Patentrecherche im Internet eine gewisse Einarbeitungszeit, um beispielsweise die spezielle Syntax der einzelnen Datenbanken zu erlernen.

5. ZUSAMMENFASSUNG

Der Nutzung von Patentliteratur wird immer noch eine zu geringe Beachtung geschenkt. Dabei wurde gezeigt, dass die Patentrecherche zusammen mit einer Bewertung in vielen verschiedenen Bereichen essenziell ist. Wird keine oder nur eine unzureichende Recherche betrieben, so kann dies zu hohen Kosten durch Rechtsverstöße oder Doppelentwicklungen führen.

Die Patentanalyse ist eng mit der Patentrecherche verknüpft. Welche konkrete Vorgehensweise sich hierfür empfiehlt, kann nicht generalisiert werden, da dies von unterschiedlichen Faktoren abhängig ist. Dazu gehören beispielsweise das Anwendungsgebiet und die Anzahl der Patente in einem durch die Patentklassifikation beschränkten Bereich. Eine Voraussetzung für eine zielführende Recherche ist jedoch ein grundlegendes Verständnis von Patenten und ein breites Grundwissen über den jeweiligen Fachbereich. Dieses Wissen lässt sich unter anderem durch Literatur oder durch eine grobe Patentrecherche aneignen. Anschließend kann eine Patentanalyse durchgeführt werden, wobei hier mehrere Indikatoren betrachtet werden sollten. Im Anschluss dazu empfiehlt sich eine detaillierte Patentrecherche, die sich auf die in der Analyse identifizierten relevanten Dokumente beschränkt.

Auf den ersten Blick mag eine Patentrecherche durch die Digitalisierung der meisten Patente sehr einfach wirken. Es wurde jedoch in dieser Arbeit gezeigt, dass eine solche Recherche zusammen mit einer Bewertung eine große Herausforderung darstellt und mit sehr viel Aufwand verbunden ist. Der Umgang mit den riesigen Datenmengen, vielen verschiedenen Datenbanken, teilweise fehlenden Standards, Fehler in den Patentschriften und sprachliche Barrieren erschweren die Recherche maßgeblich. Zudem kann eine umfassende Analyse nur teilweise automatisiert werden, womit der personelle Aufwand entscheidend steigt. Es sei davon insbesondere bei wichtigen Entscheidungen davon abgeraten, eine Recherche lediglich über das Internet zu führen. Es sollten hierfür unbedingt Experten in Patentämtern oder einschlägige Institute konsultiert werden.

doi: 10.2313/NET-2011-07-2_02

Trotz der hohen Komplexität und den damit verbundenen Kosten sollten umfangreiche und professionelle Patentrecherchen in vielen unterschiedlichen Situationen durchgeführt werden. Der dadurch entstehende langfristige Gewinn übersteigt die Kosten üblicherweise um ein Vielfaches.

6. LITERATUR

[1] Gassmann, O., Bader, M. Patentmanagement, August 2005. ISBN: 354068729.

[2] Wurzer, A., Jäger, G. Handbuch für Patentrecherche - Innovation durch Patentinformation, Mai 2005.

[3] Charles, G. Schutz von geistigem Eigentum.

[4] Bundesministerium der Justiz. Patentgesetz, 1936.

[5] Deutsches Patent- und Markenamt. Patente, Gebrauchsmuster, Marken, Geschmacksmuster im Überblick, 2011.

[6] Schramm, R. Einführung in das Patentwesen, 2010.

[7] Schwarz, C. Schutz von Erfindungen durch Patente und Gebrauchsmuster, 2010.

[8] Krieger, H. Richtlinien für die Durchführung der Druckschriftenermittlung nach §43 PatG. http://transpatent.com/gesetze/patrecrl.html, , zugegriffen am 23.04.2011.

[9] WIPO. WIPO-Administered Treaties. http://www.wipo.int/treaties/en/ShowResults.jsp, zugegriffen am 23.04.2011.

[10] Ensthaler, J., Strübbe, K. Patentbewertung - Ein Praxisleitfaden zum Patentmanagement, 2006. ISBN: 3-540-34413-6.

[11] Slaby, S. Online Recherche in Patentdatenbanken, Oktober 2005.

[12] Deutsches Patent- und Markenamt. DEPATISnet. http://depatisnet.dpma.de, zugegriffen am 23.04.2011.

[13] Bartowski, A. Grundlagen der Patentanalyse, 2010.

[14] Thomä, E. Leitfaden für Patentrecherchen mit STN Easy, 2005.

[15] Thomson. Delphion - an overview of Delpion Features, 2004.

[16] Ensthaler, J. Gewerblicher Rechtsschutz und Urheberrecht, Januar 2009. ISBN: 3540435670.

[17] Europäisches Patentamt. espacenet. http://esp.espacenet.com, zugegriffen am 23.04.2011.

[18] Europäisches Patentamt. Einführung in die Datenbank der Ideen, August 2009.

[19] Deutsches Patent- und Markenamt. DEPATISnet - Weltweite Patentrecherche zum Stand der Technik, Juli 2010.

[20] Deutsches Patent- und Markenamt. IKOFAX-Recherche. http://depatisnet.dpma.de/depatisnet/htdocs/prod/de/hilfe/recherchemodi/ikofax-recherche/index.html, zugegriffen am 23.04.2011.

doi: 10.2313/NET-2011-07-2_02

Dienstgüte-Unterstützung für zukünftige Netze

Tobias B. Hlavka
Betreuer: Dr. Heiko Niedermayer
Seminar Future Internet SS2011
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
E-Mail: tobias.hlavka@in.tum.de

KURZFASSUNG

Quality of Service (QoS) ist als Merkmal für das Internet und für das zukünftige Internet von großer Bedeutung. Quality of Service umfasst die Merkmale Bandbreite, Latenz, Jitter und Paketverlust. Es ist momentan in Form des ToS-Headers in IPv4 vorgesehen. Die Arbeit zeigt, wie Differentiated Services nach nach Umdefinierung dieses Headers funktioniert. So ermöglicht es eine genauere Aufteilung in Verkehrsklassen, die in Behaviour Aggregates zusammengefasst werden und einem fest definierten Per-Hop-Behaviour unterliegen. Neben QoS kann für eine gute Netzperformance auch eine Überdimensionierung (Overprovisioning) stattfinden, was zunächst als einfacher Umsetzbar erscheint. In jedem Fall muss entschieden werden, wann eine Denial-of-Service-Situation vorliegt und wie und ob QoS-Maßnahmen in den Entwurf für ein Future Internet aufgenommen werden müssen.

Schlüsselworte

Future Internet, Quality of Service (QoS), Dienstgüte, DiffServ, Differentiated Services, Overprovisioning

1. EINLEITUNG

Keshav erkannte bereits 1997:

> „The Holy Grail of computer networking is to design a network that has the flexibility and low cost of the Internet, yet offers the end-to-end quality-of-service guarantees of the telephone network.“ [1] [9]

Diese Feststellung zeigt, dass der Gedanke eines internetartigen Netzwerks mit Unterstützung für Quality-of-Service (QoS) keineswegs neu ist. Aus wirtschaftlichen Gründen fragt sich die Branche seit Jahren, ob es möglich ist, ein höher priorisiertes „Netz im Netz“ zu schaffen - natürlich gegen Entgelt. Oder ist dafür nicht doch eine ganz neue Netzstruktur abseits des in die Jahre gekommenen WWW notwendig? Immer neue Anwendungen für das Internet lassen diese Idee plausibel erscheinen. Es entstehen Consumer-Dienste, die nach hoher Bandbreite verlangen (z.B. YouTube), aber auch kommerzielle Anwendungen wie beispielsweise Fern-Operationen durch Spezialärzte und über das Internet ferngesteuerte Roboter, welche nach äußerst ausfallsicheren Leitungen mit geringer Latenz verlangen. Andererseits ist es fraglich, ob eine solche Dienstgüteunterstützung - und damit die Aufteilung der Daten in verschiedene Klassen - überhaupt wünschenswert ist. Es darf bezweifelt werden, dass sich das WWW zu dem entwickelt hätte, was es heute ist, wenn eine solche Klassifizierung von Anfang an nach monetären Aspekten erfolgt wäre. Dies soll neben den Fragen, ob Dienstgüteunterstützung für ein „Future Internet“ überhaupt benötigt wird und wie diese QoS-Maßnahmen technisch realisiert werden könnten, im Folgenden geklärt werden.

Der zweite Abschnitt soll zeigen, um was es sich bei QoS überhaupt handelt. Dazu wird zunächst eine Definition der QoS-Parameter gegeben. Es wird erklärt, wie QoS heute in den IP-Headern verankert ist.

Der dritte Abschnitt beschäftigt sich mit der konkreten technischen Maßnahme DiffServ. Es wird eine Übersicht über die Grundsätze von DiffServ, dessen Architektur und den DiffServ Codepoint gegeben. Danach werden die verschiedenen Per-Hop-Behaviours erklärt und gegenübergestellt. Schließlich wird aufgezeigt, in welchen Gebieten DiffServ als Methode geeignet ist, QoS zu implementieren, es wird die Alternative IntServ betrachtet und eine Bewertung beider Techniken vorgenommen.

Im vierten Abschnitt wird betrachtet, inwiefern Overprovisioning QoS überflüssig machen könnte.

Welche Art von Attacken auf ein QoS-unterstüzendes Netzwerk abzielen könnten, wird in Sektion fünf aufgeklärt.

In Abschnitt sechs wird geklärt, inwiefern QoS im Future Internet von Relavanz ist.

2. QUALITY OF SERVICE ALS ANFORDERUNG FÜR ZUKÜNFTIGE NETZE

QoS ist eine der wesentlichen Gesichtspunkte bei der Gestaltung zukünftiger Netze. Dieser Abschnitt definiert zunächst QoS und zeigt die Merkmale auf, auf die QoS-Strategien angewendet werden können. Danach wird die momentane Situation von Dienstgüteunterstützung für das jetzige Internet aufgezeigt.

2.1 Was bedeutet QoS

Generell bedeutet QoS, ein bestimmtes Service Level Agreement (SLA) zu erfüllen. Dieses SLA bezieht sich auf die Qualität der Datenverbindung und kann zwischen zwei Providern oder zwischen Provider und Endkunde abgeschlossen

[1] etwa: „Der heilige Gral der Computernetze ist es, ein Netzwerk zu entwerfen, das so flexibel und preiswert wie das Internet ist, jedoch zugleich die vom Telefonnetz bekannten Dienstgüte-Garantien für Punkt-zu-Punkt-Verbindungen bietet.“ (Übers. d. Autors)

doi: 10.2313/NET-2011-07-2_03

werden. Im Allgemeinen werden dort folgende Parameter mithilfe von Kennzahlen für die jeweilige Qualitätsstufe fixiert:

1. Bandbreite: Beschreibt eine Mindestdatenrate, die für eine bestimmte Klasse von Datenverkehr garantiert werden muss
2. Latenz: Höchste Verzögerung, mit der ein Datenpaket einer bestimmten Klasse von Datenverkehr ausgeliefert wird
3. Jitter: Größte Schwankungsbreite der Latenz einer bestimmten Klasse von Datenverkehr
4. Paketverlust: Das Verhältnis von verlorenen Paketen zu gesendeten Pakete einer bestimmten Klasse von Datenverkehr

Diese Punkte lassen sich auf eine anschauliche Analogie zum Straßenverkehr übertragen, womit das Beispiel von Bricklin [3] noch erweitert werden soll: Im Falle von hohem Verkehrsaufkommen ist es zuerst einmal notwendig, Staus zu vermeiden und einen befahrbaren Weg für hoch priorisierten Verkehr, wie Feuerwehr, Notarzt und Polizei freizuhalten. Dies passiert entweder mit speziell reservierten Spuren für solchen Notfallverkehr, oder eben einer ausreichenden Anzahl an Fahrspuren (1). Verspätungen (2) sollen verhindert werden. Das wird in der realen Welt durch geeignete Lichtsignale, insbesondere Blaulicht, erreicht. Ebenso will man größere Unregelmäßigkeiten im Straßenverkehr vermeiden, man sollte für die gleiche Strecke zu unterschiedlichen Zeitpunkten gleich lang unterwegs sein (3). Die Unfallrate (4) muss natürlich niedrig gehalten werden, sowohl für allgemeinen Verkehr, aber auch für den priorisierten Blaulichtverkehr. Dies wird dadurch erreicht, dass alle anderen Verkehrsteilnehmer darauf konditioniert wurden, Blaulichtverkehr zu beachten. Diese Beachtung kann beispielsweise in Form von Bremsen und an den Rand der Fahrbahn fahren erfolgen, oder darin bestehen eine Abfahrt zu nehmen und die Straße zu verlassen, unter Umständen mit der Prämisse, das Ziel nicht oder nur verspätet zu erreichen. Es deutet sich hier schon an, dass alle diese Dienstgüteunterstützungsmaßnahmen überhaupt nur dann notwendig sind, wenn die vorhandene Straßen- bzw. Leitungskapzität nicht ausreicht. Eine solche QoS-Sicherung ist bei bestimmten Netzwerkanwendungen unabdingbar. Hier sind besonders zeitkritische Anwendungen zu nennen, die sich von Spezialgebieten wie Business-Prozessen bis zu Consumer-Themen wie Voice-over-IP erstrecken. Hohe Latenzen würden diese Verfahren ad absurdum führen. Andererseits muss auch beachtet werden, dass für einen großen Teil von Netzwerkanwendungen eine Einführung von QoS nicht notwendig ist. Generell gesagt ist das für alle diejenigen Anwendungen der Fall, deren Funktion nicht zeitlich vom Eintreffen bestimmter Pakete zu genau definierten Zeitpunkten im Kommunikationsprozess abhängig ist. Das bedeutet konkreter, dass Video-on-Demand-Portale wie YouTube, oder auch asynchrone Kommunikationsmittel wie E-Mail nicht unmittelbar von QoS profitieren, da sowohl Zeit- als auch Datenpuffer vorhanden sind.

2.2 Status Quo - QoS heute

Ansätze, um QoS in den Netzwerkverkehr zu integrieren, gab es bereits mit IPv4. IPv4 sieht in dieser Hinsicht das so genannten Type-of-Service (ToS)-Byte im Header vor. Dieses Byte ist wie in Tabelle 1 dargestellt aufgebaut.

Tabelle 1: Aufbau des IPv4 ToS-Byte [4]

Bit Nr.	0	1	2	3	4	5	6	7
Bedeutung	Priorität			Type of Service				Null

Somit ist es bereits mit IPv4 möglich, verschiedene Prioritäten wie „Immediate“ oder „Routine“ in Bit 0 bis 2 festzulegen, die im Wesentlichen an den Netzgrenzen berücksichtigt werden. Je kleiner die Priorität, desto eher darf ein Paket bei hoher Auslastung bzw. Überlastung verworfen werden um Freiraum für höher priorisierte Pakete zu schaffen. Eine weitere Klassifizierung erfolgt anhand der ToS-Bits 3 bis 6. Hier können grobe Einteilungen wie zum Beispiel „minimize monetary cost“ oder „maximize throughput“ festgelegt werden. Es muss hier also eine Abwägung stattfinden zwischen Durchsatz, Verzögerung, Zuverlässigkeit und Kosten [2]. Das letzte Bit blieb unbenutzt und muss, um ToS-konform zu sein, null sein. Für detaillierte Belegungsmöglichkeiten und resultierende Bedeutungen siehe [4]. An dieser Stelle reicht es aus, zu verstehen, dass bereits ein Klassifizierungsbyte im Header vorgesehen ist und dass dieses auch bereits mit konkreten Bedeutungen belegt ist. Das gilt es zu beachten, wenn versucht wird, für IPv4 eine neue Struktur für QoS zu schaffen.
Warum hat nun dieses ToS-Byte nicht ausgereicht um eine skalierbare QoS-Infrastruktur zu schaffen? Wieso wird ein neuer Ansatz benötigt? Dafür gibt es nach [4] mehrere Gründe:
Die Prioritäten- und Type-of-Service-Bits sind nicht flexibel genug. Sie erlauben lediglich eine Angabe der Priorität und des ToS relativ zu anderen Klassen. Absolute Angaben sind nicht möglich. Dazu kommt, dass sich keine Festlegung treffen lässt, wie Traffic in der gleichen Klasse, jedoch mit unterschiedlichem Inhalt, im Falle einer hohen Last behandelt wird. Werden beispielsweise HTTP und SSH in die gleiche Klasse eingeordnet, welcher Service wird dann zuerst fallengelassen? Es sollte möglich sein, hier eine Unterscheidung treffen zu können, damit beispielsweise wichtiger Geschäftsverkehr (HTTP) höherwertiger behandelt wird als die SSH-Session eines internen Benutzers.
Darüber hinaus gibt es zu wenige Prioritätenklassen. Da nur drei Bit dafür reserviert sind, ergeben sich $2^3 = 8$ Prioritätenklassen, wovon zwei aber schon für interne Router-Nachrichten reserviert sind, die zugleich als höchstpriorisiert behandelt werden, damit auch im High-Traffic-Fall auf jeden Fall die Netzwerkknoten untereinander kommunizieren können.
Schließlich halten sich die Hersteller in ihren Implementierungen nicht an die Bit-Definitionen im ToS-Feld, sodass hier sehr uneinheitliche Implementierungen entstanden sind. Darüber hinaus wurden die Bits in RFC 1349 [2] neu definiert, was zu zusätzlichen Überschneidungen geführt hat. Folglich ist ein Clean-Slate-Ansatz nötig geworden.
Es besteht zusätzlich das Problem, dass mit den gegebenen Mitteln QoS nur auf flow-Basis definiert werden kann. Ein flow ist ein einzelner Datenstrom. Er besteht aus dem 5-Tupel (Quell-IP-Adresse; Quell-Portnummer; Ziel-IP-

doi: 10.2313/NET-2011-07-2_03

Adresse; Ziel-Portnummer; Protokoll [UDP / TCP]) [4]. Diese sehr feingranulare Einteilung ermöglicht natürlich sehr exakte QoS-Vorgaben auf Paketbasis. Dies scheint durchaus implementierbar in kleineren Netzverbänden und an Routern mit mäßigem Traffic, denn zur Berücksichtigung der QoS-Richtlinen müssen beim Eintreffen des Pakets verschiedene Tests und Berechnungen durchgeführt werden. Dies wiederum kostet Zeit, was die Latenz bei höherem Datenaufkommen empfindlich steigern kann. Dies würde genau dem Gedanken des Verfügbarmachens von QoS widersprechen! Man mag sagen, an den Blättern des Netzes ließe sich auch das noch durch gesteigerte Rechenkraft ausgleichen. Jedoch spätestens bei Betrachtung der zentralen Backbones des Internets mit einer Anzahl von flows in vielfach höherer Größenordnung ist diese Methode nicht mehr praktikabel. Um also eine angemessene Skalierbarkeit der QoS-Maßnahmen herzustellen, müssen die flows in irgendeiner Form zusammengefasst und somit gleich zu behandelnder Traffic in gröber eingeteilten Klassen aggregiert werden. So kann eine deutliche Senkung des Overheads in den Netzknoten erreicht werden und der ganze Prozess des QoS kostet nicht übermäßig unmittelbare Rechenleistung.

3. FALLBEISPIEL DIFFERENTIATED SERVICES

In diesem Abschnitt wird zunächst DiffServ als Technik zur Umsetzung von QoS-Maßnahmen definiert und erklärt. Danach wird geklärt, wo es sich einsetzen lässt und wie dies zu Future Internet Ansätzen passt. Schließlich erfolgt noch eine kurze Darstellung von Alternativen zu DiffServ und eine vergleichende Bewertung.

3.1 Definition DiffServ / DSCP

Differentiated Services (DiffServ) wurde von der IETF[2] entworfen, wobei das Hauptaugenmerk auf Skalierbarkeit gelegt wurde. Man hat also den konsequenten Schritt gemacht, statt auf feingranularer flow-Basis, die QoS-Maßnahmen auf einer Aggregat-Basis anzuwenden. Es werden daher gleichartige Pakete zu gemeinsamen Klassen von Netzwerkverkehr zusammengefasst. So kann das Netz an sich in den Knoten recht simpel und kostengünstig gehalten werden, während die komplexeren Berechnungen und Klassifikationen an den Netzgrenzen und -blättern vorgenommen werden. Der strukturelle Aufbau des Differentiated Services Codepoints (DSCP), welcher Bit 0 bis 5 im IPv4-ToS-Byte umfasst, ist in Tabelle 2 dargestellt.

Tabelle 2: Das DiffServ Codepoint Field (nach [4])

Bit Nr.	0	1	2	3	4	5	6	7
DS-Feld	Class Selector CP						ungenutzt	
	Differentiated Services Codepoint							

Das ursprüngliche Type-of-Service-Byte wurde vollständig umdefiniert. Die ToS-Prioritäten-Bits wurden mit den weiteren Bits zusammengelegt. So festgelegt in [10], gibt es nun 2^6 Möglichkeiten, Pakete zu klassifizieren. Dies stellt eine großen Sprung zum alten ToS-Byte dar. Wichtig bei der Betrachtung dieser Neudefinition ist, dass die für DSCP definierten Bit-Sequenzen in den ersten drei Bits deckungs- und bedeutungsgleich mit der alten Definition sind. Das heißt, dass diese Technik soweit abwärtskompatibel ist, dass diejenigen Router, welche ToS-Markierungen unterstützen, weitergenutzt werden können und mit den neuen DSCP-fähigen Routern zusammenarbeiten. Das in der Tabelle gezeigte Sextett bestimmt das sogenannte Per-Hop-Behaviour, welchem die Pakete an den Netzknoten unterliegen.
Analog zur IPv4-Umdefinierung ist QoS mit Hilfe von DiffServ auch in IPv6 möglich. Dort wird die Markierung im Traffic-Class-Byte vorgenommen [10]. Die generelle Funktionsweise von DiffServ ist unabhängig davon, ob IPv4 oder IPv6 eingesetzt wird.

[2]Internet Engineering Taskforce

3.2 Aufbau der Netzstruktur mit DiffServ

Wie in Abbildung 1 dargestellt, besteht eine DiffServ-Domäne für gewöhnlich aus einer einzelnen Administrationseinheit. Innerhalb derer bestehen fest definierte Service Level Agreements, deren Einhaltung als sicher gilt. Besonders zu beachten sind hier die Eingangs- und Ausgangsknoten.

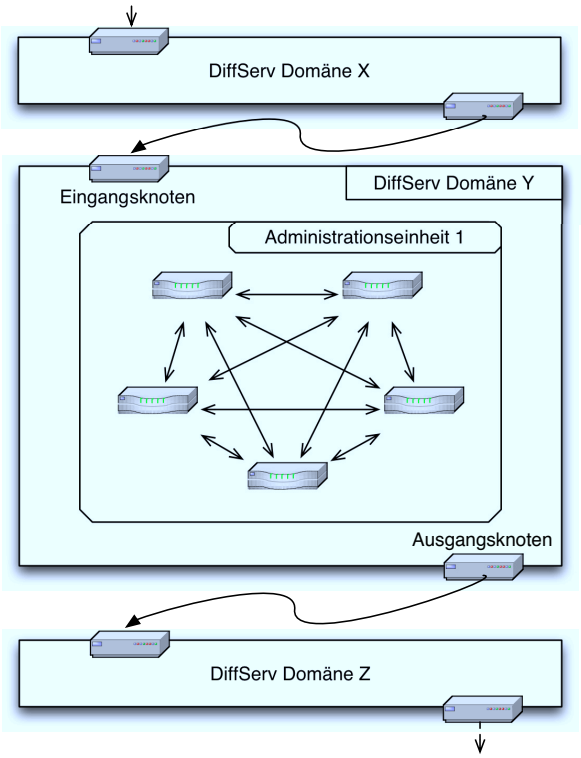


Abbildung 1: Die Architektur von DiffServ

3.2.1 Knoten innerhalb einer DS-Domäne

Die Knoten innerhalb einer Domäne können haben hauptsächlich zwei Aufgaben. Die erste Aufgabe ist das Klassifizieren und Auslesen der Codepoints. Dies beschränkt sich innerhalb einer Administrationseinheit auf das Auslesen des DSCP, denn hier herrschen übereinstimmende SLAs zwischen den Routern. Die zweite Aufgabe ist das Weiterleiten der Pakete innerhalb der DS-Domäne anhand der zuvor ausgelesenen Kriterien passend zu den vereinbarten Per-Hop-Behaviours (siehe Abschnitt 3.3).

doi: 10.2313/NET-2011-07-2_03

3.2.2 *Ein- und Ausgansknoten außerhalb einer DS-Domäne*

Diese Knoten werden auch als Grenzknoten (Boundary Nodes) bezeichnet. Sie verbinden entweder zwei DiffServ-Domänen miteinander oder aber eine DiffServ-Domäne mit einem anderen Netz, das kein DiffServ unterstützt. Diese Knoten haben neben der Klassifizierung und Weiterleitung noch die Aufgaben der Markierung und Überwachung. Ein Markieren muss immer dann stattfinden, wenn Pakete aus nicht-DiffServ-Netzen eintreffen. Dabei wird je nach geltenden SLAs eine DiffServ Codepoint zugeordnet, der dann das Verhalten definiert, welches innerhalb der Domäne auf das Paket oder das Behaviour Aggregate angewandt wird. Die Überwachung spiegelt sich in der Form wider, dass über Traffic-Shaping-Maßnahmen sichergestellt werden muss, dass die definierten QoS-Anforderungen erfüllt werden können. Abbildung 2 zeigt den typischen Aufbau dieses DiffServ Traffic Conditioner Block (TCB) [4], in dem die genannten Maßnahmen umgesetzt werden.

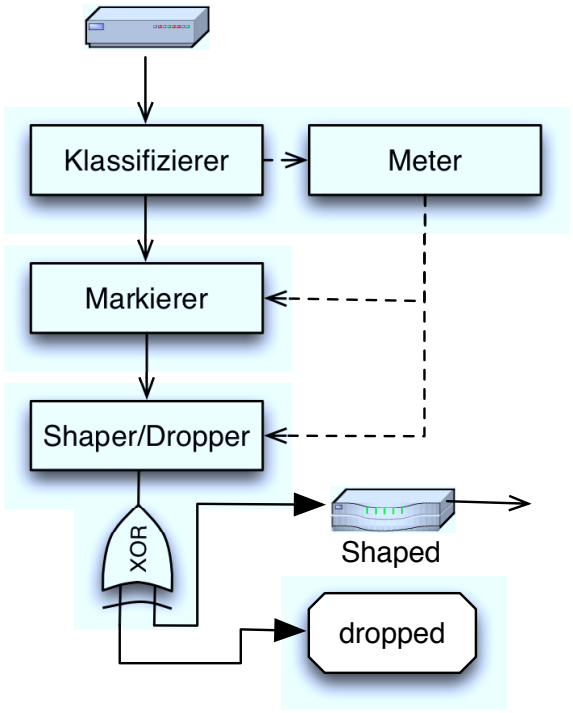


Abbildung 2: Der DiffServ Traffic Conditioner Block

Der Klassifizierer liest hier die DSCPs aus und stellt gegebenenfalls Behaviour Aggregates zusammen. Falls noch kein DSCP festgelegt ist, wird dies durch den Markierer nach der vom Klassifizierer festgestellten Klasse angelegt. Das Meter-Modul fungiert hier als eine Kontrollinstanz, die überprüft, ob der markierte eintreffende Datenstrom auch zu der Klasse gehört, die er im DSCP vorgibt zu sein. Passen Markierung und Pakettyp nicht zusammen, wird es im Shaper entweder einer anderen Klasse zugeordnet (das heißt der DSCP wird geändert) und dann in die DS-Domäne geroutet oder aber es wird verworfen und geht somit verloren. Dadurch wird sichergestellt, dass alle Pakete, die in die Domäne gelangen die dort geltenden SLAs erfüllen. Dies zeigt die enorme Wichtigkeit der Eingangs- und Ausgangsknoten.
Wie der Traffic innerhalb einer DS-Domäne behandelt wird, wird im folgenden Abschnitt dargelegt.

3.3 Per Hop Behaviours (PHBs)

Als Hop (Etappe) bezeichnet man den Weg zwischen zwei Netzknoten. Folglich versteht man unter Per-Hop-Behaviour (PHB) verschiedene Verhaltensweisen zur Behandlung und Weiterleitung einzelner Pakete oder Paket-Bündeln. Zu diesen Paketbündeln[3] werden solche Pakete zusammengefasst, welche die gleiche Bitsequenz im DSCP tragen. Im RFC 2474 wird PHB definiert als

> „[...] a description of the externally observable forwarding treatment applied at a differentiated services-compliant node to a behavior aggregate.“ [4][10]

Es muss also konkret entschieden werden, welcher CoS[5] ein Paket zugeordnet wird, insbesondere unter den Gesichtspunkten scheduling, queuing, policing und shaping - relativ zum zwischen den Endpunkten vereinbarten SLA. Die folgenden vier PHBs sind in verschiedenen RFCs beschrieben:

3.3.1 *Default PHB*

Dieses PHB wird definiert in RFC 2474 [10]. Es muss verpflichtend von allen DS-kompatiblen Knoten implementiert werden. Inhaltlich handelt es sich hierbei um die herkömmliche Best-Effort-Qualitätsstufe, bei der eben lediglich *versucht* wird, so viele Pakete wie gerade möglich so schnell wie gerade möglich weiterzuleiten. Gleichzeitig handelt es sich hier um eine Art Rückfallklasse, der alle Pakete zugeordnet werden, die keine anderweitige PHB-Markierung mit sich tragen. Dadurch wird eine gewisse Abwärtskompatibilität zu Netzteilnehmern erhalten, welche keine DiffServ-Mechanismen implementieren, wenngleich sie unter Umständen eine sehr schlechte Behandlung erhalten. Wenn man davon ausgeht, dass Default-PHB-Traffic zunächst gepuffert wird und dann nur versendet wird, wenn gerade keine höhere PHB-Klasse Bandbreite beansprucht, kann der Puffer schnell überlaufen und viele Pakete verloren gehen. Das DSCP-Bitmuster ist ’000000’, was wie eingangs erwähnt im Einklang zu ’000’ für den Prioritäten-Teil des ToS-Bytes steht. Es steht dem implementierenden Netzwerkknoten frei, die mit ’000000’ markierten Pakete mit einer höheren Priorität zu versehen, sofern das innerhalb einer Netzwerkdomäne notwendig ist. Dies könnte beispielsweise der Fall sein, wenn innerhalb der Domäne abweichende SLAs zwischen den Routern gelten.

3.3.2 *Class-Selector PHB*

Dieses PHB wird ebenfalls definiert in RFC 2474 [10]. Es existiert, weil eine - zumindest teilweise - Rückwärtskompatibilität zum vorhandenen ToS erhalten werden soll. Es

[3] Behaviour Aggregates, kurz: BA
[4] etwa: „[...] Eine Beschreibung der von außen beobachtbaren Weiterleitungsart, mit der ein Paketbündel an einem DiffServ-kompatiblen Knoten behandelt wird.“ (Übers. d. Autors)
[5] Class of Service, etwa: „Serviceklasse“ (Übers. d. Autors)

doi: 10.2313/NET-2011-07-2_03

ist erlaubt, dass mehrere Class-Selector Codepoints auf die gleiche Klasse zeigen; es muss aber auch klar definierte Unterscheidungen geben, ein Mapping auf eine einzige Klasse ist nicht zulässig. Das Bitmuster lautet hier 'xxx000' mit $x \in \{0, 1\}$. So ergibt sich eine isomorphe Abbildung der ToS-Prioritäten-Bits. Es werden auch dessen Regeln zur Behandlung der Pakete angewandt, das heißt, höhere 'xxx'-Werte bedeuten eine höhere Priorität beim Weiterleiten und Erhalten der so markierten Pakete. PHBs mit unterschiedlichen Class Selector Codepoints sollen unabhängig voneinander weitergeleitet werden. So ist es möglich, dass DiffServ-kompatible Router parallel zu Routern, die IP-Prioritäten berücksichtigen, existieren können.

3.3.3 Expedited Forwarding PHB

Dieses PHB wird definiert in RFC 2598 [8]. Expedited Forwarding[6] wird immer dann eingesetzt, wenn Datenverkehr mit geringem Paketverlust, geringer Latenz, niedrigem Jitter und mit einer garantierten Bandbreite erfolgen soll. Typische Anwendungsfälle für dieses PHB wären VoIP, Videoanwendung oder auch die Kommunikation zwischen ERP[7]-Systemen, die für die just-in-time-Abwicklung von Geschäftsprozessen auf eine Verbindung mit den genannten Eigenschaften angewiesen sind.
Die für EF vorgesehene Bitsequenz ist '101110', was der IP-Priorität '101' entspricht, jedoch mit einer weiteren Spezifizierung in den letzten drei Bits. Es gilt zu beachten, dass EF PHB sparsam eingesetzt werden muss. Schließlich ist es nicht zielführend, zu viel (oder gar allen) Traffic als EF zu betrachten, denn somit wären sämtliche Klassifizierungen egalisiert und im Falle einer hohen Netzlast käme es wiederum zu unerwünschtem Verhalten.

3.3.4 Assured Forwarding PHB

Dieses PHB wird definiert in RFC 2597 [7]. Mit Assured Forwarding[8] (AF) ist es möglich, verschiedene Klassen von Behaviour Aggregates zu schaffen. „The Internet Society" [7] schlägt hier eine „olympische Einteilung" in Gold-, Silber- und Bronzetraffic vor. Cisco Systems empfiehlt konkret eine Bandbreitenaufteilung von 50%/30%/20% [4].
Es gibt insgesamt vier AFx-Klassen ($x \in \{1, 2, 3, 4\}$), für die jeweils eine bestimmte Größe an Pufferspeicher und eine gewisse Bandbreite vorgehalten werden. Die konkrete Behandlung dieser Klassen hängt von den für die betroffenen Knoten ausgehandelten SLAs ab. Zusätzlich kann man jeder AFxy-Klasse noch drei Stufen $y \in \{1, 2, 3\}$ zuweisen, die innerhalb der einzelnen Klassen bestimmen, welche Pakete im Fall von hoher Auslastung bzw. Überlastung zuerst verworfen werden sollen. Dies macht es möglich, einzelne flows innerhalb des Behaviour Aggregates unterschiedlich zu behandeln, beispielsweise wenn ein einziger flow die gesamte für die AFx-Klase reservierte Bandbreite für sich beansprucht. So lassen sich alle AF-Klassen darstellen aus Sextetten der Form „pqrab0", wobei „pqr" die Binärdarstellung für das obige x und „ab" die Binärdarstellung für die Drop-Prioriät y darstellt. Es ergeben sich damit die in Tabelle 3 gezeigten möglichen Kodierungen.

[6] etwa: „beschleunigte Weiterleitung" (Übers. d. Autors)
[7] Enterprise Ressource Planning
[8] etwa: „garantierte Weiterleitung" (Übers. d. Autors)

Tabelle 3: DiffServ AF Codepoints Fields (nach [7], [5])

AFxy	x = 1	x = 2	x = 3	x = 4
y = 1	001010	010010	011010	100010
y = 2	001100	010100	011100	100100
y = 3	001110	010110	011110	100110

Die konkreten technischen Implementierungsöglichkeiten der einzelnen PHBs gehen über den Rahmen dieser Arbeit hinaus und können gesondert nachgelesen werden.

3.4 Eignungsgebiete Differentiated Services

Es zeigt sich, dass DiffServ geeignet ist um Datenströme in BAs zusammenzufassen und diese dann nach einem geregelten Schema zu strukturieren. Da eine Umdefinierung der PHBs und somit der Prioritäten gestattet ist, eignet sich diese Technik hauptsächlich um Traffic innerhalb einer geregelten DiffServ-Domäne zu steuern. Diese DiffServ-Domäne kann ihrerseits wieder aus verschiedenen Administrationseinheiten bestehen. Grundvoraussetzung ist hier, dass alle Router innerhalb dieser einen DiffServ-Domäne auch tatsächlich eine deckungsgleiche Menge an DiffServ-Funktionalitäten erfüllen. Viel entscheidender ist aber, dass das zwischen den Knoten bestehenden SLA innerhalb der Domäne klar definiert ist und von allen Knoten strikt eingehalten wird.
Somit empfiehlt sich der Einsatz von DiffServ insbesondere für überschaubare Netze, deren Teilnehmer wohlbekannt sind, denen vertraut werden kann und mit denen verbindliche SLAs ausgehandelt werden können.

3.5 Alternativen zu DiffServ

Der größte Gegenentwurf zu DiffServ ist IntServ (Integrated Services). Dieses System bearbeitet als wesentlichen Unterschied zu DiffServ keine zusammengefassten Klassen von Datenverkehr, sondern legt ein QoS für jede einzelne Verbindung fest [14]. Das Gegenstück zu den DiffServ BAs und PHBs stellt hier das sog. Resource Reservation Protocol (RSVP) dar. So kann jeder Router auf flow-Basis angefragte Leitungskapazitäten reservieren und muss diese auch für die Verbindungsdauer freihalten und garantieren. Diese Garantie wird so lange aufrecht erhalten, wie die Reservierung erneuert wird. Trifft nach einem definierten Timeout keine neue Reservierung ein, so werden die Ressourcen wieder freigegeben [15]. Zur Markierung des Traffics wird ebenfalls das ToS-Feld im IPv4-Header benutzt. Die zwei grundlegenden Dienstkategorien sind „Guaranteed QoS" (macht quantitative Zusagen) und „Controlled Load" (macht lediglich vage qualitative Zusagen, weitestgehend Best-Effort). Details sind in [14] spezifiziert.
Es hat sich aber als nicht global einführbar erwiesen, da ein inkrementelles Deployment nicht möglich ist. Um IntServ einzuhalten, muss explizit jeder Router diese Technik unterstützen, es gibt keine Fallback-Lösung. Darüber hinaus ist das Queue-Management auf flow-Basis im kleinen, ähnlich wie beim IPv4-ToS, noch handhabbar, in den großen Backbones mit extrem vielen flows ist das Queue-Management jedoch kaum noch möglich [15].

doi: 10.2313/NET-2011-07-2_03

3.6 Bewertung von DiffServ

Wie in Abschnitt 3.4 erwähnt, sind die SLAs ein essentieller Teil von Netzen, die DiffServ implementieren. Werden diese SLAs nicht eingehalten, kommt es zu einer großen Last an den Ein- und Ausgangsknoten einer Domäne; der Traffic muss dauerhaft geshaped werden. Eine große Gefahr stellen hier kompromittierte Knoten dar, wie in Abschnitt 5 dargelegt wird. Der wunde Punkt sind also insbesondere die Eingangs- und Ausgangsknoten einer DiffServ-Domäne und die Übergänge zwischen diesen. Hier gilt es entweder zwischen den Domänen SLAs auszuhandeln und festzulegen, oder aber eine Re-evaluierung des Traffics beim Passieren der Domänengrenzen vorzunehmen. Dies ist zeitintensiv und rechenaufwändig. Außerdem ist das end-to-end-Verhalten solcher Trafficströme, die mehrere Domänen passieren, nicht vorhersehbar. Zum einen kann es sein, dass manche Netzbereiche gar kein DiffServ unterstützen - dann ist ein QoS nicht mehr möglich. Zum anderen könnten aber verschiedene Netze den Traffic völlig unterschiedlich behandeln, obwohl sie beide DiffServ unterstützen. Denn für Onlinespieler ist natürlicherweise Spiel-Traffic wesentlich wichtiger als eine Aktienorder - und so könnte diese beim Passieren eines solchen Subnetzes durch die Router empfindlich verlangsamt werden oder im Extremfall bei hoher Netzlast verloren gehen, wenn Internetverkehr des einen Interessengebietes den Bereich des anderen durchläuft.

Weiterhin führen die diversen Aggregationsverhalten zu unvorhersehbaren Effekten bei Ende-zu-Ende-Verbindungen. Es scheint unrealistisch, dass hier Absprachen zwischen den Providern getroffen werden können, die zu einer Standardisierung führen. Diese Koordination müsste weltweit stattfinden, sodass schließlich jegliche Differenzierung zwischen den Providern verloren ginge. Eine Lösung dafür könnten Interconnection-Entgelte sein, die in dieser Form ja schon im Telefon und Mobilfunkbereich existieren. Es bleibt jedoch die Frage, wie viel Best-Effort-Kapazität man mit DiffServ vorhalten könnte, mit der sich am wenigsten Profit erwirtschaften lässt, oder ob die Provider dann beginnen, bei hoher Last keine Teilnehmer mehr zuzulassen - wieder analog zum Telefonnetz, oder ob dann die Bandbreite gleichmäßig für alle auf ein absolutes Minimum reduziert werden würde.

Aus technischer Sicht sind alle Aussagen, die in den vorigen Abschnitten aus RFCs angeführt wurden, ausschließlich als Empfehlungen zu sehen. Dies eröffnet bei der Implementierung der Richtlinien ausgesprochen große Spielräume. Unter diesem Aspekt ist klar, dass eine hohe Marktdurchdringung ohne konkrete Aussagen und Vorschriften bezüglich der Implementierung (konkrete Werte für Jitter, prozentual zugelassener Paketverlust) nicht zu erreichen ist. Zudem war noch nicht einmal die feste Behandlung der PHBs und Codepoints festgelegt. In dieser Hinsicht wurden einige Fortschritte erzielt, indem letztlich durch das EU-Projekt MUSE sogar klare Aussagen zu Puffergrößen [6] und Längen der Warteschlangen [1] gemacht wurden.

Von dem Ziel, das Internet im Kern simpel und relativ „dumm“ zu halten, muss bei der flächendeckenden Implementierung von DiffServ allerdings Abstand genommen werden. Jede weitere Berechnung, Aggregierung und (Neu-)Zuordnung von Daten ist unweigerlich mit einer gewissen erforderlichen Rechenleistung verbunden, sodass die Knoten sowohl intelligenter, als auch teurer und fehleranfälliger werden würden.

4. OVERPROVISIONING VS. QOS

Wie aus den vorhergehenden Abschnitten und insbesondere dem anfangs erwähnten Straßenverkehrszenario hervorgeht, ist QoS im Grunde nur dann notwendig, wenn das Best-Effort-Verfahren an seine Grenzen stößt. Dies ist genau dann der Fall, wenn die Straße nicht breit genug ist, wenn also auf das Netzwerk bezogen nicht genügend Bandbreite zur Verfügung steht. Erst dieser Engpass macht es überhaupt erforderlich, QoS-Maßnahmen zu ergreifen.

Nun kann argumentiert werden, dass eine großzügige Überdimensionierung der zur Verfügung gestellten Bandbreite jegliche Probleme bezüglich der Parameter, die in Sektion 2.1 erläutert wurden, vergleichsweise kostengünstig gelöst werden kann. Dies wirft jedoch zwei Probleme auf. Zum einen ist diese kostengünstige Erweiterung recht beschränkt, denn mit der Entstehung vieler neuer Anwendungen, besonders im Web 2.0, steigt der Bandbreitenbedarf rasant und kommt demnach auch schnell an seine physikalischen Grenzen. Müssen jedoch erst aufwändig neue Leitungen verlegt werden, explodieren die Kosten. Das zeigt also, dass Overprovisioning sinnvoll zunächst nur bei komplett neu zu entwerfenden und zu errichtenden Netzen möglich ist.

Dies führt jedoch zum zweiten Aspekt, der mit einer Überdimensionierung einhergehen würde: *Wie stark* kann man hier überdimensionieren? Es ist stets nur möglich, so hoch zu dimensionieren, wie es der aktuelle Stand der Technik und die Vorstellungskraft der Techniker erlaubt. Wer weiß schon, welche Anwendungen in den nächsten 5, 10 oder 20 Jahren existieren werden und wie viel Bandbreite sie beanspruchen? Schon jetzt werden große Bandbreiten für Consumer-Anwendungen wie hochaufgelöstes Fernsehen über IPTV benötigt, auch transferieren Firmen gigabyteweise Daten in die Cloud und zurück - was vor einigen Jahren noch völlig undenkbar gewesen wäre.

Dazu kommt der wirtschaftliche Aspekt. Die Überdimensionierung kostet natürlich zusätzlich Geld, was ohne unmittelbare Notwendigkeit aufgebracht werden muss. Dies widerspricht dem ökonomischen Prinzip.

Weiterhin können Netzprovider den Kunden „Best-Effort“ nicht als etwas Besonderes verkaufen. Der Ausbau der Infrastruktur kann nur bedingt auf die Endkundenpreise umgelegt werden, denn der Markt ist hart umkämpft. Setzt man hingegen auf QoS, ließen sich neue Premiumdienste schaffen. Sowohl Privat- als auch Geschäftskunden könnte man hier bevorzugte Behandlung gegen Aufpreis verschaffen und hätte so neue Geschäftsfelder im ansonsten innovationsarmen Providergeschäft erschlossen. Es muss jedoch berücksichtigt werden, dass eine gewisse Bandbreite immer für Notfälle freigehalten wird, beispielsweise für staatliche Belange. Inwiefern eine solche „Klassengesellschaft“ im Future Internet wünschenswert und mit den Grundsätzen des heutigen Internets vereinbar ist, soll im letzten Abschnitt diskutiert werden.

Insgesamt ist also zu sagen, dass Overprovisioning als die zunächst einfachere, aber auch „brachialere“ Lösung erscheint, während das Implementieren von QoS-Lösungen technisch anspruchsvoller und eleganter ist, auf vorhandener Infrastruktur aufsetzen kann, aber die Komplexität des Netzes deutlich erhöht.

doi: 10.2313/NET-2011-07-2_03

5. DENIAL OF SERVICE ALS GEFAHR FÜR QOS

Obwohl Best-Effort-Netzwerke im Allgemeinen einen stabilen und zuverlässigen Dienst bieten, kann es sein, dass sie im Fall von hoher Auslastung lediglich schlechte oder sogar gar keine Verbindungen mehr ermöglichen [11]. Die Relevanz von DoS-Attacken ist nur gegeben, weil es im Moment in Festnetzen keine Gebühren auf Bit/Byte-Basis gibt [12]. Müsste hier etwa paketweise bezahlt werden, was in Zeiten von Flatrates undenkbar ist, wäre die Gefahr eines Floodings mit Paketen weit geringer.

Um einen Dienstausfall zu vermeiden, kann man versuchen, die Auslastung statistisch vorherzusagen. Dies ist aber nur sehr schwer möglich, da die Netzlast sprunghaft ansteigen kann, wie beispielsweise bei den jüngsten Naturkatastrophen in Japan, wo die Bevölkerung der ganzen Welt nach Informationen sucht. Ein solcher Anstieg ist kaum von einer DoS-Attacke zu unterscheiden, denn solche Attacken können auch verteilt von Botnetzen initiiert werden. Es gibt hier laut Shalunov [11] viele ungeklärte Fragen, die den Umgang mit kompromittierten Routern oder Hosts betreffen, die etwa eine ganze Trafficklasse für sich beanspruchen oder sämtliche verfügbare Bandbreite reservieren. Möchte man dies verhindern, so muss der Anteil, der für den höherwertigen (nicht Best-Effort)-Traffic verwendet wird, anpassbar sein. Denn nur so kann flexibel auf hohe Last reagiert werden, wenn sichergestellt ist, dass es sich um keinen DoS-Angriff handelt. So werden dann Engpässe in der Best-Effort oder QoS-Klasse vermieden, ohne dass Pakete verloren gehen und die Leerkapazität der einen oder anderen Klasse wird sinnvoll genutzt.

Hier besteht natürlich die Möglichkeit, sich gewisse Qualitätsmerkmale bzw. deren Nichteinhaltung versichern zu lassen, oder aber die Provider müssten hier mit Geld-zurück-Garantien oder ähnlichen Zusicherungen punkten [13]. Das zieht wiederum das Problem der Nachweisbarkeit nach sich. Denn schließlich können die QoS-Zusicherungen nur im Falle extrem hoher Last getestet werden - und eine künstliche Überlastung kann auf keinen Fall im Interesse des Providers liegen. Deswegen ist es sehr schwer, hier Garantien zu geben, die auch mess- und spürbar sind.

6. QOS IM (FUTURE) INTERNET

Kann man nun Quality of Service vorbehaltlos in einem jetzigen oder einem zukünftigen Internet einführen? Das Future Internet kann einerseits als radikaler Neuanfang gedeutet werden oder aber in Form von inkrementellen Veränderungen aus dem nun vorhandenen Internet hervorgehen. Da ein radikaler Schnitt nicht praktikabel ist, müssten vorerst zwei „Internets“ parallel existieren. Lässt man aber diese erst parallel entstehen, könnten daraus untereinander nicht kompatible Netze hervorgehen und bestehen bleiben, sodass eine große Fragmentierung entsteht. Es ist außerdem nicht klar, wie hier der Traffic dann zwischen den beiden Netzen fließen sollte. Es soll ja kein unklassifizierter Verkehr aus dem alten Internet in das neue QoS-fähige Future Internet fließen. Um eine völlige Isolierung zu verhindern, und auch im Hinblick darauf, dass im Future Internet mit QoS ein neue Form der Abrechnung eingeführt werden muss, müssen providerübergreifende Vereinbarungen getroffen werden. Dies scheint schwer umsetzbar.

Denkt man hier an einen radikalen Neubeginn, könnte ein Peer-to-Peer-basierter Ansatz die Lösung sein. Wenn man den kompletten Aufbau des Internets dezentralisiert und nur noch Router teilnehmen lässt, die per Implementierung einen vereinheitlichten Standard für QoS-Maßnahmen umsetzen, können die Provider überflüssig werden. Durch den P2P-Ansatz entstünde dann ein riesiges, providerloses Netz unter einer einzigen DS-Domäne, womit grundsätzlich die Grenzknotenproblematik, insbesondere von DiffServ, gelöst wäre.

Geht man davon aus, dass QoS-Maßnahmen weitgehend selbstlos eingesetzt werden würden, so wie das in Grundsätzen der Idee des jetzigen Internets entspricht, ist es natürlich sinnvoll eine bestimmte Servicequalität garantieren zu wollen. Jedoch zeigt die Erfahrung, dass Premiumdienste oft mit einer Premiumbezahlung einhergehen und somit das Internet für den normalen Best-Effort-User unbenutzbar werden würde. Wenn mit höherwertigen Dienstleistungen mehr Geld verdient werden kann, wird die Standard-Leistung bald gekürzt werden bis hin zur Unbenutzbarkeit. Damit wird ein wichtiger Teil der modernen Kommunikation von vielen Menschen ferngehalten, was nicht mit dem Grundgedanken vereinbar ist, das Internet möglichst günstig allen Menschen zugänglich zu machen. Die Premiumservices, die noch Performance bieten würden, wären sehr teuer. Ein großer Teil von Bildungsmöglichkeiten in der modernen Gesellschaft würde eingeschränkt und den aufstrebenden Gesellschaftsteilen in anderen Ländern würde im wahrsten Sinne des Wortes der Anschluss gekappt, da sie sich keine hochwertige Dienstgüte leisten könnten.

Schafft man dagegen ein neues Internet mitsamt neuer physikalischer Beschaffenheit, ohne Rücksicht auf Kompatibilität zu vorhandenen Technologien, so scheint die Einführung von QoS realistischer. Zwar tritt auch hier das Problem auf, dass eine im QoS-Sinne „bessere“ Leitung auch teurer ist, jedoch gäbe es die Möglichkeit, Regionen mit schlechteren Leitungen aus dem QoS-unterstützten Gebiet auszunehmen. Dies trifft insbesondere auch auf Mobilfunkverbindungen zu, für die aufgrund physikalischer Gegebenheiten bestimmte Qualitätsmerkmale nicht garantiert werden können (z.B. Latenz).

7. ZUSAMMENFASSUNG UND AUSBLICK

Zusammenfassend kann gesagt werden, dass QoS für das zukünftige Internet eine sinnvolle Erweiterung darstellen kann. Mit DiffServ existiert eine gut erforschte Implementierungsmöglichkeit, es lassen sich viele Regelungen treffen, die jedoch an ein schwer zu etablierendes SLA gebunden sind. Insgesamt ist es jedoch schwierig, QoS für das zukünftige Internet zu etablieren. Zuerst gibt es einige infrastrukturelle Probleme. Beispielsweise ist es einfach nicht möglich, übergreifend für mobile und drahtgebundene Netze gleichermaßen hochwertige QoS-Kriterien anzusetzen. Latenz und Bandbreite der flächendeckend verfügbaren Mobilfunknetze lassen sich in keinster Weise mit der durch die Festnetzanbieter etablierten Netzstruktur vergleichen. Eine Festlegung auf einen geringen netzübergreifenden Standard ist auch keine Lösung, denn dieser ist oftmals sogar deutlich unter dem Niveau der Best-Effort-Lösungen in den Festnetzen anzusiedeln. Zudem haben sich die technischen Möglichkeiten wie DiffServ oder IntServ mangels früher Standardisierung und zu aufwändiger Implementierung nicht etabliert.

doi: 10.2313/NET-2011-07-2_03

Andererseits ist das Bedürfnis nach QoS in der Realität, außer in Zugangsnetzen, noch nicht vorhanden, da die Best-Effort-Leistungen der heutigen Netze als ausreichend gedeutet werden müssen. In Kombination mit Audio- und Videocodecs oder passenden Technologien für andere Einsatzfelder, die ihre Qualität an die vorhandene Bandbreite anpassen, ist auch mit dieser Methode eine absolut akzeptable Netzleistung zu erreichen.
Darüber hinaus müssen aber auch Probleme moralischer Art gelöst werden. Insbesondere das Thema Netzneutralität spielt hier eine zentrale Rolle. Wenn es schon verschiedene Klassen von Datenverkehr gibt, wer bestimmt, welche Arten von Traffic zu welcher Klasse gehören? Viel komplexer erscheint hier auch, dass der Traffic dann nicht nur nach Art klassifiziert werden könnte, sondern auch nach Organisation/Firma. Wer erhält dann ein Vorrecht auf priorisierten Internetverkehr? Wer wird im Extremfall ganz von den Backbones abgetrennt? Kann man anderen Organisationen eine großen nutzbaren Anteil von Internetkanälen „wegkaufen“?
Solange diese Probleme nicht geklärt sind, ist es zumindest zweifelhaft, dass sich QoS flächendeckend etablieren kann und muss. Der Erfindergeist der Ingenieure hat gezeigt, dass es zunehmend möglich wird, immer mehr Datenverkehr über vorhandene oder günstige Leitungen zu transportieren. Durch Beseitigung der Flaschenhälse des Internets könnte so ein großzügiges Overprovisioning und die Vermeidung der Worst-Case-Vollauslastung am Ende doch die Lösung aller QoS-Überlegungen sein.

8. LITERATUR

[1] PlaNetS QoS Solution. http://www.medea-planets.eu/QoSsolution.php?page=solution (13.03.2011, 15.30 Uhr).

[2] P. Almquist. Type of Service in the Internet Protocol Suite. RFC 1349, 1992.

[3] D. Bricklin. Why We Don’t Need QOS: Trains, Cars, and Internet Quality of Service. http://www.bricklin.com/qos.htm (09.03.11, 22.45 Uhr).

[4] Cisco Systems. *DiffServ – The Scalable End-to-End QoS Model*, 8 2005.

[5] Cisco Systems, USA. *Overview of DiffServ for QoS*, Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2 edition, 4 2007.

[6] A. Foglar. Die QoS Lösung des MUSE Projekts - Europa definiert das Breitbandnetz der nächsten Generation (The QoS Solution of the MUSE Project). *it - Information Technology*, 48(5):282–, 2006.

[7] J. Heinanen, F. Baker, W. Weiss, and J. Wroclawski. Assured Forwarding PHB Group. RFC 2597, 1999.

[8] V. Jacobson, K. Nichols, and K. Poduri. An Expedited Forwarding PHB. RFC 2598, 1999.

[9] S. Keshav. *An engineering approach to computer networking: ATM networks, the Internet, and the telephone network*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 1997.

[10] K. Nichols, S. Blake, F. Baker, and D. Black. Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers. RFC 2474, 1998.

[11] S. Shalunov and B. Teitelbaum. Quality of Service and denial of service. In *Proceedings of the ACM SIGCOMM workshop on Revisiting IP QoS: What have we learned, why do we care?*, RIPQoS ’03, pages 137–140, New York, NY, USA, 2003. ACM.

[12] B. Teitelbaum and S. Shalunov. Why Premium IP Service Has Not Deployed (and Probably Never Will). Internet2 QoS WG informational doc, May 2002.

[13] B. Teitelbaum and S. Shalunov. What QoS research hasn’t understood about risk. In *Proceedings of the ACM SIGCOMM workshop on Revisiting IP QoS: What have we learned, why do we care?*, RIPQoS ’03, pages 148–150, New York, NY, USA, 2003. ACM.

[14] J. Wroclawski. The Use of RSVP with IETF Integrated Services. RFC 2210, 1997.

[15] W. Zhao, D. Olshefski, and H. Schulzrinne. Internet Quality of Service: an Overview. Technical report, 2000.

doi: 10.2313/NET-2011-07-2_03

Strategien zur Paketverarbeitung bei Dienstgüte-Unterstützung

Krisna Haryantho
Betreuer: Heiko Niedermayer
Seminar Future Internet SS2011
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: haryanth@in.tum.de

ABSTRACT
Computer networks today often have limited resource. This limitation is one of the reasons why sometimes packets sent over the network are delayed or even dropped. The simple best-effort network or service does not support quality of service [from Wiki]. This paper introduces several bandwidth management techniques and strategies that can be used to achieve quality of service over a best effort network.

Keywords
DiffServ, Quality of Service, Traffic Shaping, Traffic Policing, RED, WRED, Two Rate Three Color Marker, Leaky Bucket, Token Bucket

1. INTRODUCTION
In computer networks, the presence of bottleneck links is hard to prevent. In the simplest operation mode (no shaping, limiting, policing, etc. used), packets that are sent through a network will be delivered in a best effort manner. This means when a packet arrives at a network point, it will either be forwarded immediately when there is enough bandwidth to do so, or discarded otherwise. In the case of aggressive hosts, where hosts try to send packets using their full bandwidth, this would lead to traffic congestion at bottleneck links. Some transport layer protocols such as TCP provide a congestion control mechanism. TCP starts by sending packets at a slow speed, and gradually increasing this speed as far as possible. When it detects congestion (usually signalized by dropped packets), it will reduce the transmission speed. When all packets can be delivered successfully, TCP will try to increase the speed again. This process continues until TCP 'finds' the ideal transmission rate for the current transfer. This mechanism is called the TCP slow-start.

The best-effort network cannot provide Quality of Service due to its somewhat indeterministic behaviors. This means, there is no way of guarantying that packet are received, and this within a specific delay and jitter (standard deviation of the delay). Currently the most common transport protocols in the packet-switched network are the TCP and UDP. While TCP provides a congestion control mechanism, UDP does not. Given this fact, UDP (or in general non-responsive flows) will tend to dominate the available bandwidth, starving out the remaining TCP traffic (or in general the responsive flows) [1].

While increasing capacity by expanding the network can address the traffic congestion issue, it does not scale up and is in most cases not the most cost-efficient way of dealing with this problem. This is where the term Quality of Service comes into play. Quality of service (QoS) is the ability to provide different priority to applications, users, data flows in order to guarantee a certain level of performance (Citation needed!) – In the best effort setting, all packet have the same priority and are treated the same way. This performance includes transfer rate, latency, jitter and drop probability. Performance is an important issue for real-time applications such as multimedia streaming, video conferencing, or online gaming, as they often require a steady transfer rate and are delay sensitive.

In the following sections we will discuss two bandwidth management mechanisms that can be used to provide quality of service. Section 3 talks about traffic shaping and algorithms that are used to realize it. Section 4 talks about congestion mechanism and some of the most popular methods of to avoid congestion. Section 5 provides a short introduction to DiffServ, the current accepted way of implementing quality of service. Section 6 concludes the paper with some closing remarks on the discussed topics.

2. TRAFFIC SHAPING/RATE LIMITING
Network providers and their customer agree upon a certain customized traffic profile - this is called the Service Level Agreement (SLA). To keep their network running smoothly, providers would want to ensure that the customers are not generating more traffic than what is specified in the SLA. One way to control the bandwidth is by doing traffic shaping. Traffic shaping is a strategy to increase performance on a resource-limited network. It works by delaying some or all of the packets in a traffic stream in order to bring the stream in compliance with a traffic profile [2].

Principally each incoming packet will be verified against a certain traffic policy. Packets will be forwarded only if it conforms to the policy. Otherwise it will either be dropped, delayed, or forwarded with lower priority. There are two basic algorithms that are used for implementing traffic shaping – the token bucket algorithm and the leaky bucket algorithm. These two algorithms will be discussed in the following subsection. But before that, let us consider the two-rate three color marker as a method to classify/differentiate traffic.

doi: 10.2313/NET-2011-07-2_04

2.1 Two Rate Three Color Marker

The two rate three color marker provides a way to classify IP packets. The two rates being used are called CIR und PIR.

Committed Information Rate (CIR) is the data rate that the service provider is guaranteeing to its subscriber. A service level agreement usually demands that all traffic at the rate of CIR or less will be delivered to its destination with high probability [3]. If a network is so provisioned, that it is capable of carrying the sum of all subscriber CIRs, that network would be underutilized. This is because it is statistically unlikely that all subscribers generate traffic at CIR at the same time. Because it is not cost efficient to operate an underutilized network, the provider would often allow the subscriber to generate traffic at a higher rate than CIR. This rate is called the *Peak Information Rate* (PIR).

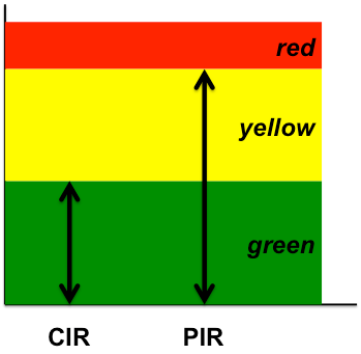


Figure 1: Different coloring for each rate

A Two Rate Three Color Marker meters IP packet stream and marks its packets green, yellow, or red [4]. The color is coded in the DiffServ field of the IP header. A packet is marked green if the stream is at or below the CIR, yellow if it is higher than the CIR but lower or equal the PIR, and red otherwise (see Figure 1: Different coloring for each rateFigure 1).

A very common practice is to forward green packets and assure their delivery, forward yellow packets with best effort. While red packets will usually be dropped, some systems might still forward red packets as if they were yellow packets [3].

2.2 Token Bucket

The token bucket algorithm can be understood as a container (a bucket) that is continuously filled with tokens at a certain rate [3]. This bucket has a size, which is the number of tokens it can hold. When the bucket becomes full, no more tokens can be added to it – any new tokens added will simply be dropped.

This token can be thought of as a stamp for each packet that needs to be forwarded. The algorithm works then as follows. Whenever a packet arrives, the algorithm will try to remove a certain amount of tokens from the bucket. Usually we measure token in the unit of byte with one token conforming to one byte. Thus packet with 500 bytes size requires 500 tokens.

By using token bucket, one can get a controlled (‘shaped’) output traffic from any input traffic. The rate of the desired output is regulated by the token fill rate. Token bucket also allows the presence of short duration burst traffic. The maximum allowed burst traffic conforms to the bucket size. Figure 2 illustrates the token bucket algorithm. Here the unregulated input traffic are shaped into a regulated output traffic with a constant rate.

Now consider the dual-rate token bucket algorithm, the extension of this algorithm where there are two buckets being used. The first bucket has the size X and is filled with the rate of the CIR (The CIR bucket). The second bucket has the size Y and is filled with the rate of the PIR (The PIR bucket). Both buckets start full and the algorithm works as following (See Figure 3): whenever a packet arrives, it checks the PIR bucket whether it currently holds enough tokens to forward the packet with. If this is not the case, the packet is marked as not conforming (red) and can later be dropped. Otherwise the algorithm will remove tokens from the PIR bucket and checks the CIR bucket whether it also holds enough tokens. If this is the case, the algorithm will remove tokens from CIR bucket and the packet will be marked as conforming (green) and will be forwarded. Otherwise the packet will be marked as exceeding (yellow) and will be forwarded in the best effort manner.

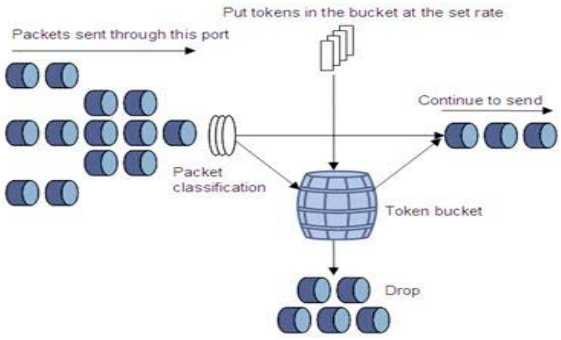


Figure 2: Token bucket algorithm (Source www.h3c.com/…/200701/195599_57_0.htm, accessed on 20th April 2011)

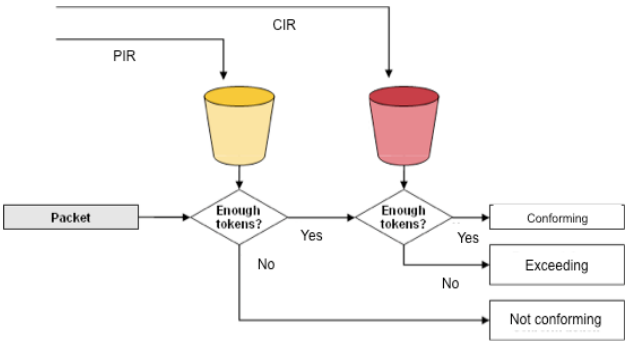


Figure 3: Dual-rate token bucket algorithm

Assume CIR is 1500 KB/s and PIR 3000 KB/s. Both buckets are set to 1500 Bytes. When a 1500 Byte packet arrives, 1500 Bytes will be removed from both bucket. The bucket is empty and that packet will be green. Then a second 1500 Byte packet arrive ½ millisecond later. By this time 1500 Bytes (½ ms x 3000 KB/s) of token has been added to the PIR bucket. The CIR bucket has 750 Bytes (½ ms x 1500 KB/s) of token. This second packet will be yellow, and 1500 Bytes are removed from the PIR bucket only. If a third 1500 Byte packet arrives ½ millisecond later, both bucket will contain 1500 Bytes and that packet will be green.

doi: 10.2313/NET-2011-07-2_04

2.3 Leaky Bucket

The leaky bucket algorithm is the other often used algorithm to shape traffic. While token bucket is typically implemented for IP networks, leaky bucket is usually implemented for ATM networks. In ATM the term cell is used instead of packet. And analog to the IP network, in ATM network the Sustained Cell Rate (SCR) and the Peak Cell Rate (PCR) are used in a similar manner to CIR and PIR respectively.

The algorithm is similar to the token bucket, only in the leaky bucket case the packets are filled into the bucket. The name leaky bucket comes from an analogy of a bucket that has a hole at the bottom. Water (ATM cell) can be filled into the bucket at any rate and leaks through the bottom hole at a certain rate until the bucket becomes empty. If the bucket is full, any added cells will be discarded.

Whenever an ATM cell arrives, the algorithm checks whether there is enough space in the bucket to contain every byte in the cell. If there is enough space, the packet is added to the bucket, otherwise it will be discarded. The desired output rate is thus the leak rate of the bucket. The leaky bucket algorithm allows input burst, meaning it will take packets at any rate as long as there is still enough space in the bucket left. The maximum burst size is thus the bucket size.

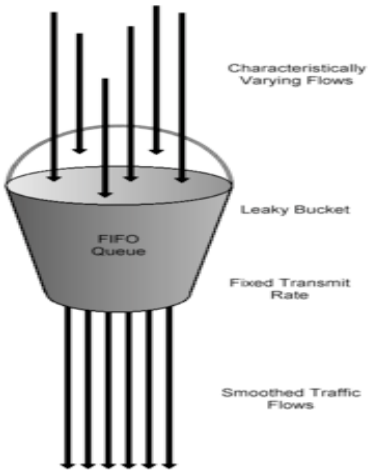


Figure 4: Leaky bucket used as queue to shape traffic (Source: Wikipedia)

Similar to the token bucket, there is a variation of the leaky bucket where two buckets are used. The first bucket is used for the guaranteed traffic. It leaks at the SCR. The second bucket is used for the excess traffic that does not fit in the first bucket anymore. This bucket leaks at PCR. The algorithm will try to fill all incoming traffic to the SCR bucket. If this bucket becomes full, the excess traffic goes to the PCR bucket and will be forwarded in a best effort basis (similar manner to yellow marked IP packet).

3. CONGESTION AVOIDANCE

The core network consists of switches and routers. These devices are prone to congestion [5]. Congestion occurs when the aggregate traffic coming through the *ingress* interface (incoming traffic) has a higher rate than that which can be successfully processed by the *egress* interface (outgoing traffic). Congestion can also occur due to the inability of the switch/router CPU to handle the size of the forwarding table [5].

In the default setting, when the internal queue of an interface is full, any new incoming packets will be dropped. Due to the first-come first-served nature of the queue, overflowed packets are dropped without regarding their previous classification or marking. This phenomenon is called *tail dropping*.

As mentioned previously in section 1, TCP provides a mechanism to control congestion in the network. With regard to the tail drop phenomenon, there are two major problems that can arise when using TCP congestion control mechanism:

- In an aggregated traffic, a large number of TCP packets that are dropped (as a result of tail dropping) can cause a large number of hosts to detect congestion. As a counter measure they will immediately reduce their transmission rate. This will make the corresponding link underutilized for a short period until the TCP hosts speed up their transmission rate again. The bandwidth adjustment can happen over and over again at the same time across all active TCP connections. This is known as the *TCP Global Synchronization*.
- In real networks there is also non-responsive traffic. Non-responsive traffic, such as the UDP, tends to be more aggressive in using available bandwidth and -in the case of UDP- lacks of congestion control mechanism. By the time a link becomes underutilized (due to result of TCP global synchronization), it will consume the remaining bandwidth leaving no resource for TCP. This effect is called *TCP starvation*.

Due to these issues, the traditional queue mechanism is not enough to guarantee Quality of Service. To do this, switches or routers must be equipped with a mechanism to queue and service high priority traffic before lower priority traffic [5]. Furthermore it must also be possible to drop lower priority packets before higher priority packets during periods of congestion.

To counter the tail drop effect resulting from the use of traditional queue, the term *active queue management* (AQM) was introduced. AQM takes advantage of the congestion control mechanism provided by TCP. Rather than dropping packet after the queue is full, it prevents the queue (an *active queue*) to become full. Commonly there are two ways to do this. The first is done by dropping packets, the second is by ECN-marking packets.

3.1 Random Early Detection (RED)

The random early detection algorithm works by randomly dropping packets with respect to the average queue length [6, 7]. When a packet arrives, the average queue length Q_{avg} is calculated. The calculation of the average queue length can vary depending of the implementation of the algorithm. A common practice is to calculate it based on the size of the previous average and the current size of the queue [8].

The average queue length is then compared with a certain configurable queue threshold (See Figure 5). If it is lower than the minimum threshold Q_{min}, the packet will be added to the queue. If it is between Q_{min} and the maximum threshold Q_{max}, the packet will either be dropped or queued depending on a certain probability. Following the increase of the average queue length,

doi: 10.2313/NET-2011-07-2_04

the drop probability grows linearly from zero to a specified maximum probability P_{max} at the point where $Q_{avg} = Q_{max}$. If the average queue length exceeds the Q_{max}, the packet will be dropped.

Note that RED will drop packet indiscriminately, meaning it has no mechanism to differentiate between traffic categories. In the case where the queue does become full, tail dropping is used.

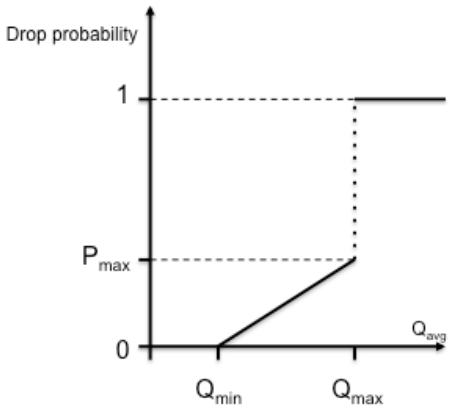


Figure 5: Random Early Detection

3.2 Weighted Random Early Detection (WRED)

The weighted RED is a variation of RED algorithm which supports multiple drop probability functions for each traffic category [6]. Principally traffic with higher drop precedence (e.g. P2P file-sharing traffic) will be discriminated against traffic with lower drop precedence (e.g. Real-time application traffic) or in other words packets with a lower priority (lower IP precedence) can be dropped more often than higher priority packets [5]. Note that all packets still share one single queue regardless of their precedence level.

Table 1: WRED Configuration

Precedence	Q_{min}	Q_{max}	MPD
0	12	20	5
1	14	20	5
2	16	25	5
3	18	25	5

Table 1 describes an example of a WRED configuration with four traffic precedence (traffic category, higher number means higher priority). The *mark probability denominator* (MPD) is here set to 5. This means that when the queue length is between Q_{min} and Q_{max} one out of five packets will be dropped (20% drop probability). With this configuration, packets with precedence level 0 will be randomly dropped once the queue size reaches 12 (12 packets are queued). In a similar manner, the algorithm will start randomly dropping packets with precedence level 2 once the queue size reaches 16. Once the queue size reaches 20, any incoming packets with precedence level 0 or 1 are dropped. For precedence level 2 or 3, packets are dropped once the queue size reaches 25.

The WRED configuration can be set up to be fully overlapped, partially overlapped or staggered [6] (See Figure 6).

The colors represent different traffic precedence (not to be confused with the three color marking scheme discussed in previously). It is worth noticing that only one single queue is being used regardless of the number of precedence levels. There is no way to control the composition of the queue, i.e. how many low priority or high priority packets there are in the queue. A fully overlapped configuration still provides a somewhat fair allocation of resource. Here we see that after a certain threshold all packet types could be dropped. Meanwhile a staggered configuration gives the advantage for high precedence packets at the cost of low precedence packets. Here we see that the minimum threshold for higher priority traffic is set higher than the maximum threshold of lower priority traffic. And due to the nature of the queue, it is possible that the queue is filled with only high priority packets up until that maximum threshold. From this point on all new lower priority packets will not have a chance to ever enter the queue.

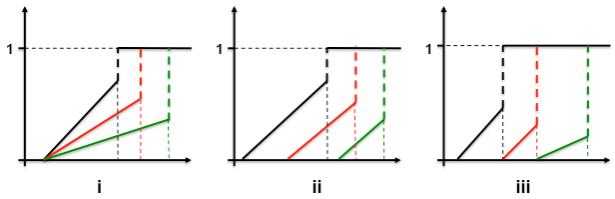


Figure 6: WRED configuration: i) fully overlapped, ii) partially overlapped, iii) staggered

3.3 RED with In/Out (RIO)

RED with In/Out queues is another extension of the RED algorithm, which uses separate (virtual) queue for each traffic precedence [1]. Incoming packets that comply with the contracted service profile are marked *In* and are added in the *In* queue. Those that do not comply with the service profile are marked *Out* and are added to the *Out* queue. It is so arranged, that during congestion the *Out* packets are dropped first. RIO can also be seen as WRED with two drop precedence, but maintain two separate queues, one for each drop precedence. This feature makes it possible to control the contribution of each precedence level in the total queue. In this respect, RIO is more appropriate to protect traffic with lower drop precedence against that with higher drop precedence [6].

3.4 Explicit Congestion Notification

The three congestion avoidance algorithms discussed previously work by dropping packets. There are two arguments that speak against this idea:

- Dropping packets while there is still available resource seems counter-intuitive, because "Why drop completely perfect packets when there is still free buffer space?"
- By dropping packet the network resource that was being used to deliver the packet up to the dropping node would be wasted.

doi: 10.2313/NET-2011-07-2_04

The RFC3168 [9] defines an extension to the Internet Protocol (IP) and to the Transmission Control Protocol (TCP) that allows an end-to-end congestion notification without the need to drop packets. This is called the *Explicit Congestion Notification* (ECN). For ECN to be effective, all nodes in along the route need to support this.

An end-point that supports ECN use the two rightmost bits of the DiffServ field in the IP header to mark that it is ECN capable (01 or 10, refer Table 2 for a complete list of the ECN bits). Although the ECN marking appears in the internet layer, ECN needs a transport protocol layer (or higher layer protocol) which not only supports the congestion control, but also has a way to deliver feedback about the occurring congestion to the transmitting end. TCP works fine because it has a congestion control mechanism and can support delivery of the feedback by using the ECE flag in the TCP header (refer to [9] for further details).

Table 2: ECN Bits

ECN Bit	***Meaning***
00	*Non-ECT* (Non ECN Capable Transport)
01	*ECT(1)* (ECN Capable Transport)
10	*ECT(2)* (ECN Capable Transport)
11	*CE* (Congestion Encountered)

When congestion occurs, an ECN capable router will set the ECN bit of an incoming ECN packet with 11 (Congestion Encountered) and still forward the packet (instead of dropping it). When the packet finally arrives, the transport layer of the receiving end will notice this congestion and will send feedback to the transmitting end. The latter will later be informed that congestion occurs and will adjust its transmission speed to avoid further congestion.

4. DIFFERENTIATED SERVICE

Differentiated Service (DiffServ) is the current accepted standard of implementing Quality of Service. It describes a computer network architecture that enable a simple and scalable mechanism to classify and manage network traffic. The RFC 2474 defines DiffServ as an enhancement to the internet protocol to enable scable service discrimination in the internet without the need for per-flow state and signaling at every hop. Services can be constructed by means of setting bits in an IP header (marking) at network boundaries, using those bits to determine how packets will be forwarded inside the core network, and conditioning the marked packets in accordance with the SLA [10].

DiffServ information is coded in the DiffServ field of the IP header (this is called the DiffServ codepoint). Differentiated services are realized by mapping the DiffServ codepoint to a particular forwarding behavior – the so called per-hop behaviors (PHB) at each node. The mapping also represent the classification of traffic. Traffic can be classified based on different parameters such as source address or destination address. Once a packet enters a DiffServ domain, it is subject to classification and conditioning. A packet entering a DiffServ domain may already have a DiffServ marking given by the DiffServ domain which forwarded it. A DiffServ domain may honor the previous marking, ignore it, or overwrite it.

Theoretically the six bits available for DiffServ codepoint allow network operators to specify up to 64 (2^6) different traffic classes (or PHB). However only four PHBs are commonly used. These are:

1. The default PHB. This PHB is defined in RFC 2474 and should be supported by all DiffServ capable domains. The default PHB is typically used for best-effort traffic.
2. Expedited Forwarding (EF) PHB. This PHB is defined in RFC 3246 [11]. It is usually used for low-loss and low-latency traffic.
3. Assured Forwarding (AF) PHB. This PHB is described in RFC 2597 [12]. It is used to guarantee packet delivery under certain conditions according to the AF class. Currently there are four AF classes specified, each with its own drop precedence.
4. Class selector PHB. Defined in RFC 2474, this PHB allows backward compatibility with the ToS bits of the earlier IP header specification for systems without DiffServ support (both ToS and DiffServ bits occupy the same location in the IP header).

5. CONCLUSION

Traffic shaping and congestion avoidance are techniques that can be used to increase performance and guarantee Quality of Services. They can be used in parallel. A typical scenario would be to monitor and mark packets at network edges, and set up an active queue management mechanism in the core network [13]. To protect traffic against future delay or congestion in core network, traffic shaping can be used.

When dealing with traffic shaping, there are some issues to be considered such as picking the correct values. Choosing CIR is a business decision. Choosing PIR in the other hand is a business decision with a technical impact [3]. As a link approaches its maximum capacity, the average packet latency becomes higher. When choosing bucket size, it is important to set it in respect to the maximum packet size that can be received on the link (otherwise it can never be forwarded, as it never gets the required amount of token, i.e. the policy is never met).

There are also issues to be considered when using active queue management. Generally all active queue management only performs well with responsive flows (such as TCP). With the co-existence of other non-responsive flows (such as UDP), dropping packet does not necessarily prevent hosts from sending too fast and thus congestion still cannot be avoided. This issue is discussed in [6]. Another issue is fairness across concurrent connection. A solution for this problem is proposed in [1].

Finally, maintaining a consistent Quality of Service is not an easy task to do. First it must be supported by all nodes along the path. Secondly we are also aware that packets may travel between multiple autonomous systems, which may have different QoS policy. In other words, a high priority traffic for one autonomous system might be just a low priority traffic for another one. To better ensure quality of service, a common understanding of traffic policing is needed. But again, this is not trivial.

doi: 10.2313/NET-2011-07-2_04

6. REFERENCES

[1] I. Andrikopoulos, L. Wood, and G. Pavlou. “A Fair Traffic Conditioner for the Assured Service in a Differentiated Service Internet”, Proceedings of IEEE International Conference on Communications ICC2000. 2000

[2] S. Blake, D. Black, M. Carlson, et. al. An Architecture for Differentiated Services. RFC 2475. 1998

[3] BTI Systems White Paper. Understanding Traffic Policing. 2010. http://www.btisystems.com/_documents/white-papers/Understanding-Traffic-Policing-WP0102.pdf

[4] J. Heinanen and R. Guerin. A Two Rate Three Color Marker. RFC 2698. 1999

[5] A. Balchunas. QoS and Congestion Avoidance. 2010. www.routeralley.com/ra/docs/qos_congestion_avoidance.pdf

[6] E. Bowen and C. Jeffries, L. Kencl, et. al. Bandwidth Allocation for a Non-Responsive Flows with Active Queue Management. 2002

[7] S. Floyd and V. Jacobson. “Random Early Detection Gateways for Congestion Avoidance”, ACM Transactions on Networking. August 1993

[8] Cisco Document. Distributed Weighted Random Early Detection. http://www.cisco.com/en/US/docs/ios/11_1/feature/guide/WRED.pdf

[9] K. Ramakrishnan, S. Floyd, and D. Black. The Addition of Explicit Congestion Notification (ECN) to IP. RFC 3168. 2001

[10] K. Nichols, S. Blake, F. Baker, and D. Black. Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers. RFC 2474.1998

[11] B. Davie and A. Charny, K. Benson, et. al. An Expedited Forwarding PHB. RFC 3246. 2002

[12] J. Heinanen, F. Baker, W. Weiss, and J. Wroclawski. Assured Forwarding PHB Group. RFC 2597. 1999

[13] Virpi Laatu, Jarmo Jarju and Pekka Loula. “The Impacts of Aggregation on the Performance of TCP Flows in DS Networks”, Proceedings of ICN2004. March 2004

doi: 10.2313/NET-2011-07-2_04

User Interfaces for Smart Ambiences: A State of the Art Analysis

Denys F. Artmann
Betreuer: Mac-Oliver Pahl
Seminar Future Internet SS2011
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
E-Mail: artmann@in.tum.de

KURZFASSUNG

Benutzerschnittstellen bezeichnen die Brücke zwischen Mensch und Computer. Sie dienen der Kommunikation des Menschen mit einer Maschine. Für die Interaktion eines Nutzers mit einem System existieren bestimmte Kriterien, um die Verständigung des Menschen mit dem System so schnell, intuitiv und angenehm wie möglich zu gestalten. Um solche entscheidenden Kriterien und Aspekte wird es im Folgenden gehen. Drei aktuelle Benutzerschnittstellen sollen auf die Einhaltung dieser Kriterien untersucht und ausgewertet werden. Es wird gezeigt in welcher Art und Weise sich die Anwendung von solchen Benutzerschnittstellen, speziell in der Umgebung des zukünftigen Eigenheims des Menschen etabliert.

Schlüsselworte

Benutzerschnittstelle, Future Home, Touchscreen, Interaktion

1. EINLEITUNG

Arbeitet der Mensch mit einem (Computer-)System, ist es wünschenswert mit diesem, auf eine für den Nutzer angenehme Art interagieren zu können. Hierfür existieren sogenannte Benutzerschnittstellen oder „User Interfaces“. Sie ermöglichen die Kommunikation zwischen Mensch und Maschine.

Bereits zu Beginn der 1960er Jahre entwickelte ein Team um Douglas C. Engelbart und William English am Stanford Research Institute (SRI), eine der wichtigsten und meist gebrauchten Benutzerschnittstelle für den Menschen: Die Computermaus [8]. Noch heute gilt die Erfindung der Computermaus, als der Anstoß zum Zeitalter des „Personal Computer“. Dies zeigt wie wichtig die Mensch-Computer-Schnittstellen sind, welchen Einfluss sie haben und auch was sie ermöglichen können.

Constantine Stephanidis, Professor an der Universität von Kreta und Verantwortlicher in mehr als 40 geförderten Projekten im Bereich der Mensch-Computer-Interaktion, stellt fest, dass gute und erfolgreiche Benutzerschnittstellen dafür sorgen, dass weltweit komplexe Daten und Informationen bearbeitet und verstanden werden können [14, 5]. Ohne die Wahl einer geeigneten Benutzerschnittstelle wäre es bei vielen Aufgaben, Probleme und Sachverhalte nicht möglich gewesen, diese zu bearbeiten und zu lösen. Für die Interaktionen mit einem System stehen eine Reihe von verschiedenen Möglichkeiten zur Verfügung. Die klassischen Schnittstellen, welche viele Menschen aus dem täglichen Leben kennen, wie ein Desktop, auf welchem mit Computermaus und Tastatur mit dem System kommuniziert wird, fallen unter den Typ der „Graphical User Interfaces“ (GUI) [11]. Diese Ermöglichen eine Ein- und Ausgabeorientierte Kommunikation. Der Mensch kann Befehle und Eingaben an das System senden, welches die Antwort beispielsweise auf einem Bildschirm zeigt. Die Darstellung und Interaktionsmöglichkeit wird mit Hilfe von Symbolen, Fenstern und Menüs verwirklicht. Der klassische Personal Computer basiert auf einer solchen Darstellung und Wechselbeziehung. Des weiteren sind mittlerweile Bildschirme mit Berührungseingabe eine weit verbreitete Interaktionsmöglichkeit. Diese so genannten Touchscreens ermöglichen die Befehlseingabe über das Berühren des Bildschirms. Diese Benutzerschnittstelle gewinnt zunehmend an Wichtigkeit, vor allem durch die Entwicklung von Tablet Computer und Smartphones. Im Folgenden befassen wir uns mit den genannten Interaktionsmöglichkeiten und vor allem mit Kriterien, welche die Bewertung der verschiedenen Benutzerschnittstellen ermöglichen.

Es existieren noch einige weiter Typen von Benutzerschnittstellen. „Voice User Interfaces“ werden mithilfe von verbal vorgetragenen Befehlen gesteuert. Der Mensch kommuniziert mit dem Computer also mit Hilfe seiner Sprache.

Des weiteren existieren „Tangible User Interfaces“, welche Eingabegerät und Systemfunktionalität in einem Gerät vereinen. Bekanntester Vertreter solcher fassbaren Benutzerschnittstellen ist das Smartphone. Es kombiniert Eingabegerät und Funktionen mit Anzeigemöglichkeit in einem Gerät. Solche Benutzerschnittstellen existieren nicht nur am heimischen PC oder auf Smartphones, sondern kommen viel mehr stetig und überall vor. So finden wir Mensch-Computer-Schnittstellen an Bahnhöfen, Flughäfen, in Parkhäusern und öffentlichen Gebäuden. Grund hierfür ist die steigende Signifikanz von Computern und Systemen im Alltag des Menschen. Daher werden Möglichkeiten gesucht diese Systeme verständlich, einfach und bedienbar zu machen.

In dieser Arbeit wird es um Benutzerschnittstellen im Bereich von Gebäuden, genauer in Eigenheimen und Privathäusern gehen. Interessant ist die Vernetzung der einzelnen Teilkomponenten eines solchen Systems und besonders wichtig die Darstellung über geeignete Benutzerschnittstellen für den Nutzer. Im Folgenden soll es darum gehen, Bewertungskriterien für Benutzerschnittstellen aufzuzeigen, um diese beurteilen und vergleichen zu können.

doi: 10.2313/NET-2011-07-2_05

2. BEWERTUNGSKRITERIEN FÜR BENUTZERSCHNITTSTELLEN

Wie erwähnt existieren verschiedene Arten von Benutzerschnittstellen. In einem intelligent-vernetzten Eigenheim können diese verschiedenen Schnittstellen zur Mensch-Computer-Kommunikation vorkommen. Tatsächlich aber werden hauptsächlich Touchscreens und „Graphical User Interfaces“ in derartigen futuristischen Häusern verwendet. Um verschiedene Arten, Klassen und Ausprägungen in diesem Bereich bewerten und beurteilen zu können, werden diese nach bestimmten Gesichtspunkten und Merkmalen beleuchtet und untersucht. Solche Kriterien sind Adaptionsfähigkeit, Konsistenz, Benutzerfreundlichkeit, Nutzerbeanspruchung und Fehlerbehandlung. Diese fünf Kriterien sollen nun im Folgenden genauer beschrieben und erklärt werden.

2.1 Adaptionsfähigkeit

Nach Bastien handelt es sich bei der Adaptionsfähigkeit um die Eignung der Benutzerschnittstelle, je nach Anforderung der Situation und den Umständen der Umwelt, seine Bedienbarkeit anzupassen [1]. Auch die Adaption der Benutzerschnittstellen auf Bedürfnisse und Vorlieben des Nutzers ist Aufgabe einer anpassungsfähigen Mensch-Computer-Schnittstelle. Zudem geht es um die Art und Weise, wie die Komponenten des Systems, also verschiedene Sensoren und Aktoren, vernetzt sind. Hierfür existieren verschiedenste Standards zur Gerätevernetzung [9]. Die Adaptionsfähigkeit besteht aus zwei Teilbereichen. Zum Einen die Flexibilität, zum anderen die Erfahrungen des Nutzers.

2.1.1 Flexibilität als Teil der Adaptionsfähigkeit

Bei der Flexibilität einer Benutzerschnittstelle handelt es sich um die Fähigkeit des Interfaces, sich den aktuellsten Bedürfnissen des Nutzers situativ anzupassen [1]. Wichtig ist beispielsweise wie die Vernetzung der einzelnen Sensoren und Aktoren gelöst ist und in diesem Zusammenhang, wie flexibel diese im Raum aufgeteilt und verbreitet sind und dementsprechend wie häufig und intensiv eine Anpassung erfolgen kann. Je nach Gewohnheit und Anforderung ist es wünschenswert die individuell beste Interaktionsmöglichkeit zwischen Nutzer und System zu finden. Die Flexibilität stellt dar, wie formbar und anpassbar eine Benutzerschnittstelle ist. Hat ein Interface den Anspruch hohe Flexibilität zu besitzen, muss es fähig sein auf Änderungen der Anforderungen in Bereich Darstellung, Ausgabe, Eingabe etc. reagieren zu können. Beispielsweise passt eine flexible Benutzerschnittstelle die Helligkeit des Bildschirms je nach Intensität der Sonneneinstrahlung an. Ist es einer Benutzerschnittstelle dagegen nicht möglich auf Änderungen des Anforderungsgebildes zu reagieren, kann es als unflexibel bezeichnet werden [1].

2.1.2 Erfahrung des Nutzers als Teil der Adaptionsfähigkeit

Eine Benutzerschnittstelle mit Anspruch auf hohe Adaptionsfähigkeit muss anpassungsfähig sein. Aber nicht nur nach den Anforderungen eines Nutzers, sondern vielmehr den verschiedenen Fähigkeiten grundverschiedener Nutzer. Je nach dem, ob es sich beim Nutzer um einen erfahrenen Kommunikationspartner handelt, also ein Nutzer der bereits Erfahrung in der Interaktion mit dem System hat, oder ob es ein komplett unerfahrener Nutzer ist, muss die Schnittstelle reagieren. Ein erfahrener Nutzer kann mit komplizierten und vielen Informationen umgehen, um so die Effizienz zu steigern. Ein unerfahrener Anwender dagegen braucht klare, einfache und eindeutige Darstellung der Information. Deshalb sollte eine adaptive Benutzerschnittstelle jederzeit die Möglichkeit bieten das Interaktionsniveau je nach Anwender anzupassen. Besonders Wichtig ist, dass der Nutzer beim Austausch mit der Schnittstelle seine Fähigkeiten und Erfahrungen verbessert.

2.2 Beständigkeit

Beständigkeit beschreibt mit welcher Konstanz Namen, Formate, Prozesse und Abläufe behandelt werden. Das Einhalten von einmal gewählter Symbolik sorgt für Automatisierungsprozesse in der Handlung des Nutzers. Wichtig um hohe Beständigkeit und damit einfache Interaktion zu gewährleisten ist, in einem System Abläufe zu standardisieren und so für einheitliche und gleichbleibende Nutzerbedienung zu sorgen. Für den Bereich der futuristischen Eigenheime bedeutet dies beispielsweise, dass die graphischen Benutzerschnittstellen in den verschiedenen Räumlichkeiten des Heims alle eine einheitliche Benutzeroberfläche aufweisen. Für identische Funktionen sollte immer das gleiche Symbol gewählt werden. Ben Shneiderman versteht unter Beständigkeit etwa „die Durchgängigkeit von Terminologien und Visualisierungen“ [13]. Dies führt zum schnelleren Verständnis seitens des Nutzers und hat die Konsequenz, dass der Anwender durch gleichen Aufbau, direkt auf Eigenschaften schließen kann. Shneiderman unterscheidet die Beständigkeit in drei Teile. Innere, äußere und metaphorische Beständigkeit [13].

2.2.1 Innere Beständigkeit

Die innere Beständigkeit beschreibt, wie einheitlich Darstellung, Graphiken und Formen innerhalb einer Anwendung dargestellt werden. So sollte zum Beispiel das Symbol zum Speichern einer Datei immer das Gleiche sein und einheitlich gehalten werden. Ziel der inneren Beständigkeit ist, dem Nutzer Abläufe so analog zu gestalten, dass er langfristig ohne große Überlegung automatisierte Handlungen vollziehen kann.

2.2.2 Äußere Beständigkeit

Mit äußerer Beständigkeit wird die Durchgängigkeit beschrieben, mit der Programme untereinander übereinstimmend gestaltet sind. So zeigt die Erfahrung, dass Microsoft Word Nutzer relativ schnell den Umgang mit dem ähnlich gestalteten Microsoft Excel lernen können. Aufgrund der konsequent gleich gehaltenen Symbolik in der Benutzerschnittstelle, ist bei beiden Programmen die äußere Beständigkeit hier gut gelungen.

2.2.3 Methaphorische Beständigkeit

Methaphorische Beständigkeit beschreibt den Zusammenhang zwischen der realen Welt und einer Benutzerschnittstelle. Können wir Zeichen und Symbole in der Schnittstelle bestimmten Zuständen und Gegenständen aus der echten Welt zuordnen, fällt es dem Nutzer einfacher einen Zusammenhang zu Funktionalität herzustellen. So stellt beispielsweise der Schreibtisch in der Welt von Mac OS einen Ort dar, an dem Dokumente, Bilder und andere Dateien hinterlegt

doi: 10.2313/NET-2011-07-2_05

werden können. Wichtig ist also, dass dieser Zusammenhang zwischen echter Welt und Computersystem strikt eingehalten wird. Der Nutzer bekommt so die Möglichkeit intuitiv zu handeln und erhöht damit Bedienungskomfort, Effizienz und Übersichtlichkeit. Das Symbol für das Bedienen einer Lampe, sollte also auch in der Benutzerschnittstelle mit einem Lampen-ähnlichen Zeichen belegt werden.

2.3 Benutzerfreundlichkeit

Bei Benutzerfreundlichkeit handelt es sich um Führung und Unterstützung, sowie die Hilfestellung beim Bedienen einer Anwendung [1]. So ist das Ziel einer solchen Unterstützung, dem Nutzer stets informieren zu können wo er sich gerade im Programm befindet. Ebenfalls ist entscheidend, aufzuzeigen welche Möglichkeiten er hat und im Idealfall sogar was sein Verhalten für Auswirkungen mit sich bringt. Der Anwender kann so ebenso schnell lernen wie bedienen und die Anzahl der Fehler kann minimiert werden. Zudem geht es um die Art und Weise wie gesteuert wird. Ist die Bedienung intuitiv und einfach oder schwierig und kompliziert. Ziel einer Benutzerschnittstelle muss sein, die ideale Balance zwischen schneller, unkomplizierter und instinktiver Anwendbarkeit zu finden. Benutzerfreundlichkeit gliedert sich in vier Untergebiete: Steuerung, Bündelung, Rückmeldung und Lesbarkeit [1].

2.3.1 Steuerung

Steuerung meint, dass dem Nutzer immer seine Wahlmöglichkeiten aufgezeigt werden. Das heißt, dass der Anwender in jeder Situation in der er sich befindet Handlungsalternativen präsentiert bekommt und nur noch wählen muss, welche die für ihn situativ richtige ist. Außerdem soll dem Nutzer schon vor der nächsten Handlung gezeigt werden, was für Konsequenzen seine Entscheidung mit sich bringt. Aber auch der aktuelle Zustand und Inhalt des Systems soll dargestellt werden. Muss etwa das Datum eingegeben werden, so wird dem Anwender die Arbeit erleichtert wenn die gewünschte Reihenfolge von Tag, Monat und Jahr exemplarisch dargestellt wird. Diese Darstellungen helfen dem Nutzer die Zusammenhänge des Systems zu verstehen und so weniger Fehler zu machen.

2.3.2 Bündelung

Unter Bündelung ist die Darstellung von Begriffen, Daten und Elementen inklusive derer Beziehungen und Verknüpfungen zu verstehen. Hierbei ist die Anordnung der Daten ebenso wichtig, wie Format und Verflechtung. Werden die verschiedenen Gruppen von Daten (Texte, Bilder, Befehle etc.) für den Anwender dementsprechend visualisiert, kann er leichter Zusammenhänge und Unterschiede verstehen. Diese vernetzte Darstellung verhilft dem Nutzer zur leichteren Wiedererkennung, schnellerem Lernen und stellt so eine gute Benutzerführung dar. So ist es wichtig, dass beispielsweise sämtliche Illuminationsmöglichkeiten unter dem gleichen Menüunterpunkt anzuwählen sind. Befindet man sich dann in einem tieferen Menüpunkt, muss wieder die Bündelung, zum Beispiel nach Licht je Raum erfolgen. Diese Verstrickungen und Gruppierungen helfen dem Nutzer.

2.3.3 Rückmeldung

Beim Thema Rückmeldung geht es um die Art, Qualität und Geschwindigkeit mit welcher die Benutzerschnittstelle die Antworten, auf Anfragen oder Befehle des Nutzers darstellt. Sowohl Qualität als auch Geschwindigkeit liefern einen entscheidenden Faktor für die Zufriedenheit des Nutzers. Nur mit guter Rückmeldung kann der Anwender die Aktionen und Prozesse des Systems verstehen und dementsprechend handeln. Aber auch Antworten des Systems, die dem Nutzer nicht schnell durch die Benutzerschnittstelle gezeigt werden, können zu Ungeduld, Verwirrung und dann zu Fehlern im Verhalten des Anwenders führen. Braucht die Darstellung von Informationen oder beispielsweise die Anpassung der Lautstärke über einen Lautstärkebalken zu lange, so kann durch Mehrfachbedienung ein ungewünschtes Ergebnis folgen, oder es kommt sogar zu einem Fehler. Folglich sollte immer eine schnelle und verständliche Rückmeldung des Systems erfolgen.

2.3.4 Lesbarkeit

Entscheidend für jede Benutzerschnittstelle ist, dass sie für den Menschen lesbar erscheint. Ein „normaler“ Nutzer kann mit einer Darstellung in implementierungsnahem Quellcode nichts anfangen, deshalb ist es wichtig dem Anwender die Interaktionsmöglichkeit mit der Benutzerschnittstelle derart zu gestalten, dass dieser verstehen kann was im System passiert. Die Benutzerschnittstelle muss auch Kontraste, Helligkeit, Hintergrund, Zeilenabstand und Schriftgröße so darstellen, dass der Nutzer im Stande ist die Informationen einwandfrei zu lesen. Ist beispielsweise die Schriftfarbe ähnlich wie jene des Hintergrundes, so kann der Nutzer die Informationen nur schwer oder sogar gar nicht lesen.

2.4 Nutzerbeanspruchung

Bastien sieht in der Nutzerbeanspruchung die Art und Weise, wie eine Benutzerschnittstelle auf den Anwender wirkt. Die Schnittstelle kann komplett überladen sein, was die Folge hat, dass der Nutzer schnell überfordert ist und eigentlich einfache Sachverhalte aufgrund von visuellem Überfluss nicht mehr erkennen und verstehen kann. Dies führt zu deutlich weniger effektiver Mensch-Computer-Kommunikation. Oder anders: Mit Steigender Beanspruchung des Anwenders erhöht sich die Wahrscheinlichkeit, dass dieser Fehler macht. Entscheidend ist bei der Nutzerbeanspruchung, die Klarheit und Kürze sowie Informationsdichte der Benutzerschnittstelle [1].

2.4.1 Klarheit und Kürze

Das Kurzzeitgedächtniss des Menschen ist begrenzt, deshalb ist es sehr wichtig, ihn nicht mit zu viel Informationen auf einmal zu belasten. Folglich gilt als Ziel von Klarheit und Kürze in einer Benutzerschnittstelle, die Sachverhalte, Einträge, Fragen und Antworten so kurz und trotzdem so eindeutig wie möglich zu gestalten. Dadurch entsteht für den Nutzer einerseits der Vorteil, dass er weniger zu lesen und zu antworten hat, was zwangsläufig zu einer besseren Performance führt. Andererseits verringert sich die Wahrscheinlichkeit von fehlerhaften Eingaben und Kommandos, wenn der Sachverhalt klar und kurz dargestellt ist. Nur wenige Anwender haben Ambitionen einen langen Text zu lesen um eine simple Frage zu beantworten.

2.4.2 Informationsdichte

Bei der Informationsdichte geht es um die Menge an Informationen und Eindrücken einer Benutzerschnittstelle. So

doi: 10.2313/NET-2011-07-2_05

sollten nur die aktuell zur Aufgabe gehörenden Informationen angezeigt werden und den Nutzer konfrontieren. Zu viel und zu unwichtige Eindrücke und Informationen behindern den Anwender. Wird er durch verschiedenste, eigentlich irrelevante Anzeigen und Informationen irritiert, so hemmt das Effizienz und Komfort in der Interaktion mit der Benutzerschnittstelle.

2.5 Fehlerbehandlung

Bastien sieht in der Fehlerbehandlung, die Notwendigkeit Fehler zu vermeiden (Schutz vor Fehlern) [1]. Beim dennoch Auftreten sollen diese Fehler richtig eingeordnet (Art des Fehlers), ebenso koriegiert (Fehlerbehebung) und vermieden werden, damit sie nicht erneut auftreten. Wenn Fehler auftreten bedeutet dies automatisch Qualitätsverlust für den Nutzer, er wird in der Ausführung von Befehlen an das System behindert oder kann gewünschte Informationen nicht abrufen. Im Zuge von Effizienz, Arbeitsleistung und Freude gilt es Fehler stets zu vermeiden. Mindestens jedoch muss ein auftretender Fehler schnell und richtig behandelt werden können.

2.5.1 Schutz vor Fehlern

Im Idealfall existieren Fehler nicht, oder werden zumindest verhindert, bevor sie auftreten. Schutz vor Fehlern heißt, diese zu vermeiden. So können etwa Eingabefehler vermieden werden, wenn der Nutzer darauf hingewiesen wird, dass durch seine angestrebte Handlung etwas gelöscht oder überschrieben werden kann. Aber auch aufzeigen was der Befehl für Konsequenzen haben kann und haben wird. So können eventuelle Fehler noch rechtzeitig aufgehalten und ungewünschte Änderungen vermieden werden. Hierfür ist es aber zwingend notwendig, dass eine Benutzerschnittstelle existiert, welches die Fähigkeit besitzt dem Nutzer graphisch oder in Form einer Ausgabezeile mitzuteilen, was sein Verhalten für Konsequenzen mit sich bringt. Wird zum Beispiel die Eingabe der Adresse verlangt, so wäre es ratsam zu definieren in welche Reihenfolge die Parameter (Straße, Nr., PLZ etc.) angegeben werden sollen. Damit wird die Chance auf das Auftreten eines Fehlers, durch falsche Eingabe des Nutzers, reduziert.

2.5.2 Art des Fehlers

Kommt es trotz Fehlerschutz zum Auftritt eines solchen, ist es entscheidend diesen richtig einordnen zu können. Dafür muss die Art des Fehlers (Syntax, Semantik, Formal etc.) definiert werden. Zudem ist entscheidend, dass die Benutzerschnittstelle im Stande ist dem Nutzer mitzuteilen, um was für einen Fehler es sich handelt und wo dieser Auftritt. Handelt es sich beispielsweise um einen Eingabefehler, so kann der Nutzer mit einem guten Hinweis seitens des Systems, eventuell den Fehler beheben. So kommt es nebenbei zusätzlich zum Lerneffekt, und der Anwender wird den gleichen Fehler mit großer Wahrscheinlichkeit nicht erneut machen. Probleme tauchen dann auf, wenn der Fehler nicht im Zusammenhang mit der Schnittstelle steht, sondern im System liegt. Hier wird Fachwissen benötigt, was über die Fertigkeiten eines „normalen“ Nutzers reicht. Eine genauere Beleuchtung solcher Fehler führt im Rahmen dieser Arbeit aber zu weit.

2.5.3 Fehlerbehebung

Bei der Fehlerbehebung geht es darum, was für Möglichkeiten und Mittel der Nutzer hat, um die Fehler zu korrigieren. Dabei entscheiden Schwierigkeit, Größe und Tiefe des Fehlers darüber, wie einfach und ob der Fehler überhaupt durch den Anwender lösbar ist [1]. Einfach wäre es, wenn der Fehler durch das Zurücknehmen des letzten Befehls (z.B. klicken eines Symbols, berühren beim Touchscreen des Bestätigungsfeldes etc.) behoben werden kann.

3. BEISPIELE FÜR AKTUELLE BENUTZERSCHNITTSTELLEN IM BEREICH DER HEIMAUTOMATISIERUNG

Im Folgenden werden drei Beispiele aktueller Benutzerschnittstellen, welche bereits im Bereich der Heimautomatisierung angewand werden, gewählt. Hierbei handelt es sich um Benutzerschnittstellen, die durch Touchscreens oder einen Personal Computer mit einem entsprechenden „Graphical User Interface“ gesteuert werden können. Diese Benutzerschnittstellen werden nun anhand der erwähnten Kriterien untersucht.

3.1 denro ONE - Room Controller

Der denro ONE von denro ist eine Benutzerschnittstelle, welche als „Room Controller“ bezeichnet wird. Es ist eine Benutzerschnittstelle welche Raumfunktionen steuert [6]. Hierfür wird ein Touchscreen an eine beliebige Wand im Haus installiert, über welches der Nutzer mit dem System kommunizieren kann.

Abbildung 1: denro ONE

Beim denro ONE (siehe Abbildung 1) handelt es sich um einen Raum Manager, mit welchem es möglich ist, Licht, Elektrik, Heizung, Lüftung, Klima und Home Entertainment zu steuern. Bedient wird das Gerät über ein Touchpanel und einen Red Green Blue Drehknopf [3].

doi: 10.2313/NET-2011-07-2_05

3.2 Busch-ComfortPanel

Das Busch-ComfortPanel (siehe Abbildung 2) ist eine Benutzerschnittstelle welche Haussteuerungsfunktionen und „Entertainmentcenter“ vereint. Mit dieser Benutzerschnittstelle ist es möglich im Eigenheim Licht, Jalousien und Raumtemperatur zu steuern [2].

Abbildung 2: Busch-ComfortPanel

Aber auch die Sicherheit kann durch Informationsmeldung und Kameras, um welche das System beliebig erweitert werden kann, erhöht werden. Außerdem fungiert das Busch-ComfortPanel als Audio- und Videoplayer und kann, wenn mit dem Internet verbunden, aktuelles Wetter, Nachrichten aus Politik, Finanzen und Sport, sowie E-Mails abrufen und anzeigen. Auch bei dieser Benutzerschnittstelle handelt es sich um ein in das Haus integriertes Touchscreen, von welchem aus die Steuerung erfolgt.

3.3 mControl

Als dritte Benutzerschnittstelle wird die Digital Home Software mControl (siehe Abbildung 3) untersucht. Hierbei handelt es sich um eine Software, welche eine Benutzerschnittstelle für den Personal Computer, Touchscreens und mobile Geräte, wie Smartphones stellt.

Abbildung 3: mControl

Mit dem mControl können verschiedene Funktionen und Geräte im Haus gesteuert werden. Auch mit dieser Benutzerschnittstelle ist die Steuerung von Licht, Entertainment, Klima, Sicherheitssystemen, sowie Video und Audio Ausstattung möglich [12].

4. BEWERTUNG DER BENUTZERSCHNITTSTELLEN ANHAND DER KRITERIEN

4.1 Kriterium Adaptionsfähigkeit

Der denro ONE RoomContoller verwendet KNX als Bustechnologie, welche sowohl aus Bedienungkomponenten und den ausführenden Geräten besteht. Das macht es dieser Benutzerschnittstelle möglich, Funktionen im Raum und im Gebäude je nach Bedürfnis des Nutzers anzupassen [7]. Die Adaption ist nur möglich, wenn Sensoren und Aktoren überall verteilt sind und so dauerhaft eine Anpassung gewährleistet ist. Die Menüpunkte, die auf der „Home-Seite“ angezeigt werden sind vom Nutzer frei wählbar und können beliebig bezeichnet werden, was die Adaptionsfähigkeit des denro ONE noch zusätzlich erhöht.
Beim Busch-ComfortPanel erfolgt die Kommunikation der einzelnen Komponenten ebenfalls über den Vernetzungsstandard KNX. So ist es hier möglich, Sensoren und Kameras mit Bewegungsmeldern in Überwachungsbereichen auszustatten, was das Busch-ComfortPanel zu einer adaptionsfähigen Benutzerschnittstelle macht. Zusätzlich wird dies durch die Bereitstellung einer KNX-Telefonschnittstelle bestärkt. Außerdem kann das System flexible Anpassungen an die Bedürfnisse des Anwenders vornehmen, bevor dieser überhaupt das Haus betreten hat. Ist beispielsweise ein Raum nicht belegt, so kann diese Benutzerschnittstelle die Raumtemperatur energieeffizient absenken. Auch die Bedienung per Fernsteuerung über das Handy mit Hilfe von VNC-Client (Software, welche die Möglichkeit bereitstellt, auf einem entfernenten Rechner zu arbeiten) ist möglich. Daraus ergibt sich ein weiterer Vorteil bei der Adaptionsfähigkeit und Flexibilität des Busch-ComfortPanel, sowie in diesem Zusammenhang hohe Einsparung in Energie und damit Geld.
Die Benutzerschnittstelle mControl bietet eine solche Geräte- bzw. Hausvernetzung. Hier existiert die Möglichkeit, zwischen verschiedenen Vernetzungsmöglichkeiten (Z-Wave, KNX, ZigBee) zu wählen, was die Wahlmöglichkeit des Standards zur Vernetzung für den Anwender erhöht. Was besonders dadurch einen Mehrwert bedeutet, da der feste Standard für die Gerätevernetzung noch nicht gefunden ist. Diese Wahlmöglichkeit erweitert das Potenzial der Vernetzung, und schafft so einen Vorteil bei der Adaptionsfähigkeit [12]. Keine der Benutzerschnittstellen schafft eine nutzerspezifische Anpassung. So kann keines der Systeme auch bei einem erfahrenen und versierten Nutzer seine Oberfläche erweitern, sondern bleibt simpel und einfach, und folglich in den Fähigkeiten begrenzt.

4.2 Kriterium Konsistenz

Beim Busch-ComfortPanel ist im Bezug auf seine innere Konsistenz zu erkennen, dass Symbole und Zeichen aber auch Einstellungsfunktionen strikt einheitlich gehalten wurden. Beim mControl ist dies nicht der Fall. Man gewinnt hier den Eindruck, dass bei zunehmender Menütiefe, die grafische Benutzerschnittstelle immer knapper und dadurch nicht komplett konsistent erscheint.
Beim denro ONE ist die Einhaltung von Symboliken kontinuierlich. Die Benutzerschnittstelle ist konstant zwar einfach gehalten, aber es ist ein klarer roter Faden auch in der Tiefe von bis zu 32 Ebenen der Programmpunkte zu erkennen. Geht es um die äußere Konsistenz so ist beim Busch-

doi: 10.2313/NET-2011-07-2_05

ComfortPanel zu erkennen, dass auch bei der Fernsteuerung, etwa über ein Smartphone die gleiche Oberfläche zu erkennen und anzuwenden ist. Also kann hier auch eine hohe äußere Konsistenz festgestellt werden.
Das mControl kann auch über ein Smartphone ferngesteuert werden, allerdings lässt sich erkennen, dass es hier nicht so gut gelungen ist, die Konsistenz zwischen verschiedenen Geräten zu erhalten. So unterscheidet sich die Oberfläche je nach Anwendung bei verschiedenen Interfaces (Windows Vista Media Center, Internet Explorer oder Mobile Anwendungsbereiche).
Beschäftigt man sich mit der Methaphorischen Konsistenz, so ist das denro ONE eine gute Benutzerschnittstelle für intuitive, plausible und intelligente Wahl von Symbolen und Zeichen. Bei jedem Zeichen das angezeigt wird, ist sofort klar was es bedeutet und wofür es gedacht ist. Auch das Busch-ComfortPanel zeigt eine selbsterklärende Zeichenbelegung. Will man auf Musik zugreifen, so ist das Symbol mit der Musiknote zu wählen. Das ist selbsterklärend und schnell zu lernen. Das mControl dagegen gestaltet sich nicht durchgängig intuitiv. Die Schnittstelle wirkt häufig sehr implementierungsnah und deshalb sind teilweise nicht ideale und selbsterklärende Zeichen und Symbole gewählt und teilweise sogar nur mit ihrem Namen aufgelistet.

4.3 Kriterium Benutzerfreundlichkeit

Das denro ONE bietet in der Steuerung eine sehr gute Lösung. Die Bedienung der Benutzerschnittstelle läuft über ein Touchscreen mit aktiven Schaltflächen und über einen RGB-LED (Red Green Blue) Drehknopf. So ist es stets möglich, egal in welchem Menübereich man sich befindet, über das wählen des „Home-Buttons“ wieder direkt zurück ins Hauptmenü zu gelangen. Außerdem sind die verschiedenen Themengebiete im Homemenü so gruppiert und zusammengefasst, dass intuitiv klar ist, unter welchem Menüpunkt sich konkretere Anwendungen finde lassen. Dabei wird unter Home-Seite, Funktionsseite und Bedienungsseite unterschieden. Auch die Steuerung um zwischen den Menüseiten zu wechseln, ist mit stetig anwesenden Pfeilen für vorwärts und rückwärts Sprünge schnell und einfach gelöst. Die Rückmeldung darüber, ob die gewünschte Aktion erfolgreich war, wird mit Hilfe eines zwei-Farben Systems geregelt. Als Problem in Sachen Benutzerfreundlichkeit steht die Lesbarkeit, zwar ist mit den Symbolen meist klar was gemeint ist, jedoch fehlt für komplizierte Bereiche, wie beispielsweise die Wetterfunktion, mit vielen verschiedenen Parametern, genauere, eventuell in Worten verfasste Anweisungen.
Beim mControl funktioniert die Steuerung teilweise sehr kompliziert. Betrachtet man beispielsweise die Benutzeroberfläche mit Windows Media Center, wird klar das die Anwendung für das Bedienen mit einer Computermaus ausgelegt ist. Dennoch ist meist klar wo man sich befindet, da auch diese Benutzerschnittstelle eine Art Menühierarchie bietet. Die Rückmeldung der Schnittstelle ist klar und verständlich. Wählt man beispielsweise eine bestimmte Lampe im Raum an, so ist auf der Benutzeroberfläche klar zu sehen, ob diese an oder aus ist. Dies wird simpel mit Hilfe einer „ÀN“ bzw. „AUS“ Anzeige realisiert. Vorteil hierbei ist die klare Lesbarkeit. Es ist stets ersichtlich an welcher Stelle man sich im System befindet. Nicht zuletzt auch durch die in Worten beschriebenen Aktions- und Wahlmöglichkeiten. Als Sprache ist nur Englisch möglich, was die Benutzerfreundlichkeit für nicht-englisch Sprechende klar erschwert oder das Benutzen dieser Benutzerschnittstelle nahezu unmöglich macht. Dagegen bieten das denro ONE alle Zeichen nach ISO-8859-1 Standard und unterstützt so viele Sprachen.
Das Busch-ComfortPanel funktioniert mit direkter und einfacher Steuerung. So sind sogar Farbkombinationen je nach Anwendungsbereich logisch ausgewählt. Befindet man sich beispielsweise im Menüpunkt Licht, so funktioniert die Dosierung der Illuminationsstärke über einen Balken in gelb. Mit diesem Konzept werden themenverwandte Bereiche einfach gebündelt und für den Anwender verständlich angezeigt. Im unteren Teil des Touchscreens findet man auch stets das Hauptmenü, was ermöglicht jederzeit von einem Menü ins Nächste zu steuern. Klare Lesbarkeit am Busch-ComfortPanel ist absolut gegeben, nicht zuletzt durch die Wahlmöglichkeit der Hintergrundfarbe. Hier entsteht eine ausgewogene Kombination aus intuitiven Symbolen und geschriebenen Worten.

4.4 Kriterium Nutzerbeanspruchung

Beim Busch-ComfortPanel wird ein hoher Wert auf schönes und ästhetisches Design gelegt. Die Benutzerschnittstelle wirkt überlegt und stellt genau die erforderliche Menge an Informationen, welche für den Menschen richtig ist, dar. Außerdem sind sämtliche Anwendungsbereiche und Funktionen klar erkennbar und deutlich dargestellt. Auch bei unteren Menüpunkten ist die Darstellung noch deutlich und schafft eine ideale Benutzeroberfläche zur Mensch-Computer Interaktion.
Beim denro ONE ist die angezeigte Information der Oberfläche ebenfalls gut zu erkennen. Der Nutzer kann mit den angezeigten Symbolen interagieren, ohne durch zu ungenaue, überladene und unwichtige Eindrücke gestört zu werden. Diese extreme Reduktion auf nur wenige Symbole und Zeichen, wirkt aber schon fast zu oberflächlich. Um zu einem bestimmten, tiefer im Menü liegenden Unterpunkt zu gelangen, muss man einige Ebenen durchlaufen. Dies kann aufgrund der sehr geringen Informationsdichte zu Verwirrung seitens des Nutzers führen. Jedoch wäre das denro ONE dadurch auch von Kindern gut zu bedienen.
Das mControl dagegen findet ein gutes Mittel, zwischen klarer Informationsmenge und Dichte von Eindrücken. Der Nutzer weiß in jeder Ebene um was es geht und ist auch nicht mit der Menge überfordert. Nur in tiefen Menüunterpunkten ist zu erkennen, dass teilweise zu viel Information aufgezeigt wird. Diese Information ist dann zudem nicht klar strukturiert und so schwer zu verstehen und folglich kann dies zu Überforderung und Missverständnis seitens des Nutzers führen.

4.5 Kriterium Fehlerbehandlung

Die denro ONE Benutzerschnittstelle schafft durch ihre einfache Bedienung und klare Darstellung eine Umgebung, in der der Nutzer nur sehr selten Fehler bei der Eingabe machen. Kommt es trotzdem zur fehlerhaften Eingabe, kann der Anwender mit der Zurücktaste wieder einen Menüpunkt retour. Gibt der Anwender beispielsweise ein Datum im falschen Format ein, so wird er darauf hingewiesen. Es können aber auch Fehler auftreten, bei denen eine sprachspezifische Fehlermeldung nicht mehr möglich ist. Etwa wenn bestimmte Parameter bei der Benutzerschnittstelle nicht mehr übereinstimmen. Hier sind auch keine Designs zur Darstellung der Fehlermeldung vorhanden und der Nutzer hat so keine Möglichkeit bei Systemfehlern zu reagieren.

doi: 10.2313/NET-2011-07-2_05

Die Software mControl ist auch bei der Fehlerbehandlung abhängig von dem jeweiligen Gerät, auf dem es läuft. Am Beispiel mit Windows Vista Media Center ist zu sehen, dass es möglich ist, bei einfachen fehlhaften Eingaben mit einem Zurückbefehl wieder in einen Menüpunkt davor zu gelangen.
Beim Busch-ComfortPanel gibt es zwar keine Möglichkeit mit Pfeiltasten vor und zurück zu springen, aber diese wechseln in der Tiefe ist auch nicht nötig, da das Benutzerschnittstelle auch so alle nötigen Einstellungen bereithält. Durch die übersichtliche Gestaltung sind auch hier nur selten Eingabefehler seitens des Nutzers zu erwarten. Insgesamt ist festzustellen, dass einfache Eingabefehler bei allen Benutzerschnittstellen leicht zu sehen und zu verbessern sind, kommt es jedoch zu einem Fehler, der sich tiefer im System, dann ist es für den Nutzer schwer zu handeln. Es ist folglich nötig Experten einzubeziehen.

Tabelle 1: Ausprägung der Kriterien bei verschiedenen Benutzerschnittstellen (BCP = Busch-ComfortPanel)

	denro ONE	BCP	mControl
Adaptionsfähigkeit	mittel	gut	gut
Beständigkeit	gut	gut	schlecht
Benutzerfreundl.	gut	gut	mittel
Nutzerbeanspr.	gut	mittel	gut
Fehlerbehandlung	mittel	mittel	mittel

5. FAZIT

Das Busch-ComfortPanel vereint in meinen Augen die Erfüllung aller Kriterien am Besten. Sowohl Design der Benutzerschnittstelle, als auch Benutzerfreundlichkeit und Konsistenz sind hier an Besten gelöst.
Anhand der steigenden Anbieter und Produkte im Bereich der „Future Homes“ ist zu erkennen, dass solche Systeme zunehmend an Interesse gewinnen. Für die Zukunft ist zu erwarten, dass die Benutzerschnittstellen noch deutlich adaptionsfähiger werden. So sind etwa Schnittstellen denkbar, die allein durch Gedanken und Verhaltensmuster des Nutzers Anpassungen vornehmen und die Vorstellungen des Anwenders so verwirklichen [4]. Wie auch am denro ONE und Busch-ComfortPanel zu erkennen, stellt KNX als Standard für Datenübertragung in Heimautomatisation sowie Haus- und Gebäudetechnik eine gute Möglichkeit für die Gerätevernetzung dar [10]. Grund hierfür sind Effizienz, Sicherheit und auch geringerer Energieverbrauch mit KNX. Auch bei der Entwicklung von Konsistenz solcher Schnittstellen ist zu erkennen, dass die Anwendungen übergreifend vereinheitlicht werden. So ist das Ziel, die Benutzerschnittstellen im Haus, in jedem Raum, auf jedem mobilen Gerät und außerhalb des Hauses zu standardisieren. Daraus entsteht ein Gewinn im Alltag des Menschen. In Zukunft werden auch die Hardwarekomponenten erweitert werden. Neben Kameras und Displays werden auch Temperatursensoren, Lichtsensoren, Fingerscanner, Netzhautscanner und andere Komponenten mit dem System in Verbindung stehen.
Auch im Bereich der mobilen Geräte wird die Entwicklung weiter gehen. Während heute der Personal Computer oder ein zentral gelegenes Touchscreen als Anlaufstelle für Musik, Video und weiter Einstellungen existiert, wird in Zukunft jeder Raum mehrfach mit Interaktionsmöglichkeiten ausgestattet sein. Hier sind die Grenzen zur „Augmented Reality“ und zum „Ubiquitous Computing“ fließend. Meiner Meinung nach haben wir im Bereich der Benutzerfreundlichkeit jetzt schon ein sehr hohes Niveau erreicht. Die meisten Benutzeroberflächen sind schon heute sehr gut durchdacht.
Zusammenfassend ist festzustellen, das die Signifikanz der Heimautomatisierung zwar noch in ihren Kinderschuhen steckt, sich langfristig aber im Bereich des menschlichen Zuhauses etablieren und vermehren wird.

6. LITERATUR

[1] J. C. Bastien. Ergonomic Criteria for the Human-Computer Interfaces. *inria*, 2006.
[2] busch jaeger. Busch-ComfortPanel. http://www.busch-jaeger.de/de/gebaeudesystemtechnik/comfortpanel.htm.
[3] cebit. cebit-denro. http://www.cebit.de/de/ueber-die-messe/themen-und-trends/cebit-neuheiten/neuheiten-aus-forschung-und-entwicklung/unternehmen/denro-ag.
[4] C. Chapman. the-future-of-user-interfaces. http://sixrevisions.com/user-interface/the-future-of-user-interfaces/.
[5] constantine Stephanidis. constantine. http://www.imbb.forth.gr/.
[6] denro. denro ONE. http://www.denro.com/de/produkte.html.
[7] C. H. Hermann Merz, Thomas Hansemann. *Gebäudeautomation: Kommunikationssysteme mit EIB/KNX, LON und BACnet*. 2007.
[8] jeremy reimer. A History of the GUI. http://www.arstechnica.com/old/content/2005/05/gui.ars (28.3.2011, 14.05).
[9] knx. http://www.knx.de/. http://www.knx.de/.
[10] knx.org. knx2. http://www.knx.org/de/was-ist-knx/was-knx-ist/.
[11] linux. The Linux Information Project - GUI Definition. http://www.authone.de.
[12] mControl. mControl. http://www.embeddedautomation.com/products/index.asp.
[13] B. Shneiderman. 8 Goldene Regeln Ben Shneiderman. http://win2web.com/de.aspx?seite=Design/Tutorial.
[14] C. Stephanidis. *Interfaces For All*. Constantine Stephanidis, 2001.

doi: 10.2313/NET-2011-07-2_05

Standards zur Gerätevernetzung

Andy Großmann
Betreuer: Andreas Müller, Corinna Schmitt
Seminar Future Internet SS2011
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: andy.grossmann@mytum.de

KURZFASSUNG

Offene Standards zur Gerätevernetzung stellen den Schlüssel für zukünftige Geräte dar, die untereinander kommunizieren können, um uns ein neues Maß an Komfort und Effizienz zur Verfügung zu stellen.

Die heute etablierten kabel- und funkgebundenen Standards zur Gerätevernetzung bauen auf Standards wie Ethernet, WLAN und Bluetooth auf. Darüber können z.B. die Protokollfamilie TCP/IP oder Standards wie UDP betrieben werden. Besonders zu betrachten sind jedoch die Standards ab OSI Layer 5 aufwärts, da hier auch Informationen zur Geräte- und Funktionsbeschreibung übertragen werden können. Unter anderem werden Standards wie UPnP, Jini, SNMP usw. betrachtet. In der Heimautomatisierung kommen KNX, ZigBee und Z-Wave hinzu.

Zukunftsweisend zeigt sich hier der neue hardwareunabhängige Standard OSGi. Seine Architektur ist modular, skalierbar und besitzt einen dynamischen Aufbau. Das zugrundeliegende Programmiermodell basiert auf einer Java Virtual Machine (JVM). OSGi kann Schwächen anderer Standards beseitigt und ist in der Lage andere Standards auf eine sehr transparente Art und Weise zu integrieren [1, 2].

Doch die Gerätevernetzung von Morgen kann neben dem Komfortgewinn auch einen wesentlichen Beitrag im Rahmen der Energiesicherheit bieten. Die Übertragung von Information unterstützt Strom- und Kosteneinsparungen und ermöglichen eine ganz neue Qualität des Leistungsmanagement von Stromnetzen. Benötigt werden dazu Informationen wie Energieverbrauch und Betriebszeitpunkt auf Verbraucherseite und Informationen zur Einspeisung alternativer Energiequellen wie Solar- und Windkraftanlagen auf Produzentenseite.

Zur Umsetzung intelligenter Stromnetze (engl. Smart Grid) wird der auf OSGi aufbauende OGEMA Standard und der EEBus Standard betrachtet. Beide unterstützen gängige Standards zur Gerätevernetzung und entstammen dem Förderprojekt E-Energy des Bundesministerium für Wirtschaft und Technologie (BMWi) und dem Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU)[3].

Schlüsselworte

Gerätevernetzung, Heimvernetzung, intelligente Netze, Smart House, Residential Gateway, OSGi, UPnP, Jini, SNMP, EIB/KNX, ZigBee, Z-Wave, LCN, intelligentes Stromnetz, Smart Grid, Smart Energy, EEBus, E-Energy, OGEMA, BEMI

1. EINLEITUNG

Die Idee der Gerätevernetzung ist nicht neu, das intelligente Haus soll eine höhere Lebensqualität ermöglichen, indem Geräte miteinander kommunizieren können, von der Ferne aus gewartet und gesteuert werden. Auch das Energiesparen soll durch die Gerätevernetzung unterstützt werden. Jedoch soll trotz der ständig zunehmenden Technik im intelligenten Haus auch die Bedienung einfacher und intuitiver werden.

Die Attraktivität dieser Technologie wird deutlich wenn man sich einige Anwendungsbeispiele betrachtet.

Die Vernetzung von TV-Gerät, HiFi-Anlagen, Laptop, Lichttechnik, Heizungs- und Klimaanlage, sowie der Internetanbindung vereinfacht beispielsweise die Bedienung dieser Geräte, sie können nun zentral über ein Smartphone gesteuert werden und sich auch untereinander steuern. Beim Start eines Films, könnte das Abspielgerät ja nach Tageszeit das Raumlicht dimmen oder die Jalousie absenken, einen Beamer aktivieren und die Leinwand herunterfahren, sowie das Soundsystem aktivieren.

Im Urlaub sorgen automatische Fensteröffner für die Belüftung der Wohnung und die Lichttechnik simuliert ein bewohntes Heim. Vor Antritt der Heimreise wird die Heizungs- und Klimaanlage per Smartphone auf die gewünschte Temperatur reguliert. Das Auto ermittelt bei Bedarf automatisch die günstigste Tankstelle auf dem Heimweg und das moderne Verkehrsleitsystem lenkt Fahrzeuge an Staus vorbei und zeigt den nächsten freien Parkplatz am Ziel an.

Doch neben diesen Beispielen zum Komfortgewinn im privaten Bereich gibt es auch jede Menge Anwendungsbeispiele im öffentlichen Bereich und in der Wirtschaft. Dabei stellen

doi: 10.2313/NET-2011-07-2_06

Energiesicherheit und die Kosten für Energie wichtige Faktoren dar.

Mit dem Trend hin zu alternativen Energien, wie Solar- und Windkraftanlagen steigt auch das Risiko, dass die Netzstabilität durch Über- oder Unterspannung des Stromnetzes gefährdet ist.

Die Netzstabilität kann sichergestellt werden, indem eine moderne Lastreglung der Stromnetze realisiert wird. Diese benötigt zeitnahe Informationen zum Verbrauch und zur Produktion von Strom und kann sogar regulierend eingreifen, indem variable Strompreise das Konsumverhalten der Nutzer beeinflussen.

Mit Hilfe neuer Standards zur Gerätevernetzung können Informationen zum Strombedarf und Betriebszeitpunkt von Geräten verwendet werden, um den Strombedarf genau zu ermitteln oder Lastverschiebungen für Geräte mit variablen Betriebszeitpunkten zu ermöglichen. Strompreise könnten an die Verfügbarkeit gekoppelt werden und der Nutzer kann seinen Verbrauch Preisabhänig konfigurieren. Auch das Einbeziehen neuer Stromspeicher, wie die Akkumulatoren der Elektro- und Hybridfahrzeuge ist denkbar.

Den Schlüssel zum Durchbruch all dieser Technologien stellen Standards zur Gerätevernetzung dar. Doch der Erfolg eines solchen Standards hängt auch vom Erreichen einer Kritischen Masse ab, erst so wird es sich auch für die Wirtschaft lohnen auf spezielle Standards zu setzen.

Wichtige Eigenschaften für den Erfolg eines Standards zur Gerätevernetzung sind ein offenes, serviceorientiertes und herstellerübergreifendes Modell, mit klar definierten Schnittstellen und der Möglichkeit eine Geräte- und Funktionsbeschreibung zu übertragen.

Diese Arbeit behandelt bestehende Standards der Gerätevernetzung und geht dabei insbesondere auf das OSGi Framework ein. In einem zweiten Teil werden Standards vorgestellt, die um die Smart Grid Funktionalität (intelligentes Stromnetz) erweitert wurden [1, 3].

2. STANDARDS ZUR GERÄTEVERNETZUNG

„Ein Standard ist ein öffentlich zugängliches technisches Dokument, das unter Beteiligung aller interessierter Parteien entwickelt wird und deren Zustimmung findet. Der Standard beruht auf Ergebnissen aus Wissenschaft und Technik und zielt darauf ab, das Gemeinwohl zu fördern.“ [4]

Unter diesem Gesichtspunkt soll die Thematik Standards zur Gerätevernetzung in dieser Arbeit betrachtet werden.

2.1 Etablierte Standards zur Gerätevernetzung

Schon heute gibt es eine Vielzahl von Standards im Bereich der Gerätevernetzung, dabei sind Ethernet, WLAN und Bluetooth im ISO/OSI Modell den Layern 1 und 2 zugeordnet. Gebräuchliche Standards zur Gebäudeautomation sind EIB/KNX, ZigBee, Z-Wave und der LCN-Bus, sie werden ab Layer 3 aufwärts zugeordnet. Die Standards UPnP, Jini und SNMP werden den anwendungsorientierten Layern 5 bis 7 zugeordnet.

Die hier vorgestellten Standards sollen lediglich einen Einblick in verwendete Standards auf dem Weg zur Gerätevernetzung geben und haben keinen Anspruch auf Vollständigkeit.

Tabelle 1. ISO/OSI 7 Schichtenmodell

Layer	Einordnung	Protokolle
7 Anwendung	Anwendungs-orientiert	HTTP, FDP, XML, SOAP, UPnP, Jini, SNMP, ZigBee, KNX
6 Darstellung		
5 Kommunikation		
4 Transport	Transport-orientiert	TCP, UDP, ZigBee KNX
3 Vermittlung		IP, IPsec, ZigBee
2 Sicherung		Ethernet, WLAN, Bluetooth
1 Übertragung		

2.1.1 Der IEEE 802.3 Standard (Ethernet)

Das Ethernet ist ein kabelgebundener Standard im Bereich der LAN-Verbindungen. Auf ihn kann die Protokollfamilie TCP/IP und UDP betrieben werden. Dieser Standard stellt die meist verwendete Grundlage für standardisierte Technologien wie HTTP, XML und SOAP dar.

Die Bandbreite im Gigabit-Ethernet ist zur Zeit auf bis 100 Gigabit/s spezifiziert [2].

2.1.2 Der IEEE-802.11 Standard (WLAN)

Das Wireless Local Area Network (WLAN), ist ein funkbasierter Standard, genau wie im Ethernet laufen auf ihm Technologien wie TCP/IP und UDP und somit die darauf aufbauenden Standards. In der Praxis verfügt WLAN über eine Bandbreiten von 100 bis 120 Mbit/s und kann dabei handelsübliche Endgeräte auf einer Reichweite von bis zu 100 Meter auf freier Fläche erreichen. Ebenso ist es möglich über WLAN Ad-hoc-Netze aufzubauen, hier sind alle Geräte im Netz gleichwertig [2].

2.1.3 Der IEEE 802.15.1 Standard (Bluetooth)

Wie WLAN ist auch Bluetooth ein funkbasierter Standard, der eine Datenübertragung zwischen den Geräten über kurze Distanzen ermöglicht. Bluetooth baut dabei kleine Ad-hoc-Netze auf. Hauptzweck ist die kabellose Verbindung von mobilen Kleingeräte und ihren Peripheriegeräten [2].

2.1.4 IEEE 802.15.4 Standard (ZigBee)

ZigBee ist ein funkbasierter Standard für die Vernetzung von Haushaltsgeräten, Sensoren und verschiedensten aktiven Komponenten in Gebäuden auf Entfernungen von bis zu 100 Meter. Dabei nehmen die Geräte eine der folgenden Rollen ein: Endgerät, Router oder Koordinator [2, 5].

2.1.5 Z-Wave Standard

Z-Wave ist wie ZigBee ein funkbasierter Standard für die Heimautomatisierung des dänischen Unternehmen Zensys. Eine Besonderheit bei Z-Wave ist, dass es ein vermaschtes Netz aufbaut und jedes Gerät im Netz die Reichweite des Netzes erhöhen kann und Informationen redundante Wege gehen können [6].

doi: 10.2313/NET-2011-07-2_06

2.1.6 Der EN 50090 Standard (EIB/KNX)

Die Standards Europäische Installationsbus (EIB) und KNX beschreiben wie in einem Gebäude Sensoren und Aktoren miteinander kommunizieren. Ziel ist ein höherer Komfort und große Flexibilität durch Gebäudeautomation. Die Steuerung erfolgt dabei über einen Computer. Das KNX-Protokoll arbeitet via IP-Multicast (Vermittlungsschicht). Der KNX+ Standard ist sowohl für Funkt als auch Kabel gebundene Kommunikation definiert [7].

2.1.7 Der LCN-Bus

Der Local Control Network Bus (LCN-Bus) ist ein kabelgebundener Standard, der über das Stromnetz betrieben wird. Da jedoch eine zusätzliche Drahtleitung benötigt wird, sollte die Nutzung dieses Standards bereits beim Neubau von Gebäuden berücksichtigt werden. Der Standard stammt von dem Unternehmen Issendorff Mikroelektronik GmbH. Die Steuerung erfolgt über eine passende Software am Computer [8].

2.1.8 Der UPnP Standard

Universal Plug and Play (UPnP) ist auf Microsoft zurückzuführen und wird heute von dem UPnP-Forum spezifiziert. UPnP dient zur herstellerübergreifenden Ansteuerung von Endgeräten und läuft auf allen IP basierten Netzwerken wie Ethernet, WLAN, Bluetooth und FireWire. UPnP unterstützt standardisierte Technologien wie TCP, UDP, HTTP, XML, Multicast und SOAP. Die zentrale Kontrolle durch einen Residential Gateway ist bei UPnP optional. Die Besonderheit von UPnP ist, dass jedes Kontrollgerät in der Lage ist, vollautomatisch weitere UPnP fähige Endgeräte zu erkennen und in Betrieb zu nehmen [2, 9].

2.1.9 Der Jini Standard

Jini ist ein auf Java basiertes Framework des Unternehmens Sun Microsystems. Dabei setzt es ein existierendes Netzwerk zwischen den einzelnen Geräten voraus. Mit dem Jini Framework soll es ermöglicht werden verteilter Anwendungen derart zu programmieren, dass möglichst flexibel Dienste im Netzwerk bereitgestellt werden können [10].

2.1.10 Der SNMP Standard

Das Simple Network Management Protocol (SNMP) dient der zentralen Überwachung und Steuerung von Geräten im Netzwerk. Dabei wird lediglich der Aufbau der Datenpakete und der Kommunikationsablauf geregelt. Als Besonderheit kann SNMP nicht nur in IP basierten Netzwerken eingesetzt werden, sonder arbeitet auch mit den Standards SPX/IPX und AppleTalk. Entwickelt wurde SNMP von der Internet Engineering Task Force (IETF) [11].

2.1.11 Zwischenbetrachtung

Für eine weitgehende kommunikative Vernetzung von Geräten der verschiedensten Hersteller existieren bereits viele Standards. Jedoch fehlte den hier vorgestellten Standards eine einheitliche Schnittstelle. Solch eine Schnittstelle sollte hardwareunabhängig, offen, dynamisches, skalierbar und serviceorientiert sein.

2.2 Der OSGi Standard

Die OSGi Plattform stellt einen solchen Standard dar. Urheber ist die OSGi-Alliance (Open Services Gateway Initiative), ein Industriekonsortium bestehend aus Großunternehmen wie der IBM Corporation, Siemens AG, SAP AG, Oracle Corporation, der Deutsche Telekom und vielen weiteren großen und kleineren Unternehmen, unter anderem aus dem Open Source Software-Bereich [1].

Die OSGi Plattform ist ein offener Standard der lediglich Programmierschnittstellen (APIs) und Testfälle definiert und eine Referenzimplementierung zur Verfügung stellt. Die OSGi Plattform bietet ein OSGi Programmiergerüst (aktuell Version 4.1), dass als übergeordnete Schicht auf eine Java Virtual Machine (JVM) aufbaut [1, 12].

2.2.1 Wesentliche Eigenschaften von OSGi

Nach Heiko Seeberger (Technical Director Weigle Wilczek GmbH) zählt zu den drei wesentlichsten Eigenschaften, die die OSGi-Plattform bietet, zum einen die Modularisierung. OSGi bietet oberhalb der Package-Ebene in Java klar definierten öffentlichen Schnittstellen und Abhängigkeiten für seine Bundles (Module). Eine zweite, wesentliche Eigenschaft ist, dass Bundles zur Laufzeit eingespielt, aktualisiert und wieder entfernt werden können, also dynamisch sind. Die dritte wesentliche Eigenschaft von OSGi ist das serviceorientierte Programmiermodell. Bundles können, nach der Registrierung in der OSGi Service Registry, ihre Objekte als Service bereitstellen, welche wiederum von anderen Bundles verwendet werden können [13].

Besonders aus Sicht der Hersteller von Servicelösungen und Geräten für das Smart Home stellt die Kombination dieser drei Eigenschaften deutliche Vorteile dar.

Die Entwicklungskosten können durch ein breites Angebot an Standardservices und die lose Kopplung der Bundles, sowie der guten Testbarkeit und Wiederverwendung eingespart werden. Die klare Trennung von API und Implementierung erhöht die Flexibilität und das standardisiertes Lifecycle-Management spart Betriebskosten [13].

2.2.2 Die OSGi Gesamtarchitektur

Die OSGi Spezifikation liegt in Form einer Core Specification und eines Service Compendium vor, es definiert das OSGi Framework sowie die OSGi Standard Services [14].

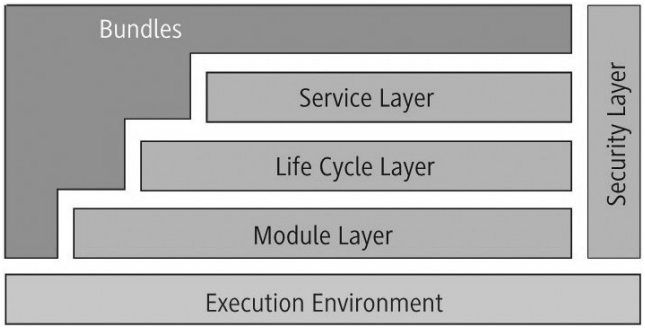


Abbildung 1: Die OSGi Architektur [11]

doi: 10.2313/NET-2011-07-2_06

Die Abbildung 1 zeigt das OSGi-Framework, bestehend aus einer Reihe von Schichten, die aufeinander aufbauen. Sie erweitern das durch Java und der JVM vorgegebene Modell um die bereits beschrieben drei Eigenschaften Dynamik, Modularisierbarkeit und Serviceorientierung.

Die Ausführungsumgebung ist auf verschiedenen Java fähigen Hardware-Plattformen lauffähig und spezifiziert lediglich welche Klassen, Interfaces und Methoden vorhanden sein müssen, damit ist OSGi hardwareunabhängig.

Die unterste logische Schicht definiert als kleinste Einheit im OSGi-Framework das Bundle (Modul). Bundles können eigenständig installiert und genutzt werden. Jedes Bundle muss sein Abhängigkeiten in einer standardisierten Forum innerhalb der Datei MANIFEST.MF hinterlegen.

Die Life Cycle Layer definiert den Managementagenten, der ein Interface zum OSGi Framework implementiert, von dem die Bundle-Zustände gesteuert werden können.

Damit ein Bundle genutzt werden kann und auch von anderen Bundles gefunden wird, muss es sich über die Service Registry im OSGi-Framework registrieren. Die Registrierung ist dabei nur während der Laufzeit aktiv [14].

Die Standardservices nehmen im OSGi-Framework eine wichtige Rolle ein. Sie implementieren verschiedenste Lösungen und können von anderen Bundles genutzt werden. Unter anderem gehören dazu ein standardisierter Log-Service, ein HTTP-Service, ein UPnP-Service, einen XML-Parser-Service und viele weitere Services. Dadurch garantiert das OSGi-Framework, auf einer sehr transparenten Art und Weise, andere Standards zu integrieren [1].

Die Security Layer bietet Mechanismen die auf dem Java-Sicherheitsmodell basieren, daher können Ausführungsrechte einzelner Bundles gezielt eingeschränkt werden [14].

2.2.3 Fazit zum OSGi-Framework

Die OSGi-Plattform bietet für die Vernetzung von intelligenten Endgeräten, die Möglichkeit der klassischen Fernsteuerung, des Fernmanagement, sowie der Installation neuer Service-Komponenten im laufendem Betrieb. Dabei kann OSGI verschiedene Standards wie Ethernet, WLAN, EIB/KNX, UPnP, und viele weitere nutzen und stellt den bisher aussichtsreichsten Standard im Bereich der Gerätevernetzung dar.

Bereits heute existieren neben der Referenzimplementierung eine Vielzahl an kommerziellen und freien (Open Source) Implementierungen [1].

Doch wie zu Beginn dieser Arbeit beschrieben, liegen noch weitere Potentiale in der Gerätevernetzung. Zu ihr gehört die intelligente Vernetzung des Stromnetzes. Standards die diese Smart Grid Funktionalität unterstützen wollen, müssen über eine erweiterte standardisierte Geräte- und Funktionsbeschreibung verfügen und spezifische Funktionen bereitstellen.

3. DAS INTELLIGENTE STROMNETZ

Betrachtet man nun die Möglichkeit in der Gerätevernetzung auch die Stromnutzung intelligent zu steuern, bieten sich weitere Möglichkeiten, die über den Ansatz des Smart Home weit hinaus reichen. Das intelligente Stromnetz (engl. Smart Grid) ist eine großflächige kommunikative Vernetzung von Stromerzeugern, elektrischen Verbrauchern, Speicherquellen und deren Netzinfrastruktur zur Steuerung und Überwachung des Strombedarfs [15].

3.1 Das aktuelle Stromnetz in Europa

Der heutige Strommarkt in Europa zeichnet sich durch die zentralisierte Bereitstellung von Strom über ein weit vernetztes Stromnetz aus. Doch schon heute ist ein deutlicher Trend zu dezentralen Stromerzeugungsanlagen zu erkennen. Betrachtet man die Zunahme von kleinen Kraft-Wärme-Kopplungsanlagen, Windkraftanlagen, Solarthermische- und Photovoltaikanlagen, sowie Biogasanlagen im Bereich des Kleingewerbe und der Ein- und Mehrfamilienhäuser in den letzten Jahren [16, 17].

Die Folge ist eine deutlich komplexere Struktur des Stromnetzes, besonders im Bereich der Lastregelung, was zu zunehmenden Risiken im Bereich der Netzstabilität führen kann. Besonders die Einspeisung von Strom aus Wind- und Solarkraftwerken unterliegt einer stark schwankenden Stromproduktion und führt somit zu unvorhersehbaren Schwankungen in der Netzeinspeisung. Zusammen mit unvorhersehbarer Spitzenlast stellt dies eine zunehmende Gefahr für das Stromnetz dar. Wie anfällig unser weit verzweigtes Stromnetz ist, zeigte am 6. November 2006 ein großflächige Stromausfall in vielen Teilen Europas. Ursache war die Abschaltung einer Starkstromleitung für die Durchfahrt eines Kreuzfahrtschiffes, welche erst eine Überlastung im nordwestdeutschen Netz zufolge hatte und danach eine Kettenreaktion auslöste, die sich auf große Teile Europas fortsetzte [18].

3.2 Die Idee des intelligenten Stromnetzes

Die Möglichkeiten, die eine kommunikative Vernetzung vom Stromerzeuger bis hin zum elektrischen Verbraucher bietet sind vielseitig, dabei soll das intelligente Stromnetz nicht nur die Netzstabilität der Zukunft sicherstellen, sondern auch zum Energiesparen beitragen.

Um Unterspannung zu verhindern werden Energieversorgungsnetze auf die mögliche Höchstbelastung ausgelegt, dabei gibt es vorhersehbare und unvorhersehbare Spitzenlast. Besonders letztere stellt eine Gefahr für die Netzstabilität dar und kann durch intelligente Stromnetze deutlich reduziert werden.

Da viele elektrische Verbraucher eine Flexibilität in ihren Betriebszeitpunkten besitzen, ohne dabei in ihrer Funktionalität beeinträchtigt zu werden, ist es im intelligenten Stromnetz möglich, die Spitzenlast deutlich zu reduzieren, indem Lastverschiebungen durchgeführt werden [19].

Gemäß dem Fraunhofer Institut entsteht über 40% des Energieverbrauchs in Deutschland in und an Gebäuden [19]. Dabei entfallen wiederum 80% dieses Stromverbrauchs auf elektrische Verbraucher, die ihrem Betriebszeitpunkt variieren können [18]. Doch auch in Industrie und Wirtschaft ist eine zeitliche Verlagerung des Stromverbrauchs möglich. Dabei ist eine solche Verlagerung je nach Anforderung des elektrischen Verbrauchers von wenigen Minuten bis hin zu vielen Stunden möglich.

doi: 10.2313/NET-2011-07-2_06

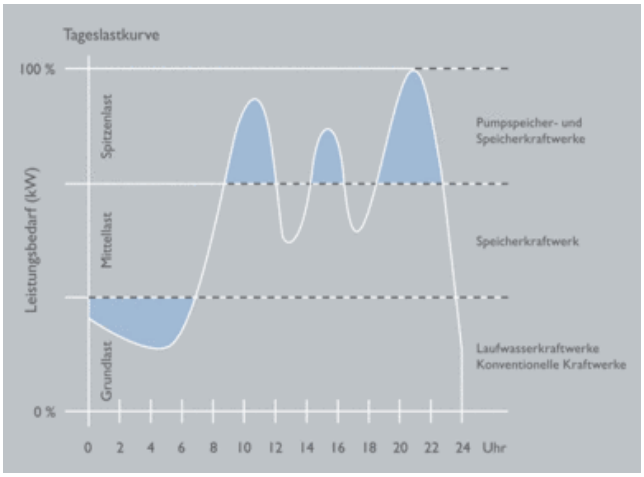


Abbildung 2: Beispiel des Stromlastverlauf eines Tages [29]

Doch auch die Speicherung von Energie spielt im intelligenten Stromnetz eine wichtige Rolle, beispielsweise kann in der Nacht kostengünstig Energie in Pumpspeicherwerken oder auch in den Batterien von Elektro- und Hybridautos gespeichert werden. Dazu müssten Fahrzeuge und Parkplätze dafür ausgelegt werden, Strom auch wieder in das Netz zurückzuspeisen. Die Regulierungsleistung, könnte sehr groß sein, besonders unter dem Gesichtspunkt, dass Autos im Durchschnitt 95% der Zeit nicht betrieben werden.

Die dezentralisierte Stromerzeugung wird durch virtuelle Kraftwerke ermöglicht, welche aus einem Verband mehreren kleiner kommunikativ Vernetzten Stromerzeuger besteht, die dabei ihren Strom auch direkt in das Niederspannungsnetz oder das Mittelspannungsnetz einspeisen [21].

Erst das Zusammenspiel von Stromerzeugung, Speicherung, Netzmanagement und Verbrauch, in einem Smart Grid System, ermöglicht es den Stromverbrauch deutlich zu reduzieren. Die Kostenreduzierung wird durch zwei Faktoren erreicht. Zum einem wird nur der Strom produziert, der auch nachgefragt wird und zum anderen kann man durch Lastverlagerung die Produktion der kostenintensiven Spitzenlast vermeiden (vgl. Abbildung 2). Als Nebeneffekt der besseren Vorhersagbarkeit von Strombedarf und Stromproduktion entsteht eine neue Qualität der Netzstabilität.

In Deutschland wird das intelligente Stromnetz durch das E-Energy Projekt des Bundesministerium für Wirtschaft und Technologie (BMWi) und des Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU) gefördert. Dabei wird die Auswirkung dieser Technologie in sechs Modellregionen untersucht [3].

Im Folgenden werden zwei Standards, die aus dem E-Energy Projekt stammen. Vorgestellt. Das OGEMA-Framework und der EEBus.

3.3 Der OGEMA Standard

Die Open Gateway Energy Management Alliance (OGEMA) ist ein Konsortium aus Forschung und Industrie. Federführend ist das Fraunhofer Institut für Windenergie und Energiesystemtechnik (IWES). Das IWES arbeitet dabei mit Partnern des E-Energy-Projekt Modellstadt Mannheim zusammen. Darunter zählen Unternehmen wie MVV Energie, IBM Deutschland und der Solargroßhändler Entrason [19].

Ziel der OGEMA ist es, eine offene Software-Plattform für Energiemanagement anzubieten, mit der beteiligte Unternehmen und Entwickler Ideen zur Nutzung von Smart Grid, effizient umsetzen können. Das OGEMA Framework soll dabei ähnlich wie im Smartphonebereich ein breites Angebot an Applikationen entstehen lassen. Somit soll den Bedürfnissen von Privathaushalten über öffentlichen Einrichtungen bis hin zum Gewerbe und der Industrie entsprochen werden.

3.3.1 Die OGEMA Architektur

Einen interessanten Weg hat man mit der OGEMA Architektur genommen, indem das OGEMA Framework auf den vielversprechenden OSGi Standard aufbaut, wie in Abbildung 3 zu sehen.

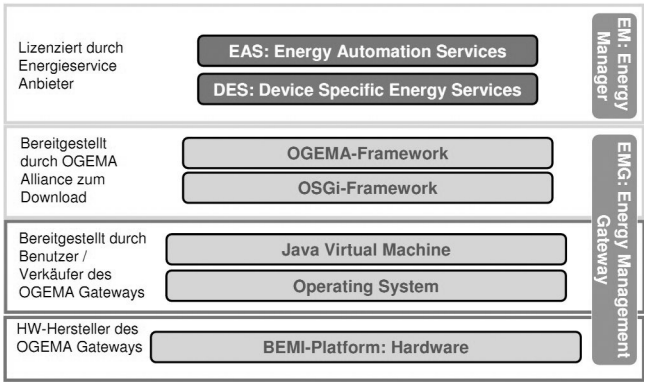


Abbildung 3: Die OGEMA Architektur [22]

Basis für das OGEMA Framework bildet das Bidirektionale Energiemanagement Interface (BEMI), ebenfalls eine Lösung des Fraunhofer IWES aus dem Jahre 2007. Besonderheit hier ist die dezentrale Steuerung im Smart Grid.

Die Abbildung 3 zeigt das Zusammenspiel von „Energy Manager“ und „Energy Management Gateway“ auf Basis der BEMI Hardware [22].

3.3.2 Das OGEMA Framework

Das OGEMA Framework ist in vier Schichten gegliedert (vgl. Abbildung 4).

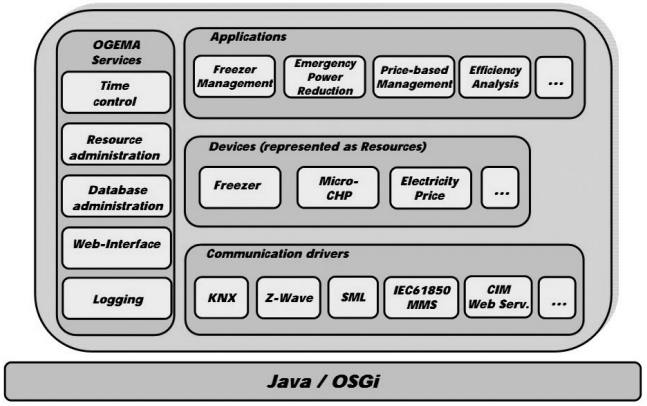


Abbildung 4: Das OGEMA Framework [22]

doi: 10.2313/NET-2011-07-2_06

Die OGEMA Services Schicht stellt die Standardservices wie Zeitkontrolle, Administration, Log Service, sowie ein Web Interface Service zur Verfügung.

Für die Kommunikation stehen Standards für die Heimautomatisierung wie die KNX und Z-Wave, der Common Information Model Standard (CIM), der für das Management von IT-Systemen ausgelegt ist [24], sowie viele weitere Standards zur Gerätekommunikation bereit.

Die Geräteschicht bildet die am OGEMA Gateway registrierten Sensoren und Aktoren ab, wie kleine Kraft-Wärme-Kopplungs-Anlagen, Lichttechnik und andere Endgeräte. Die Registrierung der Endgeräte erfolgt vollautomatisch (Plug & Play) [22, 23].

Die Applikationsschicht definiert konkrete Applikation auf die ein Nutzer Zugriff hat. Anbieter von Software können ihre Produkte ohne das Offenlegen des Sourcecode in OGEMA einbinden [23].

3.3.3 Das Zusammenspiel im OGEMA Ansatz

Einen Überblick über das Zusammenspiel im OGEMA-Ansatz liefert die Abbildung 5. Die Nutzerinteraktion erfolgt über ein Terminal (User display). Endkunden sollen damit ihren Energieverbrauch steuern können. Die Konfiguration der Energieverbraucher versetzt den Nutzer in die Lage automatisch Strom zu verwenden, wenn dieser kostengünstig ist. Auf diese Weise entsteht eine Selbstregulierung des Energieverbrauchs entsprechend des Preises und Angebots. Sicherheit vor Manipulation und Datenschutz soll die Firewall Funktionalität des OGEMA Gateway bieten, da das Gateway zwischen dem privaten Bereich des Kunden und dem öffentlich zugängigen Bereich der Dienstanbieter und Energieversorgungsnetze liegt. Den Serviceanbietern und Leitstellen der Energieversorger stehen ebenfalls offene Schnittstellen zur Integration in das OGEMA Smart Grid zur Verfügung [23].

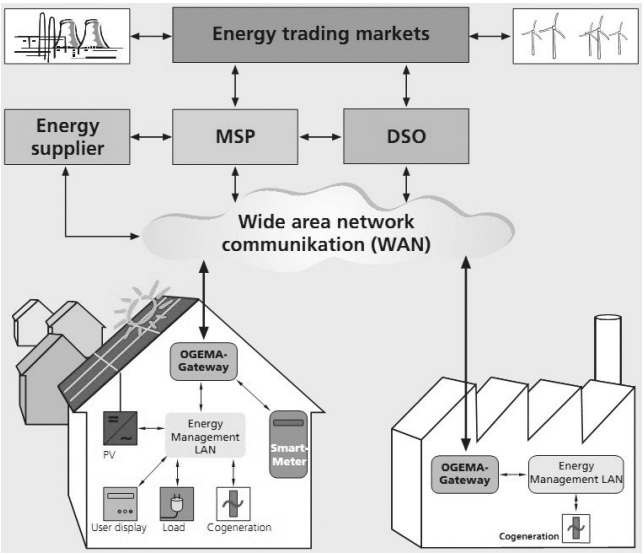


Abbildung 5: Das Zusammenspiel im OGEMA Ansatz [22]

3.4 Der EEBus Standard

Genau wie der OGEMA Standard stammt auch der EEBus Standard aus dem Förderprogramm E-Energy des BMWi und BMU und gehört dort zum Subprojekt Smart Watts [3, 27].

Gemäß [26] „beschreibt der EEBus die Nutzung bestehender Kommunikationsstandards, und -normen mit dem Ziel, Energieversorgern und Haushalten den Austausch von Anwendungen und Diensten zur Erhöhung von Komfort und Effizienz zu ermöglichen.

Zu diesem Zweck stellt der EEBus eine anwendungsneutrale, genormte Schnittstelle bereit.“

3.4.1 Architektur des EEBus

Der EEBus definiert lediglich die Schnittstelle zwischen allen Geräten im Gebäude und den Energieversorgern. Die Kommunikation zum Energieversorger über die Netzinfrastruktur definiert der EEBus nicht, um mehrere Lösungen zu ermöglichen [27].

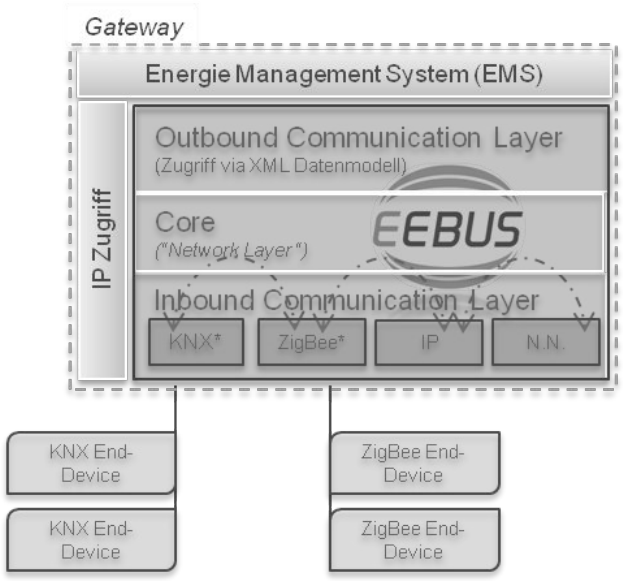


Abbildung 6: Die EEBus Architektur [26]

Wie in Abbildung 6 zu sehen unterscheidet der EEBus die Kommunikation in einer internen (Inbound Communication Layer) und einer externen (Outbound Communication Layer) Kommunikation.

Die Gebäudeinterne Kommunikation erfolgt über die bereits integrierten Standards KNX, ZigBee und TCP/IP. Gemäß [29] sind die Standards UPnP und LoWPAN sind in Vorbereitung. KNX kann im Bereich der kabelgebundenen Datenübertragung per Stromleitung (KNX Powerline) und per Funk (KNX RF) genutzt werden. Alternativ steht mit ZigBee eine weiterer funkgebundener Standard verwendbar, was die Wahl möglicher Endgeräte erhöht. Über die Protokollfamilie TCP/IP kann eine Verbindung zum Ethernet hergestellt werden.

Interessant ist, dass der EEBus sowohl auf Softwareebene, als auch auf Hardwareebene über einen Modularen Aufbau verfügt.

doi: 10.2313/NET-2011-07-2_06

Dadurch wird es ermöglicht in bestehender Hardware neue Standards zu integrieren.

Die externe Kommunikation des EEBus erfolgt über standardisierte XML-Dateien.

Kern der EEBus Architektur ist die Network Layer, sie vermittelt zwischen den im Gebäude installierten Geräten und ermöglicht deren Kommunikation untereinander und interpretiert die XML-Daten der externen Kommunikationspartnern für die jeweiligen Endgeräte im Gebäude [27].

3.4.2 Die Erweiterungen bestehender Standards

Das Problem der teilweise fehlenden Möglichkeit bestehender Standards einer Smart Grid spezifischen Geräte- und Funktionsbeschreibung entgegnet EEBus indem diese Informationen zum Energiemanagement ergänzt werden.

Unter anderem gibt es auch eine direkte Zusammenarbeit mit der KNX-Association, aus der der Standard KNX PL+ stammt. KNX PL+ besitzt eine um 15-fach höhere Bandbreite [26, 7].

3.4.3 Der EEBus im Projekt Smart Watts

Wie beschrieben stellt der EEBus im Projekt Smart Watts die Schnittstelle zwischen hausinterner Kommunikation und den Energieversorgern dar. Die Kommunikation zwischen den Energieversorgern und der Stromnetzinfrastruktur bis zum Gebäude wird separat erarbeitet. Im Smart Watts Projekt ist ein eigenes Netzwerkadresssystem für die Kommunikation vorgesehen. Eine Datenzentrale soll Daten sammeln und aufbereiten um einen Mehrwert für den Endnutzer zu generieren [28].

4. AUSSICHTEN UND FAZIT

Im Bereich der allgemeinen Gerätevernetzung stellt OSGi einen zukunftsweisenden und vielversprechenden Standard dar. Seine offene, hardwareunabhängige, skalierbare und dynamische Struktur, sowie das serviceorientierte Programmiermodell ermöglicht es beispielsweise jedem Unternehmen und Softwareentwickler sehr flexibel weitere Kommunikationsstandards in das OSGi zu integrieren. Einer großflächigen Geräteintegration stehen damit weniger Steine im Weg.

Vor dem Hintergrund immer knapperer Energieressourcen und der aktuellen Diskussion um die Kernkraft, wird die Entwicklung der intelligenten Stromnetze von besonderem Interesse sein. Grundlage könnte einer der vorgestellten Standards mit Smart Grid Funktionalität sein. Denkbar ist, dass auch der EEBus OSGi unterstützt oder OSGi selbst um Standardservices mit Smart Grid Funktionalität ergänzt wird.

Letztlich wird der Erfolg von OSGi, OGEMA und EEBus vom erreichen der Kritischen Masse abhängen, so dass Produkte und Servicelösungen wirtschaftlich hergestellt werden können. Und wie bei anderen modernen Technologien werden auch hier staatliche Subventionen einen entschiedenen Beitrag leisten können. Für Prognosen ist es jedoch noch zu früh.

5. LITERATUR

[1] OSGi Alliance, Zugriff April 2011, http://www.osgi.org/About/Mission, http://www.osgi.org/About/Technology, http://www.osgi.org/About/Members

[2] Internetauftritt der IEEE, Zugriff April 2011, http://www.ieee802.org/11/index.shtml, http://grouper.ieee.org/groups/802/3/index.html, http://grouper.ieee.org/groups/802/15/index.html

[3] E-Energy Smart Grids made in Germany, Zugriff April 2011, http://www.e-energy.de/de/auf_einen_blick.php

[4] British Standards Institute, Zugriff April 2011, http://www.bsigroup.com

[5] ZigBee Alliance, Zugriff April 2011, http://www.zigbee.org/Specifications/ZigBee/Overview.aspx

[6] Z-Wave Alliance, Zugriff April 2011,http://www.z-wavealliance.org/modules/AboutUs/

[7] KNX-Association, Zugriff April 2011, http://www.knx.org/knx-standard/knx-specifications/

[8] Issendorff Mikroelektronik GmbH, Zugriff April 2011, http://www.lcn.de/einleitung1.htm

[9] UPnP-Forum, Zugriff April 2011, http://upnp.org/sdcps-and-certification/resources/whitepapers/

[10] Sun Microsystems Jini, Zugriff April 2011, http://sunsite.uakom.sk/sunworldonline/swol-08-1998/swol-08-jini.html

[11] SNMP, Zugriff April 2011, http://www.snmp.com/products/technology.shtml

[12] Dr. Susan Schwarze, Was sind die Vorteile einer OSGi-Lösung für Hersteller und Service Provider?, http://test.osgi.org/wiki/uploads/News/ArtikelVorteileOSG-EmbeddedWorld03.doc

[13] IT-Republik, Erste Schritte mit OSGi, Zugriff April 2011, http://it-republik.de/jaxenter/artikel/Erste-Schritte-mit-OSGi-2077.html

[14] IT-Republik, Das OSGi Framework, Zugriff April 2011, http://it-republik.de/jaxenter/artikel/Das-OSGi-Framework-2221.html

[15] Normungsroadmap E-Energy / Smart Grid Deutschland, http://www.smartgrid.ch/images/normungsroadmap_smart_grid.pdf

[16] Arnold Picot, Karl-heinz Neumann, E-Energy: Wandel und Chance durch das Internet der Energie, 2009 ISBN 978-3-642-02932-5

[17] European SmartGrids Technology Platform, http://ec.europa.eu/research/energy/pdf/smartgrids_en.pdf

[18] Die Zeit, Stromausfall in Europa am 6. November 2006, http://www.zeit.de/online/2006/45/Stromausfall

[19] Start des ersten Home-Automation-Betriebssystems für intelligente Netze, Pressemeldung Fraunhofer, 2009,

doi: 10.2313/NET-2011-07-2_06

http://www.iset.uni-kassel.de/public/IWES_PM_OGEMA_2009-11-25.pdf

[20] Bundesverband der Energie- und Wasserwirtschaft, Zugriff April 2011, http://www.bdew.de/bdew.nsf/id/DE_BDEW-Jahresstatistik

[21] Forschungsstelle für Energiewirtschaft e. V., Zugriff Aprill 2011, http://www.ffe.de/taetigkeitsfelder/technikanalysen-und-energiemanagement/156

[22] Open Gateway Energy Management Alliance Concept, Zugriff April 2011, http://www.ogemalliance.org/downloads/ogema-alliance_20100119.pdf

[23] OGEMA Technology-brief, Zurgiff April 2011, http://www.ogemalliance.org/downloads/ogema_technology-brief.pdf

[24] The Common Information Model (CIM), Zugriff April 2011, http://www.dmtf.org/standards/cim

[25] E-Energy-Projekt Modellstadt Mannheim, OGEMA-Alliance, http://www.modellstadt-mannheim.de

[26] Der EEBus, Zugriff April 2011, http://www.eebus.de/eebus-die-technologien.html, http://www.eebus.de/smart-energy.html

[27] Kellerdonk, Zugriff April 2011, http://www.kellendonk.de/eebus

[28] Projekt Smart Watts, Zugriff April 2011, http://www.smartwatts.de

[29] Grafik Lastverlagerung, Zugriff April 2011, http://www.hydros.bz.it/index.php?id=666

doi: 10.2313/NET-2011-07-2_06

Der neue, elektronische Personalausweis

Maximilian Imhof
Betreuer: Holger Kinkelin
Seminar Future Internet SS2011
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
E-Mail: imhof@in.tum.de

KURZFASSUNG

Jeder Bundesbürger ist dazu verpflichtet, ab seinem 16. Lebensjahr ein Ausweisdokument mit sich zu führen. Aufgrund dessen wird jeder Bürger früher oder später den neuen Personalausweis beantragen müssen. Bislang gab es weder einen Standard-Identitätsnachweis für die Online-Welt, noch war es möglich rechtskräftige Willenserklärungen im Internet abzuschließen. Der fehlende Identitätsnachweis ermöglicht Cyberkriminalität wie zum Beispiel Phishing oder Identitätsdiebstahl. Die Einführung des neuen, innovativen Personalausweises soll Onlinegeschäfte erleichtern und die Kriminalität im zukünftigen Internet erschweren oder gänzlich verhindern. Um den elektronischen Identitätsnachweis zu realisieren, wurde eine neue Infrastruktur mit dazugehörigen Sicherheitsmerkmalen entwickelt. Am 1. November 2010 war es soweit und der neue Ausweis wurde eingeführt. Doch neben den innovativen Vorteilen kamen auch Sicherheitslücken sowie weitere Probleme zum Vorschein. Der Personalausweis ist in der hoheitlichen Funktion im Moment das sicherste Ausweisdokument in Deutschland. Die Nutzung der Onlinefunktionen muss sich allerdings noch bei den Nutzern sowie bei den Dienstanbietern etablieren.

Schlüsselworte

nPA, eID, QES, Infrastruktur, PersAuswG, CAN, eID-PIN, PACE, EAC, PA, PKI, CSCA, CVCA

1. EINLEITUNG

„1400 Buchdruck, 1930 Fernseher, 1941 Computer, 1956 Faxgerät, 1969 Kartenchip, 1. November 2010 elektronischer Personalausweis". Unter dem Titel „Gute Ideen aus Deutschland" wirbt das Bundesministerium des Inneren (BMI) für den neuen Personalausweis [7]. Seit dem 1. November 2010 kann dieser in Deutschland in den Bürgerämtern beantragt werden. Die elektronische Multifunktionskarte gilt im Reiseverkehr, in der Personenkontrolle sowie in der elektronischen Welt. Der Ausweis wurde nicht nur als modernes, sichereres hoheitliches Dokument eingeführt, sondern auch mit zusätzlichen elektronischen Funktionen versehen, wie dem elektronischen Identitätsnachweis (eID) und der qualifizierten elektronische Signatur (QES). Mit diesen Funktionen können Onlinegeschäfte des alltäglichen Lebens sicherer abgeschlossen und Verträge unterzeichnet werden.

Im folgenden Abschnitt wird allgemein auf den neuen Personalausweis eingegangen. Im Besonderen werden die Einführung, der Aufbau mit den Erneuerungen und weitere Informationen die zu beachten sind, erläutert. Der dritteAbschnitt gibt einen Überblick über die drei neuen Funktionen: Die hoheitliche Biometriefunktion, der elektronische Identitätsnachweis und die qualifizierte elektronische Signatur. Der elektronische Identitätsnachweis wird Allgemein erläutert. Desweiteren wird die Infrastruktur beschrieben. Im Anschluss werden die Komponenten zur Nutzung der Funktionen für die Bürger als auch für Unternehmen veranschaulicht. Der 5. Abschnitt handelt von Sicherheitsmechanismen zum Schutz der personenbezogenen Daten. Die Sicherheitslücken werden neben weiteren Problematiken im nächsten Abschnitt thematisiert. Abschließend wird ein kurzes Fazit gegeben.

2. ALLGEMEIN

Schon im Mittelalter musste man sich mit Wappen, Orden oder Zunftzeichen ausweisen. In der Bundesrepublik gibt es seit 1951 einen Pass. Hingegen wurde in der damaligen DDR erst 1953 ein Ausweisdokument eingeführt. Der Personalausweis, den wir bis vor kurzem noch hatten und zum Teil noch haben, existiert seit dem 1. April 1987. Am 18. Dezember 2008 wurde der neue Personalausweis, auch nPA[1] genannt, vom Bundestag bewilligt und am 1. November 2010 eigeführt. Neben dem neuen Ausweis trat auch das „Gesetz über Personalausweise und den elektronischen Identitätsnachweis" (PersAuswG) in Kraft [12].

Der Ausweis wurde mit dem Hintergrund eingeführt, ein neues, sichereres Ausweisdokument zu schaffen. Durch die neuen Funktionen soll das Dokument viele Dienstleistungen der öffentlichen Verwaltung sowie Aktivitäten und Einkäufe des alltäglichen Lebens erleichtern. Einen standardisierten, elektronischen Identitätsnachweis gab es bislang noch nicht. So ist es fortan möglich sich gegenüber Behörden in Bereichen des E-Gouvernements auszuweisen. Dadurch kann sich der Bürger „lästige" Behördengänge ersparen. Des Weiteren ist das Ausweisen im Bereich des E-Business möglich und wird als schneller, einfacher und sicherer vom Bundesministerium des Inneren beschrieben. Folglich soll der Ausweis Internetgeschäfte sicherer machen und Cyberkriminalität wie Phishing und Identitätsdiebstahl verhindern.

Der neue deutsche Personalausweis ist fünf Gramm leicht, grün-blau unterlegt und wird aus Polykarbonat hergestellt. Er besitzt nicht mehr wie der Alte das ID-2

[1]Sollte erst „elektronischer Personalausweis" (ePA) genannt werden, jedoch führte Kritik an diesem Namen zur Umbenennung in „neuer Personalausweis" (nPA)

doi: 10.2313/NET-2011-07-2_07

Format sondern hat mit 8,6cm Länge und 5,4cm Breite die gleichen Abmessungen wie übliche Scheckkarten und ist somit im Besitz des ID-1 Formats. Wie schon der Vorgänger enthält dieser Ausweis zahlreiche Sicherheitsmerkmale, welche die Fälschungssicherheit erhöhen. Er verfügt über mehrfarbige Guillochen, Mikroschriften, UV-Aufdrucke, einen 3-D Bundesadler, Kontrastschriften, Melinfasern, ein Laserkippbild und viele weitere Merkmale [17]. Auf der Vorderseite ist der Familienname sowie der Geburtsname, der Vorname, ein gegebenenfalls vorhandener Doktorgrad, Tag und Ort der Geburt, die Staatsangehörigkeit, das Lichtbild, die Unterschrift, Gültigkeitsdatum, die Seriennummer und die Card Access Number (CAN) zu lesen. Die Card Access Number ist eine auf der Vorderseite des Personalausweises aufgedruckte sechsstellige dezimale zufällige Nummer. Die CAN lässt sich nicht aus personen- oder dokumentenbezogenen Daten berechnen. Die Card Access Number wird bei der hoheitlichen Biometriefunktion (siehe auch 3.1), der Änderung von Daten in den Ausweisbehöden sowie beim Verbindungsaufbau zur Signaturanwendung benötigt. Neben den Aufgedruckten Daten ist auf der Vorderseite, wie in Abbildung 1, das biometrische Passbild zu erkennen.

Abbildung 1: Ausweisansicht Vorderseite [16]

Auf der Rückseite des Ausweisdokumentes befinden sich die Augenfarbe, die Größe, die Anschrift, die Stadt mit Postleizahl der ausstellenden Behörde, Ausstelldatum, Ordens- bzw. Künstlername und das Logo sowie die maschinenlesbare Zone(MRZ). Die Ansicht auf die Rückseite des Ausweises ist in Abbildung 2 dargestellt.
Im Vergleich zum vorherigen Ausweis sind die CAN und die Postleizahl neu hinzugekommen. Das Ausweisdokument ist nach ISO 14443 mit einem kontaktlosen Chip ausgestattet. Auf dem Dokument sind nach §5 Abs. 5 PersAuswG Familienname, Geburtsname, Vorname, Doktorgrad, Tag und Ort der Geburt, Lichtbild, Anschrift, Staatsangehörigkeit, Seriennummer, Ordensname beziehungsweise Künstlername und die Daten der maschinenlesbaren Zone auf dem radiofrequency identification(RFID)-Chip gespeichert[12]. Neben den genannten Daten können auch freiwillig Fingerabdrücke, sowie die Qualität und Bezeichnung dieser gespeichert werden. Diese Daten dienen zur eindeutigen Zuordnung von Ausweis und Inhaber.

Abbildung 2: Ausweisansicht Rückseite [16]

Nach §1 Abs. 1 des PersAuswG ist jeder Bürger, der die deutsche Staatsangehörigkeit innehat und somit der Meldepflicht unterliegt, oder sich überwiegend in Deutschland aufhält, ab 16 Jahren dazu verpflichtet einen Ausweis zu besitzen. Kinder und Jugendliche unter 16 Jahren können ebenfalls einen Personalausweis beantragen, allerdings ohne den elektronischen Identitätsnachweis. Bei der Beantragung werden ein aktuelles, biometrisches Lichtbild und ein gültiges Identitätsdokument benötigt. Die eID kann jederzeit im Bürgeramt nachträglich ein- oder ausgeschaltet werden. Der Personalausweis kostet für Personen ab 24 Jahren 28,80 Euro und für Antragsteller unter 24 Jahren 22,80 Euro. Er ist mehr als 3,5 mal so teuer wie der alte Ausweis. Weitere Kosten sind in der „Gebührenverordnung für den neuen Personalausweis“ zu entnehmen[8].

Bei Verlust oder Diebstahl des Ausweises ist der Inhaber dazu verpflichtet, den Verlust der Personalausweisbehörde zu melden. Hat der Ausweis die eID Funktion, muss diese mit Hilfe des Sperrkennworts gesperrt werden. Dies sollte schnellstmöglich im Bürgeramt oder über den 24-Stundensperrnotruf 0180-1-33 33 33[2] geschehen. Falls auch die Qualifizierte Elektronische Signatur genutzt wird, muss das Signaturzertifikat beim jeweiligen Anbieter gesperrt werden.

3. FUNKTIONEN

Das Ausweisdokument dient weiterhin als Sichtausweis, wurde jedoch um zusätzliche Funktionen ergänzt. Die hoheitliche Biometriefunktion soll das Ausweisen an Grenzkontrollen erleichtern und den Ausweis sicherer machen. Zusätzlich kann der elektronische Identitätsnachweis und die qualifizierte elektronische Signatur beantragt werden. Um diese freiwilligen Funktionen zu nutzen, wird eine Software, welche als Schnittstelle zwischen Ausweis, Kartenlesegerät und der einzelnen Funktion fungiert, benötigt. Diese Software wird

[2]3,9 Ct/Min. aus dem dt. Festnetz, aus dem Mobilfunknetz maximal 42 Ct/Min.. Auch aus dem Ausland erreichbar

doi: 10.2313/NET-2011-07-2_07

vom Bundesamt für Sicherheit in der Informationstechnik (BSI) für Windows, Linux und MacOS zur Verfügung gestellt und trägt den Namen „AusweisApp“[3]. Im Folgenden werden die einzelnen Funktionen betrachtet. Es wird besonders auf den elektronischen Identitätsnachweis eingegangen.

3.1 Die Hoheitliche Biometriefunktion

Mit dem Terrorismusbekämpfungsgesetz vom 9. Januar 2002 wurden die biometrischen Merkmale mit in den deutschen Personalausweis aufgenommen. Der nPA ist weiterhin als Sichtausweis verwendbar und als Passersatz innerhalb der Europäischen Union gültig. Die elektronisch gespeicherten Daten sind nur mit einem hoheitlichen Berechtigungszertifikat auslesbar. Biometrische Daten dürfen nur von Polizeivollzug, Zoll, Steuerfahndung der Länder, sowie der Pass-, Personalausweis- und Meldebehörden ausgelesen werden. Um die biometrischen Daten auszulesen, muss die auf dem Ausweis aufgedruckte Card Access Number eingegeben werden. Um Grenzkontrollen zu beschleunigen kann statt der CAN das Basic Access Control (BAC) Verfahren verwendet werden. Bei diesem Verfahren liest das Durchzugslesegerät der Behörden die optischen Daten aus der MRZ und erstellt einen SHA-1-Hashwert aus der 9 stelligen Seriennummer, dem Geburtsdatum und dem Ablaufdatum. Die ersten 16 Byte des Hashwertes bilden einen Schlüssel. Der Ausweischip hat ebenfalls anhand der eigenen Daten einen Schlüssel berechnet. Sind diese Schlüssel gleich, wird ein gemeinsamer Schlüssel zwischen Chip und Lesegerät bestimmt. Darauffolgend gibt der Chip die Daten für das Lesegerät frei.[9]

3.2 Der elektronische Identitätsnachweis

Die wohl größte Innovation des neuen Personalausweises ist der elektronische Identitätsnachweis, welcher als Online-Authentifizierung am PC dient. Mit den auf dem Ausweis gespeicherten Datenfeldern kann sich der Ausweisinhaber im elektronischen Rechts- und Geschäftsverkehr eindeutig identifizieren. Der Inhaber legitimiert sich über den Personalausweis und seine eID-PIN. Die Dienstanbieter weisen sich mit einem staatlichen Berechtigungszertifikat aus. Das Zertifikat gestattet nur das Auslesen der im Berechtigungszertifikat aufgeführten Datenfelder und die Gültigkeit des Ausweises. Um dies zu ermöglichen wurde eine neue Infrastruktur realisiert.

3.2.1 aus der Sicht des Anwenders

Möchte der Ausweisnutzer die elektronische Identifikation auf einer Website nutzen, klickt er auf den eID-Button. Folglich öffnet sich die AusweisApp lokal auf seinem Rechner. Für den Nutzer gibt es vier sichtbare Schritte in der Applikation. Im ersten Schritt erfährt der Benutzer, wer auf seinen Ausweis zugreifen will, wie lange dessen Berechtigungszertifikat gültig ist und von wem das Zertifikat ausgestellt wurde. Im nächsten Schritt zeigt die Anwendung eine Übersicht, der von dem Dienstanbieter angeforderten Datenfelder. Daraufhin kann der Benutzer Datenfelder hinzufügen oder entfernen. Im dritten Schritt muss der Nutzer seine eID-PIN eingeben um die Daten freizugeben. Im letzten Abschnitt werden die PIN, sowie die Gültigkeit des Personalausweises und die Anbieterberechtigung geprüft. Wenn die Überprüfung erfolgreich war, werden die Daten übertragen. Infolgedessen schließt sich die Applikation und das Ergebnis wird im Browser dargestellt.

[3]Download auf www.ausweisapp.bund.de

3.2.2 eID-PIN

Nach Beantragung eines Ausweises mit eID wird ein PIN-Brief per Post, welcher eine 5-stellige zufällige Transport-PIN, die PUK Nummer und ein Sperrkennwort beinhaltet, zugestellt. Diese 5-stellige Nummer, muss durch einen 6-stellige, dezimale persönliche eID-PIN beim Bürgeramt oder an einem passenden Lesegerät ersetzt werden. Ohne eigene eID-PIN ist die eID Funktion nicht nutzbar. Um das Erraten der eID-PIN durch Ausprobieren zu verhindern enthält der Chip einen Fehlbedienungszähler (FBZ), welcher die die Karte nach drei falschen Eingaben sperrt. Der dritte Eingabeversuch ist erst nach Eingabe der CAN möglich um einen Denial of Service-Angriff zu verhindern. Das PIN-Schema ist in Abbildung 3 dargestellt.

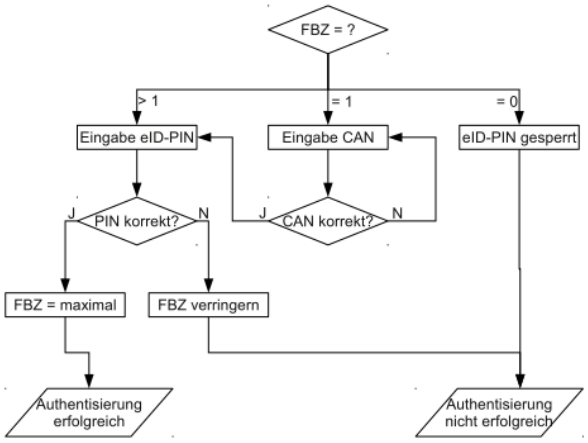


Abbildung 3: Eingabe der eID-PIN [5]

3.2.3 Pseudonym

Der Personalausweisinhaber hat die Möglichkeit sich bei Internetdiensten mit Pseudonymen anzumelden. Dieses Pseudonym wird bei jeder späteren Anmeldung vom Dienstanbieter wiedererkannt und ohne personenbezogene Daten wie zum Beispiel Name und Adresse weitergegeben. Diese Funktion ist karten- und dienstspezifisch, dies bedeutet, dass für jedes Pseudonym ein Schlüssel aus einem Ausweis-Chipschlüssel und Schlüssel des Betreibers berechnet wird. Somit ist das Abgleichen der Datenbanken von Dienstanbietern, um personenbezogene Daten zu bekommen, nutzlos.

3.2.4 Infrastruktur

Auf der Seite des Bürgers ist der Kartenleser an den PC angeschlossen. Auf diesem PC ist die AusweisApp installiert. Ein Plug-in im Browser startet diese Applikation bei dem Aufruf der eID Funktion. Auf Seiten des Dienstanbieters, wie in Abbildung 3 zu erkennen, arbeitet ein Webserver als Frontend, welcher über einen eID-Connector mit dem eID-Server kommuniziert. Der eID-Server, der entweder vom Betreiber der Website oder einem weiteren Dienstanbieter unterhalten wird, übernimmt die Kommunikation mit der AusweisApp, den Abruf von Berechtigungszertifikaten und der Sperrliste. Die Sperrliste ist eine Liste, welche die gesperrten Ausweise beinhaltet. Als Schnittstelle wird

doi: 10.2313/NET-2011-07-2_07

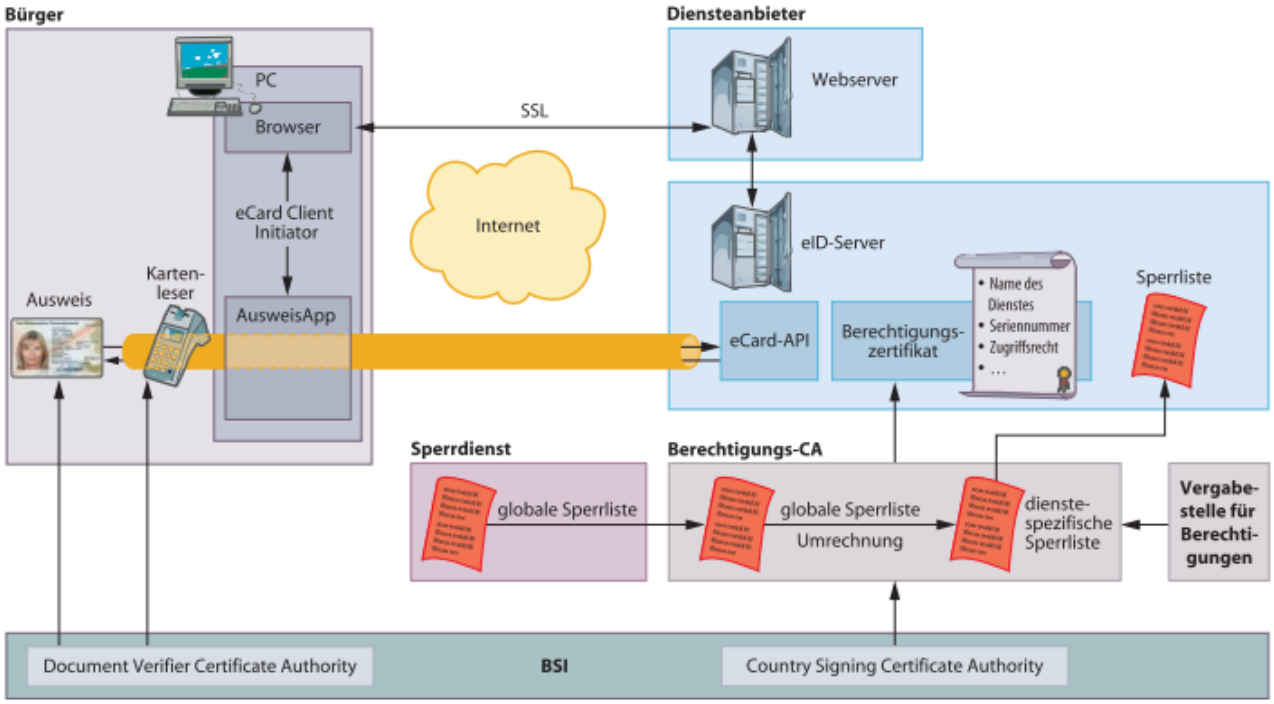


Abbildung 4: Infrastruktur [1]

die eCard-API verwendet. Die Daten werden zwischen eID-Server und Webserver, bei einem offenen Netz, verschlüsselt und signiert übertragen. Klickt nun der Ausweisinhaber auf die eID-Funktion auf einer Website eines Dienstanbieters, öffnet sich lokal die Applikation. Diese erhält die notwendigen Parameter wie zum Beispiel die Adresse des zuständigen eID-Servers. Mit dem Erhalt der Parameter wird der sichere Verbindungsaufbau zwischen Chip des Ausweises und dem eID-Server veranlasst. Diese Verbindung ist in Abbildung 4 zu erkennen. Die Zugriffskontrolle übernimmt das PACE-Protokoll (siehe 5.1) um die Verbindung abzusichern. Der eID-Server muss seine Leseberechtigung mit einem Zertifikat nachweisen.

3.3 Die qualifizierte elektronische Signatur

Neben dem elektronischen Identitätsnachweis wurde die qualifizierte elektronische Signatur, auch Unterschriftsfunktion genannt, eingeführt. Diese ermöglicht dem Auswisinhaber das digitale Signieren von Dokumenten.

3.3.1 Allgemein

Der Ausweisinhaber kann freiwillig, je nach Bedarf die Unterschriftfunktion auf seinem Ausweis aktivieren. Für die Nutzung der Funktion wird ein Signaturzertifikat benötigt. Dieses verursacht jährliche Zusatzkosten in Höhe von ungefähr 60 bis 80 Euro. Die Signatur wird von verschiedenen Anbietern angeboten, hierdurch entsteht der Unterschied in den Kosten. Wie bei der eID-Funktion ist eine Geheimnummer, die Signatur-PIN erforderlich. Zum Auslieferungszeitpunkt des Ausweises ist keine Signatur-PIN gesetzt, das heißt der Inhaber muss diese PIN selbst bestimmen. Die Signatur ist der eigenhändigen Unterschrift rechtlich gleichgestellt und es können somit rechtsverbindliche Willenserklärungen abgegeben werden. Aus diesem Grund sind die Anforderungen an die Sicherheit größer als bei der eID. Die QES kann nur mit einem Komfortlesegerät (siehe 4.1) genutzt werden.

3.3.2 aus der Sicht des Anwenders

Möchte der Bürger ein Dokument signieren, öffnet er die AusweisApp. Zunächst muss die zu signierende Datei ausgewählt werden. Daraufhin wird der Ausweisinhaber nach der auf dem Ausweis aufgedruckten CAN gefragt. Infolgedessen kann der TrustedViewer[4] den Inhalt des zu unterzeichnenden Dokuments anzeigen und warnt vor unsichtbaren Inhalten. Mit der Eingabe der Signatur-PIN ist das Dokument unterschrieben. Nachträgliche Veränderungen des Dokuments werden angezeigt.

4. KOMPONENTEN ZUR NUTZUNG

Um Funktionen wie eID oder QES zu nutzen, wird gewisses Zubehör benötigt. Was benötigt wird und welche Kosten dabei für Nutzer und Unternehmen anfallen wird in diesem Abschnitt genauer dargestellt. Es wird auf die Komponenten sowie auf die entstehenden Kosten näher eingegangen.

4.1 Für Ausweisinhaber

Für die Nutzung der elektronischen Identifikation und der qualifizierten elektronischen Signatur wird neben der AusweisApp auch ein kontaktloses Kartenlesegerät benötigt. Es gibt drei verschiedene Arten von Lesegeräten: den Basisleser für 10 bis 25 Euro, den Standardleser für 30 bis 80 Euro und den Komfortleser für 90 bis 160 Euro. Lesegeräte sind im freien Handel zu erwerben. Somit ist der Preisunterschied zu erklären. Für die eID-Funktion reicht ein Basislesegerät aus,

[4]Der TrustedViewer ist ein Programm welches das Dokument vor der Unterzeichnung auf versteckte Inhalte überprüft

doi: 10.2313/NET-2011-07-2_07

bei welchem die PIN über den Computer eingegeben werden muss. Das Standardlesegerät hat ein seperates Tastenfeld sowie ein Display. Das Komfortlesegerät hat ebenfalls einPIN-Pad und ein Display. Das Komfortlesegerät ist jedoch mit dem EAL4+ Modul ausgestattet, welches zur Nutzung der QES notwendig ist. Es ist darauf zu achten, dass nur vom BSI zertifizierte Lesegeräte verwendet werden, welche an einem aufgedruckten Personalausweis-Logo zu erkennen sind. Auf der Internetseite der AusweisApp sind die von der Applikation unterstützten Lesegeräte gelistet.

4.2 Für Unternehmen

Damit Unternehmen die eID Funktion nutzen und auf Daten zugreifen können, müssen sie über ein Berechtigungszertifikat verfügen. Diese kann bei der Vergabestelle für Berechtigungszertifikate, welches dem Bundesverwaltungsamt unterliegt, beantragt werden. Laut Detlef Borchers von „C't“ kostet die Beantragung 105 Euro [1]. Zur Beantragung muss das Unternehmen glaubhaft nachweisen, weshalb sie die Datenfelder nutzen möchte. Die Vergabestelle prüft, welche Daten das Unternehmen für seine Zwecke wirklich braucht und ob es ein vertrauenswürdiges Unternehmen ist. Derzeit werden nach Borchers nur zwei Gründe akzeptiert, ein gesetzlicher Grund wie zum Beispiel die Altersverifikation oder, wenn ein erhebliches „kreditorisches Risiko“ angenommen werden muss. Die Zertifikate sind in der Regel drei Jahre gültig, können jedoch auch jederzeit entzogen werden. Um die eID zu nutzen müssen zusätzlich zu dem Zertifikat noch ein eID-Server und Hardware Security Module angeschafft werden. Die Server kosten schätzungsweise 200.000 bis 300.000 Euro, ohne die laufenden Kosten. Für Unternehmen mit geringen Anfragen ist ein eID-Service-Provider die bessere Alternative. Der Provider „]init[“ bietet zwei unterschiedliche Services an. Für die Nutzung von einem Zertifikat bietet „]init[“ den „Trusted eID-Service Premium“ für 250 Euro im Monat plus 750 Euro Einrichtungsgebühr an. Der „Trusted eID-Service Enterprise“ welcher bis zu 16 Berechtigungszertifikate verwalten kann, kostet 2750 Euro im Monat zuzüglich 7500 Euro Einrichtungsgebühr [18]. Der Service, das Hardware Security Modul, von D-Trust, einer Tochterfirma der Bundesdruckerei kostet 250 Euro pro Monat und jedes weitere Modul 150 Euro. Die Einrichtungsgebühr hierfür liegt bei 750 Euro. Zur Beantragungsgebühr, dem Server und dem Modul kommen noch die Zertifikatgebühren hinzu. Das erste Zertifikat kostet 2000 Euro pro Jahr und jedes weitere jeweils 500 Euro pro Jahr. Für Behörden der Bundesländer und Kommunen sind die eID-Server kostenlos. Jedoch muss die Kommune mindestens 5700 Euro im Jahr für das Berechtigungszertifikat bezahlen [1].

5. SICHERHEITSMECHANISMEN

Zur Sicherung der personenbezogenen Daten, welche auf dem kontaktlosen Chip gespeichert sind, wurden neue Sicherheitsmechanismen entwickelt. Unter anderem das Password Authenticated Connection Establishment, das Extended Access Control, die Passive Authentication, sowie die Public Key Infrastructures.

5.1 Password Authenticated Connection Establishment (PACE)

Password Authenticated Connection Establishment, kurz PACE, ist ein kryptografisches Protokoll für den gegenseitigen Authentisierungsmechanismus zwischen Terminal und Chip. PACE wurde vom Bundesamt für Sicherheit in der Informationstechnik für den neuen Personalausweis entwickelt und wird in der Technischen Richtlinie TR-03110 [4] beschrieben. Das PACE-Protokoll sorgt für die verschlüsselte und integritätsgesicherten Kanal zwischen Kartenleser und Chip. Welches Passwort für die Generierung eines Verschlüsslungspassworts benutzt wird hängt vom Lesegerät und Nutzen des Ausweises ab. Zur Nutzer-Authentifikation beim Verwenden der eID-Funktion wird die 6-stellige eID-PIN verwendet. Bei hoheitliche Kontrollen wird die auf dem Kartenkörper aufgedruckte Card Access Number oder die Hashnummer aus der Basic Access Control verwendet[5]. Der Chip generiert eine Zufallszahl, welche er mit dem Passwort über eine Hashfunktion verschlüsselt. Das Lesegerät muss zur Entschlüsselung ebenfalls die Hashfunktion sowie das Passwort kennen. Hat das Lesegerät die geheime Zufallszahl herausgefunden wird ein gemeinsamer symmetrischer AES-Schlüssel für Secure Messaging zwischen Chip und Lesegerät abgeleitet[9]. Kern des Verfahrens ist der Diffie-Hellman-Schlüsseltausch. Das Protokoll soll vor dem unbefugten Auslesen des Chips aus der Entfernung schützen.

5.2 Extended Access Control (EAC)

Extended Access Control, kurz EAC, ist eine erweiterte Zugangskontrolle zwischen Lesegerät oder Dienstanbieter und Chip. EAC besteht aus zwei Unterprotokollen, der Chip Authentication (CA) und der Terminal Authentication (TA). Es wird ebenfalls in den Technischen Richtlinien TR-03110 [4] des BSI beschrieben.

5.2.1 Chip Authentication

Die Chip Authentication dient zur Überprüfung der Echtheit des Chips, sowie dem sicheren Verbindungsaufbau zwischen Chip und Lesegerät, beziehungsweise den Dienstanbietern bei der Nutzung der eID-Funktion. Die CA basiert auf dem Diffie-Hellmann-Schlüsselaustausch. Das Lesegerät nutzt ein flüchtiges Schlüsselpaar und der Chip ein statisches Paar. Der Schlüssel des Ausweischips wird während der Herstellung signiert. Dadurch wird die Echtheit des Chips und damit auch der auf dem Chip gespeicherten Daten nachgewiesen. Weiter dient die Authentifizierung zum Aufbau eines sicheren Kanals zwischen Kartenlesegerät oder Dienstanbierter und RFID-Chip.

5.2.2 Terminal Authentication

Der Zweck der Terminal Authentication ist die Authentisierung des Lesegeräts oder eines Dienstanbieters zum Auslesen von Daten. Hierzu verschickt das Lesegerät oder der Dienstanbieter seine Leseberechtigung in Form des Terminal-Zertifikats an den Chip. Des Weiteren wird das Country Verifying Certificate Authority (CVCA) sowie die Zertifikate in der Zertifikat-Hierarchie zwischen Terminal-Zertifikat und CVCA mitgeschickt. Darauf prüft der Chip die Echtheit und Unverfälschtheit des Terminals. Es müssen alle Zertifikate mit dem geheimen Schlüssel des Vorgängers signiert worden sein beginnend mit dem CVCA-Zertifikat um ein positives Ergebnis zu erhalten. Das CVCA-Zertifikat wurde bei der Herstellung des Chips auf dem Chip gespeichert. Wenn die Echtheit und Unverfälschtheit des Terminal-Zertifikates erfolgreich festgestellt wurde, muss geprüft werden ob dieses Zertifikat auch wirklich für dieses Lesegerät ausgestellt wurde. Hierzu schickt der Chip eine Zufallszahl an das Lesegerät.

doi: 10.2313/NET-2011-07-2_07

Die Zahl wird mit dem geheimen Schlüssel des Terminal-Zertifikats signiert und an den Chip zurückgesand. Durch den öffentlichen Schlüssel des Lesegeräts, kann der Chip die Signatur der Zahl überprüfen und feststellen, ob das Lesegerät den passenden Schlüssel besitzt[3].

5.3 Passive Authentication (PA)

Die Passive Authentication, kurz PA, dient zur Überprüfung der Echtheit und Unverfälschtheit der Daten auf dem Chip. Bei der Herstellung des Ausweisdokuments werden die elektronischen Daten mit dem Document Signing-Zertifikat digital signiert. Dieses Zertifikat ist wiederum mit dem Country Signing Certificate Authority (CSCA), welches nur dem Ausweishersteller zur Verfügung steht, signiert. Beim Lesen eines Ausweises wird anhand der passiven Authentisierung die Signatur der Daten geprüft und bis zum CSCA zurückverfolgt. So kann festgestellt werden, ob die Daten vom offiziellen Passhersteller im Chip gespeichert wurden und ob diese unverfälscht sind.

5.4 Public Key Infrastructures (PKI)

Die Public Key Infrastructures, kurz PKI, ist die Hierarchie von digitalen Zertifikaten. Für den Ausweis werden zwei PKI benötigt, die Country Signing Certificate Authority und die Country Verifying Certificate Authority. Diese Infrastrukturen werden in den Technischen Richtlinien TR-03128 [6] beschrieben. Das CSCA ist laut BSI die Hierarchie von digitalen Zertifikaten zur Signierung von Daten in elektronischen Ausweisdokumenten. Dagegen ist das CVCA die Hierarchie von digitalen Zertifikaten zur Leseberechtigung bei elektronischen Ausweisdokumenten[3].

6. SICHERHEITSLÜCKEN UND WEITERE PROBLEME

In der Presse und anderen Medien wird immer wieder Kritik zum Personalausweis ausgeübt. Es heißt, Betrügern sei es problemlos möglich sensible Daten sowie die geheime PIN abzufangen. Die Bundesregierung behauptet hingegen, der Ausweis sei sicher. In der Kritik stehen auch die Umsetzung und die daraus resultierenden Probleme für die Kommunen und den Bürger. Diese Kritik wird im folgenden Abschnitt genauer dargelegt.

6.1 Sicherheitslücke

Der neue Personalausweis geriet wegen Sicherheitsmängel unter heftigen Beschuss in den Medien. So auch vom Westdeutschen Rundfunk (WDR). Dieser thematisierte im „Bericht aus Brüssel“ vom 22. September 2010, 21:55 Uhr, den Ausweis und dessen festgestellte Sicherheitsmängel. Mittelpunkt des geschilderten Angriffsszenarios ist ein mit einem Trojanischen Pferd infizierter Rechner. Die Schadsoftware wurde mithilfe eines Hackerangriffs unbefugt platziert. Der Hacker sieht darauffolgend alle Tastatureingaben oder kann Bildschirmanzeigen mitlesen. Mit Hilfe eines Keyloggers können diese Daten aufgezeichnet werden. Im Beispiel wurde so die PIN herausgefunden und konnte vom Angreifer geändert werden. Im schlimmsten Fall könnte der Hacker online einkaufen oder ein Konto eröffnen. Das BSI nimmt in einer Pressemitteilung [2] Stellung zum „Bericht aus Brüssel“ und weist die Sicherheitsbedenken erneut zurück. So heißt es in dieser, der Angreifer könne zwar die PIN erspähen und ändern, aber dies würde zur Entdeckung des Angriffs und somit zur Sperrung des Ausweises führen. Darüber hinaus zählt das BSI grundlegende Sicherheitsmaßnahmen im Umgang mit dem Ausweis auf. Peter Schaar, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, äußerte sich in einer Pressemitteilung [13] zum Personalausweis am 29.Oktober 2010: „Wer die Gefahr des Ausspähens der PIN mittels einer Schadsoftware umgehen will, sollte lieber ein höherwertiges Lesegerät einsetzen“. Das Ausspähen der PIN ist ausschließlich bei der Nutzung eines Basislesers möglich. Grund hierfür ist, dass Basisleser nicht über eine PC externe Hardware zum Eingeben der PIN verfügen. Des Weiteren ist ein Angriff nur möglich, wenn der Ausweis auf dem Lesegerät liegt. Der Ausweis sollte daher laut BSI immer sicher verwahrt werden und nur bei Nutzung auf das Lesegerät gelegt werden. Aufgrund dieser Tatsachen gilt der neue Personalausweis als sichere Alternative zu den ursprünglich Benutzerdaten im E-Business. Jedoch belegen Banking-Trojaner, dass Betrüger sicher bereit sind, vergleichbaren Aufwand zu betreiben, wenn die Gewinnerwartung hoch genug ist. Für die Nutzer der eID und der QES ist die Nutzung und ständige Aktualisierung von Firewall, Antivirensoftware und Systemupdates im eigenen Interesse Pflicht.

6.2 Weitere Probleme

Neben den Sicherheitslücken im technischen Bereich sind auch zusätzliche Probleme entstanden. Probleme wie die Schlüsselfunktion des Staates, die Belastung für die Verwaltung und die Akzeptanz des Ausweises. Desweiteren ist die Haftung bei Angriffen zu nennen. Auf diese Schwachstellen wird in den folgenden Abschnitten näher eingegangen.

6.2.1 Einführung durch den Staat

Die technische Sicherheit und die Sicherheitslücken sind die eine Seite. Auf der anderen Seite hingegen steht die Kritik an der politischen Sicherheit. Peter Schaar kritisierte in seinem Vortrag auf dem Chipkarten-Kongress Omnicard 2011, dass der Staat nun „ein neue Schlüsselfunktion“ zwischen Konsumenten und Dienstanbietern einnimmt. Dies geschieht durch die Zertifikatausteilung und -entziehung.

6.2.2 Belastung für Verwaltung

Ein weiteres Problem bei der Einführung des Ausweisdokuments ist die zusätzliche Belastung für Kommunen und Ordnungsämter. So schrieb die Hessische/Niedersächsische Allgemeine Zeitung am 23.07.2010: „Der neue Ausweis, der ab dem 1. November beantragt werden kann, soll 28,80 Euro kosten. Die sechs Euro, die davon bei den Städten und Gemeinden bleiben sollen, reichten nicht, um deren Kosten zu decken. 22,70 Euro gehen an den Hersteller, zehn Cent fließen in die notwendigen Computerprogramme. Grund für die Mehrkosten bei den Städten ist vor allem eine längere Bearbeitungszeit: Bisher kalkulieren sie mit siebeneinhalb Minuten Bearbeitungszeit für einen Ausweis“ [15]. Das Hamburger Abendblatt datierte den Personalaufwand auf bis zu dreimal so hoch wie bisher [14]. Darüber hinaus müssen die Mitarbeiter auf den neuen Ausweis geschult werden. Anton Hanfstengl, Leiter des Bürgerbüros München berichtet davon, dass sich die Änderungsterminals der Bundesdruckerei für PIN und PUK oft aufhängen und sich somit die Ausweisausgabe verzögert [11]. Jedoch ist das größte Bedenken der Bürgerämter, dass die Bürger bei technischen Problemen mit Kartenlesern oder Software die Bürgerbüros aufsuchen.

doi: 10.2313/NET-2011-07-2_07

6.2.3 Basisleser und Haftung bei Angriffen

Im Rahmen des IT-Investitionsprogramms des Konjunkturpakets II stellt der Bund 24 Millionen Euro für die Förderung von Lesegeräten zur Verfügung. Durch diese Unterstützung können rund 1,5 Millionen IT-Sicherheitskits kostenfrei oder verbilligt ausgegeben werden. Diese Kits enthalten einen Basiskartenleser und Informationsbroschüren zur Nutzung mit Chipkarten. Die Verteilung dieser Kits wird jedoch kritisiert, da die Basisleser als unsicher gelten. Der Staat haftet nicht bei Hackerangriffen, so Ex-Bundesinnenminister de Maizière in einem Interview mit Plusminus vom 24. August 2010. Somit bleibt den Nutzern bei Angriffen nur die Hoffnung auf Kulanz bei Dienstanbietern.

6.2.4 Akzeptanz des Ausweises

Das Bundesministerium des Innern hat eine Studie von der Universität Potsdam durchführen lassen, um die Akzeptanz des neuen Personalausweises zu prüfen [10]. Untersucht wurden drei Zielgruppen, die Bürger, die Verwaltung und die Unternehmen. Die Studie zeigte, dass es bei den Bürgern Skepsis aber auch Begeisterung gibt. So weiß ein Drittel noch gar nicht über den neuen Personalausweis Bescheid. Jedoch will jeder zehnte Bürger noch vor Ablauf seines alten Ausweises den Neuen beantragen. Auf Seiten der Unternehmer sind die Funktionen des Ausweisdokumentes weitestgehend unbekannt. So gibt es derzeit erst wenige Unternehmen die die Nutzung der eID-Funktion anbieten[5]. Die großen Internationalen Unternehmen wie Google, Amazon, PayPal oder eBay werden nach eigenen Aussagen die Entwicklung des neuen Personalausweises beobachten.

7. FAZIT

Zusammenfassend kann festgestellt werden, dass der neue Personalausweis ein sicheres Ausweisdokument darstellt. Wer den elektronischen Identitätsnachweis nutzen möchte, kann das Vertrauensverhältnis zwischen Verbrauchern und Dienstanbietern im Internet durch mehr Sicherheit verbessern. Der Ausweisinhaber kann mit der qualifizierten elektronischen Signatur fortan rechtsgeschäftliche Abschlüsse elektronisch tätigen, was den Geschäftsverkehr erleichtert und beschleunigt. Dadurch setzt Deutschland neue Maßstäbe im Identitätsmanagement. Doch den Ausweis neben Erfindungen, wie den Buchdruck oder das Auto zu stellen ist vom Bundesministerium des Inneren übertrieben. Weiterhin ist die Belastung in der Verwaltung kritisch zu betrachten, denn die Bürgerämter sind jetzt schon überfordert. Ebenso zeigt die Studie, dass die Bürger und vorallem die Unternehmen der Bundesrepublik Deutschland bisher wenig über den neuen Personalausweis Informiert sind. Die frühe Einführung zeigt die Dringlichkeit mit welcher der Staat dieses Dokument herbeiführen wollte. Trotz der neu entwickelten Sicherheitsmechanismen ist aufgrund der aufgezeigten Sicherheitslücke das Nutzen eines Basislesers nicht zu empfehlen. Ein Standardleser oder Komfortleser ist daher zu bevorzugen. Letztendlich bleibt abzuwarten, inwieweit die neuen Funktionen des Personalausweises von den Bürgern und Unternehmen akzeptiert und zu einem festen Bestandteil des Internets werden.

[5]Eine Liste von Unternehmen ist unter www.npa-in-aktion.de zu finden

8. LITERATUR

[1] Detlef Borchers: *Digitale Identität: Anwendungszenarien für den elektronischen Personalausweis*, Report, C't, Heise Zeritschriften Verlag, Oktober 2010

[2] Bundesamt für Sicherheit in der Informationstechnik: *BSI weist Sicherheitsbedenken zum neuen Personalausweis erneut zurück*, Pressemitteilung, Bonn, September 2010

[3] Bundesamt für Sicherheit in der Informationstechnik: *Innovationen für eine eID-Architektur in Deutschland*, Broschüre, Bonn, September 2010

[4] Bundesamt für Sicherheit in der Informationstechnik: *Technical Guideline TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents*, Version 2.05, Technische Richtlinie, Bonn, Oktober 2010

[5] Bundesamt für Sicherheit in der Informationstechnik: *Technische Richtlinie TR-03127: Architektur elektronischer Personalausweis und elektronischer Aufenthaltstitel*, Version 1.13, Technische Richtlinie, Bonn, Oktober 2010

[6] Bundesamt für Sicherheit in der Informationstechnik: *Technische Richtlinie TR-03128: EAC-PKI'n für den elektronischen Personalausweis*, Version 1.1, Technische Richtlinie, Bonn, Oktober 2010

[7] Bundesministerium des Inneren: *Der elektronische Personalausweis*, Broschüre, Berlin, Februar 2009

[8] Bundesministerium des Inneren: *Gebührenverordnung für den neuen Personalausweis*, Gebührenverordnung, Berlin, August 2010

[9] Prof. Dr. Claudia Eckert: *Vorlesung IT-Sicherheit, WS 10/11*, Vorlesung, München, Januar 2011

[10] Jasper Hugo Grote, Daniela Keizer, Dominik Kenzler, Patrick Kenzler, Prof. Dr. Christoph Meinel, Maxim Schnjakin, Lisa Zoth: *Vom Client zur App: Ideenkatalog zur Gestaltung der Software zum Einsatz des neuen Personalausweises*, Universität Potsdam, Studie, Potsdam, September 2010

[11] Kolja Kröger: *Computer-Probleme mit dem neuen Personalausweis*, Artikel, merkur-online, München, Dezember 2010

[12] Horst Köhler, Dr. Angela Merkel, Dr. Wolfgang Schäuble: *Gesetz über Personalausweise und den elektronischen Identitätsnachweis sowie zur Änderung weiterer Vorschriften*, Gesetz, Bundesanzeiger Verlag, Berlin, Juni 2009

[13] Peter Schaar: *Neuer Personalausweis: Sie haben die Wahl!*, Pressemitteilung, Bonn / Berlin, Oktober 2010

[14] Fabian Schindler: *Neuer Ausweis - Kommunen fürchten hohe Kosten*, Zeitungsartikel, Hamburger Abendblatt, Hamburg, Juli 2010

[15] Olaf Weiß: *Neuer Personalausweis: Hohe Kosten für Städte und Gemeinden*, Zeitungsartikel, Hessische Allgemeine, Northeim, Juli 2010

[16] *Aufbau Personalausweis*, `http://www.personalausweisportal.de/SharedDocs/Bilder/DE/Ausweisansicht.jpg?__blob=poster&v=7,(26.03.2011,17.34Uhr)`

[17] *Sicherheitsmerkmale des neuen Personalausweises*, `http://www.personalausweisportal.de/`

doi: 10.2313/NET-2011-07-2_07

SharedDocs/Downloads/DE/Flyer_Bundesdruckerei_Sicherheitsmerkmale_nPA.pdf?__blob=publicationFile,(30.03.2011,12.37Uhr)

[18] *Trusted eID-Services*, http://www.init.de/sites/default/files/downloads/Trusted_eID-Services_print.pdf,(04.04.2011,15.00Uhr)

doi: 10.2313/NET-2011-07-2_07

DNSSEC vs. DNSCurve for Securing the Net

Daniel Raumer
Betreuer: Ralph Holz
Seminar Future Internet SS2011
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: daniel.raumer@mytum.de

KURZFASSUNG

DNSSEC und DNSCurve sind zwei Alternativen zur Absicherung des Domain Name Systems (DNS). Vom abgesicherten DNS wird erwartet, dass dieses eine Möglichkeit bietet, die momentan anfällige X.509 PKI abzulösen. Nach einer kurzen Einführung zu DNS und einiger Angriffszenarien, wird die Funktionsweise der beiden Protokolle vorgestellt. DNSSEC baut hierbei durch Signieren der im DNS verwendeten Resource Records eine für jeden Teilnehmer überprüfbare Vertrauenskette vom Rootserver bis zum zu überprüfenden Record auf, während CurveCP durch Verschlüsselung zusätzlich auch Vertraulichkeit schafft und so bei direkter Kommunikation mit einem Nameserver Vertrauen in dessen Antwort gesichert werden kann. Beide Ansätze werden miteinander verglichen und in Bezug auf Performanz, Schwachstellen und sich eröffnende Möglichkeiten, wie die Ablösung der existierenden X.509 PKI, bewertet. Dabei werden unter Anderem Argumente aus der laufenden Debatte zwischen Dan Kaminsky und Daniel J. Bernstein, für und gegen die jeweiligen Protokolle, vorgestellt.

Schlüsselworte

Domain Name System Security, DNSSEC, DNSCurve, Authentisierungsprotokoll

1. MOTIVATION FÜR DNSSEC

Das 1983 erfundene und 1986 standardisierte Domain Name System (DNS) [11, 14, 15] liefert ein Mapping von menschenlesbaren Adressen auf in Netzwerken gebräuchliche Internet Protokoll (IP) Adressen. In seiner Basisversion gibt es keinen Mechanismus zur Sicherstellung von Authentizität und Integrität dieser Informationen, so dass bereits nach kurzer Zeit (1990) die ersten Angriffe beschrieben wurden [2]. Das Vertrauen eines Benutzers in die Authentizität Anderer beruht meistens nicht auf der IP-Adresse, sondern auf dem Domainnamen. Dies gilt oft auch wenn Zertifikate verwendet werden, da beispielsweise beim erstmaligen Beziehen der Zertifikate oft das DNS verwendet wird. Angriffe, die das DNS oder dessen Antworten manipulieren, umgehen darauf folgende Sicherheitsmechanismen, wenn der sichere Kanal nicht mit dem eigentlichen Ziel aufgebaut wird. Der 1995 beschriebene erste[1] Ansatz zur Absicherung von DNS, DNS Security (DNSSEC) [8], wurde auf Grund zu aufwändiger Schlüsselverwaltung jedoch nicht angenommen. Daher wurde zehn Jahre später eine neue überarbeitete Fassung veröffentlicht [1]. In der aktuellen Fassung wird DNSSEC von einer zunehmenden Anzahl an Nameservern unterstützt. Dennoch ist der Einsatz bis heute noch sehr gering. Eine Verbreitung von DNSSEC eröffnet neue Möglichkeiten und Potentiale bei der Nutzung des DNS.

Nach einer kurzen Einführung über DNS, soll DNSSEC zunächst in aktueller Fassung beschrieben werden. Anschließend wird mit DNSCurve ein alternativer Ansatz vorgestellt. Diese Ansätze werden bewertet. Danach werden Argumente aus der Performanzdebatte zwischen Dan Kaminsky und Daniel J. Bernstein um DNSSEC und die Alternative, DNSCurve, vorgestellt.

1.1 DNS - eine kurze Übersicht

Das DNS [14, 15] ist eine verteilte, hierarchisch aufgebaute Datenbank zur Übersetzung zwischen für Menschen verstehbaren Hostnamen und IP-Adressen. Abbildung 1 zeigt

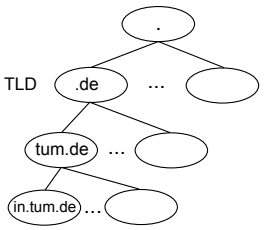


Abbildung 1: DNS Domains

dabei den hierarchischen Aufbau einer DNS Domain und damit der dahinter liegenden Anordnung der Server, durch die eine zur Absicherung nötige Public Key Infrastruktur (PKI) vorgegeben wird. Eine PKI ist ein System, das neben Benutzern, Zertifikaten und Speicher- beziehungsweise Abruforten für Zertifikate, eine hierarchisch angeordnete Struktur von Zertifizierungsstellen beinhaltet. Dabei signiert eine teilnehmende Zertifizierungsstelle (CA) der höheren Ebene, die öffentlichen Schlüssel (Public Keys), der in der Hierarchie unter ihr liegenden Teilnehmer. An oberster Stelle steht die sogenannte Wurzel, welche der oberste Vertrauensanker einer PKI ist. Vertrauensanker bezeichnet hierbei eine Autorität, deren Vertrauenswürdigkeit nicht mehr durch eine Signatur auf eine andere vertrauenswürdige Autorität zurückgeführt wird. Auch Certificate Revocation Lists (CRLs), die gesperrte Zertifikate auflisten, so wie eine Registration Authority (RA) sind oft Teil einer PKI [16].

[1]TSIG kann auf Grund der Nichtpraktikabilität in großen Netzwerken im WWW nicht verwendet werden und wird daher in dieser Arbeit vernachlässigt

doi: 10.2313/NET-2011-07-2_08

1.1.1 Resource Records

Im DNS werden Webadressen auf die sogenannten **Resource Records** (RRs), oft auch nur Records genannt, abgebildet. Diese können verschiedene Typen haben:

A: Der A Record wird genutzt, um einen Hostnamen auf eine IPv4-Adresse zu mappen. Zum Mapping auf IPv6-Adressen wurde das AAAA Record eingeführt.

CNAME: Der CNAME Record definiert ein Alias zu einem anderen Namen.

MX: Der MX Record bildet einen Namen auf einen Mailserver ab.

NS: Der NS Record verweist auf den in der Hierarchie darunter liegenden Nameserver, wenn der angefragte Nameserver den angefragten Bereich delegiert hat. Somit liefert es den Anfragenden, die dieses Record erhalten an einen speziellere Nameserver weiter.

TXT: Das TXT Record erlaubt beliebige, anwendungsspezifische Texte im DNS abzulegen.

Mit DNSSEC eingeführte RRs werden im weiteren Verlauf der Arbeit vorgestellt.

1.1.2 Nameserver

RRs werden von sogenannten **Nameservern** verwaltet. Einen Nameserver, der für einen bestimmten Bereich nicht mehr auf einen in der Hierarchie darunter liegenden Nameserver verweist, nennt man einen autoritativen Nameserver. Ein Anfrager gibt an, welchen RR er haben möchte. Auf Grund des Mappings zusammengehörende RRs werden als Set bezeichnet. In einem Set besteht keine Ordnung. Jedoch werden die RRs oftmals nach einer Round Robin Strategie abgewechselt, um Lastbalanzierung zu erreichen. Die Gesamtheit aller Adressen, für die ein Nameserver zuständig ist, wird Zone genannt. Eine angefragte Domain wird von rechts nach links abgearbeitet und so aufgelöst. Die einzelnen Hierarchieebenen werden dabei durch einen Punkt getrennt. Diese erste Ebene wird als Top-Level-Domain (TLD) bezeichnet.

1.1.3 Resolver

Das Auflösen einer Adresse wird vom **Resolver** durchgeführt. Der Resolver ist dabei ein Softwaremodul, das auf dem Rechner eines DNS-Teilnehmers beheimatet ist und die Informationen von Nameservern abruft. Er bildet also die Schnittstelle zwischen Anwendungen und Nameserver. Der Resolver löst eine Anfrage einer Anwendung auf, indem er sie um zur Auflösung nötige Informationen ergänzt und an einen normalerweise fest zugeordneten Nameserver, den sogenannten Rootserver, übermittelt. Das Auflösen kann rekursiv oder iterativ erfolgen. Beim rekursiven Auflösen leitet ein Nameserver die Anfrage so lange weiter, bis die Adresse des angefragten Server feststeht, während sich beim iterativen Auflösen der Client von Nameserver zu Nameserver in der Hierarchie nach unten arbeitet. Normalerweise arbeiten Nameserver rekursiv und liefern dem anfragenden Resolver die vollständige Antwort. Bei stark ausgelasteten Servern wie den Root-Servern ist die Rekursion jedoch deaktiviert um die Belastung für das weitere Auflösen einer Anfrage auf die anfragenden Resolver zu verteilen. In der Antwort wird dem Anfragenden dann mittels des Authoritative Response Flags mitgeteilt, ob ein Request autoritativ, also direkt aus einer lokalen Zonendatei, oder iterativ beziehungsweise rekursiv aufgelöst wurde.

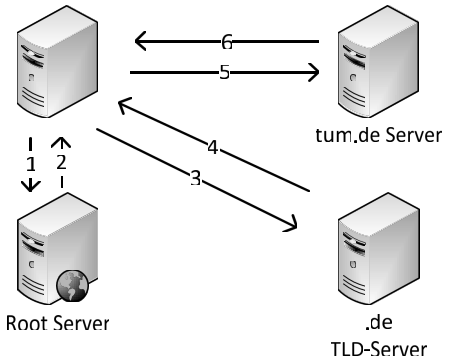


Abbildung 2: iterative Adressenauflösung über DNS

Abbildung 2 zeigt das schrittweise iterative Auflösen der Adresse www.tum.de unter der Voraussetzung, dass noch keine Adressen gecached sind. Zuerst wird vom Rootserver die Adresse des TLD-Servers zu „.de“ erfragt. An diesen Server wird dann die Frage nach dem tum.de Server gerichtet, der dann wiederum eine IP Adresse für „www.tum.de“ zurücksendet. Gewöhnlich werden Anfragen eine definierte Zeit vom Anfragenden selbst, aber auch vom Internet Service Provider gecached, um einerseits Datenverkehr aus dem Providernetz heraus zu verhindern und vor allem kürzere Latenzen zu ermöglichen. Auch kann es vorkommen, dass bestimmte, meist häufig angefragte, IP-Adressen bereits vom Server der höheren Hierarchieebene vollständig ausgeliefert werden.

1.2 Angriffszenarien

Dieser Abschnitt beschreibt Angriffszenarien, die Schwachstellen im DNS ausnutzen. DNS-Angriffe zielen meist darauf ab, durch Manipulation DNS-Nutzer auf falsche Webseiten zu lenken, um anschließend sensible Benutzerdaten durch Phishing zu erhalten. Aber auch Denial-of-Service-Attacken (DoS-Attacken) auf DNS-Server können Schaden anrichten, da wie beschrieben viele Anwendungen den Resolver und damit DNS Dienste nutzen und deren Funktionalität von diesen abhängt. Dieses Kapitel beschreibt **DNS-Spoofing**, **Cache Poisoning** und **DoS-Angriffe** mit, beziehungsweise auf, das DNS.

1.2.1 DNS-Spoofing

Als DNS-Spoofing wird das Manipulieren einer DNS-Anfrage und damit das Umlenken des Anfragers an eine andere Website bezeichnet. Möglich ist dies, indem beispielsweise eine gefälschte DNS-Antwort noch vor der offiziellen DNS-Antwort beim Anfrager ankommt. Da im normalen DNS kein Authentizitätsnachweis besteht, verarbeitet und behandelt dieser die Antwort wie die offizielle. Ein Benutzer kann so ohne dass er es merkt mit einem schädlichen Server kommunizieren. In Folge dessen werden viele der danach ablaufenden Sicherheitsmechanismen, wie SSL oder IPsec, ausgehebelt.

doi: 10.2313/NET-2011-07-2_08

1.2.2 *Cache Poisoning*

Als Cache Poisoning wird das „Verschmutzen“ eines Caches mit manipulierten Daten bezeichnet. Besonders wenn Integrität und Authentizität nicht überprüft werden, können manipulierte Daten somit verteilt werden. Ein alleiniges Sicherstellen der Authentizität eines Nameservers und der Aufbau eines sicheren Kanals hilft hierbei nicht, sofern dieser Nameserver bereits gefälschte Informationen enthält. Wird ein bereits beschriebener Spoofing Angriff auf die Anfrage hinter einem Cache durchgeführt merkt sich der Cache die falschen Daten. Handelt es sich hierbei jetzt nicht nur um einen Cache auf einem lokalen Rechner, sondern um einen größeren Cache, wie er beispielsweise beim Internet Service Provider (ISP) steht, erhalten auch alle anderen Anfragenden hinter dem betroffenen Cache die kompromittierte DNS-Antwort.

1.2.3 *DoS-Angriff*

Bei einem Distributed-Denial-of-Service-Angriff auf einen Nameserver (DDoS-Angriff) wird dieser durch einen hohen Datenstrom von DNS-Anfragen überlastet, so dass legitime Anfragen nicht mehr beantwortet werden können. Möglich wird dies vor allem dadurch, dass der Empfänger eines IP, beziehungsweise UDP-Pakets das Paket nicht annehmen muss, da dieses einfach geschickt wird. Diese Angriffe können nur schwer verhindert werden. Allerdings können sie durch ein Protokoll, das die Möglichkeit bietet, im Vergleich zur Anfragegröße viel größerer Antworten zu erzeugen, begünstigt werden. Auch der DNS-Amplification-Angriff ist ein Denial-of-Service-Angriff. Er macht sich die Vervielfachung der Datengröße durch einen DNS-Server zu Nutze. Das Opfer ist hierbei der Empfänger der DNS-Antworten. Die ausgenutzten DNS Server dienen hierbei lediglich als Verstärker des Angriffes.

Ziel eines sicheren DNS muss es also sein, diese Angriffslücken zu schließen, oder zumindest nicht zu vergrößern, ohne dabei neue Angriffe zu ermöglichen. Zusätzlich spielt der Preis an Komplexität und Einrichtungsaufwand eine entscheidende Rolle für die Akzeptanz einer neuen Technik. Sicherheit darf ein hoch skalierbares System, wie das DNS, nicht zu stark verlangsamen oder dessen Skalierung verschlechtern.

2. DNSSEC

DNSSEC kann den Ursprung und die Integrität von DNS-Daten sicherstellen. Es enthält ebenso Mechanismen, die die Nichtexistenz von DNS Daten überprüfen. Erreicht wird dies durch diverse Veränderungen und Erweiterungen des DNS-Protokolls. Es werden vier neue RR-Typen eingeführt: Resource Record Signature (RRSIG), DNS Public Key (DNSKEY), Delegation Signer (DS) und Next Secure (NSEC). Zusätzlich werden 2 neue Bits im Messageheader eingeführt: Checking Disabled (CD) und Authenticated Data (AD). DNSSEC macht dabei von bereits bekannten Erweiterungen wie Extended DNS Gebrauch, um auch DNS Pakete mit mehr als 512 Bytes senden zu können. Beim Design von DNSSEC wurde zu Gunsten der Performanz darauf geachtet, dass die Anzahl der kryptographischen Operationen eines Nameservers nicht mit der Zahl der Anfragen steigt [1].

2.1 Authentizität und Integrität von DNS Informationen

Ursprung und Integrität von DNS-Informationen werden sichergestellt, indem DNSSEC eine Digitale Signatur der DNS RRs anlegt und diese in einem neuen RR, dem RRSIG Record speichert. Wenn ein Resolver DNS-Informationen überprüfen will, kann er dies über die Signatur machen, indem er eine normale DNS Auflösung macht und dabei die Signatur anfrägt. Dieser kann er dann direkt vertrauen oder eine Vertrauenskette zu einer bereits vertrauenswürdigen Autorität bilden. Dafür wird der öffentliche Schlüssel im neuen DNSKEY RR gespeichert und kann so vom entsprechenden Nameserver selbst ausgeliefert werden. Dieses Record muss zum Aufbau einer Vertrauenskette wiederum von der höheren Instanz signiert sein. Momentan ist hierbei der Einsatz von RSA Verschlüsselung vorgesehen. Dennoch gibt es Entwicklungen modernere, kleinere und damit schnellere ECC[2] für DNSSEC zu verwenden [10]. DNSSEC basiert nicht auf gesicherten Verbindungen zwischen den Instanzen sondern lediglich auf gesicherten Objekten [1].

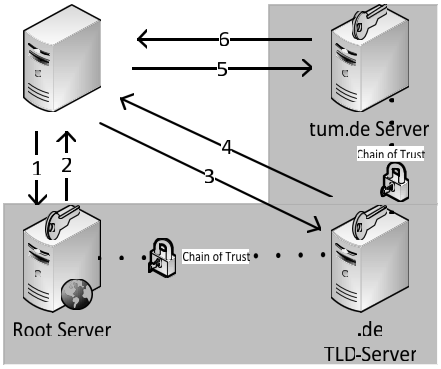


Abbildung 3: DNS mit DNSSEC

Abbildung 3 erweitert das Szenario aus Abbildung 2 um die zur Absicherung nötigen DNSSEC Elemente: Die im grauen Kasten enthaltenen Server benötigen jeweils einen öffentlichen und einen privaten Schlüssel. Durch gegenseitiges Signieren der Keys entsteht eine Vertrauenskette (gepunktete Linie), durch welche es dann möglich ist die RRs bezüglich Authentizität und Integrität auf einen Server höherer Ebene zurückzuführen und, bis hin zu einer Vertrauenswürdigen Autorität, zu überprüfen.

Auch delegierte Anfragen können mittels des DS RR-Types von DNSSEC überprüft werden, indem ein signiertes DS Record wiederum einen neues DNSKEY Record signiert. Dadurch werden auch komplexere Authentisierungspfade möglich, die es zum Beispiel auch ermöglichen, zusätzliche Ebenen und Pfade in der PKI einzuschieben.

2.2 Sicherstellen der Nichtexistenz von Namen oder Typen

Nachdem nun existierende RRsets signiert werden können, muss DNSSEC auch in der Lage sein, die Nichtexistenz eines

[2]Elliptic Curve Cryptography (ECC) bezeichnet asymmetrische Kryptosysteme, die Operationen auf elliptischen Kurven über endlichen Körpern verwenden.

doi: 10.2313/NET-2011-07-2_08

Namen oder RR Typs sicherzustellen.

2.2.1 NSEC Resource Record

Da ohne eine überprüfbare Negativantwort das unterdrücken einer Nachricht einen Angriff darstellen würde, muss es möglich sein auch Negativantworten zu verifizieren. Die bisher verwendete NXDOMAIN Nachricht kann hierbei nicht verwendet werden, da diese lediglich eine Negativantwort ist, die keinen eindeutigen Bezug zur Anfrage hat. Sie fällt daher auf jede Anfrage nach einer nicht existierenden Domain gleich aus. Daher ist der neue RR-Type NSEC eingeführt worden. Durch eine einheitliche Darstellung und Anordnung der Domainnamen in den Zonen kann ein Nameserver die ebenfalls signierte Information über den leeren Namensbereich schicken, indem er die nächsten existierenden Namen schickt [1]. Abbildung 4 zeigt NSEC am Beispiel eines Na-

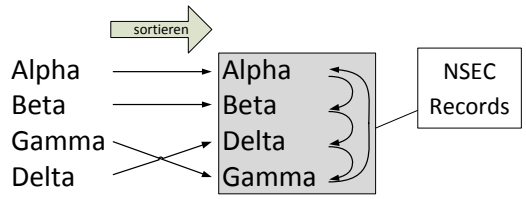


Abbildung 4: NSEC Beispiel

meservers, der die Zonen „Alpha“, „Beta“, „Gamma“ und „Delta“ hält. Hat Alice beispielsweise die nicht existierende Domain „Epsilon“ angefragt, bekommt sie das NSEC Record „Delta“ und „Gamma“ als Antwort, da dies die nächsten existierenden Zonen sind.

2.2.2 NSEC3 Resource Record

Allerdings ermöglicht das schrittweise Abfragen der NSEC RRs, also der leeren Namensbereiche, einen Rückschluss auf alle existierenden Namen der Zone. Da dieses Verhalten unerwünscht sein kann, wurde der NSEC3 RR eingeführt. Der NSEC3 RR ist ein Hash des nächsten existierenden Namens. Der Empfänger kann dadurch überprüfen, wenn der Hash des angefragten Namen kleiner ist als der empfangene [3]. Abbildung 5 verdeutlicht NSEC3 am Szenario aus Abbildung 4. Als Antwort auf Alices Frage nach der nicht existierenden Domain „Epsilon“ mit Hash „bx42“ erhält sie nun den Hash „bb3y“ und „c56b“ als Antwort. Sie kann nachprüfen, dass der hash von Epsilon dazwischen liegt

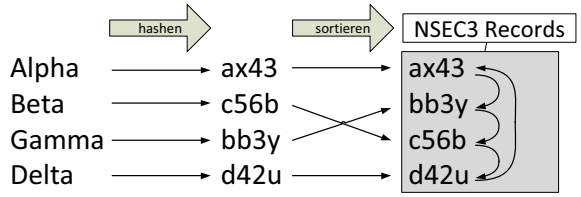


Abbildung 5: NSEC3 Beispiel

Hashwerte dieser Art können bei ausreichend kurzen Eingaben zurückgerechnet werden. Daher ist es dennoch mit genügend Aufwand möglich, die Namen zu erraten [7]. Da DNS öffentliche Informationen ohne Zugangsbeschränkungen bereitstellt, müssen geheime Informationen hinter einer Firewall versteckt werden. Das Problem kann dennoch durch sogenannte NSEC3 „White Lies“ gelöst werden. Ein Unsichtbarer Name wird beim Hash, den der Anfrager eines nichtexistierenden Namens erhält, einfach nicht berücksichtigt: Angenommen Domain „Alpha“ soll nur von Alice gesehen werden. Bob will wissen, ob die Domain „Epsilon“ mit dem Hash „ab42“ existiert. Da diese nicht existiert, antwortet der Nameserver mit einem NSEC3 Record. Bob wird nun aber nicht den Hash von „Alpha“ erhalten, sondern den Hash des nächst höheren Namens, „bb3y“.

2.3 Schlüsselmanagement in DNSSEC

Um eine PKI entlang der Domainhierarchie zu etablieren, nutzt DNSSEC pro Zone zwei verschiedene Keys, die in Tabelle 1 aufgelistet sind.

Tabelle 1: Schlüssel in DNSSEC

Schlüsselname	Schlüssellänge	Gültigkeitsdauer
Key-Signing-Key:	2048 Bit	2-4 Jahre
Zone-Signing-Key:	512 Bit	1-2 Monate

Dabei signiert der durch den eigenen Key-Signing-Key (KSK) signierte, kurzlebige Zone-Signing-Key (ZSK) die DNS-Einträge der eigenen Zone. Der KSK signiert, neben dem eigenen ZSK, KSKs der darunter liegenden Zonen und ist wiederum von der übergeordneten Zone signiert, beziehungsweise bei der Root-Zone von sieben Personen, die nach einem Schema zur Geheimnisteilung zusammen den Schlüssel besitzen. Die Indirektion von KSK und ZSK bringt für den kürzeren ZSK einen verminderten Rechenaufwand zur Überprüfung und weniger zu übertragende Daten bei DNSSEC-Anfragen. Da kurze Schlüssel weniger sicher sind, wird für den langlebigeren KSK eine höhere Schlüssellänge gewählt. Zusätzlich wird durch die Aufteilung offline Signing ermöglicht. Der mächtigere Schlüssel kann in einem sicheren Bereich aufbewahrt werden.

Da offline Signaturen auch Nachteile mit sich bringen, wird ihre Verwendung an DNSSEC auch kritisiert [7]. Offline Signaturen, wie sie in DNSSEC verwendet werden, seien nicht in der Lage dynamisch Links zu erzeugen, müssten zwischengespeichert werden und seien auf Grund der vergleichsweise langen Lebensdauer anfällig für Angriffe wie beispielsweise das Finden einer zu einem Hash passenden Signatur. Während in DNSSEC sich sehr frequent ändernde Links, auf Grund der ständig nötigen Neuzertifizierung, tatsächlich Probleme bereiten, seien laut Dan Kaminsky die anderen Punkte nicht haltbar [13], da mit DNSSEC auch online Signing möglich ist. So sei zum Beispiel on demand online Signing, also das sofortige automatische Absichern einer Domain, durchaus möglich für DNSSEC (RFC4470, RFC4471), wie es das auch für alle gängigen Protokolle und sogar DNSCurve sei.

Resolver können sich bereits verifizierte ZSKs cachen, damit diese nicht bei jeder Anfrage überprüft werden müssen. Beim Cachen kommt neben der alten Time to Live (TTL) nun noch ein neues Verfallsdatum hinzu. Während die TTL beim normalen DNS vom Cachezeitpunkt abhängt, muss diese neue Zeit ein absoluter, vom Zertifikat beziehungsweise Schlüssel abhängiger Wert sein, der gecachete

doi: 10.2313/NET-2011-07-2_08

Daten mit abgelaufenen Zertifizierungen entfernt. Im Resolver kann als Vertrauensanker also entweder ein KSK oder ein ZSK gewählt werden. Ersteres authentisiert damit nur die DNS-Antworten dieses Servers, während Zweiteres die ganze Zone authentisiert. Ist dem Resolver nur der Hash eines Schlüssels bekannt, kann der Schlüssel über DNS erhalten werden. Sofern Platz in der DNS Antwort ist, werden die Signaturen einer Zone, die zum Authentisieren der öffentlichen Schlüssel nötig sind, automatisch mitgesendet um die Zahl der Roundtripps klein zu halten.

2.4 DNSSEC als Nachfolger der X.509 PKI

Die X.509 PKI [4] wird zur Absicherung der meisten verschlüsselten Kommunikationen im Web verwendet. Ein Zertifikat wird dabei meist ausschließlich auf Seite des Servers eingesetzt, um den Schlüsselaustauschpartner zu authentisieren. Clients verfügen hingegen nur selten über Zertifikate. Immer wieder kommt es dabei vor, dass eine CA die sich unterhalb eines vertrauten Knotens befindet kompromittiert wird. Dadurch können bösartige Webseiten dem Browser als gültige, gesicherte Webseiten angezeigt werden. So zwang beispielsweise Mitte März eine kompromittierte CA und die fehlerhafte Umsetzung der CRL Prüfung den Browserhersteller Mozilla zum Nachbessern.

In einer durch DNSSEC aufgebauten PKI kann dagegen eine CA, auf Grund der nun existierenden, strukturbedingten Bindung von CAs und deren öffentlichen Schlüsseln an die Domainnamen, lediglich in ihrem Namensbereich zertifizieren. Das dadurch entstehende Konzept der Zertifizierung relativer Namen wurde bereits vor über 30 Jahren in [9] beschrieben. Es wird die Gefahr durch eine kompromittierte Autorität minimiert. Auch das Verwenden von Aliasen ist in einer solchen Zertifizierungsstruktur möglich. Will ein Benutzer also beispielsweise weder dem „.de“ TLD Nameserver noch dem obersten Knoten vertrauen, so kann er, falls diese Domain auch unter einer „.com“ Endung existiert, auch dem „.com“ TLD Nameserver vertrauen und so eine Vertrauenskette zum unter der gewünschten Domain registrierten Server aufbauen.

Zum Erhalten des öffentlichen Schlüssels, beziehungsweise des eigentlichen Zertifikats gibt es verschiedene Ansätze: DNS kann den öffentlichen Schlüssel im DNSKEY RR speichern oder kann lediglich einen Hash davon enthalten. Da X.509 Zertifikate [4] sehr viele, meist überflüssige, Verwaltungsinformationen enthalten, kann es sinnvoll sein ganz auf Zertifikate zu verzichten und nur den öffentlichen Schlüssel zu verwenden. Werden, zum Beispiel durch bereits für X.509 Zertifikate entwickelte Software, X.509 Zertifikate benötigt, können diese über die Website erhalten werden und deren Authentizität über das DNS gesichert werden. Aber auch den im X.509 Zertifikat eingekapselten, öffentlichen Schlüssel kann man im DNS mittels des CERT RRs hinterlegen. Für die Ablage neuer Informationen spielt die Größe eine entscheidende Rolle. DNS verwendet meistens UDP, muss aber bei größeren Datenmengen auf TCP ausweichen, da die Wahrscheinlichkeit, dass die Antwort bei Verwendung von UDP nicht ankommt, mit der Zahl der für eine Nachricht nötigen Pakete steigt. Hierbei sind vor allem die Größen 512 Bytes und 1500 Bytes relevant. Erstere ist die maximale Größe, bei der die Fragmentierung verhindert werden kann, während Zweiteres die Größe ist ab der auf jeden Fall fragmentiert wird. Mit DNSSEC wächst die Auffassung, man könne das DNS auch zur Auslieferung neuer, größerer Daten nutzen. Daher ist es, da es die einzige Möglichkeit ist, vertretbar bei Größen die UDP überfordern würden, auf TCP auszuweichen und den mit TCP verbundenen Overhead in Kauf zu nehmen. Ebenfalls kann durch die Verwendung von TCP die Verstärkungswirkung durch DNS Server eingeschränkt werden, da hier bereits nach dem vergleichsweise wenig Bandbreite benötigendem Handshake die Verbindung abgebrochen wird, sofern Anfragesteller und Antwortziel nicht identisch sind [13].

Als Kritik an einem vollständigen Ersatz der X.509 PKI sei angeführt, dass DNSSEC lediglich Domains, jedoch keine direkten Personen authentisiert. Zusätzlich weist die Infrastruktur der DNS-Anbieter oft keine mit den X.509 Zertifizierungsstellen vergleichbare RA auf.

2.5 Nutzen und Schwachstellen von DNSSEC

DNSSEC ermöglicht es sicherheitsbewussten Nameservern und Resolvern, die Verlässlichkeit von DNS-Anfragen zu validieren und als sicher, unsicher, gefälscht oder unvertraut einzustufen. Unvertraut meint hierbei, dass die Anfrage zwar überprüfbar ist, aber eine Kette zu einem Vertrauensanker nicht existiert. Wie dann beispielsweise mit einer unvertrauten Antwort umgegangen wird, hängt von der jeweiligen Sicherheitspolitik ab. Als Beispiel kann ein Resolver der DNSSEC unterstützt, aber rekursiv hinter einem anderen, nicht DNSSEC unterstützendem Resolver ist, eine Antwort nur als unsicher einstufen. Wenn DNSSEC von allen an einer Anfrage beteiligten Server und vom Client unterstützt wird, kann DNSSEC Spoofing und Poisoning-Angriffe verhindern. DNSSEC kann also als Security-Enabler dienen. Es kann neue Sicherungsmechanismen ermöglichen, stellt jedoch alleine keinen Garant für Sicherheit dar.

Für DNSSEC wird eine globale, hierarchische PKI mit relativen Namen aufgebaut, die auch für andere Szenarien eingesetzt werden kann. Der Vorteil dieser PKI ist, dass DNS in Verbindung mit DNSSEC eine einzige Instanz, die über ein überall genutztes System authentisierte Zertifikate verteilen kann, darstellt. Jeder Nameserver kann hierbei nur Aussagen in seinem Namensbereich machen. Dies löst ein bekanntes Problem der älteren X.509 PKI, bei dem es durch Vertrauen einer CA vorkommen kann, dass weiter unten in der Hierarchie eine weniger vertrauenswürdige CA falsche Zertifikate erstellt und diesen dann vertraut wird.

DNSSEC war ursprünglich angedacht, um die Kommunikation unter Nameservern abzusichern. Der Benutzer sollte ursprünglich nur durch ein Bit erfahren dass die Adresse sicher ist. Dennoch konnten Daten dann am Ende verfälscht werden. Daher war schnell klar, dass auch Endgeräte die Ergebnisse der DNS Anfrage überprüfen können sollten. Allerdings findet DNSSEC zur Zeit vor allem auf vielen Endgeräten und Routern noch nicht die für eine lückenlose Kette nötige Verbreitung. Daher liefert DNSSEC oft noch keine Ende zu Ende Sicherheit. DNSSEC sieht aber dennoch vor, dass auch Endbenutzer DNS Informationen überprüfen können.

DNS wurde ursprünglich in der Annahme entwickelt, jedem Anfragenden auf eine identische Anfrage die gleiche Ant-

doi: 10.2313/NET-2011-07-2_08

wort zu liefern. DNS-Daten sind also für jeden Anfragenden sichtbar, weswegen DNSSEC keine Vertraulichkeit, Zugriffsschutz oder differenzierte Antworten für unterschiedliche Anfragende schafft. DNSSEC bietet keine Schutzmaßnahmen gegen DoS-Angriffe, wie sie bereits bei DNS ohne DNSSEC möglich waren. Durch die Verursachung von Rechenaufwand für kryptographische Operationen entstehen sogar weitere Möglichkeiten für DoS-Angriffe. Kritiker warnen, dass DNSSEC Amplification Angriffe ermögliche, da teilweise mit sehr großen Datenmengen geantwortet wird [7]. Dies ist, wie bereits erwähnt, ein generelles IP- beziehungsweise UDP-Problem. Pakete können einfach gesendet werden ohne dass sie angenommen werden müssen. Auch DNS ermöglicht schon die Wirkung als Verstärker. Laut Dan Kaminsky liefert DNSSEC, gemessen an DNS, etwa die doppelte Verstärkung. Größere Antworten müssen vom DNS per TCP verschickt werden. Die dadurch vergrößerte Anfälligkeit für Amplification Angriffe werde aber laut Dan Kaminsky ohnehin durch effektiveres HTTP Flooding in den Schatten gestellt [13].

Ebenfalls sieht DNSSEC keine Schutzmaßnahmen für Zonenübertragungen oder dynamisches Updates vor. Da DNSSEC, wie beschrieben, die Objekte und nicht die Verbindung schützt, besteht die Möglichkeit, veraltete Informationen, so lange der ZSK gültig ist, wieder einzuspielen. Somit kann ein nicht mehr gültiger Verweis auf eine IP-Adresse, die nicht mehr unter Kontrolle des ehemaligen Besitzers ist, noch verwendet werden. Da diese Adresse nun beispielsweise für das Betreiben einer Phishingwebsite genutzt werden könnte, stellt dies ein Sicherheitsrisiko dar.

3. DNSCURVE

DNSCurve ist im Vergleich zu DNSSEC eine deutlich jüngere Erweiterung des DNS. Es wurde vom Kryptologen Daniel J. Bernstein (DJB) vorgestellt, mit dem Ziel, Schwachstellen von DNSSEC zu beheben. DNSCurve soll im Gegensatz zu DNSSEC auch Vertraulichkeit schaffen. DNSCurve sichert die Verbindungen ab und dadurch nur indirekt die Objekte. DNS-Anfragen werden dabei mit CurveCP gesichert. Der Name bezieht sich auf die Verwendung von ECC auf Curve25519, im Gegensatz zur in DNSSEC verwendeten RSA-Verschlüsselung. ECC bietet den Vorteil, mit deutlich kürzerer Schlüssellänge bereits vergleichbare Sicherheit zu erreichen. Die kürzere Schlüssellänge ermöglicht performantere kryptographische Berechnungen. CurveCP ist ein ebenfalls von DJB entwickelter und vorgestellter Ansatz zur Absicherung des Internetverkehrs. CurveCP verschlüsselt Pakete der Anwendungsschicht und versendet diese per UDP. Es ersetzt TCP und baut eine verlässliche Verbindung innerhalb von CurveCP nach.

Abbildung 6 veranschaulicht den Ablauf einer DNS-Anfrage mit CurveCP. Jeder DNSCurve Teilnehmer besitzt einen öffentlichen und einen privaten Schlüssel. Dadurch können einem DNSCurve-Teilnehmer Pakete verschlüsselt geschickt werden, wenn dem Sender der öffentliche Schlüssel bekannt ist. Ein DNSCurve Client schickt eine Anfrage an einen Nameserver, indem er die DNS-Anfrage mit dem öffentlichen Schlüssel des Nameservers, dem eigenen privaten Schlüssel und einer Nonce zu einer „kryptographischen Box“ verschlüsselt. Anschließend wird die Nonce und der eigene öffentliche Schlüssel dazu gepackt. Dadurch kann der CurveCP-fähige

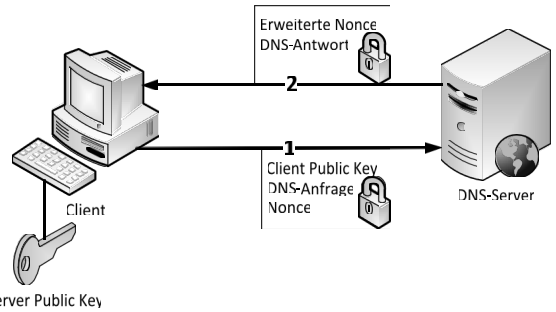


Abbildung 6: CurveCP: Beispiel einer Anfrage

Nameserver über den verwendeten privaten Schlüssel des Senders dessen Identität sicherstellen. Durch die Verwendung des öffentlichen Schlüssels des Nameservers wird sichergestellt, dass nur dieser in der Lage ist die Nachricht zu entschlüsseln. Durch die Kombination von Signatur und Verschlüsselung in einen Ablauf, kann dies mit weniger Rechenaufwand erreicht werden. Eine exakte Beschreibung der zugrunde liegenden Kryptographie und des Aufbaus der „kryptographischen Box“ kann in [6] nachgelesen werden. Dieses Paket wird anschließend per UDP an den Nameserver geschickt. Zunächst wird das Paket vom DNSCurve-fähigen Nameserver als CurveCP Paket behandelt. Es wird entpackt und dabei auf Authentizität und Integrität überprüft. Wenn dies fehlschlägt, wird das Paket wie ein normales DNS-Paket behandelt, damit auch weiterhin normale DNS-Anfragen möglich sind, wenn DNSCurve von einem Server verwendet wird. Wenn die Prüfung erfolgreich war, wird auf das entpackte DNS-Paket geantwortet. Die Antwort wird mit einer erweiterten Nonce und dem selben Schlüssel, der zum Entpacken des CurveCp-Pakets benutzt wurde, wieder in eine „kryptographische Box“ gepackt. Das entstehende Paket wird anstatt des DNS Pakets an den Client geschickt.

Wenn der wartende Client ein nicht gültiges DNSCurve-Paket, ein Paket mit ungültiger Nonce oder eine anderweitig ungültige kryptographische Box erhält, verwirft er diese. Erreicht ihn eine gültige Antwort, wird diese geöffnet und ist damit als original DNS Antwort des Server identifiziert [5].

3.1 Schlüsselmanagement in DNSCurve und CurveCP

Der folgende Abschnitt beschreibt wie der öffentliche Schlüssel eines Nameservers an den Anfrager ausgehändigt wird.

3.1.1 Selbstzertifizierende URLs

Wie beschrieben, hat jeder DNSCurve-Client und Server einen geheimen Schlüssel und den dazugehörigen öffentlichen Schlüssel. Server verteilen ihren öffentlichen Schlüssel, indem sie ihn in den Servernamen, wie er im normalen NS RR steht, einbetten. Hierbei wird die Idee selbstzertifizierender URLs verwendet, wie sie bereits in [12] beschrieben wurden. Die Schlüssel der TLD Nameserver müssen dem Resolver als Vertrauensanker bekannt sein. So müsste beispielsweise zur Einführung von DNSCurve für `www.tum.de` lediglich folgendes RR an den .de Nameserver gemeldet werden: `www.tum.de CNAME 1238675309.tum.de`. 123 ist in diesem verkürzten Beispiel ein Schlüsselwort zur Erkennung,

doi: 10.2313/NET-2011-07-2_08

dass es sich um einen öffentlichen Schlüssel für DNSCurve handelt. Der Client kann daher den Schlüssel 456789 extrahieren. Die Verwendung von selbst zertifizierenden URLs ermöglicht es bestimmten Anwendungen selbst zu definieren, welchen Schlüssel sie verwenden. Ihren eigenen öffentlichen Schlüssel fügen Clients dagegen einfach in ihre Anfragen ein, um sie für die Antwort dem Server mitzuteilen.

3.1.2 Kritik am Schlüsselmanagement in DNSCurve

Dan Kaminsky kritisiert Bernsteins DNSCurve, da es nicht möglich ist sichere, dezentrale und menschenlesbare URLs zu haben [13]. Bernstein benutzt URLs wie beschrieben als Vertrauensanker, präsentiert aber eine Möglichkeit, diese lesbar zu machen und dadurch durch Benutzer handhabbar. Das von Bernstein vorgestellte System ist als problematisch anzusehen, wenn sich IP-Adressen ändern. Kaminsky befürchtet, dass, falls sich Keys ändern, das Internet bald voll sein wird mit nicht funktionierenden Links. Bernsteins Lösung, hierbei mit einem noch nicht genauer spezifizierten P2P DNS Abhilfe zu schaffen, würde dann Sicherheit ausschließen. Ohne eine ausgearbeitete Lösung für das Keymanagement sei DNSCurve jedoch nicht voll funktionstüchtig. Weiter kritisiert Kaminsky die Tatsache, dass DNSCurve nur online Nachrichten unterzeichnen kann, während DNSSEC sowohl online als auch offline Signieren ermöglicht [13]. Der Vorteil von offline Signaturen ist, dass sie erlauben, geheime Schlüssel an einem sichereren Platz aufzubewahren. Beim online Unterzeichnen müssten beispielsweise alle Server einer TLD den privaten Schlüssel haben, was ein Sicherheitsrisiko darstellt.

3.2 DNSCurve als Nachfolger der X.509 PKI

Auch DNSCurve soll, sofern es eingesetzt wird, zur Absicherung der gängigen für X.509 Zertifikate aufgebauten PKI dienen. Eine klassische PKI kann mit DNSCurve jedoch nicht aufgebaut werden, da DNSCurve lediglich Verbindungen absichert. Wenn alle Verbindungen abgesichert und der Client entweder iterativ alle Daten selbst abholt oder allen rekursiv arbeitenden Nameserver vertraut, ist jedoch ein sicherer Kanal mit dem authentisierten Server aufgebaut. Auch wenn Zertifikate in diesem Fall dann auf Grund des sicheren Kanals meist nicht mehr nötig sind, können diese vom Server einfach über den sicheren Kanal geschickt werden. Die Existenz einer ganzen PKI ist in diesem Fall nicht mehr nötig. Jeder Server kann sich sein Zertifikat selbst erstellen und über den bereits existierenden sicheren Kanal selbst verteilen.

3.3 Nutzen und Schwachstellen von DNSCurve

DNSCurve bietet im Gegensatz zu DNSSEC nicht nur Integrität und Authentizität, sondern durch Verschlüsselung auch Vertraulichkeit. Es nutzt ECC und ist dadurch deutlich performanter. DNSCurve ist eine minimalistische Lösung und daher einfach in bestehende Systeme zu implementieren. Es muss nur ein DNSCurve-Modul auf dem Server beziehungsweise dem Client installiert werden. Manipulierte Pakete werden sehr effizient verworfen, was gut gegen DoS-Angriffe ist.

Als problematisch kann der erhöhte kryptographische Aufwand für die Server angesehen werden, da die Ver- und Entschlüsselungen, im Gegensatz zu DNSSEC, bei jeder Verbindung durchgeführt werden muss. Misst man DNSCurve an dem Ziel, Vertraulichkeit zu schaffen, wird dieses nicht voll erreicht, da Sender, Empfänger und die Paketlänge sichtbar bleiben.

DNS-Caches müssen erweitert werden um DNSCurve zu unterstützen. Auch die Caches müssen Ver- und Entschlüsselungen für jede Anfrage durchführen. Hierfür wird für effizienteres Weiterverarbeiten ein geheimer Schlüssel sc zwischen Caches c und Servern s eingesetzt. Ein Cache wird jedes Mal, wenn er einen neuen öffentlichen Schlüssel s eines Servers erhält, daraus einen neuen geheimen Schlüssel sc berechnen.

Nach herkömmlicher Art des Cachings im DNS kann DNSCurve nur Sessions cachen, während mit DNSSEC Records gecached werden. Cachen pro Session benötigt aber eine bedeutend größere Anzahl an Cacheinträgen, da die Anzahl der Sessions hoch ist und die Anfragelast pro Session eine deutlich niedrigere Varianz aufweist als die gesamte Anfragelast. Neben dem geringeren Nutzen eines solchen Vorgehens, führt dies zu einem deutlich erhöhten Aufwand für Caches.

Auch werden Firewallprobleme mit CurveCP durch das Tunneln von größeren Datenmengen über DNS-Port 53, ohne DNS zu emulieren, befürchtet. Daher wäre es Sinnvoll einen anderen Port zu verwenden [13].

4. PERFORMANZVERGLEICH

Der folgende Abschnitt behandelt die Performanzdebatte über DNSSEC und DNSCurve zwischen Dan Kaminsky [13] und Daniel J. Bernstein [7]. Dan Kaminsky ist ein Spezialist für Computersicherheit und Geschäftsführer des Penetration-Testing-Unternehmens IOActive. Er arbeitete unter anderem für Cisco, Avaya und Microsoft. Seit 2010 ist er, als einer der sieben Schlüsselträger des DNS-Rootkeys, der amerikanische Repräsentant. Daniel Julius Bernstein ist Professor an der University of Illinois in Chicago. Er ist unter anderem Autor der DNS Serversoftware djbdns und entwickelt zurzeit DNSCurve und CurveCP, um damit das aufkommende, seiner Meinung nach nicht ausreichende, DNSSEC und die bestehenden Ansätze wie HTTPS zu ersetzen.

Wie in den vorangegangenen Abschnitten beschrieben, versuchen sowohl DNSSEC als auch DNSCurve durch sichere Authentisierung, über DNS eine Grundlage für sichere Kommunikation im Netz zu legen. DNSSEC ermöglicht einen Vertrauensanker für TLS oder IP-Sec, während DNSCurve mit der dazugehörigen Lösung CurveCP funktionieren soll. DNSCurve und CurveCP gleicht dabei noch mehr einem Entwurf, während DNSSEC bereits auf eine immer größer werdende, installierte Basis zurückgreifen kann.

4.0.1 Einsatz von Eliptic Curve Kryptographie

In der Analyse von DNSCurve kann Kaminsky den von Bernstein festgestellten Performanzvorteil von Curve25519 bestätigen [13]. Curve25519 ist etwa um Faktor 4 bis 8 schneller als RSA1024. Jedoch sei zu bedenken, dass RSA besser unterstützt ist und auf modernen Rechnern daher dank besserer Hardware einer durch Software berechneten Curve25519 überlegen sein wird. Kaminsky nimmt das bei gleicher Schlüssellänge niedrigere Level an Sicherheit von RSA

doi: 10.2313/NET-2011-07-2_08

dabei in Kauf. Als weitere Kritik am Einsatz von Curve25519 in DNSCurve muss angesehen werden, dass ein Beweis gegenüber einer dritten Person nicht wie mit mit RSA signierten Nachrichten in DNSSEC möglich ist. Das führt dazu, dass es in DNSCurve keinen Mechanismus gibt, eine ganze Vertrauenskette in einer einzigen Anfrage zu überprüfen. Der Client muss daher zu jedem Beteiligten eine Verbindung aufbauen.

4.0.2 Caching abgesicherter DNS-Pakete

Als größte Schwäche von DNSCurve nennt Kaminsky die Unmöglichkeit, DNSCurve-Nachrichten für andere Benutzer zu cachen [13]. Dies würde, im Gegensatz zu DNSSEC, den ISP Cache komplett aushebeln. Kaminsky schätzt hierbei eine deutlich erhöhte Belastung für die autoritativen Nameserver, während Bernstein von einer 1,15 fachen Belastung ausgeht. Dies würde jedoch nur eine Trefferrate pro Cache von gemittelt 6% bedeuten. Providerstatistiken lassen eine Trefferrate der ISP-Caches von etwa 80% -90% vermuten - also 5x-10x Belastung [13]. Bernstein argumentiert, dass lokales Caching dennoch möglich sei und Cachen in zweiter Ebene irrelevant sei. Kaminsky erwidert, dass lokales Caching bereits gemacht werde und alleine nicht ausreichen würde. Dabei stützt er sich auf Messwerte großer Caches, während Bernstein sich auf ein seiner Meinung nach unrealistisches Laborexperiment beziehe. Schließlich sei Caching zweiter Ebene auch für die Latenz meistens besser als den autoritativen Nameserver anzufragen.

4.0.3 CurveCP vs. SSL

Bernstein nennt Performanzprobleme als Grund für die nicht volle Verbreitung von HTTPS und damit als Motivation das performantere CurveCP zu verwenden [7]. Er führt dabei Google an, das nicht alle Daten mittels HTTPS verschlüsselt. CurveCP dagegen sei performanter, da Verschlüsselte Pakete nicht in einem TCP-Stream, sondern per UDP versendet werden. Verlässlichkeit wird durch das Imitieren einer TCP Verbindung innerhalb des CurveCP Protokolls erreicht. Laut Kaminsky, der sich unter Anderem auf Aussagen von Verantwortlichen bei Google stützt, ist Performanz jedoch keiner der Gründe die gegen HTTPS sprechen. HTTPS sei vor allem aufwändig „anzuschalten“, da die meisten Webseiten aus einem Konglomerat diverser Komponenten, die durch Links zusammengehalten werden, bestehen. Dabei ist vor allem der Aufwand zur Absicherung jeder einzelnen Komponente ein großes Hindernis. Hier kann eine Absicherung des DNS einen Vertrauensanker schaffen und, zum Beispiel durch wegfallende Arbeit mit einer PKI Struktur, den Einstiegsaufwand senken.

5. FAZIT

DNSSEC bietet die Möglichkeit, die Authentizität und Integrität von allen Informationen im DNS zu sichern. Neben den im DNS enthaltenen IP-Adressen kommen öffentliche Schlüssel, oder zumindest Hashes davon, hinzu. Dies motiviert dazu, das überall verfügbare und, zum Beispiel durch das TXT Record, sehr flexible DNS für weitere Einsatzszenarien als dem bloßen Ablegen von IP-Adressen zu verwenden. Zusätzlich können dank DNSSEC Schwachstellen bisheriger X.509 PKIs überwunden werden. DNSSEC kann den Verbindungsaufbau für IP-Sec oder TLS erheblich vereinfachen, absichern und auch beschleunigen. Auch DNSCurve mit CurveCP verfolgt das Ziel, das komplette Internet abzusichern. Es soll hierbei zusätzlich zur Authentizität auch Vertraulichkeit geschaffen werden, ohne dabei auf weitere, bereits existierende Protokolle angewiesen zu sein. Beide Ansätze besitzen Probleme mit gerade in letzter Zeit aufkommenden Vorschlägen für ein P2P DNS umzugehen.

DNSSEC, mit seiner langen Entwicklungsgeschichte, erfreut sich immer größerer Verbreitung. Der sehr einfach konzipierte Ansatz von DNSCurve stellt dagegen eine Alternative zur Verfügung, die allerdings noch diverse Tests bezüglich Einsetzbarkeit und Klärung einiger ungelöster Probleme benötigt. Anschließend müsste DNSCurve den Vorsprung von DNSSEC aufholen. Welche Entwicklungen am Ende von den diversen Stakeholdern angenommen werden, bleibt abzuwarten.

6. LITERATUR

[1] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose: *DNS Security Introduction and Requirements*, RFC 4033, März 2005

[2] S. M. Bellovin: *Using the Domain Name System for System Break-ins*, In Proceedings of the Fifth Usenix Unix Security Symposium, Seite 199-208, Salt Lake City, USA, Juni 1995

[3] D. Blacka: *DNS Security (DNSSEC) Hashed Authenticated Denial of Existence*, RFC 5155, Februar 2008

[4] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk: *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, RFC 5280, Mai 2008

[5] M. Dempsky: *DNSCurve: Link-Level Security for the Domain Name System*, Internet-Draft, Februar 2010

[6] D. J. Bernstein: *Cryptography in NaCl*, Networking and Cryptography library, 2009

[7] D. J. Bernstein: *High-speed high-security cryptography: encrypting and authenticating the whole Internet*, 27C3, Berlin, Deutschland, 2011

[8] D. Eastlake: *Domain Name System Security Extensions*, RFC 2535, März 1999

[9] M. Gasser, A. Goldstein, C. Kaufman, B. Lampson: *The digital distributed systems security architecture*, Proc. of the 12th National Computer Security Conference, Seite 305-319, NIST, Gaithersburg, USA, 1989

[10] P. Hoffman: *Elliptic Curve DSA for DNSSEC*, Internet-Draft, Dezember 2010

[11] M. Lottor: *Domain Administrators Operations Guide*, RFC 1033, November 1987

[12] M. Kaminsky, E. Banks: *SFS-HTTP: Securing the Web with Self-Certifying URLs.*, MIT Laboratory for Computer Science, Cambridge, USA, 1999

[13] D. Kaminsky's Blogg `http://dankaminsky.com`

[14] P. Mockapetris: *Domain Names - Concepts and Facilities*, RFC 1034, November 1987

[15] P. Mockapetris: *Domain Names - Implementation and Specification*, RFC 1035, November 1987

[16] A. S. Tannenbaum: *Computer Networks*, vierte Auflage, Prentice Hall, New Jersey, USA, 2003

Locator/Identifier Split

Wiebke Köpp
Advisor: Alexander Klein
Seminar Future Internet SS2011
Chair for Network Architectures and Services
Department of Computer Science, Technical University of Munich
Email: koepp@in.tum.de

ABSTRACT

The size of routing tables in the default free zone (DFZ) has exceeded 350000 entries by now and will grow even more in the future. The reasons behind this rapid growth are provider-independent addressing, multihoming and traffic engineering. IPv6, providing a much bigger address space than IPv4, allows for more devices to be connected. As a consequence, routing does not scale anymore and measures have to be taken in order to reconstitute scalability in the Internet. Many approaches which try to do that are based on a Locator/Identifier (Loc/ID) split. It modifies the current addressing paradigm by splitting locators for routing purposes from identifiers of end-systems. This paper is a survey of the Loc/ID split. It explains its general ideas and describes implementation efforts.

Keywords

Locator/Identifier Split, Routing, Scalability, LISP

1. INTRODUCTION

In its early stages, the Internet was only a network of a few research facilities. Nowadays over 2 billion people have access to the Internet, with even more to come [1]. The number of hosts has reached a point where they cannot be numbered using the address space of IPv4. IPv6 provides a much bigger address space, making it possible to connect more users and devices, as a result solving the issue of address depletion. However, IPv6 reinforces scalability problems at the same time. Besides the increase of users, different behaviors of Internet Service Providers (ISPs) and their customers challenge the current Internet architecture. There has been a shift in how customers use the Internet. A growing interest in multihoming, thus being connected to multiple providers instead of just one, can be recognized since users want reliable access to the Internet at all time. Also, an increasing number of mobile devices are connected to the Internet, creating a demand for support of mobility. Providers on the other hand perform traffic engineering. The way these actions are performed and these demands are fulfilled today are reasons for the rapid growth of routing tables in the DFZ, as shown in Figure 1. The present routing architecture will not be able to scale having to cope with the resulting entries. Another reason for the observed scalability problems are the overloaded semantics of IP addresses [27]. IP addresses are used for both identifying end-systems and locating them for routing purposes. Yakov Rekhter once stated: *"Addressing follows topology or topology follows Addressing. Choose one."* [27] But routing is most efficient when addresses are assigned topologically, while handling of end-systems requires exactly the opposite. The single numbering space currently in use certainly cannot serve both. Therefore, a split into two separate spaces, one for identifiers and one for locators has been proposed. Using Loc/Id split principles a host has an identifier and a locator instead of one address for both purposes. Some of the Loc/ID split proposals mainly focus on mobility, but other approaches are expected to solve all the issues addressed above.

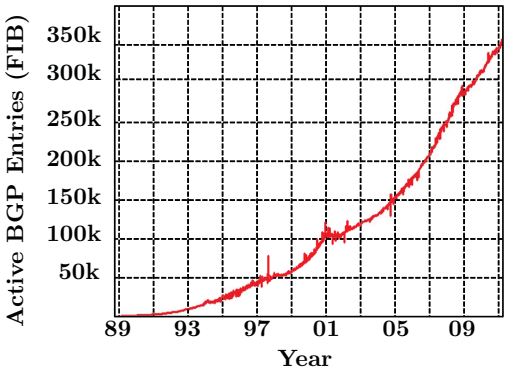


Figure 1: Size of routing tables in the DFZ [14]

This paper is structured as follows. A motivation for the Loc/ID split and a short review of current routing is given in Section 2. General ideas and performance measurements are explained in Section 3. Section 4 introduces one specific implementation in detail and gives a brief overview of other approaches. Section 5 finally concludes the paper.

2. MOTIVATION FOR THE SPLIT

As already mentioned in the introduction, today's routing does not scale anymore for various reasons. Accordingly, some changes to the inter-domain routing protocol Border Gateway Protocol (BGP) have been proposed (e.g. [2, 31, 7]). Unfortunately they imply changes that are hard to deploy.

2.1 State-of-the-art routing and its problems

2.1.1 Current routing

The Internet consists of over 35000 autonomous systems (ASes) [14]. Communication can happen either within a single AS or between multiple ASes. Therefore, a distinction

doi: 10.2313/NET-2011-07-2_09

between intra- and inter-domain routing is drawn. Intra-domain routing takes place within a single AS, while Inter-domain routing handles communication between different ASes. Both use different routing protocols that are adapted to the location where they are deployed.

Routing tables within an AS are created by assigning administrative costs to all links and then use the path with the lowest cost to forward traffic. Intra-domain routing mostly uses link-state routing protocols like OSPF [30] or IS-IS [29]. In link-state routing protocols, routers do not only learn who their neighbors are, they also receive the topology of the system. Using this information, routers can calculate the best path to a desired destination. In intra-domain routing an additional default route can be specified if routing tables contain no match to the destination address. Larger ASes sometimes divide their network into several smaller networks to keep routing within their AS simple and scalable.

Inter-domain routing, on the other hand, uses BGP, which is a path vector protocol. A BGP router tells its neighbors which prefixes are reachable over its own network and which ASes need to be traversed to reach a destination AS. A router then looks up a packet's next hop by searching for the longest prefix match in its forwarding information base (FIB) which is based on the information found in routing tables. Contrary to routers in edge networks, routers in the DFZ do not provide a default route if no match for the destination address can be found. They have an entry for each reachable prefix, causing routing tables to grow with every additional reachable prefix [23].

2.1.2 Scalability

The number of entries in routing tables in the DFZ is increasing rapidly. Along with routing table size, update rates also rise. Update rates are usually around 1–10 update messages per second and peak at approximately 1000 updates per second. Additionally, with the transition to IPv6, larger update rates and routing tables can be expected. As a result, future routers must be very powerful in order to answer all route requests without significant delay. They need to process traffic fast, handle a large amount of updates and store all needed information in their memory. Researchers argue this cannot be accomplished at reasonable cost [27].

Thus, handling the growth of routing tables can only be achieved by eliminating the reasons for the growth. The reasons are provider-independent addressing, multihoming, traffic engineering and countermeasures against prefix hijacking.

In general, IP address space can be owned by either providers or customers. If the provider is the owner of the address space and the customer only rents it, the addresses are called provider-aggregatable (PA). If the addresses belong to the customer, they are provider-independent (PI). A customer with PA addresses has to renumber all his devices when changing providers. Since his new IP address space is a subspace of the providers AS, no additional entries or BGP updates are needed. However, the renumbering is still a costly process which customers would rather avoid. In consequence many customers prefer PI addresses. Provider changes of customers with PI addresses cause updates and new BGP entries because their addresses are usually not aggregatable with the ones of the new provider.

Customers can be interested in multihoming for different purposes. Reliability and service differentiation are two examples. The connection to multiple ISPs can make the Internet connection of a customer more reliable. If the connection to one ISP fails, a fallback connection to another provider can be used. This causes several BGP entries for a single prefix. A customer could also decide to use different providers for diverse services. A portion of the customer's network is assigned to each service, which is then connected to an ISP. Several longer prefixes are announced to BGP instead of one prefix for the whole network.

Providers use traffic engineering to improve performance and use their network's resources more efficiently. For example, they announce more specific routes, thus longer prefixes, to BGP in order to attract traffic at certain gateways. Countermeasures against prefix hijacking also cause providers to announce long prefixes into BGP. In this case, the longest possible prefix is injected into BGP, to prevent a malicious AS to insert a longer prefix and thereby attracting all the traffic. This is mostly done for important services like the Domain Name System (DNS) [27, 23].

2.1.3 Mobility

Researchers expect the number of mobile Internet users to surpass the number of fixed Internet users by 2014 [12]. They also state that with use of the Loc/ID split the impact on routing scalability could be kept at a minimum. The main challenge in mobility is to maintain the connection between hosts, e.g. TCP/IP connections, even if one of the hosts is changing its location. TCP uses IP addresses as identifiers for a connection. When a host moves from one network to another, his IP address changes and the connection is lost. For this reason, the IP address should stay the same, but this interferes with Internet routing. The Loc/ID split provides a solution to accomplish both, keeping IP address and still be able to route properly at the same time.

2.2 Proposed Enhancements to BGP

Efforts have been made to make BGP scalable again, but those are almost impossible to deploy since the Internet is too widely distributed to swap out a protocol on a certain day. Other proposals leave BGP as it is today and introduce an overlaying architecture. Among these are aggregation proxies [34] and lookup systems for nonroutable prefixes [13]. Unfortunately, both approaches are hard to deploy since they require major changes to the Internet in order to work efficiently [23].

2.2.1 Aggregation proxy

ISPs do not announce their prefixes directly to BGP, but to an aggregation proxy. The proxy receives multiple long prefixes, aggregates them to a shorter prefix and then announces the result to BGP. Traffic directed to one of these ISPs is always routed via the proxy, which tunnels the packets to the right destination. The example in Figure 2 shows four networks with prefixes `10.10.0.0/24`, `10.10.1.0/24`, `10.10.2.0/24` and `10.10.3.0/24`. The aggregation proxy aggregates the networks to the shorter prefix `10.10.0.0/22`

doi: 10.2313/NET-2011-07-2_09

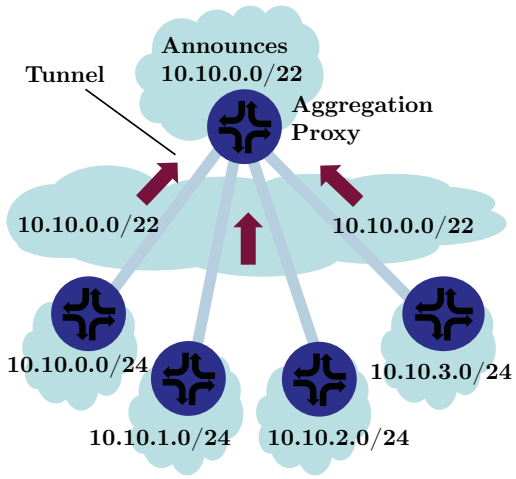


Figure 2: Aggregation Proxy, see [23]

and inserts it into BGP routing tables. This way, routing tables altogether contain fewer entries. In the example, the routing table size is reduced by 3. However, routing via the proxy could lead to longer paths compared to the original BGP path. Another disadvantage is that it is not clear who should be in charge of operating proxies [23].

2.2.2 Lookup System for nonroutable prefixes

Similar to the concept of aggregation proxies, long prefixes are not announced, when using a lookup system for nonroutable prefixes. Instead, they are put in a DNS-like lookup system. Along with the prefix, an entry contains a router over which the prefix is reachable. This router is usually part of the same AS as the prefix. The prefixes in the lookup system do not occur in BGP routing tables, thus they are not routable in the DFZ. If a router receives a packet he cannot find a matching prefix for, he queries the lookup system. The lookup system replies with the address of the router the destination address can be reached over. The router then encapsulates the packet towards the received address, where it is decapsulated again and forwarded to the destination address via intra-domain routing. The process is shown in Figure 3.

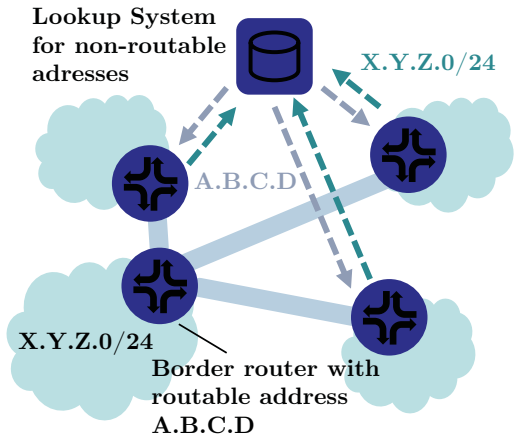


Figure 3: Lookup System, see [23]

Deploying this approach requires even more reformation than the deployment of aggregation proxies. The functionality of looking up nonroutable prefixes on one hand and tunneling packets on the other hand has to be introduced in BGP routers. Additionally, the lookup system itself needs to be created [23].

3. THE LOCATOR/IDENTIFIER SPLIT

The Loc/ID split is a principle many proposals solving scalability issues use. The following section first describes general ideas different approaches have in common and then analyses the performance of those approaches.

3.1 General Ideas

All Loc/ID split solutions have in common that they create two different namespaces for locators and identifiers. While in some approaches both locator and identifier remain IPv4 or IPv6 addresses, other solutions create a new namespace for identifiers.

The Loc/ID solutions that have been proposed so far, fall into two major categories: Map-and-encap and Address Rewriting. [6] gives a detailed comparison of both approaches that will be briefly explained in the following. They can also be classified by the network element, at which they require changes. Host-based solutions require changes at hosts while router-based solutions imply new functionalities in routers. Hybrid solutions also exist.

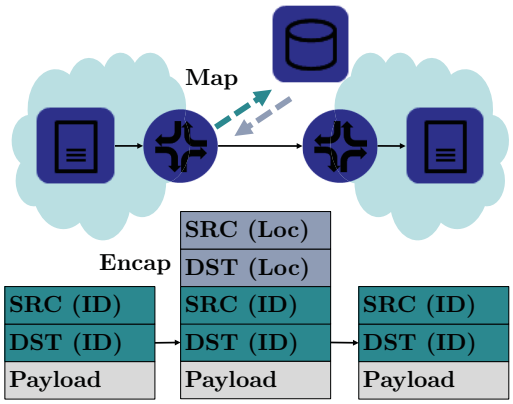


Figure 4: Map and Encap

Map-and-encap stands for approaches that use a mapping system and encapsulation. A host that wants to send data to another host outside its own domain starts by looking up the IP-address of the desired destination in DNS and fills it into the IP-header. Then, the packet travels through the AS. The border router looks up the locator for the destination address and encapsulates the packet. Next, BGP is used to transport the data to the router with that address, where it is decapsulated again and then forwarded to the destination host. The principle can be seen in Figure 4. Map-and-encap solves discussed challenges for scalability issues: Customers can easily switch providers because instead of BGP updates and new entries, only the locator-identifier-mapping in the mapping systems has to be updated. Multihoming and traffic engineering are also supported. The mapping-system can contain several locators for an identi-

doi: 10.2313/NET-2011-07-2_09

fier. Inside an entry in the mapping system, priorities and weights can be assigned to a locator, so that traffic can be directed in a desired way. However, encapsulation adds an additional header to a packet. Packet sizes might come in conflict with Maximum Transfer Units (MTU) and require fragmentation in consequence [23, 25].

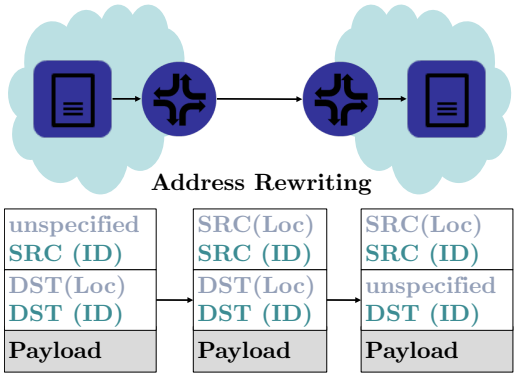


Figure 5: Address Rewriting

Address rewriting solutions take advantage of 128-bit IPv6 address, using the top 64 bits as a locator and the lower 64 bits as an identifier. A host sending a packet specifies the lower 64 bits by inserting its identifier. What happens to the top 64 bits differs in the individual implementations. The top 64 bits could for example be filled with an unspecified value, when a host has no information about its corresponding locator. The locator is then filled in by the border router from where the packet is traversed to the border router of the destination AS. This router replaces the destination locator bits and directs the packet to the destination host [25]. The basic concept can be seen in Figure 5. While some address rewriting approaches require a mapping system, other assume certain host abilities. Once a border router has made an initial address choice, the host is supposed to use that choice in ongoing communications. Multihoming and traffic engineering are also controlled by border routers. They can change the source address of outgoing data in order to redirect returning traffic. When changing providers there is again no need for renumbering since the global routing architecture has no knowledge of identifiers. [6]

In the area of mapping systems used by map-and-encap approaches, several things need to be considered. One goal is to keep the product $State \times Rate$ small. Rate refers to the update rate of identifier-locator-mappings. State means the size of the mapping system in bits. Since most estimates put state around $\mathcal{O}(10^{10})$ [26], the update rate should be small. The same accounts for latency triggered by the lookup in the mapping system. Since a router has to query the mapping system every time it has no information about an identifier, it is convenient for routers to have a local cache. In some mapping system proposals, a router even holds a copy of the whole mapping database. If a mapping is not in the cache, a packet can either be stored and delayed, dropped or forwarded to a place where the mapping is known. Obviously this should occur very infrequently. There exist three different kinds of mapping systems: Pull, Push and hybrid systems that apply a push/pull strategy. In pull systems the router is responsible to maintain mapping entries, while in a push model the mapping service itself initiates updates. Hybrid systems push only some of the data, for example to intermediate databases, while others mappings need to be specifically pulled [23, 25].

Another issue to be considered when implementing a new protocol is incremental deployability. That means protocols should always provide ways to interoperate with the legacy Internet [18]. Otherwise, a protocol has to be deployed in a widely manner from a specific day on to benefit the Internet's architecture. Some approaches achieve incremental deployability by introducing additional proxy gateways, others do not need additional entities.

3.2 Performance Analysis

In terms of scalability, the Loc/ID split has two major implications on inter-domain routing. First, BGP routing tables are reduced and second, the BGP update rate decreases. Using data from a time span from January 2004 until June 2008, Dong et al. [8] could make assumptions on how big the impact of Loc/ID split would be. They came to the following results. There are two different kinds of ASes: stub ASes and transit ASes. Transit ASes deliver data to other ASes and correspond to service providers. Stub ASes, on the other hand, only appear at the end of an ASes path, hence they are customer networks. Stub ASes account for about 80 percent of the total number of ASes, leaving around 20 percent for transit ASes. Even though transit ASes take up only about 20 percent of the number of ASes, the fraction of prefixes belonging to them is much bigger with 60 to 65 percent. This is because transit ASes usually are larger than stub ASes. The Loc/ID split keeps multihoming and traffic engineering activity in customer networks away from routing in the DFZ. Prefixes of customer networks are not announced into BGP. Thus, routing tables can be reduced by the number of prefixes in stub ASes. Dong et. al. also state that stub ASes are responsible for approximately 50 to 60 percent off the updates in BGP which would be eliminated with Loc/ID deployment. BGP update rates are thereby also reduced.

Map-and-encap protocols add an additional header. On account of this header, traffic overhead is produced. Iannone and Bonaventure measured this overhead among other things using data collected at their university and published their results in [15]. They state that 4 to 15 percent overhead in outgoing and 2 to 10 percent in incoming traffic are produced. In their opinion overhead caused by encapsulation should therefore not cause any problems. In [16], the authors report that the additional delay due to encapsulation and decapsulation packet forwarding is around $1\mu s$, only decapsulation in IPv6 causes higher delay with approximately $3\mu s$. The extent to which encapsulation causes problems with MTU is to date unclear, but some possibilities to deal with MTU issues are suggested in [9].

The performance of many Loc/ID solutions additionally depends on the mapping system. In general, in push systems latency is small, while state is big. With pull systems it is the other way around. In push systems, routers already have all the mapping information on cost of having to save it. Pull systems require less memory, but have to query the mapping system more often instead. Hybrid systems create

doi: 10.2313/NET-2011-07-2_09

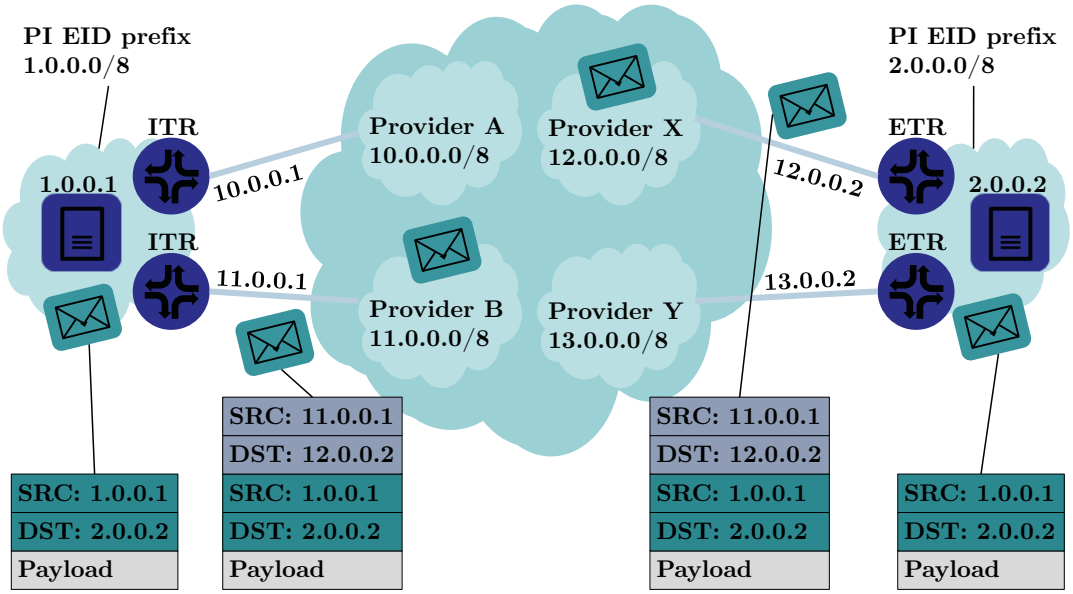


Figure 6: Path of a packet in LISP, see [26]

a balance between state and latency. The state of databases in mapping systems has been addressed in [22]. Assuming that the average identifier multihomes with three ISPs and additional information for, e.g. security, is saved in an entry, the authors of this paper claim that the entry in a mapping database when using IPv6 is about 178 bytes long. With currently about 10^6 needed entries, mapping databases take up about 178 MB. Evaluation of performance in mapping systems in terms of caching hit rates and update rates have also been discussed in several papers [22, 15, 33]. But they each focus on one specific approach and are, therefore, not discussed here.

4. IMPLEMENTATION

This section covers specific Loc/ID split solutions. First, the Locator Identifier Separation Protocol (LISP) is explained. Since LISP-Alternative-Topology (LISP+ALT) is the currently preferred mapping system with LISP, it is discussed as well. Finally, a brief overview on other Loc/ID protocols is given.

4.1 Locator Identifier Separation Protocol

LISP is a map-and-encap-protocol. The split is done by introducing endpoint identifiers (EIDs) and routing locators (RLOCs). Both are IPv4 or IPv6 addresses, but only RLOCs are routable in BGP. The border router performing encapsulation and decapsulation are called ingress tunnel routers (ITR) and egress tunnel routers (ETR) [9]. The communication between two hosts in the same LISP-domain works exactly as it does today. But, if two hosts in different LISP-domains want to communicate, the map-and-encap mechanism is needed. For this, the mapping system is required. It is queried by an ITR, when the ITR does not have a so-called EID-to-RLOC mapping in its local cache. An ITR is responsible for encapsulating a package and sending it towards the specified ETR in the destination domain. An ETR on the other hand has to decapsulate incoming traffic and forward data to its destination.

An example for the path of a packet can be seen in Figure 6. The steps from the first host sending the packet until the second host receives it are the following [26]:

1. The host with EID `1.0.0.1` wants to send a packet to the host with EID `2.0.0.2`. It simply puts those addresses in an IP packet and sends it.
2. The packet traverses the AS until it reaches a border router. In this case, it is the ITR with RLOC `11.0.0.1`
3. Assuming the ITR already has a mapping for `2.0.0.2` in its cache, it encapsulates the packet with a new header. Here, the mapping of EID `2.0.0.2` returns the RLOC `12.0.0.2`. `13.0.0.2` also could have been chosen. The additional header has the RLOC of the ITR as source address and the result of the EID-to-RLOC-mapping of `2.0.0.2` as destination address.
4. Next, the data is send to the ETR with RLOC `12.0.0.2` using BGP.
5. The ETR decapsulates the packet and forwards the packet to the destination address.

As already mentioned, protocols should provide some way to be reachable by hosts in the legacy Internet and also reach those nodes themselves. When a host wants to send packets to a non-LISP host, the ITR could simply forward the packet without encapsulation. But most providers make sure they do not process traffic not belonging to their customers. As a solution, a proxy ETR (PETR) and a proxy ITR (PITR) have been introduced. They are located in networks that do not check source addresses that way. The IP address of a legacy host is not listed in the mapping system with EID-to-RLOC-mappings. So, if an ITR cannot find a mapping for

doi: 10.2313/NET-2011-07-2_09

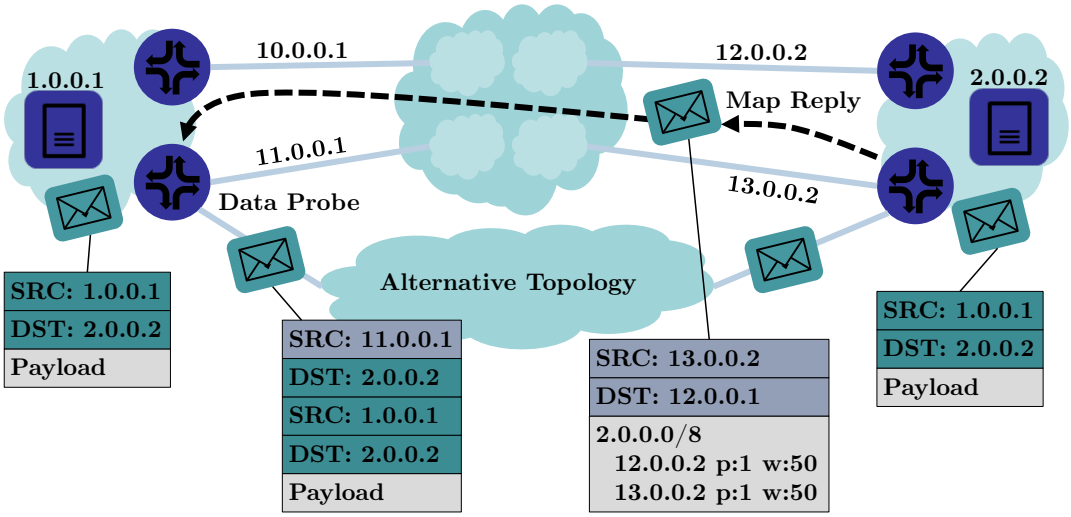


Figure 7: Path of a packet in LISP+ALT when a cache miss occurs, see [26]

an EID it detects that communication with a legacy host is wished. Then, the ITR forwards the data to a corresponding PETR, which can simple transport it to the destination. In case of the other direction, PITRs announce all prefixes via anycast, they want to attract traffic for, thus all addresses used for EIDs. This has to be done since EIDs are not globally routable. PITRs then basically work like normal ITRs. They perform a mapping and then tunnel data to their destination [24].

LISP is a protocol that also provides an architecture to integrate mobile hosts. Its name is LISP Mobile Node (LISP MN). LISP MN allows mobile hosts to multihome and TCP connections to stay alive while roaming. The current proposal of LISP MN seems to have some advantages over Mobile IP, the most common approach to provide mobility, but new problems have also been experienced. A detailed description is given in [24]. The problems are also addressed in this article.

4.2 LISP Alternative Topology

LISP Alternative Topology (LISP+ALT) [10] is the currently preferred mapping systems used with LISP. Basically this mapping system introduces an overlay structure only for handling EID-to-RLOC-mappings. LISP+ALT is a hybrid push/pull model. In case the whole database is pushed to LISP+ALT routers and ITRs have a cache pulling mappings as needed. In case of an ITR needing to get a specific mapping, thus when a cache miss occurs, the ITR can send either a Mapping Request or a Data Probe. Both are routed over the alternative topology and result in a Map Reply sent by the ETR of the original destination EID. A Data Probe is a special kind of Map Request which already contains the data to be sent. This prevents dropping or delaying packets at the ITR. The alternative topology then uses BGP to forward the data. In order to send a data probe an ITR has to encapsulate the packet. Since the destination RLOC is unknown, the destination EID is simply copied.

Figure 7 shows a scenario when a cache miss is experienced. Here, a data probe is used to retrieve the mapping. The following steps are performed.

1. The host with EID `1.0.0.1` wants to send a packet to the host with EID `2.0.0.2`.
2. The packet traverses the AS until it reaches a border router. In this case, it is the ITR with RLOC `11.0.01`
3. This time the ITR does not have a mapping for `2.0.0.2` in its cache. It therefore encapsulates the packet with a new header and sends it to the mapping system. Since the ITR has no knowledge of the destination RLOC it fills the destination EID in the header instead.
4. The mapping system then takes care of transporting the package to the destination RLOC. In this example `13.0.0.2` is used.
5. The ETR decapsulates the packet and forwards the packet to the destination address. It also sends a map reply to back to `11.0.0.1` telling this ITR that the prefix `2.0.0.0/8` can be reached over the two RLOCs `12.0.0.2` and `13.0.0.2`. Additionally a priority (p) and a weight (w) for each RLOC are provided. Here, both RLOCS have the same priority and weight, so that traffic should be split equally among both.

Researchers proposed many other approaches for mapping systems, namely: APT [20], CONS [4], DHT [19], EMACS [5], FRMS [22] and NERD [17]. Table 1 shows which distribution model is used on each case. A brief description of these mapping systems can be found in [21].

4.3 Other Approaches

The Host Identity Protocol (HIP) is a Loc/ID split protocol that adds an additional layer between transport and network layer in the OSI model. IP addresses are kept as locators, but identifiers get a completely new namespace. The so-called Host Identifier (HI) is a cryptographic public key. HIs are usually not used directly. Instead, a Host

doi: 10.2313/NET-2011-07-2_09

Table 1: Distribution Models [19]

Mapping system	Distributions Model
ALT	Hybrid Push/Pull
APT	Push
CONS	Hybrid Push/Pull
DHT	Pull
EMACS	Pull
FRMS	Hybrid Push/Pull
NERD	Push

Identifier Tag (HIT) is used to represent the HI. The HIT is a hash of the HI and has a fixed length of 128 bit, exactly the size of IPv6 addresses. A representation having the size of an IPv4 address also exists, the Local Scope Identifier (LSI). These sizes are used for support of legacy applications. HITs or LSIs replace IP addresses as identifiers in TCP connections. In order to establish a connection a four-way handshake between two hosts, called Initiator and Responder, is performed. HIP is expected to improve mobility and make multihoming easier. Furthermore, connections over HIP are more secure due to the use of public keys as identifiers. Therefore, HIP combines several functionalities that are usually provided by separate protocols [28].

The Shim6 architecture is a Loc/Id approach dealing mostly with multihoming. Both Shim6 and HIP are host-based. The Shim6 architecture introduces a new layer like HIP and two new protocols: Shim6 and the reachability protocol (REAP). Shim6 is the protocol establishing a connection between two hosts, thus creating a Shim6 context. Shim6 also uses a four-way handshake. During that handshake a set of locators for the two identifiers, called upper-layer identifiers (ULID) in Shim6, is exchanged. A different context can be used for each direction. During ongoing connections a host can send an Update Request containing a new set of locators, which is then answered by an Update Acknowledgment. REAP is a protocol in charge of failure detection. A communication usually consists of data traffic in both directions. If there is only traffic in one direction, REAP will send keepalives in the other direction. If at some point there is no incoming traffic at either one of the hosts, a failure is assumed [11].

Six/One Router is an address rewriting approach acting at the router. A network deploying Six/One Router usually consists of so-called PI edge addresses. Additionally the network is assigned a set of transit addresses by each of its providers. One edge address can be mapped on exactly one transit address per provider and one transit address corresponds to one edge address. Six/One Router uses a mapping system. Either one of the mapping systems proposed for LISP can be used for that purpose. Border routers, also called Six/One Routers are responsible for translating edge to transit addresses. Edge addresses in Six/One Router networks are not routable in the DFZ directly, they can only be reached through their transit addresses. Each time a packet crosses the border of an edge network a mapping has to be performed. For incoming packets, the destination address has to be translated into an edge address. For outgoing data the source address has to be modified. Six/One Router is a protocol designed to solve multihoming issues [32].

Another address rewriting approach is the Identifier-Locator Network Protocol (ILNP). It is also a host-based solution. ILNP uses the same packet format as IPv6, but splits source and destination address in half. 64 bits are used as a locator and 64 bits are used as an identifier. In this protocol, the identifiers are encoded MAC-addresses. Locators specify a subnet. ILNP works with DNS, where new kinds of entries need to be created [3].

5. CONCLUSION

The Loc/ID split is a principle expected to overcome scalability issues in the current Internet routing architecture while maintaining efficient support for multihoming, traffic engineering and PI addresses. The performance analysis confirmed that routing tables in the DFZ as well as the BGP update rate can be significantly reduced by deploying a Loc/ID principle. 35 to 40 percent of the prefixes in routing tables can be eliminated by deploying a Loc/Id principle. Updates can be reduced by 50 to 60 percent. Many different proposals for new protocols using a Loc/ID approach exist. This paper described LISP as an example of an implementation mainly focusing on scalability. In the following a few other approaches have been mentioned. These are HIP, Shim6, Six/One Router and ILNP. HIP, Shim6 and ILNP are host-based solutions, which means that they require changes to the host. Six/One Router and LISP are router-based protocols and basically require no changes to hosts. While LISP is a protocol mostly focusing on scalability issues, HIP for example addresses secure mobility. Thus, the Loc/Id split can contribute to solving different issues. LISP and some of the other approaches require an additional mapping system to map identifiers to locators. LISP+ALT has been discussed in order to give such an example. In general, mapping systems should minimize the product of update rate and size of the mapping system ($State \times Rate$). Since the number of hosts already is high and will grow further in the future, the update rate in the mapping system should be kept low. Performance in mapping systems has been discussed in several papers, but still requires further investigation. This should be done to show that mapping systems are really efficient and are not only shifting scalability problems from the routing architecture to mapping systems. The new scalable routing architecture relies on a mapping system. If that mapping system does not scale no progress will be made by introducing it.

6. REFERENCES

[1] ITU Statistics. `http://www.itu.int/ITU-D/ict/statistics/`, Mar. 2011 (accessed March 28, 2011).

[2] Y. Afek, A. Bremler-Barr, and S. Schwarz. Improved BGP Convergence via Ghost Flushing. *IEEE Journal on Selected Areas in Communications*, 22(10):1933–1948, 2004.

[3] R. Atkinson. An Overview of the Identifier-Locator Network Protocol (ILNP). Research Note RN/05/26, University College London, Sept. 2005.

[4] S. Brim, N. Chiappa, D. Farinacci, V. Fuller, D. Lewis, and D. Meyer. LISP-CONS: A Content distribution Overlay Network Service for LISP `http://tools.ietf.org/html/draft-meyer-lisp-cons-04`, IETF, Apr. 2008. Work in

doi: 10.2313/NET-2011-07-2_09

progress.

[5] S. Brim, D. Farinacci, D. Meyer, and J. Curran. EID Mappings Multicast Across Cooperating Systems for LISP. http://tools.ietf.org/html/draft-curran-lisp-emacs-00, IETF, Nov. 2007. Work in progress.

[6] L. Burness, P. Eardley, S. Jiang, and X. Xu. A pragmatic comparison of locator ID split solutions for routing system scalability. In *Third International Conference on Communications and Networking in China, 2008. ChinaCom 2008.*, pages 1024–1028, 2008.

[7] J. Chandrashekar, Z. Duan, Z.-L. Zhang, and J. Krasky. Limiting Path Exploration in BGP. In *INFOCOM 2005*, volume 4, pages 2337–2348, 2005.

[8] P. Dong, H. Wang, Y. Qin, H. Zhang, and S.-Y. Kuo. Evaluation of Scalable Routing Architecture Based on Locator/Identifier Separation. In *GLOBECOM Workshops, 2009 IEEE*, pages 1–6, Dec. 2009.

[9] D. Farinacci, V. Fuller, D. Meyer, and D. Lewis. Locator/ID Separation Protocol (LISP). http://www.ietf.org/id/draft-ietf-lisp-11.txt, IETF, Mar. 2011. Work in progress.

[10] V. Fuller, D. Farinacci, D. Meyer, and D. Lewis. LISP Alternative Topology (LISP+ALT). http://tools.ietf.org/html/draft-ietf-lisp-alt-06, IETF, Mar. 2011. Work in progress.

[11] A. Garcia-Martinez, M. Bagnulo, and I. Van Beijnum. The Shim6 Architecture for IPv6 Multihoming. *IEEE Communications Magazine*, 48(9):152–157, 2010.

[12] M. Grayson, K. Shatzkamer, and K. Wierenga. *Building the Mobile Internet*. Cisco Press, Feb. 2011.

[13] W. Herrin. Tunneling Route Reduction Protocol (TRRP). http://bill.herrin.us/network/trrp.html, 2008 (accessed March 31, 2011).

[14] G. Houston. The BGP Routing Table. http://bgp.potaroo.net/, Mar. 2011 (accessed March 25, 2011).

[15] L. Iannone and O. Bonaventure. On the Cost of Caching Locator/ID Mappings. In *Proceedings of the 2007 ACM CoNEXT conference*, pages 7:1–7:12. ACM, 2007.

[16] L. Iannone, D. Saucez, and O. Bonaventure. Implementing the Locator/ID Separation Protocol: Design and experience. *Computer Networks*, 55(4):948–958, Mar. 2011.

[17] E. Lear. NERD: A Not-so-novel EID to RLOC Database. http://tools.ietf.org/html/draft-lear-lisp-nerd-08, IETF, Mar. 2010. Work in progress.

[18] T. Li. Design Goals for Scalable Internet Routing. http://www.ietf.org/id/draft-irtf-rrg-design-goals-06.txt, IETF, Jan. 2011. Work in progress.

[19] L. Mathy and L. Iannone. LISP-DHT: Towards a DHT to map Identifiers onto Locators. In *Proceedings of the 2008 ACM CoNEXT Conference*, CoNEXT '08, pages 61:1–61:6, 2008.

[20] M. Meisel, D. Massey, L. Wang, B. Zhang, and L. Zhang. APT: A Practical Transit Mapping Service. http://tools.ietf.org/html/draft-jen-apt-01, IETF, Nov. 2007. Work in progress.

[21] M. Menth, M. Hartmann, and M. Hoefling. Mapping Systems for Loc/ID Split Internet Routing. Technical Report 472, University of Würzburg, May 2010.

[22] M. Menth, M. Hartmann, and M. Hofling. FIRMS: A Mapping System for Future Internet Routing. *IEEE Journal on Selected Areas in Communications*, 28(8):1326–1331, 2010.

[23] M. Menth, M. Hartmann, P. Tran-Gia, and D. Klein. Future Internet Routing: Motivation and Design Issues. *it - Information Technology*, 50(6):358–375, 2008.

[24] M. Menth, D. Klein, and M. Hartmann. Improvements to LISP Mobile Node. In *ITC 22nd International Teletraffic Congress (ITC22), Amsterdam 2010*, pages 1–8, 2010.

[25] D. Meyer. Update on Routing and Addressing at IETF 69. *IETF Journal*, 3(2):21–24, Oct. 2007.

[26] D. Meyer. The Locator Identifier Separation Protocol (LISP). *The Internet Protocol Journal*, 11(1):23–36, 2008.

[27] D. Meyer, L. Zhang, and K. Fall. Report from the IAB Workshop on Routing and Addressing. RFC 4984, http://www.ietf.org/rfc/rfc4984.txt, Sept. 2007.

[28] P. Nikander, A. Gurtov, and T. Henderson. Host Identity Protocol (HIP): Connectivity, Mobility, Multi-Homing, Security, and Privacy over IPv4 and IPv6 networks. *Communications Surveys Tutorials, IEEE*, 12(2):186–204, 2010.

[29] D. Oran. OSI IS-IS Intra-domain Routing Protocol. RFC 1142, http://www.ietf.org/rfc/rfc1142.txt, Feb. 1990.

[30] J. Oran. OSPF Version 2. RFC 2328, http://www.ietf.org/rfc/rfc2328.txt, Apr. 1998.

[31] W. Sun, Z. Mao, and K. Shin. Differentiated BGP update processing for improved routing convergence. In *Proceedings of the 14th IEEE International Conference on Network Protocols, 2006. ICNP '06.*, pages 280–289, 2006.

[32] C. Vogt. Six/One Router: A Scalable and Backwards Compatible Solution for Provider-Independent Addressing. In *Proceedings of the 3rd international workshop on Mobility in the evolving internet architecture*, MobiArch '08, pages 13–18, 2008.

[33] H. Zhang, M. Chen, and Y. Zhu. Evaluating the performance on Id/Loc mapping. In *IEEE GLOBECOM 2008*, pages 1–5, 2008.

[34] X. Zhang, P. Francis, J. Wang, and K. Yoshida. Scaling IP routing with the Core Router-integrated overlay. In *Proceedings of the 2006 14th IEEE International Conference on Network Protocols, 2006. ICNP '06.*, pages 147–156, 2006.

doi: 10.2313/NET-2011-07-2_09

How Secure are Secure Interdomain Routing Protocols?

Anatol Dammer
Advisor: Dr. Nils Kammenhuber
Seminar Future Internet SS2010
Chair for Network Architectures and Services
Fakultät für Informatik, Technische Universität München
Email: anatol.dammer@mytum.de

ABSTRACT

Ever since the 1990s, the de facto standard for Internet inter-AS[1] routing has been BGP, the Border Gateway Protocol. Security issues caused or abetted by BGP, some of which have been known for considerable time, have become increasingly apparent. Long-running efforts of making BGP and inter-AS routing more secure have produced a number of proposals, none of which have managed to gain traction. This is at least partly due to the fact that even the most popular and well-regarded proposals fail to prevent strategic attacks. We provide an overview of several popular proposals and how they address, or fail to address, a range of attacks on inter-AS routing.

1. INTRODUCTION

In recent years, several high-profile attacks and outages caused by exploitation of BGP's flaws or simple misconfiguration have risen awareness of actually long-known deficiencies of inter-AS routing. In 1997, a misconfigured border router of one AS led to major Internet-wide disruptions lasting up to a few hours [3], in 2008 Youtube.com was unreachable for several hours for most of the Internet, due to misconfiguration at Pakistan Telecom [12, 14], and in 2010 IDC China briefly announced 40,000 prefixes owned by other entities [10], attracting traffic for those destinations. In 2002, 200–1200 routing prefixes per day were found to suffer from misconfiguration, with about 15 prefix hijacks occurring per day [11]. BGP has been the de facto standard for inter-AS routing ever since the 1990's, and the protocol has not changed fundamentally since then – this alone should raise a few flags, considering the explosive growth of the Internet and its increasingly complex dynamics. Also, it is clear that if simple misconfigurations can have such considerable impact on the Internet, the potential for deliberate, strategic attacks should be quite profound.

Introductions on BGP usually emphasize the fact that BGP relies on an optimistic approach to routing, basically trusting routing information received by peers blindly. As will become apparent, this is not the whole truth: while BGP by itself is certainly not a very secure protocol, attacks on inter-AS routing can also hugely benefit from other, partly non-technical, aspects like business relationships between network operators. The quantitative data by Goldberg et al. [5] shows how relatively simple attack strategies can easily diminish the benefits promised by proposals such as S-BGP, which at first might appear to provide very substantial gains in security. On the other hand, they also show how comparatively simple measures could actually prevent a large proportion of attacks.

After an introduction to inter-AS routing and BGP, this paper succinctly describes and then compares four approaches to improve several security aspects of inter-domain routing. Main source for this information is the paper by Goldberg et al. who ran simulations of various inter-AS-level attacks on an internetwork model based on Internet AS-graph data sets, and published quantitative information on how well those four major security proposals fared.

[1]Autonomous system, a collection of networks administered by one entity, e.g., a large corporation

2. INTER-AS ROUTING AND BGP

As its name suggests, the Internet is a network of networks. Due to the very large number of destinations reachable in the Internet, routing tables can not sensibly include all single destinations. This motivated a routing scheme where destinations are aggregated into *prefixes*. Also, since organizations often want to have sole authority over routing in their own networks, an organization's networks can be combined into one or more so-called *Autonomous Systems (AS)*, each carrying a unique number (*ASN*) assigned by IANA[2]. For example, large corporations and Internet service providers operate their own AS(es).

To establish connectivity to the Internet, an AS operator employs so-called *border* or *gateway* routers that exchange inter-AS routing information with other AS border routers, route traffic between the inner part of the AS and the Internet, and may also act as intermediaries for traffic between two other ASes. Border routers establish "peer" relationships with other border routers via BGP, and can then exchange prefix routing information, which may be called sending route or path "announcements", and make forwarding decisions based on this information. For example, a border router can *originate* prefixes, which means announcing a network prefix included in its own AS, or *propagate* routing information learned from other routers, offering the own AS as an intermediary willing to proxy traffic along such a path.

BGP is a path vector protocol; the routing information it disseminates includes the full path, specified by ASNs, to reach a destination. For this, a router *prepends* its own ASN to a path attribute in the BGP path announcement message[3].

[2]Internet Assigned Numbers Authority, `http://www.iana.org/`

[3]This is a slight simplification; the PATH attribute in BGP UPDATE messages can be more complex – for our purposes, this is irrelevant

doi: 10.2313/NET-2011-07-2_10

The case where an AS acts as an intermediary for traffic between two other ASes is a good starting point for introducing a very important aspect of inter-AS routing in the current Internet: business relationships. While intra-AS routing is mainly concerned with purely technical aspects such as finding and distributing shortest paths, inter-AS routing involves different, possibly competing, organizations and is thus heavily influenced by political and business decisions. A protocol for inter-AS routing has to offer support for enforcing policies based on such decisions. BGP offers support for *import* and *export* policies, which respectively control which routes from BGP peers are entered into a BGP router's local route database and which routes are announced to BGP peers.

To provide an example: a network operator might like to only relay traffic between two parties if at least one of the parties pays for this service, usually by data volume. In addition to this *customer–provider* relationship, organizations such as major telecommunication companies also enter into so-called *peering* agreements: two organizations see themselves as peers in that they both benefit about equally from exchanging traffic, and are thus willing to mutually waive traffic fees. These relations allow for a classification of organizations into *Tiers*. "Tier 1"-providers have only customers and peers; because they do not have a "default route" to a provider, they constitute what is called the *Default-Free Zone* (DFZ) and are entirely reliant on peering agreements and customer contracts for connectivity. "Tier 2" providers, the most common providers in the Internet, have peering agreements but are also customers to Tier 1 providers. Tier 3 providers usually entirely rely on higher-tier providers, etc. Another concept that will be relevant later on are *stubs*, which are ASes that are only connected to one other AS and do not have any customers.

3. ROUTE SELECTION AND POLICIES

To understand the attacks that will be discussed later on, it is necessary to understand the criteria BGP uses to select routes and make forwarding decisions.

3.1 Route selection

Basically, a BGP router takes all routes it receives from its neighboring BGP routers, performs basic checks (the most relevant for us being routing loop detection), then runs all remaining routes through a decision process that decides if the routes are new or better than existing routes. Loop detection is based on the route path – if the own ASN is included in the path, the route information is discarded. Otherwise, a degree of preference for each route is calculated based on local preference, shortest AS path and tie-breaking rules, in that order. Local preference usually reflects policy decisions. Note that the path length comes second – a strong reminder of how important policy decisions are, and an aspect that will become important for attack strategies later on. After calculating the degree of preference, the best route for each destination is chosen and installed in a table that serves as input to the algorithms that make forwarding and route export decisions.

3.2 Policy scenarios

The aforementioned business relationships inherent to inter-AS routing have strong influence on which routes are exported by a router. ASes likely select and export routes

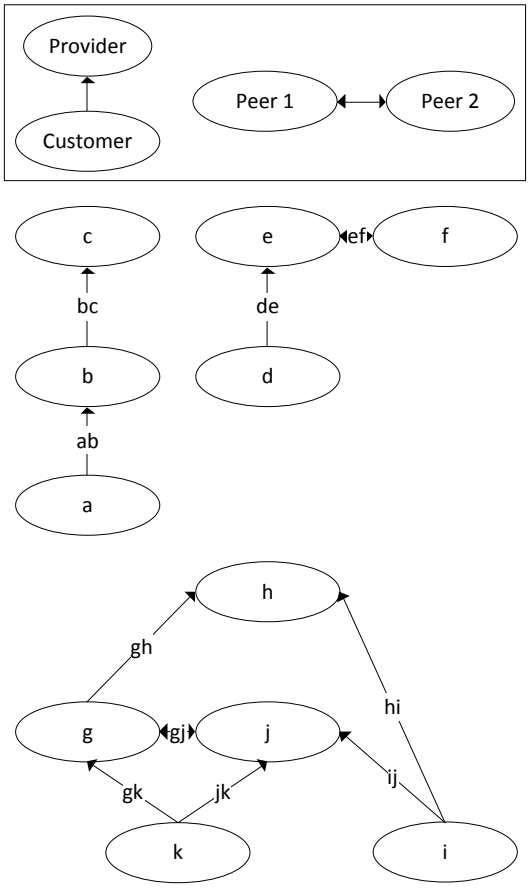


Figure 1: Routing policy examples

such that their own financial gain is maximized and financial loss is avoided unless absolutely necessary, e.g., to preserve connectivity. A few basic cases are illustrated in Figure 1. Here, AS b would export the route $a \to b$[4] to c to make its customer's AS available to the Internet (assuming c provides further connectivity), paying to its provider c but also getting paid by customer a. AS e would export the route $d \to e$ to its peering partner f – while e loses no money by relaying traffic to and from d over $e \to f$, it gains money from its customer d in the process. Likewise, f would not export a route to d, as doing so would mean using up capacities without gaining money from forwarding traffic over $e \to f$. In the last example, h will export the route $h \to i$ to g just like j will export $i \to j$ to g. AS g will then choose the peering link $g \to j$ to reach i, as this means avoiding costs for using the so-called transit or provider link $g \to h$. For some AS x, a *customer link* is a link to a customer of x, like $h \to i$ is a customer link to h.

[4]Note that route names were simply chosen alphabetically – in a BGP message, ASes prepend their ASN to the path, so *ba* would be a more "realistic" name for *ab*

doi: 10.2313/NET-2011-07-2_10

Figure 1 shows ASes in top-to-bottom hierarchical order with providers above their customers. This allows for easy illustration of the concept of *valley-free routing*, which directly follows from the business aspects of inter-AS routing. Simply put, paths are usually established such that packets never cross "valleys" in this hierarchical graph, such as the one created by the stub k. More precisely, packet flow conforms to the following scheme:

1. Travel upstream, i.e., towards a provider, across zero or more links
2. Traverse at most one peering link
3. Travel downstream, i.e., towards a customer, across zero or more links

The rationale for valley-free routing quickly becomes apparent if one considers each step and verifies that routes not conforming to the scheme would create financial loss for at least one AS.
In the following, we assume that every "honest", that is, non-malicious, AS follows these policies.

4. SECURITY PROPOSALS

Goldberg et al. mainly evaluate four different security protocols and plain BGP. While there are more specific proposals, the protocols they chose cover many proposals in terms of the security guarantees they provide[5]. Their order is strict from weakest to strongest security guarantees: any attack that is possible against a stronger protocol is also possible against all weaker protocols. An important factor to consider for all protocols is the substantial challenge of introducing a new protocol into the world of inter-AS routing, especially if computationally intensive cryptography would suddenly have to be performed by routers.

4.1 Origin authentication

Aiello, Ioannidis and McDaniel address the problem of address ownership [1]. In plain BGP, any AS can claim ownership of any prefix. This obviously provides ample opportunity for prefix hijacking attacks[6], and anomalies such as the one caused by AS 7007 in 1997 [3]. They state that origin authentication is a necessary but insufficient precondition for any inter-AS routing security infrastructure. Their fundamental work describes approaches to building a system that, from a database, can verify if a prefix announced by an AS has been assigned to that AS by an organization which in turn can provide a chain of address delegation up to IANA, the root authority for address assignment. In experiments, they found evidence that their approach should be deployable in terms of resource cost.

4.2 soBGP

On top of origin authentication, Secure Origin BGP (soBGP), described by Russ White et al. [15], proves validity of a path originated by an AS. Validity in this case means a path that physically exists in the Internet: The route path consists of real, interconnected ASes. Validation is provided by having routers disseminate signed local topology information, i.e., routers announce their peers to other routers, in effect establishing a global topology graph that every router knows. An attacker might still announce some path that is not actually available because it violates one of the standard policies of intra-AS routing described in section 3.2. While running attacks in an internetwork secured with soBGP requires knowledge of physically existing paths, such information can be obtained without too much effort – for example, from the very database that soBGP requires and maintains, as Goldberg et al. note. soBGP requires a PKI for origin authentication and path validation. Adjustments to BGP, such as a specific message type for exchange of security information, are suggested but, according to the authors, not necessary [16].

4.3 S-BGP

S-BGP, proposed by Kent et al. [9], provides path verification, meaning that an AS a can only announce a path $a \to b \to c$ if b actually announced $b \to c$ to a. S-BGP requires a PKI[7] that supports certificates for prefix ownership and granting authorization to ASes for announcing specific paths to specific prefixes. Simply put, path verification is achieved by a chain of signatures in route advertisements. This, combined with origin authentication provided by the PKI, seems to provide considerable security as a can only announce actually available paths that end with the rightful owner of a prefix. Besides a few other comparatively minor issues, an interesting aspect is that S-BGP does not ensure correct and honest application of policies by BGP peers. For example, nothing stops an attacker from announcing one path but actually forwarding incoming traffic that is meant for that path on an entirely different path.
BGP usually transmits messages in plaintext over TCP. S-BGP addresses this important security issue by using IPsec for all BGP messages. This ensures integrity, sender identity and even protection against message replay and DoS attacks which can be a significant problem with TCP.
The substantial amount of cryptography entailed by an Internet-wide deployment of S-BGP might seem challenging. One requirement for S-BGP was deployability and scalability; when the paper [9] was published in 2000, the authors concluded that deployment was feasible.

4.4 Data Plane Verification

A still relatively new research effort with groundwork by Wong et al. [17, 4] concerns itself with the actual path that data takes when it is forwarded by BGP routers. As mentioned, a router might advertise one path, but forward data on a different one. An AS might advertise an attractive path which would actually incur financial loss for the advertiser, and then use a cheaper path to forward the attracted traffic. S-BGP only protects the *control plane*, where routing information is exchanged. Goldberg et al. propose a verification scheme that works with shared secrets between routers along a route path. Basically, data packets are used as probes: a router can tag data packets with secrets shared with a router along the prospective route path. Only the expected

[5] A more comprehensive description can be found in [4]
[6] An attacker hijacks a prefix by directing traffic meant for that prefix to himself
[7] Public Key Infrastructure. For S-BGP, one PKI with two certification hierarchies is necesssary; the original paper thus describes two PKIs.

doi: 10.2313/NET-2011-07-2_10

recipient can return the correct "answer" to the tags and thus confirm that the packet reached the correct router. With an extension, entire paths can be verified.

4.5 Defensive Filtering

Defensive filtering is not actually a novel security protocol but more of a best practice that can also be used on top of other security proposals. It describes filtering of route announcements that, according to predefined rules or heuristics, are estimated to be invalid or malicious. Defensive Filtering is particularly interesting in the case of stubs. As mentioned before, stubs are ASes without any customers. This means that they can only legitimately announce prefixes they themselves own – according to the assumed BGP policies from section 3.2, they can not sensibly serve as transit networks for other prefixes. Thus, providers of stub ASes should keep a list of prefixes owned by their connected stubs and discard any announcements for other prefixes, thereby greatly diminishing or even eliminating the potential damage attacks or misconfiguration by a stub could cause to other networks.

5. METHODOLOGY

Before we turn to the quantitative analysis of the effects various attacks have on the aforementioned security proposals, a short introduction of assumptions and methodology is necessary.

5.1 Threat model, data set, quantification

Goldberg et al. chose traffic attraction and traffic interception attacks for their analysis. While other attacks surely are relevant in today's Internet, it will become apparent that resilience to those two attacks is a critical aspect of inter-AS routing security proposals and serves well as a test case. Traffic attraction denotes the scenario where an AS tries to attract traffic destined for a prefix it does not actually own, usually trying to maximize the number of ASes that route through the attacker. This can be motivated by a number of reasons: performing a DoS attack on the prefix by dropping the attracted traffic (routing blackhole), modifying or examining traffic (interception) and, again, non-technical goals such as increasing revenue or causing financial damage by "forcing" traffic through paths the affected parties would rather avoid. Interception requires, on top of attraction, that intercepted data eventually reaches its correct destination.
Goldberg et al. ran their attack simulations on internetwork models based on data from CAIDA[8], who offer an inter-AS graph from inferred AS business relationships and available BGP peering data. All attacks they ran could have been performed just as well on the corresponding ASes in the real Internet, provided the CAIDA model was accurate enough in those cases. Success of attacks was measured by running attacks on multiple, random pairs of attacking ASes and victim ASs, measuring the fraction of ASes whose traffic the attacker managed to attract and computing the distributions of these fractions.
The authors tried to assume the worst case, attacking each protocol with the worst possible attack, i.e., the optimal strategy for the attacker.

[8]Cooperative Association for Internet Data Analysis, `http://www.caida.org/home/`

5.2 Underlying assumptions, caveats

Goldberg et al. made several choices that understate the effect of their attacks while at the same time making reasonable assumptions on aspects that might benefit attacks, such as assuming that ASes announce all paths except those "forbidden" by the policies stated in section 3.2. They also assume a static AS graph, which is certainly not true for the real Internet, but probably justified by their argument that AS graph changes occur on a much longer timescale than BGP execution.
A significant caveat is their assumption that no monitoring services are used for defense against attacks. Such services, e.g. offered by Renesys and RIPE (RIS), monitor inter-AS routing with a large number of probes placed at various points in the Internet and make BGP peering data available publicly or to their customers[9]. Users of such services can spot suspicious local changes in their routing information or use the data to search for larger anomalies in inter-AS routing. Also, for some attacks, Goldberg et al. grant some knowledge of global routing configuration to the attacker, justifying this with the assumption that the attacker acts strategically and with preparation. Important is also the fact that only single attacking ASes were considered – colluding ASes have interesting attack options as well, such as tunneling route announcements between each other that then offer shorter, bogus, paths [7]. S-BGP can not prevent this attack if the routers sign each other's paths.

6. ATTRACTION ATTACKS

The strategy for the first set of attacks, traffic attraction attacks, is as follows: announce the shortest possible paths that are allowed by the respective security protocol to all BGP peers to attract traffic, disregarding the routing policies we are assuming for honest ASes. That means, for plain BGP the attacker would announce the victim prefix as his own, *originating* it. In case of origin authentication, the attacker will announce a *direct link to the owner* of the prefix and soBGP requires at least a *physically existing path*. For S-BGP, the attacker has to choose the *shortest path to the victim that is actually available* to him. As Goldberg et al. point out for the case of S-BGP, if the attacker decides to actually forward traffic on the path he could already announce without S-BGP raising an alarm, the attack is not detected by data plane verification either.
Figure 2 shows the probability an attacker can attract at least 10% of ASes in the internetwork with his announcements. See Figure 3 for a more detailed plot, showing the cumulative probability for some fraction of ASes routing through the attacker. Note the high probabilities of success for this relatively unsophisticated attack strategy, especially considering that these are lower bounds – Goldberg et al. even prove that finding the optimal attack strategy is NP-hard.

6.1 Findings

Goldberg et al. draw several conclusions from the results above. This paper concentrates on two significant and simple findings; for a full list with several intriguing findings see the full version of the source paper [6].

[9]Customers being regular business customers in this case, not traffic customers

doi: 10.2313/NET-2011-07-2_10

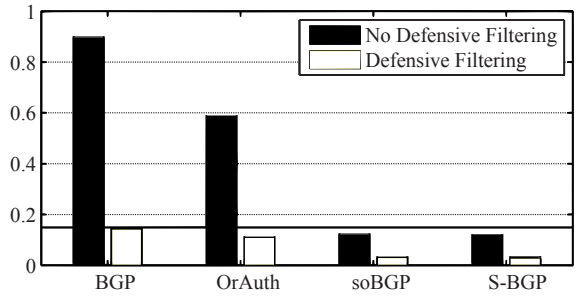


Figure 2: Lower bounds on the probability of attracting at least 10% of ASes in the internetwork [5]

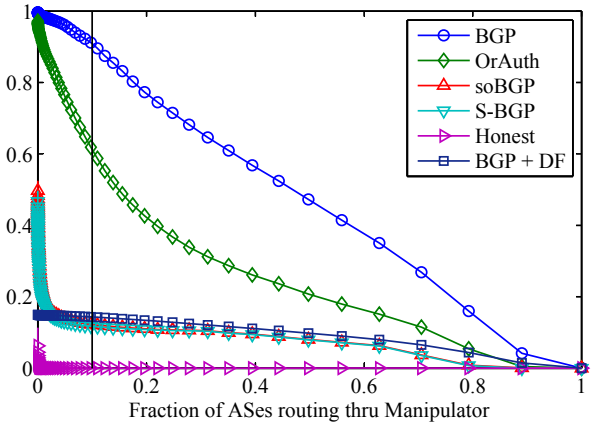


Figure 3: CCDF for the "Shortest-Path Export-All" attack strategy [5]

6.1.1 *Defensive filtering*

The first result that is quite striking and one of the most significant findings of the paper is apparent in Figure 2. The plot shows the large influence defensive filtering of stub announcements has in preventing attacks. Defensive filtering combined with plain BGP works almost as well as S-BGP alone – without requiring any changes to routing protocols, PKIs or other computationally intensive cryptography. This result will reappear when we discuss other attack strategies.

6.1.2 *Export policies*

The only minor difference between soBGP and S-BGP serves as a hint to another important finding. While S-BGP does restrict possible paths the attacker can announce, and thus forces the attacker to announce longer paths compared to, e.g., soBGP, this does not make the attack much less efficient. Goldberg et al. show that this is just a side effect of a very important point – path lengths are often less relevant for a route's attractiveness than export policies. This is easily understood by considering the case where an attacker ignores his policy of not incurring financial loss and announces provider paths to his provider. A provider will likely, according to the BGP route selection process and policies, prefer a customer route before even considering path lengths!
Because route announcements are not binding, with the exception of data plane verification, an attacker can use the announcement of a path that is attractive to other ASs but costly for the attacker, but then forward attracted traffic on a cheap or free path, if at all.

6.1.3 *Tier 2 attackers*

A somewhat surprising result is that the most efficient attackers for traffic attraction are ASes located in Tier 2. While Tier 1 is often still viewed as the "backbone" or "core" of the Internet[10], with short path lengths to most destinations, path length is trumped by policy considerations once again. Tier 1 networks are always providers or peers, never customers. This makes them less attractive for all lower tiers, as those would usually have to pay for forwarding traffic to a Tier 1 or occupy peering capacities. Tier 2 networks provide an ideal combination of good connectivity and attractive customer links. For the same reason, Tier 1 ASes are more vulnerable to traffic attraction attacks than Tier 2's – ASes that want to reach a Tier 1 can only be customers or peers of their destination and as such are more likely to accept alternative paths introduced by an attacker which are cheaper or even earn them money, in case of customer paths.

7. INTERCEPTION ATTACKS

Like attraction attacks, interception attacks aim at attracting as much traffic as possible, but also at preserving a path to the victim on which the intercepted traffic is ultimately delivered. The attacker typically wants to snoop traffic or modify it, ideally without the victim noticing anything out of the ordinary. This means that the attacker must not cause routing blackholes, which happen when the attacker attracts traffic meant for his victim but has no available route to the victim – typically, because he attracts the traffic from his providers to his victim as well. Interestingly, Goldberg et al. provide proof that in many scenarios, blackholes are impossible: see Table 1.
An attacker who wants to preserve a customer path to a victim can announce any path to any neighbor type, while there are counterexamples that show that for example peer paths can not always be preserved if an attacker indiscriminately announces paths to providers. This makes attackers in Tier 1 ideal interceptors – they do not have provider paths, and thus do not have to worry as much about introducing routing blackholes as lower-Tier-ASes.

	May announce to		
Preserve path of type	Customers	Peers	Providers
Customer	✓	✓	✓
Peer	✓	✓	×
Provider	✓	×	×

Table 1: Blackhole prevention [5]

7.1 Three different strategies

The first strategy for interception is, like in section 6, shortest path export all – for each security protocol, announce the shortest possible paths to all neighboring BGP routers. Attacks with this strategy on less secure systems such as BGP are more likely to cause blackholes compared to, e.g., S-BGP

[10] A notion that has been outdated for some time now, actually, since before the introduction of BGP

doi: 10.2313/NET-2011-07-2_10

because S-BGP forces the attacker to announce an available path – which can not be a blackhole. This implies an easy way to circumvent the problem of blackholes: instead of announcing shortest paths, announce shortest available paths not only in case of S-BGP. While this prevents blackholes, this strategy appears to be less-than-ideal in internetworks without S-BGP. A hybrid strategy of using shortest path export all per default, checking if a path to the victim is still available, and switching to shortest available path export all if necessary seems like a sound strategy.

7.2 Results

Results for interception attacks on plain BGP are plotted in Figure 4. Goldberg et al. provide no results for these interception attacks on any of the security proposals. For plain BGP, the attacks are obviously quite successful. Results are likely to be similar or identical for the security proposals, as shortest available path export all will circumvent all proposals up to and including S-BGP.

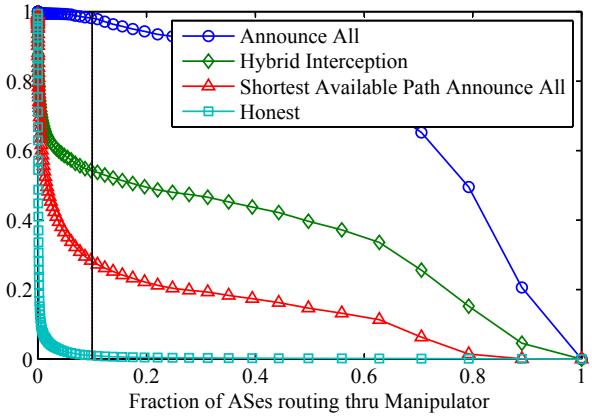


Figure 4: Interception attacks on (plain) BGP [5]

8. COUNTERINTUITIVE ATTACKS

Attacks on inter-AS routing are not always obvious, and understanding attacks is made more complicated by the heavy influence of non-technical considerations. Goldberg et al. found three interesting AS subgraphs in their data set for which they demonstrated very counterintuitive attacks that were astonishingly successful in their simulations; demonstrating that shortest path export all is not optimal for attackers. Figures used in this section show the amount of providers etc. for some ASes; these are in plain text next to the AS in the graph. Colored numbers in triangles state the number of customer ASes which route through the attacker via the AS the triangle's arrow points to.

8.1 Announcing longer paths

For this example, we assume that soBGP, S-BGP or data plane verification is implemented in the internetwork. Figure 5 shows the AS subgraph this attack will be run on. On top, the green arrows indicate a scenario where the attacker m intercepts traffic to v from $a2$ and $a3$ by using the shortest path export all strategy by announcing the path $m \rightarrow a1 \rightarrow v \rightarrow prefix$. Including $a3$'s customers, this attack manages to attract 2546 ASes. The attacker can do even better, though. If m announces $m \rightarrow a2 \rightarrow a3 \rightarrow v \rightarrow prefix$, this longer path will actually be preferred by m's provider $a1$ over its own *direct peering link* to v! Because in this specific case $a1$ has considerably more customers than $a2$, the attacker increases attracted traffic – *threefold*, as shown in the lower part of Figure 5! Note that because $p1$ and $p2$ are now using customer links to reach v instead of their peering links, they are in principle willing to announce this path *to anyone*. To avoid this attack scenario, one would probably have to implement checks that ASes follow standard path export policy – m is not announcing false paths, claiming ownership of prefixes it does not own or announcing one path but forwarding on another, thereby circumventing all security proposals up to and including data plane verification. The sole exception are stub attackers when defensive filtering is in place.

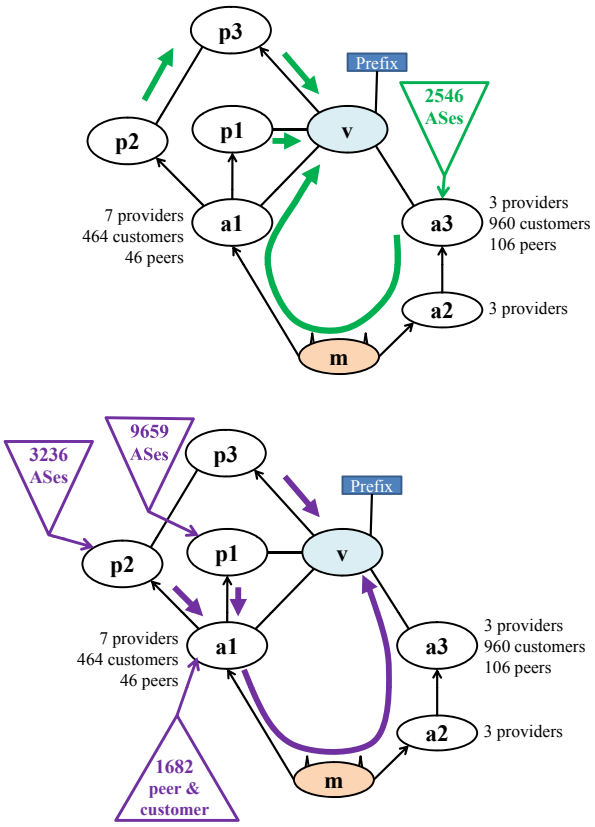


Figure 5: Announcing a longer path [5]

8.2 Exporting less

Figure 6 again shows shortest path export all in green: m announces $m \rightarrow v \rightarrow prefix$ to Tier 2 provider $T2$ and both $T1a$ and $T1b$ choose their customer link to $T2$ for reaching v: $T2 \rightarrow m \rightarrow v \rightarrow prefix$. If m stops this announcement, $T2$ has to use the peering link $T1c$ and, following policy guidelines, stops propagating his route to v to his providers $T1a$ and $T1b$. $T1a$ and $T1b$ now have to use their peering links with m to reach v. So far, nothing seems to have been accomplished by v; actually, traffic form $T2$ is now no longer attracted. What makes this attack superior in this case is the fact that the Tier 1 networks now announce shorter paths to v to their customers, attracting more traffic. For this specific

doi: 10.2313/NET-2011-07-2_10

case, traffic attraction could be increased *fourfold*. So, by *forcing* Tier 1 ASs, which have a large number of customers, to use shorter paths, the attacker massively increases the attracted traffic. This attack, just like the previous one, requires no overtly malicious activity – only strategic route export policies. It works in presence of all security protocols discussed here.

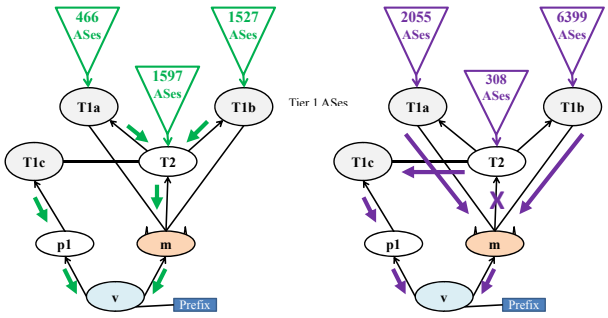


Figure 6: Exporting less [5]

8.3 False loops

The last attack described here aims at creating a black-hole. On the left in Figure 7, the attacker chooses the very aggressive attack strategy of originating the prefix that rightfully belongs to v. $T1a$ will choose the route $a3 \rightarrow a2 \rightarrow a1 \rightarrow m \rightarrow prefix$ because it is a customer path. In this dataset, Goldberg et al. showed that 32010 ASes could be attracted this way, which is the majority of ASes in that dataset. Now the attacker aims at something similar to the strategy in section 8.2: shortening the path of which $T1a$ thinks that it leads to v through m. In this AS subgraph, m can achieve this by announcing $m \rightarrow a2 \rightarrow prefix$ to $a1$, which will forward its customer's route to $T1a$ and $a2$. At $a2$, BGP loop detection will reject this path as invalid. $T1a$ thus loses its path over $a2$ and starts using the manipulated peering path $a1 \rightarrow m \rightarrow a2 \rightarrow prefix$, drawing more traffic into the trap set up by m; 32370 ASes in this case. This slight increase is due to the increased attractiveness of the path, which is now shorter[11]. S-BGP catches this attack because it recognizes the illegal paths announced by m.

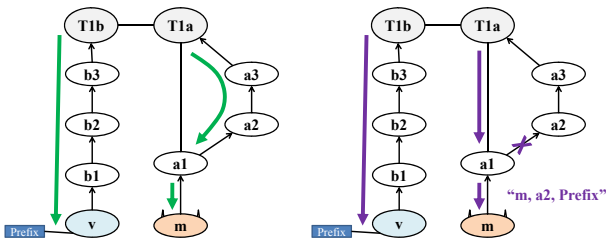


Figure 7: False loops [5]

[11]Actually, the situation is slightly more complicated, see [6] for a detailed description. The reason for the increased effectiveness of the attack is the same.

9. RELATED WORK

The security proposal SPV [7] was not considered by Goldberg et al.; except for origin authentication and use of IPSec, it provides similar guarantees as S-BGP. However, Butler et al. find its reliance on probabilistic arguments in some cases too problematic and refer to Raghavan et al. [13], who found that a majority of ASes can forge routes in SPV with high probability.

Another surprisingly multifaceted, but not very high-profile, attack on inter-AS routing that was not discussed by Goldberg et al. is link cutting [2].

Some of the proposals described here are already under way, an example being a PKI for origin authentication [8].

10. CONCLUSION

This paper described quantitative comparisons by Goldberg et al. of four inter-AS routing security proposals, which show that even quite sophisticated and seemingly secure proposals can still be circumvented by surprisingly easy attacks. Especially two findings are important: first, traffic attraction attacks *can* be mitigated. For example, defensive filtering alone would probably significantly reduce the number of possible attraction attacks, see Figure 2. Second, strategic configuration of export policies by an attacker can easily circumvent even the most sophisticated proposals – which only makes the Internet-wide implementation of defensive filtering more important for improving inter-AS routing security.

Goldberg et al. used mostly convincing methods for their analysis. While they omitted some interesting attack and defense strategies, only focused on traffic attraction and interception and had to concede that the specific subgraphs used for their counterintuitive, but very effective, attacks were hard to find, their general findings seem sound. On the non-technical side, issues such as single points of trusts in PKIs needed for example for S-BGP were not addressed.

In conclusion, inter-AS routing remains remarkably insecure. While work is under way to improve the situation, currently, effective tools like defensive filtering are not universally used due to the fact that providers do not directly benefit from its implementation *on their own network*. Sophisticated security schemes in development might require major overhaul of Internet routing architecture and significantly increase resource use while still failing to address relatively simple attacks. Unfortunately, it seems that apart from using route monitoring services and implementing best practices such as defensive filtering, there is not much an AS operator can do to improve BGP security today – except to wait for the rest of the Internet to follow suit with implementing best practices.

doi: 10.2313/NET-2011-07-2_10

11. REFERENCES

[1] W. Aiello, J. Ioannidis, and P. McDaniel. Origin Authentication in Interdomain Routing. In *Proceedings of the 10th ACM conference on Computer and Communications Security*, CCS '03, pages 165–178, New York, NY, USA, 2003. ACM.

[2] S. M. Bellovin and E. R. Gansner. Using Link Cuts to Attack Internet Routing. Technical report, ATT Research, 2003.

[3] V. J. Bono. 7007 Explanation and Apology. `http://www.merit.edu/mail.archives/nanog/1997-04/msg00444.html`.

[4] K. Butler, T. R. Farley, P. McDaniel, and J. Rexford. A Survey of BGP Security Issues and Solutions. *Proceedings of the IEEE*, 98(1):100–122, 2010.

[5] S. Goldberg, M. Schapira, P. Hummon, and J. Rexford. How Secure are Secure Interdomain Routing Protocols? *SIGCOMM Comput. Commun. Rev.*, 40:87–98, August 2010.

[6] S. Goldberg, M. Schapira, P. Hummon, and J. Rexford. How Secure are Secure Interdomain Routing Protocols? Technical Report MSR-TR-2010-18, Microsoft Research, 2010.

[7] Y.-C. Hu, A. Perrig, and M. Sirbu. SPV: Secure Path Vector Routing for Securing BGP. *SIGCOMM Comput. Commun. Rev.*, 34:179–192, August 2004.

[8] IETF. Secure Inter-Domain Routing Working Group, 2011. `http://datatracker.ietf.org/wg/sidr/charter`.

[9] S. Kent, C. Lynn, J. Mikkelson, and K. Seo. Secure Border Gateway Protocol (S-BGP). *IEEE Journal on Selected Areas in Communications*, 18:103–116, 2000.

[10] C. Labovitz. China Hijacks 15% of Internet Traffic? `http://asert.arbornetworks.com/2010/11/china-hijacks-15-of-internet-traffic/`.

[11] R. Mahajan, D. Wetherall, and T. Anderson. Understanding BGP misconfiguration. *SIGCOMM Comput. Commun. Rev.*, 32:3–16, August 2002.

[12] D. McPherson. Internet Routing Insecurity::Pakistan Nukes YouTube? `http://asert.arbornetworks.com/2008/02/internet-routing-insecuritypakistan-nukes-youtube/`.

[13] B. Raghavan, S. Panjwani, and A. Mityagin. Analysis of the SPV Secure Routing Protocol: Weaknesses and Lessons. *SIGCOMM Comput. Commun. Rev.*, 37:29–38, March 2007.

[14] RIPE. YouTube Hijacking: A RIPE NCC RIS case study. `http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study`.

[15] R. White. Architecture and Deployment Considerations for Secure Origin BGP (soBGP). `ftp://ftp-eng.cisco.com/sobgp/drafts/draft-white-sobgp-architecture-01a.txt`.

[16] R. White. Securing BGP Through Secure Origin BGP. `http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_6-3/securing_bgp_sobgp.html`.

[17] E. L. Wong, P. Balasubramanian, L. Alvisi, M. G. Gouda, and V. Shmatikov. Truth In Advertising: Lightweight Verification of Route Integrity. In *Proceedings of the twenty-sixth annual ACM symposium on Principles of Distributed Computing*, PODC '07, pages 147–156, New York, NY, USA, 2007. ACM.

doi: 10.2313/NET-2011-07-2_10

Erkennung „bösartiger“ Domains

Tobias Niedl
Betreuer: Lothar Braun
Seminar Future Internet SS2011
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: niedl@in.tum.de

KURZFASSUNG

Als „bösartig“ werden Domains bezeichnet, die zu illegalen bzw. kriminellen Aktivitäten im Internet verwendet werden, beispielsweise in sog. Botnetzen. Neben Botnetzen können „bösartige“ Domains jedoch auch in anderen Zusammenhängen auftreten. Traditionell wurde und wird mittels Sperrlisten (engl. „blacklists“) versucht, die Nutzung solcher Domains zu unterbinden. Blacklists sind zwar ein einfaches und effizientes Mittel, besitzen jedoch den Nachteil, dass das Erkennen und Aufnehmen einer Domain in eine Blacklist eine gewisse Zeit in Anspruch nimmt. Entsprechend ist es das Ziel verschiedener Forschungsarbeiten, „bösartige“ Domains schnell und automatisiert zu erkennen, bevor ein Schaden durch ihre Verwendung entsteht. Diese Arbeit stellt drei solcher Arbeiten vor: „Proactive Domain Blacklisting“, „EXPOSURE“ und das „Fast-flux Botnet observation“-Verfahren. Wobei sich letzteres speziell auf die Erkennung von sog. Fast-flux Domains konzentriert, um die zugehörigen Botnetze näher untersuchen zu können.
Alle drei Verfahren nutzen bestimmte Eigenschaften von Domains bzw. Nameservern, um Domains zu klassifizieren, d.h. zu entscheiden ob diese „gut“ oder „böse“ sind. Da die Verfahren verschiedene Ziele verfolgen, werden unterschiedliche Ansätze verfolgt, die zu unterschiedlichen Ergebnissen führen.

Schlüsselworte

Malicious Domains, Botnet, Proactive Domain Blacklisting, EXPOSURE, Fast-flux Domains

1. EINLEITUNG

Eine Domain an sich ist weder „gut“ noch „böse“. Erst ein bestimmter Verwendungszweck bzw. eine bestimmte Anwendung lässt eine Domain als „böse“ erscheinen. Zu solchen Anwendungen gehören u.a. sog. Botnetze, die das „Domain Name System“ (DNS) und somit bestimmte Domains nutzen. Der Begriff Botnetz beschreibt ein Netzwerk von infizierten Computern (sog. „Bots“), die durch die Installation von Schad-Software (engl. „malware“) Teil des Netzwerks wurden. Die Bots stehen unter der Kontrolle eines Administrators, dem sog. „Botmaster“ (vgl. [1]). Dieser kann das Botnetz zu den verschiedensten Zwecken nutzen, z.B. für „Distributed Denial of Service“-Angriffe (DDoS), zum Versenden von Spam-E-Mails, zum sammeln sensibler Benutzerinformationen wie Bankverbindungs- oder Kreditkartendaten (vgl. [8]) usw. Außerdem können Botnetze auch zum Bereitstellen bzw. Vermitteln von Webinhalten genutzt werden, als „Content Distribution Netzwork“ (CDN) (vgl. [6]).
Da Botnetze auf eine Steuerung durch den „Botmaster“ angewiesen sind, müssen die einzelnen Bots regelmäßig Kontakt zu dessen Steuerungsrechner aufnehmen [8]. Würde die IP-Adresse des Steuerungsrechners fest in den Bots kodiert werden, könnte der „Botmaster“ relativ schnell gefunden und dessen Steuerungsrechner abgeschaltet werden. Das Botnetz wäre dann nicht mehr in der Lage, neue Anweisungen zu erhalten und somit unschädlich gemacht. Um diese Gefahr zu umgehen, nutzen Botnetze Domainnamen bzw. das DNS.
Werden Botnetze zur Bereitstellung von Webinhalten verwendet (als CDN), nutzen sie ebenfalls das DNS. Dann sind unter einem Domainnamen (einer sog. Fast-flux Domain) die meist illegalen Web-Inhalte abrufbar.

Neben Botnetzen gibt es auch andere Verwendungszwecke von Domains, die diese als „bösartig“ erscheinen lassen. Wird beispielsweise eine sog. Phishing-Seite auf einem regulären Webserver betrieben, so gilt die dazu genutzte Domain ebenfalls als bösartig. Phishing-Seiten werden von Kriminellen betrieben und sind den Webseiten von Unternehmen nachempfunden. Sie versuchen die Kunden der entsprechenden Unternehmen zur Eingabe ihrer Kennwörter (bei Banken auch PINs und TANs) zu bewegen.
Botnetze und Phishing-Seiten dienen an dieser Stelle als Beispiel, um aufzuzeigen in welchem Zusammenhang in dieser Arbeit von „bösartigen“ Domains gesprochen wird.

In dieser Arbeit werden drei Ansätze vorgestellt und verglichen, die versuchen zu erkennen, ob eine Domain für kriminelle Zwecke verwendet wird. „Proactive Domain Blacklisting“ [9] und „EXPOSURE“ [8] versuchen Domains zu finden, die bisher noch nicht durch bösartige Aktivitäten aufgefallen sind. Das „Proactive Domain Blacklisting“-Verfahren versucht anhand bekannter „bösartiger“ Domains, die bereits auf einer Blacklist geführt werden, ähnliche Domains zu finden, bevor diese ebenfalls zu bösartigen Zwecken verwendet werden können. „EXPOSURE“ versucht mithilfe von Datamining-Methoden „bösartige“ Domains im live DNS-Verkehr zu erkennen. Beide Verfahren können „bösartige“ Domains unabhängig davon erkennen, ob diese in Botnetzen eingesetzt werden oder nicht.
Das Ziel des „Fast-flux Botnet observation“-Verfahrens [6] ist hingegen *nicht*, bisher unbekannte Schad-Domains zu finden. Stattdessen werden Domains aus verschiedenen Quellen analysiert, um zu erkennen, ob diese als Fast-flux Domains in Botnetzen eingesetzt werden. Anschließend werden die zugehörigen Botnetze näher untersucht. Da Fast-flux Domains nur im Zusammenhang mit Botnetzen auftreten, kann das

doi: 10.2313/NET-2011-07-2_11

Verfahren – im Gegensatz zu den beiden anderen Methoden – nur Schad-Domains finden, die in bzw. für Botnetze genutzt werden.

Die genannten Verfahren werden hier gegenüber gestellt, da sie Beispiele für unterschiedliche Techniken zur Erkennung „böser“ Domains darstellen. „Proactive Domain Blacklising“ versucht eine Erkennung anhand statistischer Eigenschaften der Domains. „EXPOSURE“ nutzt Verkehrsanalysen sowie maschinelles Lernen und das „Fast-flux Botnet observation“-Verfahren stellt schließlich einen Mechanismus für eine spezielle Klasse von Schad-Domains dar, nämlich Fast-flux Domains von Botnetzen.

Alle drei Verfahren versuchen aus bestimmten Eigenschaften einer Domain jeweils automatisch zu erkennen, ob diese zu bösartigen Zwecken verwendet wird. Entsprechend müssen bei den Ergebnissen vier Fälle unterschieden werden:

- *true positive*: Eine Domain wird für bösartige Zwecke eingesetzt und vom angewendeten Verfahren als solche erkannt
- *false positive*: Eine Domain wird nicht für bösartige Zwecke verwendet, aber als solche eingestuft
- *false negative*: Eine Domain wird für bösartige Zwecke eingesetzt, aber nicht als bösartig erkannt
- *true negative*: Eine Domain wird nicht für bösartige Zwecke verwendet und auch nicht als solche eingestuft

Das Ziel aller Verfahren ist es, eine möglichst hohe „true positive“- bzw. „true negative“-Rate und eine möglichst geringe „false positive“- bzw. „false negative“-Rate zu erreichen.

Der Aufbau dieser Arbeit gliedert sich im Weiteren wie folgt: In Abschnitt 2 werden die für diese Arbeit wichtigsten Bestandteile und Funktionsweisen des DNS erläutert. In Abschnitt 3 werden die Verfahren „Proactive Domain Blacklisting“, „EXPOSURE“ und „Fast-Flux Botnet observation“ genauer vorgestellt und in Abschnitt 4 verglichen. Abschnitt 5 fasst diese Arbeit schließlich kurz zusammen.

2. DAS „DOMAIN NAME SYSTEM“ (DNS)

Menschen können sich i.d.R. aussagekräftige Namen wie „tumuenchen.de“ besser merken, als Ziffernkolonnen von IP-Adressen wie „129.187.39.3“. Allerdings funktioniert das Finden von Hosts im Internet nur über solche schwer merkbaren IP-Adressen. Das DNS übernimmt die Aufgabe, Domains bzw. Hostnamen, mit denen Benutzer arbeiten, in die zugehörigen IP-Adressen umzuwandeln, die in den Knoten des Internet verwendet werden (vgl. [11]).

2.1 Domain Bestandteile

Eine Domain besteht aus mehreren Teilen, wobei die einzelnen Teile durch einen Punkt getrennt werden. Die Informationen im Domainnamen werden von links nach rechts immer allgemeiner oder „unschärfer“. Am rechten Ende steht die Topleveldomain (TLD), wie *.com* oder *.de*.

Links von der TLD folgt der Domainname. Vor dem Domainnamen können keine, eine oder mehrere Subdomains stehen, d.h. weitere Domainnamen. Durch die verschiedenen Domainnamen bzw. die TLD entsteht eine Hierarchie. Für jeden Domainnamen innerhalb einer Domain kann ein eigener DNS-Server in der DNS-Hierarchie verantwortlich sein.

2.2 DNS Hierarchie

Das DNS arbeitet als eine verteilte Datenbank, die hierarchisch organisiert ist. An der Wurzel stehen die sog. Root-Server. Diese kennen die DNS-Server, die für die verschiedenen TLDs verantwortlich sind. In den DNS-Servern der TLDs sind für jeden registrierten Domainnamen die verantwortlichen „authoritive“ Nameserver hinterlegt. Die „authoritive“ Nameserver wiederum kennen schließlich die IP-Adresse für einen Domainnamen.

Die einzelnen DNS-Server speichern jeweils nur bestimmte Teile der DNS-Datenbank in sog. „Ressource Records“ (RRs). Ein RR ist ein 4-Tupel und besteht aus aus den Feldern „Name“, „Value“, „Type“ und „TTL“ („Time-to-live“). Es gibt verschiedene RR-Typen, die jeweils die Bedeutung der Felder Name und Value festlegen. Für diese Arbeit sind vor allem die Typen „Address“ (A) und „Nameserver“ (NS) von Bedeutung.
Beim Typ A enthält das Feld Name einen Domainnamen und das Feld Value die IP-Adresse des zugehörigen Hosts. Einer Domain können mehrere IP-Adressen zugeordnet sein. Dann existieren mehrere A-RRs mit gleicher Domain und den verschiedenen IP-Adressen. Bei einer Anfrage für eine solche Domain werden alle A-RRs als Antwort zurück gegeben. Das anfragende Programm entscheidet sich dann für die Verwendung einer dieser IP-Adressen. Durch dieses „Round Robin“-Verfahren kann eine Lastverteilung auf DNS-Basis erzielt werden (vgl. [8, 14]).
Beim RR-Typ NS enthält das Feld Name einen Domainnamen und das Feld Value den Domainnamen eines dazu gehörigen „authoritive“ Nameservers. Auch hier sind mehrere NS-RRs für mehrere Nameserver möglich.

Das Finden einer IP-Adresse zu einem Domainnamen wird als „auflösen“ eines Domainnamens bezeichnet. Diesen Prozess übernimmt ein sog. „Resolver“. Dieser ist i.d.R. Teil des Betriebssystems und schickt eine DNS-Anfrage an einen Nameserver, der die eigentliche Arbeit übernimmt. Das TTL-Feld in einem RR gibt an, wie lange ein RR von einem solchen Server bzw. dem „Resolver“ zwischengespeichert werden darf (engl. „caching“), bevor eine neue Anfrage gestartet werden muss. Durch das „Caching“ wird die Last im DNS verringert, da Hosts in einem Zeitraum ort dieselbe Domain mehrmals aufrufen und somit mehrmalige DNS-Anfragen vermieden werden. Der Richtwert für den TTL-Wert eines Domaineintrags (A-RR) liegt für „typische Hosts“ in der Größenordnung mehrerer Tage (vgl. [10]).

3. VERFAHREN ZUR ERKENNUNG „BÖSARTIGER“ DOMAINS

Alle drei im folgenden vorgestellten Verfahren zielen darauf ab, Domains zu erkennen, die bereits in Botnetzen genutzt oder mit hoher Wahrscheinlichkeit in Zukunft in solchen verwendet werden.

doi: 10.2313/NET-2011-07-2_11

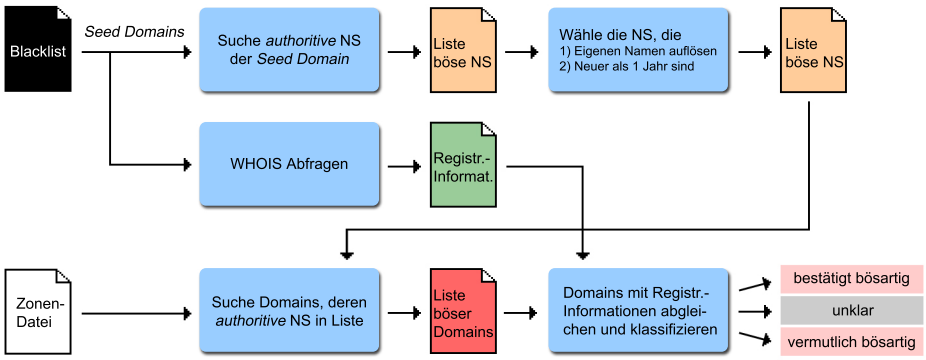


Abbildung 1: Ablauf des „Proactive Domain Blacklisting"-Verfahrens

3.1 Proactive Domain Blacklisting

Die Betreiber von Botnetzen registrieren meist mehrere Domains in Gruppen (vgl. [4]), die dann nach und nach verwendet werden. Wird eine verwendete Domain in eine Blacklist aufgenommen (oder gesperrt), können die Botnetzbetreiber schnell auf eine andere Domain wechseln und so einen Ausfall des Botnetzes vermeiden.
Das Verhalten der Botnetz-Betreiber, die meist mehrere Domains in einem Durchlauf registrieren bzw. administrieren, wird im „Proactive Domain Blacklisting"-Verfahren [9] dazu genutzt, weitere Schad-Domains, evtl. auch vor deren erster Nutzung, zu erkennen. D.h. ausgehend von einer oder mehreren Domains, die von einem Botnetzbetreiber administriert werden und die bereits auf einer Blacklist stehen, können weitere, evtl. ungenutzte Domains des Betreibers anhand verschiedener Eigenschaften gefunden werden. Die gefundenen Domains können dann auf eine Blacklist gesetzt oder durch den Registrar gesperrt werden, bevor weiterer Schaden durch ihre Verwendung entsteht.

3.1.1 Untersuchte Eigenschaften

Das Verfahren nutzt Eigenschaften des „authoritive" Nameserver einer untersuchten Domain. Dazu zählen der Domainname des NS, das Alter dieser NS-Domain und ob der Nameserver seinen eigenen Domainnamen selbst auflöst. Ist der Domainname des NS noch nicht lange registriert (jünger als ein Jahr) und übernimmt der NS selbst seine Namensauflösung, spricht dies für die Nutzung von sog. „double-flux" Techniken in einem Botnetz. „Double fluxing" funktioniert ähnlich wie „single fast-flux" (siehe Abschnitt 3.3.1), allerdings übernimmt nicht ein regulärer „authoritive" NS die Namensauflösung der Domain, sondern das Botnetz selbst[1].

Darüber hinaus werden zwei Eigenschaften der untersuchten Domain betrachtet, nämlich das Registrierungsdatum und der Registrar, also das Unternehmen, bei dem die Domain registriert ist. Die Verwendung aller genannten Eigenschaften wird im folgenden Abschnitt erläutert.

3.1.2 Ablauf des Verfahrens

Als Eingabe dient eine Blacklist, von der zufällige Domains ausgewählt werden, die sog. „Seed Domains." Diese werden dann weiter untersucht. Es werden die „authoritive" Nameserver, die einmal eine solche „Seed Domain" aufgelöst haben, bestimmt und auf einer Liste festgehalten.
Da die so erstellte Liste „böser" Nameserver auch die Nameserver großer „Internet Service Provider" (ISPs) enthalten kann, die normalerweise für mehr „normale" als „bösartige" Domains verantwortlich sind, wird in einem zweiten Schritt versucht, diese ISP-Nameserver herauszufiltern. Dazu wird die ursprüngliche Liste auf die Nameserver verkürzt, die die folgenden zwei Kriterien erfüllen:

1. Frische: Die Domain des Nameservers ist erst vor kurzem (innerhalb des letzten Jahres) registriert worden

2. Selbst-auflösend: Der Nameserver ist selbst für die Auflösung seines Domainnamens verantwortlich

Im nächsten Schritt werden die Registrierungsinformationen der „Seed Domains" mittels „WHOIS"-Abfragen ermittelt. Dadurch werden das Registrierungsdatum und der Registrar der Dominas bekannt gemacht. „WHOIS" [7] ist ein Client-Server Protokoll zur Abfrage von Domain-Informationen.

Als letztes findet die eigentliche *pro-aktive* Untersuchung von Domains statt. Dazu ist eine Quelle für Domains nötig, die auf ihre „Bösartigkeit" untersucht werden sollen. Prinzipiell ist jede Liste von Domains als Quelle nutzbar. Allerdings müssen neben den zu untersuchenden Domains auch deren NS-RRs, sowie das Registrierungsdatum bekannt sein. In [9] wird als Quelle die Zonen-Datei der *.com* TLD verwendet. Darin sind neben allen Domainnamen, die auf *.com* enden, auch deren „authoritive" Nameserver, also die NS-RRs, aufgeführt. Die Nutzung der *.com* Zonen-Datei stellt jedoch nur ein Beispiel zum Testen des Verfahrens dar. Es können auch andere Listen oder die Zonen-Dateien anderer TLDs genutzt werden, wenn diese zur Verfügung stehen.
Die Auswertung erfolgte über mehrere Wochen. Da täglich die aktuelle Zonen-Datei zur Verfügung stand, ist durch das Erscheinen von neuen Domains implizit auch deren Registrierungsdatum bekannt. Abbildung 1 stellt den Aufbau bzw. Ablauf des Verfahrens nochmals graphisch dar.

Die Auswertung der Zonen-Datei läuft dabei wie folgt ab: Wenn zum Zeitpunkt T eine Schad-Domain auf einen Nameserver A wechselt, werden alle Domains in der Zonen-Datei gesucht, die ebenfalls zum Zeitpunkt T auf den Nameserver

[1] Für eine detaillierte Darstellung von „single flux" und „double flux" Netzen sei auf [15] verwiesen

doi: 10.2313/NET-2011-07-2_11

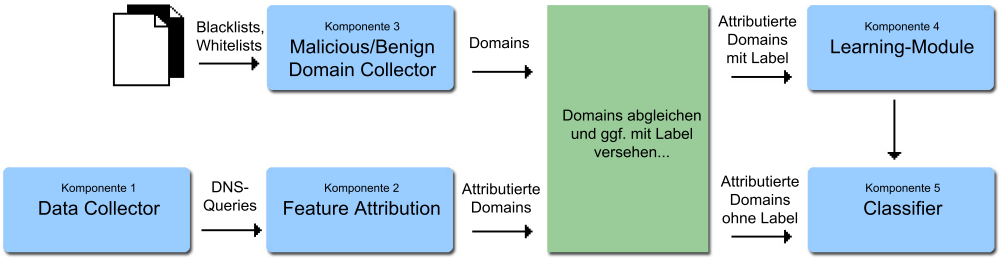


Abbildung 2: Die Architektur von EXPOSURE (nach [8])

A wechselten. Wenn eine Schad-Domain zu einem Zeitpunkt T auf Selbst-auflösung umgestellt wird, werden die Domains gesucht, die ebenfalls zum Zeitpunkt T auf Selbst-auflösung gewechselt wurden (vgl. [9]). Abschließend werden die Domains der Zonen-Datei jeweils einer Kategorie zugeordnet:

- Nachweislich bösartig: Die Domain wurde als „bösartig“ erkannt und steht bereits auf einer Blacklist
- Unbekannt: Es ist nicht eindeutig, ob die Domain zu bösartigen Zwecken verwendet wird
- Vermutlich bösartig: Die Domain wird vermutlich für bösartige Zwecke eingesetzt werden. Andere Verfahren (URIBL gold, SiteAdvisor) schätzen die Domain ebenfalls als „bösartig“ ein

3.2 EXPOSURE

Im Gegensatz zum „Proactive Domain Blacklisting“, das aktiv nach „bösartigen“ Domains innerhalb einer Zonen-Datei sucht, ist EXPOSURE ein System, das passiv arbeitet. Es analysiert den DNS-Verkehr von „authoritive“ Nameservern und stuft eine angefragte Domain anhand von 15 Kriterien als „gutartig“ oder „bösartig“ ein. EXPOSURE nutzt dazu Verfahren des maschinellen Lernens. Mit einem Trainingsset werden dem System Regeln beigebracht wie es „bösartige“ Domains erkennen kann. Das verwendete Trainingsset besteht aus den DNS-Antworten von „authoritive“ Nameservern auf rekursive DNS-Anfragen. Die Daten des Trainingssets stammen aus dem „Security Information Exchange“-Programm [5].

3.2.1 Untersuchte Eigenschaften

Die Domains werden anhand von 15 verschiedenen Attributen (engl. „features“) untersucht, die sich in folgende Klassen einteilen lassen: Zeit-basierte Eigenschaften, DNS-Antwort-basierte Eigenschaften, TTL-basierte Eigenschaften und Domainnamen-basierte Eigenschaften.

Die untersuchten Zeit-basierten Eigenschaften sind nicht fest an eine Domain gebunden, sondern ergeben sich stattdessen aus der Analyse des DNS-Verkehrs, der Aufschluss über die Zeitpunkte und Häufigkeiten von Anfragen gibt.
Zu den untersuchten Eigenschaften gehört u.a. die Lebensdauer der Domain. Eine Domain wird als kurzlebig eingestuft, wenn sie nur innerhalb eines relativ kurzen Zeitfensters von wenigen Tagen nachgefragt wird. Ein solches Verhalten wird als „abnormal“ eingestuft, da eine gewöhnliche Domain, auch wenn sie nicht sehr bekannt ist, doch mehrmals über den Beobachtungszeitraum hinweg nachgefragt werden sollte (vgl. [8]). Im Weiteren wird u.a. geprüft, ob sich die Anfragen für eine Domain zu bestimmten Tageszeiten regelmäßig häufen.

Die DNS-Antwort-basierten Eigenschaften unterteilen sich wie folgt: Es wird die Anzahl der IP-Adressen in den A-RRs bestimmt. Viele IP-Adressen sind zwar ein Indiz, deuten alleine jedoch noch nicht auf eine „bösartige“ Domain hin, da mehrere IP-Adressen auch von regulären Internet-Diensten zur Lastverteilung verwendet werden. Zusätzlich wird daher untersucht, zu wie vielen verschiedenen Ländern die IP-Adressen in den A-RRs gehören und wie viele Domains unter jeder einzelnen IP-Adresse zu erreichen sind.

Aufgrund der Infrastruktur von Botnetzen, deren Bots über verschiedene Internetzugänge verfügen und die über verschieden lange Zeiträume erreichbar sind, ändern sich die TTL-Werte „bösartiger“ Domains öfter, als die Werte gewöhnlicher Domains. Daher werden die TTL-Werte in den DNS-Antworten ebenfalls untersucht. Zu den TTL-basieren Eigenschaften gehört der durchschnittliche TTL-Wert in den A-RRs, sowie die TTL Standardabweichung. Im Weiteren wird gezählt, wie oft sich die TTL-Werte für eine Domain ändern und zu welchem prozentualem Anteil ein bestimmter TTL-Bereich von einer Domain genutzt wird. Ein TTL-Wert im Bereich [0,100) wird nach [8] besonders häufig für Schad-Domains verwendet.

Schließlich werden zwei Eigenschaften untersucht, die auf dem Domainnamen selbst basieren. Damit sollen Domainnamen erkannt werden, die durch einen Algorithmus erzeugt werden. Einige Botnetze wie „Conficker“, „Kraken“ und „Torpig“ erzeugen mehrmals täglich mehrere hundert Domains mittels eines „Domain Generation Algorithmus“ (GDA). Einige der erzeugten Domains registriert der Botnetzbetreiber und leitet sie auf die Steuerungsrechner des Botnetzes weiter. Die Bots fragen die generierten Domains an, bis ein Name aufgelöst wird und somit eine Kommunikation mit dem Steuerungsrechner möglich ist (vgl. [13]).
„EXPOSURE“ untersucht den prozentualen Anteil von Ziffern im Domainnamen sowie den prozentualen Anteil des längsten sinnvollen Substrings, d.h. ein Wort aus einem englischen Wörterbuch (engl. „longest meaningful substring“) um solche algorithmisch generierten Domainnamen zu finden. Da es jedoch auch bekannte Domains gibt, die keinen sinnvollen Ausdruck enthalten, z.B. „google.com“ oder „yahoo.com“, werden Domainnamen zusätzlich einer Google-Suche unterzogen (vgl. [8]).

doi: 10.2313/NET-2011-07-2_11

3.2.2 Komponenten

Das System besteht aus folgenden Komponenten: Ein „Data Collector“ sammelt die DNS-Anfragen eines Netzwerks ein, das beobachtet werden soll. Eine zweite Komponente, die „Feature Attribution“, versieht die gesammelten Domains mit deren Eigenschaften. Ein drittes Teilsystem „Malicious/Benign Domain Collector“ sammelt, unabhängig von den ersten beiden Komponenten, Domainnamen von Black- und Whitelists. Für diese Domainnamen ist somit explizit bekannt, ob sie „gut-“ oder „bösartig“ sind.

Die vom „Data Collector“ gesammelten und mit Attributen versehenen Domainnamen werden mit den explizit „gut-“ oder „bösartigen“ Domainnamen, die der „Malicious/Benign Domain Collector“ gesammelt hat, abgeglichen. Ist ein Domainname auf einer White- bzw. einer Blacklist enthalten, wird bei den bereits attribuierten Domainnamen jeweils zusätzlich ein Label für „gut“ oder „böse“ gesetzt. Ist eine Domain nicht explizit in einer White- oder Blacklist enthalten, wird kein Label gesetzt.

Die Domainnamen, die mit Label versehen sind, werden an die vierte Komponente, das „Learning Module“ übergeben. Dessen Ergebnisse, sowie die Domainnamen, die nicht mit einem Label versehen sind, werden der fünften Komponente übergeben, dem „Classifier“. Dieser entscheidet anhand der gelernten Muster und den Attributen einer Domain jeweils, ob diese zu bösartigen Zwecken verwendet wird, oder nicht.

Abbildung 2 stellt die Architektur von EXPOSURE nochmals graphisch dar.

3.2.3 Nutzung des Systems

Die Nutzung von „EXPOSURE“ unterteilt sich in zwei Phasen. In einem „offline Experiment“ wurden DNS-Anfragen verschiedener „authoritive“ Nameserver untersucht. Die Daten stammten vom „Security Information Exchange“ [5] und bestehen aus ca. 100 Mrd. DNS-Anfragen über einen Zeitraum von zweieinhalb Monaten. Da diese Datenmenge zu groß für eine Analyse war, wurde sie mittels zweier Maßnahmen verkleinert: Zum einen wurden, mittels einer Whitelist von Alexa [2], die Anfragen für die 1.000 bekanntesten Domainnamen herausgefiltert. Zum anderen wurden Anfragen für Domains, die älter als ein Jahr sind, entfernt. Damit reduzierte sich die Datenmenge auf die Hälfte. Mit diesen Daten wurde das System trainiert.

In einer zweiten Phase wurde EXPOSURE im Netzwerk eines ISP mit ca. 30.000 Kunden eingesetzt. In einem Zeitraum von zwei Wochen wurden dort im live DNS-Verkehr die DNS-Anfragen untersucht, um neue Schad-Domains zu finden. Anders als im „offline Experiment“ wurden die gesammelten DNS-Anfragen vor der Analyse nicht gefiltert.

3.3 Fast-flux Botnet observation

Wie bereits erwähnt, können Botnetze auch als Hosting-Plattform verwendet werden, um Webinhalte bereitzustellen bzw. zu vermitteln (vgl. [6]). Botnetze verwenden dazu eine Technik namens „Fast-flux“, die ein schnelles Mapping zwischen Domainnamen und IP-Adressen auf DNS-Basis ermöglicht (vgl. [6]). Das Ziel ist es, die meist illegalen Webseiten möglichst lange bereitzustellen und die eigentlichen Quellen zu verschleiern. Durch die Fast-flux-Technik wird das Finden der Webserver und das Unterbinden der kriminellen Aktivitäten wesentlich erschwert (vgl. [15]). Da dieselbe Technik auch von regulären Internet-Diensten zur Last-Balancierung verwendet wird, ist das Finden von Fast-flux Domains bzw. die Unterscheidung von „gutartigen“ und „bösartigen“ Domains jedoch schwierig.

3.3.1 Gewöhnliche und Fast-flux Domains

Für eine gewöhnliche Webseite (ohne Lastverteilung auf DNS Basis) stellt sich der Prozess nach dem Aufruf im Browser wie folgt dar: Der Webbrowser nutzt den „Resolver“ des Betriebssystems, um die IP-Adresse des eingegebenen Domainnamens zu erhalten. Zu dieser IP-Adresse baut der Webbrowser eine TCP-Verbindung auf Port 80 auf, um anschließend einen „HTTP-Request“ an den Webserver zu senden. Der Webserver antwortet – falls keine Fehler aufgetreten sind – mit einer „HTTP-Response“ Nachricht, die das angeforderte Objekt enthält (vgl. [12]), siehe Abb. 3.

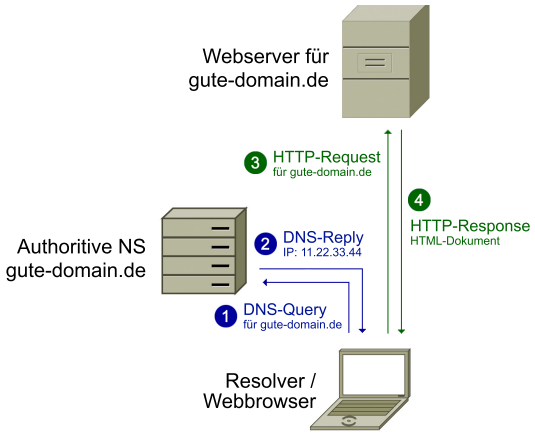


Abbildung 3: Vereinfachter Webseitenaufruf von einem gewöhnlichen Webserver (nach [15])

Würden Kriminelle solche „gewöhnlichen“ Webserver verwenden, könnten diese anhand ihrer IP-Adresse schnell gefunden und vom Netz getrennt werden. Das Fast-flux-Verfahren führt in den geschilderten Ablauf eine bzw. mehrere zusätzliche Schichten ein. Der „Resolver“ liefert auch hier eine IP-Adresse für den Domainnamen. Allerdings gehört diese IP-Adresse nicht zu einem Webserver, sondern zu einem Bot, der Teil eines Botnetzes ist. Der Webbrowser baut eine TCP-Verbindung auf Port 80 zu diesem Bot auf. Dieser nimmt die Anfrage entgegen und leitet sie an den zentralen Computer des Botnetzes weiter, das sog. „Mothership“. Das „Mothership“ sendet dann die angefragten Daten an den Bot, der sie wiederum an den Webbrowser weiterleitet (s. Abb. 4).

3.3.2 Ziel und Ablauf des Verfahrens

Ziel des „Fast-flux Botnet observation“-Verfahren ist – im Gegensatz zu „Proactive Domain Blacklising“ und „EXPOSURE“ – nicht das Finden unbekannter bzw. ungenutzter Schad-Domains, sondern die Untersuchung bestehender Botnetze, die Fast-flux Techniken verwenden. Dazu nutzt das Verfahren das „ATLAS“-System von Arbor Networks [3].

Dazu werden aus verschiedenen Quellen Domains gesam-

doi: 10.2313/NET-2011-07-2_11

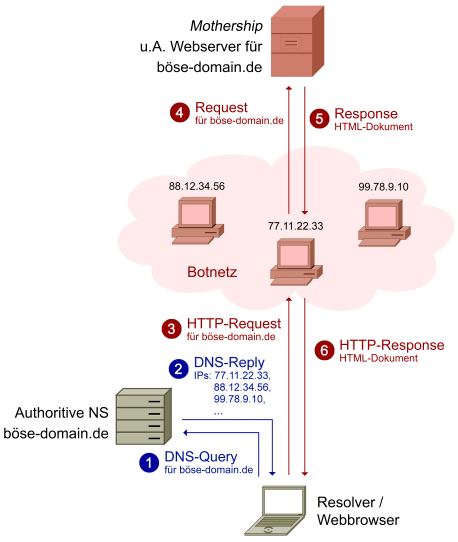


Abbildung 4: Vereinfachter Webseitenaufruf in (single) Fast-flux Botnet („single flux“) (nach [15])

melt, die bekanntermaßen zu bösartigen Zwecken verwendet werden. Zu diesen Quellen zählen Spam-E-Mails, Blacklists und die manuelle Analyse von Schad-Software.

Die gefundenen Domains werden anschließend einen „Quantifier“ übergeben, der anhand verschiedener Kriterien für jede Domain entscheidet, ob diese für Fast-flux Netzwerke verwendet wird oder nicht. Da viele reguläre Internet-Dienste eine Lastbalancierung auf DNS-Basis nutzen, besteht die Schwierigkeit darin, Fast-flux Domains, die für Botnetze verwendet werden, von regulären Domains zu unterscheiden, die eine gewöhnliche DNS-Lastbalancierung verwenden.

3.3.3 Verwendete Eigenschaften

Um zu entscheiden, ob eine Domain zu einem Fast-flux Netzwerk gehört, untersucht das „Fast-flux Botnet observation“-Verfahren u.a. die folgenden Eigenschaften. Hat eine Domain im A-RR einen TTL-Wert von weniger als 900 Sekunden, gilt dies als erstes Indiz dafür, dass es sich um eine Fast-flux Domain handelt. Für „gutartige“ Domains, die keine DNS-Lastbalancierung nutzen, wird ein TTL-Wert von einigen Tagen vorgeschlagen (vgl. [10]). Botnetze verwenden kurze TTL-Werte (nach [15] durchschnittlich 3 bis 10 Minuten) da die Erreichbarkeit einzelner Bots weder sichergestellt noch vorausbestimmt werden kann.

Im Weiteren werden die einzelnen IP-Adressen, die einer Domain zugeordnet sind, analysiert. Dazu gehört die Anzahl der IP-Adressen einer Domain (d.h. die Anzahl der A-RRs für eine Domain). Je mehr IP-Adressen für eine Domain gefunden werden, desto höher ist die Wahrscheinlichkeit, dass es sich um IP-Adressen aus einem Botnetz handelt. Zusätzlich wird der durchschnittliche „Abstand“ der IP-Adressen betrachtet, d.h. in welchen Adress-Bereichen die IP-Adressen liegen, und zu welchen „Autonomous Systems“ (ASs) sie gehören. Wenn reguläre Internet-Dienste Lastverteilung nutzen, werden die genutzten IP-Adressen i.d.R. im gleichen oder zumindest in benachbarten Netzen liegen und mit einer hohen Wahrscheinlichkeit nicht über viele verschiedene ASs im Internet verteilt sein. Die einzelnen Bots eines Botnetzes werden dagegen mit hoher Wahrscheinlichkeit weltweit verteilt sein, um eine hohe Verfügbarkeit des Botnetzes zu gewährleisten. Dies kann anhand der IP-Adress-Abstände und den „Autonomous System Numbers“ (ASNs) festgestellt werden.

Darüber hinaus werden auch einige Eigenschaften des bzw. der „authoritive“ NS untersucht. Sind mehr als drei solcher NS für eine Domain eingetragen, gilt dies als verdächtig. Werden mehrere NS verwendet, wird die Anzahl die ASNs der NS IP-Adressen gezählt. Sind die NS auf mehr als zwei ASs verteilt, gilt dies ebenfalls als verdächtig. Der „Abstand“ der IP-Adresse des NS zu den IP-Adressen der Domain wird ebenfalls betrachtet. Ein großer Abstand bedeutet, dass NS und Webserver in weit voneinander entfernten Netzen liegen, was ungewöhnlich ist.

4. VERGLEICH

Die vorgestellten Verfahren verwenden zur Klassifizierung der Domains verschiedene Eigenschaften von Domains bzw. deren Nameserver. Im folgenden sollen die Erfolgsraten und die genutzten Eigenschaften verglichen werden.

4.1 Erfolgsraten

Das „Proactive Domain Blacklisting“-Verfahren nutzt die Eigenschaften der verwendeten „authoritive“ Nameserver: die NS-Domainnamen, das Alter der NS-Domainnamen und ob der NS seinen Domainnamen selbst auflöst. Zusätzlich gehen in die Untersuchung der Zeitpunkt der Registrierung und der Registrar einer Domain ein.
Das Verfahren nutzt somit relativ wenig Informationen, kann aber dennoch registrierte und ungenutzte Schad-Domains finden, die zusammen mit bereits verwendeten „bösartigen“ Domains registriert bzw. verwaltet werden, sog. Cluster. Je nach Größe der Eingabe, d.h. wie viele „Seed Domains“ verwendet werden, werden unterschiedlich große Cluster gefunden. Bei 25 zufällig gewählten „Seed Domains“ wurden durchschnittlich 443 Schad-Domains gefunden, was einem Faktor von 17,7 entspricht. Die „true positive“-Rate liegt dann bei 74,1%, die „false positive“-Rate bei 1,3%. Wird eine größere Eingabemenge verwendet, nämlich alle 3.653 Domains in der Blacklist, die auf *.com* enden, so umfasst das Cluster 11.053 Einträge. Die „true positive“-Rate beträgt dann noch 73,7% und die „false positive“-Rate 6,6%. Die beste durchschnittliche „true positive“-Rate mit 81,4% erreichte das Verfahren bei einer Eingabegröße von 50. Dabei erreichte das Cluster eine durchschnittliche Größe von 649,7, was einem Faktor von 13,0 entspricht (vgl. [9]).

Das Verfahren hat jedoch zwei Nachteile: Zum einen benötigt es Ausgangsinformationen in Form von „Seed Domains“, die von Blacklists entnommen werden. D.h. es müssen bereits Domains zu bösartigen Zwecken verwendet (und erkannt) werden, bevor das Verfahren weitere Domains finden kann. Zum anderen ist eine Liste mit zu untersuchenden Domains nötig. Neben den Domains sollte auch deren NS-RRs und das Registrierungsdatum in der Liste enthalten sein. Je umfangreicher die zu untersuchende Liste, desto mehr potentielle Schad-Domains kann das Verfahren finden. In [9] wird die Verwendung der Zonen-Datei der *.com* TLD zum Testen des Verfahrens beschrieben. Dadurch können jedoch nur Schad-Domains gefunden werden, die auf *.com* enden. Die

doi: 10.2313/NET-2011-07-2_11

Nutzung weiterer Zonen-Dateien anderer TLDs ist prinzipiell möglich (und sinnvoll). Allerdings könnte der Zugriff auf die TLD Zonen-Dateien bestimmter Länder wie *.ru* eventuell schwierig sein (vgl. [9]), da hier die jeweiligen Registrare die Datei bereitstellen müssten.

„EXPOSURE“ analysiert live DNS-Verkehr und nutzt im Vergleich zum „Proactive Domain Blacklisting“ wesentlich mehr Domain-Eigenschaften zur Klassifizierung. Der Einsatz von „EXPOSURE“ erfolgte in zwei Phasen (siehe Abschnitt 3.2). Während des „offline Experiments“ erreichte das System eine Erkennungsrate von 98% mit einer „false positive“-Rate von 7,9%. In der „online Phase“ bei einem ISP wurden in einem Zeitraum von zwei Wochen 100 Millionen DNS-Anfragen analysiert. Dabei wurden 3.317 „bösartige“ Domains entdeckt, die dem System nicht aus den Trainingsdaten bekannt waren. Die „false positive“-Rate lag dabei bei 0% (vgl. [8]).
„EXPOSURE“ kann jedoch nur Schad-Domains finden, die nachgefragt, d.h. bereits von Botnetzen verwendet werden. Das Verfahren findet Schad-Domains mit verschiedenen TLDs, allerdings ist dazu der DNS-Verkehr zur Auswertung notwendig.

Da das Ziel des „Fast-flux Botnet observation“-Verfahrens nicht das Finden neuer, ungenutzter Schad-Domains ist, sondern die Analyse der Botnetze, die Fast-flux Techniken verwenden, lassen sich die Ergebnisse hier nicht direkt vergleichen. Als Datenquellen werden zwar u.a. Spam-E-Mails und Blacklists verwendet, allerdings dienen die dort gefundenen Domains nicht dazu, weitere Domains zu finden. Stattdessen wird versucht zu entscheiden, ob eine solche Domain eine Fast-flux Domain darstellt. Dazu werden verschiedene Eigenschaften der Domain bzw. der zugehörigen IP-Adressen untersucht (siehe Abschnitt 3.3.3) und die Domain entsprechend bewertet. Allerdings legt [6] keine Zahlen über den Erfolg dieser Maßnahmen offen.

4.2 Verwendete Eigenschaften

Wie schon festgestellt, nutzt das „Proactive Domain Blacklisting“ Eigenschaften der „authoritive“ Nameserver. Es wird eine Liste der NS erstellt, die bereits einmal eine Schad-Domain aufgelöst haben. Dann wird das Alter dieser Nameserver bzw. deren Domainnamen betrachtet. Zur Untersuchung werden nur die Nameserver herangezogen, die jünger als ein Jahr sind. Außerdem wird die Liste dieser „bösartigen“ Nameserver auf diejenigen verkleinert, die ihren Domainnamen selbst auflösen.
Neben diesen Nameserver-Eigenschaften werden der Registrar und das Registrierungsdatum der Domains selbst in die Untersuchung aufgenommen. Alle genannten Eigenschaften werden von den beiden anderen vorgestellten Verfahren nicht verwendet.

„EXPOSURE“ nutzt insgesamt 15 Eigenschaften. Einige davon sind Zeit-basiert und können nur über eine Beobachtung des DNS-Verkehrs festgestellt werden, z.B. ob eine Domain ausschließlich innerhalb eines kurzen Zeitraumes nachgefragt wurde. Weitere Eigenschaften basieren auf der Auswertung der DNS-Antworten, beispielsweise wie viele IP-Adressen einer Domain zugeordnet sind und in welchen Ländern diese IP-Adressen liegen. Darüber hinaus wird der TTL-Wert der A-RRs näher untersucht, beispielsweise wie lange ein A-RR durchschnittlich gültig ist. Abschließend werden zwei Eigenschaften untersucht, die sich auf den Domainnamen selbst beziehen, nämlich der Anteil der enthaltenen Ziffern und der Anteil des längsten enthaltenen „meaningful substring“.

Um zu entscheiden, ob eine Domain zu einem Fast-flux Netzwerk gehört, untersucht das „Fast-flux Botnet observation“-Verfahren neun Eigenschaften von Domains. Ebenso wie in „EXPOSURE“ wird die Anzahl der IP-Adressen für eine Domain sowie der TTL-Wert der A-RRs betrachtet. Die weiteren sieben Eigenschaften wie IP-Adressabstände, Anzahl von ASNs oder Anzahl der *authoritive* Nameserver usw. (siehe Abschnitt 3.3) werden von den anderen Verfahren nicht verwendet.

5. ZUSAMMENFASSUNG

Die vorgestellten Verfahren „EXPOSURE“, „Proactive Domain Blacklisting“ und „Fast-flux Botnet observation“ verfolgen das Ziel, „bösartige“ Domains zu erkennen, d.h. Domains, die zu kriminellen oder illegalen Zwecken von bzw. in Botnetzen verwendet werden. Alle drei erreichen dieses Ziel mit verschiedenen Ansätzen.

„EXPOSURE“ und „Proactive Domain Blacklisting“ versuchen „bösartige“ Domains zu finden, die bereits registriert aber noch nicht als „bösartig“ aufgefallen sind. D.h. die Domains wurden noch nicht auf eine Blacklist gesetzt oder gesperrt. Während „EXPOSURE“ versucht, derartige Domains bei deren Nutzung im live DNS-Verkehr zu erkennen, geht „Proactive Domain Blacklisting“ einen Schritt weiter und versucht anhand bekannter Schad-Domains weitere Domains zu finden, die bisher noch nicht für kriminelle Zwecke verwendet wurden, deren Einsatz zu solchen Zwecken aber absehbar ist.

„Fast-flux Botnet observation“ verfolgt hingegen nicht das Ziel, unbekannte Schad-Domains zu finden. Stattdessen werden Domains aus verschiedenen Datenquellen untersucht, um festzustellen, ob es sich dabei um Fast-flux Domains handelt. Das Ziel ist das Finden von Fast-flux Domains sowie die Untersuchung der zugehörigen Botnetze.

Alle drei Verfahren nutzen bestimmte Eigenschaften der untersuchten Domains bzw. deren *authoritive* Nameserver. Trotz des einheitlichen Ziels – das Erkennen „bösartiger“ Domains – nutzen die Verfahren weitgehend verschiedene Eigenschaften. Lediglich der TTL-Wert der A-RRs sowie die Anzahl der IP-Adressen für eine Domain wird sowohl von „EXPOSURE“ als auch vom „Fast-flux Botnet observation“-Verfahren verwendet.

6. LITERATUR

[1] Abu Rajab, Moheeb and Zarfoss, Jay and Monrose, Fabian, Terzis, Andreas. A multifaceted approach to understanding the botnet phenomenon. In *Proceedings of the 6th ACM SIGCOMM conference on Internet measurement*, IMC '06, pages 41–52, New York, NY, USA, 2006. ACM.

[2] Alexa. Top Sites. http://www.alexa.com/topsites. Letzter Zugriff: 28.04.2011.

[3] Arbor Networks. ATLAS. http://atlas.arbor.net. Letzter Zugriff: 28.04.2011.

doi: 10.2313/NET-2011-07-2_11

[4] Christian Kreibich, Chris Kanich, Kirill Levchenko, Brandon Enright, Geoffrey M. Voelker, Vern Paxson und Stefan Savage. Spamcraft: an inside look at spam campaign orchestration. In *Proceedings of the 2nd USENIX conference on Large-scale exploits and emergent threats: botnets, spyware, worms, and more*, LEET'09, pages 4–4, Berkeley, CA, USA, 2009. USENIX Association.

[5] Internet System Consortium. Security Information Exchange (SIE) Portal. https://sie.isc.org/. Letzter Zugriff: 28.04.2011.

[6] Jose Nazario und Thorsten Holz. As the net churns: Fast-flux botnet observations. In *3rd International Conference on Malicious and Unwanted Software*, pages 24–31, September 2008.

[7] L. Daigle. WHOIS Protocol Specification. RFC 3912, IETF, September 2004.

[8] Leyla Bilge, Engin Kirda, Christopher Kruegel und Marco Balduzzi. EXPOSURE: Finding Malicious Domains Using Passive DNS Analysis. In *18th Annual Network and Distributed System Security Symposium*, San Diego, Februar 2011.

[9] Mark Felegyhazi, Christian Kreibich und Vern Paxson. On the potential of proactive domain blacklisting. In *Proceedings of the 3rd USENIX conference on Large-scale exploits and emergent threats: botnets, spyware, worms, and more*, LEET'10, Berkeley, CA, USA, April 2010.

[10] P. Mockapetris. DOMAIN NAMES - CONCEPTS AND FACILITIES. RFC 1034, IETF, November 1987.

[11] Paul Albitz und Cricket Liu. *DNS und BIND*. O'Reilly, Köln, 1997. Deutsche Ausgabe der 2. Auflage, ISBN 3-930673-54-1.

[12] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee. Hypertext Transfer Protocol – HTTP/1.1. RFC 2616, IETF, Juni 1999.

[13] Sandeep Yadav, Ashwath K. K. Reddy, A.L. Narasimha Reddy, Supranamaya Ranjan. Detecting algorithmically generated malicious domain names. In *Proceedings of the 10th annual conference on Internet measurement*, IMC '10, pages 48–61, New York, NY, USA, 2010. ACM.

[14] T. Brisco. DNS Support for Load Balancing. RFC 1794, IETF, April 1995.

[15] The Honeynet Project & Research Alliance. Know Your Enemy: Fast-Flux Service Networks. http://www.honeynet.org/book/export/html/130, Juli 2007. Letzter Zugriff: 28.04.2011.

doi: 10.2313/NET-2011-07-2_11

Network Virtualization - An Overview

Kilian Rausch
Advisor: Michael Herrmann
Seminar Innovative Internet-Technologies and Mobile Communications
Chair for Network Architectures and Services
Department for Computer Science, Technische Universität München
Email: rauschki@in.tum.de

ABSTRACT

This paper introduces the basic approach of *Network Virtualization*, as well as Xen and OpenFlow as two opportunities to realize this approach. A virtual network is an autonomous, fully isolated network above an existing physical infrastructure. The goal of virtual networks is to run side-by-side to productive networks without affecting them and consequently to enable new network innovations to be tested safely. Xen is a hypervisor running directly on the hardware and able to host a large number of guest systems. This paper presents the qualifications of Xen to act as a virtual router platform. OpenFlow itself is an open standard for network devices to enable the easy deployment of experimental networks over an existing infrastructure. The related FlowVisor project expands OpenFlow by the opportunity to create and administrate fully isolated virtual networks. These two approaches were chosen among others because of their advanced progress and relevancy to practice.

Keywords

Network Virtualization, Router Virtualization, Software Designed Networking, Virtual Networks, Xen, OpenFlow, FlowVisor

1. INTRODUCTION

In the past years a high interest in reconsidering the existing network and Internet architecture came up. Some even describe the todays Internet architecture as "ossified" [10]. This movement was mainly carried by researchers, wanting to experiment with new network innovations. But building a realistic network environment for experimental purposes would require enormous investments. Therefore the success of new protocols and network architectures depends the possibility to run and test them coexistent, but isolated to existing network infrastructures. So they can not affect the productive networks, but can be tested in detail under real conditions. Productive networks are networks, which reliably carry out the everyday load. *Network Virtualization* is an efficient way to overcome this obstacle and to pave the way for new network ideas and developments. Network Virtualization is generally achieved through running an additional software on the network devices.

Besides the named above, Network Virtualization offers other various benefits. For example it allows the network operators to save a fix state of the network (In this paper we will describe this operation with the term *"Checkpoint Saving"*). This works like saving an image of a virtual operating system (OS) and could be very useful before changes are deployed. Then the previous state of the complete virtual network can be restored in the case of an error.

Another application scenario would be, that Network Infrastructure Providers have the potential to host multiple customers on the same hardware. Consequently they could coordinate the load in a much more efficient way. This leads to immense cost reductions for both parties and promotes competition, because then even smaller network operators have the possibility to use large-scale network infrastructure. Recently the *Open Network Foundation* (ONF) was established to support the development of the so called *Software Designed Networking* (SDN). Among the members are leading players like Facebook, Google, Microsoft, Deutsche Telekom and IBM. This non-profit organization especially supports the development and rollout of OpenFlow.

This paper gives an overview of Network Virtualization and presents two possible solutions and their relevancy for praxis. On that account we will especially look at the problems and challenges, which were discovered in several test cases. Given, that Virtualization in general brings a performance loss, we will highlight this topic in the dedicated Sections. In Section 2 the general approach of Network Virtualization is illustrated. In Section 3 Xen Hypervisor as solution for hosting multiple virtual routers is presented and in Section 4 we deal with OpenFlow and FlowVisor as the second possible solution. Finally we conclude in Section 5.

2. NETWORK VIRTUALIZATION - OVERVIEW AND GENERAL APPROACH

Virtualization in general is a method to concentrate or divide resources of a computer. It abstracts from the physical hardware, but gives the user the impression of interacting directly with it through the allocation of hardware resources. Besides the rapid development of virtualization of operating systems, researchers began to pay more attention to the virtualization of routers. This means running several virtual routers on the same machine as the basis of administrating multiple networks. Every router then belongs to a dedicated network, giving the full administrative power. The approach of Network Virtualization itself is not really new, as we already know *Virtual Private Networks* (VPNs) as solution for connecting different networks. The difference between VPNs and Virtual Networks (VNs) is illustrated in [1, page 2] as follows:

Although VPNs provide a virtualized channel above a physical network infrastructure, they have a few disadvantages in comparison with Virtual Networks. So all virtual networks have to be based on the same protocols, topology and

doi: 10.2313/NET-2011-07-2_12

addressing schemes. This mainly penalizes the reasearchers, wanting to deploy many different kinds of experimental networks. Another big issue is the missing isolation of the VPNs. While a few workarounds exist to deal with that problem, even these solutions provide no real isolation. Furthermore the infrastructure provider and the VPN service provider are normally the same entities. This disadvantage is among other things caused by the missing resource isolation. So multiple providers can not be sure, that another one is not affecting his network (for example by stressing the infrastructure). But the most important advantage of Virtual Networks over VPNs is the true isolation of the different Virtual Networks [1, page 2]. This mainly targets on hiding of network infrastructure specifications and even the existence of another administrative domain. But of course, we must consider the different use cases of VPNs and VNs. VPNs are often used to safely connect two networks or to establish a single connection remotely, for example to and within company networks. On the other hand a Virtual Network is used when researchers want to deploy a complete network over an existing one to test it under real conditions. So the Virtual Network provides the feature to be programmed individually with experimental protocols, address schemes et cetera.

Another commonly used technique are Virtual Local Area Networks (VLANs).VLANs are able to set virtual links above physical ports. The difference to Virtual Networks is, that they only can virtualize one specific forwarding algorithm. So the flexibility of choosing and developing new network innovations is not supported here [12].

The basic elements of a virtualized network environment are the *substrate layer*, where the physical resources (like CPU, memory or storage) are located, and the *virtual network layer*. The substrate layer contains the *substrate nodes*, mostly represented through typical network hardware like routers or switches, which must support virtualization. On these substrate nodes multiple virtual nodes are hosted, as well as the physical link contains multiple virtual links. Figure 1 shows the interaction of the virtual and the substrate layer. Virtual links are bundled to an aggregate. In order to clearly identify a specific VN in a wide infrastructure, a Virtual Network ID is used. This ID is globally unique and consists of the responsible organization ID and the virtual link ID [1]. When a Virtual Network is set up, a special *VNP/InP Inteface* provides all relevant information needed to build the VN, like the topology of nodes and virtual links, physical location and traffic characteristics.

3. XEN

In this Section Xen and an approach to use its virtualization technology to build and operate a virtual network is introduced. Xen is a hypervisor on x86 base which allows multiple operating systems to run on the same hardware. It is widely known as virtualization platform for operating systems. Xen is operating directly on the hardware and is able to host different OSs in the so called domains at the same time. The primary intention was to keep the performance overhead as small as possible to simultaneously host up to 100 Virtual Machines [3, page 1] and to isolate the domains safely. In the following we will introduce how the virtualization capabilities of Xen can be used to host virtual

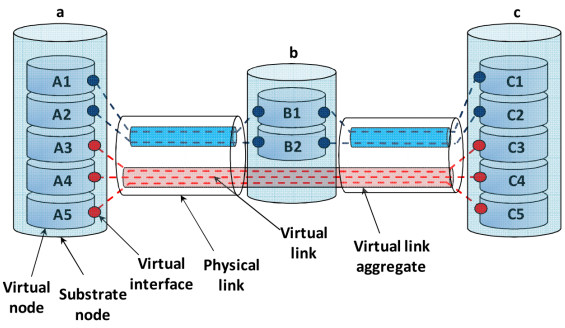


Figure 1: The substrate layer contains the *substrate nodes*. On these substrate nodes multiple virtual nodes are hosted. One physical link contains multiple virtual links, mostly bundled to an aggregate. [1]

routers.
Mainly the following challenges occurred when developing Xen [3, page 1]:

1. True Isolation of the Virtual Machines
2. Support of various operating systems
3. Keep the performance overhead as small as possible

3.1 Overview and Design Issues

In a traditional *Virtual Machine Monitor* (VMM) the hardware is emulated [5]. In contrast to this technique Xen uses paravirtualization to host a guest OS. This means a software interface is provided for the hardware; similar, but not equal to the hardware (no hardware emulation). As a consequence of that some slight modifications of the OS are indispensable. But the relative low costs to port an OS to Xen are worth to invest. This results in a system, which is nearly as efficient as a native system [13]. Figure 2 shows the efforts, measured in lines of codes (LOC), of porting a convenient OS to Xen.

OS subsection	**# lines**	
	Linux	**XP**
Architecture-independent	78	1299
Virtual network driver	484	–
Virtual block-device driver	1070	–
Xen-specific (non-driver)	1363	3321
Total	**2995**	**4620**
(Portion of total x86 code base	**1.36%**	**0.04%)**

Figure 2: porting costs, measured in lines of codes (LOC), of porting Linux or Windows®XP to Xen. [3]

Important to mention is, that the the guest applications remain unaffected here. The big difference of Xen to a convenient operating system, hosting the virtual machines ("normal" Virtualization), is the possibility to provide *performance isolation* [4]. Performance isolation ensures, that

doi: 10.2313/NET-2011-07-2_12

one virtual machine's performance can not impact the performance of another one (what of course is a desirable goal). But as in [4, page 19] mentioned, this works only under certain conditions. We will treat this especially for virtual router purposes in detail in the Section "Evaluation and Performance".

3.2 Xen and the x86 architecture

The Virtual Machine Interface for x86 architecture consists of three main elements [3]. *Memory Management, CPU Management* and *I/O Device Management.*

3.2.1 Memory Management

The memory management on x86 is quite difficult, because there is no software-managed *Translation Lookaside Buffer* (TLB), which translates virtual memory to physical memory. So Xen is designed to hand over the responsibility of allocating and managing the hardware page tables to the guest OSs.

3.2.2 CPU Management

In CPU Management x86 can play to its strength by having four *privilege levels* (alternatively called *rings*). Most other architectures have only two privilege levels. Mostly one privilege level for sensitive and one for non-sensitive commands (Popek and Goldberg Theorem [7]). Because Xen must urgently be located in level 0 (to have all possible rights), here the problem occurs, that the guest system has to share the same level with its applications. The guest system then runs in a separate address space. This leads to expensive TLB flushes through permanently involving the hypervisor for access control of the applications [3, page 4]. Running a guest system in level 0 would completely destroy the idea of isolation, because then this system would be in the position to change the whole system and consequently the other guest systems too. So the four rings of x86 are essentially needed to assign the highest privilege level to Xen, the second one to the guest OS and the third or fourth one to the applications. This avoids any influence of errors to the hypervisor and the expensive TLB Flushes.

3.2.3 I/O Device Management

The complete I/O Device Communication of each domain is processed by Xen with the embedded interfaces of several device abstractions. As mentioned above, the hardware is not emulated. The embedded interfaces in combination with the adapted OS result in much more performance. Additionally this allows Xen to manage and ensure the isolation of the guest operating systems.

In Figure 3 a sample configuration with Xen and different operating systems is illustrated. Dom0 must be emphasized as privileged control domain of Xen, able to start and stop other domains (to make this possible, this functionality should be implemented in the operating system of dom0. Here a XenoLinux is used).

3.3 Evaluation and Performance

As mentioned before in Section 1 there is a high interest of dedicated network operators and researchers in changing the existing network and Internet architecture. This Section

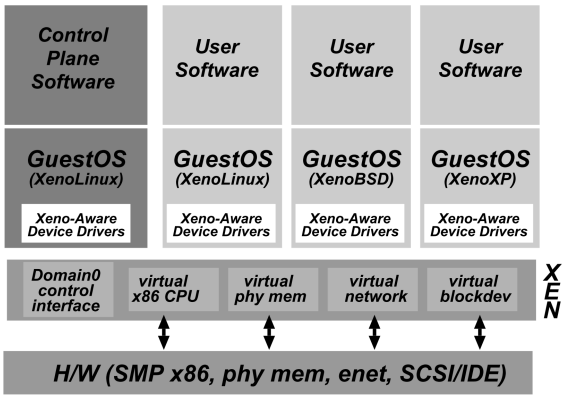


Figure 3: Architecture of a machine using Xen with different guest operating systems and the privileged dom0 control domain [3]

treats the capability of Xen to be used as a system for driving virtual routers. Multiple logically independent software routers are hosted on one single hardware. Each of them is responsible for his own isolated Virtual Network. The following statements and evaluations are based on [6] and [2]. Enabled by by powerful hardware and virtualization support, Xen's guest domains (called domU) can be equipped with virtual routers.

The fact, that Xen controls every privileged action of the domains results in two possible scenarios regarding packet forwarding [6]:

- each domU executes the forwarding itself
- dom0 bears all the forwarding activities

In both of the scenarios, the packets have to be allocated to the belonging domU out of the network stream and reverse. Dom0 sits behind the physical Network Interfaces (*Network Interface Cards*) and forwards the packet to the belonging virtual Interface of the domUs. So there is a lot of packet traffic between domU (what appears as the real network interface to the outer devices) and dom0, which has to be coordinated.
This can be done by a *bridging* (default) or a *routing mechanism.* In bridging a software bridge within dom0 executes this task and in routing IP-Adresses are assigned to the physical interfaces, as well as to the virtual interfaces within dom0.
In [6] several tests with different scenarios and combinations are carried out in competition with a single native linux. The authors draw the conclusion, that routing the packets through dom0 is the better solution (in contrast to bridging), especially with increasing number of domU's. Furthermore they found out, that handing over the forwarding function to the domU's results in a great performance loss. So when the forwarding task is operated by dom0 with a routing mechanism, then and only then Xen is able to forward packets as quick as a native linux. Surprisingly, the number of running virtual routers does not have any impact on the performance in this scenario. Finally the authors concluded, that when

doi: 10.2313/NET-2011-07-2_12

these conditions are taken into account, Xen is suited for the application as a virtual router platform.

In [2] another test scenario is evaluated by the use of a Click Router in combination with Xen. Click is a modular Open-Source Software-Router, implemented as Linux Kernel Add-On [8] with multi-threading support. In several scenarios it is analyzed, how fast packets are forwarded by the Click-Xen combination. Here it is experienced, that the smaller the forwarded packets are, the lower becomes the forwarding rate (measured in Gb/s). This is caused by the amount of memory accesses, that small packets are generating. This bottleneck can indirectly be handled by the CPU. CPU core switching during handling one packet and the triggered memory accesses can be avoided by allocating each virtual router to one particular core. Unfortunately this is the only way to influence the memory access bottleneck.

Another big challenge is sharing a *Network Interface Card* (NIC). Hardware-based allocation (every packet to the appropriate virtual router) is not fully supported neither by Click nor by Xen. But in contrast to the scenario above, here no software-based allocation is used. In the performed tests in [2] it is simply assumed, that the NICs are able to handle this demultiplexing. So the tests here are targeted a bit different. The results show, that core allocation becomes very difficult, when forwarding paths have different forwarding costs. Forwarding costs are for example composed of table lookups and the packet size. This issue is solved by a complex extended CPU Scheduler [2, page 5]. But as the authors appositely presume, sharing a single core might not be the issue in future, because development heads to increasing numbers of cores in CPUs. So it is concluded, that even today a virtual router can be realized using Xen and Click with the given problems to be solved in future. A similar project, just to be mentioned, is Trellis, where the same conclusion is drawn [9]. Finally, also in [3] the conclusion is drawn, that Xen is qualified for deploying "network-centric services".

4. OPENFLOW AND FLOWVISOR

The OpenFlow standard [10] is another possibility to enhance the possibilities of given networks. This open standard runs as an AddOn on Ethernet switches and routers and primarily separates the data path from the control path. The network is programmable and allows administrators to individually control and channel their data. Therefore only one single control unit is needed to administrate multiple routers and switches. This communication is carried out via a special OpenFlow Protocol, which has the benefit of beeing independent from hardware vendors. At the moment major device vendors are implementing OpenFlow in their hardware. OpenFlow is already be seen as a network virtualization technology by some members of the ONF, because it provides similar benefits. But this depends on the definition and point of view, of course. But to clarify: no multiple virtual router instances are running on the devices, like in Xen. To achieve real Network Virtualization FlowVisor is used [Section 4.2].

4.1 OpenFlow - Experimental Approach and Functionality

The most popular use case is the experimental test of new network protocols. This can be pefectly established in campus networks [10], because the researchers here can use their familiar environment and profit from the OpenFlow Roll-out at campus networks. The goal is to run experiments in the existing campus infrastructure without affecting the everyday work of others. Therefore a normal Computer is not sufficient, because of the low paket forwarding rate and the small number of ports. Consequently there is a need for an idealized OpenFlow Switch (Figure 4). This switch meets the demands of high-performance, low-cost, isolation and commercial vendors needs.

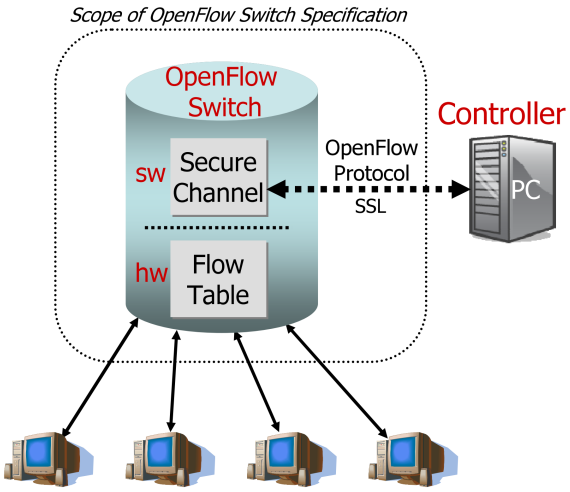


Figure 4: structure of an OpenFlow switch, showing the OpenFlow Software running above the hardware, modifying the FlowTable and communicating with the *Controller* [10]

The data path is still a task of the switch hardware, based on the flow table (provided by the OpenFlow controller). Here OpenFlow provides an interface to modify the flow tables of commercial router or switch products, exploiting the fact of many identical functions in the different products. As a result the experimental network traffic can be segregated from production traffic. All in all this enables similar benefits to the introduced solution with Xen (experiment with new routing protocols, addressing schemes and even IP alternatives [10]). The control instance saves a kind of forwarding rules as flow entries in the flowtable, each containing how to handle specific packets. A normal procedure in an OpenFlow-based hardware is to forward packets, when a flow entry already exists. The OpenFlow Software then knows how to forward the packet to which port. Another case is, that the arriving packet is unknown. Then OpenFlow sends the packet to the Controller via the encrypted OpenFlow Protocol. The Controller then decides, whether to create a new entry in the flow tables and to send it back to the switch, or to drop the packet.
So in an example configuration with many switches and routers, when a flow is defined at the control unit a new protocol comes into operation and automatically creates a new route for the packets by entering automatically all relevant FlowEntries in each switch. This is called a flow.

doi: 10.2313/NET-2011-07-2_12

In OpenFlow there are two major opportunities to achieve traffic isolation:

- forward the packets through the switch's normal processing pipeline
- assign VLAN IDs to the groups of packets to allocate them to different VLANs

Many sample applications are given in [10, page 4], just as creating VLAN similar environments, establishing VoIP connections, defining new addressing, naming and routing schemes and even abstracting from flow processing of the controller to programmable router based processing.

4.2 FlowVisor Network Virtualization Layer

One step ahead goes FlowVisor, "a special purpose OpenFlow controller that acts as a transparent proxy between OpenFlow switches and multiple OpenFlow controllers" [11]. So in a FlowVisor application field, when a packet arrives at an OpenFlow Switch, it is routed by the FlowVisor to the belonging Controller and reverse forwards the packets back to the switches. This is performed in an isolated way by assuring, that no resources, like the FlowTables can affect each other. So FlowVisor supplements OpenFlow by adding real virtualization possibilities. FlowVisor provides virtualization of switches to build a divided, fully isolated and autonomous network above the physical structure. Every network is logically independent and runs in addition to a productive network on the same hardware. In [12] these virtual networks are called *slices*. FlowVisor regards a slice as any combination of switch ports and layer 2, 3 and 4 of the OSI-model [14]. Of course, FlowVisor follows the virtual network approach and supports its advantages, like resource allocation or Checkpoint Saving [Section 1].

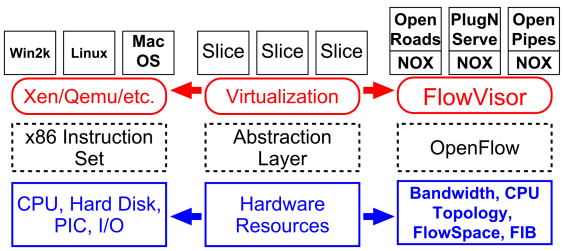


Figure 5: FlowVisor layer comparison to Xen and abstract virtualization - Flow Visor is located betweeen the OpenFlow Switch Software and the Controllers above. Open Roads, PlugN and Open Pipes are examples of virtual network controllers [12]

The layer location of FlowVisor in Figure 5 shows, that it is comparable to other virtualization technologies and of course to Xen, we treated before. Flow Visor is located between the OpenFlow Switch(forwarding path) Software and the Controllers (control path) above. Open Roads, PlugN and Open Pipes are examples of virtual network controllers [12]. To the controllers FlowVisor appears as a set of OpenFlow Switches and to the OpenFlow Switches it appears as a set of Controllers. FlowVisor itself hosts multiple OpenFlow guest controllers, as shown in Figure 6, one for each virtual network. The design focuses here on strong isolation. This involves the controllers of the different slices, as well as the belonging datapath traffic. One slice should not be able to influence another one. This Isolation is achieved by following which flow entry to which controller belongs and assigning a minimum data rate to a slice [10]. FlowVisor should be transparent (with the meaning of imperceptible) for the controller and the OpenFlow Switch. This is for example important when an error or bug occurs in a test environment. It simplifies the finding and fixing process. Furthermore FlowVisor should support resource allocation. This is implemented by a special module, called the *Resource Allocation Policy* [12].

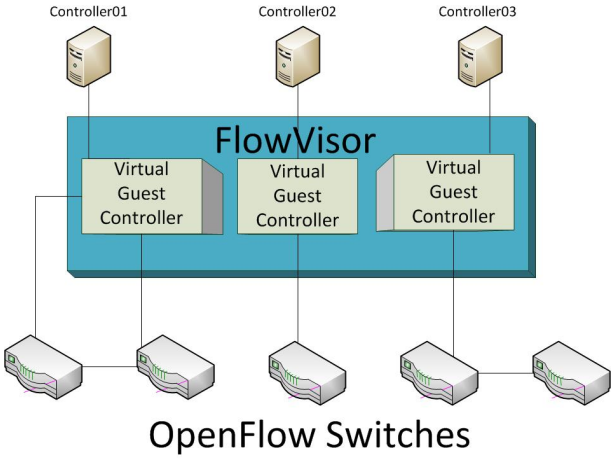


Figure 6: FlowVisor internal structure - FlowVisor hosts multiple virtual guest controllers, each responsible for one virtual network

The three major design goals of FlowVisor are summed up in [12] as follows:

1. Transparency
2. Isolation
3. Extensible Slice Definition

4.2.1 *Isolation and Challenges*

Since isolation is one of the critical issues in Network Virtualization, this Section treats the isolation capabilities of FlowVisor. *Bandwidth Isolation* is only provided with the instruments of VLANs. Each packet has a VLAN Priority Code Point field, where an entry assigns a packet to a certain priority level. Combined with the traffic class in the Resource Allocation Policy this enables a kind of bandwith allocation. But the big disadvantage is, that the exact specifications of a traffic class must be manually implemented in each switch. This shows, that in this field future research has to be done to make this issue more practicable. *Topology Isolation* means, that FlowVisor transmits only information of the belonging switches to each of its virtual guest controllers inside. So each virtual network, or each guest controller gets only information about his own network. Due to the fact most switch hardware has low-performance CPUs, the risk of a breakdown of the OpenFlow Software is very high on an overload. FlowVisor does not support CPU Isolation at the

doi: 10.2313/NET-2011-07-2_12

moment. Only a few workarounds exist, which explain how to deal with the limited CPU. Furthermore the *FlowSpace Isolation* assures, that one virtual guest controller can only affect the own virtual network with its created rule. Even the connection to the OpenFlow controller is virtualized and controlled by transaction IDs. This ensures, that no guest controller can block or even catch a transaction of another guest controller.

4.2.2 Performance

As mentioned in Section 1, adding a additional virtual layer between two instances results in performance deficits. Of course this is for FlowVisor as well true as for any other virtualization technology. The goal rather is to reduce this performance overhead to a negligible amount. FlowVisor realizes this through only acting in situations where it is really necessary. All data and control paths work at full line rate, without beeing slowed down by FlowVisor. This also applies for any route selection, carried out by a controller. The only situation when FlowVisor intervenes, is when a new flow message is send by the switch (a new unknown packet arrived) and port status messages (controller demands switch to send byte and packet counters for a specific port). The tests in [12] show, that the average overhead of a port status request is about 0.483ms and for flow messages 16.16ms. So we see the latency for port status request is quite acceptable, where in contrast the 16.16ms latency is probably a bit too high for time sensitive applications.

5. CONCLUSION

Our goal was to give an overview over Network Virtualization and to highlight the ability of Xen and OpenFlow/ FlowVisor to realize this approach. So all-in-all the topic of Network Virtualization is still an experimental field. But recent developments show, that the industry is interested in deploying this technique in praxis [Section 1]. What solution has the best chances to become successfully deployed in large scale networks, depends on many factors and can not be clearly identified. Here future research is needed. So Xen provides a relative stable technology yet, while the quite young OpenFlow Project now receives great support by the ONF. But a disadvantage of FlowVisor is, that at this time the software itself is not stable enough to be transferred into production. Given the quite big performance overhead of the flow messages, we can summarize, that a lot of work has to be done in future. With the given constraints, Xen can even nowadays provide a functional platform for virtual routers and networks. Due to the increasing interest in programmable, virtual networks, this is going to be a subject of interest in the future. Especially science will benefit from this demand in research.

6. REFERENCES

[1] Jorge Carapinha and Javier Jimnez: *Network Virtualization – a View from the Bottom*, VISA '09 Proceedings of the 1st ACM workshop on Virtualized infrastructure systems and architectures, pages 1-3, ACM New York, NY, USA ©2009

[2] Norbert Egi, Laurent Mathy, Mickael Hoerdt, Adam Greenhalgh, Mark Handley and Felipe Huici: *Fairness Issues in Software Virtual Routers*, PRESTO '08 Proceedings of the ACM workshop on Programmable routers for extensible services of tomorrow, ACM New York, NY, USA ©2008

[3] Paul Barham, Boris Dragovic, Keir Fraser, Steven Hand, Tim Harris, Alex Ho, Rolf Neugebauer, Ian Pratt and Andrew Warfield: *Xen and the Art of Virtualization*, SOSP '03 Proceedings of the nineteenth ACM symposium on Operating Systems principles, ACM New York, NY, USA ©2003

[4] Diwaker Gupta, Ludmila Cherkasova, Rob Gardner and Amin Vahdat: *Enforcing Performance Isolation Across Virtual Machines in Xen*, PROCEEDING - Middleware '06 Proceedings of the ACM/IFIP/USENIX 2006 International Conference on Middleware , Springer-Verlag New York, Inc. New York, NY, USA ©2006

[5] L. Seawright and R. MacKinnon: *VM/370 - A Study of Multiplicity and Usefulness*, IBM Systems Journal, pages 4-17, 1979

[6] Norbert Egi, Adam Greenhalgh, Mark Handley, Micka"el Hoerdt, Laurent Mathy and Tim Schooley: *Evaluating Xen for Router Virtualization*, Proceedings of 16th International Conference on Computer Communications and Networks, Computer Communications and Networks, 2007. ICCCN 2007, Honolulu, HI ©2007

[7] Gerald J. Popek and Robert P. Goldberg: *Formal requirements for virtualizable third generation architectures*, Commun. ACM, 17(7):412–421, 1974.

[8] Daniel Schwencke: *Click – ein modularer Router*, Seminary paper, TU Braunschweig, July 2006

[9] Sapan Bhatia, Murtaza Motiwala, Wolfgang M"uhlbauer, Vytautas Valancius, Andy Bavier, Nick Feamster, Larry Peterson and Jennifer Rexford: *Hosting Virtual Networks on Commodity Hardware*, WORKSHOP ON REAL AND OVERLAY DISTRIBUTED SYSTEMS (WORLDS), 2008

[10] Nick McKeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker and Jonathan Turner: *OpenFlow: Enabling Innovation in Campus Networks*, Newsletter ACM SIGCOMM Computer Communication Review archive, Volume 38 Issue 2, April 2008, ACM New York, NY, USA

[11] *FlowVisor: Home*, `https://openflow.stanford.edu/display/flowvisor/Home` accessed on May 24th, 2011

[12] Rob Sherwood, Glen Gibb, Kok-Kiong Yap, Guido Appenzeller, Martin Casado, Nick McKeown and Guru Parulkar: *FlowVisor: A Network Virtualization Layer*, OPENFLOW-TR-2009-1

[13] Christian Kern: *Paravirtualisierung, Vanderpool*, Haupseminar Virtualisierungstechnologien, Technische Universität München, Institut für Informatik, Lehrstuhl für Rechnertechnik und Rechnerorganisation, Prof. Dr. Arndt Bode, 22.07.2005

[14] Hubert Zimmermann: *OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnection*, IEEE TRANSACTIONS .ON COMMUNICATIONS, VOL. COM-28, NO. 4, APRIL 1980

doi: 10.2313/NET-2011-07-2_12

Correlated Network Flows Detection

Olga Birth
Betreuer: Michael Herrmann
Hauptseminar- Innovative Internettechnologien und Mobilkommunikation SS2011
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: birth@in.tum.de

ABSTRACT

Traffic monitoring and analysis plays an essential role in today's network security, since an unsecured network represents a grateful target to intruders. The goal of traffic analysis is, to obtain an intruders identity or to detect correlated network flows in order to allocate them to an individual. In that case, probable attacks can be answered appropriate.
Most offenders try to conceal their identity while performing attacks on their target destination. Thereby the most popoular way to stay hidden is, to link the traffic through several intermediate hosts, which had been compromised earlier. Correlated network flow detection (CNFD) would then try to detect these linked connections and reveal an attackers identity, even if the traffic is encrypted.
CNFD can also be used to detect an individuals identity in an *anonymous communication system*. Anonymous communication systems, were designed to obtain users anonymity while surfing the web. CNFD can detect senders and receivers identity and also the linkage between those two in an anonymous communication system. While traditional methods are performed by passively observing the possible connections and trying to find correlations by performing different statistical approaches [4][5][9][13], *watermarks* seem to be an elegant way to make CNFD more efficient and less expensive. Watermarking flows provide a novel approach, to reveal correlated flows. Nobody would even notice, if the traffic is been observed. Good watermarks can be inserted invisibly into the network and are more scalable than traditional passive analysis methods.
This paper is intended to give an overview of traffic analysis techniques, how they can be applied to detect correlated network flows and how watermarks can be used in this context.

Keywords

correlation, intrusion detection, watermark, flow transformation, active traffic analysis, stepping stones, anonymous communication systems

1. INTRODUCTION

Traffic analysis is the best way to keep track of all traffic that is traversing a network. If this is not performed carefully, an intruder can easily access a network and perform several attacks, without even being noticed [13]. An enemy usually knows everything about common monitoring techniques presented below, so if he/she wants to enter a network he/she always tries to stay anonymous. Besides spoofing the IP address, an intruder can obtain anonymity by using *stepping stones* [20]. Stepping stones are intermediate hosts that are used by an invader to launch an attack not from his own computer, but from compromised hosts. In addition to that, usually the traffic between the enemy and the target is encrypted. Without appropriate traffic analysis, nobody can never detect an intruder. To reveal such an attacker, it is very important to detect *similarities* between incoming and outgoing flows at the stepping stones [17]. This is also called *correlated network flow detection*.

CNFD can also be applied to anonymous communication systems. For a long time many have been convinced that with applying different transformations, a flow will become unique and so stable to correlation detection [16]. An attacker could now start applying several flow transformation techniques, in order to prevent unique network flows to be discovered [16]. This would modify a flow, that it would look completely different and could not be identified by an observer anymore. But there are still properties of flows, that cannot be erased by these transformations, like packet timing. This makes an flow, no matter how often the transformations have been applied, still unique [16].

This is where watermarking becomes important. The idea of watermarking is to uniquely identify a network flow by content-independent manipulations [4]. If two flows contain exactly the same pattern, they can be assumed to be linked. Watermarks are a new approach to traditional active monitoring techniques, because they need less computations than traditional techniques. Good watermarks are scalable, robust to packet losses and invisible [4]. This makes watermarks a good alternative to detect stepping stones and links in anonymous communication systems.
The remainder of this paper is structured as follows: the second Section is about the basics, such as traffic analysis methods, anonymous communication systems, stepping stones and different flow transformations. This should show, how traffic can be manipulated, in order to hide an individuals identity.
The second part is about traditional CNFD methods. This includes different correlation detection besides watermarking. In this work, watermarks have been picked, as a new and elegant approach to correlation detection in network flows. But there are other techniques, how correlated network flows can be detected.
Up next is a Section about watermarking, with the differ-

doi: 10.2313/NET-2011-07-2_13

ent watermarking approaches. It is aimed to provide a brief overview of the different watermarking techniques, without going into very detail.
Section 4 discusses the applications of watermarking and Section 5 concludes this topic.

2. BACKGROUND

There are several concepts that should be described first, such as diverse monitoring techniques and some term descriptions to provide the basics for this topic.
As mentioned above, there are several traffic monitoring techniques, which can basically be separated into two groups: the *router based monitoring techniques* and the *non-router based monitoring techniques* [6].
The difference between those two is simple: the former ones have the monitoring functionalities built in the routers, whereas the non-router based require further installation of hardware and software [6]. It would simply go beyond the scope to explain both techniques in detail. To understand this paper, there is no need to know the functionalities behind the router-based monitoring techniques. For further information on the router-based techniques, such as RMON or Netflow RFC see: [3][2].
The non-router based can again be separated into *active* and *passive* monitoring techniques.

2.1 Active Monitoring Techniques

To monitor traffic using active monitoring techniques, an active communication between not less than two points (sender/ recipient) is needed. For measurement issues, when using active monitoring, packets need to be inserted actively into the network. Perhaps the best known active monitoring techniques are *ping*, *traceroute* and *iperf* [6]. All techniques are dealing with availability, routes, packet inter-arrival jitter, packet delays, packet losses or bandwidth measurements [6]. They are called activity monitoring techniques, because using the ping example, the sender needs to actively send ICMP echo requests to an endpoint and waiting for the response.

2.2 Passive Monitoring Techniques

Passive monitoring, on the other hand, does not create additional traffic to the network. It simply listens to the traffic and collects information about packet rates/timings and inter-arrival timings [6]. At the end of a day, the administrators need to handle a huge amount of collected information. Packet sniffing is a good example how to perform passive monitoring. The drawback behind this monitoring technique is, that it can only be performed off-line.

Because active monitoring does inject to much overhead into the network and passive monitoring can only be done off-line, there are also combinational monitoring techniques possible, such as WREN [11] and SCNM [7].

2.3 Anonymous Communication Systems

Anonymous communication systems are designed to help people stay unrecognizable while surfing designated web sites. It is a privacy concern, when someone do not want to get profiled by a random website [16]. Tor[8] is a popular example of such anonymous communication systems, to address such privacy concerns.

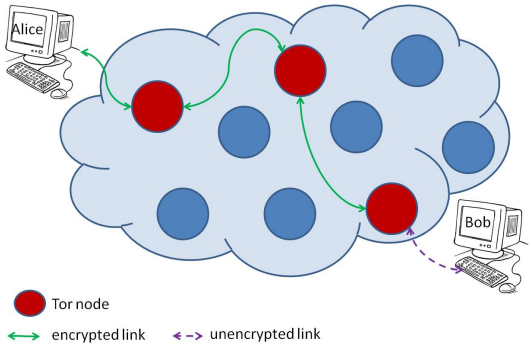


Figure 1: Anonymous Communication System (adopted by [8])

An anonymous communication system should have these three desirable features to ensure anonymity: it should provide sender anonymity, receiver anonymity and unlinkability of sender and receiver [16][12]. Sender and receiver anonymity simply means, that it cannot be identified who is communicating. Unlinkability of sender and receiver means, that even if the identity of both is known, the connection between them should be hidden [16].
Based on Tor, the functionality behind those systems should be described roughly (see Figure 1): Alice wants to communicate with Bob, but Alice wants to stay anonymous. Instead of establishing a direct connection between Alice and Bob, Alice installs an Onion proxy on her computer, which establishes a connection over three randomly chosen with Tor nodes. Between two nodes a tunnel is established using the public key of the communication node. The message travels over this tunnel encrypted. For each connection, a new random walk is chosen by the software. At no step, it can not be discovered where the traffic came from, and where it has been relayed to. Bob receives the message from Alice, but thinks that the message came from the last communicating node.

2.4 Flow Transformations

Flow transformations are applied to network flows to make them unrecognizable in order to achieve non-correlated flows. There are a few techniques, that can be applied to flows, to get rid of identifying characteristics. These techniques can widely be separated into *intra-flow transformations* and *inter-flow transformations* [16]. The former ones, are based on flow transformation within one flow without involving additional flows. The second ones produce transformation on flows by adding further unrelated flows.

2.4.1 Intra-Flow Transformation

Basically within one flow, following transformations can be applied (see Figure 2): adding chaff, packet dropping (also de-chaff) and repacketization (packet merge and fragmentation)[16]. Chaff is any cover-traffic within an anonymous system. Packet dropping can be enforced to make a flow unrecognizable. Repacketization can be done by combining packets, or by splitting a packet. Packet dropping and

doi: 10.2313/NET-2011-07-2_13

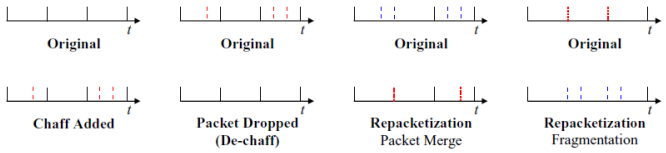


Figure 2: intra-flow transformations: adding chaff, packet dropping and repacketization (packet merging and fragmentation) (adopted by [16])

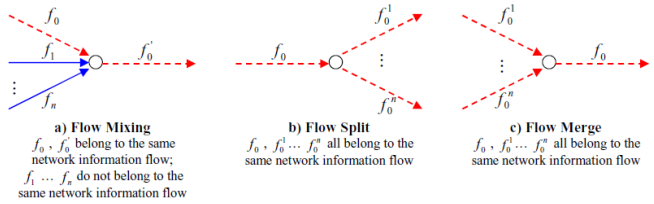


Figure 3: inter-flow transformations: flow mixing, flow splitting and flow merging (adopted by [16])

repacketization can be done intentionally, but also can happen naturally as for example by using SSH. [16].

2.4.2 *Inter-Flow Transformation*

Here, transformations are applied that include: flow mixing, flow splitting and flow merging [16]. Thereby it is important to notice, that a flow is mixed/splitted or merged with unrelated flows (see Figure 3) in contrast to intra-flow transformation where a flow was transformed within one flow without involving additional flows. As can be seen in figure 3, flow mixing mixes a random flow with unrelated flows. However flow merging combines a flow with flows that belong to the same network information flow [16].

Such flow transformations occure in anonymous communication systems to change a flow to an unrelated one. As the presented flow transformation can be applied arbitrary often, it has been believed, that the produced flows are indistinguishable. However, with the use of watermarking, correlated flows, even if they are distorted like that, can be found.

2.5 Stepping Stones

Beside anonymous communication systems, stepping stones are a popular technique to conceal an atteckers identity. The idea is simple: instead of using the real computer for attacks, the attacker can connect through a sequence of intermediate hosts, which were compromised earlier. This example is from [17] and describes, how stepping stones can be applied: consider an attacker at host A, who can use SSH to login into B. B is now the stepping stone, if the attacker plans to start an attack on C, which he will do of course from B. Here comes the crucial part: the two connections between A and B, and between B and C are correlated. They are basically the same, besides the fact that they have been forwarded at the point B. This is where CNFD applies. It is searching for correlated network flows to link them together and thus to identify the attacker. Notice that SSH has been used to encrypt the traffic, so content-based analysis would not work here. Since an attacker has the authority over the stepping stone, he can apply multiple flow transformations to make the flows look different (not correlated). Watermarks can identify such flows in stepping stones.

3. CORRELATION DETECTION

The rudimentary approach to detect similarities in flows, is by comparing two flows. The procedure is described below: [21]:

1. Data Collection
2. Distance Function Selection
3. Flow Correlation

To detect correlated flows, information needs to be collected (e.g. arrival time using tcpdumb or NetFlow [1]) about the incoming and outgoing flows. Then those arrival times need to be compared. The arriving times form a series with $A_i = (a_{i,1}, ..., a_{i,n})$ at the input and $B_i = (b_{i,1}, ..., b_{i,n})$ [21]. The similarities between those flows, are measured, by applying distance functions. It can be assumed, that the smaller this distance is, the more similar the packets are. This is the most important part of flow correlation detection and can be done in different ways (depending on the technology which is used to determine the similarities between two flows). The last step simply takes those flows with the minimum distance and identify them as correlated.
Generally, network flows correlation can depend on three characteristics [17]:

- host activity, which records every user login.
- And/or connection content, for example packet payload.
- And/or connection timing, that is the arrival and departure time of each packet.

CNFD can address one or more of these points.

3.1 Correlation Detection Based On Host Activity

This technique monitors the logins of an user on stepping stones. It is an passive traffic monitoring technique.
If the login information of e.g. 5 hosts is known, it is not that difficult to determine, whether there is a correlation or not. As described above, an attacker knows this problem and would try to manipulate the logins. The funny thing is, that he has the authority to do that, because every stepping stone used by an intruder, has been compromised earlier by him. As soon, as an attacker has the authority over an host, he/she can manipulate the login information.
The best known representatives for this technique are DIDS [14] and CIS [10]. Distributed Intrusion Detection System (DIDS) is the oldest approach, first published in 1991 in [14]. It is a network wide intrusion detection system with a centralized DIDS director and monitored hosts in the DIDS

doi: 10.2313/NET-2011-07-2_13

domain. Each host collects information about ingoing and outgoing flows and sends this information to the DIDS director for analysis. The system keeps tracks of all movements of the users in the DIDS domain, concerning all TCP connection in this domain. Caller identification system (CIS) is aimed to authenticate an users identity. If a user logs into several hosts, each hosts asks the previous one, where the user came from and receives a list of all visited hosts. The last host in the conenction chain, knows where the user came from originally. If an attack happens to the last host, the users identity can be tracked back to the first host in the connection chain, and the attacker can be verified.
The host based approach is based upon trust of the monitored hosts. If one host is compromised, the whole idea behind host based approach fails. As mentioned before, an attacker does have authority over the hosts, so he can easily manipulate them.
There is also another technique known, which uses the host-based approach for detecting correlated networks, but this technique should not be applied because it's illegal. The US Air Force used this technique to trace intruders by breaking into the hosts the same way as the intruder did but this time backwards, applying the same techniques and methods as the intruder did. This technique is called Caller ID [19]. In contrast to DIDS and CIS, Caller ID is an active traffic analysis technique.

3.2 Correlation Detection Based On Connection Content

Connection Content, that is the payload of the each connection, is of course a good characteristic, and probable it is unique enough to identify correlated flows. But this is only possible, if the connection is not encrypted. In cases, where the connection is encrypted, the content does not reveal to much information. This approach can be neglected, as the flow is mostly encrypted. Encryption has the property, to create a completely different output, otherwise it would not be a good encryption algorithm. In addition, a good encryption algorithm creates a one-way function, that means that, given the output, it is computationally infeasible to determine the input. So, for correlation detection purpose, this approach is not helpful. Nevertheless there are techniques for correlation detection based on connection content in unencrypted traffic, like in Thumbprinting[15].
In Thumbprint a function is applied to the connection, which can distinguishes a given connection from all other ones but returns the same value over related connections. All participating hosts store this thumbprint (the unique value over a connection) and in case of an attack the stored thumbprints can be compared and related connections can be identified.

3.3 Correlation Detection Based On Connection timing

This approach is at present the most promising one. It takes the arriving and departure times of packets. The best known representatives are IPD-based [18] and ON/OFF-based [20] techniques.
The IPD-based approach takes the inter-packet arrival times of packets for correlation detection. These timings do not differ across the stepping stones [17]. In IPD-based, the timestampes of packets are measured and stored in a vectors.

Table 1: Overview Correlation Detection Approaches

	Passive	Active
Host-Based	DIDS, CIS	Caller ID
Content-Based	Thumbprinting	
Timing-Based	ON/OFF	IPD-Based

A correlation point function (CPF) compares two flows X and Y with their two timestamp vectors. If $max(CPF(X,Y))$ is greater than a threshold δ then the two flows X and Y can be considered related.
The ON/OFF-approach is based on ON and OFF periods of network traffic. The ON period starts, every time a packet appears on a network. It proceeds, until there are no packets traversing the network for at least T seconds, then the OFF period begins[20].
The reason, why ON/OFF periods are very interesting for correlation detection, is that it reveals keystroke interactions [20].
It has been discovered that keystroke inter arrivals produce always significant OFF periods. For example: 25% of interactive traffic arrives 500 msec or more appart, and 15% even 1 sec or more apart [20]. In other words: interactive traffic will always produce clear OFF periods. [17].
This approach has also an important advantage over the content based one. To detect similarities in the connection there is no need to know the content, but only the arriving and leaving time at a host. This method can thus be applied to encrypted traffic.
Of course an attacker can try to manipulate the timing by introducing delays. As described above, an attacker has the authority over stepping stones, and thus can change the timing-characteristics of packets. The result can be, that unrelated flows become suddenly related [17].
Watermarked-based techniques to detect correlated network flows are robust against those modifications on timing characteristics of packets and represent a new approach to CNFD.

4. WATERMARKS

Watermarks constitute a technique to recognize similarities in network flows, by using the timing-based approach on encrypted packets. In watermarking, a router "watermarks" a flow by adjusting the *timing-information* by applying delays of selected packets in a flow [17]. After the watermarking, the flow passes different distortions, described in 2.4, in a network. Finally, the watermarked flow arrives at a "detector", who knows the original flow and the shared secret parameters between the detector and the watermarker. The detector applies the same modification to the timing of the packets as the watermarker. If the resulting pattern is the same, the two flows can be considered correlated (see Figure 4).
Watermarking can achieve a detection rate by almost 100% and a pattern correlation by almost 0% [17]. This two rates are called true positive *tp* and false positive *fp* [17].
Compared to passive monitoring analysis, watermarking requires less computation and thus is more scalable. In passive techniques n incoming flows need to be compared with m outgoing flows to identify similarities. Therefore, $O(nm)$ computations are needed. Watermarking on the other hand only needs $O(n)$ computations and $O(1)$ for the shared key.

doi: 10.2313/NET-2011-07-2_13

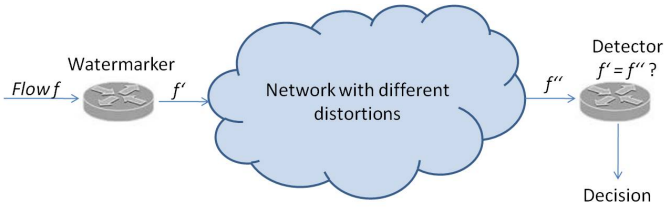


Figure 4: Network Flow Watermarking

As described above, intruders can modify the timing of packets in a flow. Here watermarks have an advantage over passive timing-based approaches, by being resistant against this kind of counter measurements by an attacker, as the detecter would recognize a timing perturbation on the flow. An attacker can perhaps identify the watermarking pattern applied to the flow, but he does not know the secret parameters, and thus can't corrupt watermarks.

In the following, two techniques are described for correlation detection using watermarks: Interval-Based Watermarking Scheme and SWIRL. Both techniques work on intervals and are therefor robust to packet losses. In addition to that SWIRL is a invisible watermark because the insertion of watermark is not noticeable to outstanders. This makes SWIRL at the moment the most interesting approach in correlation detection with watermarks.
Interval based approaches divide the flow into T intervals and applie different patterns depending on the timing of the packets.

Interval-Based Watermarking Scheme

In Interval-based watermarking, the flow is devided into intervals and watermarking is done by manipulating the rate of the traffic in intervals. For watermarking, there are two options: *clearing* and *loading*. Clearing means, that an Interval I is cleared by delaying all packet from it. Loading means, that an interval is loaded by delaying all packets from the previous interval to the current.
Watermarking:
To insert Bit 0 in position i, the packets in interval I at position i are delayed and the next interval gets the packets from the previous one. To decode Bit 1 at position i, all packets from interval I at position *i-1* are delayed to the next interval (see Figure 5).
Detection:
The detector checks for existence of watermarks, as he knows the secret parameters such as the list of positions S and the interval lengths T.
Advantage:
This approach is robust to repacketization and losses.

SWIRL: Scalable Watermark that is Invisible and Resilient to packet Losses

[4]
As the title may suggest, this watermark approach can be applied to large scenarios, as it needs less computation and communication time. It is also invisible, because of small amount of distortion, that makes a multi flow attack impossible and it is resilient to packet losses [4]. **Watermarking:** First, a flow is divided into a set of intervals of length T. For

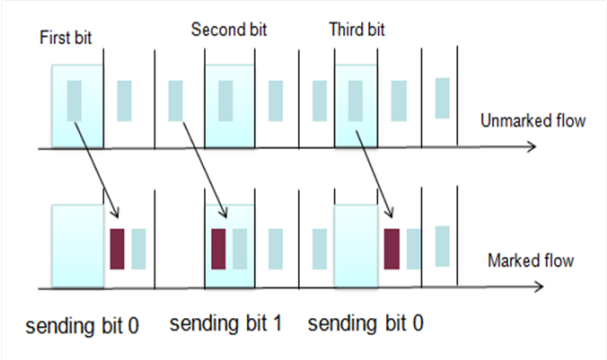


Figure 5: Interval-Based Watermarking

this kind of watermarking, there are two intervals needed: a mark and a base interval. It is completely irrelevant which one is the base and which one the mark intervals. As soon as they are determined, they are fixed for the whole flow. The base interval needs to come before the mark intervals, no other restrictions apply [4].
The mark interval is subdivided into r subintervals of length T/r [4]. Then the subintervals are again subdivided into m slots, which contain packets (or not) (see Figure 6) [4].
One of the secret parameters between the watermarker and the decoder is the permutation which is now applied. After applying the permutation, each packet is delayed, such that it falls into designated slots[4] (compare Figure 6). The grey slots are the result of the applied permutation. For the first subinterval that means, that all packets in the first subinterval should appear in slot 1 (that's the grey slot in subinterval 1). For the next slot, all packets should appear in 0 of subinterval 2, but there are no packets before this slot, so it remains empty. This is continued again, until all packets are in their designated slot.
Decoding:
The detector analyses the packets in the base interval, applies the permutation function and knows how the mark interval should look like. He then determines if the watermark is detected or not.
Advantage:
It could have been shown, that SWIRL can be applied to flows as short as 2 minutes with error rates in order of 0.000001 or less[4].
Table 1 compares the watermarking approaches according to robustness against losses and invisibility.

4.1 Applications

Stepping stones and anonymous communication systems are the particular applications of the presented correlation detection techniques, especially for watermarks. Following is described, how watermarks can be applied on both.

4.1.1 Anonymous Communication System

As a number of input flows enter the anonymous communication system, they are mapped to a number of output flows. But, how the flows are related is not known to outstanders. Tor is one example of such a system described in Section 2. The main objective of an attacker is to spy out, how the input and output flows are related. Watermarks in this case

doi: 10.2313/NET-2011-07-2_13

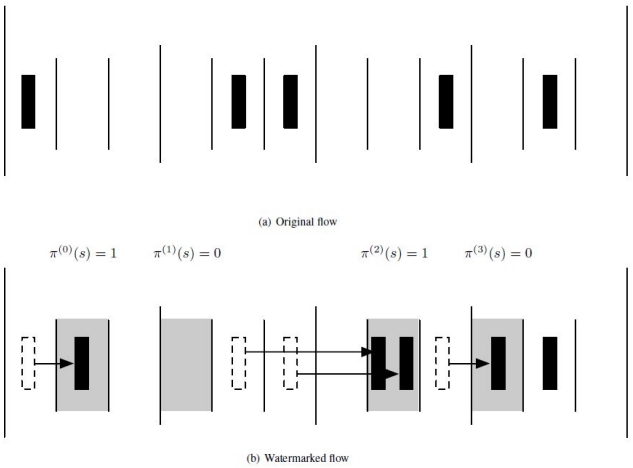


Figure 6: SWIRL (adopted by [4])

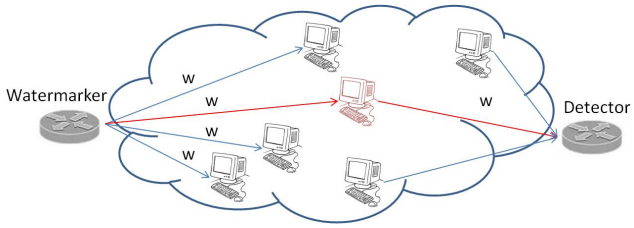


Figure 7: Stepping Stone Detection (adopted by [4])

are also called a privacy-invasive tool, because they can find out, which flows are related, because of the marks applied to incoming flows and spotted at outgoing flows.
An invader can detect such correlations by compromising an entry router in Tor (see Figure 1), then the flows are marked and detected on cooperating exit routers. Watermarking makes the attack much more efficient, since only *O(n)* instead of *O(nm)* computations (see Section 3) are needed, compared to other passive detection techniques.

4.1.2 Stepping Stones

Stepping stones were described earlier (see Section 2). The situation can be compared to the anonymous communication systems, because the incoming traffic has to be compared to the outgoing traffic. As shown in figure 10, the border routers are inserting watermarks on incoming flows, and the corresponding router is checking for watermarks on outgoing flows. Again, this can be done by passive traffic analysis but as stated before, watermarking gives a more efficient approach for detection.

5. CONCLUSION

This paper was intended to give an overview over correlation detection techniques, especially by using watermarks to detect similarities in network flows. Correlation detection is a traffic analysis method that can be applied for intrusion detection.
Correlations can be found in anonymous communication systems but also in stepping stones. The watermarking approach is based on introducing timing-delays to packets in a flow. Intrusion detection can be done in other ways, than by watermarking flows, but that is much more expensive and is very difficult to apply to large networks. Watermarking on the other hand gives a new approach on detecting correlated flows, as it is more scalable and produces less errors. By using interval-based watermarks, lower error rates are produced and they are not as vulnerable to packet droppings. The most promising one by now is SWIRL, because of its low error rates and high correlation detection. Furthermore it is invisible to attackers and can be applied to large networks.

6. REFERENCES

[1] Cisco systems inc. netflow services solutions guide.
[2] Rmon: Remote monitoring mibs.
[3] Remote monitoring, internetworking technologies handbook, 1992-2006.
[4] H. Amir and N. Borisov. Swirl: A scalable watermark to detect correlated network flows. 2011.
[5] A. Blum, D. Song, and S. Venkataraman. Detection of interactive stepping stones: Algorithms and confidence bounds. *Recent Advances in Intrusion Detection*, pages 258–277, 2004.
[6] A. Cecil. A summary of network traffic monitoring and analysis techniques. visited on May 15, 2011.
[7] A. Deb, G. J. Maria, J. Goujun, and T. Brian. An infrastructure for passive network monitoring of application data streams. *Proceedings of the 2003 Passive and Active Monitoring Workshop*, 2003.
[8] D. Dingledine, N. mathewson, and P. Syverson. Tor: The second generation onion router. *Proceedings of the 13th USENIX Security Symposium*, August 2000.
[9] D. Donoho, A. Flesia, U. Shankar, V. Paxson, J. Coit, and S. Staniford. Multiscale stepping-stone detection: detecting paris of jittered interactive streams by exploiting maximum tolerable delay. *International Symposium on Recent Advances in Intrusion Detection*, 2516:17–35, October 2002.
[10] H. Jung. Caller identification system in the internet environment. *Proceedings of 4th USENIX Security Symposium*, 1993.
[11] Z. Marcia and L. B. B. Using passive traces of application traffic in a network monitoring sytem". *IEEE Computer Society*, 2004.
[12] A. Pfitzmann and M. Waidner. Networks without user observability - design options. *Computer and Security*, 6 (2):158 – 166, 1987.
[13] J. Raymond. Traffic analysis: Protocols, attacks, design issues, and open problems. *Designing Privacy Enhancing Technologies*, pages 10–29, 2001.
[14] S. Snapp. Dids (distributed intrusion detection system) - motivation, architecture and early prototype. *Proceedings of 14th National Computer Security Conference*, 1991.
[15] S. Staniford-Chen and L. Heberlein. Holding intruders accountable on the internet. *Proceedings of the IEEE Symposium on Security and Privacy*, 1995.
[16] X. Wang, S. Chen, and S. Jajodia. Network flow watermarking attack on low-latency anonymous communication systems. *IEEE Symposium on Security and Privacy*, pages 116–130, 2007.

doi: 10.2313/NET-2011-07-2_13

[17] X. Wang and D. Reeves. Robust correlation of encrypted attack traffic through stepping stones by manipulation of interpacket delays. *Proceedings of the 10th ACM conference on Computer and communication security*, page 20, 2003.

[18] X. Wang, D. Reeves, and S. Wu. Inter-packet delay-based correlatioin for tracing encrypted connections through stepping stones. *7th European Symposium on Research in Computer Security*, 2002.

[19] K. Yoda and H. Etoh. Finding a connection chain for tracing intruders. *6th European Symposium on Research in Computer Security*, 2000.

[20] Y. Zhang and V. Paxson. Detecting stepping stones. *Recent Advances in Intrusion Detection*, pages 258–277, 2004.

[21] Y. Zhu, X. Fu, B. Graham, R. Bettati, and W. Zhao. On flow correlation atttacks and countermeasures in mix networks. *Privacy Enhancing Technologies*, pages 207–225, 2005.

doi: 10.2313/NET-2011-07-2_13

Verkehrsmenge und Caching von Videos

Adrian Schnell
Betreuer: Dr. Heiko Niedermayer
Hauptseminar - Innovative Internettechnologien und Mobilkommunikation, SS2011
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: schnell@in.tum.de

KURZFASSUNG

Das Web 2.0, speziell Videodienste, erzeugen einen unvorstellbar viel Datenverkehr. Um die Inhalte trotzdem schnell und kostengünstig an Benutzer ausliefern zu können, werden drei verschiedene Caching Verfahren vorgestellt. YouTube selbst setzt ein CDN [1] (Limelight Networks) ein, um die Informationsflut den Nutzern bereitstellen zu können.

Schlüsselworte

Verkehrsmenge, Caching, Streaming, Videos, YouTube, content distribution network

1. EINLEITUNG

Durch die zunehmende Verbreitung und Nutzung des Web 2.0 und der dadurch stark wachsende benutzergenerierte Inhaltsflut durch soziale Netzwerke wie Facebook, Flickr, My Space, Twitter und YouTube entstehen neue Probleme. Zum einen müssen diese Daten gespeichert werden, aber auch wieder den Nutzern zur Verfügung gestellt werden. Dabei entstehen jeweils Kosten, die man versucht möglichst gering zu halten. Im Folgenden werden die Probleme durch den wachsenden Datenverkehr sowie Lösungen besprochen.

Besonders soziale Netzwerke, wie Facebook oder Google Plus, fördern stark die Verbreitung von Medieninhalten wie Videos und Bildern. Im Januar 2011 waren 600 Millionen aktive Benutzer weltweit auf Facebook zu verzeichnen [9], die untereinander stark vernetzt sind und Nachrichten, Internetseiten, Fotos, Blogs und auch Videos teilen. Durch dieses sogenannte „friend-casting“hat es Facebook inzwischen sogar geschafft, den Internetgiganten Google vom Thron der meist aufgerufenen Internetseite zu stoßen [7].

Dieser Artikel ist wie folgend aufgebaut. Kapitel 2 geht auf näher auf YouTube, dessen Entstehung und technische Funktionsweise ein. In Kapitel 3 wird ein Versuch unternommen, die gespeicherte Datenmenge von YouTube zu schätzen. Diese Ergebnisse werden in Kapitel 4 verwendet, um die Verkehrsmenge von YouTube grob einzuordnen. Kapitel 5 führt verschiedener Cachingstrategien auf und Kapitel 6 erläutert den Einsatz eines CDN. Beide haben die Aufgabe, die genutzte Bandbreite von Dienstleister und ISP[2] zu reduzieren sowie die Daten schneller an den Benutzer auszuliefern. Kapitel 7 fasst die Ergebnisse zusammen und liefert einen Ausblick.

[1] content distribution network
[2] internet service provider

2. YOUTUBE

2.1 Entstehung

YouTube ist eine der größten und erfolgreichsten Internetseiten, laut dem Ranking von Alexa liegt YouTube auf Platz zwei der am schnellsten wachsenden Websites im Internet [2]. Laut einer älteren Studie von Nielsen Netratings von 2006 wuchs YouTube alleine in einer Juliwoche 2006 um 75% von 7,3 auf 12,8 Millionen Usern [10].

Bei YouTube handelt es sich um eine Webcommunity zur Bereitstellung von Kurzvideos und deren Bewertung und Kommentierung. Gegründet wurde YouTube 2005 in San Bruno, Kalifornien. Aufgekauft wurde YouTube bereits 2006 von Google für umgerechnet etwa 1,3 Milliarden Euro [14].

Bereits März 2008 stellte das Marktforschungsinstitut *Hitwise* fest, dass 73% aller Besucher von Videoportalen in den USA YouTube zuzuordnen sind [14].

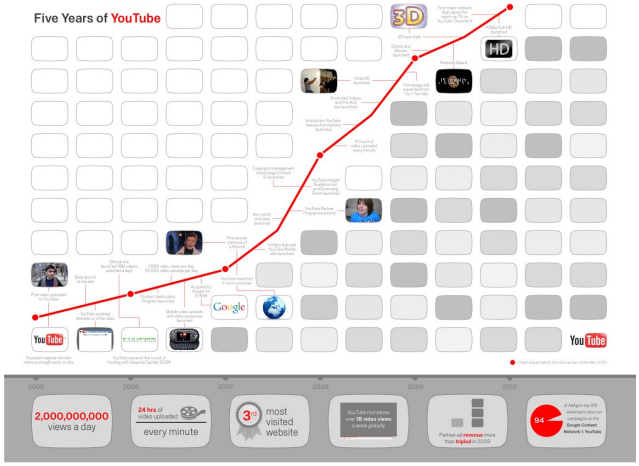


Abbildung 1: Weiterentwicklung von YouTube anhand einer Zeitachse, aus [15]

In Abbildung 1 sind einige der wichtigsten Eckpunkte in der zeitlichen Entwicklung von YouTube festgehalten. Unter anderem, dass 2008 jede Minute etwa 15 Stunden Filmmaterial von den Nutzern hochgeladen wurde [15]. Im Jahr 2010 ist diese Zahl bereits auf 24 Stunden pro Minute angewachsen und verzeichnet täglich bis zu zwei Milliarden Seitenaufrufe [16]. Aktuell im Jahr 2011 sind diese Zahlen erneut drastisch gewachsen. Inzwischen können drei Milliarden Seitenaufrufe

doi: 10.2313/NET-2011-07-2_14

täglich verzeichnet werden sowie 48 Stunden Videodaten je Minute [17]. Mit dazu beigetragen hat sicherlich auch das Einbetten von Videos in andere Internetseiten und soziale Netzwerke. Die Verteilung der Videos an letztere kann der Nutzer auch vollautomatisch nach dem Hochladen neuer Videodateien von YouTube übernehmen lassen.

Im Dezember 2008 startete der erste HD Dienst mit 720 Pixeln. Etwa ein Jahr später, November 2009, startete der Full HD Dienst, der Videos mit 1020 Pixeln zur Verfügung stellt [16]. Die Benutzer haben bei jedem Video die Möglichkeit, die gewünschte Darstellungsqualität selbst festzulegen. Wenn beispielsweise ein Video mit 1080 Pixeln angeboten wird, besteht zusätzlich die Auswahl von 240, 360, 480 und 720 Pixeln Auflösung.

Erst seit kurzem ist es unter *http://www.youtube.com/movies* sogar möglich, Spielfilme in voller Länge und auch teilweise in HD anzuschauen. Die Nutzung dieses Dienstes ist nach derzeit noch zum Großteil kostenfrei.

2.2 Funktionsweise

YouTube ist ein internetbasierter Dienst, auf dem Nutzer ihre Videos, für die allgemeine Öffentlichkeit oder auch nur für Freunde, veröffentlichen können.

Dabei können alle heute gängigen Videoformate wie .WMV, .AVI, .MPG, .MP4, .FLV, .MKV und .MOV bis zu einer Abspieldauer von 15 Minuten und 2 GB Datengröße hochgeladen werden.

Bisher wurden die Videos ausschließlich über den Adobe Flash Player ausgeliefert, wobei der Sorenson Spark H.263 Video Codec verwendet wurde [2]. Dies hatte den Vorteil, dass jeder Nutzer die Videos anschauen konnte, unabhängig vom verwendeten Betriebssystem oder Browser, solange das Flash Plugin installiert war. Es wird davon ausgegangen, dass über 90% der Nutzer dieses installiert haben [4].

Seit Januar 2010 experimentiert YouTube allerdings auch mit den Audio/Video Tags von HTML5. Damit lassen sich die Videos ohne das Flash Plugin abspielen und auch mobile Geräte, wie zum Beispiel iOS Geräte[3] wie das iPhone beziehungsweise iPad, sind in der Lage, HTML5 Videos abzuspielen.

Über eine Suchfunktion auf der Website, beziehungsweise Software auf mobilen Geräten, können diese dann gefunden und gestreamt werden [18]. Das Herunterladen beziehungsweise persistente Speichern der Daten ist nach YouTube Nutzerbestimmungen untersagt, sollte kein spezieller Link dazu auf der Internetseite vorhanden sein.

Um sich den Ablauf genauer vorstellen zu können, wie genau das Übertragen der Videodaten funktioniert, betrachten wir Abbildung 2. Hier ist dargestellt, wie die Kommunikation via HTTP Befehlen zwischen dem Nutzer, dem YouTube Server und dem CDN abläuft.

Jedes Video hat eine eindeutige und einzigartige 11 stellige ID zugewiesen. Hat sich der Nutzer festgelegt, welches Video

[3]mobile Geräte vom Hersteller *Apple*

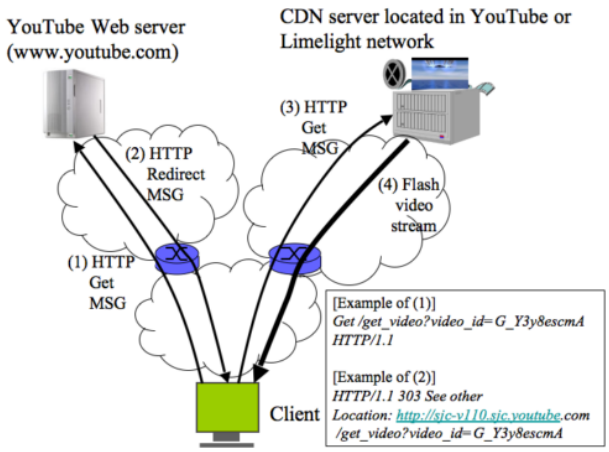


Abbildung 2: Kommunikation zwischen Nutzern, YouTube Server und CDN, aus [18]

er sehen möchte, schickt er eine HTTP Get Anfrage an den Server:
GET /get_video?video_id=G_Y3y8escmA

In dieser Nachricht fragt der Nutzer nach einem speziellen Video und überträgt dazu die Video ID, in diesem Beispiel lautet diese *G_Y3y8escmA*.

Der YouTube Server antwortet auf diese Anfrage mit einer HTTP 303 Nachricht [4] und der Umleitungsinformation:
Location:
http://sjc-v110.sjc.youtube.com/get_video?video_id=G_Y3y8escmA

Durch dieses Header Feld wird der Nutzer auf den entsprechenden Videoserver umgeleitet, von wo dann das gewünschte Video geladen werden kann.
Auf welchen Server man umgeleitet wird, entscheidet der YouTube Webserver, um damit eine Lastverteilung im System zu erreichen. Dazu benötigt er Kenntnis über den Zustand aller CDN Server, wie zum Beispiel CPU Auslastung und aktuelle Verkehrsbelastung [18]. Darauf wird in Kapitel 6 detaillierter eingegangen.

3. GESPEICHERTE DATENMENGE

Leider gibt YouTube, beziehungsweise Google, selbst keine Statistiken und Daten frei. Daher beruhen alle hier gezeigten Zahlen auf Schätzungen oder Hochrechnungen, die auf umfangreichen Versuchen und Analysen beruhen.

In einer Untersuchung der Simon Fraser Universität (Kanada) von Xu Cheng, Cameron Dale sowie Jiagchuan Liu wurde ein Datensammler [5] eingesetzt, der in den Rubriken „Recently Featured“, „Most Viewed“, „Top Rated“und „Most Discussed“, über die Zeiträume „Heute“, „diese Woche“, „dieser Monat“sowie „gesamter Zeitraum“am ersten Tag der Testreihe Videodaten gesammelt hat. Ausgelesen wurden die Metadaten über die von YouTube bereitgestellt

[4]die Fehlermeldung HTTP 303 meldet, dass die geforderten Ressourcen vorübergehend unter der im Location Feld angegeben URL erreichbar sind [13]
[5]englisch: crawler

doi: 10.2313/NET-2011-07-2_14

Entwickler API [2].

ID	Y3y8escmA
Uploader	Alkarin
Date Added	May 19, 2007
Category	Entertainment
Video Length	268 seconds
Number of Views	596.272
Rating	4,83
Number of Ratings	1.227
Number of Comments	1.475
Related Videos	wX7B2WyqhMU, ...

Tabelle 1: Die meistverwendeten Anwendungen im Inter-Domain Verkehr zwischen July 2007 und 2009 basierend auf den Protokoll Klassifizierungen, aus [6]

Anschließend wurden bei jedem der dabei gefundenen Videos die ersten 20 Vorschläge von YouTube weiter verfolgt, bis zu einer Tiefe von vier Ebenen. Dieser Vorgang wurde die darauffolgenden Wochen etwa alle zwei bis drei Tage wiederholt. Dabei wurden insgesamt 3.269.030 verschiedenen Videos zwischen dem 22.02.2007 und 18.05.2007 indiziert.

Festgehalten wurden dabei jeweils die in Tabelle 1 aufgeführten Informationen. Dabei fand man heraus, dass 97,9% aller Videos kürzer als 600 Sekunden sind und 99,1% kürzer als 700 Sekunden. Weitaus interessanter ist dabei jedoch, dass 98,3% aller Videos kleiner als 25 MB sind sowie die Durchschnittsgröße 8,4 MB beträgt [2].

Eine Wildcard Suche, also einer Suchanfrage mit „*“,ergab 2007 noch 77,1 Millionen Videos insgesamt, wodurch 650 TB Daten bereitgehalten wurden.

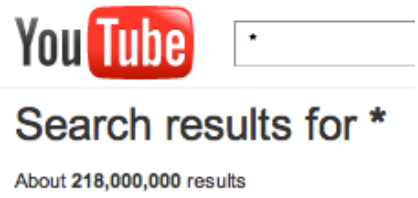


Abbildung 3: Bildschirmfoto einer Wildcard-Testsuche zur Ermittlung der Gesamtzahl der von YouTube gespeicherten Videos am 20.05.2011

Eine Wiederholung dieser Suche am 20.05.2011 ergab 218 Millionen Videos (siehe Abbildung 3). Davon ausgehend, dass sich die durchschnittliche Größe der Videos in den letzten Jahren nicht verändert hat, müsste YouTube inzwischen 1746 TB gespeichert haben. Jedoch ist von weitaus größeren Zahlen auszugehen, da inzwischen Videos in HD mit 720 Pixeln sowie Full HD mit 1080 Pixeln angeboten werden, welche weitaus mehr Speicherplatz benötigen. Genaue Zahlen dazu stehen derzeit nicht zur Verfügung.

4. VERKEHRSMENGE

In Abbildung 2 ist zu erkennen, dass im Jahr 2009 52% des Internetverkehrs auf Webanwendungen anzurechnen ist. Interessant ist an dieser Abbildung, dass Videos 2,64% ausmachen, wodurch sie in dieser Einstufung Platz zwei belegen. Protokoll- und Portanalysen geben allerdings keine volle Einsicht in die Internetnutzung, wodurch 2009 insgesamt 37% des Verkehrs nicht eindeutig zugeordnet werden konnten.

Diese Ergebnisse von den Arbor Networks sowie der Universität Michigan decken sich mit denen anderer Untersuchungen [6].

Interne Messungen bei diesen Untersuchungen ergaben, dass HTTP Videoübertragungen 25-40% des HTTP Verkehrs ausmachen. YouTube als größte aller Videoseiten nutzt zunehmend HTTP Videos und kann daher als einer der Verantwortlichen für diesen riesigen Anteil an HTTP Videos gemacht werden [6].
Dies deckt sich auch mit einer Veröffentlichung einer Studie von 2007 von Ellacoya Networks, wobei 10% des gesamten HTTP Verkehrs durch YouTube verursacht werden sollen [5].

Rank	Application	2007	2009	Change
1	Web	41,68	52,00	+10,31
2	Video	1,58	2,64	+1,05
3	VPN	1,04	1,41	+0,38
4	eMail	1,41	1,38	-0,03
5	News	1,75	0,97	-0,78
6	P2P	2,96	0,85	-2,11
7	Games	0,38	0,49	+0,12
8	SSH	0,19	0,28	-0,08
9	DNS	0,20	0,17	-0,04
10	FTP	0,21	0,14	-0,07
	Other	2,56	2,67	+0,11
	Unclassified	46,03	37,00	-9,03

Tabelle 2: Die meistverwendeten Anwendungen im Inter-Domain Verkehr zwischen July 2007 und 2009 basierend auf den Protokoll Klassifizierungen, aus [6]

Item	Image	Text	Application	Video
Responses	13.217.499	2.020.436	1.828.486	556.353
Bytes (GB)	37.58	18.59	28.93	5.787.05
% Requests	75,00	11,46	10,38	3,16
% Bytes	0,64	0,32	0,49	98,55
File Size				
Mean (KB)	3,18	18,62	5,84	10.110,72
Median (KB)	3,17	25,76	0,22	8.215,00
COV	0,29	2,31	0,66	0,97
Transfer Size				
Mean (KB)	3,08	9,60	15,97	10.332,44
Median (KB)	3,24	7,26	21,99	8.364,00
COV	0,51	1,26	0,65	0,99

Tabelle 3: korrekt übertragene Daten (HTTP Status 200) zwischen YouTube und einem Campus Netzwerk, aus [4]

In Tabelle 3 wurde zusammengestellt, welche Daten genau übertragen werden und in welchem Verhältnis sie stehen. Den größten Teil der HTTP 200 Antworten machen Bilder und Text mit 86% aus. Anwendungen wie XML und Java Script machen immerhin zusammen 10%, Videos dagegen nur 3%. Im Gegensatz dazu steht, dass Videos für etwa 98,6% der übertragenen Datenmenge verantwortlich sind [4].

doi: 10.2313/NET-2011-07-2_14

Um festzustellen, was für eine Verkehrsmenge das gesamte Internet benötigt wurde eine Studie unter 110 unabhängigen großen Providern angefertigt. Die Ergebnisse des ASN Verkehrs der größten 12 dieser Anbieter wurde in Abbildung 4 dargestellt und extrapoliert. Die dabei entstandene Gerade hat eine Steigung von 2,51, was bedeutet, dass 2,51% des Inter-Domain Verkehrs etwa 1 Tbps darstellt [6]. Damit lässt sich das gesamte Verkehrsaufkommen mit $\frac{1}{2,51} = 39,8$ Tbps im Juli 2009 berechnen [6]. Auf den Monat gerechnet ergeben das etwa 106.600.320 TB an Datenverkehr.

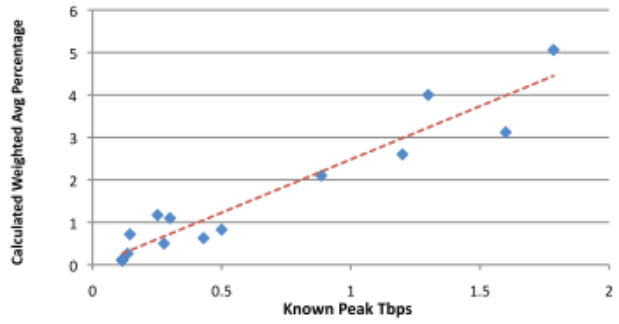


Abbildung 4: Inter-Domain Verkehr aus ASN Analysen, aus [6]

5. CACHING

Um die in Kapitel 4 aufgeführten Datenmengen bewältigen zu können und dabei die Performance aufrecht zu erhalten, müssen technische Lösungen gefunden werden.

In den folgenden Abschnitten werden verschiedene Caching Strategien aufgeführt, die dieses Problem lösen sollen. Bezug genommen wird dabei auf Simulationen der Universität Massachusetts, die den Datenverkehr zwischen Universitätsnetzwerk und YouTube protokolliert und ausgewertet haben.

Caching Strategien sind allgemein immer dann sinnvoll, wenn ein Benutzer beziehungsweise mehrere Benutzer in einem Netzwerk die selben Daten mehr als einmal aufrufen.

5.1 Lokales Caching auf Benutzerseite

Das Caching auf Benutzerseite macht dann Sinn, wenn ein Nutzer das selbe Video öfters als einmal aufruft. Eine Studie hat ergeben, dass allerdings lediglich 25% aller Videos öfter als einmal aufgerufen werden [18]. Wenn weitere Informationen mit in die Cachingstrategie einfließen, wie beispielsweise wie beliebt das jeweilige Video ist, kann die Effizienz gesteigert werden.

Um das zu testen wurde in einem Experiment von einem Nutzer mehrfach das selbe Video aufgerufen. Dabei stellte man fest, dass bei jeder Anfrage ein neuer Datenstrom vom CDN gesendet wurde. Als Schlussfolgerung kann man daher feststellen, dass weder der Browser noch der Flashplayer die Videodaten gespeichert hat [18].

Die Standardeinstellung der Cachegröße der meisten Browser liegt bei 50 MB. Wenn wir weiterhin von 7 MB je Video ausgehen, könnten etwa 7 Videos komplett im Browsercache zwischengespeichert werden. Der Nutzer würde dadurch von

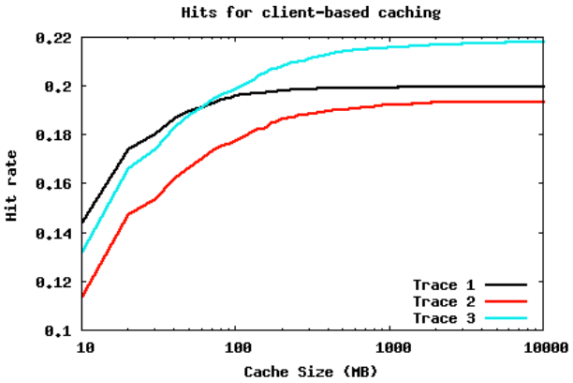


Abbildung 5: erfolgreiche Aufrufe aus dem Browsercache des Benutzers, aus [18]

einer schnelleren Startzeit der Videos sowie einer unterbrechungsfreien Wiedergabe profitieren [18].

In einer Simulation des lokalen Cachings wurde von einem Cache von 50 MB sowie einer Videogröße von 7 MB ausgegangen. Sollte der Speicher nicht ausreichen, wurde nach dem FIFO Prinzip [6] Speicher freigeräumt. Abbildung 5 zeigt die Effizienz dieser Strategie. Bereits ein kleiner Browsercache zeigt im Vergleich zu einem System ohne Cache, dass 3283 von 3899 Videos mit mehreren Aufrufen eines Benutzers von dem lokalen Cache gespeichert werden könnten. [18]

Diesen Trend haben bereits große Browserentwickler entdeckt. So wird Apple mit seinem Betriebssystem OSX Lion eine neue Version des eigenen Browsers Safari freigeben, der das Caching von Video- und Audiodaten erlauben wird [1].

5.2 Peer-to-Peer Caching

Peer-to-Peer Caching ist eine Variante von der in Kapitel 5.1 vorgestellten Caching Strategie. Bei Peer-to-Peer Caching wird auch lokal gespeichert. Wird ein Video aufgerufen, wird überprüft ob das gewünschte Video bereits lokal zwischengespeichert ist. Wenn dies nicht der Fall ist, wird innerhalb des Peer-to-Peer Netzwerkes, zum Beispiel mit Hilfe einer Hash-Tabelle oder einer Datenbank, nachgeschaut ob ein anderer Nutzer dieses Video in seinem Cache hat. Es ist jedoch möglich, dass ein Cache-Treffer im Peer-to-Peer Netzwerk erzielt wird, der entsprechende Nutzer allerdings derzeit nicht online ist. In diesem Fall wird das Video von einem der YouTube Server geladen [18].

Für die Simulation dieser Strategie wird davon ausgegangen, dass der Benutzer online ist. Dies kann festgestellt werden, indem ein Protokoll aller eingehenden und ausgehenden TCP Header angelegt wird. Bei jeder Suchanfrage für ein Video wird nachgeschaut, ob dieses Video bereits im Cache eines anderen Nutzers liegt. Diese Nutzer-Netzwerk-Aktivität wird mit einem Zeitfenster von beispielsweise 30 Minuten analysiert. Es kann dabei davon ausgegangen werden, dass der Nutzer 15 Minuten vor und nach dem Netzwerkzugriff selbst aktiv war.

[6] first in first out

doi: 10.2313/NET-2011-07-2_14

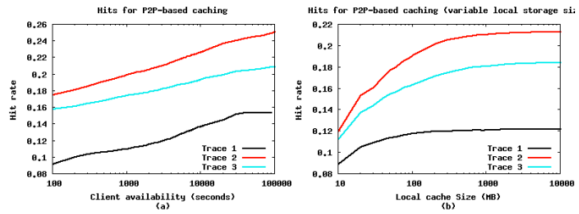


Abbildung 6: Cache Treffer bei Peer-to-Peer Caching, aus [18]

Es wurden für diese Simulation zwei verschiedenen Varianten durchgeführt. In Abbildung 6.a zeigt die X-Achse das jeweilige Zeitfenster und die Y-Achse die Cache-Treffer. In der Variante, die in Abbildung 6.b dargestellt ist, ist das Zeitfenster auf 30 Minuten festgelegt, die X-Achse zeigt hier die Cachegröße zwischen 10 MB und 10 GB an. Dabei ist festzustellen, dass ab einer Cachegröße von etwa 1 GB nur noch geringfügige Verbesserungen zu sehen sind.

5.3 Proxy Caching

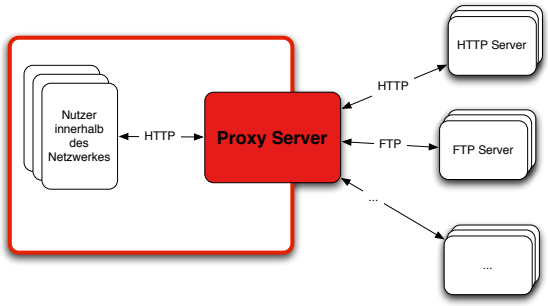


Abbildung 7: Proxy Server als Diensterbringer, nach [3]

Die dritte und letzte Caching Strategie in dieser Arbeit ist Proxy Caching. Das lokale Netzwerk, beziehungsweise der ISP, muss dabei über einen Proxy Server verfügen.

Abbildung 7 zeigt die allgemeine Funktionsweise eines Proxy Servers. Nutzer innerhalb eines geschlossenen Netzwerkes, meist hinter einer Firewall, haben nur Kontakt mit einem Proxy Server. Alle Anfragen, die von den Nutzern gemacht werden, müssen daher zunächst an den Proxy Server gesendet werden, der diese beispielsweise an FTP oder HTTP Server weiterleitet. Die Ergebnisse der Anfragen werden dann an den Nutzer zurück geleitet. [3]

Proxy Caching ist eine effizientere Caching Strategie als beispielsweise lokales Caching, da nur eine Kopie der Daten gehalten wird und damit Festplattenspeicher eingespart werden kann.

Wenn nun ein Nutzer aus diesem Netzwerk eine Anfrage an YouTube senden möchte, muss er sich zunächst an den Proxy wenden. Dieser muss feststellen können, ob dieses Video bereits im Cache liegt. Dazu können ähnlich wie bei Peer-to-Peer Caching Hash-Tabellen oder Datenbanken verwendet werden. Tritt ein Cache-Treffer ein, wird direkt an den Nutzer übertragen - im Idealfall mit der vollen verfügbaren Bandbreite.

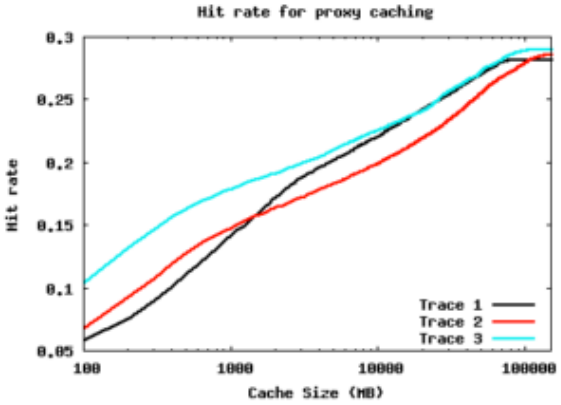


Abbildung 8: Cache Treffer bei Proxy Caching, aus [18]

Andernfalls, also falls das Video nicht im Cache liegt, gibt es zwei Entscheidungsmöglichkeiten für den Proxy Server. Zum einen gibt es die Möglichkeit, dass das gewünschte Video im Cache abgelegt werden soll. Dafür wird die Anfrage des Nutzers vom Proxy an YouTube weitergeleitet und das vom Server gesendete Video zunächst zwischengespeichert und dann direkt an den Nutzer weitergeleitet.
Die zweite Möglichkeit ist, dass sich der Proxy Server dazu entschließt, das Video nicht zu cachen. In diesem Fall wird die Benutzeranfrage nur an den YouTube Server weitergeleitet und der Nutzer erhält direkt das Video, ohne weiteres Caching [18].

Die Simulation dieses Verfahrens ist in Abbildung 8 zu sehen. Auf der X-Achse ist die Cachegröße des Proxy Server verzeichnet, die Y-Achse gibt die Cache-Treffer an.

Bereits kleine Änderungen an der Cachegröße haben dabei einen enormen Einfluss auf die Trefferquote. Bereits der Schritt von 100 MB zu 1 GB steigert die Chance auf einen Cache-Treffer um 10%. Auch eine Erweiterung des Speichers bis zu 100 GB verbessert noch das Ergebis auf bis nahezu 25%. Wie wir in Kapitel 5.1 festgestellt haben, werden nur 25% aller Videos mehr als einmal angesehen. Dadurch haben wir bei Proxy Caching mit 100 GB Cachegröße nahezu das erreichbare Maximum erreicht.

Diese Simulation bestätigt unsere Annahme, dass Proxy Caching eine sehr effektive und kostengünstige Möglichkeit ist.

Als weiteren Vorteil könnte man auch betrachten, dass Netzdienste zeitweise nicht verfügbar sind. Sollte die bereitgestellten Daten allerdings bereits im Cache des Proxy Server vorliegen, hätten die Nutzer in diesem Netzwerk trotzdem die Möglichkeit, darauf zuzugreifen [3].

Doch bei all diesen Vorteilen bietet Proxy Caching unter Umständen auch Nachteile. Nehmen wir an, wir sind in einem Netzwerk, in dem nur wenig Nutzer immer auf die selben Dienste zugreifen. In diesem Fall würden die zwischengespeicherten Daten durch den Cache-Manager, je nach ein-

doi: 10.2313/NET-2011-07-2_14

gesetzter Verdrängungsstrategie, kontinuierlich durch neue ausgetauscht. Der Proxy Server würde daher nur als Gateway zwischen Nutzer und dem Netzdienst fungieren [3].

Weiterhin wäre denkbar, dass die gespeicherten Daten zum Zeitpunkt des Abrufes durch den Nutzer bereits veraltet sind. Es gibt verschiedene Ansätze, um diesem Problem entgegen zu wirken. Es kann jedoch nicht garantiert werden, dass immer die aktuellste Version ausgeliefert wird.

5.4 Vergleich der Cachingstrategien

Alle drei hier aufgeführten Cachingstrategien sollen Netzverkehr vermindern und Vorteile für die Benutzer bringen wie verkürzte Startzeiten der Videos sowie eine unterbrechungsfreie Wiedergabe. Aber auch der Netzbetreiber wie zum Beispiel eine Universität oder ein ISP profitieren von sinnvollen Caching Strategien, es können je nach Region 40-60% Bandbreite [8] eingespart werden.

Wenn wir uns die Simulationen genauer betrachten, stellen wir schnell fest, dass sich die Verfahren in ihrer Effizienz stark unterscheiden.
Während Peer-to-Peer Caching lediglich eine leichte Verbesserung zum lokalen Caching darstellt, ist es mit Proxy Caching möglich, nahezu alle mehrfach angesehenen Videos zwischenzuspeichern und anderen Nutzern aus dem selben Netzwerk auszuliefern.

6. CONTENT DISTRIBUTION NETWORK (CDN)

YouTube untersagt laut Nutzungsbestimmungen das (persistente) Speichern der geladenen Videos. Caching dagegen, wie in Kapitel 5 vorgestellt, ist allerdings nicht persistent. In einem Cache werden nur die Datenblöcke gehalten, auf die oft zugegriffen wird.

Da der Datenverkehr von YouTube sehr groß ist, werden die Videos nicht nur von einem Server bereitgestellt. Aus diesem Grund werden die Videos von einem CDN (Limelight Networks [4]) ausgeliefert.

Bei einem CDN handelt es sich um ein stark verteiltes Netz von Servern, die über das Internet miteinander verbunden sind. Ziel dieses Netzwerkes ist es, (meist) Medieninhalte an Nutzer auszuliefern.

Ein CDN besteht aus einem Ursprungsserver, auf dem der Diensteanbieter seine Inhalte ablegt, einem Distributionssystem, das die Inhalte auf zahlreiche Replica-Server verteilt, die Kopien der Mediendaten speichern. Die Nutzeranfragen werden von dem Request-Routing-Server auf die Replica-Server weitergeleitet. Auf welchen Server weitergeleitet wird, bestimmt eine Kennzahl, die von dem Accounting-System festgelegt wird. Kriterien für die Kennzahl sind unter anderem CPU Auslastung sowie die Anzahl der aktuell aktiven Verbindungen sowie die geographische Entfernung, um die Daten möglichst nahe am Benutzer auszuliefern. In seltenen Fällen kann es auch relevant sein, ob der Nutzer für die gewünschten Dienste bezahlt hat oder nicht [12]. In Abbildung 9 sehen wir eine vereinfachte Darstellung eines CDN. Um es übersichtlich zu halten, werden hier nur die Replica-Server gezeigt.

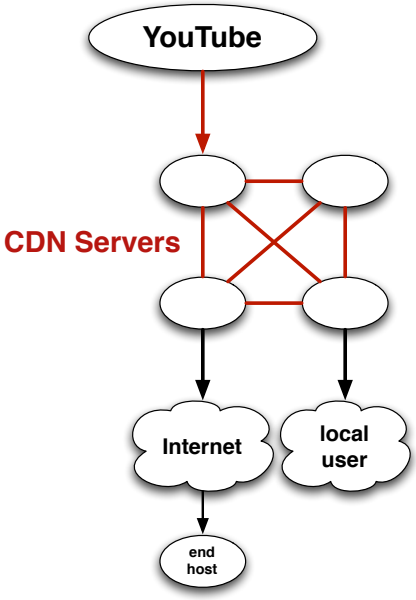


Abbildung 9: Content Distribution Network, nach [11]

Sollte ein oder mehrere der Replica Server eines solchen CDN innerhalb eines großen Netzwerkes sein, wie bisher von einer großen Universität, hätte dies den Vorteil, dass keine Internetverkehr erzeugt wird sondern die Mediadaten innerhalb des Netzwerkes verteilt werden.

Ein CDN hat also besonders dann einen großen Vorteil, wenn der Nutzer geographisch möglichst nahe an einem der Replica Servern ist.

7. ZUSAMMENFASSUNG

Wir haben gesehen, dass der Internetverkehr sehr groß ist. Im Jahr 2009 war von geschätzten 40 TB je Sekunde die Rede. Einen großen Teil davon nehmen Web 2.0 Anwendungen wie YouTube ein, die sehr große Datenmengen bereithalten. Um diese Daten kostengünstig, schnell und sicher an den Benutzer zu senden, haben wir uns verschiedene Caching Strategien angeschaut, wobei wir zu dem Ergebnis gekommen sind, dass die effektivste Möglichkeit die Daten zu Cachen der Einsatz eines Proxy Servers ist, wie er heute auch von vielen ISP betrieben wird.

Allerdings ist fraglich, in wie fern die Ergebnisse der hier aufgeführten Studien verallgemeinert werden können. Die Versuche wurden in einem großen, lokalen Netzwerk von Universitäten durchgeführt. Es ist davon auszugehen, dass Studenten ein anderes Verhalten aufweisen als der Großteil der Bevölkerung, da sie zum einen recht jung sind und daher mit der Materie Internet eher vertraut sind und das Web 2.0 vermutlich daher auch intensiver nutzen. Zum anderen sind die Gruppierungen innerhalb der Studentengemeinschaft recht groß, wodurch das „friend-casting“, also das Teilen von interessanten Inhalten schneller und in größerem Umfang statt findet.

doi: 10.2313/NET-2011-07-2_14

Weiterhin fraglich ist auch, in wie fern sich die Ergebnisse aus Kapitel 3 von der heutigen, realen Datenmenge unterscheiden. Die aufgeführten Zahlen stammen von 2007, wurden also bereits zwei Jahre vor Einführung von HD Videos auf YouTube ermittelt. Aktuell ist es möglich, Videos mit einer Größe von bis zu 2 GB auf die YouTube Server zu übertragen. In wie fern diese noch komprimiert werden war in Recherchen zu diesem Artikel nicht heraus findbar. Man kann allerdings davon ausgehen, dass die damalige Durchschnittsgröße eines Videos von 8,4 MB heute weit nicht mehr ausreichen wird.

Interessant wäre eine Kombination der hier vorgestellten Möglichkeiten zur Auslieferung der Daten und Vermindert des Datenverkehrs. Vorstellbar wäre weiterhin der Einsatz eines CDN, im Idealfall mit jeweils mindestens einem Replica Server in jedem großem Netzwerk wie Universitäten und Firmen. Wenn zusätzlich noch ein Proxy Server eingesetzt wird, könnten die Replica Server zusätzlich entlastet werden, wodurch die Performance für Nutzer außerhalb dieses Netzwerkes vermutlich steigen würde.

8. LITERATUR

[1] Apple. Osx lion. http://www.apple.com/de/macosx/whats-new/features.html#safari, 2011.

[2] X. Cheng, C. Dale, and J. Liu. Statistics and Social Network of YouTube Videos. *2008 16th Interntional Workshop on Quality of Service*, June 2008.

[3] J. Elkner. Wissenswertes über proxy caches. http://www.linofee.org/ jel/proxy/Knowledge/german.shtml.

[4] P. Gill, M. Arlitt, and Z. Li. YouTube Traffic Characterization : A View From the Edge. *Technical*, 2007.

[5] Google Blog. YouTube verursacht 10% des HTTP-Traffics. http://www.googlewatchblog.de/2007/06/youtube-verursacht-10-des-http-traffics/, Juni 2007.

[6] C. Labovitz, S. Iekel-johnson, A. Arbor, J. Oberheide, and F. Jahanian. Internet Inter-Domain Traffic. *Communication*, 2008.

[7] Online Medienbeobachtung. Social media monitoring und empfehlungsmarketing. http://www.medien-beobachtung-blog.de/tag/friend-casting/, März 2010.

[8] OpteQ. Isp web caching & netcache clusters. http://www.opteqint.net/content/isp-web-caching-netcache-clusters, Februar 2009.

[9] P. Roth. Neuer rekord: 600 millionen aktive facebook nutzer. http://allfacebook.de/news/neuer-rekord-600-millionen-aktive-facebook-nutzer, Januar 2011.

[10] B. Suzy and H. Leilani. Youtube U.S. Web Traffic grows 75 percent week over week , according to NIELSEN // Netratings. (408), Juni 2006.

[11] P. D. Tsang. Content distribution backbone network. http://mwnet.cse.ust.hk/p2pstream/research_cdbn.html, 2008.

[12] Wikipedia. Content distribution network. http://de.wikipedia.org/wiki/Content_Distribution_Network, April 2011.

[13] Wikipedia. Http-statuscode. http://de.wikipedia.org/wiki/HTTP-Statuscode, Mai 2011.

[14] Wikipedia. Youtube. http://de.wikipedia.org/wiki/YouTube, Mai 2011.

[15] Youtube. At five years, two billion views per day and counting. http://youtube-global.blogspot.com/2010/05/at-five-years-two-billion-views-per-day.html, Mai 2010.

[16] Youtube. Zeitachse. http://www.youtube.com/t/press_timeline, Mai 2010.

[17] Youtube. Thanks, youtube community, for two big gifts on our sixth birthday! http://youtube-global.blogspot.com/2011/05/thanks-youtube-community-for-two-big.html, 2011.

[18] M. Zink, K. Suh, Y. Gu, and J. Kurose. Watch Global , Cache Local : YouTube Network Traffic at a Campus Network - Measurements and Implications. *Network*, 2010.

doi: 10.2313/NET-2011-07-2_14

Smart Grids

Falco Cescolini
Betreuer: Ali Fessi
Seminar - Innovative Internettechnologien und Mobilkommunikation SS2011
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: cescolini@mytum.de

KURZFASSUNG

Für das Funktionieren einer modernen Volkswirtschaft und Gesellschaft ist eine kostengünstige und störungsfreie Stromversorgung unerlässlich. Smart Grids sind eine neue Entwicklung um diesen Aspekt der Energieversorgung zu erhalten und zu optimieren. Sie erlangen vor allem durch den jährlich steigenden Energieverbrauch und dem massiven Ausbau erneuerbarer Energien an Bedeutung, der andernfalls zu einer Instabilität im Verbundnetz führen würde. Diese Arbeit skizziert die Probleme des aktuellen Stromnetzes aus technischer und wirtschaftlicher Sicht, beschreibt die Smart Grid Technologie und zeigt ihre bisherige Verwendung anhand von Fallstudien.

Schlüsselworte

Smart Grid, Smart Meter, Telegestore, SmartGridCity, AMI, AMR, PLC, Strom

1. EINLEITUNG

Die Stromproduktion basiert derzeit hauptsächlich auf der Verbrennung fossiler Brennstoffe und der Kernspaltung in leistungsstarken Großkraftwerken. [2] Die Stromübertragung findet über ein zentrales Netz statt, das darauf ausgelegt ist unidirektional vom Energieerzeuger zum Energieverbraucher Strom zu transportieren. Ein Stromnetz ist ein Netzwerk, in dem abgesehen von den Verlusten bei der Übertragung und Transformation des Stroms genau soviel Strom erzeugt werden muss wie verbraucht wird. Zudem ist jede Leitung bezüglich der maximal übertragbaren Leistung beschränkt. Ist die maximale Übertragungsleistung des Netzes unterdimensioniert und wird die maximale Leistung eines Stromkabels überschritten, muss der Stromfluss zu dessen Schutz unterbrochen werden, was in der Regel zu einem lokalen Stromausfall führt. Die Verbraucherseite in einem Stromnetz wird als variabel angenommen. Somit muss die Erzeugerseite zu jedem gegebenen Zeitpunkt so geregelt werden, dass der erzeugte Strom mit dem verbrauchten übereinstimmt.

Wird mehr Strom verbraucht, als erzeugt, so wird die zusätzlich benötigte Energie aus der Rotationsenergie der Turbine entnommen. Durch die verminderte Drehgeschwindigkeit sinkt die erzeugte Wechselstromfrequenz unter die vom European Network of Transmission System Operators for Electricity (ENTSO-E) vorgeschriebenen 50Hz. [20] Wird weniger Strom verbraucht als erzeugt, so sinkt der Widerstand, gegen den die Turbine ankämpfen muss. Das führt zu einer Erhöhung der Drehzahl der Turbine und als Folge zu einer Erhöhung der Wechselstromfrequenz. Beide Zustände sind unerwünscht, da sie die Turbine und den Netzzusammenhalt des Verbundnetzes gefährden und zu einem Blackout führen können.

Die Änderung der Frequenz tritt noch vor einer Spannungsänderung im Netz auf und wird daher als Indikator für eine Über- oder Unterlast verwendet. Die Abweichung vom Nominalwert 50 Hz darf maximal 800 mHz betragen. Wird dieser Wert unterschritten, wird ein Teilnetz abgeworfen, was zu einem lokalen Stromausfall führt. [20]

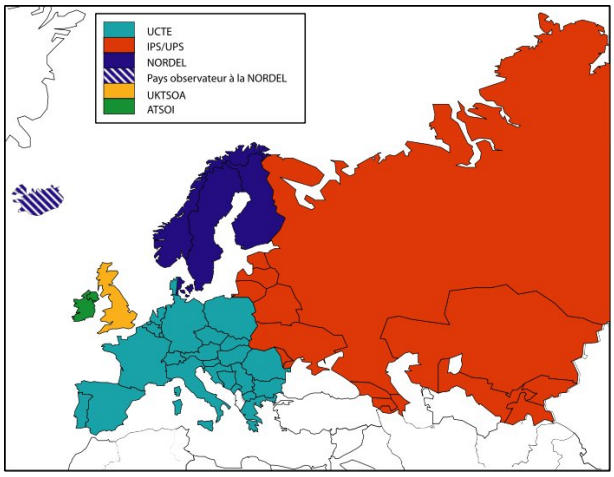


Abbildung 1: UCTE Region[3]

Um Stromausfälle zu vermeiden aen Kraftwerksbetreiber eine sogenannte Regelleistung zur Verfügung stellen, welche in Primär-, Sekundär- und Minutenregelung unterteilt ist. Die Regelleistung dient dazu, auf Lastspitzen reagieren zu können und diese störungsfrei abzufedern. Die Primärregelung beträgt für die UCTE Region (siehe Abbildung 1) 3000 MW und ist innerhalb von 15-30 Sekunden abrufbar. Dazu müssen in designierten Primärregelkraftwerken bis zu 5% der Leistung frei gehalten werden. [30] Diese Leistung bereitzustellen ist teuer aber unerlässlich.

Mit dem geplanten Ausbau der erneuerbare Energien gemäß dem „Nationalen Aktionsplan für erneuerbare Energie gemäß der Richtlinie 2009/28/EG zur Förderung der Nutzung von Energie aus erneuerbaren Quellen“ soll in Deutschland der Anteil der erneuerbaren Energien im Stromsektor bis 2020 auf 38,5% ausgebaut werden.[7] Windräder oder Pho-

doi: 10.2313/NET-2011-07-2_15

tovoltaikanlagen sind weder regelbar noch zuverlässig und dadurch wird ein weiterer Teil des Stromnetzes ähnlich variabel wie die Verbraucherseite. Zudem sind die Stromanbieter nach §3 EEG gesetzlich dazu verpflichtet den durch regenerative Quellen erzeugten Strom abzunehmen und zu vergüten[6], weswegen diese Kraftwerke bei einem Stromüberschuss nicht vom Netz genommen werden dürfen. Anbieter von konventionell erzeugtem Strom müssten somit eine höhere Regelleistung zur Verfügung stellen, um im Bedarfsfall, z.B. einer Flaute oder einem bewölkten Himmel, einen störungsfreien Betrieb zu gewährleisten. Dies senkt die Effizienz und Wirtschaftlichkeit dieser Kraftwerke und stellt eine technische Herausforderung für Kraftwerk- und Netzbetreiber dar.

Diesem Problem kann durch bessere Prognosen bezüglich des Strombedarfs und durch Möglichkeiten der Einflussnahme auf den Stromverbraucher entgegengewirkt werden. Dazu muss jedoch das derzeitige Stromnetz mittels eines bidirektionalen Kommunikationssystems zwischen Erzeugern und Verbrauchern zu einem Smart Grid erweitert werden.

2. SMART GRIDS

Abbildung 2: Smart Grid Übersicht [5]

In einem Bericht des Electric Power Research Institute (EPRI) an das amerikanische National Institute of Standards and Technology (NIST) wird der Begriff „Smart Grid“ definiert als „eine Modernisierung des Stromnetzes, so dass es den Betrieb seiner miteinander verbundenen Elemente überwacht, schützt und automatisch optimiert - vom zentralen und verteilten Erzeuger über das Hochspannungs- und Verteilernetz bis hin zu industriellen Verbrauchern, Gebäudeautomationssystemen, zu Energiespeichereinrichtungen und Endverbrauchern, deren Thermostaten, elektrischen Vehikeln, Apparaten und anderen Haushaltsgeräten“ [11]. Weiter wird ausgeführt, dass „ein Smart Grid sich durch einen bidirektionalen Energie- und Informationsfluss auszeichnen wird, um ein automatisiertes und weit verteiltes Stromnetz zu ermöglichen. Es integriert die Vorteile von Verteilten Systemen, um Echtzeitinformationen zu übermitteln und ein beinahe augenblickliches Gleichgewicht zwischen Zufuhr und Nachfrage auf Geräteebene zu ermöglichen“ [11].

Abbildung 2 stellt ein Smart Grid schematisch dar. Es basiert meist auf einer AMI (Advanced Metering Infrastructure), welche mit Sensoren an Transformationsstationen und Smart Metern ausgestattet ist und die benötigte Telekommunikationsinfrastruktur bereitstellt.

Smart Grids übernehmen üblicherweise nicht nur die automatische Stromregulierung sondern bieten auch Schnittstellen zu elektronischen Strommärkten an, was den Stromhandel beschleunigen und erleichtern soll.

Eine weitere Besonderheit ist, dass durch Smart Grids virtuelle Kraftwerke möglich sind. Das sind mehrere Kraftwerke, welche meist an unterschiedlichen Orten stehen und aus verschiedenen regenerativen Energiequellen Strom gewinnen. Der Vorteil dabei ist, dass sich das Verhalten eines virtuellen Kraftwerks im Schnitt dem eines konventionellen Kraftwerks annähert und sich so wetterbedingte Leistungsänderungen besser kompensieren lassen.

Auch im Bereich der elektrischen Fahrzeuge können Smart Grids eine wichtige Rolle spielen. Hierbei geht es in erster Linie um eine für das Stromnetz optimale „Betankung“, also um eine Entlastung zu Spitzenlastzeiten, und um eine Infrastruktur, die es ermöglicht, an einem beliebigen Ort das Auto aufzuladen und die Stromabrechnung trotzdem einfach und korrekt umzusetzen.

Zu guter Letzt kann ein Smart Grid bis hin zu einzelnen Geräten in einem privaten Haushalt reichen. Damit könnte es regelnd auf große Stromverbraucher wie Klimaanlagen, Boiler und Waschmaschinen einwirken, sofern diese das unterstützen. Dazu muss aber meist das Home Area Network (HAN) mit dem Datennetz des Stromanbieters verbunden werden.

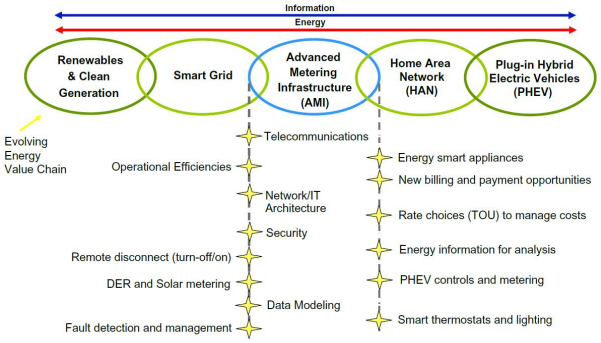


Abbildung 3: Smart Metering im Zentrum der Smart Grid Entwicklung [12]

Die in diesem Abschnitt behandelten Begriffe wie Smart Grid, AMI und HAN sind - wie in Abbildung 3 verdeutlicht wird - oft eng miteinander verflochten, beschreiben aber eigenständige Sachverhalte. So kann z.B. eine AMI auch ohne Smart Grid existieren und einzelne Smart Grid Technologien können auch ohne ein AMI realisiert werden.

2.1 Stromnetze

Das Stromnetz besteht wie das Internet aus verschiedenen und verschiedenartigen Teilnetzen. Die Teilnetzarten unterscheiden sich vor allem durch ihre Spannung und werden gemäß dieser kategorisiert. An ihren Übergängen sorgen Transformatoren für die Umsetzung der Spannung. Die Transformator Station, welche mit dem Kunden über eine Niederspannungsleitung () verbunden ist wird im Englischen „secondary station“ oder „LV station“ (LV = Low voltage)

doi: 10.2313/NET-2011-07-2_15

genannt. Das Umspannwerk, das mit einem Hochspannungsnetz auf der einen Seite und über eine Mittelspannungsleitung mit mehreren LV Stationen auf der anderen Seite verbunden ist wird „primary station“ oder MV station (MV = Medium Voltage) genannt. Daneben gibt es noch Hoch- und Höchstspannungsnetze, die aber in dieser Arbeit nicht weiter betrachtet werden.

2.2 Smart Meter

Um einen Großteil der Funktionen eines Smart Grids realisieren zu können, müssen die Stromkonsumenten mit Smart Metern ausgerüstet werden. Ein Smart Meter ist ein netzwerkfähiger Stromzähler und Sensor. Es implementiert AMR (Automated Meter Reading - Remote-Zählerablesung) Funktionalitäten, ermöglicht die Anbindung an eine und ist Teil einer AMI (Advanced Metering Infrastructure) und stellt meist einen Abschaltmechanismus zur Verfügung, mit dem das Energieversorgungsunternehmen oder der Netzbetreiber einen Kunden gezielt vom Netz nehmen kann. Smart Meter können außerdem eine Schnittstelle zwischen dem Datennetz des Energieversorgers und dem „Home Grid“ bzw. Home Area Network (HAN) realisieren.

2.3 Netzwerktechnologien

Eine der größten Schwierigkeiten bei der Gestaltung eines Smart Grids liegt darin, die zentrale IT eines Energieversorgers mit allen für ihn wichtigen Knoten des Smart Grids, insbesondere den Smart Metern, zu verbinden. Diese können laut Thilo Sauter und Maksim Lobashov auf drei verschiedene Arten verbunden werden[29].

1. Der Energieversorger verlegt eigene Datenkabel zum Kunden oder Netzwerkknoten. Dies funktioniert nur unter der Annahme, dass der Versorger bereits einen Zugangspunk zu seinem Netz in der Nähe hat. Das könnte zum Beispiel eine schon in das Smart Grid eingebundene LV Station sein. Diese Verbindungsart bietet die Vorteile einer hohen Bandbreite, Unabhängigkeit von Telekommunikationsanbietern und eine permanente Verbindung, ist aber in der Regel zu teuer. Eine Variante hiervon ist eine Funknetzverbindung einzurichten, welche jedoch in ihrer Ausdehnung limitiert ist.

2. Der Energieversorger verwendet das schon bestehende Netz eines Telekommunikationsanbieters. Dabei können beliebig kabellose Standards wie GSM oder WiMAX oder kabelgebundene wie ISDN gewählt werden. Vorteilhaft hierbei ist die meistens schon existierende Infrastruktur. Existiert sie noch nicht, muss das Energieunternehmen die Infrastruktur selbst bereitstellen und es ergibt sich dasselbe Problem wie in Punkt 1. Nachteilig bei dieser Variante sind die zusätzlichen laufenden Kosten, eine meist geringe zur Verfügung stehende Bandbreite, sowie die Abhängigkeit von einem Telekommunikationsanbieter im Störungsfall.

3. Der Anbieter nutzt seine schon bestehende Stromkabel Infrastruktur zu Datenübertragung. Diese Variante wird „Power Line Communication“ (PLC) genannt. Weitere gebräuchliche Bezeichnungen für diese Technik sind „Power line Digital Subscriber Line“ (PDSL), „Broadband over Power Lines“ (BPL) oder im Heimnetz PowerLAN. Das Stromnetz des Versorgers muss dabei nur mit einigen zusätzlichen Netzwerkelementen erweitert werden. Dafür ist diese Methode jedoch technisch komplexer, da das Übertragungsmedium verrauscht ist und sich das Rauschen abhängig von Faktoren wie der momentanen Last, dem Wetter und an das Netz angeschlossene Geräte ändert. [22] Das Signal kann außerdem nicht über einen Transformator hinweg gesendet werden.

Sauter schlägt vor den Accespoint zum IP Netz des Anbieters an eine MV Station zu legen. Dies hat jedoch mehrere Nachteile. Zum einen kann sich die Netzwerktopologie aufgrund von Stromnetzschaltungen jederzeit ändern und das System muss damit in Echtzeit umgehen können. Zum anderen kann eine Primärstation mit zehntausenden Netzwerkknoten konfrontiert sein, was die Bandbreite sprengen könnte.[29] Aus Sicht der zentralen Unternehmens-IT wäre es vorteilhaft, die Kommunikation TCP/IP basiert stattfinden zu lassen. Die von den Versorgerunternehmen verwendeten SCADA Systeme basieren meist jedoch auf simplen Request/Response Mechanismen und verlangen andere Lösungen.[29].

3. CHANCEN UND RISIKEN

Wie jede neue Technologie bergen auch Smart Grids neben ihren Vorteilen auch neue Risiken und Probleme. Dieser Abschnitt wird auf beide Aspekte näher eingehen.

3.1 Einflussnahme auf den Verbrauch

Durch Smart Grid Technologien haben die Stromversorger die Möglichkeit erhalten, Einfluss auf den Stromverbrauch zu nehmen. Bisher ging das nur in sehr bescheidenem Ausmaß, wie dem Angebot von Nachtstromtarifen oder der Komplettabschaltung eines Netzsegments. Insbesondere Smart Meter ermöglichen es nun über direkte und indirekte Maßnahmen, den Verbrauch vor allem zu Spitzenlastzeiten zu reduzieren.

Die indirekten Maßnahmen umfassen Tarifmodelle, die von der zeitnahen Kommunikation mit den Smart Metern und deren flexiblen Programmierung profitieren. Sie sollen den Verbraucher auf freiwilliger Basis durch Preisanreize zur Reduzierung seines Verbrauchs zu Spitzenlastzeiten veranlassen. Die einfachste Variante sind weiterhin die sogenannten zeitgesteuerten TOU (Time of Use) Tarife, bei welchen je nach Tageszeit, ähnlich wie beim Nachtstrom, der Preis angepasst wird. Anders ist jetzt jedoch, dass der Tarif nun pro Tag feiner unterteilt werden kann oder Abhängigkeiten von Jahreszeiten oder von Wochenend- oder Feiertagen realisiert werden können. Eine weitere Tarifoption sind Peak Time Rebates (PTR), welche den Verbraucher dafür belohnen nur eine bestimmte Anzahl an kWh zu einer vorher definierten Spitzenlastzeit verbraucht zu haben. Bei Critical Peak Price (CPP) Tarifen kann der Stromversorger eine pro Jahr begrenzte Anzahl an Critical Peak Time Events ankündigen. Dies geschieht üblicherweise einen Tag im voraus per E-Mail und bedeutet eine extrem starke Preiserhöhung für einige wenige Stunden. Der Verbraucher soll so dazu animiert werden in dieser Zeit keinen Strom zu nutzen und erhält dafür Rabatte zu anderen Zeiten. [25]

doi: 10.2313/NET-2011-07-2_15

Anders als bei den indirekten Maßnahmen greifen Demand Response Verfahren direkt auf die Geräte des Verbrauchers zu. Dies kann z.B. über den bidirektionalen Kommunikationskanal des Smart Meters geschehen. Der Stromversorger kann dabei Klimaanlagen, Boiler oder andere große Stromverbraucher des Kunden temporär abschalten, um seine Last in Spitzenlastsituationen zu verringern.[31]

Eine gänzlich andere Maßnahme ist den Stromkunden bezüglich seines Verbrauchs zu sensibilisieren. Dazu versorgt meist das Smart Meter eine Displayeinheit mit Daten über den bisherigen und aktuellen Stromverbrauch und den dabei entstandenen Kosten. Die Displayeinheit zeigt dem Kunden zudem Möglichkeiten zur Verbrauchsreduzierung auf und bringt ihn so dazu, Energie zu sparen.[31]

3.2 Erwarteter Nutzen

Bei der bisherigen Betrachtung ist die Frage nach der Rentabilität eines Smart Grid Ausbaus offen geblieben. Insbesondere muss jeder Haushalt mit Smart Metern aufgerüstet werden und eine geeignete Telekommunikationsinfrastruktur bereit gestellt werden, sofern diese noch nicht vorhanden ist. Zudem verbrauchen Smart Meter und die Anbindung an ein Datenübertragungsnetz selbst Strom und verursachen unter Umständen zusätzliche Telekommunikationskosten.

Dem gegenüber steht eine bessere Planbarkeit des Verbrauchs und eine Reduzierung der Lastspitzen. Dies führt zu einer Reduktion der bereitzustellenden Regelleistung und damit zu Kosteneinsparungen auf Seiten der Energieversorger. Sofern die preisbezogenen Maßnahmen zur Regulierung des Verbrauchs wirken, sich die Last homogener über den Tag verteilen lässt und die maximalen Lastspitzen dadurch gedrückt werden, können die Stromleitungen niedriger dimensioniert oder erst später ausgebaut werden. Das führt zu immensen Kosteneinsparungen. Nach dem ENTSO-E TYNDP (Ten-Year Network Development Plan) Plan von 2010 betragen die Kosten für Erneuerung und Ausbau von Stromleitungen in Europa 23-28 Milliarden Euro bis 2015. Dies repräsentiert jedoch nur einen Bruchteil der Kosten, die in ganz Europa für die Instandhaltung und den Ausbau des Stromnetzes erbracht werden müssen, da nationale und regionale Projekte nicht mit eingerechnet sind. [21]

Der Hauptnutzen eines Smart Grids liegt demnach bei Einsparungen und Effizienzsteigerungen auf Seiten des Energieerzeugers. Der Verbraucher wird meist nur indirekt über angepasste und variable Stromtarife davon profitieren können. Insbesondere in Hinblick auf den Ausbau der erneuerbaren Energien können Smart Grids jedoch zu Optimierungen führen, die einen Preisanstieg und eine Netzdestabilisierung vermeiden.

3.3 Sicherheit und Datenschutz

IT-Sicherheit in Smart Grids ist ein sehr komplexes Thema. Der Anschluss des Stromnetzes an und seine Steuerung über ein Datennetz birgt gewisse Risiken, denn es öffnet das System gegenüber Angriffen wie Buffer Overflows, Man-in-the-middle Attacken, DoS und DDoS Angriffen und Risiken wie Covert Channels. Zudem beträgt die Netzwerkknotenanzahl in ausgebauten Smart Grids meist mehrere Millionen und diese verteilen sich üblicherweise auf verschiedene, technologisch unterschiedliche Subnetze. Dies macht das Netz unübersichtlich und erschwert es, eine durchgehende Sicherheit zu gewährleisten. [27] Hinzu kommt, dass sich viele, eigentlich netzinterne Knoten, wie Smart Meter und einige Knoten an Transformatoren, außerhalb einer Zugangskontrolle wie Zäunen befinden und physikalisch leicht zugänglich sind.[26]

Eine Manipulation der gesendeten Daten könnte zu einer falschen Regulierung des Netzes führen, welche die Versorgungssicherheit bedrohen würde. Daher müssen geeignete Authentifizierungs- und Verschlüsselungsmechanismen bereit gestellt werden. Wegen der Größe von Smart Grids wird für die zur Verschlüsselung und Authentifizierung nötigen Zertifikate und Schlüssel eine leistungsfähige Schlüsselverwaltung benötigt.[27] Khurana führt dazu an, dass aus Laborerfahrungen gewonnene Erkenntnisse bezüglich üblicher PKI Management Software nahelegen, dass für die Pflege der PKI Daten von 5,5 Millionen Smart Metern 500 Mitarbeiter gebraucht würden, was nicht bezahlbar wäre.[26]

Zudem wird beschrieben, dass in Umspannwerken manchmal strikte Echtzeitanforderungen eingehalten werden müssen, da gewisse Multicast Nachrichten in maximal 4 ms übermittelt sein müssen. Dies stellt eine zusätzliche Herausforderung für die Authentifizierungsmechanismen dar.[26]

Die von den Smart Metern in üblicherweise 15 Minuten Intervallen erhobenen Daten können zu einem detaillierten Profil über die in einem Gebäude lebenden Personen zusammengefügt werden. Insbesondere können Gewohnheiten, Tätigkeiten, An- und Abwesenheiten und die Zeiten, an denen die Personen schlafen, daraus abgeleitet werden.[27] Informationen aus dem HAN und vom AMR können zudem genauere Informationen zu den im Haus installierten Geräten liefern. Diese Daten könnten von Kriminellen bei der Auswahl und Vorbereitung von Diebstählen verwendet werden. Im Geschäftsbereich könnten diese Informationen Rückschlüsse über die derzeitigen geschäftlichen Aktivitäten einer Firma an einen Konkurrenten liefern. [26]

Auch hier müssen geeignete Sicherheitsmaßnahmen getroffen werden, um diese Daten zu schützen.[27] Diese müssten aber erst noch genauer erforscht werden [26]

4. FALLSTUDIEN

Über das letzte Jahrzehnt hinweg gab es verschiedene Groß- und Pilotprojekte, welche Smart Grid Technologien in unterschiedlichem Umfang und Ausmaß umsetzten. Die dabei verwendeten Technologien und die angestrebten Ziele unterschieden sich dabei erheblich. Dies ist insofern keine Überraschung, da eine einheitliche Standardisierung dieses Themengebietes noch im Gange ist und bisher keine allgemein durchgesetzten, gemeinsame Standards existieren. Die nachfolgenden Kapitel enthalten drei Fallbeispiele ausgesuchter prominenter Projekte.

4.1 Telegestore Projekt von Enel S.p.A.

Enel S.p.A. („Ente nazionale per l'energia elettrica“ , S.p.A ist italienisch und bedeutet AG) ist ein italienisches, öffentliches Versorgungsunternehmen. Das Unternehmen ist nach eigenen Angaben in 40 Ländern auf 4 Kontinenten präsent und es ist in Italien der größte Stromversorger und zweitgrößte Gasversorger. Im europäischen Vergleich ist es der zweitgrößte Stromversorger gemessen an der installierten

doi: 10.2313/NET-2011-07-2_15

Nettokapazität. In Italien hat es 32,3 Millionen Kunden, davon 29,4 Millionen im Strommarkt. Weltweit versorgt Enel 61 Millionen Kunden mit Strom und Gas und besitzt eine installierte Netto-Kraftwerkskapazität von 97.000 MW (zum Vergleich: Deutschland hatte 2009 153,8 GW Netto-Kraftwerkskapazitäten [4]). [16]

Das Enel Telegestore Projekt begann 1999. 2001 wurde mit der Installation der Smart Meter begonnen, welche bis zum Ende des Projekts 2006 [23] andauerte. Das Projekt sah vor, alle Kunden in Italien innerhalb von 5 Jahren mit Smart Metern auszurüsten und diese mit dem hauseigenen AMM (Automated Meter Management) System zu verbinden, welches dadurch unter anderem AMI und AMR Funktionalitäten integriert. Die Kosten beliefen sich auf 2,1 Milliarden Euro und es wurden 32 Millionen Kunden umgerüstet.

Die Hauptziele waren unter anderem die Reduzierung der Spitzenlast, Kosteneinsparungen bei der Rechnungsstellung und bei den Betriebskosten und die Möglichkeit flexible Tarife anbieten zu können. [13]

4.1.1 Verwendete Technik

Die Smart Meter sind meist an eine LV Transformatorstation über PLC angebunden, wie Abbildung 4 zeigt. Dem Transformator ist ein Konzentrator vorgeschaltet, der bis zu 1000 Smart Meter verwalten kann. Der Konzentrator ist über GSM, PSTN oder Satellitenkommunikation mit dem zentralen AMM System verbunden. Technisch kann das System in Zukunft mit BPL erweitert werden und damit auch die Mittelspannungsleitungen zur Datenübertragung Nutzen. Dies würde das System von zusätzlichen Telekommunikationsinfrastrukturen wie GSM weitestgehend unabhängig machen. Zur Modulation im LV-Netz wurde wegen seiner Einfachheit und der geringen Kosten ein Schmalbandverfahren gewählt.[9]

Der Konzentrator wurde dahingehend entwickelt die Protokolle SITRED, ein proprietäres HDLC Protokoll, oder Lontalk für PLC zu verwenden und TCP/IP und PPP für GSM sowie PSTN Verbindungen zu unterstützen. Er hat zudem eine Verbindung zu den den drei Phasen (R,S,T) und neutral für die Kommunikation mit den Smart Metern und einen RS-232 Anschluss und einen optischen Port. [9]

Die Smart Meter können alle 15 Minuten ausgelesen werden. Sie beinhalten Techniken zur Manipulations- und Störungserkennung, können über vier verschiedene Tarife mit flexiblen Preisen abrechnen und können aus der Ferne upgedatet und abgeschaltet werden. [9]

Das System schließt gleichzeitig die LV Trafostationen an das AMM Netz an und ermöglicht so auch direkte Messungen an diesen Knoten. Es ist zudem noch genug Bandbreite vorhanden, um andere Dienste einzubinden und das Smart Meter Gas und Wasser abrechnen zu lassen. [9]

4.1.2 Ergebnis und weitere Entwicklung

Streng genommen wurde bis 2006 durch den flächendeckenden Ausbau des AMM Systems mit Smart Metern nur ein kleiner aber essentieller Teil möglicher Smart Grid Technologien implementiert Diese Maßnahme allein führte bereits zu erstaunlichen Kosteneinsparungen und Leistungssteigerungen. So konnten im Zeitraum von 2001 bis 2009 die min. Ausfallzeiten von 128 Minuten auf 49 Minuten pro Jahr und die Ausgaben pro Kunde von 80 Euro auf 48 Euro gesenkt werden. [28] 2008 beliefen sich die so eingesparten Betriebskosten auf über 500 Millionen Euro. [10]

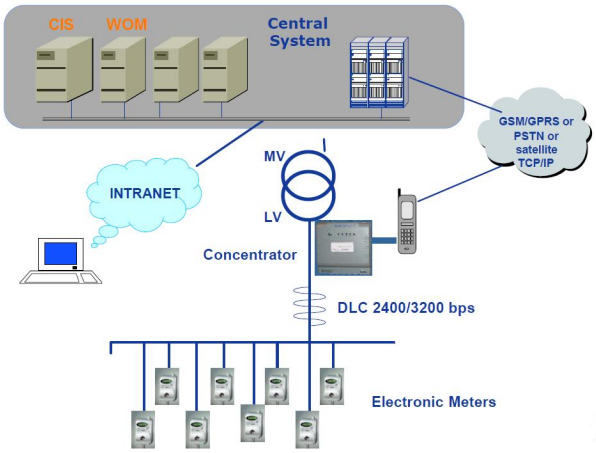


Abbildung 4: Telegestore System Architecture [8]

Enel konnte durch diese Maßnahme Tarifwechsel sofort und automatisch vornehmen. Zudem wurden verschieden Tarife auf TOU-Basis (Time of Use) angeboten. Beim „Sera“ Tarif wurde der Strompreis zwischen 19:00 Uhr und 01:00 Uhr um 16%, bei „Week End+“ am Wochenende um 22% reduziert. Bei „Otto Sette & Weekend“ zahlte man nur an Werktagen zwischen 07:00 und 20:00 Uhr den normalen Tarif und sonst 6% weniger. [8]

Das System ermöglichte außerdem eine erhöhte Aufklärungsrate bei Stromdiebstählen und ähnlichen Betrugsfällen. Technische Störungen und Ausfälle konnten durch die zusätzlichen Daten schneller lokalisiert und behoben werden.

Ein Nebeneffekt der Smart Grid Technologie soll die Sensibilisierung des Kunden bezüglich seines Stromverbrauchs sein. Enel ließ den Enel Display Market Test von einem unabhängigen Umfrageinstitut bei mehr als 1000 Familien in 50 Städten durchführen. Das Hauptziel dieser Untersuchung war ein Verständnis bezüglich dem Verhalten der Kunden gegenüber Energieüberwachungsgeräten zu erlangen. Dies ist einer der sogenannten „Indoor Energie Services“, die eine Erweiterung des Smart Grids in Richtung Home Grid darstellen. Zentraler Bestandteil dieses Projekts war ein Gerät zur Darstellung und Analyse des Energieverbrauchs, um Alarme und Optimierungsvorschläge darzustellen. Die Auswertung dieses Studie zeigt, dass 57% der Kunden aufgrund von „Smart Info“ ihr Stromverbrauchverhalten verändert haben. Sie beweist außerdem die These, dass die Sensibilisierung des Kunden bezüglich seines Stromverbrauchs und dessen Visualisierung tatsächlich zu einer Verbrauchssenkung und einer Änderung des Verbrauchsverhaltens führt. [10] Dies geht auch aus einer Aussage Livio Gallos, Enels Direktors der Infrastrukturabteilung, hervor, nach der die Spitzenlasten um geschätzte 5% gesenkt werden konnten.[23]

Enel führt seit dem Telegestore Projekt weitere Forschungs-

doi: 10.2313/NET-2011-07-2_15

und Pilotprojekte durch, um die Reichweite und Funktionalität seines Smart Grids zu erhöhen. So gibt es ein Projekt unter der Bezeichnung „Active Control for Distributed Energy Resources connected to the MV network“. Dieses fortschrittliche Kontrollsystem fügt zu den Knoten des MV Netzes eine Spannungs- und Leistungsflusskontrolle hinzu und wird Ereignisse wie eine Umschaltung auf den Inselbetrieb effizient und zuverlässig regeln. Im Energy@Home (E@H) Projekt soll mit anderen Firmen zusammen eine gemeinsame auf ZigBee basierende Kommunikationsplattform für Elemente in einem HAN entwickelt werden.[28] Darüber hinaus wird an einer verteilten Infrastruktur zum Aufladen von Elektroautos gearbeitet.[10]

4.2 SmartGridCity von Xcel Energy

Xcel Enegy ist ein US amerikanischer Strom- und Gasversorger mit 3,4 Millionen Strom- und 1.9 Millionen Erdgaskunden. Das Unternehmen ist in Colorado, Michigan, Minnesota, New Mexico, North Dakota, South Dakota, Texas und Wisconsin aktiv und hat eine installierte Netto-Kraftwerkskapazität von über 16 GW. [19] Nach eigenen Angaben wird 9% des Stroms allein durch Windenergie erzeugt und dieser Wert soll bis 2020 auf 20% angehoben werden.[18]

2008 begann Xcel mit der Durchführung des SmartGridCity Projekts und stellte es 2010 fertig. Ziel des Projekts war es in Erfahrung zu bringen, was mit bereits existierenden Technologien, die zu einem Smart Grid verbunden werden, gemacht werden kann. Dabei wurden in der Stadt Boulder, Colorado, über 20000 Smart Meter installiert und die Stromnetz-Infrastruktur wurde aufgerüstet. Dies umschloss u.a. die Aufrüstung von 4600 Transformatoren mit Kontrollgeräten, die Installation von verschiedenen Geräten zur Messung der Stromqualität und zur Schaltung, sowie ein auf BPL basierendes Kommunikationssystem und ein Glasfasernetz. Das BPL System beginnt in einem MV Stromnetz an einem sogenannten Backhaul-Point, welcher das BPL Netz mit einem Glasfasernetz verbindet. Von dort aus werden die Signale durch das Stromnetz, wenn nötig über ein LV Station hinweg, zu Netzwerkelementen wie den Smart Metern oder Sensoren geroutet. In einigen Fällen wurde aus Kostengründen oder aus technischen Erwägungen statt BPL eine drahtlose Verbindung verwendet. Das eigens für das Smart Grid errichtete Glasfasernetz, hier auch Backhaulnetz genannt, besitzt eine Ringtopologie und verbindet alle Backhaul-Points mit dem Boulder Service Center. Eine untersuchte Alternative zu dem Glasfasernetz war DSL Verbindungen zu nutzen. Es wurde gezeigt, dass dies technisch möglich ist, aber es gab kein passendes Angebot von Providerseite. [24]

Es wurden zwei Arten von Smart Metern verwendet, BPL fähige für Privatkunden und kabellose Smart Meter von SmartSynch, welche GPRS verwenden. Die Smart Meter sind in der Lage in einem 15 Minuten Intervall ausgelesen zu werden und sollen den Kunden möglichst zeitnah über eine bei Xcel zentral bereitgestellte Webschnittstelle mit aktuellen Informationen über seinen Verbrauch informieren.[24]

Es wird ein Tarifmodel mit zwei unterschiedlichen Tarifen angeboten. Im Zeitraum zwischen 14:00 und 20:00 Uhr an Werktagen gelten die On-Peak-Preise (Spitzenlastpreise). Der Tarif „Shift&Save“ unterscheidet nur zwischen On- und Off-Peak-Zeiten. Zu den On-Peak-Zeiten kosten die kWh im Sommer 17 US Cent und im Winter 6 US Cent, sonst nur 4 US Cent. Der Tarif „Peak Plus Plan“ kostet zu On-Peak-Zeiten im Sommer 12 US Cent und im Winter 5 US Cent, und zu Off-Peak-Zeiten nur 4 US Cent. Dafür kann der Versorger 15 Mal im Jahr sogenannte „Peak Energy Events„ ankündigen, in welchen eine kWh 33 US Cent im Winter und 51 US Cent im Sommer kostet. Diese werden einen Tag vorher per E-Mail bekannt gegeben. [17]

Dieses Projekt lieferte nach seiner Fertigstellung die Basis für weitere Projekte wie die Erprobung verschiedener Geräte im HAN Bereich, z.B. fernabschaltbare Klimaanlagen, oder die Erprobung der Auswirkung von Tarifmodellen auf die Spitzenlast. Zu den positiven Ergebnissen dieses Projektes zählen eine verbesserte Netzstabilität, eine beschleunigte Erkennung und Behebung von Ausfällen aufgrund der verbesserten Informationslage und eine bessere Planbarkeit, weil die aktuelle Lastverteilung auf den Transformatoren nun bekannt ist. Finanziell gesehen war das Projekt jedoch nicht erfolgreich, da es 44,8 Millionen US Dollar statt den geschätzten 15 Millionen kostete. Dies lag vornehmlich an der Verlegung der unterirdischen Glasfaserkabel, die sich als unerwartet aufwändig herausstellte. [1]

4.3 Direct Load Control von Con Edison

Con Edison ist ein in New York City aktiver Strom-, Gas- und Fernwärmeversorger.

Seit 2002 bietet Consolidated Edison seinen Kunden intelligente Thermostate zur Regulierung ihrer zentralen Klimaanlage an. Das DLC (Direct Load Control) Projekt realisiert ein Demand Response Verfahren und dient somit ausschließlich zur Reduzierung der Spitzenlast. Die Kunden erhalten den von Carrier Electronics entwickelten 300 US Dollar teuren Thermostat kostenlos und einmalig 25 Dollar geschenkt, wenn sie Con Edison erlauben, den Kompressor ihrer Klimaanlage zu Spitzenlastzeiten abzuschalten. Der Kunde hat jedoch die Möglichkeit diese Regelung außer Kraft zu setzen, sollte sie ihm Unbehagen bereiten.[14]

Bei diesem Geräte findet die Datenübertragung über ein bidirektionales Pager Netzwerk statt und es kann darüber vom Stromanbieter gesteuert werden. Darüber hinaus wird keine weitere Infrastruktur benötigt [15]

Es wurden 17200 intelligente Thermostate bei Privatkunden und 7200 bei Geschäftskunden installiert. Die Spitzenlast konnte durch diese Maßnahme um 29 MW gesenkt werden.[14] Interessant ist hierbei vor allem, dass dieses System ohne die sonst für Smart Grid Technologien übliche, zusätzliche und eigens errichtete Infrastruktur auskommt.

5. ZUSAMMENFASSUNG

Obwohl Smart Grid Technologien noch sehr jung sind und sich teilweise noch in der Erforschung und Entwicklung befinden, zeigen die vorgestellten Projekte ihr hohes Potential. Sie ermöglichen einerseits eine billigere, umweltfreundlichere und zuverlässigere Stromversorgung, aber führen andererseits auch neue Sicherheits- und Datenschutzprobleme ein.

Zudem führt der bisherige Mangel an einheitlichen Standards zu Schwierigkeiten bei der Interoperabilität der Smart

doi: 10.2313/NET-2011-07-2_15

Grids untereinander.[29] Um dem entgegen zu wirken, Forschungs- und Entwicklungskosten für einzelne Firmen zu senken und die Umsetzung der europäischen Energie- und Klimaziele zu forcieren, wurde die European Electricity Grid Initiative von der ENTSO-E, der Europäischen Kommission, sowie Firmen wie Enel und RWE ins Leben gerufen.

Für die Umsetzung sowohl wirtschaftlich motivierter Ziele als auch politisch gesetzter Ziele, wie die Reduzierung der Kohlenstoffdioxid-Emission der EU um 20% oder ein eventueller Atomausstieg, werden Smart Grid Technologien unerlässlich sein. Es ist also nur noch eine Frage der Zeit, bis Smart Grids das klassische Stromnetz abgelöst bzw. erweitert haben werden.

6. LITERATUR

[1] Before the public utilities commission of the state of Colorado in the matter of the application of public service Company of Colorado for an order approving a SmartGridCityMCPCN. http://www.xcelenergy.com/staticfiles/xe/Regulatory/smart-grid-city-cpcn-application.pdf, gelesen: 08.07.2011.

[2] Bruttostromerzeugung nach Energieträgern in Deutschland für das Jahr 2010. http://upload.wikimedia.org/wikipedia/commons/7/74/Strommix-D-2010.svg, gelesen: 08.07.2011.

[3] Map of of european Transmission System Operators Organizations . http://upload.wikimedia.org/wikipedia/commons/6/6d/ElectricityUCTE.svg, gelesen: 08.07.2011.

[4] BDEW. Energiemarkt Deutschland. http://www.vewsaar.de/fileadmin/dokumente/Energie/pdf/EnergieMarktDeutschland_2010.pdf, gelesen: 23.06.2011.

[5] BDEW. Intelligent, flexibel, zuverlässig: Netze der Zukunft. www.bdew.de, gelesen: 23.06.2011.

[6] BMU. Gesetz für den Vorrang Erneuerbarer Energien (Erneuerbare-Energien-Gesetz -EEG). http://bundesrecht.juris.de/bundesrecht/eeg_2009/gesamt.pdf, gelesen: 23.06.2011.

[7] BMU. Nationaler Aktionsplan für erneuerbare Energie gemäß der Richtlinie 2009/28/EG zur Förderung der Nutzung von Energie aus erneuerbaren Quellen. http://www.erneuerbare-energien.de/files/pdfs/allgemein/application/pdf/nationaler_aktionsplan_ee.pdf, gelesen: 23.06.2011.

[8] F. Borghese. The Telegestore Automatic Meter Management System AMM, ready for SMART GRIDS. http://www.aneel.gov.br/Arquivos/PDF/ENEL-Fabio_Borghese.pdf, gelesen: 23.06.2011.

[9] B. Botte, V. Cannatelli, and S. Rogai. The Telegestore Project in Enel's Metering System. http://www.cired.be/CIRED05/papers/cired2005_0406.pdf, gelesen: 23.06.2011.

[10] F. Caleno. The Enel Smart Info A first Smart Grids step to addressing in-home energy efficiency. http://www.cired.be/CIRED09/round_tables/RT4b/Federico%20Caleno%20RT4b.pdf, gelesen: 23.06.2011.

[11] D. V. Dollen. Report to nist on the smart grid interoperability standards roadmap. http://www.nist.gov/smartgrid/upload/Report_to_NIST_August10_2.pdf, gelesen: 23.06.2011.

[12] C. M. Drago. Smart Grids in Italy - an example of successful implementation. http://www.ure.gov.pl/download.php?s=1&id=2670, gelesen: 23.06.2011.

[13] S. e Business Watch. Case Study - Telegestore ENEL. http://ec.europa.eu/enterprise/archives/e-business-watch/studies/case_studies/documents/Case%20Studies%202009/CS09_SmartGrids1_ENEL.pdf, gelesen: 23.06.2011.

[14] C. Edison. Direct Load Control. http://www.dps.state.ny.us/07M0548/workgroups/inventory/WG2_PS_ConEd_Direct_Load_Control.pdf, gelesen: 23.06.2011.

[15] C. Edison. FAQ. http://www.conedprograms.com/faq/faqCommercial/, gelesen: 23.06.2011.

[16] Enel S.p.A. Homepage - gruppo enel. http://www.enel.it/it-IT/azienda/profilo/gruppo_enel/, gelesen: 23.06.2011.

[17] X. Energy. Smartgridcity pricing plan comparison chart. http://smartgridcity.xcelenergy.com/media/pdf/SGC-pricing-plan-chart.pdf, gelesen: 23.06.2011.

[18] X. Energy. Xcel energy homepage. http://www.xcelenergy.com/Environment/Renewable_Energy/Wind/Wind_Power_on_Our_System, gelesen: 23.06.2011.

[19] X. Energy. Xcel energy homepage - our company. http://www.xcelenergy.com/About_Us/Our_Company/Company_Profile/Operations_at_a_Glance, gelesen: 23.06.2011.

[20] ENTSO-E. P1 - Policy 1: Load-Frequency Control and Performance. https://www.entsoe.eu/fileadmin/user_upload/_library/publications/entsoe/Operation_Handbook/Policy1_final.pdf, gelesen: 23.06.2011.

[21] ENTSO-E. Ten-Year Network Development Plan 2010-2020. https://www.entsoe.eu/fileadmin/user_upload/_library/SDC/TYNDP/TYNDP-final_document.pdf, gelesen: 23.06.2011.

[22] S. Galli, A. Scaglion, and Z. Wang. For the Grid and Through the Grid:The Role of Power Line Communications in the Smart Grid. *Proceedings of the IEEE*, 06:998–1027, 2011.

[23] L. Gallo. Enel: Italy reaping first-mover benefits of smart meters. http://www.euractiv.com/en/climate-environment/enel-italy-reaping-first-mover-benefits-smart-meters, gelesen: 23.06.2011.

[24] R. Huston. Before the public utilities commission of the state of Colorado in the Matter of the application public service company of Colorado for approval of the SmartGridCity CPCN direct Testimony of Randy Huston. http://www.xcelenergy.com/staticfiles/xe/Regulatory/smart-grid-city-cpcn-testimony.pdf, gelesen: 08.07.2011.

[25] C. Ivanov. Price Impacts on Peak Demand. http://www.powersystem.org/docs/publications/price-impacts-on-peak-demand.pdf, 2009, gelesen:

doi: 10.2313/NET-2011-07-2_15

23.06.2011.

[26] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke. Smart-Grid Security Issues . *Security & Privacy, IEEE*, 8:81–58, 2010.

[27] NIST. Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security. `http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf`, gelesen: 23.06.2011.

[28] P. Petroni. From Smart Metering to Smart Grid. `http://www.ieee-isgt-2010.eu/_pdf/petroni_paola_plenary-3.pdf`, gelesen: 23.06.2011.

[29] T. Sauter and M. Lobashov. End-to-End Communication Architecture for Smart Grids. *IEEE Transactions on Industrial Electronics*, 58:1218–1228, 2011.

[30] C. Theobald, K. Hummel, C. Jung, J. Müller-Kirchenbauer, D. Nailis, and W. Zander. R-A-N Gutachten zu Kosten der Beschaffung und Abrechnung von Regel- bzw. Ausgleichsenergie im Blick auf die kartellrechtliche Angemessenheit der Netznutzungsentgelte der RWE Net AG. `http://www.wind-energie.de/fileadmin/dokumente/Themen_A-Z/Regelenergie/Studie_BWT_Regelenergie.pdf`, 03 2003, gelesen: 23.06.2011.

[31] J. Wang, M. Biviji, and W. M. Wang. Case Studies of Smart Grid Demand Response Programs in North America, 2011.

doi: 10.2313/NET-2011-07-2_15

Probleme beim Einsatz von DTNs

Gerhard Steffek
Betreuer: Nils Kammenhuber
Seminar Innovative Internet Technologien und Mobilkommunikation SS2011
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: steffek@in.tum.de

KURZFASSUNG

Als Disruption and Delay Tolerant Networks (DTNs) werden Netzwerke bezeichnet, die darauf ausgelegt sind, trotz nicht durchgängig verfügbarer Verbindungen und Netzwerk-Teilnehmer eine gewisse Konnektivität zu gewährleisten. In dieser Arbeit wird der experimentelle Einsatz eines DTNs in Lappland und die dabei auftretenden Probleme vorgestellt. Außerdem werden der Aufbau und die Vor- und Nachteile eines DTNs zur mobilen Datenkommunikation in Autos und Zügen besprochen und verschiedene Übertragungsmethoden miteinander verglichen.

Schlüsselworte

Delay-Tolerant Network, DTN, HTTP-DTN, SNC, HTTP, MIME

1. Einleitung

In vielen Bereichen ist die Internetanbindung selbstverständlich. Zuhause haben viele Menschen Zugang zu einer Internetverbindung und auch in Cafés, Restaurants und Universitäten ist Wlan immer häufiger verfügbar. An Orten an denen kein Wlan vorhanden ist wird mittlerweile häufig auf Mobilfunk zurückgegriffen, welches großteils selbst in U-Bahnen verfügbar ist. Bewegt man sich jedoch außerhalb der Ballungszentren , beispielsweise bei einer Fahrt auf der Autobahn oder im Zug, lässt die Netzabdeckung stark nach und es treten vermehrt Verbindungsabbrüche auf. Aber auch hier gibt es Ansätze und Ideen die Internetversorgung, kostengünstiger als durch das Aufstellen weiterer Mobilfunkmasten, unterwegs zu gewährleisten.

Problematischer gestaltet sich die Netzabdeckung in manchen Ländern mit einer, im Vergleich zu Deutschland, sehr viel geringeren Bevölkerungsdichte. Ein Beispiel dafür sind die Rentierhüter Lapplands im Norden Schwedens die weder über eine Internetanbindung noch ein Stromnetz verfügen. Diese verändern mehrmals jährlich ihren Standort, teilweise um mehrere hundert Kilometer innerhalb weniger Wochen. Nötig ist dies aufgrund vieler Faktoren (Verhalten der Rentiere, Klima, Gesetze, Tourismus etc.) [2].

DTNs sind jedoch auch in anderen Gebieten wichtig. Ursprünglich wurde bei der Entwicklung an interplanetare Kommunikation und ihre Probleme gedacht. Hier treten hohe Fehlerraten (Bit Error Rates, BER) zusammen mit hohen Latenzen auf. Dies stellte andere Anforderungen an die Übertragungsprotokolle als beim Internet über Kabelverbindungen auf der Erde. Zum Beispiel dauert mit Lichtgeschwindigkeit eine Übertragung zum Mond 1,7 Sekunden, zum Mars sogar 8 Minuten [7]. Da auch auf der Erde eine Verbindung immer und überall unabhängig von Kabelverbindungen erwünscht ist, finden mittlerweile viele Entwicklungen im Bereich DTNs für die Kommunikation auf der Erde statt. Hierzu gehört nicht nur die Verbindung zum Internet sondern auch die Datenübertragung innerhalb lokaler Netzwerke wie zum Beispiel in Sensornetzwerken.

In den folgenden Kapiteln werden unterschiedliche Einsatzzwecke für DTNs aufgezeigt. Dazu wird neben dem Einsatzzweck auch ein möglicher Aufbau eines DTNs für diesen erklärt, sowie auf die möglichen Schwachstellen und Schwierigkeiten eingegangen. Als erstes wird das genannte DTN in Lappland beschrieben, danach ein DTN für mobile Kommunikation. Im Anschluss daran wird der Einsatz und die Vorteile von HTTP in DTNs erklärt. Als letztes wird mit der Beschreibung eines Sensornetzwerkes für die Landwirtschaft noch ein weiterer Einsatzort für DTNs gezeigt.

2. Einsatz eines DTN in Lappland

2.1 Überblick

In Lappland wurde bereits ein DTN in einer wenig besiedelten Gegend zu Testzwecken eingesetzt. Beim Projekt „Sámi Network Connectivity“ wird versucht die Rentierhüter Lapplands mit einer Internetanbindung zu versorgen. Dies geschieht um ihnen die Möglichkeit zu geben sich weiterzubilden, aber auch um Kontakt mit der Familie oder das Lesen von Nachrichten zu ermöglichen. Durch eine Internetanbindung sind Kontakt zu Schulen und Universitäten aber auch neue Möglichkeiten der Arbeit denkbar (Heimarbeit, Internetgeschäfte usw.). Dadurch soll der Beruf des Rentierhüters an Attraktivität gewinnen und erhalten bleiben [2].

Die Anwendungen, die anfangs implementiert werden sollten sind daher [2]:

- Senden und Empfangen von Emails
- Übertragen von Dateien
- Zugriff auf Websites und Web Services

Aufgrund fehlender Infrastruktur, großer Entfernungen und des Nomadenverhaltens der Sámi sind nicht nur eine direkte Anbindung an das Internet (über Kabel oder kabellos) sondern auch eine Stromversorgung über das Stromnetz nicht möglich. Große Teile der zu versorgenden Gebiete befinden sich in Nationalparks, hier ist auch aus gesetzlichen Gründen der Aufbau einer festen Infrastruktur (Verlegen von Internet- oder

doi: 10.2313/NET-2011-07-2_16

Stromkabeln, festes Anbringen von Antennen usw.) häufig nicht möglich. Auch die Kosten spielen eine große Rolle und sollten möglichst niedrig gehalten werden, da der Internetzugriff eine Verbesserung der Lebensqualität und eventuell eine finanzielle Entlastung bedeuten sollte und nicht eine weitere finanzielle Belastung darstellen [2].

2.2 Anwendungen

Neben den anfangs genannten Anwendungen war auch eine Funktion angedacht, um Rentiere über Sensoren aus der Entfernung überwachen und ihren Aufenthaltsort bestimmen zu können. In dem hier beschriebenen Experiment wurde diese Funktion aber nicht implementiert.

Stattdessen wurde versucht das System so zu gestalten, dass es mit gewöhnlichen Programmen für den Zugriff auf Websites und das Verfassen und Empfangen von Emails funktioniert, wie sie normalerweise in dauerhaft mit dem Internet verbundenen Systemen verwendet werden. Aufgrund sehr hoher Latenzen und der asynchronen Art des DTNs sind Verbindungen nur sehr schwer zu implementieren, die eine Authentifizierung oder Rückmeldung vom Benutzer benötigen. Daher wurden sie hier vernachlässigt [2].

Die Bereitstellung eines Email Services wurde dabei einerseits durch seine asynchrone Art der Verbindung als theoretisch recht einfach betrachtet, andererseits aber auch als sehr wichtig eingestuft da Emails eine grundlegende Art der Kommunikation und Datenübertragung sind und eventuell sogar die „killer application“ für das ganze Projekt darstellen. Zwar sind die Protokolle (SMTP, POP3 und IMAP) eigentlich für eine synchrone Internetverbindung ausgelegt, aber durch eine Ausstattung der Hotspots mit Gateways, die einen Email Server vorgeben, wird es möglich mit normalen Email Programmen Emails zu versenden und zu empfangen. Durch einen bereitgestellten Webmail Service konnte man Emails über den Browser betrachten und verfassen. Die vom Hotspot angebotenen Email Server hatten alle den Internetgateway als Ziel. Dadurch wurden alle Emails zu diesem weitergeleitet, woraufhin er sie versendete. Ankommende Emails wurden vom Internetgateway an sämtliche Hotspots weitergeleitet, hier konnten die Benutzer sie dann abrufen [1].

Auch der Zugriff auf Websites muss von einem Projekt, dass das Internet für Privatpersonen bereitstellen möchte, natürlich ermöglicht werden. Dies ist eine sehr viel interaktivere Tätigkeit und aufgrund der hohen Latenzen um einiges aufwendiger zu implementieren. Während des Tests wurden fest eingerichtete Websites vom Internetgateway immer wieder automatisch aktualisiert und auf sämtliche Hotspots übertragen [1].

2.3 Theoretischer Aufbau

Das Netzwerk sollte aus mehreren festen Hotspots, die eine WLAN Verbindung zur Verfügung stellen und den Zugriff auf Emails und Websites ermöglichen, bestehen. Da diese Hotspots mehrere Kilometer auseinander liegen sollten (Abb. 1), wurde eine direkte drahtlose Kommunikation aus (energie-)technischen und monetären Gründen ausgeschlossen. Stattdessen sollten mobile Datenspeicher (Relays) zum Einsatz kommen, die in der Nähe eines Hotspots die Daten mit diesen austauschen. Da Speicherplatz und Bandbreite beschränkt sind kommt hier ein Protokoll namens “PRoPHET” zum Einsatz [1].

2.3.1 PRoPHET

PRoPHET steht für “Probabilistic Routing Protocol using History of Encounters and Transitivity”. PRoPHET wurde anderen Routing-Protokollen, beispielsweise dem einfachereren Epidemic Routing, vorgezogen. Beim Epidemic Routing werden bei einem Datenabgleich alle Synchronisationsknoten auf den gleichen Stand gebracht indem jeder Knoten alle Daten erhält. Da dies zwar effektiv jedoch auch ressourcenintensiv ist, wurde stattdessen PRoPHET eingesetzt, um die Verteilung der Daten auf die Knoten zu bestimmen. Hierbei wird es von der Wahrscheinlichkeit der Knoten A und B den Zielknoten C eines Pakets direkt oder indirekt zu erreichen abhängig gemacht, ob A oder B die Daten erhält. Dadurch soll nicht nur eine schnelle Übertragung der Daten ermöglicht sondern auch die von und zu den Knoten übertragene Datenmenge reduziert werden [1].

2.3.2 Datenübertragung über Middleware

Momentan basiert Internet großteils auf dem Transmission Control Protocol (TCP) zur Datenübertragung. TCP hat viele Eigenschaften, wie die Erkennung und Behebung von Fehlern bei der Datenübertragung, weswegen es für viele Bereich, ob mit oder ohne Kabel, geeignet ist. Andererseits benötigt TCP eine end-to-end Verbindung von der Quelle zum Ziel, weswegen es für ein DTN ungeeignet ist. Hier kann für gewöhnlich entweder eine end-to-end Verbindung nicht garantiert werden (mobile Anwendungen) oder ist erst gar nicht möglich (wie in diesem Fall). In einem solchen DTN muss deswegen die Datenübertragung anders gelöst werden. Da bisherige Programme wie Browser und Email Programm auf einer TCP Verbindung basieren und weiterverwendet werden sollten, wurde in den Gateways eine Middleware eingesetzt. Die Middleware ist dabei der Endpunkt für die Anwendung an den diese, über TCP, ihre Dateien schickt. Danach fasst sie die Pakete der Programme und andere für die Zustellung notwendigen Metadaten zu einem einzigen Bundle zusammen, welches über das DTN übertragen werden kann. Die Daten werden also auf den mobilen Datenspeicher übertragen und dort gespeichert, bis sie an einen anderen mobilen Datenspeicher oder Hotspot weitergegeben werden können. Diese Pakete können dabei über eine Ablaufzeit verfügen nach der sie verworfen werden, die aber für gewöhnlich nicht im Bereich von Sekunden liegt (wie die Round Trip Time bei TCP, nach Ablauf derer das Paket als verloren angesehen und erneut versendet wird) sondern mehrere Stunden, Tage oder gar Monate lang sein kann [2].

2.4 Praktischer Aufbau

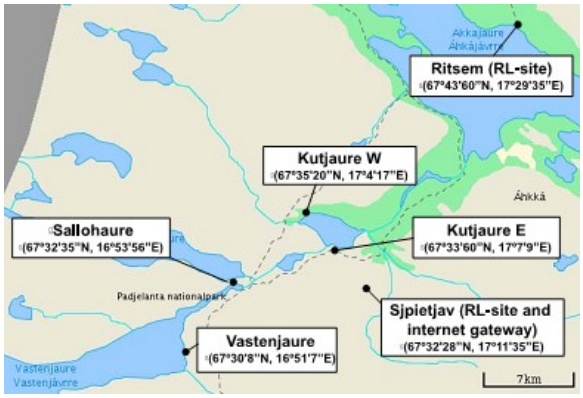


Abb. 1: Karte des Testgebiets [1]

doi: 10.2313/NET-2011-07-2_16

Im Einsatz bestand das Netzwerk aus 4 fixen Hotspots und 7 mobilen Geräten um die Kommunikation zwischen diesen zu ermöglichen. Die Internetanbindung des Internetgateways (Sjpietjav) konnte dabei jedoch nicht direkt erfolgen, sondern musste auf einer kabellosen Verbindung (mit Sichtkontakt) zu einem Dorf (Ritsem) in ca. 20 km Entfernung basieren. Die Entfernungen zwischen den einzelnen Hotspots betrugen ca. 10 km und der Internetgateway hatte eine Entfernung von 5 km zum nächsten Hotspot [1].

Freiwillige sorgten dabei für die Verbindung der Hotspots durch die mobilen Datenspeicher [1].

Als Hardware kamen Laptops und Tablet PCs zum Einsatz auf denen sowohl Windows als auch Linux verwendet wurden. Die Akkulaufzeit war dabei ein wichtiges Thema für die Geräte [1].

2.5 Schlussfolgerungen aus dem Projekt

2.5.1 Email Implementation

Wie erwartet wurde die Email-Funktion stark genutzt. Da PRoPHET zu debug-Zwecken über eine graphische Oberfläche verfügte über die sich auch Nachrichten direkt zustellen ließen, ergab sich eine Art „interne Email“. Diese erwies sich als schneller da dadurch der Umweg über das Internetgateway, über das sämtliche normalen Emails geleitet wurden, eingespart werden konnte, falls eine schnellere Verbindung direkt über die Hotspots möglich war. Um die Zustellung von internen Emails zu beschleunigen und Datenverkehr einzusparen, sollte in Zukunft automatisch überprüft werden ob der Empfänger sich innerhalb des Netzwerks befindet und gegebenenfalls die Email direkt intern zustellen. Während des Tests hatte es keinen negativen Einfluss, dass sämtliche Emails an alle Hotspots zugestellt wurden. Bei einem größeren und stärker benutzten Netzwerk könnte aber Bandbreite und Speicherplatz eingespart werden, wenn die Nachrichten nur an die Hotspots zugestellt würden, bei denen sich die Benutzer vorher angemeldet haben oder in deren Nähe sie sich wahrscheinlich momentan aufhalten [1].

2.5.2 Zugriff auf Websites

Das implementierte Caching-System hat funktioniert, aber der Funktionsumfang war sehr begrenzt, weswegen hier noch viel Raum für Verbesserungen bleibt.

So fehlte beispielsweise eine Funktion, die den Benutzern die Möglichkeit gibt Websites, die sich nicht im Speicher befinden, vom DTN laden zu lassen. Hier wären auch Techniken von Vorteil, die bestimmen welche weiterführenden Links mitgeladen werden sollten (intelligent prefetching). Außerdem sollten häufig besuchte Websites automatisch aktualisiert werden oder zumindest die Möglichkeit gegeben sein, sich für Updates von Websites einzutragen und dann automatisch neue Versionen der Seite zu bekommen [1]. Dadurch könnte zum Beispiel eine Nachrichtenseite oder ein Forum aktuell gehalten und die Beiträge automatisch mitgeladen werden.

Diese häufigen Updates würden jedoch auch eine Verbesserung der Übertragungsart der Websites benötigen. Während des Tests wurde beim Update einer Website immer die gesamte Seite durch das DTN geschickt und auf den Hotspots gespeichert anstatt nur ein inkrementelles Update zur bereits vorhandenen Version zu speichern. Dadurch würden sich Übertragungsdauer und Speicherbedarf bei der Aktualisierung von Websites verringern [1].

3. DTN für mobile Kommunikation

3.1 Anwendungsbereiche

Für gewöhnlich wird über die Verwendung von DTNs im Zusammenhang mit dem Erschließen neuer Kommunikations-möglichkeiten diskutiert. Dabei kann ein DTN auch in bereits existierende Kommunikationslösungen integriert werden, um diese zu verbessern. Eine dieser bereits existierenden Lösungen stellt der Mobilfunk dar. Die Netzabdeckung wird zwar stetig verbessert, aber in abgelegeneren Gebieten oder bei hohen Geschwindigkeiten (Auto, Zug) treten immer noch häufige Verbindungsabbrüche auf, mit denen bisherige Netze (und Programme) große Probleme haben [3]. Auch die Kosten mobiler Datenübertragung (über UMTS oder GSM) sind, verglichen mit lokalen (drahtlosen) Netzwerken, noch um ein Vielfaches höher und die Übertragungsgeschwindigkeiten langsamer [4].

3.2 Theoretischer Aufbau

3.2.1 Aufbau mit direkter Verbindung

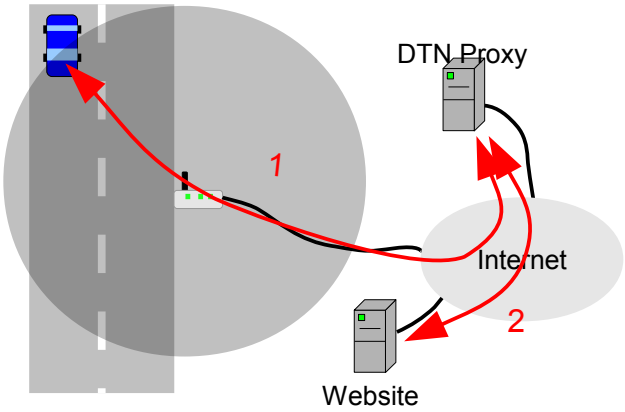


Abb. 2: Aufbau eines DTNs zur mobilen Kommunikation

Beim Projekt „Drive-thru-Internet“ soll dabei die Netzabdeckung nicht auf Ebene der Mobilfunkkommunikation (UMTS, GSM) verbessert werden, sondern durch Wlan. Dazu werden Wlan Hotspots, die aus mehreren Access Points bestehen können, am Rande des Weges dazu verwendet in kurzer Zeit große Mengen Daten zu übertragen (Abb. 2, Verbindung 1). Ein DTN Proxy entpackt dann die übertragenen Anfragen und Daten (Verbindung 2) und gibt die Antworten wieder an das Fahrzeug weiter (Verbindung 1). Solche Hotspots könnten dabei extra für Reisende von Raststätten und Tankstellen bereitgestellt werden, oder sie existieren schon, beispielsweise bei Cafés, Restaurants und Hotels [3].

In Tests [4] konnten dabei auch bei Geschwindigkeiten von 120 km/h (~33 m/s) noch Datenraten von 15 Mbit/s erreicht werden, wodurch bei einer Strecke von 2 km (60 s Verbindungsdauer) 110 Mbyte Daten übertragen werden konnten. Die hohe Reichweite von 2 km wird durch entsprechende Antennen und ohne besondere Technik erreicht, wenn keine Gebäude die Verbindung beeinträchtigen, was Zuhause für gewöhnlich der Fall ist, beim Einsatz entlang einer Autobahn jedoch nicht. Bei mehreren Teilnehmern verteilt sich aber die zur Verfügung stehende

doi: 10.2313/NET-2011-07-2_16

Bandbreite auf diese [4]. Da die Tests bereits vor mehreren Jahren durchgeführt wurden (basierend auf IEEE 802.11g Hardware), sollten die Ergebnisse mit moderner Hardware nach IEEE 802.11n sowohl im Bereich der Reichweite als auch der Übertragungsgeschwindigkeit übertroffen werden können.

Um die benötigten Daten dabei in dem kurzen Zeitraum der Verbindung schnell und effizient übertragen zu können, werden die Daten nicht als TCP Stream übertragen sondern von einem lokalen DTN-Proxy in Bundles umgewandelt und als solche zu einem entfernten DTN Proxy (Internetgateway) übertragen. Dieser stellt für das DTN die Verbindung zum Internet her [2].

3.2.2 Aufbau mit lokalen DTN Proxys

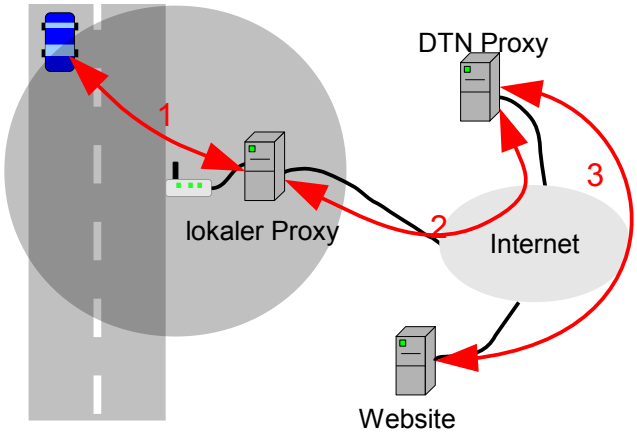


Abb. 3: Aufbau eines DTN mit lokalen Proxys

Um die Datenmenge, die während der Verbindung übertragen werden kann, weiter zu erhöhen wurde auch ein Ansatz mit lokalen DTN Proxys entwickelt. Diese befinden sich bei den Hotspots und funktionieren als Buffer. Innerhalb des Übertragungsfensters können dadurch Daten mit voller Geschwindigkeit zwischen Fahrzeug und Hotspot übertragen werden (Abb. 3, Verbindung 1) auch wenn die Internetanbindung des Hotspots langsamer ist (Verbindung 2). Der lokale Proxy überträgt die Daten dann an das Internetgateway auch nachdem die Verbindung zum Fahrzeug beendet wurde [3].

Besonders bei großen Datenmengen kann dieses System den Durchsatz erhöhen, erfordert jedoch eine Bevorzugung interaktiver Verbindungen und ihrer Daten, damit diese nicht in Warteschleifen auf ihren Upload warten müssen. Ein weiteres Problem ist, dass auf eine Authentifizierung beim lokalen Proxy verzichtet werden sollte, um Wartezeiten und Datenverkehr zu vermeiden. Der Proxy wird dadurch leicht angreifbar für DoS (Denial of Service) Attacken, bei denen einer oder mehrere Angreifer große Datenmengen auf den Hotspot laden, was sowohl bei der lokalen Datenspeicherung als auch bei der Datenübertragung über Verbindung 2 zu Überlastungen, beziehungsweise großen Verzögerungen, führen kann. Gleichzeitig kann auch schon die übertragene Datenmenge der normalen Nutzer dazu führen dass sich große Datenmengen im Buffer ansammeln und zu einer Verzögerung der Übertragung führen. Dies führt zu einer verspäteten Verarbeitung durch das Internetgateway und zu zusätzlicher Latenz bei der Übertragung und erschwert es den richtigen Ziel-Hotspot für die Bundles zu wählen. Die Auswahl sollte abhängig sein von der noch zu erwartenden Verbindungsdauer zum momentanen Hotspot, der Auslastung der Internetverbindung und dem Füllstand des Buffers. Außerdem sollte es eine Rolle spielen wann eine Verbindung zum nächsten Hotspot hergestellt werden kann und wie dieser ausgelastet ist [3].

Dieses Routing-Verhalten könnte verbessert werden. Dazu müsste der mobile Proxy im Fahrzeug den Metadaten des Bundles auch Informationen über die geplante Route und voraussichtlichen Kontaktzeiten mit weiteren Hotspots beifügen [3]. Diese Daten zu erfassen beziehungsweise vorherzusagen, zeitnah an den Internetgateway zu übertragen und auszuwerten, ist sehr aufwendig und könnte die zur Verfügung stehende Bandbreite weiter verringern.

3.3 Testaufbau

Die Datenübertragung muss nicht über das Bundle-Protokoll stattfinden, auch andere Methoden sind möglich. Um diese miteinander zu vergleichen wurde ein Testaufbau verwendet der dem Aufbau ohne lokalen Proxys entspricht (siehe 3.2.1).

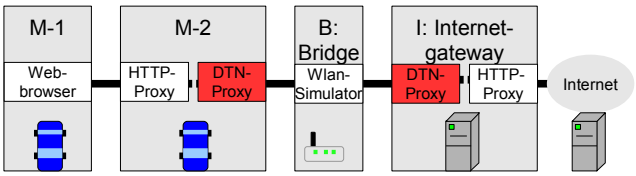


Abb. 4: Testaufbau (ohne lokale Proxys)

Der Aufbau (Abbildung 4) besteht aus vier Computern (Hosts) die mit Linux 2.4 betrieben werden, untereinander mit 100 Mbit/s schnellen full-duplex Ethernet-Verbindungen verbunden. Im praktischen Einsatz wäre M-1 und M-2 Teil des Systems im Fahrzeug, B entspräche dem Wlan Router und der Internetgateway wäre ein DTN Server irgendwo im Internet. Für den Test wurde M-1 und M-2 aufgeteilt, da dies ein Überwachen der ausgetauschten Daten erlaubt. Auf M-1 wird Firefox als der Webbrowser verwendet dessen Ladezeiten später verglichen werden. M-2 enthält den HTTP-Proxy an den M-1 die Seitenaufrufe sendet. Dieser sendet die Anfragen an den DTN-Proxy Host-intern weiter, der sie dann entsprechend verpackt und an Host B weitergibt. Auf Host B läuft ein Wlan-Simulator, der packet loss und Latenz eines Wlan mit unterschiedlicher Auslastung und Verbindungsqualität simulieren kann. Für dieses Netzwerk stellt Host I den Internetgateway dar. Auf diesem entpackt der DTN-Proxy die Anfragen und reicht sie an den HTTP-Proxy weiter. Dieser ruft die Website auf und gibt sie an den DTN-Proxy zurück. Die Internetanbindung von Host I ist dabei 155 Mbit/s schnell [2].

doi: 10.2313/NET-2011-07-2_16

3.4 Zugriffsmethoden

Für den Vergleich des Bundle-Protokolls mit anderen Methoden zur Datenübertragung kommen vier verschiedene Programme mit unterschiedlicher Übertragungsart als DTN Proxy zum Einsatz. Auch der direkte Zugriff wurde mitgetestet.

- Direkter Zugriff: Hier werden keine Proxyserver verwendet und der Zugriff erfolgt direkt.
- HTTP-Proxy: Um die Unterschiede bei der Kommunikation über das Bundle-Protokoll genauer messen zu können, werden hier HTTP-Proxys (an der Stelle der DTN-Proxy) auf Host M-2 und Host I zwischengeschaltet. Das soll es ermöglichen zu unterscheiden welche Verzögerung durch die Bundle-Kommunikation und welche durch die zwischengeschalteten Proxys entsteht.
- PCMP: Bei dieser Zugriffsmethode wird das Persistent Connection Management Protocol (PCMP) des Drive-thru Projekts zwischen Host M-2 und Host I verwendet.
- DTN: Hierbei werden die Seitenaufrufe von einem DTN-HTTP-Proxy (dtnhttp) angenommen. Dieser gibt sie an den DTN-Proxy weiter. Die Datenübertragung zwischen den DTN-Proxys von M-2 und I findet dann nach dem Bundle-Protokoll statt.
- DTN mit Prefetching: Anstatt alle Anfragen des Webbrowsers einzeln abzuarbeiten, versucht I beim Prefetching mithilfe von wget auch alle in die angeforderte Website eingebetteten Objekte, beispielsweise Bilder, zu erkennen, herunterzuladen und in ein einziges Bundle-Paket zu packen. Dieses Paket wird dann an M-2 geschickt, der es entpackt und an den HTTP-Proxy weiterreicht. Dieser kann dann (im Optimalfall) alle Anfragen von M-1 nach weiteren Ressourcen direkt beantworten ohne weitere Anfragen bei I.

  (Abb. 4) [3]

3.5 Geschwindigkeit

Um die einzelnen Methoden miteinander zu vergleichen wurden unterschiedliche Websites mit jeder Methode mehrmals aufgerufen. Manche Websites waren lokal auf dem Universitätsgelände, auf dem der Test stattfand, angesiedelt und hatten dementsprechend eine relativ geringe Paketumlaufzeit (Round Trip Time, RTT) von 1-10 ms. Andere waren weiter entfernt wodurch sich RTTs von bis zu 1 s ergaben. Die meisten Websites hatten jedoch RTTs von 10-100 ms. Gemessen wurde die Zeit von der ersten Anfrage durch Firefox bis zum letzten übertragenen Datenpaket zwischen M-1 und M-2 mithilfe von Ethereal [3].

Ohne künstliche Latenz durch B zeigte sowohl der HTTP-Proxy als auch der PCMP-Proxy eine Verzögerung von wenigen zehntel ms verglichen mit dem direkten Zugriff. Dies ist zwar messbar, dürfte aber nur von den wenigsten Anwendern wahrgenommen werden [3].

Bei Betrachtung der Messwerte mit dem DTN-Proxy zeigen sich jedoch durchweg Zugriffszeiten, die um ein vielfaches höher liegen als bei direktem Zugriff oder Zugriff über den HTTP- oder PCMP-Proxy. Diese brauchten beim Laden der 45 Objekte von Ebay ~4,5 s, mit DTN-Proxy musste man 64 s auf die vollständige Seite warten. Eine der lokalen Seiten (TZI) mit nur 11 Objekten wurde ohne DTN-Proxy in weniger als 0,5 s geladen, mit DTN-Proxy dauerte es 17 s. Auch von den anderen Websites wurde mit DTN-Proxy keine in weniger als 10 s geladen. 6 der 12 getesteten Websites konnten bei direktem Zugriff (oder Zugriff über HTTP-/PCMP-Proxy) in weniger als 2 s geladen werden, während es bei Zugriff über den DTN-Proxy zwischen 10 s und 59 s benötigte um sie vollständig aufzubauen [3, Table II].

Dies ist darauf zurückzuführen, dass ohne Prefetching die Objekte der Website nacheinander vom Browser angefordert werden müssen. Dabei muss jedes mal gewartet werden bis das angeforderte Objekt übertragen wurde. Dann kann Host I es in ein Bundle verpacken und an M-2 zustellen, dessen DTN-Proxy es wieder entpackt und an den HTTP-Proxy zustellt. Dadurch dauert es je nach Website durchschnittlich 1–3 s um ein Objekt zu übertragen und entsprechend lange um die gesamte Website aufzubauen (die getesteten Websites hatten zwischen 6 und 65 Objekte) [3].

Beim DTN mit Prefetching ergaben sich bei manchen Zugriffen signifikant bessere Zeiten (26 s statt 72 s, 3 s statt 17 s) bei anderen jedoch keine oder geringere Unterschiede. Dies lag am unterschiedlichen Erfolg von wget die eingebetteten Objekte zu erkennen und herunterzuladen. Bei manchen Websites erkannte wget alle oder fast alle eingebetteten Objekte wodurch die Übertragungsdauer mehr als halbiert wurde. Bei anderen erkannte wget nur sehr wenige oder gar keine Objekte weswegen sich die Übertragungsdauer kaum änderte. Um die Übertragungszeiten des DTN mit Prefetching zu verbessern, sollte wget die Objekte genauso anfordern wie ein Webbrowser und diese über mehrere TCP Verbindungen laden anstatt über eine einzelne wie im Test [3].

Eine genauere Betrachtung der Kommunikation zwischen M-2 und I zeigt, dass ca. 80 % der Zeit für das Senden und Empfangen der Bundles verbraucht wird. Durch eine Optimierung der Implementierung des DTN-Proxys könnte diese Zeit verringert werden. Auch ein Start der Bundle-Übertragung bevor die Daten für das Bundle vollständig vorhanden und verpackt sind ist denkbar [3].

Tabelle 1. Auszug der getesteten Websites mit Zugriffszeit [3]

Seite	Direkt	HTTP-Proxy	DTN	DTN mit prefetch	Anzahl Objekte
TZI[1]	0,3 s	0,5 s	17,0 s	3,1 s	11
KDDI[2]	12,8 s	10,0 s	72,6 s	26,2 s	37
Ebay[3]	4,5 s	4,5 s	64,2 s	65,5 s	45
Apache[4]	0,9 s	1,6 s	59,4 s	25,0 s	21

[1] http://www.dmn.tzi.org/

[2] http://www.kddi.com/english/

[3] http://www.ebay.com/

[4] http://cocoon.apache.org/

doi: 10.2313/NET-2011-07-2_16

3.6 Overhead

Die Qualität des Prefetchings hat nicht nur einen Einfluss auf die Latenz bei der Übertragung der Websites. Von ihr ist auch die zu übertragende Datenmenge abhängig, da jedes Bundle auch einen gewissen Overhead hat. Die Übertragung der Bundles findet über TCP statt, aber jedes Bundle beinhaltet auch den HTTP Overhead und Informationen über das DTN. Zusammen ergeben diese einen Overhead von 100 bytes pro übertragenem Bundle, oder 20 %, da eine HTTP Anfrage im Normalfall 400-600 bytes groß ist. Findet Prefetching statt müssen zudem auch Name und Dateigröße der einzelnen Objekte übertragen werden [3].

Die übertragene Datenmenge von M-2 zu I dürfte sich dabei durch prefetching verringern lassen da hier im Idealfall nur noch eine einzelne Anfrage nötig ist. Dadurch sollte sich gegenüber den vielen einzelnen Anfragen mehr Volumen einsparen lassen als der Overhead des DTNs hinzufügt. Von I zu M-2 wird das kaum möglich sein, allerdings sollte es hier möglich sein durch Kompression den Overhead des DTNs auszugleichen [3].

3.7 Folgerung

Aus dem Test geht hervor, dass es möglich ist HTTP über das Bundle-Protokoll zu übertragen, aber die Performanz für den realen Einsatz zu schlecht ist. Hierfür müssten das Prefetching und die Effizienz der DTN-Proxys verbessert werden. Aber auch mit annehmbaren Übertragungszeiten würde das DTN dem Anwender langsamer vorkommen als bei direktem Zugriff. Beim DTN wird auf das Übertragen sämtlicher Objekte an den Internetgateway und des gesamten Bundles an M-2 (Abb. 4) gewartet, erst dann wird die Seite aufgebaut. Beim direkten Zugriff hingegen werden Objekte nach und nach dargestellt. Dies erscheint dem Benutzer für gewöhnlich schneller, auch wenn die vollständige Darstellung der Website die gleiche Zeit benötigt. Außerdem ist zu beachten, dass sich HTTP, solange es zustandslos verwendet wird, relativ einfach über ein DTN übertragen lässt. Interaktive Dienste (wie ein Chat) wären mit der momentanen DTN Implementation jedoch nicht möglich und sichere Verbindungen stellen auch ein großes Problem dar. Deswegen sollte auf das DTN nur zurückgegriffen werden, wenn eine konstante Verbindung nicht verfügbar ist. Abhängig von Signalstärke und Verbindungsschwankungen könnte die Auswahl des Netzwerks automatisch, ohne Eingriff des Benutzers, durch den DTN-Proxy erfolgen. Ein weitergeben der Verbindungsart vom Betriebssystem an die Anwendungen könnte es ermöglichen, dass diese ihr Verhalten in einem DTN anpassen. Dadurch sollten die Unterschiede zwischen den Übertragungsarten für den Benutzer verringert werden können, dieser aber auch auf Einschränkungen hingewiesen werden können wenn nötig [3]. So könnte beispielsweise ein Instant Messenger seinen Benutzer nicht abmelden, sondern ihm und seinem Kommunikationspartner anzeigen, dass er momentan keine dauerhafte Verbindung hat. Die Daten werden übertragen sobald wieder eine Netzwerkverbindung vorhanden ist. So könnte ein DTN eine nützliche Erweiterung unserer bisherigen Kommunikationsnetze darstellen.

4. Weitere Entwicklungen im Bereich DTN

4.1 HTTP in DTNs

4.1.1 MIME und HTTP

Ein wichtiger Faktor der Kommunikation heutzutage ist das Übertragen von Dateien, seien es nun Bilder, Dokumente oder Programme. Dies wird fast immer durch MIME (Multipurpose Internet Mail Extension) realisiert, das längst nicht mehr nur in Emails Anwendung findet, sondern auch zusammen mit HTTP verwendet wird. Durch MIME wird bei der Nachrichten-übertragung die Art der Nachricht beschrieben. Hierzu gehört ihr Typ (Content-Type, beispielsweise „text/plain“ oder „image/gif“) als auch die verwendete Kodierungsart, wobei eine Email mit Texten und Bildern aus mehreren, unterschiedlichen Content-Types besteht. Die mit MIME beschrieben Daten werden dabei als Binär-Stream über das Übertragungsprotokoll HTTP übertragen. Dies wird selbst fast ausschließlich mit TCP als Transportprotokoll verwendet [5].

4.1.2 HTTP ohne TCP

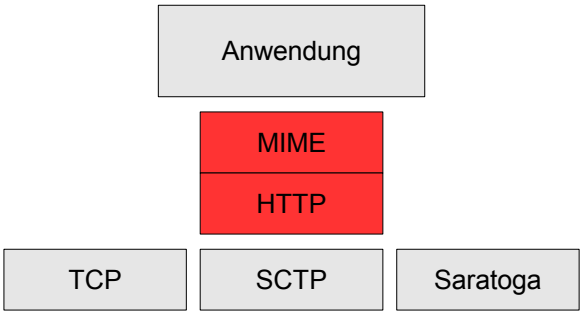


Abb. 5: HTTP und MIME zwischen Anwendung und Transportprotokoll

Für die Verwendung in DTNs ist TCP jedoch häufig ungeeignet, da hier andere Anforderungen an Transport und Routing gestellt werden als in normalen Netzwerken. Bei diesen kann mit einer dauerhaften, durchgehenden Verbindung der Kommunikations-partner ausgegangen werden. Bei einem DTN ist jedoch häufig keine durchgehende Verbindung möglich, oder die Kommunikationspartner sind nur zu unterschiedlichen Zeiten verfügbar. Auch unterstützen kleine Systeme (beispielsweise bei Sensornetzwerken) manchmal kein TCP, könnten aber trotzdem HTTP verarbeiten. Andere Netzwerke, beispielsweise lokale Netzwerke mit geringen Bit Error Rates und Latenzen, sind eigentlich gut für TCP geeignet, hier gibt es jedoch mittlerweile modernere Protokolle, die einige Vorteile gegenüber TCP aufweisen können beispielsweise SCTP (Stream Control Transmission Protocol). Um trotzdem die Übertragung von Daten in diesen Fällen zu ermöglichen, eignet sich HTTP als zustandsloses, von einem Transportprotokoll unabhängiges Übertragungsprotokoll. Die Anforderungen von HTTP an das Transportprotokoll sind dabei relativ gering und es könnten problemlos Protokolle wie Saratoga oder SCTP zur Übertragung von HTTP verwendet werden [5].

4.1.3 Eignung von HTTP für DTNs

Um Daten in einem DTN optimal zu übertragen, kann es auch nötig sein unterschiedliche Protokolle für die Subnetze zu verwenden. Auch das ist mit HTTP kein Problem, da es erlaubt

doi: 10.2313/NET-2011-07-2_16

weitere „Content-*:“ Header einzuführen. So können mit „Content-Source:“ und „Content-Destination:“ die Quelle und das Ziel der Daten unabhängig vom Subnetz angegeben werden, während mit „Host:“ das Ziel innerhalb des Subnetzes gemeint ist [5].

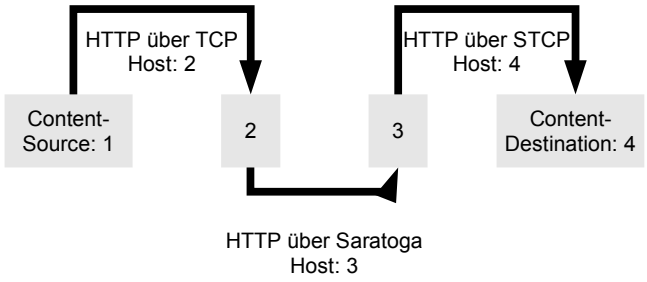


Abb. 6: HTTP in einem DTN über mehrere Transportprotokolle

Wichtig ist dabei, dass ein HTTP-Server Übertragungen mit unbekanntem Content-* Typ ablehnt. Dadurch können in einem Netzwerk auch normale HTTP-Daten neben den HTTP-DTN-Daten im Netzwerk existieren, da hier die DTN-Daten von den normalen HTTP-Servern abgelehnt und nur von den HTTP-DTN-Servern angenommen und verarbeitet werden [5].

Da HTTP von sich aus kein Ablaufdatum für die Daten enthält lassen sich damit auch große Distanzen (sowohl zeitlich als auch räumlich) überwinden, vorausgesetzt das Transportprotokoll unterstützt diese. Mit HTTP/1.1 werden noch mehr für DTNs nützliche Funktionen unterstützt. So ist es durch Pipelining möglich mehrere Objekte direkt nacheinander zu verschicken ohne nach jedem auf eine Antwort warten zu müssen [5].

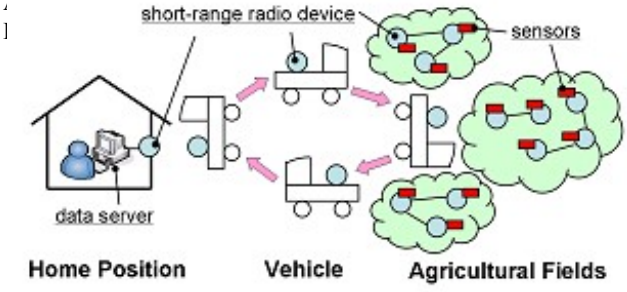
4.1.4 HTTP und das Bundle Protokoll

Bei der Verwendung von HTTP (mit MIME) anstelle des Bundle Protokolls in einem DTN bleiben viele Probleme bestehen. So ist es bei der Implementierung eines Ablaufdatums wichtig, die Zeit über den gesamten Übertragungsweg synchron zu halten. Auch die Probleme beim Routing in einem DTN bleiben gleich. Trotzdem hat HTTP einen großen Vorteil gegenüber dem Bundle-Protokoll. Durch die als Text spezifizierten Header ist es bei HTTP leichter möglich diese zu verändern und anzupassen. Beim Bundle-Protokoll ist diese Information im Binärformat gespeichert, dies erschwert die Anpassung des Protokolls [5].

4.1.5 Folgerung

HTTP als vom Transportprotokoll unabhängiges Übertragungsprotokoll sollte nicht nur zusammen mit TCP verwendet werden. Für viele Anwendungszwecke gibt es geeignetere Transportprotokolle, hierdurch wäre HTTP mit MIME für die Datenübertragung in einem DTN geeignet. Die Anwendungen sollten dabei HTTP (und MIME), unabhängig vom Transportprotokoll, verarbeiten können. Dies lässt Flexibilität bei der Wahl des Transportprotokolls und Netzwerkaufbaus zu.

4.2 DTNs in der Landwirtschaft



DTNs können auch in der Landwirtschaft benutzt werden. Um den Ertrag zu steigern und die Arbeit besser planen zu können, sind detaillierte Informationen über Temperatur sowie Luft- und Bodenfeuchtigkeit notwendig. Lässt man diese Informationen von Sensoren sammeln, muss die Übertragung der Daten zur Auswertung geklärt werden. Mobilfunkkommunikation ist zwar technisch möglich, jedoch sind hierbei die monatlichen Kosten nicht unerheblich. So können mehrere Sensoren für ein Feld nötig sein. Bei einer Anbindung dieser Sensoren über Mobilfunk müsste für jeden von ihnen eine Gebühr bezahlt werden, was in der Praxis häufig zu teuer ist [6]. Auch ist eine lückenlose Netzabdeckung in landwirtschaftlichen Gebieten nicht gewährleistet.

Um diese Kosten einzusparen kann ein DTN zum Sammeln dieser Daten eingesetzt werden. Hierbei kann die Übertragung zwar nicht so häufig stattfinden wie beim Mobilfunk, dafür fallen jedoch, neben den Anschaffungskosten, keine weiteren Kosten für die Datenübertragung an. Die Sensoren sind dabei mit Nahfunk ausgestattet, um ihre Daten kabellos an mobile Datenspeicher (wie beim Lappland-Experiment) zu übertragen. Diese Datenspeicher werden dabei entweder von den Arbeitern bewegt, oder an den Landmaschinen angebracht (Abb. 7). Die Landmaschinen sammeln dann automatisch Informationen während der Arbeit. Nach Beendigung dieser können die gesammelten Informationen dann übertragen und ausgewertet werden [6].

Eine solche Lösung kann vergleichsweise kostengünstig eingeführt und betrieben werden, erfordert aber mehr Aufwand als bei Übertragung über Mobilfunk da die Sensoren immer wieder abgefragt werden müssen. Abhängig vom Zeitintervall dieser Abfragen ist die Aktualität der Daten [6].

5. Zusammenfassung

Die betrachteten Experimente und Tests zeigen, dass DTNs ein Bereich sind in dem zwar geforscht wird und vieles theoretisch klar scheint, beispielsweise der Vorteil des Bundle-Protokolls beim DTN für die mobile Kommunikation (siehe Kapitel 3), in dem es aber auch einigen Platz für Optimierung gibt. Diese können sowohl praktischer (Verbesserung der Geschwindigkeit der DTN-Proxys und der Prefetching Effizienz) als auch theoretischer (Routing interner Emails) Art sein.

Auch zeigt sich, dass DTNs in vielen unterschiedlichen Bereichen hilfreich sein können. In Gebieten mit schwacher Infrastruktur zur Bereitstellung eines Internetzugangs und in Gebieten mit starker Infrastruktur zur Beseitigung der letzten Versorgungslücken und zur Entlastung der Netzwerke mit weniger Kapazität. Probleme

doi: 10.2313/NET-2011-07-2_16

wie die Identifizierung des Zielknotens und das Routing haben die meisten DTNs gemeinsam. Auch die Auswahl des richtigen Protokolls zur Bündelung der Daten ist in einem DTN sehr wichtig. Funktionierte das Bundle-Protokoll in Lappland gut so zeigte sich trotzdem (Kapitel 3), dass es noch viel Optimierung bedarf, um es in zeit- und bandbreitenkritischeren Umgebungen einsetzen zu können.

Kaum Beachtung findet bei diesen Projekten für gewöhnlich das Transportprotokoll. Bei näherer Betrachtung sollte jedoch klar werden, dass hier, ein entsprechendes Protokoll auf Anwendungsebene vorausgesetzt, ein Wechsel auf ein anderes Protokoll sinnvoll und möglich sein könnte. Durch Wahl eines geeigneten Transportprotokolls, in einigen Bereichen gibt es gute Alternativen zu TCP, kann die Effizienz und Stabilität des DTNs erhöht werden.

Nicht zu vernachlässigen ist jedoch, dass immer mehr Einsatzgebiete für DTNs mittlerweile von Mobilfunk abgedeckt werden können. Aufgrund fortschreitender Entwicklung im Mobilfunkbereich, sowohl auf Technologie- als auch auf Kostenebene, könnte direkter Mobilfunk in Zukunft die dem DTN bevorzugte Alternative sein. Grund dafür sind niedrigere Latenzen und dauerhaft verfügbare Verbindungen mit stetig steigenden Übertragungsraten, während der Stromverbrauch und die Kosten immer niedriger werden. Dadurch kommt er für immer mehr Gebiete in Frage.

6. Quellen

[1] Lindgren A. und Doria A.; „Experiences from Deploying a Real-Life DTN System“, IEEE, 2007

[2] Doria A., Uden M. und Pandey D.P.; „Providing connectivity to the Saami nomadic community“, ThinkCycle, 2002

[3] Ott J. und Kutscher D.; „Applying DTN to Mobile Internet Access: An Experiment with HTTP“, Technical Report TR-TZI-050701, 2005

[4] Ott J. und Kutscher D.; „The „Drive-thru“ Architecture: WLAN-based Internet Access on the Road“, IEEE Semiannual Vehicular Technology Conference Mai 2004, 2004

[5] Wood L., Holliday P., Daniel Floreani und Psaras I.; „Moving data in DTNs with HTTP and MIME“, IEEE, 2009

[6] Ochiai H., Ishizuka H., Kawakami Y., Esaki H.; „A Field Experience on DTN-Based Sensor Data Gathering in Agricultural Scenarios“, IEEE Sensors 2010 Conference, 2010

[7] http://www.nasa.gov/mission_pages/station/research/experiments/DTN.html, aufgerufen am 24.05.2011

doi: 10.2313/NET-2011-07-2_16

Vergessene DTNs: Mailbox-Netze und UUCP

Alexander Waldmann
Betreuer: Nils Kammenhuber
Hauptseminar - Innovative Internettechnologien und Mobilkommunikation
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: waldmann@in.tum.de

KURZFASSUNG

Diese Arbeit beschäftigt sich mit historischen Delay-Tolerant Networking Systemen, die vor der Verbreitung des Internets existierten. Neben UUCP und dem Usenet werden auch heute kaum noch wahrnehmbare Netze, wie das FidoNet und das Z-Netz, beleuchtet. Neben den technischen Details der damaligen Protokolle werden besonders die Netzstrukturen und die Verbreitung betrachtet. Für jedes der behandelten Netze bzw. ihre Protokolle wird erklärt, warum diese heute nicht oder kaum mehr verfügbar sind.

Schlüsselworte

DTN, Delay Tolerant Networking, Unix to Unix Copy, UUCP, FidoNet, Zconnect, UseNet

1. EINLEITUNG

Heutige Rechensysteme basieren meist auf einer durchgehend verfügbaren Verbindung in das World Wide Web[1]. Die Entwicklung des WWW begann in den 1969 und wurde in den folgenden Jahrzehnten rasant voran getrieben. Heute ist ein Anschluss an das globale Netz für einen großen Teil der Bevölkerung selbstverständlich. Der Umbruch zwischen 1970 und 2000 ging aber nicht ohne Konkurrenzmodelle vonstatten. Die flächendeckende Versorgung mit Hochgeschwindigkeitsanbindungen begann erst Ende der 90er Jahre. In dieser Zeit war eine stabile und lang währende Verbindung zwischen zwei Rechensystemen nicht die Regel, sondern die Ausnahme. In diesem Kontext behandelt diese Arbeit "Delay-Tolerant Networking"-Systeme, die vor der breiten Versorgung privater Haushalte mit Internet-Anschlüssen entstanden. Der Fokus liegt dabei auf vier Systemen, die heute nicht mehr oder nur noch wenig im Gebrauch sind, zu ihrer jeweiligen Höchstzeit aber weit verbreitet waren.

1.1 Motivation

"Delay Tolerant Networking"[2] beschäftigt sich mit der Problematik nicht ständig verbundener, heterogener Netzwerke[1]. Ende der 90er Jahre wurde im Auftrag der NASA ein Konzept und eine grundlegende Architektur für ein "Interplanetary Internet (IPN)"[3] geschaffen, das sich im Besonderen auf Probleme bezog, die bei Netzwerkverbindungen ins All entstehen würden. Im Jahr 2003 griff Kevin Fall dieses Konzept auf und veröffentlichte sein eigenes Konzept unter dem Namen "Delay Tolerant Networking"[51], welches in den folgenden Jahren viel diskutiert wurde und schließlich zum RFC 5050[4] und RFC 4838[5] führte, die sich mit der "für die Entwicklung von Algorithmen und Anwendungen notwendigen Übersicht über Anforderungen für die in einem DTN eingesetzte Software"[1] beschäftigt.

Allerdings entwickelten sich Ende der 70er Jahre aus der Not, dass das Internet noch nicht bis in die privaten Haushalte vorgedrungen war, die Vorläufer dessen, was man heute unter dem Sammelbegriff DTN versteht (siehe Abb. 1). Das Internet, wenn seine Anfänge auch im Jahre 1969 liegen [2], war in den 80er Jahren noch Unternehmen vorbehalten, für die eine teure Datenleitung rentabel war [29]. In dieser Zeit finden sich eben jene Voraussetzungen, die DTN zu meistern versucht: Rechensysteme waren nur spärlich über Telefonleitungen verbunden, da die Preise für Telefongespräche nur nachts in überschaubaren Dimensionen lagen. Standards setzten sich nur allmählich durch und das Netz war meist heterogen zusammengesetzt. Ohne die erst später geschaffenen Grundlagen erschufen die gerade entstehenden Netz-Gemeinden Applikationen, die dieser Problematik Rechnung trugen und trotz kleiner Kommunikationszeitfenster ein dynamisches Netz schufen. Abbildung 1 beschreibt den Zeitraum in welcher die in dieser Arbeit behandelten Technologien entwickelt und genutzt wurden. Jede dieser Technologien wird im folgenden kurz angeschnitten und in einem eigenen Kapitel ausführlich behandelt und eingeordnet.

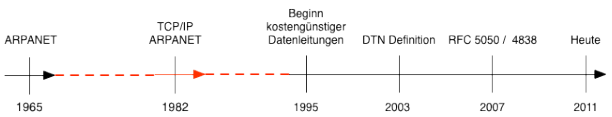


Abbildung 1: Einordnung des behandelten Themas (rote Linie)

1.2 Überblick

Die folgenden vier Systeme werden in dieser Arbeit näher beleuchtet. Vor allem ihre Verbreitung sowie ihre technische Legitimation wird betrachtet:

1. **Unix to Unix Copy Protocol** [6]

   Das UUCP ist ein Protokoll, das ursprünglich zum direkten Datenaustausch zwischen zwei Endpunkten

[1] Abkürzung: WWW
[2] Abkürzung: DTN
[3] Übersetzung: Internet zwischen Planeten
[4] http://tools.ietf.org/html/rfc5050
[5] http://tools.ietf.org/html/rfc4838
[6] Abkürzung: UUCP

doi: 10.2313/NET-2011-07-2_17

(meist Unix Derivaten) benutzt wurde und wird. Aufgrund seiner universellen Einsetzbarkeit und der Unterstützung einer Vielzahl von Transportmedien [7] war es weit verbreitet. Auf ihm basierte anfänglich das Usenet.

2. **FidoNet**

   Das FidoNet ist ein hierarchisch angeordnetes Mailbox-Netz, das zu Spitzenzeiten ca. 30.000 Teilnehmer aufweisen konnte[29] und global verfügbar war. Mit dem Siegeszug des Internets wurde das FidoNet nach und nach verdrängt.

3. **ZConnect**

   ZConnect ist ein Protokoll-Standard, der sich mit dem Austausch von Mails und auch Foren beschäftigt[26]. Bereits 1998 wurde die Entwicklung mangels Kompatibilität mit anderen Netzen und größerem Wachstum dieser Netze eingestellt[26].

4. **Usenet**

   Das Usenet ist ein weltweites Foren-Netzwerk, das Diskussionsraum für beliebige Themen bietet und jedem Interessenten offen steht. Ursprünglich sollte es als freie Alternative zum ARPANET dienen[37].

2. UNIX TO UNIX COPY

Das "Unix to Unix Copy"-Protokoll ist kein alleinstehendes Protokoll, sondern vielmehr eine Reihe von Programmen und zugehörigen Protokollen, die in den Bell Laboratories[7] unter Mike Lesk entstanden. Der Zweck von UUCP liegt nicht nur in der Übertragung von Daten und Mails zwischen zwei Endpunkten, sondern auch in der Ausführung von Programmen auf einem Zielrechner. Anfang der 80er Jahre begann die Verbreitung der Programmsammlung und wurde in den darauffolgenden Jahren zu einem der de-facto Standards zum Datenaustausch. Bereits 1979 wurde das Programmpaket in Unix Version 7 [6] ausgeliefert. Das ursprünglich für UNIX entwickelte Paket ist allerdings auch auf anderen Plattformen verfügbar (MSDOS[7]) und noch heute integraler Bestandteil aller UNIX-Derivate.

Einige der wichtigsten Programme des UUCP Paketes: [4]

- **uucp** Mit diesem Programm werden Daten zwischen zwei Endpunkten ausgetauscht. Die Adressierung wird über einen Bangpath realisiert.
- **uux** Durch dieses Kommando wird auf einer entfernten Maschine die Ausführung eines Programms beantragt.
- **uustat** Dieses Werkzeug kontrolliert das langfristige Verhalten von UUCP. Aufträge können gestoppt und angezeigt werden, sofern sie noch nicht abgearbeitet sind.
- **uuname** Der Name der eigenen Maschine im UUCP-Namensraum, sowie alle bekannten Rechensysteme, werden durch dieses Programm aufgelistet.
- **uulog** Logfiles werden durch dieses Programm gelesen. Es dient zu Verwaltungs- und Wartungsaufgaben.
- **uuto, uupick** Erweitert UUCP um die Benachrichtigung des Nutzers am Zielrechner.

Die kleine, lose Programmgruppe, die das UUCP-Paket bereitstellt, war die Basis des schnell wachsenden UUCP-Netzes in den 80er Jahren. Im Hintergrund arbeiten auf einem Rechensystem, welches sich dem UUCP-Netz anschließen will, zwei Daemons.

- **uucico** Dieser Daemon kommuniziert mit dem entfernten System und wird direkt über das Programm uucp angesprochen.
- **uuxqt** Dieser Daemon führt die durch uux in Auftrag gegebenen Programme aus.[4]

UUCP vollzog zwischen 1980 und 1991 eine bemerkenswerte Evolution: Nicht nur der Umfang der Programmgruppe wuchs, sondern das Paket wurde von AT&T[8] Mitarbeitern auch neu geschrieben. Diese stellten ihre Implementierung kostenpflichtig zur Verfügung. Das ab 1990 verwendete Taylor UUCP[9] ist allerdings nach Ian Lance Taylor benannt, dem Autor der abermals neu geschrieben Programmgruppe, der diese jedoch kostenfrei unter der GPL veröffentlichte[5].

2.1 Der Handshake

Ein Verbindungsaufbau zwischen zwei Punkten setzt voraus, dass beide Partner das UUCP Paket gestartet haben. Dies wird durch einen vorausgehenden Login auf dem Zielrechner und das anschließende Starten des UUCP Programmpakets bewerkstelligt. Dieser Schritt ist zwar für jede UUCP Kommunikation notwendig, ist aber nicht Teil der Protokollspezifikation. Das Basisprotokoll für einen Handshake ist insofern ungewöhnlich, als dass der Handshake nun vom angewählten Zielrechner begonnen wird[11]. Der Handshake läuft folgendermaßen ab:

Listing 1: Ein UUCP Handshake

```
called: '\020Shere=hostname\000'
caller: '\020Shostname␣options\000'
called: '\020ROK\000'
called: '\020Pprotocols\000'
caller: '\020Uprotocol\000'
```

Ein Zielsystem teilt seinem Ansprechpartner, mit dem er direkt verbunden ist in einer ersten Phase seinen Hostnamen mit, um daraufhin eine Antwort des verbindenden Hosts zu bekommen, die eine Reihe von Optionen spezifizieren kann. Im Anschluss werden diese Optionen ausgehandelt und das zu verwendende UUCP Basisprotokoll spezifiziert. Dieser letzte Schritt ist notwendig, da UUCP nicht über Versionsnummern verfügt, sondern stets um neue Protokoll-Spezifikationen erweitert wurde. Die letzte einflussreiche Spezifikationen stellt das durch Taylor-UUCP eingeführt i-Protokoll dar[11]. Nach einem solchen Handshake nehmen UUCP-Teilnehmer Befehle entgegen, die auch das Weiterleiten von Nachrichten auf ein weiteres System[10] beinhalten können.

[7] Microsoft Disk Operating System

[8] American Telephone & Telegraph Corporation

[9] http://www.airs.com/ian/uucp-doc/uucp_toc.html

[10] Auch "Hop"genannt

doi: 10.2313/NET-2011-07-2_17

2.2 Das UUCP Netz

Das UUCP Netz ist ein loses Netz aus Knoten. Es verfügt über keinerlei zentrale Instanzen. Der Name UUCP-NET steht für die Gesamtheit aller lose gekoppelten Systeme innerhalb dieses Verbundes[7]. Eine Stärke und gleichzeitig auch Schwäche von UUCP ist diese Struktur des Netzes. Das Netz ist aufgrund der inhärenten Eigenschaften eines DTN schwach gekoppelt. Es existiert kein Routing wie es durch das Internet üblich wurde. Pfade durch das Netz müssen manuell von Teilnehmern des Netzes beschrieben werden. Dies ist nützlich, da verschwindende Knoten keine Problematik darstellen, erhöht aber den Aufwand, diese Netze zu nutzen und zu warten. Jeder Knoten verwaltet stets eine Liste von anwählbaren Systeme. Dies waren im Allgemeinen jene Systeme, die auch geografisch in der Nähe des Teilnehmers lagen, meist sogar im selben Ortsteil, um billige Telefonangebote nutzen zu können. Andere Teilnehmer konnten nicht automatisiert identifiziert werden. Aus dieser Problematik erwuchs das UUCP Mapping Projekt. Es versuchte, diese Unzulänglichkeiten im Bereich der Mail-Relays zu beheben. Anbieter eines Mail-Relays sendeten dem Projekt per E-Mail Listen mit anwählbaren Knoten und ihrer Bewertung der zugehörigen Verbindung zu. Diese Daten wurden gesammelt, zusammengeführt und monatlich in Newsgroups veröffentlicht, um das Routing durch das Netz zu erleichtern. War ein Teilnehmer im Besitz einer solchen Liste, konnte er selbst oder mit Hilfe eines Path-Finding[11] Programms Routen zu Zielrechnern berechnen.

E Mail-Adressierung. Besondere Popularität genossen Mail-Box Systeme, die in ihrer Struktur heutigen Webforen ähnelten. Die Adressierung innerhalb des Netzes wird durch sogenannte ”bangpaths”realisiert. Eine Mail-Adresse bestand aus dem voll qualifizierten Namen eines Rechensystems und der zugehörigen Route. Die einzelnen Hosts werden dabei durch ”bangs”[12] getrennt und der Zielteilnehmer durch seinen Namen beschrieben.

nextMachine!targetMachine!targetUser (Abb.: 2)

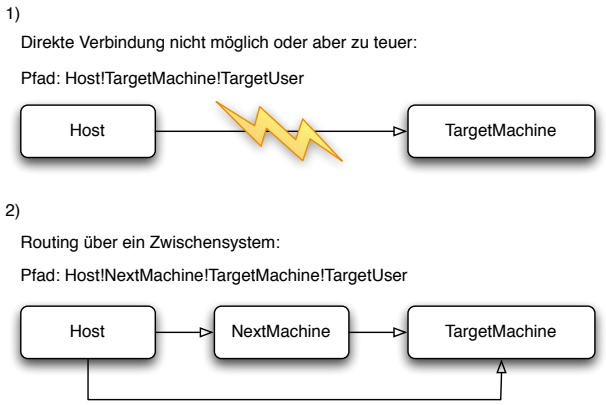


Abbildung 2: Bangpath Routing ohne HOP (1) und mit HOP (2)

[11]Beliebter Path-Finder: pathalias
[12]Ausrufezeichen

Diese Adressierung ist heute noch in Usenet Gruppen üblich, auch wenn sie keine technische Legitimation mehr besitzt. In den 80er Jahren waren Bangpaths mit bis zu 10 Hosts nicht außergewöhnlich[7].

Netzgröße. Die ehemaligen UUCP Netze (und das darauf basierende Usenet) waren neben FidoNet der de-facto Standard für die Kommunikation mit Endsystemen. Die Teilnehmerzahl war bereits Anfang der 1980er beträchtlich, wie die UUCP-Maps dieser Jahre zeigen. 1983 hatte sich in Amerika eine feste Netzgemeinde gebildet (Eine alte Karte des UUCP-Netzes ist in Abbildung 3 zu sehen). Das UUCP-Netz war nicht regional beschränkt, sondern agierte global.

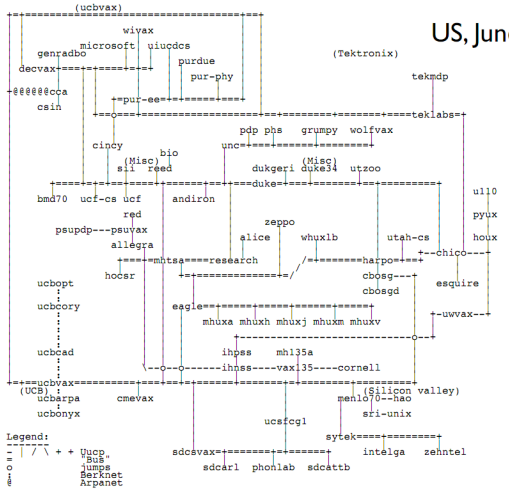


Abbildung 3: UUCP Map 1981[3]

Das Internet. Mit den nahenden 90er Jahren boten immer mehr UUCP-Teilnehmer Schnittstellen in das Internet an und boten so einer großen Gruppe Zugang zu diesem Netz, ohne dass diese selbst eine entsprechende Datenleitung besitzen mussten[2].

2.3 Aussterben

Kleine Netze existieren bis heute, der Großteil der Community ist aber zerfallen. Das Ende der UUCP basierten Netze markiert das Auflösen des UUCP Mapping Projektes Ende 2000. Das später in dieser Arbeit behandelte Usenet, das anfänglich auf UUCP beruhte, begann bereits Mitte der 80er Jahre auf NNTP[13] umzusteigen und basiert heute nicht mehr auf UUCP. Datenleitungen wurden zunehmend billiger und die Legitimation des UUCP, das DTN, wurde zunehmend unwichtiger. TCP/IP[14], SMTP[15] sowie NNTP ersetzten UUCP.

[13]Network News Transfer Protocol
[14]Transmission Control Protocol / Internet Protocol
[15]Simple Mail Transfer Protocol

doi: 10.2313/NET-2011-07-2_17

3. FIDONET

Das FidoNet ist ein ab den 80er Jahren äußerst populäres, demokratisch aufgebautes Mail-Box Netz, das weltweit genutzt und unterstützt wurde[30]. Das Netzwerk basiert auf einem 1984 veröffentlichten Mailbox-Programm namens "Fido", benannt nach dem Hund seines Autors "Tom Jennings"[28]. Fido und FidoNet stellen eine Protokollsammlung für "Bulletin Board System"[16][17] dar. Jennings ist aber nicht alleiniger Gestalter und Erbauer des Netzes. Die Fido-Protokolle und mechanismen wurden schnell von anderen Autoren und BBS-Betreibern adaptiert, um ein heterogenes Netz zu ermöglichen. Das FidoNet war ursprünglich auf dieses Anwendungsgebiet (Netmail) begrenzt[30]. Seine enorme Popularität führte aber schnell zur Erweiterung der Protokolle. Die bekannteste und wichtigste Erweiterung, die das FidoNet definiert und dem UseNet annähert, ist EchoMail:

EchoMail. Die bedeutendste Protokollerweiterung ist das Echomail Protokoll. Dieses spezifizierte das Übertragen gebündelter BBS Nachrichten und ermöglichte es dadurch einer großen Gruppe von Teilnehmern zu diskutieren[29]. Diese Struktur ist mit heutigen Webforen vergleichbar, die allerdings, anders als im Fido Netzwerk, nicht untereinander vernetzt sind. Abbildung 4 zeigt einen alte FidoNet Mail-Reader der eine EchoMail anzeigt. Im unteren Teil des Fensters zeigt sich die hierarchische Struktur der EchoMail. Ein

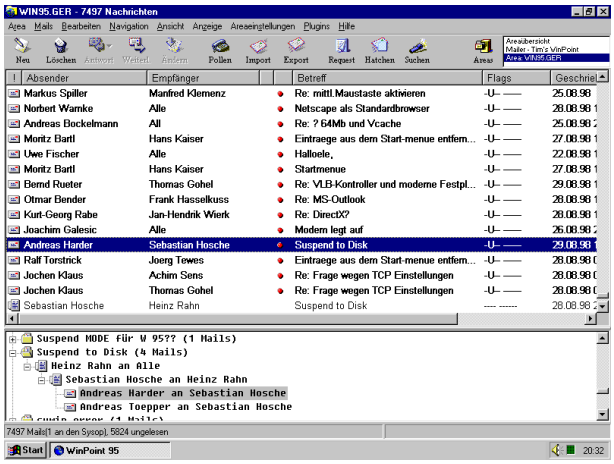


Abbildung 4: WinPoint 95 EchoMail [17]

Echo besaß im Allgemeinen einen Moderator, der für das Einhalten der Netiquette verantwortlich war. Echomails waren ursprünglich nicht vorgesehen, bildeten aber bald nach ihrer Verwirklichung den wesentlichen Bestandteil des Netzes. [30][16][18].

3.1 Die Struktur des Netzes

Das FidoNet teilt allen Rechensystemen im Netzwerk unterschiedliche Rollen zu. Diese wiederum sind hierarchisch organisiert. Die Rollen tragen der geografischen Verteilung des Netzes Rechnung. Eine Adresse innerhalb des FidoNet besitzt folgende Struktur:

[16] AKBürzung: BBS
[17] Deutsch: Mailbox-System
[18] Archiv: http://fidonet.ozzmosis.com/

Tabelle 1: Die 6 Zonen des FidoNet[22]

Zone 1	Nordamerika - USA, Kanada
Zone 2	Europa & Westeuropa, Osteuropa
Zone 3	Australien
Zone 4	Lateinamerika (Südamerika)
Zone 5	Afrika
Zone 6	Asien

Tabelle 2: Einige Regionen de FidoNet[16]

...	...
Deutschland	Region 24
...	...
Schweiz	Region 30
Oesterreich	Region 31
...	...

2:244/1120.1

Die durch :, / und . getrennten Zahlen stellen die einzelnen Ebenen des Netzes dar. Beginnend mit der ersten Nummer beschreiben sie folgende Hierarchie:

1. **Zonen** Die Zone ist das höchste Element der Hierarchie[19]. Eine Zone ist ein geografisch abgegrenzter Raum, in dem sich FidoNet Systeme befinden. Das FidoNet teilt sich in die Zonen aus Tabelle 1.

   Alle Systeme, die nicht dem FidoNet angegliedert waren, sich also strukturell und politisch davon trennten, wurden in den Zonen 7-4095 zusammengefasst[33]. Zonen werden von mehreren, organisatorisch getrennten Koordinatoren geleitet und überwacht[22]. Diesen Zonenkoordinatoren fällt die Aufgabe der Verwaltung von Nodelisten zu, das Überwachen von Echomails und andere organisatorischen Aufgaben[18]. Ihnen ist nur der internationale Zonenkoordinator übergeordnet, der "vergleichbar mit einem Aufsichtsratsvorsitzenden einer AG"[21] ist.

2. **Netz/Region** Netze stellen das nächste Glied in der baumartigen Struktur des FidoNet dar[20]. Sie beschreiben einen kleineren geografischen Bereich innerhalb einer Zone (meist Länder oder Bundesstaaten) und besitzen, ähnlich einer Zone, einen Koordinator. Teil einer Netzbeschreibung war oft eine Region, die einen administrativen Überblick geben sollte. Die Region besteht aus den ersten beiden Ziffern eines Netzes[21], die folgenden Ziffern beschreiben das Netz[22][21]. Administrativ wurde sowohl der Zone als auch dem Netz ein Koordinator zugeteilt. Einige Regionen stellt beispielhaft Tabelle 2 dar.

3. **Knoten**[23] Ein Knoten ist ein aktiver Teilnehmer des FidoNet, meist ein privater Nutzer. Knoten folgen der

[19] Im Beispiel: 2
[20] Im Beispiel: 244
[21] Im Beispiel: 24
[22] Im Beispiel: 4
[23] Meist als Node bezeichnet

doi: 10.2313/NET-2011-07-2_17

FidoNet-Policy und können als sogenannter Bossnode fungieren. Ein Bossnode wiederum ist ein Anwahlpunkt eines Punktes, der meist im selben Ortsteil des Knoten zu erwarten ist, um Telefonkosten zu sparen[20]. Ein solcher Knoten hat alle Rechte und Pflichten, die die FidoNet-Policy definiert. Die Menge aller Knoten wird in der "Nodelist" festgehalten und beschreibt alle aktiven Teilnehmer des Netzes. Die jeweiligen Koordinatoren sind für das Zusammenstellen ihrer Liste verantwortlich und leiten diese an die nächst höhere Instanz weiter.

4. **Punkte**[24] Ein Punkt ist der hierarchisch niedrigste Teilnehmer des Netzes. Er ist allen anderen Teilnehmern des Netzes untergeordnet und nimmt am Mail-Austausch des FidoNet teil. Gewöhnliche Anwender teilen sich in Knoten und Punkte. Abbildung 5 stellt anhand des gewählten Beispiels die Struktur des Netzes dar.

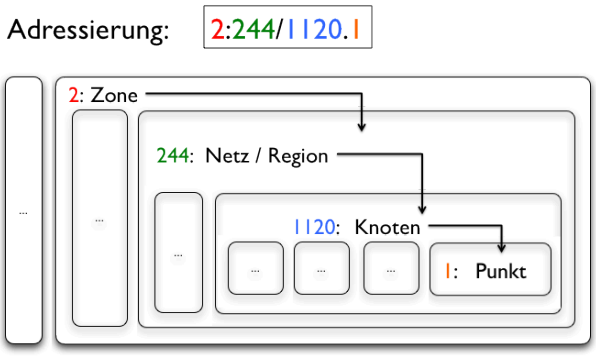


Abbildung 5: Hierarchie der Rollen des FidoNet

Technical Standards. Die FidoNet Community bildete ein "FidoNet Technical Standards Committee"[25], das sich mit der Dokumentation der technischen Entwicklung des FidoNet auseinandersetzte[19]. Dieses Komitee brachte ein Standarddokument hervor, das die Mindestanforderungen für ein System spezifiziert, das am FidoNet teilnehmen will[30]: FTS-001, das bis 1995 aktualisiert wurde[26]. FTS-001 spezifiziert im Detail:

Handshake Die erforderlichen Protokolle zum Verbindungsaufbau zwischen Fido Systemen.

Transfer Eine Sammlung von Protokollen zum Austausch von Netnews und Daten.

Message Format Das Format, in dem Nachrichten im FidoNet übertragen werden.

[32]

[24]Meist als Point bezeichnet
[25]Abkürzung: FTSC
[26]http://www.ftsc.org/docs/fts-0001.016

Routing. Das Routing innerhalb des FidoNet folgt meist der hierarchischen Struktur, die durch die Zonen, Regionen und Netze vorgegeben ist. Das Netz ist sternförmig um einen Punkt der nächsten Ebene organisiert. Innerhalb eines Netzes existieren Elemente, die nicht explizit in der Hierarchie Erwähnung finden. Sogenannte HUBs nehmen Mail-Pakete entgegen und verteilen sie unter den Nodes. Grundsätzlich kann jeder FidoNet-Teilnehmer direkt mit einem anderen kommunizieren. In der Realität wurden aber vor allem Echo-Mails durch die Hierarchie geleitet.

Eine Nachricht, die Teil einer Echomail ist, bewegt sich von einem Node entlang der Hierarchie:

1. **1:170/918.12 (point)** Ein Punkt erstellt eine Mail.
2. **1:170/918.0 (node)** Ein Knoten empfängt die Mail aus einem Bereich, für den er sich verantwortlich zeichnet.

   (1:170/900 (hub) Dieser legt seine Mails auf einem Sammelsystem, dem HUB, ab oder sendet direkt an den zuständigen Netz-Koordinator.**)**
3. **1:170/0.0 (net coordinator)** Der Netz-Koordinator empfängt die Nachricht und schleust sie in der Hierarchie weiter hinauf.
4. **1:19/0 (region coordinator)** Der Region-Koordinator teilt seine gesammelten Informationen wiederum mit dem nächsten Element der Hierarchie:
5. **1:1/0 (zone coordinator)** Der Zonen-Koordinator stellt das letzte Element der Routing-Kette dar. Von hier aus werden Nachrichtenpakete zwischen den Zonen, über sogenannte Zonen-Gateways, verteilt. Für jede Zone innerhalb des FidoNet existiert hierfür ein eigenes Gateway pro sendende Zone[23].

[31][21]

Diese Schema ist in Abbildung 6 noch einmal zusammengefasst. Die nachricht bewegt sich vom niedrigsten Teil der Hierarchie bis zum höchsten, dem Netz-Koordinator. Um die zeitnahe Übertragung von Nachrichten zu garantieren, wurde eine Zone-Mail-Hour eingeführt, die einen Zeitraum spezifizierte, in dem Nodes für eingehende Nachrichten erreichbar sein mussten. Dieser Umstand erwuchs aus der Tatsache, dass die meisten Teilnehmer sowohl für das Senden als auch Empfangen dieselbe Telefonleitung nutzten[30]. Eine parallele Verarbeitung (wie zum Beispiel über Datenleitungen) war nicht möglich.

3.2 Das Netzwerk

Das FidoNet wuchs Mitte der 80er Jahre rasant an und entwickelte sich in den folgenden 10 Jahren zum größten Mailbox-Netz weltweit. Die Nutzerzahlen wuchsen bis ins Jahr 1995 fast exponentiell an. Jeder konnte und kann noch immer Teilnehmer des FidoNet werden. Einzige Voraussetzung sind der Besitz der Software und die Kenntnis eines Einwahlpunktes. Das FidoNet ist strukturell wesentlich klarer organisiert als beispielsweise UUCP. Mitglieder konnten

doi: 10.2313/NET-2011-07-2_17

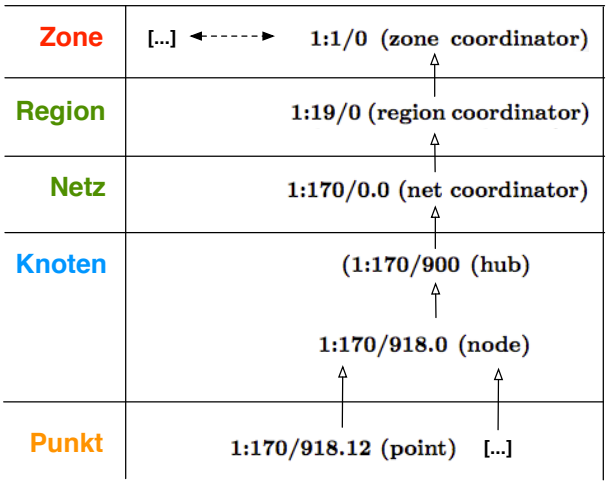


Abbildung 6: Routing durch das FidoNet

demokratisch an der Gestaltung des Netzes teilnehmen, indem sie ihre Vertreter (bzw. Koordinatoren) auf der jeweiligen Ebene wählten. Dieses Recht war jedem Teilnehmer vorbehalten. Politische Diskussionen über den Aufbau des Netzes waren nicht ungewöhnlich, was 1993 aufgrund steigender Kosten für Hubs und Netzkoordinatoren sogar zu einem Abspalten der Region 2:24 (Deutschland) führte. Aus dieser Trennung erwuchsen das FidoNet-Lite (der sich abspaltende Teil) und FidoNet-Classic (der alte Teil des FidoNet)[29], welche sich Ende 1995 aber wieder vereinten[12] und ein Netzwerk mit über 35.000 Teilnehmern bildeten[14].

Das Internet. Das FidoNet selbst war strukturell dem Internet entgegengestellt, da es seinen eigenen Adressraum pflegte und sich selbst verwaltet. Es existieren trotz alledem Gateways zum Internet oder in das Usenet[30]. Diese Gateways sind die vom FidoNet abgetrennten Zonen (ab Zone 7). Aus diesen Zonen erwachsen auch Konzepte, FidoNet über IP zu nutzen [15].

3.3 Aussterben

Seine Blütezeit hatte das FidoNet 1995 mit 35.787 gelisteten Teilnehmern (Abb.: 7).

Mit dem Ende der 90er Jahre und dem Einzug des Internets in private Haushalte fallen auch die Nutzerzahlen des FidoNet dramatisch ab. Email-Verkehr wie auch Diskussionen sind im Internet wesentlich leichter und schneller nutzbar. Im Januar 2006 waren weltweit nur noch knapp 7000 Nutzer gelistet (Abb.: 8).

Diese Teilnehmerzahl wird von vielen Webforen bereits in den Schatten gestellt. Auch die Software um das FidoNet wird nicht mehr gepflegt. Die erwähnten technischen Dokumente (FTSC) liegen seit 2009 still[27]. Ein überraschendes Anwachsen der Teilnehmer des FidoNet wurde am 30. Januar 2011 beobachtet, als die ägyptische Regierung große Teile des Internets blockte. Da FidoNet für Telefon-Leitungen konzipiert wurde, konnten viele Knoten trotz der Abschaltung Informationen über das FidoNet verteilen[27].

[27]FTSC Archiv: http://www.ftsc.org/docs/

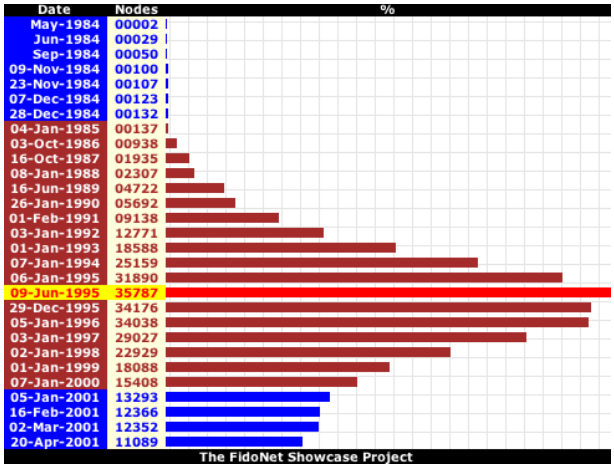


Abbildung 7: FidoNet Knoten bis 2001[14]

		Anzahl Nodes						
Zone	Name	1/1995	4/1996	1/1998	1/2000	1/2002	1/2004	1/2006
1	Nordamerika	18242	14079	6199	2003	1268	940	687
2	Europa	13378	16512	14598	11873	11067	8768	6906
3	Ozeanien	1183	1103	580	197	122	75	60
4	Lateinamerika	615	573	435	207	49	35	29
5	Afrika	126	117	91	53	87	87	14
6	Asien	1317	1228	1091	916	112	87	29
	gesamt	34866	33612	22934	15249	12655	9992	7725

Abbildung 8: FidoNet Knoten bis 2006[29]

4. ZCONNECT

ZConnect ist ein offener Protokoll-Standard aus dem Jahre 1992, der in seiner Entwicklung ein Konkurrenzmodell zum RFC-Standardisierungsverfahren darstellt[26]. Das Protokoll geht aus dem Mailboxprogramm “Zerberus“ hervor. Diese Programm wurde, ähnlich dem FidoNet, eingesetzt, um E-Mails über asynchrone Leitungen auszutauschen. Zerberus setzte hierfür anfänglich auf ein proprietäres Protokoll, das die Entwicklerfirma entwarf. Auf Zerberus basierte das Z-Netz (die Menge aller über Zerberus vernetzten Systeme) und das unter Aktivisten seinerzeit bekannte CL-Netz, das auch heute noch in Form von Usenet-Gruppen verfügbar ist. ZConnect ist ein Analogon des FidoNet und hatte folglich mit denselben Problemen zu kämpfen.

4.1 Der Entwicklungsprozess

Der Standard zeichnet sich besonders durch seinen basisdemokratischen Entwicklungsprozess aus. Der proprietäre Standard, auf welchem Zerberus aufsetzte, stellte sich Anfang der 90er als problematisch heraus: Viele Mailboxnetze folgten dem Zerberus Nachrichtenformat. Auch alternative E-Mail-Anwendungen implementierten diese Formate. Der de-facto Standard war allerdings wenig dynamisch entworfen worden. So konnten E-Mail-Adressen nicht beliebige Längen annehmen und auch die Länge des Betreffs einer Nachricht war beschränkt. Aus diesen Beschränkungen heraus er-

doi: 10.2313/NET-2011-07-2_17

schien das Entwickeln eines neuen Protokolls sinnvoll. Die Entwicklergemeinschaft hatte zu diesem Zeitpunkt bereits schlechte Erfahrungen mit der Gateway-Programmierung in das UUCP und Internet gemacht und hielt daher das RFC-Standardisierungsverfahren für unzulänglich, im Besonderen für zu ungenau. Infolgedessen entschied man sich dazu, einen eigenen Standardisierungsprozess zu entwerfen [26][28].

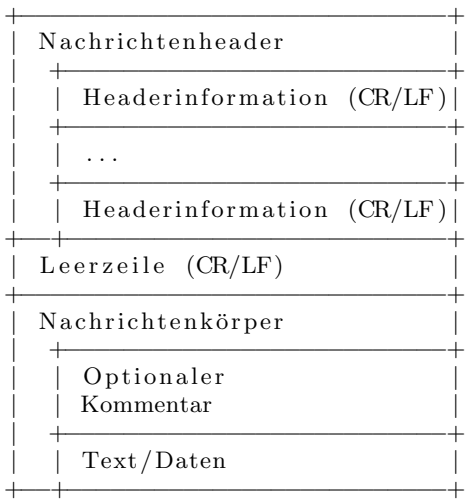
ZConnect wurde durch ein unabhängiges Gremium weiterentwickelt, das aus Anwendern, Entwicklern und Mitarbeitern der Zerberus GmbH bestand, die das ursprüngliche Protokoll entworfen hatte. Das Gremium war jederzeit in der Lage, neue Mitglieder aufzunehmen[26]. Dies ist auch heute ein noch unübliches Verfahren zur Entwicklung von Standards.

4.2 Das Protokoll

Der Standardisierungsprozess brachte einige ungewöhnliche Definitionen hervor. So wurde an einigen Stellen, meist wenn es um die konkrete Repräsentation von Inhalten ging, auf eine äußerst genaue Definition Wert gelegt, um den RFC-Unzulänglichkeiten entgegen zu wirken:

> "... der Adreßanteil vor dem "@", darf die ASCII-Codes 35 bis 124, abzüglich der Codes 64, 60, 62, 92, 28, 29, 39, 44, 91, 93, 96 und 123, enthalten. Die Codes 33, 37 und 47 (!reserviert ..."[13]

An anderen Stellen versuchte man aber, sich gleichzeitig die Flexibilität zu bewahren, die ungenaue Definitionen mit sich bringen. So wurde beispielsweise die Größe des Headers nicht beschränkt und auch nicht weiter definiert. Die Definition des Headers beschränkt sich ausschließlich auf seinen Inhalt, nur der logische Aufbau wurde konzipiert. Die folgende Definition stammt direkt aus dem ZConnect Standard:



[13]

4.3 Das Netzwerk

Auf Zerberus und ZConnect basiert das Z-Netz, über welches, ähnlich dem FidoNet und UUCP, Mails und später auch Diskussionen verschickt und geführt wurden. Der Name leitet sich von Zerberus ab, nach dem das Netz anfänglich auch benannt war. Nachdem sich Alternativen zu dieser proprietären Software entwickelten, benannte man den Verbund aus Mailboxen in Z-Netz um[24]. Aus diesem Netz löste sich auch das damals unter Aktivisten bekannte CL-Netz heraus. Innerhalb dieses Netzwerks waren "Friedens-, Menschenrechts- und Umweltgruppen und -organisationen"[50] verbunden. Seine Blütezeit erreichte dieses Splitternetz 1996, als es aus 200 Systemen bestand und auch mit anderen Ländern verbunden war[50]. 1989 begann beispielsweise Amnesty International die heute noch üblichen "urgent actions"[49] innerhalb des CL-Netzes zu verbreiten[50]. Ebenfalls wurden von den Teilnehmern rechtsextreme Vorkommnisse dokumentiert und diskutiert [50]. Diesem Mailboxnetz wurde so viel Bedeutung beigemessen, dass die rechtsextreme NPD dazu überging, das Netz zu infiltrieren [8].

4.4 Aussterben

Es stellte sich heraus, dass auch das neu eingesetzte Standardisierungsverfahren das Protokoll nicht genau genug beschrieb. Trotz penibler Definitionen der Header-Inhalte[13] stellte sich der Standard als zu ungenau heraus. Die Gateways in das immer schneller wachsende Internet stellten die Entwickler vor nahezu unlösbare Probleme[26]. Das ZConnect-Gremium stellte infolgedessen 1998 die Entwicklung des Standards ein, da er den zeitgenössischen Protokollen wenig entgegenzusetzen hatte. So fehlte in ZConnect das einfache Verschicken von Daten über eine Mail, obwohl der Standard ein eigenes Datenübertragungsprotokoll hervorbrachte[26]. Einzige überlebende des auf Zerberus und ZConnect basierenden Netzes sind Usenet-Gruppen um das Z-Netz[29] und Splittergruppen um das CL-Netz[30], die auch heute noch per Modem anwählbar sind[31] (obwohl die zugehörigen Webseiten seit Jahren (2007) nicht mehr gewartet werden[9]).

5. DAS USENET

Das Usenet basiert auf einer Gruppe von Protokollen, die die Verarbeitung von "News-Artikeln"[32] beschreibt. Es ähnelt heutigen Webforen und früheren Mailboxen, ist aber ein zusammenhängendes Netz. Die Keimzelle ist eine Sammlung von Shell-Skripten aus dem Jahr 1979 von Tom Truscott und Jim Ellis [41], Studenten der Duke University. Diese Skripte verteilten ursprünglich Nachrichten innerhalb des universitären Netzes in Form kompilierter Programme [41]. Bald darauf wurden News in Form von mailähnlichen Nachrichten ausgetauscht. Das Usenet geht aus dem bereits erwähnten UUCP Netz hervor. Es war von Beginn an ein Teil dessen und spaltete sich 1983 unter seinem heutigen Namen ab. Trotzdem basierte es lange Zeit weiter auf der UUCP Technologie. Zeitweise nutzte es auch das FidoNet zum Verteilen seiner Nachrichten. Strukturell entspricht das Usenet aber nicht dem FidoNet [41]. Das Usenet löste sich 1985 durch die Einführung des Network News Transfer Protocol[33] auch technisch von UUCP und seinem Netz. Dieses hat die Verteilung von Nachrichten basierend auf TCP/IP zum Ziel[47].

[28] Der gesamte Abschnitt stützt sich auf diese Quelle

[29] GoogleGroups unter: http://groups.google.com/groups/dir?q=z-netz

[30] Erreichbar unter: http://www.cl-netz.de/

[31] Liste unter: http://www.z-netz.de/systemliste.html

[32] Im folgenden synonym mit "Nachricht" gebraucht

[33] Abkürzung: NNTP

doi: 10.2313/NET-2011-07-2_17

Das Netzwerk steht jedem Anwender offen, der Zugang zu einem News-System hat, das Teil des Netzes ist.

5.1 Das Network News Transfer Protocol

Das NNTP ist im Zuge des Usenet entstanden und regelt die Art und Weise, in welcher Daten zwischen News-Servern aber auch News-Servern und Teilnehmern übertragen werden. Es wurde im Zuge des erstarkenden Internets im Jahre 1985 entwickelt und basiert auf TCP/IP. Seine Spezifikation wurde in RFC 997 festgehalten[34] und 2006 durch RFC 3977[35] erneuert. Die Übertragung ist dabei von der Form der Inhalte losgelöst. Nachrichten, die durch das Usenet wandern, werden unabhängig von NNTP in RFC 850[36] spezifiziert[43]. Das NNTP definiert unter anderem eine URL für Anfragen in das Usenet:

nntp://<host>:<port>/<Gruppenname>/<Artikel-ID>

[47] Auf die Host-Adresse folgt der Gruppenname und die eindeutige Artikelnummer innerhalb der Gruppe. Hierbei ist die innere Struktur der Threads und Gruppen (im Folgenden genauer erklärt) nicht von Relevanz, da jeder Beitrag eindeutig identifizierbar ist.

5.2 Das Netzwerk

Oftmals wurde der Zugang zum Usenet von Internet-Providern oder Universitäten zur Verfügung gestellt. Diese Provider stellten einen eigenen News-Server, der am Nachrichtenaustausch des Usenet teilnahm. Sie fungierten ähnlich wie ein heutiger Mail-Host. Das Bereitstellen eines solchen News-Servers stand prinzipiell jedem offen, so lange die immensen Datenmengen verarbeitet werden konnten. Bereits im Jahr 1996 transportierten einige News-Server 4,5GB Daten pro Tag[44]. In den Anfangsjahren war das Usenet kaum zensiert. Mit dem Auftreten der heute noch populären alt.binarys Gruppen, die Binärdaten sammeln, begannen einige News-Server, diese Gruppen systematisch herauszufiltern, da sie das Datenvolumen sprengten und bis zu 99% der Datenmenge ausmachten (und noch heute machen[46]).

Die Gruppen. Nachrichten werden im Usenet in Form von Gruppen gesammelt, ähnlich einem Webforum. Zwar unterstützt das Usenet das Moderieren von Gruppen, im Allgemeinen wird davon allerdings kein Gebrauch gemacht[42]. Das Usenet selbst ist nicht hierarchisch organisiert, wohl aber seine Beiträge. Jede Diskussion wird in eine Gruppe, die wiederum Gruppen beinhalten kann, einsortiert. Optisch wird diese Hierarchie durch den Pfad zu einer Diskussion sichtbar:

comp.sys.amiga[37]

Gruppen werden durch Punkte getrennt, ihre Spezialisierung von links nach rechts größer. Jede Gruppe die einen Vorgänger in diesem Pfad besitzt ist diesem direkt untergeordnet. Das obenstehende Beispiel bezeichnet das Thema des Betriebssystems “Amiga“ in der Kategorie “System“, das der Gruppe “Computer“ untergeordnet ist. Diskussionen sind öffentlich und jeder Teilnehmer, der sie lesen kann, kann ebenso an ihnen teilnehmen. Die wichtigsten Gruppen des Usenet waren und sind noch heute die ”Big Eight”[39][38]. Ursprünglich gab es nur 7 große Gruppen, die ”Major Seven”[38]. 1995 wurde aber die Gruppe “humanities“ hinzugefügt[34]:

- comp.* : Diskussionen rund um Computer (z.B.: comp.software, comp.sys.amiga)
- humanities.* : Kunst, Literatur und Philosophie, wird im deutschsprachigen Raum nicht zu den wichtigen Usenet-Gruppen gezählt (z.B.: humanities.classics, humanities.design.misc)
- misc.* : Alles was nicht in anderen Kategorien passt (misc.education, misc.forsale, misc.kids)
- news.* : Diskussionen und Neuigkeiten (Usenet Neuigkeiten, z.B.: news.groups, news.admin)
- rec.* : Entertainment (z.B.: rec.music, rec.arts.movies)
- sci.* : Wissenschaftliche Diskussionen (z.B.: sci.psychology, sci.research)
- soc.* : Soziale Diskussionen (z.B.: soc.college.org, soc.culture.african)
- talk.* : Diskussionen über kontroverse Themen (z.B.: talk.religion, talk.politics, talk.origins)

[39] Außer diesen Gruppen besitzen die meisten News-Server noch weitere Gruppen, z.B. die heute noch populären *alt.binarys*.

Der Thread. Ein Artikel bzw. eine Nachricht in einer Gruppe wird durch das Antworten eines Teilnehmers auf selbige/n zum ”Thread”[39] (Siehe Abb. 9). Jede Antwort innerhalb eines Threads ist abermals als Artikel zu verstehen und kann daher Ansatzpunkt eines untergeordneten Threads sein[40]. Diese Struktur ermöglicht angeregte Diskussionen zwischen den Teilnehmen eines Threads (ähnlich dem Zitieren von Nachrichten in einem Webforum).

Die Struktur. Das Usenet ist entgegen dem ersten Eindruck kein gekoppeltes festes Netz. Seine Inhalte sind nicht synchronisiert und erscheinen zeitversetzt auf zusammenhängenden Systemen. Das Usenet unterscheidet zwischen News-Server und einfachem Teilnehmer. Die einzelnen Server sind lose vernetzt und unterrichten sich gegenseitig über Artikel, die ihre Teilnehmer ihnen zusenden. Sind neue Inhalte verfügbar, werden diese übertragen. Usenet News-Server verlinken sich folglich nicht sondern replizieren die Daten der ihnen bekannten Systeme. Dies führt zu einer enormen Redundanz innerhalb des Netzes. Auf Basis dieses Flooding-Konzepts[45][40] erreicht ein Beitrag nach einer gewissen Zeit

[34] http://tools.ietf.org/html/rfc977
[35] http://tools.ietf.org/html/rfc3977
[36] http://tools.ietf.org/html/rfc850
[37] Nachlesbar unter: groups.google.com/group/de.comp.sys.amiga
[38] Übersetzung: Die großen Acht
[39] Folge von Diskussionsbeiträgen[48]
[40] Meint das Überschwemmen eines Netzes mit Nachrichten

doi: 10.2313/NET-2011-07-2_17

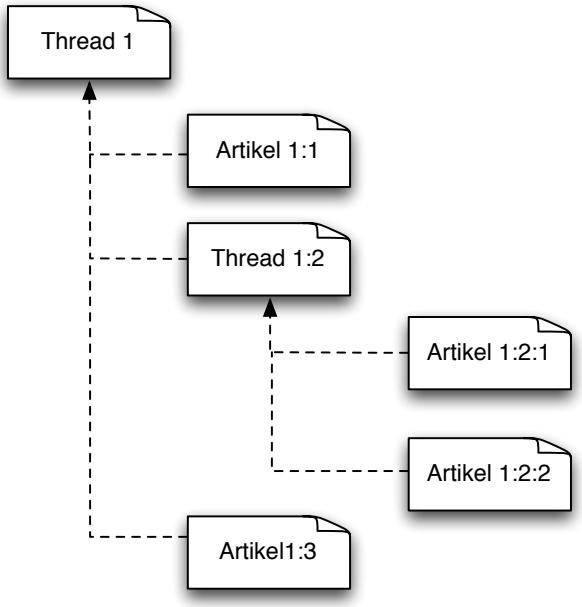


Abbildung 9: Mehrstufige Struktur einer Usenet Diskussion

alle zusammenhängenden News-Server. Spaltet sich ein News-Server vom Hauptteil des Usenet, können seine Nutzer weiterhin diskutieren, sie befinden sich aber nicht mehr auf demselben Datenstand wie der Rest des Netzes. Diese lose Struktur brachte ein global agierendes Netz hervor, wie Netflow-Diagramme aus dem Jahr 1993 offenbaren (Abb.: 10).

Abbildung 10: Newsflow 1993 innerhalb des Usenet[3] bzw. [10]

5.3 Überleben

Große Teile des Usenet bestehen bis heute und sind dank des Google Groups Projekts[41] auch für jedermann sicht- und nutzbar. Dieser Dienst bietet große Teile des Usenet an, zurückreichend bis in das Jahr 1981[35]. Auch heute existieren noch große Usenet-Anbieter, wie z.B. GigaNews[42].

[41]https://groups.google.com/
[42]https://giganews.com/

Der Traffic-Flow[43] steigt seit den ersten Tagen des Usenet stetig an. Dieser Trend ist bis heute unverändert. Im Januar 2011 bewegten sich täglich ca. 7.52 TB zwischen den News-Servern (Abb.: 11) und ca. 1,800 neue Nachrichten wurden verfasst. Dies ist aber nicht die Folge einer wach-

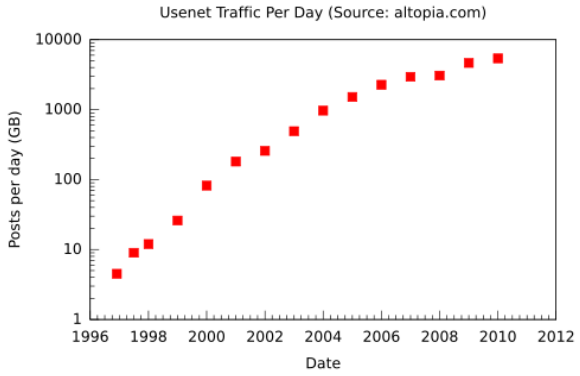


Abbildung 11: Newsflow Volumen von 1996 bis 2011[44]

senden Nutzerzahl, sondern auch auf massives Spamming zurückzuführen[44]. Viele Internetprovider schalteten in den vergangen Jahren nach und nach ihre Usenet-Zugänge ab[36]. Die Keimzelle des Usenet, die Duke University, die die erste Newsgroup bereitstellte, schaltete im Mai 2010 ihren Server ab[25] und das PC-Mag[44] schrieb 2008 das Usenet als "gestorben" ab. Die Diskussion über die Vitalität des Usenet hält an, das Usenet selbst erfreut sich aber in seiner ursprünglichen Form nur noch geringer Popularität. Die *binarys* Gruppen, die massiv durch Zugangsprovider[45] beworben werden, sind heute der größte Reiz für neue Teilnehmer.

6. ZUSAMMENFASSUNG

Die meisten der vorgestellten Netze und Technologien sind heute nur noch schwer erreich- bzw. nutzbar. Die einzige Ausnahme bildet das Usenet. Allerdings ist auch dies den jüngeren Netzteilnehmern kein Begriff mehr und gilt als veraltete Technologie. Alle Protokolle und Netze haben gemein, dass sie unter anderen Anforderungen entstanden sind, als sie heute durch das weltweite Netz vorgegeben werden. Da sie meist auf jenen Anforderungen basierten und nur durch sie legitimiert waren, haben nur wenige den Sprung in das digitale Zeitalter geschafft. Fehlende Standardisierungsverfahren und rasant voranschreitende Entwicklungen in der Protokollentwicklung und der Informatik machen sie obsolet. Nichtsdestoweniger sind diese Technologien, wenn sich die Anforderungen ändern, wieder nutzbar. So interessant und ungewöhnlich die vorgestellten Protokolle und Netze auch sein mögen, eine relevant große Teilnehmerzahl werden sie höchstwahrscheinlich nie wieder erreichen.

[43]Menge der transportierten Nachrichten
[44]http://www.pcmag.com/
[45]http://www.usenext.de/

doi: 10.2313/NET-2011-07-2_17

Literatur

[1] Delay-tolerant networking. URL http://en.wikipedia.org/w/index.php?title=Delay-tolerant_networking\&oldid=426030867. Wikipedia, Abgerufen am: 15.05.2011.

[2] Internet. URL http://de.wikipedia.org/w/index.php?title=Internet\&oldid=88785480. Wikipedia, Abgerufen am: 15.05.2011.

[3] UUCP Mapping, . URL http://meetings.ripe.net/ripe-50/presentations/ripe50-plenary-tue-uucp-mapping.pdf. Jaap Akkerhuis, Abgerufen am: 15.05.2011.

[4] Introduction to Taylor UUCP, . URL http://www.airs.com/ian/uucp-doc/uucp_2.html\#SEC2. Ian Lance Taylor, Abgerufen am: 15.05.2011.

[5] Ian Lance Taylor Homepage, . URL http://www.airs.com/ian/. Ian Lance Taylor, Abgerufen am: 15.05.2011.

[6] Version 7 Unix manual: UUCP Implementation Description, . URL http://meetings.ripe.net/ripe-50/presentations/ripe50-plenary-tue-uucp-mapping.pdf. D. A. Nowitz and M. E. Lesk, Abgerufen am: 15.05.2011.

[7] UUCP, . URL http://en.wikipedia.org/w/index.php?title=UUCP\&oldid=422315656. Wikipedia, Abgerufen am: 15.05.2011.

[8] "Befreite Zone"Thule-Netz?, . URL http://www.doew.at/publikationen/rechts/netz/thule.html. Martin Dietzsch, Anton Maegerle, Abgerufen am: 20.05.2011.

[9] inoffizielle Z-Netz Homepage, . URL http://www.z-netz.de/. Dirk Meyer, Abgerufen am: 20.05.2011.

[10] Flowing From Site to Site, 1995. URL http://mappa.mundi.net/maps/maps_021/. Brian Reid, Abgerufen am: 16.05.2011.

[11] UUCP Protocol, 1995. URL http://www.faqs.org/faqs/uucp-internals/section-6.html. Ian Lance Taylor, Abgerufen am: 15.05.2011.

[12] Fidonet: Dokumente und andere Informationen, 1998. URL http://home.nrh.de/fido/docs/index.shtml.de.

[13] Die komplette Dokumentation zu ZConnect 3.1 dem offenen Datenformat fuer Mailboxnetze, 2000. URL http://www.elektron-bbs.de/zconnect/index.htm\#_3.3.1.1.Headerinformationen_. Udo Berthold, Abgerufen am: 20.05.2011.

[14] The FidoNet Showcase Project, 2001. URL http://winramturbo.com/fnsp/nl/nl-history.htm. The FidoNet Showcase Project, Abgerufen am: 15.05.2011.

[15] Fido over IP, 2005.2011. URL http://www.was-ist-fido.de/pages/foiindex.htm. Wikipedia, Abgerufen am: 15.05.2011.

[16] Was ist Fido, 2005.2011. URL http://www.was-ist-fido.de/. Jens Hassler, Christoph Ripp, Michael Kleerbaum, Abgerufen am: 15.05.2011.

[17] WinPoint 95, 2005.2011. URL http://www.was-ist-fido.de/pages/wp_shots.htm. Jens Hassler, Christoph Ripp, Michael Kleerbaum, Abgerufen am: 15.05.2011.

[18] Zone Coordinator, 2006. URL http://fidopedia.fido.de/fido.de/index.php/Zone_Coordinator. Fidopedia, Abgerufen am: 15.05.2011.

[19] FTSC, 2006. URL http://fidopedia.fido.de/fido.de/index.php/FTSC. Fidopedia, Abgerufen am:15.05.2011.

[20] Node, 2006. URL http://fidopedia.fido.de/fido.de/index.php/Node. Fidopedia, Abgerufen am: 15.05.2011.

[21] FidoNet Struktur, 2006. URL http://fidopedia.fido.de/fido.de/index.php/Kategorie:Struktur. Fidopedia, Abgerufen am: 15.05.2011.

[22] Zone, 2006. URL http://fidopedia.fido.de/fido.de/index.php/Zone. Fidopedia, Abgerufen am: 15.05.2011.

[23] Zonegate, 2006. URL http://fidopedia.fido.de/fido.de/index.php/Zonegate. Fidopedia, Abgerufen am: 15.05.2011.

[24] ZNetz, 2009. URL http://de.wikipedia.org/w/index.php?title=Z-Netz\&oldid=62871735. Wikipedia, Abgerufen am: 20.05.2011.

[25] A Piece of Internet History, 2010. URL http://today.duke.edu/2010/05/usenet.html. Duke University, Abgerufen am: 16.05.2011.

[26] ZConnect, 2010. URL http://de.wikipedia.org/w/index.php?title=ZConnect\&oldid=80792965. Wikipedia, Abgerufen am: 20.05.2011.

[27] Fidonet and BBSes back in business for Egypt, 2011. URL http://emuconsoleexploitnews.blogspot.com/2011/01/fidonet-and-bbses-back-in-business-in.html.

[28] Tom Jennings, 2011. URL http://en.wikipedia.org/wiki/Tom_Jennings. Wikipedia, Abgerufen am: 15.05.2011.

[29] FidoNet, 2011. URL http://de.wikipedia.org/w/index.php?title=FidoNet\&oldid=88752832. Wikipedia, Abgerufen am: 15.05.2011.

[30] FidoNet, 2011. URL http://en.wikipedia.org/w/index.php?title=FidoNet\&oldid=438828007. Wikipedia, Abgerufen am: 15.05.2011.

[31] FidoNet: Routing of FidoNet mail, 2011. URL http://en.wikipedia.org/w/index.php?title=FidoNet\&oldid=438828007\#Routing_of_FidoNet_mail. Wikipedia, Abgerufen am: 15.05.2011.

[32] FidoNet: Technical specifications, 2011. URL http://en.wikipedia.org/w/index.php?title=FidoNet\&oldid=438828007\#Technical_specifications. Wikipedia, Abgerufen am: 15.05.2011.

doi: 10.2313/NET-2011-07-2_17

[33] FidoNet: Geographic structure, 2011. URL http://en.wikipedia.org/w/index.php?title=FidoNet\&oldid=438828007\#Geographic_structure. Wikipedia, Abgerufen am: 15.05.2011.

[34] Major Seven/Big Eight, 2011. URL http://www.open-news-network.org/index.php/Usenet. OpenNews, Abgerufen am: 16.05.2011.

[35] Google Groups, 2011. URL https://groups.google.com/?hl=de. Google, Abgerufen am: 16.05.2011.

[36] Usenet-Aus bei der Deutschen Telekom, 2011. URL http://www.heise.de/newsticker/meldung/Usenet-Aus-bei-der-Deutschen-Telekom-1220735.html. Heise, Abgerufen am: 16.05.2011.

[37] Usenet, 2011. URL http://de.wikipedia.org/w/index.php?title=Usenet\&oldid=88343099. Wikipedia, Abgerufen am: 16.05.2011.

[38] Usenet: Geschichte, 2011. URL http://de.wikipedia.org/w/index.php?title=Usenet\&oldid=88343099\#Geschichte. Wikipedia, Abgerufen am: 16.05.2011.

[39] Big 8 (Usenet), 2011. URL http://en.wikipedia.org/w/index.php?title=Big_8_(Usenet)\&oldid=406695514. Wikipedia, Abgerufen am: 16.05.2011.

[40] Usenet, 2011. URL http://en.wikipedia.org/w/index.php?title=Usenet\&oldid=429265996. Wikipedia, Abgerufen am: 16.05.2011.

[41] Usenet: History, 2011. URL http://en.wikipedia.org/w/index.php?title=Usenet\&oldid=429265996\#History. Wikipedia, Abgerufen am: 16.05.2011.

[42] Usenet: Moderated and unmoderated newsgroups, 2011. URL http://en.wikipedia.org/w/index.php?title=Usenet\&oldid=429265996\#Moderated_and_unmoderated_newsgroups. Wikipedia, Abgerufen am: 16.05.2011.

[43] Usenet: Technical Details, 2011. URL http://en.wikipedia.org/w/index.php?title=Usenet\&oldid=429265996\#Technical_details. Wikipedia, Abgerufen am: 16.05.2011.

[44] Usenet: Traffic, 2011. URL http://en.wikipedia.org/w/index.php?title=Usenet\&oldid=429265996\#Usenet_traffic_today. Wikipedia, Abgerufen am: 16.05.2011.

[45] Flooding-Algorithmus, 2011. URL http://de.wikipedia.org/w/index.php?title=Flooding-Algorithmus\&oldid=83691881. Wikipedia, Abgerufen am: 16.05.2011.

[46] Usenet: ISPs, news servers, and newsfeeds, 2011. URL http://en.wikipedia.org/w/index.php?title=Usenet\&oldid=429265996\#ISPs.2C_news_servers.2C_and_newsfeeds. Wikipedia, Abgerufen am: 16.05.2011.

[47] Network News Transfer Protocol, 2011. URL http://de.wikipedia.org/w/index.php?title=Network_News_Transfer_Protocol\&oldid=88452427. Wikipedia, Abgerufen am: 16.05.2011.

[48] Thread, 2011. URL http://de.wikipedia.org/w/index.php?title=Thread\&oldid=83651375. Wikipedia, Abgerufen am: 16.05.2011.

[49] Amnesty International: Urgent Actions, 2011. URL http://www.amnesty.de/urgent-actions-0. Amnesty International, Abgerufen am: 20.05.2011.

[50] CLNetz, 2011. URL http://de.wikipedia.org/w/index.php?title=CL-Netz\&oldid=83328251. Wikipedia, Abgerufen am: 20.05.2011.

[51] K. Fall. A Delay-Tolerant Network Architecture for Challenged Internets. 2003.

doi: 10.2313/NET-2011-07-2_17

Transmission Protocols for Delay-Tolerant Networks

Adrian Rumpold
Betreuer: Dr. Nils Kammenhuber
Seminar Innovative Internettechnologien und Mobilkommunikation SS2011
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: rumpold@in.tum.de

ABSTRACT

In this paper, we provide an overview of important transmission protocols for a certain class of challenged heterogeneous networks commonly termed *delay-* or *disruption-tolerant networks* (DTN). We outline basic requirements and limitations for these protocols, including the Bundle Protocol and the LTP and Saratoga convergence layer protocols, sketch their respective solution approaches and provide and overall comparison. Finally, we discuss some inherent shortcomings and operational challenges of the Bundle Protocol specification regarding areas of reliability, routing and time synchronization as well as schematic examples for future improvements.

Keywords

DTN, delay-tolerant networks, disruption-tolerant networks, network protocols, Bundle Protocol, convergence layer protocols, LTP, LTP-T, Saratoga

1. INTRODUCTION

Wide-area communication today is far from being limited to the Internet only, but rather includes challenging environments such as near- and deep-space satellite links, underwater equipment and various forms of wireless sensor networks. These usage scenarios differ significantly in their characteristics from the well-known Internet architecture in terms of link availability, signal quality and communication channel bandwidth. As network connectivity might only be available sporadically, the foremost goal is maximal utilization of transmission opportunities, even if this might imply decreased reliability. A framework for such scenarios is given by delay- or disruption-tolerant networks (DTN), omitting a traditional end-to-end conversation paradigm in favor of a store-and-forward architecture.

Work on DTN technologies commenced in the late 1990s following the vision of an *Interplanetary Internet* (IPN), where communication delays of multiple hours and frequent link outages had to be considered and expected [4, p. 3]. Given their aptitude for highly dynamic and resilient communication architectures with ad-hoc connectivity, disruption-tolerant network protocols also elicited interest in military circles as an enabler for wireless integrated battlefield networks [12, p. 2].

In their reference specification, Cerf et al. [4] (first drafted in 2003) propose an end-to-end message-oriented overlay protocol, the *Bundle Protocol*; this architecture was subsequently further refined by Scott and Burleigh [8]. We briefly describe the Bundle layer protocol's structure and important aspects in section 2. This protocol can either be used directly on top of a regular TCP/IP network connection or use specialized *convergence layer protocols*, bridging the gap between the abstract bundle overlay structure and the underlying network connection.

In section 3 we introduce two important convergence layer protocols, the *Licklider Transport Protocol* (LTP) and the *Saratoga* protocol. Section 4 provides a discussion of some major challenges and obstacles frequently encountered in DTN applications. In section 5 we present an outlook onto possible future developments in DTN research as well as a technology for delay-tolerant communication without the Bundle Protocol.

Figure 1 demonstrates how the protocols discussed can be integrated into the stack of preexistent Internet protocols for use in DTN applications. The Bundle Protocol exposes the abstracted interface to the application layer, the Bundle layer in turn accesses underlying convergence layer protocols. Besides the specialized convergence layer protocols presented in this paper, the TCP/IP protocol can also be used for reduced configuration complexity in testing environments [4, p. 29].

An in-depth discussion of standard protocols like *TCP*, *UDP* and the Internet Protocol *IP* as well as various data link layer protocols is beyond the scope of this work; interested readers can find further reading regarding their properties for example in Tanenbaum [11].

2. BUNDLE PROTOCOL

In the following subsections, we describe the basic concepts and properties behind the Bundle Protocol first proposed by Internet pioneer Vint Cerf in 2003 as a communication protocol for the envisioned Interplanetary Internet. Shortly after the initial drafts, the IRTF Delay-Tolerant Networking Working Group published two RFCs 4838 and 5050 [4, 8], defining the general architecture for DTN environments as well as the Bundle Protocol itself.

2.1 Protocol overview

The Bundle Protocol constitutes a message-oriented overlay atop various transport protocols. It may be used over TCP/IP connections as well as convergence layer protocols, such as the Licklider Transmission Protocol (LTP) and the

doi: 10.2313/NET-2011-07-2_18

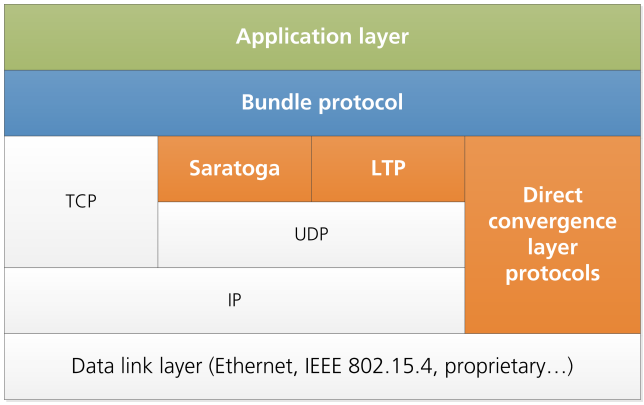


Figure 1: Classification of DTN protocols in the Internet protocol hierarchy

Saratoga protocol discussed later in section 3. The following brief description of the protocol is based on the DTN architecture specification [4] and the Bundle Protocol specification [8] where not stated otherwise.

Applications using the Bundle Protocol may send messages of arbitrary length. These application data units (ADU) are encapsulated into protocol data units (PDU) when passed to the bundle layer; a single ADU is usually transmitted completely by a PDU, but may also be segmented by the bundle layer. PDUs in the Bundle Protocol are referred to as *bundles* and are transmitted between nodes in a store-and-forward fashion. This communication paradigm distinguishes delay-tolerant networks from traditional IP-based local- and wide-area networks, where packets are usually stored in transmission buffers only for short periods of time during inter-node routing. Rather, en-route bundles may be stored for indefinite amounts of time by their current hop until a suitable connection for forwarding towards its final destination is available. Such connections may present themselves for example in the form of a scheduled communication contact with a space vessel or opportunistic contacts in wireless sensor networks.

Bundle sources and destinations are identified by means of *Endpoint identifiers* (EID). Multiple naming schemes for EIDs are proposed by the Bundle Protocol specification, each conforming to a common Uniform Resource Identifier (URI) format and consist of a scheme name[1] and a scheme-specific part (SSP). Therefore, the URI `ipn:rover.mars` is one of the numerous possible examples of such an endpoint identifier with `ipn` as the scheme name and `rover.mars` as the SSP.

Associations between endpoint identifiers and node addresses are not established at creation time of a bundle. Instead rather a late binding occurs, so a specific EID might be reinterpreted several times during bundle delivery. This late binding facilitates bundle delivery in cases of changes in the network topology of which the originating node is not yet aware or if the transit duration of a message exceed validity times of EID registration bindings [4, p. 9].

A simplistic quality-of-service approach is included in the Bundle Protocol by class of service specifiers in a bundle's header information. A message may take a relative priority indicator of *bulk*, *normal* or *expedited*, however the specification does not prescribe any detailed handling policy for forwarding nodes [8, pp. 13 f.].

To increase transmission efficiency during phases of intermittent connectivity, the DTN architecture includes considerations for proactive as well as reactive fragmentation. Proactive fragmentation precludes transmission of messages larger than a scheduled contact between two nodes by breaking up larger bundles into smaller fragments suitable for the scheduled connection and its total data volume. Reactive fragmentation on the other hand is employed as a reaction to interrupted connections, where only partial content has been transmitted successfully. The forwarding node is permitted to break the incomplete message into two fragments, so the content already received correctly may instantaneously be transmitted further without the need for retransmitting the complete bundle [3, p. 18].

Figure 2 illustrates how the Bundle Protocol can be integrated with heterogeneous network architectures comprising different technology stacks. Heterogeneity with respect to communication protocols can occur on any of the protocol layers underneath the Bundle Protocol. Such configurations may be found in operations where DTN traffic is subsequently forwarded across Internet TCP/IP connections to its final destination. Bundle protocol routers along the communication path are capable of bridging between different network layer and convergence layer protocols (see section 3).

2.2 Reliable transmission support in the Bundle Protocol

TCP provides end-to-end conversational reliability by means of retransmission of segments not acknowledged by the destination host [11, pp. 532 ff.]. This technique cannot be directly applied to delay-tolerant network architectures, however, where a continuous end-to-end connectivity is oftentimes not available. Therefore, the Bundle Protocol supports node-to-node retransmission of incorrectly transferred data. As a single DTN may incorporate a number of incompatible transport layer protocols, end-to-end reliability in such inhomogeneous environments can only be achieved at the bundle layer [12, p. 17].

Node-to-node reliability in the bundle layer is provided by *custody transfers* between two neighboring nodes. Intending such a hand-off, a bundle's current custodian transmits the bundle to the next node and starts a retransmission timer. If the receiving peer does not complete the custody transfer by acknowledging correct reception, the transmission is repeated until successful acknowledgment by the designated custodian. After completing a custody transfer, the previous custodian may safely delete the bundle from its long-term storage, as the current custodian is now responsible for reliable forwarding of the bundle to its destination or subsequent custodians.

[1] IANA assigned URI schemes are published at `http://www.iana.org/assignments/uri-schemes.html`

doi: 10.2313/NET-2011-07-2_18

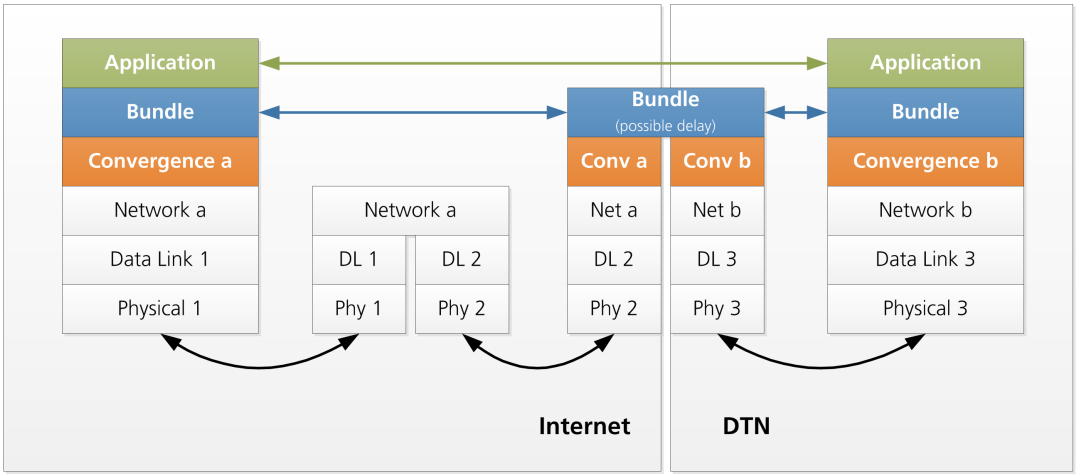


Figure 2: End-to-end bundle routing across heterogeneous protocol stacks and network architectures (based on [3])

To achieve end-to-end reliability, transmission of *return receipts* is required besides enforcement of node-to-node custody transfers. This additional confirmation is required, since a bundle may have been discarded by an en-route custodian after expiry of its time-to-live timestamp before arriving at its designated destination node.

3. CONVERGENCE LAYER PROTOCOLS

While the Bundle Protocol in theory can be operated over arbitrary transport protocols, oftentimes the need for specialized protocols arises, which address the various dissimilarities in heterogeneous network environments found in DTN setups. These class of protocols is subsumed under the term *convergence layer protocols*. Their main task is to provide an abstraction over underlying network protocol layers and permit best possible link utilization. Convergence layer protocols may themselves either operated on top of transmission protocols such as UDP or directly access the data link layer if desired [15, p. 4].

3.1 Licklider Transmission Protocol (LTP) & LTP-T

The Licklider Transmission Protocol (LTP), named after Internet pioneer J.C.R. Licklider, provides selective-reliability communication over high-latency links. It is purposed as a block-oriented convergence-layer protocol for use in interplanetary communication segments in delay-tolerant multihop networks [6, pp. 1 f.].

LTP operations between two communication nodes consist of two distinct parts: a reliably transmitted red part and following green part segments, for which no reliability is assured by the protocol. On start of transmission a red part segment and one or more checkpoints (including a special red part segment – end-of-red-part [`EORP`]) are transferred to the receiver, which in turn sends out report segments containing information about successfully received segments. Reception of these reports is subsequently acknowledged by the original sender. If a timeout occurs while waiting for an acknowledgment, the respective segment is retransmitted until its reception has been successfully confirmed [7, section 6].

Following the `EORP` message one or more green segments are transmitted without acknowledgment of successful reception to maximize communications throughput during limited phases of episodic connectivity. After conclusion of a conversation by means of a end-of-block (`EOB`) message, all transmitted data is passed to the application layer. [6, p. 1].

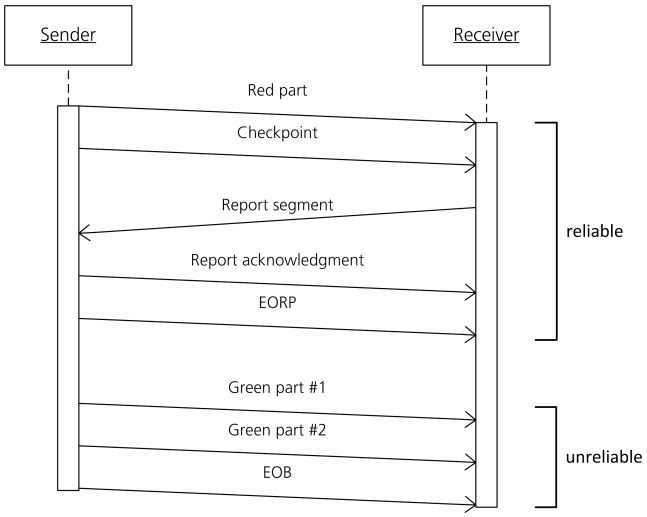


Figure 3: LTP transmission sequence

Figure 3 shows a complete LTP communication session between two node consisting of one red part and two green part segments without any transmission errors. Only the red part segment is transmitted in a reliable fashion, whereas reception of the green part segments is not acknowledged by the remote peer and the communication is terminated by the sender after the `EOB` segment. The depicted communication session can be envisioned during transmission of satellite imaging data: Here, meta-information about transmitted records have to be transmitted reliably in order to successfully process the following image data. Such metadata is therefore a candidate for inclusion into the red part segment at the beginning of the conversation. Errors with regard

doi: 10.2313/NET-2011-07-2_18

to the image data itself, however, can be tolerated. Thus, such information is suitable for bulk transmission within the subsequent green part segments.

As the LTP protocol was primarily developed for single-hop connections only, it was subsequently extended under the name of LTP-T to form a transport protocol and accommodate multi-hop architectures. During normal operation, LTP-T generally performs as if a single LTP connection was used between every two nodes. Major differences when compared to the LTP protocol can be found in case of transmission errors: Correctly received segments are forwarded to the next hop, while only corrupted or lost segments are requested to be retransmitted from the original sender. Because of this mechanism, the ordering of transmitted segments is possibly changed, so re-ordering of the segment sequence and checkpoint scheduling become important issues and are subjects of ongoing research work [6].

3.2 Saratoga Protocol

The Saratoga protocol, named after United States World War II aircraft carrier USS Saratoga, was originally designed as a IP-based store-and-forward file transmission protocol for small satellites in a near-Earth low orbit [9, p. 4]. As opposed to regular Internet communication, connectivity in such scenarios is only intermittent in nature and highly asymmetrical in terms of up- and downstream bandwidth, a configuration commonly found in delay-tolerant networks. The UK-DMC imaging satellite, for example, features a downstream bandwidth of 8.1 Mbps opposed to an upstream of only 9.6 kbps [ibid.] resulting in a bandwidth asymmetry of around 844 : 1 – compared to commercial ADSL2 lines featuring a factor of merely 8 : 1. The TCP protocol performs increasingly worse for links exhibiting asymmetries greater than 50 : 1, as the return path to the sender is congested by acknowledgment segments [1].

If the TCP protocol were to be used for communication, every segment sent over the network link would have to be acknowledged by the receiver, leading to reduced bandwidth utilization and impact on overall transfer performance. Moreover, the TCP slow start mechanism further hinders effective link utilization [13, pp. 3 f.]. Additional challenges are constituted by high round-trip-times (RTT), bit error rates (BER) and frame loss rates (FLR) on interplanetary communication links.

Therefore, the lightweight Saratoga protocol does not rely on TCP as a transport protocol, but instead uses the connectionless UDP and UDP Lite protocols, which do not require acknowledgment of transmitted datagrams and therefore do not provide a reliable service [11, pp. 525 f.]. By omitting the premise of fair line contention and focusing on communication scenarios with only two participants, Saratoga strives to achieve complete utilization of the communications link and maximization of data throughput [13, p. 1].

As a file transmission protocol, Saratoga provides support for transactions operating on files and directories as their underlying basic entities. Accordingly, the protocol implements operations similar in nature to the well-known FTP protocol, including instructions for fetching or deleting files (`_get_`, `_delete_`), transferring files to a remote peer (`_put_`)

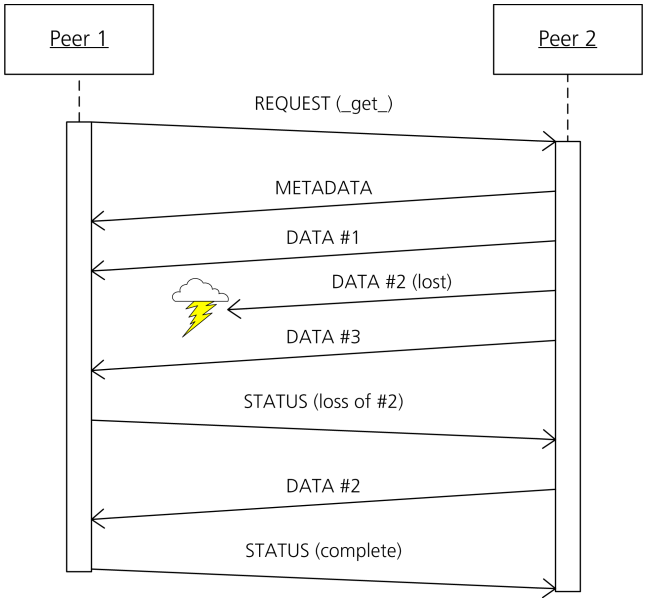


Figure 4: Retransmission during _get_ request

and querying remote directory listings (`_getdir_`) (nomenclature as described in [13, pp. 6 f.]).

Given that the underlying UDP protocol does not provide an indication of correctly transmitted datagrams, the Saratoga specification introduces a selective negative-acknowledgment (SNACK) status message. Communicating peers may exchange `STATUS` packages indicating ranges of successful and failed `DATA` packages during the active conversation, permitting for a selective retransmission of lost segments to be initiated. Figure 4 illustrates this technique with a exemplary `_get_` request consisting of three distinct `DATA` packages, one of which is lost during transmission. This condition is indicated in the client's `STATUS` packet, resulting in the subsequent repetition of `DATA` package #2.

To increase data throughput in deployments with high round-trip latencies, speculative `_get_` requests with an empty file path are permitted. As an answer to such a request the remote Saratoga peer may send any file it deems relevant for the client and immediately commence its transmission. Analogous procedures are also specified for optimistic `_put_` operations, where the sending peer will begin its data transfer without waiting for a corresponding `STATUS` response by the receiving peer [13, p. 9].

In addition to being used in standalone applications, Wood et al. [15] demonstrate how the Saratoga protocol can be used as a convergence layer with the Bundle Protocol. The bundle agent can cooperate with the Saratoga peer by using a shared directory, wherein the DTN bundle agent stores completed bundles as files. Those bundle files can subsequently be requested via the `_get_` transaction or pushed to another Saratoga peer using the `_put_` operation.

4. CHALLENGES AND OBSTACLES

As a fairly recent area of research, many issues in the field of delay-tolerant networking have yet to be solved. In the

doi: 10.2313/NET-2011-07-2_18

following section we identify and present three distinct challenges to the Bundle Protocol; in particular regarding insurance of bundle integrity, routing and time synchronization across intermittently connected networks. These issues and several others were discussed by Wood et al. [14].

4.1 Bundle integrity

Lacking support for checksums, the Bundle Protocol is unable to detect errors in transmitted application data or bundle header metadata. Custody transfers on the other hand can only provide protection against loss of complete bundles and facilitate fast retransmission in such cases. Although error detection and correction could be implemented at the application level, this technique still does not guard against corruption of header information which is not propagated up to the application. Furthermore such an application-provided integrity mechanism introduces a tighter coupling between sending and receiving applications and is therefore not a viable remedy. Resulting from these shortcomings, the Bundle Protocol in its basic form as specified in [8] does not sufficiently support reliable end-to-end transmissions with integrity guarantees.

Instead of introducing header checksums or similar integrity checking measures, Wood et al. [14] propose a different approach making use of the optional security extensions of the Bundle Protocol [10]. Usually the problem of efficient and secure key distribution arises when using either symmetrical or asymmetrical cryptographic systems. However, if only integrity of transport is to be assured, use of a common ciphersuite and a well-known key shared between all participating communication nodes is sufficient. This cryptographic system permits wrapping immutable header information as well as application data in order to defend against incidental errors introduced during transmission, reassembly of fragments or in-memory storage of bundles.

This approach may even be used in conjunction with end-to-end encryption to enhance performance by permitting intermediary routers to check for possible modification of the bundle's content, although they are unable to decrypt the encapsulated ADU. In contrast to a mere end-to-end encryption, corrupted bundles may be retransmitted faster, thus leading to increased overall network performance.

4.2 Name Resolution and Routing

The issue of routing in delay-tolerant networks is closely connected to the set of problems revolving around common naming schemes for endpoint identifiers in the Bundle Protocol. Since no name-resolution protocols such as the Domain Name System (DNS) have been defined for DTNs yet, resolving a bundle's destination EID and deriving routing information is inherently difficult. Late binding of EIDs onto network addresses further complicates routing in scenarios with multi-homed or mobile peers roaming between several subnetworks.

This problem could be tackled by providing static routing information to each participating node in the network, however this approach poses a stark contrast to the ad-hoc networking architecture found in DTN applications. Another possibility is the usage of source routing, possibly deriving routing information and forwarding rules from the EID itself by postulating a distinct hierarchy within the naming scheme.

Traditional Internet routing protocols, for example the Routing Information Protocol (RIP) and the Border Gateway Protocol (BGP), are not suitable for long-delay networks with intermittent connectivity, as they require excessive exchange of routing information metadata to accommodate for changing network topologies. Candidates for routing in DTN bundle architectures have yet to be fully specified and should be independent from underlying convergence layer protocols to facilitate integration and interconnection of various heterogeneous networks.

The use of replication-based routing protocols instead of forwarding strategies with a singular transmission path is a recent but promising area of development. These protocols enable a DTN router to propagate multiple instances of a single Bundle to its neighboring peers for further transmission. While being more resource-intensive, these approaches help to address and alleviate the problematic issues raised above. Examples for replication-based routing protocols for delay-tolerant networks include the simplistic epidemic routing and its more complex enhancement, the *PRoPHET* protocol (Probabilistic Routing Protocol using History of Encounters and Transitivity) [5].

4.3 Time synchronization

Another pressing issue in DTN architectures presents itself in the form of time synchronization. Timestamps are employed in several places in the Bundle Protocol, including the lifetime and creation header fields. The lifetime works analogously to the time-to-live (TTL) header field of the IP protocol and helps to prevent messages in the network from looping indefinitely in case of routing malfunctions. Moreover, this approach facilitates discarding of packets which carry data of limited usefulness after certain expiration times. Messages may be uniquely identified by their creation timestamp, which is used for example during fragment reassembly – its semantics are similar to the identification field of the IPv4 header.

For the aforementioned reasons a common notion of time as well as mechanisms for time synchronization are required across a delay-tolerant network using the Bundle Protocol overlay. Time synchronization in those scenarios cannot be achieved by the Bundle Protocol itself, as correct time information must be acquired first for production of valid bundles. Wood et al. [14] propose an additional simple time exchange protocol, where network nodes claim different confidence levels for themselves regarding internal clock accuracy. Peers with low confidence levels can subsequently improve their clock precision by acquiring current time from nodes with higher confidence levels.

In addition to operational difficulties, security considerations must also be taken into account when designing strategies and protocols for network time synchronization. Only authorized and authenticated nodes should be able to distribute time information to other clients in the network and adequate measures must be taken to assure their identity. Failure to comply with this requirement enables a malicious entity to isolate peers from the network using a denial-of-

doi: 10.2313/NET-2011-07-2_18

service attack, effectively preventing them from communicating with other Bundle Protocol hosts.

5. OUTLOOK AND CONCLUSION

As we discussed in section 4, the young family of protocols for delay-tolerant networks contains room for enhancements and ongoing research, especially considering security, communication integrity and routing issues. Most of these topics are still work in progress, therefore no final statement can be given regarding their future development. It seems plausible, however, that with continuously increasing application scenarios involving the need for delay-tolerant networking, the protocols involved will rapidly reach a more mature status by successive improvements.

DTN applications are not limited to the Bundle Protocol however: Wood et al. [14] propose an alternative approach using an extension of the HTTP protocol (*HTTP-DTN*) directly atop of a convergence layer protocol. Instead of passing Bundle PDUs, application data is encapsulated into HTTP requests, newly defined `Content-*` headers carry accompanying delivery metadata. `Content-MD5` headers are capable of providing end-to-end reliability by inclusion of a payload checksum.

HTTP clients unable to understand the additionally defined headers are required to disregard the respective request, so the proposed HTTP-DTN architecture should not interfere with ordinary Internet HTTP traffic. Albeit sharing some of the shortcomings of the Bundle Protocol, its integrated support for integrity checks as well as higher familiarity of developers with HTTP implementations might make the HTTP-DTN protocol attractive for certain application cases.

References

[1] H. Balakrishnan, V. N. Padmanabhan, and R. H. Katz. The effects of asymmetry on TCP performance. *Mobile Networks and Applications*, 4:219–241, 1999. ISSN 1383-469X. URL `http://dx.doi.org/10.1023/A:1019155000496`.

[2] S. Burleigh, M. Ramadas, and S. Farrell. RFC 5325, Licklider Transmission Protocol Motivation. IRTF Delay-Tolerant Networking Research Group, September 2008. URL `http://tools.ietf.org/pdf/rfc5325.pdf`.

[3] V. Cerf. InterPlaNetary Internet – presentation at DARPA Proposers' Day, 21 January 2004.

[4] V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, and R. Durst. RFC 4838, Delay-Tolerant Networking Architecture. IRTF Delay-Tolerant Networking Research Group, April 2007. URL `http://tools.ietf.org/pdf/rfc4838.pdf`.

[5] A. Lindgren, A. Doria, E. Davies, and S. Grasic. Probabilistic Routing Protocol for Intermittently Connected Networks. IRTF Delay-Tolerant Networking Research Group, 2011. URL `http://tools.ietf.org/pdf/draft-irtf-dtnrg-prophet-09.pdf`.

[6] F. S. Muhammad, L. Franck, and S. Farrell. Transmission protocols for challenging networks: LTP and LTP-T, Sept. 2007. URL `http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4409406`.

[7] M. Ramadas, S. Burleigh, and S. Farrell. RFC 5326, Licklider Transmission Protocol Specification. IRTF Delay-Tolerant Networking Research Group, September 2008. URL `http://tools.ietf.org/pdf/rfc5326.pdf`.

[8] K. Scott and S. Burleigh. RFC 5050, Bundle Protocol Specifications. IRTF Delay-Tolerant Networking Research Group, November 2007. URL `http://tools.ietf.org/pdf/rfc5050.pdf`.

[9] C. Smith, C. Jackson, W. Eddy, L. Wood, and W. Ivancic. Saratoga: A Scalable File Transfer Protocol. Transport Area Working Group, 2010. URL `http://tools.ietf.org/html/draft-wood-tsvwg-saratoga-08`.

[10] S. Symington, S. Farrell, H. Weiss, and P. Lovell. RFC 6257, Bundle Security Protocol Specification. IRTF Delay-Tolerant Networking Research Group, May 2011. URL `http://tools.ietf.org/pdf/rfc6257.pdf`.

[11] A. S. Tanenbaum. *Computer Networks*. Prentice Hall PTR, 4th edition, 2003. ISBN 9780130661029.

[12] F. Warthman. Delay-tolerant networks (DTNs): A tutorial, 2003. URL `http://www.dtnrg.org/docs/tutorials/warthman-1.1.pdf`.

[13] L. Wood, W. M. Eddy, W. Ivancic, J. McKim, and C. Jackson. Saratoga: a Delay-Tolerant Networking convergence layer with efficient link utilization. In *2007 International Workshop on Satellite and Space Communications*, pages 168–172. IEEE, Sept. 2007. ISBN 978-1-4244-0938-9. doi: 10.1109/IWSSC.2007.4409410. URL `http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4409410`.

[14] L. Wood, W. Eddy, and P. Holliday. A bundle of problems. *IEEE Aerospace conference*, pages 1–17, 2009. doi: 10.1109/AERO.2009.4839384. URL `http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4839384`.

[15] L. Wood, J. McKim, W. M. Eddy, and W. Ivancic. Using Saratoga with a bundle agent as a convergence layer for delay-tolerant networking. IRTF Delay-Tolerant Networking Research Group, May 2011.

Side-Channel Leaks in Web-Applications

Clara Lange
Betreuer: Ralph Holz
Hauptseminar Innovative Internettechnologien und Mobilkommunikation SS2011
Lehrstuhl Netzarchitekturen und Netzdienste, Lehrstuhl Betriebssysteme und Systemarchitektur
Fakultät für Informatik, Technische Universität München
Email: langecl@in.tum.de

KURZFASSUNG

Mit der Entwicklung des World Wide Web von den Anfängen bis zum Web 2.0 stehen dem Benutzer immer mehr interaktive Dienste und Anwendungen im Internet zur Verfügung. Es können Sicherheitsprobleme entstehen, wie zum Beispiel Seitenkanalangriffe gegen Web-Anwendungen, die in dieser Arbeit behandelt werden. Eine Web-Anwendung ist aufgeteilt in eine Browser-Komponente, die die Schnittstelle für den Client bzw. den Endnutzer zur Nutzung der Anwendung darstellt, und in eine Server-Komponente. Diese Aufteilung hat zur Folge, dass ein Anteil der internen Informationen während der Kommunikation beider Komponenten im Netzwerk sichtbar wird. Daraus können Sicherheitslücken resultieren. Schwerpunktmäßig wird in dieser Arbeit das aktuelle Problem der Seitenkanalangriffe (*side-channel attacks*) gegen Web-Anwendungen behandelt, wobei der Angreifer trotz Verschlüsselung die Möglichkeit hat, Seitenkanal-Information zu belauschen, um personenbezogene Daten ausspähen zu können. Zusätzlich werden technische Herausforderungen, die sich während der Suche nach Lösungsansätzen ergeben, und Lösungsvorschläge, um die Gefahr zu beseitigen, in dieser Arbeit diskutiert. Abschließend wird der Blick auf zukünftige Entwicklungen gerichtet.

Schlüsselworte

Seitenkanalangriffe, *side-channel attacks*, Web 2.0, Web-Anwendungen, Benutzereingabe, Sicherheitslücken, Regelwerk

1. EINLEITUNG

Das World Wide Web unterlag einer drastischen Entwicklung bis hin zum Web 2.0 [6]. Früher existierten Webseiten nur als Plattformen für Informationen, das heißt es waren statische Seiten, die der Benutzer lediglich zur Informationsbeschaffung nutzte. Neben Performanzsteigerung und Reduktion der Kosten gelten Webseiten in der heutigen Zeit als Plattformen zum Mitmachen und als Plattformen, die Software-Anwendungen über das Internet bereitstellen. Immer mehr Daten, Dienste und Anwendungen werden im World Wide Web bereitgestellt. Im Web 2.0 steht der Benutzer im Fokus, es wird Wert auf Benutzerfreundlichkeit und Interaktivität gelegt. Dem Benutzer wird es ermöglicht, mehr mit dem Internet zu agieren und interaktiv an zum Beispiel der Gestaltung mitzuwirken. Daneben wird auch die Kommunikation zwischen Nutzern erleichtert, zum Beispiel durch soziale Netzwerke und Online-Communities. Durch die wachsenden Kommunikationsmöglichkeiten hat der Benutzer den Vorteil, dass Daten leichter zu jeder Zeit und an jedem Ort verfügbar sind - Webseiten spielen vor allem für den Informationsaustausch eine große Rolle.

Zusätzlich können Desktop-Anwendungen in absehbarer Zeit durch Web-Anwendungen ersetzt werden. Seit Web 2.0 wird die Funktionalität von Desktop-Anwendungen in das Internet transferiert, wobei der Browser die Schnittstelle zwischen Benutzer und Anwendung darstellt. Man spricht auch von *Software-as-a-Service* [1]. Dabei sollte Schutz vor Nutzerdaten im Vordergrund stehen, die Sicherheit für personenbezogene Daten muss gewährleistet sein.

Seitenkanalangriffe gegenüber Web-Anwendungen gewinnen immer mehr an Bedeutung. Da Web-Anwendungen unterteilt in eine Browser- und eine Server-Einheit sind, ist Kommunikation zwischen diesen beiden Einheiten notwendig. Der Seitenkanal ist hierbei der Kommunikationsweg. Trotz dass die Kommunikation zwischen Browser und Server verschlüsselt ist, kann der Angreifer Attribute dieser verschlüsselten Datenübertragung ausspähen, sog. Seitenkanal-Informationen, und dadurch Rückschlüsse auf die Eingabe des Benutzers ziehen.

Heutzutage existieren neben Seitenkanalangriffen weitere Angriffe wie zum Beispiel Phishing, Sniffen und Spoofen. Phishing-Angriffe erfolgen, indem der Angreifer eine vertraute Webseite nachbildet, um den Benutzer zu verleiten, seine persönlichen Authentifikationsdaten einzugeben. Sniffen meint das Belauschen des Netzwerkverkehrs und Spoofen das Vortäuschen einer falschen Identität während eine Kommunikation - sprich Identitätsdiebstahl [10].

Insbesondere bei extrem sicherheitsbedürftigen Web-Anwendungen werden Lösungen zum Schließen von Sicherheitslücken benötigt. Zum einem müssen Sicherheitslücken identifiziert werden; zum anderem sind Regelwerke zur Schadensbegrenzung erforderlich. Hierbei ist anwendungsspezifisches Wissen von großem Nutzen.

Überblick - Aufbau der Arbeit. In dem folgenden Abschnitt 2 werden Grundlagen zu den Themen Seitenkanalangriffe, Wandlung von Desktop- zu Web-Anwendungen und spezifische Eigenschaften von Web-Anwendungen erklärt. Abschnitt 3 zeigt explizite, aktuelle Beispiele von Seitenkanalangriffe gegen Web-Anwendungen. Die darauffolgenden Abschnitte 4 und 5 behandeln technische Herausforderungen, Lösungsansätze beziehungsweise Verteidigungsmechanismen. Abschnitt 6 enthält eine kurzes Fazit.

doi: 10.2313/NET-2011-07-2_19

2. GRUNDLAGEN

2.1 Seitenkanalangriffe

Ein Angriff kann definiert werden als ein nicht-autorisierter Zugriff auf ein schützenswertes Objekt [10].

Allgemein bezeichnen Seitenkanalangriffe Attacken, die Schwachstellen in der Implementierung bzw. im Sourcecode ausnutzen und nicht Attacken, die einen kryptographischen Algorithmus selbst angreifen [3]. Seitenkanalangriffe treten nicht nur gegen Web-Anwendungen auf.

2.1.1 Angriffsmethoden

Grundsätzlich stellen Seitenkanäle den Transportweg für die Kommunikation dar. Das Hauptproblem bei Seitenkanalangriffen ist, dass Seitenkanal-Informationen ausgenutzt werden, um auf die Inhalte rückschließen zu können. Solche Seitenkanal-Informationen können Attribute einer verschlüsselten Kommunikation, wie zum Beispiel Paketgröße oder Dauer des Paketes, sein. Meist sind es physikalische Eigenschaften, die vom Angreifer beobachtet werden.

Grundsätzlich können Seitenkanäle mit zwei verschiedenen Methoden angegriffen werden [3]:

- *Data Leakage* (auch Seitenkanalanalyse genannt): Der Angreifer belauscht passiv einen Seitenkanal, um an personenbezogene Daten zu kommen.
- *Fault Injection*: Der Angreifer manipuliert aktiv den Seitenkanal, indem er Fehler einfügt, die das Verhalten der Anwendung ändern.

2.1.2 Spezielle Seitenkanalangriffe

Spezielle, bekannte Seitenkanalangriffe sind zum Beispiel folgende [2]:

- *Timing Attack*: Angriff, bei dem der Angreifer die Zeiten beobachtet und analysiert, die gebraucht werden, um kryptographische Algorithmen auszuführen, da diese Algorithmen sehr rechenintensiv sind
- *Fault (Injection) Attack*: Angriff gegen kryptographische Hardwaregeräte (z. Bsp. Smartcards), indem der Angreifer beispielsweise fehlerhafte Eingabedaten sendet
- *Power Analysis Attack*: Angriff, bei dem der Stromverbrauch bei kryptographischen Elementen betrachtet wird
- *EM Attack*: Angriff, bei dem der Angreifer elektromagnetische Strahlung von elektronischen Geräten beobachtet
- *Acoustic Attack*: Angriff gegen einen Audio-Kanal

Auch eine Kombination mehrerer Angriffe ist möglich.

Gegenmaßnahmen können *randomization*, *blinding* und *masking* sein. Bei der Randomisierung werden die Daten, die durch Seitenkanäle durchsickern können, zufällig verteilt. *Blinding* dient dazu, dass die Eingabe eines Algorithmus in einige unvorhersehbare Zustände geändert wird. Unter Maskierung versteht man das Verdecken der Nachricht und des Schlüssels, indem man am Anfang der Berechnung sowohl die Nachricht als auch den Schlüssel mit einer zufälligen Maske umhüllt [4].

2.1.3 Seitenkanalangriffe aus der Vergangenheit

Bei dem in Referenz [8] beschriebenen Angriff handelt es sich um Seitenkanalangriffe, die im Zusammenhang mit SSH möglich sind. SSH steht für *Secure Shell* und ist ein Netzwerkprotokoll. Der Angreifer kann ein verstecktes *Markov Diagramm* erstellen. Das bedeutet, dass aus den eingegebenen Daten Wahrscheinlichkeiten vom Angreifer berechnet werden können, so dass auf die Tastenschläge des Benutzers rückgeschlossen werden kann. Mit Hilfe dieses Modells kann der Angreifer zum Beispiel ein Passwort 50 Mal schneller als mit einer *Brute-Force* Attacke erraten.

Seitenkanalangriffe können außerdem bei *Voice over IP* auftreten [9]. *Voice over IP* bezeichnet im Allgemeinen digitalisierte Telefonie über Computernetzwerke. Hierbei kann ein Angreifer, trotz verschlüsselter Übertragung der Audioanrufe, die Längen der verschlüsselten VoIP-Pakete nutzen, um gesprochene Sätze der Benutzer zu identifizieren. Dem Angreifer wird es somit ermöglicht, das Telefongespräch zu belauschen und somit die Konversation teilweise zu rekonstruieren.

2.2 Wandlung von Desktop-Anwendungen zu Web-Anwendungen

Auch gegen Web-Anwendungen sind Seitenkanalangriffe möglich. Dies wird bei den Unterschieden zwischen Desktop- und Web-Anwendungen offensichtlich.

Mit der Entwicklung des Internets kann der Benutzer interaktiver im und mit dem Internet agieren. Außerdem werden vollwertige Anwendungen und Dienste im World Wide Web bereitgestellt. Die Ähnlichkeiten zwischen Web- und Desktop-Anwendungen sind sehr groß. Eingaben kommen sowohl für Desktop- als auch für Web-Anwendungen entweder vom Benutzer selbst oder vom Dateisystem. Bei beiden Anwendungen regelt der interne Informationsfluss, der aus Daten- und Kontrollfluss besteht, die Zustandsübergänge.

Jedoch gibt es auch Unterschiede. Ein Vorteil von Web-Anwendungen besteht darin, dass der Endnutzer keine spezielle Software und die dazugehörige Installation benötigt, um diese auszuführen. Unabhängig vom Betriebssystem kann der Endnutzer die Anwendung im Browser benutzen. Außerdem existieren automatische Updates, so dass Aktualisierungen alleine durch das System durchgeführt werden und die Anwendung immer auf dem neusten Stand ist - der Nutzer hat somit keinen zusätzlichen Arbeitsaufwand.

Ein weiterer großer Unterschied ist, dass Web-Anwendungen dem Benutzer online zur Verfügung stehen. Sie bieten den gleichen Funktionsumfang und ähnliche Benutzeroberflächen wie Desktop-Anwendungen.

Desktop-Anwendungen besitzen nur den Informationsfluss, der aus Daten- und Kontrollfluss besteht. Bei Webanwendungen hingegen existieren noch die Informationen, die durch

doi: 10.2313/NET-2011-07-2_19

das Netzwerk gehen, da Web-Anwendungen in eine Browser- und eine Serverkomponente aufgeteilt sind. Diese Informationen werden *Web-Flows* genannt und existieren neben dem Informationsfluss. Dieser Unterschied führt dazu, dass Seitenkanalangriffe überhaupt gegen Web-Anwendungen möglich sind, wie weiter unten beschrieben wird.

Ein Vorteil von Web-Anwendungen ist offensichtlich: Ein Server stellt Daten zur Verfügung, speichert und verwaltet diese. Der Endbenutzer kann über den Browser, der als Schnittstelle zwischen dem Benutzer und dem Server fungiert, auf diese Daten in der Anwendung zugreifen.

Jedoch wird hier auch ein Nachteil sichtbar. Der Browser muss mit dem Server kommunizieren. Das Problem besteht darin, dass *Web-Flow* Vektoren, die durch den Seitenkanal gehen, für einen Angreifer sichtbar sind. Diese Vektoren kann der Angreifer nutzen, um Benutzereingaben zu ermitteln. In den folgenden Abschnitten wird genauer erklärt, wie Web-Anwendungen aufgebaut sind und wie daraus Seitenkanalangriffe gegen Web-Anwendungen resultieren.

2.3 Web-Anwendungen - Aufbau, Funktionalität und Schwachstellen

Web-Anwendungen sind unterteilt in eine Browser- und eine Server-Komponente. Der Webbrowser ist die darstellende Komponente bzw. das User-Inferface, die es dem Benutzer erlaubt, die Anwendung zu benutzen. Das resultierende Problem ist, dass ein Bruchteil des internen Informationsflusses im Netzwerk sichtbar wird - sprich die *Web-Flows*. Der Grund ist, dass eine Anwendung in verschiedene Zustände mit einer Zustandsübergangsfunktion übergehen kann. Diese Information kann mit Hilfe von *Web-Flow* Vektoren sichtbar werden. Der Angreifer kann Rückschlüsse auf personenbezogene Daten ziehen, sobald er *Web-Flows* belauschen kann. Es wird offensichtlich, dass *Web-Flows* den Angriffspunkt für Belauscher darstellen.

Grundsätzlich sind kryptographische Methoden notwendig, die den Netzwerkverkehr verschlüsseln, so dass der Angreifer keinen direkten Zugriff auf Klartextnachrichten hat. Abhilfe sollen HTTPS oder WPA/ WPA2 schaffen. Trotz dieser Kommunikationsprotokolle und Verschlüsselungsmethoden kann der Angreifer Seitenkanal-Informationen ausspähen, wie zum Beispiel:

- Größe des Pakets
- Anzahl der Pakete
- Dauer der Übermittlung eines Pakets

Mit Hilfe der Seitenkanal-Informationen, kann der Angreifer Rückschlüsse über interne, vertrauenswürdige Informationen und die Inhalte der Kommunikation herausfinden.

Somit sieht der allgemeine, grobe Ablauf eines Seitenkanalangriffs folgendermaßen aus: Eine Webseite hat eine individuelle Größe. Sobald Ressourcen bzw. Objekte mit verschiedenen Größen auf die Seite geladen werden und der Angreifer Seitenkanal-Informationen belauschen kann, kann der Angreifer eingegebene Informationen des Benutzers ermitteln. Die genaue Vorgehensweise des Angreifers bei einem Seitenkanalangriff wird in Kapitel 2.3.2 beschrieben.

Die Gefahr, die durch einen erfolgreichen Seitenkanalangriff entstehen kann, ist, dass ein Angreifer auf personenbezogene Daten und Online-Aktivitäten eines Benutzers zugreifen kann. Erstens resultiert daraus ein enormes Sicherheitsproblem, falls der Angreifer an extrem sicherheitsbedürftige Daten kommen kann. Zweitens stellt dies eine Verletzung der Privatsphäre des Benutzers dar.

2.3.1 Modellierung von Web-Anwendungen

Eine Webanwendung kann wie folgt als Dreiertupel beschrieben werden:

- S: S stellt die Menge aller Zustände der Web-Anwendung dar.
- Σ: Σ stellt die Menge der Eingaben dar, die akzeptiert werden.
- δ: S x $\Sigma \rightarrow$ S: δ ist die Zustandsübergangsfunktion.

Allerdings kann eine Web-Anwendung aus Sicht des Angreifers zu einem Fünfertupel erweitert werden, wie es in Referenz [1] definiert ist. Neben S, Σ und δ kommen folgende zwei Elemente dazu:

- V: V stellt die Menge aller *Web-Flow* Vektoren dar. Diese Menge beschreibt die beobachteten Eigenschaften des verschlüsselten Datenaustauschs.
- f: S x $\Sigma \rightarrow$ V: f ist die Funktion, die angibt, was der Angreifer beobachten kann. Zustandsübergänge sind immer mit *Web-Flow* Vektoren verbunden.

Die beobachteten Attribute können vom Angreifer genutzt werden, um Originalzustände und die dazugehörigen Eingaben zu rekonstruieren.

2.3.2 Seitenkanalangriffe gegen Web-Anwendungen - Reduktion des Ambiguity Sets

Das *Ambiguity Set* kann man definieren als eine Menge von Mehrdeutigkeiten. Der Angreifer versucht, die verschiedenen Bedeutungen der Benutzereingabe zu analysieren und bestimmte auszuschließen. Somit kann er eine eindeutige Lösung herleiten, wie die Benutzereingabe aussah.

Der Angreifer versucht aus den für ihn sichtbaren Daten, Rückschlüsse über die Eingabe des Benutzers zu ziehen. Er beobachtet eine Sequenz von Vektoren (v_t, ..., v_{t+n-1}) und verringert per Ausschlusskriterium das *Ambiguity Set* so weit, bis nur noch eine bestimmte eindeutige Kombination aus der Menge der möglichen Informationen für einen Vektor v übrig bleibt. Grundsätzlich muss dem Angreifer eine gewisse Grundmenge von Informationen zur Verfügung stehen, um Vektoren beobachten, identifizieren und ausschließen zu können.

Abbildung 1 veranschaulicht die Reduktion eines *Ambiguity Sets*: Zu einem bestimmten Zeitpunkt t befindet sich eine

doi: 10.2313/NET-2011-07-2_19

Anwendung im Zustand s_t, der eine Eingabe entweder vom Benutzer oder vom Dateisystem akzeptiert - mit einer Eingabe kommt die Anwendung vom Zustand s_t zum Zustand s_{t+1}. Der Eingaberaum ist in k verschiedene Mengen aufgeteilt, die disjunkt sind. Jede Eingabemenge bewirkt eine Zustandsänderung in einen Zustand, der von s_t aus erreicht werden kann (alle Zustände, die von s_t aus erreicht werden können, liegen in der Menge S_{t+1}, wobei diese Menge eine Teilmenge von S darstellt: $S_{t+1} \subset S$).

Der Angreifer betrachtet eine Sequenz von Vektoren (v_t, ..., v_{t+n-1}). Diese Vektoren veranlassen die Web-Anwendung, eine Zustandsänderung von s_t zu s_{t+1} durchzuführen. Die Sequenz entsteht demnach durch n Zustandsübergänge vom Ausgangszustand s_t. Bis jetzt hat der Angreifer lediglich die Information über die Vektoren; er hat noch keine Informationen über die Eingabe des Benutzers.

Da es k verschiedene Möglichkeiten für die Eingabe gibt, hat das *Ambiguity Set* die Größe k. Nun geht der Angreifer wie folgt vor: mit Hilfe des ersten Vektors v_t weiß er, dass nur Eingaben, die zu einer Untermenge von S_{t+1} führen, den Vektor v_t produzieren können. Das bedeutet, dass nur Übergänge zu einer bestimmte Untermenge von S_{t+1} durch diesen Vektor ermöglicht werden. Diese Untermenge wird mit D_{t+1} gekennzeichnet. Der Angreifer hat nun die Möglichkeit, eine bestimmte Menge aus der Menge der möglichen Informationen zur Eingabe auszuschließen - die tatsächliche Eingabe des Benutzers kann nur von k/α der Menge aller Eingabemöglichkeiten stammen. α ist der erste Reduktionsfaktor dieses Zustandsüberganges.

Der Angreifer wiederholt diese Prozedur und kann erneut das *Ambiguity Set* von D_{t+1} reduzieren. Hierbei betrachtet er die folgenden Vektoren (v_{t+1}, ..., v_{t+n-1}). Bei dieser Reduktion kann der Angreifer erneut eine bestimmte Menge aus der Menge der möglichen Informationen mit Hilfe des folgenden Reduktionsfaktors β ausschließen: k / (α*β). Somit wiederholt der Angreifer die Methode, die Menge an Mehrdeutigkeiten zu reduzieren, so lange, bis er eine eindeutige Lösung hat, wie die Benutzereingabe aussah. Dazu verwendet er die weiteren *Web-Flow* Vektoren ab v_{t+2}. Somit fasst der Reduktionsfaktor β alle folgenden Reduktionen des *Ambiguity Sets* zusammen. Am Ende kann die Benutzereingabe identifiziert werden. Es ist offensichtlich, dass die Reduktionsfaktoren durch Zustandsübergänge entstehen und dass sie anwendungsabhängig sind.

Die Methode, das *Ambiguity Sets* zu reduzieren, funktioniert umso besser, je weniger Möglichkeiten der Benutzer für seine Eingabe hat. Zum Beispiel erlauben Drop-Down Listen nur eine eingeschränkte Auswahl, wohingegen die Reduktion des *Ambiguity Sets* bei Freitexten aufgrund des größeren Informationsgehalts schwieriger ist.

2.3.3 Wahrscheinlichkeit eines Seitenkanalangriffs gegen Web-Anwendungen

Die Wahrscheinlichkeit eines Seitenkanalangriffs ist abhängig von der Eingabe, den Reduktionsfaktoren und signifikanter Traffic-Unterschiede.

- Die Gefahr eines Seitenkanalangriffs steigt, je weniger Möglichkeiten der Benutzer bei der Eingabe hat - das heißt die Eingabe besitzt eine geringe Entropie. Es stellt sich die Frage, ob der Angreifer effizient testen kann, um welche Benutzereingabe es sich anhand des Ergebnisses, das produziert wird, handelt.

- Bei einer zustandsbehafteten Kommunikation entstehen Reduktionsfaktoren. Je größer die Reduktionsfaktoren, desto größer die Gefahr eines Seitenkanalangriffs; denn der Angreifer kann mit großen Reduktionsfaktoren Mehrdeutigkeiten ausschließen und auf die ursprüngliche Eingabe des Benutzers schließen. Fraglich ist, wie groß das Ausmaß der Informationen ist, die der Angreifer erfahren kann.

- Je mehr signifikante Traffic Unterschiede für den Angreifer erkennbar sind, desto größer ist die Wahrscheinlichkeit, dass der Angreifer auf personenbezogene Daten rückschließen kann. Web-Traffic entsteht zum Beispiel, wenn eine Ressource auf eine Webseite hochgeladen wird.

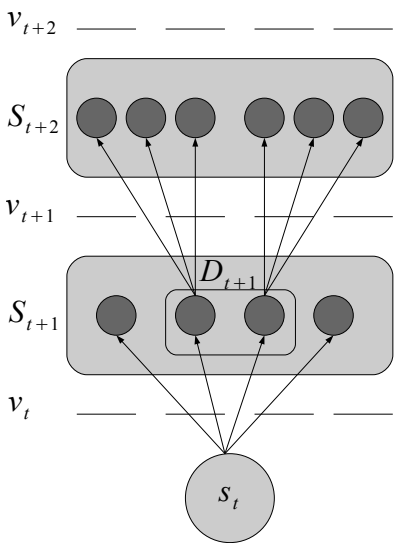


Abbildung 1: Reduktion des *Ambiguity Sets* [1]

3. BEISPIELE FÜR SEITENKANALANGRIFFE GEGEN WEB-ANWENDUNGEN

In diesem Kapitel wird auf Beispiele zu Seitenkanalangriffen speziell gegen Web-Anwendungen eingegangen, die trotz Verschlüsselung möglich sind. Vor allem das Szenario, das *Auto-Suggestion* betrifft, wird genauer erklärt.

3.1 Aktuelle Herausforderungen des Web 2.0

Mit der Entwicklung des Web 2.0 und der enormen Online-Bereitstellung von Diensten und Anwendungen, wächst die Gefahr von Seitenkanalangriffen. Die Hauptursache von Seitenkanalangriffen sind Features, die eine Web 2.0 Anwendung ausmachen, wie zum Beispiel *AJAX GUI Widget*. Dies ist ein Konzept der Datenübertragung zwischen Browser und Server, bei dem Web Traffic mit jedem Mausklick oder mit jedem Tastendruck generiert wird [7].

doi: 10.2313/NET-2011-07-2_19

Datenschutz und Sicherheit müssen trotzdem gewährleistet sein, vor allem bei extrem sicherheitsbedürftigen Web-Anwendungen und für vertrauenswürdige Daten, die zum Beispiel Gesundheitsstand, Einkommen der Familie, Investmentgeheimnisse oder Steuerinformationen betreffen.

3.2 Probleme trotz HTTPS

HTTPS steht für *Hypertext Transfer Protocol Secure* und ist ein Kommunikationsprotokoll im Internet [5]. Es wird für die Authentifizierung und Verschlüsselung der Kommunikation zwischen Webserver und Browser im Internet verwendet. Dies bedeutet, dass zum einen Daten durch Verschlüsselung geschützt sein sollten vor Sniffing-Angriffen; zum anderen sollten Phishing-Angriffe durch Authentifizierung abgewehrt werden.

3.2.1 Automatische Vorschläge bei Benutzereingabe

Seitenkanalangriffe können bei Webseiten auftreten, die bei Eingabe des Benutzers automatisch Vorschläge für die Vervollständigung der Eingabe anbieten. Das bedeutet, dass der Angreifer Rückschlüsse über die Eingabe ziehen kann, denn sobald der Benutzer einen Buchstaben eingibt, erscheint eine Liste mit Vorschlägen, die abhängig vom vorangegangenen Buchstaben verschieden groß ist und die bei jedem neuen Buchstaben aktualisiert wird.

Der Angreifer kann nun das *Ambiguity Set* - Menge mit Mehrdeutigkeiten - reduzieren, indem er zwischen der eigentlichen Eingabe des Benutzers nach jedem Buchstaben und der Größe der Antwort, also der Anzahl der Elemente in der Liste mit den automatischen Vorschlägen, vergleicht. Jeder Buchstabe generiert einen *Web-Flow* Vektor. Gleichzeitig wird die Liste mit Vorschlägen zur Vervollständigung der Eingabe automatisch angepasst. Diese Liste ist bei jedem Benutzer gleich groß, somit weiß auch der Angreifer über den Umfang der Liste Bescheid.

Zusätzlich ist die Kommunikation zustandsbehaftet. Jeder Buchstabe ist abhängig von dem vorherigen, das heißt jeder Buchstabe ist abhängig von dem eingegebenen Präfix. Somit wird es dem Angreifer weiterhin erleichtert, das Eingangssignal des Benutzers abzuleiten. Die Effektivität, mit der der Angreifer Rückschlüsse ziehen kann, ist abhängig von den Reduktionsfaktoren α und β.

Als konkretes, allerdings nicht allgemeingültiges Beispiel zum ersten Reduktionsfaktor α gibt man alle Buchstaben von ‘a’, ‘b’, ..., ‘z’ einmal als Anfangsbuchstaben ein. Die *Web-Flow* Vektoren, die jeweils dadurch erzeugt werden, werden verglichen: die Größe der Listen mit automatischen Ergänzungsvorschlägen ist verschieden, außer nach beispielsweise den Eingaben ‘h’ und ‘m’. Darauf wird im nächsten Absatz näher eingegangen. Weiterhin werden alle Buchstaben von ‘a’ bis ‘z’ eingegeben; diesmal werden diese allerdings als zweiter Buchstabe geschrieben nach einem ‘a’. Nur 20 Kombinationen erzeugen eine nicht-leere Liste mit Vorschlägen. Die restlichen Kombinationen sind ungültig. Dieses Beispiel zeigt, dass der Reduktionsfaktor α für den Angreifer von großer Bedeutung ist.

Der Reduktionsfaktor β hilft außerdem, das *Ambiguity Set* der Benutzereingabe zu verkleinern. Wie oben beschrieben, erzeugen die Buchstaben ‘m’ und ‘h’ als Anfangsbuchstaben jeweils eine gleich große Liste mit automatischen Ergänzungsvorschlägen, da beide Buchstaben einen identischen *Web-Flow* Vektor produzieren. Wenn man nun nach den Buchstaben ‘h’ oder ‘m’ einen weiteren Buchstaben eingibt, wie zum Beispiel ‘ha’, ‘hz’, ‘ma’ oder ‘mz’, erhält man 52 Möglichkeiten, wovon 20 ungültig sind, da diese eine leere Liste mit Vorschlägen liefern. Alle *Web-Flows* sind verschieden, mit der Ausnahme ‘ha’ und ‘ma’ - aus ihnen ergeben sich jeweils eine Liste, die gleich groß sind. Mit der Ausnahme von ‘ha’ und ‘ma’ kann ein Angreifer entweder ‘h’ oder ‘m’ als Anfangsbuchstaben ausschließen, indem er *Web-Flow* Vektoren belauscht.

Ein Beispiel stellt die Suchfunktion im Online-Kaufportal *http://www.amazon.de/* (Abbildung 2) dar. Sobald ein Benutzer nach einem Produkt sucht und in die Suchfunktion den Namen eingibt, schlägt diese Webseite automatisch Produkte vor.

3.2.2 Auswahl mit Mausklick aus Liste

Webseiten, bei denen man zum Beispiel zuerst den Anfangsbuchstaben wählt und anschließend per Mausklick aus einer Liste, die alle Wörter mit dem zuvor ausgesuchten Anfangsbuchstaben beinhaltet, auswählen kann, sind gefährdet.

Dieses Szenario stellt eine zustandsbehaftete Kommunikation in einer Hierarchie dar. Der Angreifer kann mit Hilfe eines Vergleichs zwischen Anfangsbuchstaben und der Größe der resultierenden Liste den Anfangsbuchstaben herausfinden - lediglich 26 Mal muss er testen, welcher Anfangsbuchstabe vom Benutzer eingetippt wurde unter der Voraussetzung, dass allen Benutzern die gleichen Daten zur Verfügung stehen. Das heißt, dass jeweils die einzelnen Listen bei jedem Benutzer gleich groß sind. Somit wird die Entropie der Benutzereingabe deutlich reduziert und die Zustände der Web-Anwendung können vom Angreifer eindeutig identifiziert werden.

Es sind auch andere Vorauswahlmöglichkeiten denkbar. Webseiten, die es dem Benutzer ermöglichen, Musik auszuwählen und anzuhören, wie zum Beispiel *http://www.lastfm.de/music*, beinhalten die Vorauswahl nach Musikgenres. Abhängig von der Auswahl eines Genres durch den Benutzer kann der Angreifer sich mit Hilfe der daraus resultierenden Liste, die Aktivität des Benutzers herleiten.

3.2.3 Drop-Down Liste gekoppelt mit Eingabe eines Namens oder eines Codes

Angreifer können bei einer Webseite, die zum Beispiel eine Drop-Down Liste gekoppelt mit der Eingabe eines Stadtnamen oder einer Postleitzahl enthält, eine Seitenkanalattacke durchführen.

Zum einen gibt der Stadtname oder die Postleitzahl dem Angreifer Aufschluss über die Eingabe des Benutzers. Der Angreifer kann diese Eingabe mit Hilfe der IP-Adresse erraten.

Zum anderen bietet die Drop-Down Liste eine geringe Entropie für die Eingabe. Die Anzahl der Möglichkeiten, ein Element aus der Drop-Down Liste auszuwählen, ist nicht

doi: 10.2313/NET-2011-07-2_19

sehr hoch. Somit ist es für den Angreifer effizient testbar, welches Element der Benutzer aus der Liste ausgewählt hat.

Erneut ist die bekannte Webseite *http://www.amazon.de/* (Abbildung 2) zu nennen, da sie Drop-Down Listen beinhaltet. Hier wird zwar kein Stadtname oder keine Postleitzahl eingegeben; allerdings kann der Benutzer ein Produkt, nach dem er sucht, eingeben. Außerdem bietet die Webseite bei der Benutzereingabe automatische Vorschläge, passend zum gesuchten Produkt, an.

Abbildung 2: Drop-Down Liste auf der Webseite *http://www.amazon.de/*

3.2.4 *Traffic-Analyse einer Anwendung*

Web-Anwendungen, bei denen der Benutzer Formulare ausfüllen und dabei einen Teil des Formulars mehrfach durchlaufen muss, sind von Seitenkanalangriffen betroffen. Ein typisches Beispiel ist ein Steuerformular, bei dem der Benutzer bei jedem einzelnen Kind ein bestimmtes Formular ausfüllen muss.

Jeder Benutzer produziert einen individuellen *Web-Flow* Vektor, weiterhin handelt es sich um eine Kommunikation mit Zuständen. Zustandsübergänge können leicht vom Angreifer mit Hilfe der *Web-Flow* Vektoren identifiziert werden. In gewissen Situationen reicht es sogar, wenn der Angreifer zählt, wie oft der Benutzer eine bestimmte Schleife durchlaufen hat.

Durch asymmetrische Ausführungspfade kommt das zusätzliche Problem hinzu, dass der Angreifer leicht Rückschlüsse ziehen kann. Der Angreifer kann sich ein Diagramm mit Zuständen und der internen Entscheidungslogik der Anwendung herleiten. Ein Beispiel wäre, wenn sich der Ausführungspfad einer Web-Anwendung in einem bestimmten Zustand in zwei parallele Pfade aufspaltet. Beide Pfade sind unterschiedlich lang und führen wieder in einen gemeinsamen Zustand. Angenommen der erste Ausführungspfad ist sehr kurz, wohingegen der andere bedeutend länger ist. Der erste, kurze Pfad produziert weniger *Web-Flow* Vektoren als der lange Ausführungspfad. Der Angreifer kann nun ermitteln, welchen Pfad der Benutzer gewählt hat.

3.2.5 *Graphische Visualisierung von Daten*

Ein Beispiel für eine gefährdete Webseite gegenüber Seitenkanalangriffen ist eine Webseite, die die Daten graphisch visualisiert. Der Benutzer klickt aus einer Liste entweder eine Graphik selbst oder einen Link zur Graphik an.

Auf der einen Seite ergibt sich abermals das Problem der geringen Entropie der Nutzereingabe. Der Benutzer hat nur begrenzte Auswahlmöglichkeiten, ein Element anzuklicken. Dadurch hat der Angreifer den Vorteil, dass er testen kann, welches Bild der Benutzer mit größter Wahrscheinlichkeit ausgewählt hat.

Auf der anderen Seite haben die Graphiken verschiedene Größen. Somit kann der Angreifer erheblich die Auswahlmöglichkeiten reduzieren. Dies ist vor allem der Fall, wenn der Angreifer die vom Server verwendeten Paketgrößen kennt.

Zum Beispiel kann sich ein Benutzer auf der Webseite *http://www.sueddeutsche.de/bilder* verschiedene Bilder ansehen. Jedes Bild hat eine individuelle Größe, so dass der Angreifer ableiten kann, welche Bilder der Benutzer angesehen hat. Grundsätzlich ist es für einen Angreifer leichter, einen erfolgreichen Seitenkanalangriff durchzuführen, umso größer die Unterschiede bezüglich der Größe von Bildern sind.

Falls die Graphiken von einer anderen, öffentlichen Webseite geladen werden, ist der Angreifer wieder im Vorteil - er kann die Paketgrößen vergleichen, welche Hinweise auf die Bildgröße geben, und sich somit die Graphik, die der Benutzer zuvor angeklickt hat, erschließen.

3.3 Probleme trotz WPA/ WPA2

WPA beziehungsweise WPA2 sind Verschlüsselungsverfahren für drahtlose Netzwerke des IEEE Standards 802.11i [10]. Der Vorgänger war WEP (= Wired Equivalent Privacy), welches ein WLAN Verschlüsselungsprotokoll darstellt [11]. WEP war allerdings anfällig, da Schlüssel geknackt werden konnten. Somit wird in der heutigen Zeit das etwas sichere WPA bzw. WPA2 verwendet. WPA steht für Wi-Fi Protection Access.

Trotz WPA bzw. WPA2 sind Seitenkanalangriffe auch ohne Anmeldeinformation oder Berechtigungsnachweis für das jeweilige WLAN möglich. Der Angreifer hat somit die Möglichkeit, aktuelle Aktivitäten von Benutzern zu ermitteln.

Seitenkanalangriffe im WLAN betreffen vor allem Suchmaschinen, wie zum Beispiel *Google* oder *Yahoo* [7]. Auf der einen Seite kann sich der Angreifer die Suchanfragehistorie beschaffen. Damit ist es möglich, vergangene Online-Aktivitäten des Benutzers nachzuvollziehen. Auf der anderen Seite beinhalten die meisten Suchmaschinen Features, so dass automatisch Vorschläge angezeigt werden. Obwohl die Menge der Vorschläge bedeutend groß ist, kann es zu Seitenkanalangriffen kommen, denn eine Folge des Features für automatische Vorschläge ist, dass die damit verbundenen Pakete leicht mit Hilfe der *Web-Flow* Vektoren identifiziert werden können.

Beispielsweise gibt ein Benutzer das Wort ‘Paket’ in eine Suchmaschine ein. Nach jedem Buchstaben wird eine neue Liste von Vorschlägen für ‘P’, ‘Pa’, ‘Pak’, ‘Pake’ und ‘Paket’ erzeugt. Mit jedem weiteren Buchstaben werden die WPA Pakete größer. Die resultierende Größe der Liste der Vorschläge wird mit jedem weiteren Vektor kleiner.

Obwohl die Liste mit den automatischen Vorschlägen enorm

doi: 10.2313/NET-2011-07-2_19

groß ist, funktioniert ein Seitenkanalangriff gegen Suchmaschinen im WLAN. Grundsätzlich hat der Benutzer die Möglichkeit, ein Suchwort über dem Alphabet inklusive des Leerzeichens einzugeben: { a, b, c, ..., z, _ }. Die Anzahl der Möglichkeiten, die der Angreifer für das Erraten des Suchwortes des Benutzers hat, ist linear zu der Länge des Wortes. Der Angreifer kann sich vorab *Google* Suchanfragen generieren, die er dann mit dem Traffic des Benutzers vergleichen und somit die Benutzersuchanfrage in Erfahrung bringen kann.

Die Autoren des Originalpapers (siehe [1]) gehen allerdings nicht auf die Frage ein, wie relevant die Problematik von Seitenkanalangriffen gegen Web-Anwendungen im Kontext von WLAN Verschlüsselungsprotokollen, wie zum Beispiel WPA bzw. WPA2, wirklich ist. Ein solcher Angriff erscheint schwierig, da ein Benutzer mehrere Onlineaktivitäten gleichzeitig durchführen kann oder da mehrere Personen im gleichen WLAN surfen können. Das bedeutet, dass nicht nur ein Datenstrom, sondern mehrere im Netzwerk vorhanden sind. Es ist fraglich, inwieweit der Angreifer den richtigen Datenstrom ermitteln kann, der zur Web-Anwendung gehört - sprich die Pakete passend zur Web-Anwendung.

4. HERAUSFORDERUNGEN

Es ist offensichtlich, dass Seitenkanalangriffe ein großes Problem darstellen, da es durch einen erfolgreichen Seitenkanalangriff gegen Webanwendungen möglich ist, dass ein Angreifer die Privatsphäre des Benutzers verletzen kann. Eine universelle Abhilfe, das Problem zu lösen, existiert nicht. Wissen über jede individuelle Anwendung ist somit unumgänglich. Zusätzlich stehen Softwareentwickler vor der Herausforderung effektive und effiziente Lösungen zu finden.

Grundsätzlich müssen Entwickler die Sicherheitslücken finden und anschließend müssen Regelwerke spezifiziert werden. Diese beiden Aspekte stellen die technischen Herausforderungen dar. Der Vorgang, um Lösungen gegen Seitenkanalangriffe zu finden, ist abhängig von der jeweiligen Anwendung.

Als erstes müssen Sicherheitslücken identifiziert werden. Notwendig ist das Wissen über den Informationsfluss einer Web-Anwendung, so dass die Identifikation von Sicherheitslücken erleichtert wird. Außerdem sollte dies schon während der Entwicklung und während des Testens einer Web-Anwendung geschehen.

Als Zweites müssen Regelwerke gefunden und durchgesetzt werden. Mit Hilfe des Verständnisses der Entwickler über eine Web-Anwendung ist das Design eines Regelwerkes möglich. Um ein Regelwerk zu spezifizieren und diese Regeln auch durchsetzen zu können, ist die Zusammenarbeit zwischen den Entwicklern der Browser und der Server sowie der Web-Anwendungen zwingend erforderlich.

Letztendlich ist das Wissen über die individuelle Anwendung notwendig. Für Softwareentwickler, die eine Lösung implementieren, ist es erforderlich, jede Web-Anwendung separat zu betrachten. Dazu gehören die Programmstruktur, Zustandsübergänge und Wissen über den Gebrauch der Anwendung. Wie oben erwähnt ist das Verständnis über den Informationsfluss zusätzlich notwendig.

5. VERTEIDIGUNGSMECHANISMEN UND LÖSUNGSANSÄTZE

Es wurde gezeigt, dass Kommunikationsprotokolle und Verschlüsselungsverfahren, wie HTTPS oder WPA/WPA2, nicht ausreichen, um Seitenkanalangriffe zu verhindern.

Allgemeine Lösungsansätze sehen wie folgt aus:

- Padding-Pakete
- Gefälschte, überflüssige Pakete
- Zerlegen von Paketen in Segmente fester Größe
- Zusammenmischen oder Trennen von Zuständen
- Kombination der oben genannten Lösungsansätze

Jedoch ist die Umsetzung und der Einsatz solcher Lösungsansätze nicht immer für Web-Anwendungen realisierbar. Da diese sehr komplex sind, sind spezielle Lösungen für Web-Anwendungen erforderlich. Vor allem müssen Lösungen getrennt voneinander für jede Anwendung entworfen werden, da es zum einem kaum generische Lösungen gibt und zum anderen anwendungsindividuelles Wissen notwendig ist.

Folgender Lösungsansatz ist für Web-Anwendungen sinnvoll: Padding. Dieser ist aber nicht effektiv bei Seitenkanalangriffen gegen Suchmaschinen, sondern bei Seitenkanalangriffen gegen Webseiten, die beispielsweise Features, wie automatische Ergänzungsvorschläge für die Benutzereingabe oder Drop-Down Listen, enthalten. Man kann unterscheiden zwischen Runden und zufälligem Padding. Beim Runden wird die Größe von jedem Paket aufgerundet, so dass das Paket durch eine bestimmte Anzahl von Bytes teilbar ist. Das zufällige Padding meint, dass jedem Paket ein zufällig langes Padding angehängt wird. Allerdings ergibt sich beim Padding das Problem eines zu großen Overheads.

Ein weiterer Lösungsansatz ist das Zusammenmischen von verschiedenen Zuständen. Dies ist vor allem sinnvoll, je länger der Ausführungspfad ist. Beispielsweise gibt es zwei parallele Ausführungspfade - einer sehr kurzer und ein sehr langer Pfad -, wobei beide einen gemeinsamen Anfangszustand und einen gemeinsamen Endzustand haben. Je länger der Pfad ist, desto mehr Zustände sind dazwischen. Der Angreifer kann nun ermitteln, welchen Pfad der Benutzer durchläuft. Denn sobald dieser den längeren Ausführungspfad durchläuft, entstehen bedeutend mehr *Web-Flow* Vektoren, die der Angreifer nutzen kann, um das *Ambiguity Set* zu reduzieren.

Außerdem ist das Produzieren von überflüssigen Paketen, um zusätzliche Zustände zu fälschen, ein weiterer Lösungsansatz. Diese Technik wird vor allem eingesetzt, je kürzer der Ausführungspfad ist. Nimmt man das obere Beispiel eines kurzen und eines langen Ausführungspfades, die parallel verlaufen, das heißt mit gleichem Start- und Endzustand, ist es offensichtlich, dass der Angreifer über die Anzahl der beobachteten *Web-Flow* Vektoren Rückschlüsse über den Inhalt ziehen kann.

Suchmaschinen müssen separat betrachtet werden. Diese stellen ein nur schwer lösbares Problem dar, jedoch wird

doi: 10.2313/NET-2011-07-2_19

sich erst in der Zukunft zeigen, wie groß das Ausmaß ist, inwieweit Suchmaschinen von Seitenkanalangriffen gefährdet sind. Es existieren keine universellen Lösungen, um Seitenkanalangriffe im WLAN gegen Suchmaschinen zu verhindern. Aufgrund der Komplexität von universellen Lösungen können diese hohe Kosten verursachen. Eine realistischere Alternative ist, empfindliche, sicherheitsbedürftige Features zu identifizieren und dafür spezielle Lösungen zu finden. Ein Beispiel für ein Feature von Suchmaschinen, sodass Seitenkanalangriffe möglich sind, ist die automatische Ergänzungsfunktion.

Probleme bei Suchmaschinen im Internet sind erstens, dass sie mit einem enorm hohen Volumen an Daten umgehen. Zweitens ist es fraglich, ob Regelwerke durchgesetzt werden können - dies ist abhängig von der Anwendung, das bedeutet, dass jede Web-Anwendung einzeln zu betrachten ist. Somit ist es schwer Lösungen zu finden, um Seitenkanalangriffe gegen Suchmaschinen im Internet zu verhindern.

Allgemein ist es sinnvoll, sich während des Entwicklungsprozesses jeder einzelner Web-Anwendung der Gefahr eines Seitenkanalangriffs zu widmen. Abbildung 3 zeigt eine mögliche Vorgehensweise für den Entwicklungsprozess einer individuellen Anwendung zur Identifizierung von Sicherheitslücken und Definition von Regelwerken. Hierbei ist es von Vorteil, mit einem Traffic-Analysetool zu arbeiten. Die Abbildung beschreibt den Entwicklungsprozess wie folgt: Jede Web-Anwendung hat individuelle Sicherheitsziele, um die Privatsphäre zu schützen. Sowohl statisch als auch dynamisch muss eine Flussanalyse durchgeführt werden, um den Informationsfluss (Daten-, Kontrollfluss und *Web Flow*) von sicherheitsbedürftigen Daten zu verfolgen und damit Verstöße gegen Sicherheitsziele zu finden. Hierbei kann ein automatisches Tool hilfreich sein. Falls Sicherheitslücken gefunden werden, muss der Entwickler herausfinden, ob diese Lücke durch eine geeignete Erweiterung der Regeln, wie zum Beispiel Padding, geschlossen werden kann. Wenn dies der Fall ist, müssen neue Regeln spezifiziert werden. Ansonsten muss das Design der Anwendung angepasst werden. Der beschriebene Vorgang für einen Entwicklungsprozess ist für jede Anwendung separat durchzuführen.

Grundsätzlich sind die Kosten für individuelle Lösungen enorm, so dass die Entwicklung von automatischen Tools unumgänglich ist.

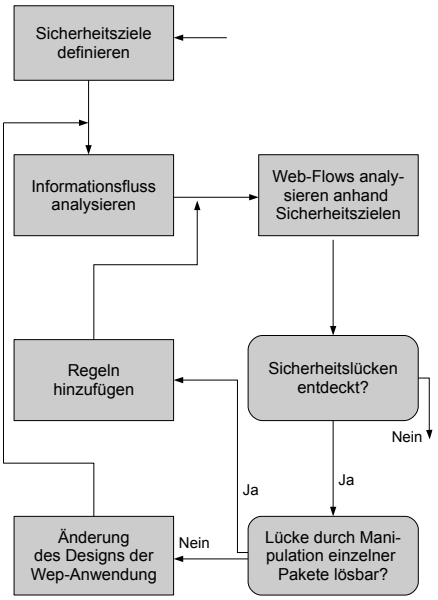


Abbildung 3: Vorgehensweise während eines Entwicklungsprozesses einer Web-Anwendung, wie in Referenz [1]

In Referenz [1] wird von den Autoren behauptet, dass keine generischen Lösungen existieren, so dass Seitenkanalangriffe gegen Web-Anwendungen abgewehrt werden können. Allerdings wird nicht explizit beschrieben, warum es keine generischen Lösungen gibt. Denkbar wäre es zum Beispiel, dass man unabhängig von der Benutzereingabe pro Zeiteinheit immer die gleiche Datenmenge versendet.

Da individuelle Lösungen außerdem sehr teuer sind, müssen automatische Tools entwickelt werden. Solche Tools sollten eingesetzt werden, um während des Entwicklungsprozesses mögliche Schwachstellen zu erkennen. Zusätzlich sollen sie als Hilfsmittel dienen, um den Sourcecode einer Web-Anwendung zu analysieren und den Umfang zu messen, inwieweit interne Daten sichtbar sind.

Fraglich ist, wie groß das Ausmaß der Gefahr von Seitenkanalangriffen gegen Webanwendungen in der Zukunft wirklich ist. Es ist außerdem abzuwarten, wie zukünftige Entwicklungen aussehen werden, um die Gefahr von Seitenkanalangriffen zu verringern und ob diese Entwicklungen es wirklich ermöglichen können, effektiv und effizient vor Seitenkanalangriffen zu schützen.

6. FAZIT

Seitenkanalangriffe stellen in der heutigen Zeit eine extreme Gefahr für personenbezogene Daten dar. Mit Hilfe von Seitenkanal-Informationen - Attributen einer verschlüsselten Datenübertragung - kann der Angreifer Rückschlüsse über die Eingaben des Benutzers ziehen. Dies geschieht unter Verwendung der aus der Benutzereingabe resultierenden Ergebnisse.

Auch wenn das Finden von Verteidigungsmechanismen schwer erscheint, ist dies notwendig, da das Problem von Seitenkanalangriffen gegen Web-Anwendung sehr aktuell ist. Zuerst müssen Sicherheitslücken identifiziert und anschließend Regelwerke definiert werden, um die Gefahr von Seitenkanalangriffen zu reduzieren.

7. LITERATUR

[1] S. Chen, R. Wang, XF. Wang, K. Zhang: *Side-Channel Leaks in Web Applications: a Reality Today, a Challenge Tomorrow*, pp.191-206, Proc. IEEE Symposium on Security and Privacy, 2010

[2] J.J. Quisquater: *Side-Channel Attacks*, 2002, `http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/1047_Side_Channel_report.pdf`, zugegriffen am 20.05.2011

[3] M. Witteman, M. Oostdijk: *Secure Application*

doi: 10.2313/NET-2011-07-2_19

Programming in the Presence of Side Channel Attacks, RSA Conference, Riscure, Netherlands, 2008, `http://www.riscure.com/fileadmin/images/Docs/Paper_Side_Channel_Patterns.pdf`, zugegriffen am 20.05.2011

[4] K. Tiri: *Side-Channel Attack Pitfalls*, Proc. of the 44th annual Design Automation Conference, Platform Validation Architecture, San Diego, California, USA, 2007

[5] E. Rescorla, A. Schiffman, *The Secure Hypertext Transfer Protocol*, RFC 2660, August 1999, `http://www.apps.ietf.org/rfc/rfc2660.html`, zugegriffen am 20.05.2011

[6] P. Anderson, *What is Web 2.0? - Ideas, Technologies and Implications for Education*, JISC, Technology and Standard Watch, 2007

[7] K. Zhang, Z. Li, R. Wang, XF. Wang, S. Chen *Sidebuster: Automated Detection and Quantification of Side-Channel Leaks in Web Application Development*, Proc. of the 17th ACM conference on Computer and communications security, Chicago, Illinois, USA, 2007

[8] D. F. Song, D. Wagner, X. Tian *Timing Analysis of Keystrokes and Timing Attacks on SSH*, Proc. of the 10th conference on USENIX Security Symposium, Vol. 10, University of California, Berkeley, USA, 2001

[9] C. V. Wright, L. Ballard, S. E. Coull, F. Monrose, G. M. Masson *Spot me if you can: Uncovering spoken phrases in encrypted VoIP conversations*, IEEE Symposium on Security and Privacy, pp.35-49, John Hopkins University, Department of Computer Science, Baltimore, USA, 2008

[10] C. Eckert, *IT-Sicherheit: Konzepte - Verfahren - Protokolle*, 6. Auflage, Oldenburg Wissenschaftsverlag GmbH, ISBN 978-3-486-58999-3, München, 2009

[11] IEEE Standards *802.11i-2004: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications*, New York, USA, 2004

doi: 10.2313/NET-2011-07-2_19

An Introduction to Duality in Convex Optimization

Stephan Wolf
Betreuer: Stephan M. Günther, M.Sc.
Hauptseminar Innovative Internettechnologien und Mobilkommunikation SS2011
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: wolfst@in.tum.de

ABSTRACT

This paper provides a short introduction to the Lagrangian duality in convex optimization. At first the topic is motivated by outlining the importance of convex optimization. After that mathematical optimization classes such as convex, linear and non-convex optimization, are defined. Later the Lagrangian duality is introduced. Weak and strong duality are explained and optimality conditions, such as the complementary slackness and Karush-Kuhn-Tucker conditions are presented. Finally, three different examples illustrate the power of the Lagrangian duality. They are solved by using the optimality conditions previously introduced.

The main basis of this paper is the excellent book about convex optimization [5] of Stephen Boyd and Lieven Vandenberghe.

Keywords

mathematical optimization problem, convex optimization, linear optimization, Lagrangian duality, Lagrange function, dual problem, primal problem, strong duality, weak duality, Slater's condition, complementary slackness, Karush-Kuhn-Tucker conditions, constrained least squares problem, water filling algorithm

1. MOTIVATION

Convex optimization[1] is very important in practice. Applications are numerous. Important areas are for example automatic control systems, estimation and signal processing, communications and networks, electronic circuit design, data analysis and modelling, statistics and finance (see [5], p. xi). Furthermore linear optimization, which is a subclass of convex optimization, bases mainly on the theory of convex optimization.

One advantage of these convex optimization problems is that there exists methods to solve them very reliably and efficiently, whereas there are no such methods for the general non-linear problem so far. One example is the interior-point method, which can be used to solve general convex optimization problems. However, its reliability and efficiency are still an active topic of research, but it is likely that these difficulties will be overcome within a few years. (See [5], p.8).

Another even more important advantage is the associated dual problem. Each convex optimization problem can be transformed to a dual problem, which provides another perspective and mathematical point of application. With the dual problem it is often possible to determine the solution of the primal problem analytically or alternatively to determine efficiently a lower bound for the solution (even of non-convex problems). Furthermore the dual theory is a source of interesting interpretations, which can be the basis of efficient and distributed solution methods.

Therefore, when tackling optimization problems, it is advisable to be able to use the powerful tool of Lagrangian duality. This paper offers an introduction to this topic by outlining the basics and illustrating these by three examples.

The following section presents an overview over the different optimization classes and explains the difference of convex and linear optimization. After that, Lagrangian duality is introduced and intuitively derived. Furthermore, weak and strong duality are explained and Slater's condition, which guarantees strong duality for convex optimization, is described. The Section 4 introduces optimality conditions, concretely the complementary slackness condition and the Karush-Kuhn-Tucker conditions. They will be used to demonstrate the power of duality to solve convex optimization problems by the dual in Section 5. In particular, duality is used to solve a constrained least squares problem and to derive the water-filling method. At the end, a conclusion is drawn and further literature hints are presented.

2. OPTIMIZATION PROBLEMS

There are different kinds of mathematical optimization problems, for example non-convex, convex and linear as well as constrained and unconstrained optimization problems. These classes do not only differ in their definition, but also in their solvability. The more specific requirements for an optimization class are, the easier it is usually to solve.

2.1 The general optimization problem

The standard form of a *mathematical optimization problem* or just *optimization problem* consists of an *optimization variable* $x = (x_1, ..., x_n)$ and an *objective function* $f_0 : \mathbb{R}^n \mapsto \mathbb{R}$. Furthermore there are *inequality constraint functions* $f_i : \mathbb{R}^n \mapsto \mathbb{R}$ and *equality constraint functions* $h_i : \mathbb{R}^n \mapsto \mathbb{R}$, which constrain the solution.

[1]The definition of convex optimization problems and convexity itself can be found in Section 2.3

doi: 10.2313/NET-2011-07-2_20

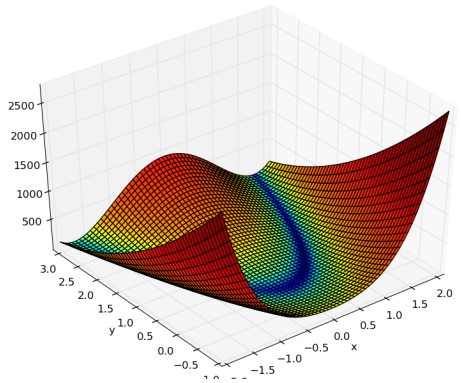


Figure 1: The non-convex Rosenbrock function $f(x, y) = (1 - x)^2 + 100(y - x^2)^2$.

The standard form of the problem is:

$$\begin{array}{ll} \text{minimize} & f_0(x) \\ \text{subject to} & f_i(x) \leq 0, \quad i = 1, ..., m \\ & h_i(x) = 0, \quad i = 1, ..., p \end{array}$$

The problem is to find x such that the *objective function* f_0 is minimized while satisfying the inequality and equality constraints. If the problem has no constraints, it is called *unconstrained*.

The set which the objective and constraint functions are defined for is called the *domain* and is defined as:

$$\mathbb{D} = \bigcap_{i=0}^{m} \mathbf{dom} f_i \cap \bigcap_{i=0}^{p} \mathbf{dom} h_i$$

A point $x \in \mathbb{D}$ is *feasible* if it satisfies the constraints. The problem itself is feasible if there exists at least one feasible point. All feasible points form the *feasible set* or *constraint set*.

A vector $x^\star = (x_1, ..., x_n)$ which is feasible and minimizes the objective function is called *optimal* or *solution*. Its corresponding value is called *optimal value* $p^\star$ and is defined as:

$$\inf\{f_0(x) | f_i(x) \leq 0, i = 1, ..., m \wedge h_j(x) = 0, j = 1, ..., p\}$$

By definition $p^\star$ can be $\pm\infty$. $p^\star$ is $+\infty$ if the problem is infeasible and $-\infty$ if the problem is *unbounded below*, that means that there are feasible points x_k with $f_0(x_k) \to -\infty$ for $k \to \infty$.

The other problem classes are subclasses of the general optimization problem. The main difference is the class of the objective and constraint functions. Figure 1 shows the Rosenbrock function.[2] It is a non-convex function, which is used as performance test for optimization algorithms for non-convex problems.

[2]The plot bases on a script from [1]

2.2 The linear optimization problem

The problem is called a *linear program*, if the objective function f_0 and the inequality and equality constraints $f_1, ..., f_m$, $h_1, ..., h_p$ are linear, that means that they fullfill the following equation for all $x, y \in \mathbb{R}^n$ and $\alpha, \beta \in \mathbb{R}$:

$$f_i(\alpha x + \beta y) = \alpha f_i(x) + \beta f_i(y)$$

One example for a two dimensional linear function is shown in Figure 2.

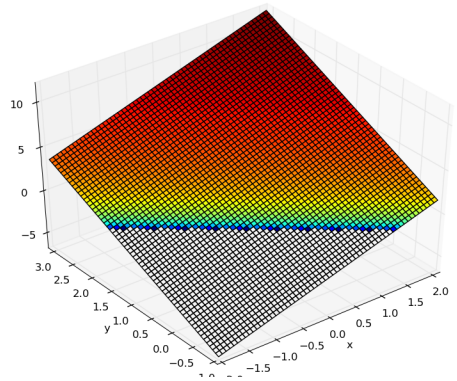


Figure 2: A linear function $f(x, y) = 3x + 2.5y$.

A linear program can also be written as:

$$\begin{array}{ll} \text{minimize} & c^T x + d \\ \text{subject to} & Gx \preceq q \\ & Ax = b \end{array}$$

The matrices $G \in \mathbb{R}^{m \times n}$ and $A \in \mathbb{R}^{p \times n}$ specify the linear inequality and equality constraints and the vectors c and $d \in \mathbb{R}^n$ parameterize the objective function. The vector d can be left out, as it does not influence the feasible set and the solution $x^\star$ (see [5], p. 146). Therefore the vector d is ignored in other definitions.

As the negation of a linear function $-f(x)$ is also linear, a linear maximization problem can be easily transformed to a linear minimization problem. For example, if the objective function $c^T x + d$ should be maximized, one can solve the problem by minimizing the objective function $-c^T x - d$. That is the reason why linear maximization problems are also linear programs.

If at least one constraint or the objective function is not linear, then the problem is called a *non-linear program*.

2.3 The convex optimization problem

The requirement for convex optimization problems is that the equality constraints are still linear but the inequality constraints and the objective function have to be convex, that means they must fulfill the following inequality for all $x, y \in \mathbb{R}^n$ and $\alpha, \beta \in \mathbb{R}$, with $\alpha + \beta = 0, \alpha, \beta \geq 0$:

$$f_i(\alpha x + \beta y) \leq \alpha f_i(x) + \beta f_i(y)$$

As one can see, this requirement is less restrictive as the previous requirement for linear programs, where equality is required. Consequently the linear programs can be seen as

doi: 10.2313/NET-2011-07-2_20

a subclass of the convex optimization problems and the theory of convex optimization can be also applied to linear programs.

Figure 3 illustrates a convex function. The intuitive characteristics of such functions is that if one connects two points, the inner line segment always lies above the graph.

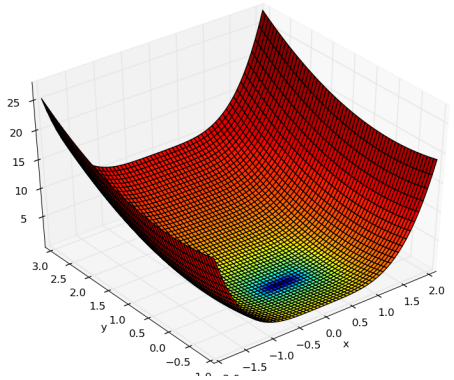


Figure 3: The convex function $f(x, y) = x^4 + y^2$.

3. THE LAGRANGE DUAL PROBLEM

Optimization problems can be transformed to their dual problems, called Lagrange dual problems, which help to solve the main problem. First, with the dual problem one can determine lower bounds for the optimal value of the original problem. Second, under certain conditions, the solutions of both problems are equal. In this case the dual problem often offers an easier and analytical way to the solution.

3.1 Lagrangian function

Let us take the general optimization problem of the standard form, of which we do not know anything about the convexity or linearity of the constraint or objective functions:

$$\begin{array}{ll} \text{minimize} & f_0(x) \\ \text{subject to} & f_i(x) \leq b_i, \quad i = 1, ..., m \\ & h_i(x) = 0, \quad i = 1, ..., p \end{array}$$

We define the *Lagrangian* $L : \mathbb{R}^n \times \mathbb{R}^m \times \mathbb{R}^p \mapsto \mathbb{R}$ of the problem as sum of the objective function and a weighted sum of the constraint functions:

$$L(x, \lambda, \nu) = f_0(x) + \sum_{i=1}^{m} \lambda_i f_i(x) + \sum_{i=1}^{p} \nu_i h_i(x)$$

The domain of the dual problem is equal to the domain of the primal problem times the domain of the parameters:

$$\mathbf{dom}\, L = \mathbb{D} \times \mathbb{R}^m_{0,+} \times \mathbb{R}^p$$

λ_i is called the *Lagrange multiplier* of the i-th inequality constraint $f_i(x) \leq 0$ and accordingly ν_i is called the *Lagrange multiplier* of the i-th equality constraint $h_i(x) = 0$. The vectors λ and ν are referred to as the *dual variables* or *Lagrange multiplier vectors*.

In addition to that, the *Lagrange dual function* (or just *dual function*) $g : \mathbb{R}^m \times \mathbb{R}^p \mapsto \mathbb{R}_{0,+}$ is the infimum of the Lagrangian over x (for all $\lambda \in \mathbb{R}^m$,$\nu \in \mathbb{R}^p$)

$$g(\lambda, \nu) = \inf_{x \in \mathbb{D}} L(x, \lambda, \nu)$$

If there is no lower bound of the Lagrangian, its dual function takes on the value $-\infty$. The main advantage of the Lagrangian dual function is, that it is concave even if the problem is not convex. The reason for this is that the dual function is the pointwise infimum of a family of linear functions of (λ, ν) (see [5], p. 216).

The basic idea behind Lagrangian duality is to take the constraints and put them into the objective function. The most intuitive way would be to rewrite the problem as the following unconstrained problem:

$$\text{minimize } l(x) = f_0(x) + \sum_{i=1}^{m} I_-(f_i(x)) + \sum_{i=1}^{p} I_0(h_i(x))$$

Here I_- and I_0 ($\mathbb{R} \mapsto \mathbb{R}$) are the indicator functions of nonpositive reals and 0 respectively:

$$I_-(u) = \begin{cases} 0 & u \leq 0 \\ \infty & u > 0 \end{cases} \qquad I_0(u) = \begin{cases} 0 & u = 0 \\ \infty & u \neq 0 \end{cases}$$

These indicator functions express our displeasure with previously infeasible points. If a point was previously infeasible, that means at least one constraint was violated, then at least one indicator function takes the value ∞ and prohibits that point from being a solution. However, this method is really brutal and causes discontinuity at the edges of the feasible set. This discontinuity is not desired as we want to use analytical techniques to solve the problem. So it is advisable to find another solution which offers a smoother transition.

In Lagrangian duality, these indicator functions are replaced by linear functions which approximate the hard indicator functions. Concretely, $I_-(u)$ is replaced by $\lambda_i u$ ($\lambda_i \geq 0$) and $I_0(u)$ is replaced by $\nu_i u$ (here the domain of ν_i is not restricted). When the inequality constraint $f_i(x)$ is 0 then our displeasure is 0. However, when the inequality constraint is greater than zero, our displeasure is finite, but depends on "how" much the constraint is violated (remind $\lambda_i \geq 0$). On the other side, our pleasure grows when the constraint is "more" fulfilled, i.e. it has more margin.

Clearly this approximation is rather poor, but it is ensured that the linear functions underestimate the indicator functions since $\lambda_i u \leq I_-(u)$ and $\nu_i u \leq I_0(u)$ for all $u \in \mathbb{R}$. As a result, the dual function is always a lower bound for the optimal value of the original function, i.e. for any $\lambda \succeq 0$ and any ν holds:

$$g(\lambda, \nu) \leq p^\star$$

This can be easily proven. Let $\tilde{x}$ be a feasible point, then $f_i(\tilde{x}) \leq 0$ and $h_i(\tilde{x}) = 0$. Consequently:

$$\sum_{i=1}^{m} \lambda_i f_i(\tilde{x}) + \sum_{i=1}^{p} \nu_i h_i(\tilde{x}) \leq 0$$

As a result the inequality follows:

$$g(\lambda, \nu) = \inf_{x \in \mathbb{D}} L(x, \lambda, \nu) \leq L(\tilde{x}, \lambda, \nu) \leq f_0(\tilde{x})$$

doi: 10.2313/NET-2011-07-2_20

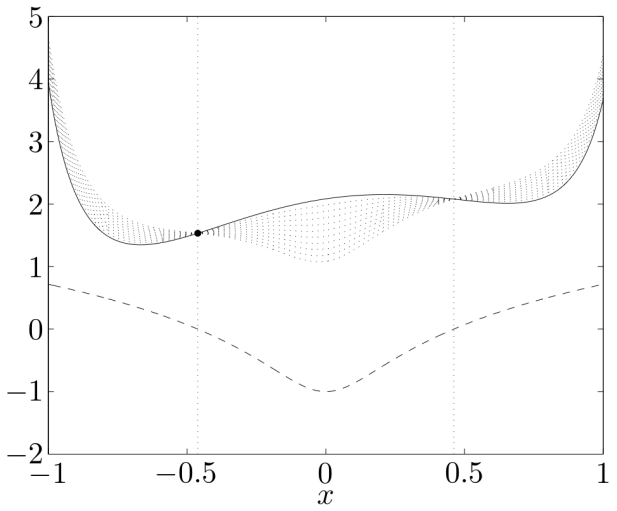


Figure 4: Illustration of the lower bound (from [5], p. 217)

Figure 4 illustrates this. The solid curve represents the objective function f_0 and the dashed curve shows the constraint function f_1. The feasible set is characterized by $f_1(x) \leq 0$ and here it is the interval $[-0.46, 0.46]$, which is indicated by the two dotted vertical lines. The circle shows the optimal point $(x^\star, p^\star) = (-0.46, 1, 54)$ and the dotted curves show $L(x, \lambda)$ for $\lambda = 0.1, 0.2, ..., 1.0$. As we see, $L(x, \lambda) \leq f_0(x)$ holds for the feasible set and $\lambda \geq 0$. Consequently, each minimum value of $L(x, \lambda)$ is less or equal to $p^\star$.

However, when $g(\lambda, \nu) = -\infty$ then the inequality is useless. The lower bound for $p^\star$ only makes sense if $\lambda \geq 0$ and $(\lambda, \nu) \in \mathbf{dom}\, g$, which means $g(\lambda, \nu) > -\infty$. We call such a pair (λ, ν) *dual feasible*.

The challenge is to find the best lower bound, which leads to the following optimization problem, called the *Lagrangian dual problem* (whereas the original problem is often referred to as *primal problem*):

$$\begin{array}{ll} \text{maximize} & g(\lambda, \nu) \\ \text{subject to} & \lambda \succeq 0 \end{array}$$

We define $(\lambda^\star, \nu^\star)$, which is one solution to this problem, as *dual optimal* or *optimal Lagrange multipliers*. As the dual objective function is concave (even if the original problem is not) and the constraints are convex, one can solve the problem by minimizing $-g(\lambda, \nu)$, which is consequently convex. Therefore the dual problem is equivalent to a convex minimization problem.

3.2 Weak duality

After estimating the optimal value of the dual problem $d^\star$, we have by definition, the best lower bound for the optimal value of the primal problem $p^\star$, which can be found using Lagrange duality:

$$d^\star \leq p^\star$$

This inequality also applies if the original problem is not convex and is called *weak duality*.

It also holds when $p^\star$ and $d^\star$ are infinite. If the original problem is unbounded below, this means $p^\star = -\infty$, then the optimal value of the Lagrange dual problem $d^\star$ is consequently also $-\infty$ and the dual problem is *infeasible*. Whereas when the dual problem is unbounded above, this means $d^\star = \infty$, then $p^\star = \infty$ and the primal problem is *infeasible*.

The difference $p^\star - d^\star$ is an important value as it characterizes the gap between the optimal value of the primal problem and its best lower bound. Accordingly it is called the *duality gap* and as a result of the previous inequality it is always non-negative.

Although the weak duality does not enable us to find the exact solution of the primal problem, it is useful in practice. The main advantage is that the dual problem is a concave maximization problem and therefore one can efficiently calculate a lower bound, as it can be easily transformed to a convex minimization problem. (see [5], p.226).

In [5] this is demonstrated by the two-way partitioning problem. Given a set of n elements, the task is to find a partition which minimizes costs. The costs are specified by a matrix W. If two elements i and j are in one partition, then they cause the cost $w_{i,j}$ and, if they are in different partitions, they cause the cost $-w_{i,j}$.

The problem can be described as a non-convex problem:

$$\begin{array}{lll} \text{minimize} & x^T W x & \\ \text{subject to} & x_i^2 = 1 & i = 1, ..., n \end{array}$$

The components x_i of the vector $x \in \mathbb{R}^n$ are restricted to -1 and $+1$ by the equality constraint and define whether the object i is in partition 1 or 2. The matrix $W \in \mathbb{R}^{n \times n}$ specifies the corresponding costs as stated before, and consequently $x^T W x$ produces the total costs. This problem is hard to solve, as the complexity rises exponentially with n.

Fortunately it can be transformed to a dual problem:

$$\begin{array}{ll} \text{maximize} & -1^T \nu \\ \text{subject to} & W + \mathbf{diag}(\nu) \succeq 0 \end{array}$$

diag creates a $n \times n$ matrix with the components of the vector on the diagonal. For a more detailed description of the derivation of the dual problem see [5], p. 219f.

This problem can be solved efficiently by semidefinite programming and delivers a useful lower bound for the hard primal problem.

3.3 Strong duality

Strong duality is even more useful. By definition, *strong duality* means that the duality gap is zero, i.e. that the optimal value of the dual problem is equal to the optimal value of the primal problem:

$$d^\star = p^\star$$

Whereas weak duality always holds, strong duality only holds

doi: 10.2313/NET-2011-07-2_20

under certain conditions. For convex problems, strong duality is mostly achieved. But to be precise, convex problems must also satisfy other conditions which are called *constraint qualifications*.

Slater's constraint qualification

One very simple and widespread example for a constraint qualification is *Slater's condition*:

$$\exists x \in \mathbf{relint}\,\mathbb{D} : \forall i = 1, ..., m : f_i(x) < 0 \wedge Ax = b$$

This means, if one can find a point which is *strictly feasible* and the problem is convex, then strong duality applies. For clearness, $\mathbf{relint}\,\mathbb{D}$ denotes the relative interior of $\mathbb{D}$, which means intuitively all interior points of the set and not the points on the edge.

For convex problems with linear inequality constraints, there also exists a *refined Slater's condition*. Given the first k constraint functions are linear, then strong duality also applies under the following condition:

$$\exists x \in \mathbf{relint}\mathbb{D} : Ax = b \wedge$$
$$\forall i = 1, ..., k : f_i(x) \leq 0 \wedge \forall i = k, ..., m : f_i(x) < 0$$

This means, strict inequality is only required for nonlinear constraint functions. As a result, the refined Slater's condition reduces to feasibility if all equality and inequality constraints are linear and the domain of the objective function f_0 is open. (See [5], p. 227)

In addition to that, Slater's condition also implies that not only strong duality holds for convex problems, but also guarantees that the dual optimal value is attained if $d^\star > -\infty$, i.e. that there exists a dual feasible point $(\lambda^\star, \nu^\star)$ with $g(\lambda^\star, \nu^\star) = d^\star = p^\star$ (See [5], p.227; [4] p.90 "dual attainment theorem")

In practice, real problems usually fulfill Slater's condition. In engineering for example, given an inequality constraint which limits the force usually satisfies Slater's condition. If Slater's condition would not apply, then this would imply, for example for the inequality constraint $F < 100$, that it is possible to have a force which is 99,9999 Newton, but it is impossible to have a force that is 100 Newton. This differentiation usually does not make sense in practice.

For a proof that Slater's condition implies strong duality see [5], §5.3.2 p.234ff

4. OPTIMALITY CONDITIONS

One motivation of the Lagrangian duality was that it provides a theoretical anchor which helps solving the problem. Above all, optimality conditions are often used to determine the solution of the primal problem by solving the dual problem analytically. As an example, the complementary slackness condition is now presented, which will be later used to solve the constrained least-square problem. Furthermore the more powerful but also more complex Karush-Kuhn-Tucker conditions are described[3] and will be used to derive the water-filling method used in information theory or the convex quadratic minimization problem.

[3]which also contain the complementary slackness condition

4.1 Complementary slackness

The *complementary slackness* condition is an optimality condition. That means, an optimal value must satisfy this condition if strong duality holds.

If $x^\star$ is the primal optimal and $(\lambda^\star, \nu^\star)$ the dual optimal, then we can state:

$$\begin{aligned} f_0(x^\star) &= g(\lambda^\star, \nu^\star) && (1)\\ &= \inf_x \left(f_0(x) + \sum_{i=1}^{m} \lambda_i^\star f_i(x) + \sum_{i=1}^{p} \nu_i^\star h_i(x) \right) && (2)\\ &\leq f_0(x^\star) + \sum_{i=1}^{m} \lambda_i^\star f_i(x^\star) + \sum_{i=1}^{p} \nu_i^\star h_i(x^\star) && (3)\\ &\leq f_0(x^\star) && (4) \end{aligned}$$

The first line results from strong duality. The second line is the definition of the dual function and the third line holds, since the infimum of the dual function over x is less or equal to its value at $x = x^\star$. As $x^\star$ is feasible, $f_i(x^\star) \leq 0$ holds for $i = 1, ..., m$ and $h_i(x^\star) = 0$ holds for $i = 1, ..., p$. In addition to that, λ_i is always non-negative and consequently the final inequality follows.

As a result, $x^\star$ minimizes $L(x, \lambda^\star, \nu^\star)$. However it does not have to be the only minimizer. The Lagrangian $L(x, \lambda^\star, \nu^\star)$ can also have other minimizers (see [5], p. 243).

Second, we can conclude:

$$\sum_{i=1}^{m} \lambda_i f_i(x^\star) = 0$$

And since each summand in this sum is non-positive, it follows:

$$\lambda_i f_i(x^\star) = 0 \qquad \forall i = 1, ..., m$$

This condition is called the *complementary slackness* condition. It states that if the i-th inequality constraint is not *active*, that means $f(x) < 0$, then λ_i must be 0. On the other hand, if $\lambda_i > 0$ then the i-th inequality constraint must be active ($f_i(x) = 0$).

$$\begin{aligned} \lambda_i^\star > 0 \quad &\Rightarrow \quad f_i(x^\star) = 0\\ f_i(x^\star) < 0 \quad &\Rightarrow \quad \lambda_i^\star = 0 \end{aligned}$$

But, to emphasize it, this requires strong duality.

4.2 Karush-Kuhn-Tucker conditions

The complementary slackness condition is part of the more comprehensive Karush-Kuhn-Tucker optimality conditions. They also require strong duality, but also differentiability of the constraint and objective functions, $f_0, ..., f_m$ and $h_1, ..., h_p$. In return, the Karush-Kuhn-Tucker conditions are more powerful compared to the complementary slackness condition. In addition to that, for convex problems, they are even sufficient and not only necessary.

4.2.1 Non-convex problems

At first we consider nonconvex problems. Let $x^\star$ and $(\lambda^\star, \nu^\star)$ again be the primal and dual optimal points. In order that $x^\star$ minimizes the Lagrangian $L(x, \lambda^\star, \nu^\star)$ its gradient

doi: 10.2313/NET-2011-07-2_20

$\nabla L(x, \lambda^\star, \nu^\star)$ must vanish. This condition is called *stationarity*:

$$\nabla f_0(x^\star) + \sum_{i=1}^{m} \lambda_i^\star \nabla f_i(x^\star) + \sum_{i=1}^{p} \nu_i^\star \nabla h_i(x^\star) = 0$$

When summarizing all conditions for the optimal point, we have collected so far, we get:

$$\begin{aligned}
\text{Primal feasibility:} \quad & \forall i = 1, ..., m: & f_i(x^\star) \leq 0 \quad (1)\\
& \forall i = 1, ..., p: & h_i(x^\star) = 0 \quad (2)\\
\text{Dual feasibility:} \quad & \forall i = 1, ..., m: & \lambda_i^\star \geq 0 \quad (3)\\
\text{Compl. slackness:} \quad & \forall i = 1, ..., m: & \lambda_i^\star f_i(x^\star) = 0 \quad (4)
\end{aligned}$$

Stationarity:

$$\nabla f_0(x^\star) + \sum_{i=1}^{m} \lambda_i^\star \nabla f_i(x^\star) + \sum_{i=1}^{p} \nu_i^\star \nabla h_i(x^\star) = 0 \quad (5)$$

These conditions are called the *Karush-Kuhn-Tucker (KKT)* conditions. Given a problem with differentiable constraint and objective function for which strong duality holds, any pair of primal and dual optimal points must fulfill these conditions. However the KKT conditions are not sufficient for non-convex problems.

4.2.2 Convex problems

For convex problems the KKT-conditions are the same, but they are now also sufficient. That means, given a pair of a primal and dual solution $(\tilde{x}, (\tilde{\lambda}, \tilde{\nu}))$, we can not only check whether this pair is not primal and dual optimal, but we can also check if it is.

Clearly, this means if the inequality constraint and objective functions $f_0, ..., f_m$ are convex and the equality constraint functions $h_1, ..., h_p$ are linear, and the KKT conditions are satisfied by some points $\tilde{x}$ and $(\tilde{\lambda}, \tilde{\nu})$, then these points are consequently primal and dual optimal points.

Furthermore, if the KKT conditions are satisfied, it implies that the duality gap is zero. The first two KKT conditions (1, 2) state that $\tilde{x}$ is primal feasible. The third condition (3) ensures that the Lagrangian $L(x, \tilde{\lambda}, \tilde{\nu})$ is convex in x, as it consists of a positive sum of convex functions. And as a result of the last condition (5) and the convexity of the Lagrangian, $\tilde{x}$ minimizes $L(x, \tilde{\lambda}, \tilde{\nu})$ over x. Thus:

$$\begin{aligned}
g(\tilde{\lambda}, \tilde{\nu}) &= L(\tilde{x}, \tilde{\lambda}, \tilde{\nu})\\
&= f_0(\tilde{x}) + \sum_{i=1}^{m} \tilde{\lambda}_i f_i(\tilde{x}) + \sum_{i=1}^{p} \tilde{\nu}_i h_i(\tilde{x})\\
&= f_0(\tilde{x})
\end{aligned}$$

The last line results from condition (3) and (4) and thus the duality gap is zero: $p^\star - d^\star = f_0(\tilde{x}) - g(\tilde{\lambda}, \tilde{\nu}) = 0$.

Although we don't need Slater's condition here to prove that the duality gap is zero, we need it for the sufficiency of the optimality criteria. The KKT-conditions depend on the existence of a pair of primal and dual optimal values. However, it is possible, that the primal problem has a primal optimum but the dual problem does not. Consequently, the KKT conditions are useless for finding the primal optimal value, as no pair of primal and dual optimal values can be found and we cannot conclude from a non-existing pair to a non-existing primal optimal. Therefore the KKT conditions alone are not sufficient for determining the primal optimum.

Here Slater's condition helps. When the problem satisfies Slater's condition, then the corresponding dual optimum is always attained. As a result, the existence of a primal optimum requires the existence of a corresponding dual optimum and vice versa. That means, that x is an optimal value of the primal problem only if there exists an (λ, ν) that fulfills the KKT conditions. Then the KKT conditions are necessary and sufficient for optimality (see [5], p.244).

The KKT conditions play an important role in convex optimization. On the one hand, they can be used to solve the problem analytically in special cases, as shown in the example of the derivation of the water filling method. On the other hand, many algorithms solving convex problems are based on the KKT conditions (see [5], p.244).

5. SOLVING THE PRIMAL BY THE DUAL

In this section, we use the optimality criteria to solve optimization problems by considering the dual.

5.1 Equality constrained convex quadratic minimization

At first, let us consider a very simple problem. The task is to minimize a convex quadratic function subject to a set of linear equality constraints (example from [5], p. 244)

$$\begin{array}{ll}
\text{minimize} & f_0(x) = \frac{1}{2} x^T P x + q^T x + r \qquad (P \in \mathbb{S}_+^n)\\
\text{subject to} & Ax = b \text{ (equal to: } Ax - b = 0)
\end{array}$$

Here the objective function is a n-dimensional quadratic function with the parameters q and P, which is a symmetric positive definite $n \times n$ matrix. It is subject to a number of linear equality constraints.

As the problem is convex and there are only linear equality constraints, Slater's condition applies.[4] Therefore we can use the KKT conditions to easily determine the solution of this problem. At first we have to satisfy the equality constraint:

$$Ax = b \quad (1)$$

Second the gradient of the Lagrangian must vanish at the optimum:

$$\begin{aligned}
L(x, \lambda, \nu) &= f_0(x) + \sum_{i=1}^{p} \nu_i h_i(x) \quad (2)\\
&= \frac{1}{2} x^T P x + q^T x + r + \nu^T (Ax - b) \quad (3)\\
\nabla L(x^\star, \lambda^\star, \nu^\star) &= \frac{\partial L}{\partial x^T} = Px^\star + q + A\nu^\star \stackrel{!}{=} 0 \quad (4)
\end{aligned}$$

As a result of 1 and 4, we get the following system of linear equations:

$$\begin{bmatrix} P & A^T \\ A & 0 \end{bmatrix} \cdot \begin{bmatrix} x^\star \\ \nu^\star \end{bmatrix} = \begin{bmatrix} -q \\ b \end{bmatrix}$$

[4] We assume that the problem is feasible

doi: 10.2313/NET-2011-07-2_20

The solution to this set of $n+m$ equations provides us the optimal primal and dual variables.

5.2 Constrained least squares problem

We consider the problem of finding a linear function $f(x) = mx + t$, which approximates the best a given set of points (x_i, y_i). Best in this case means that the sum of the squares of errors has to be minimized. Furthermore, we consider the constraint $t \leq 0$.

Figure 5 shows a random example of such a constrained least-square problem. The black circles represent the data samples which have to be approximated by a linear function. Without the constraint the solution would be the red function. However, our application domain requires $t \leq 0$, so that this cannot be a solution. The solution to the constraint problem is the blue dashed function.

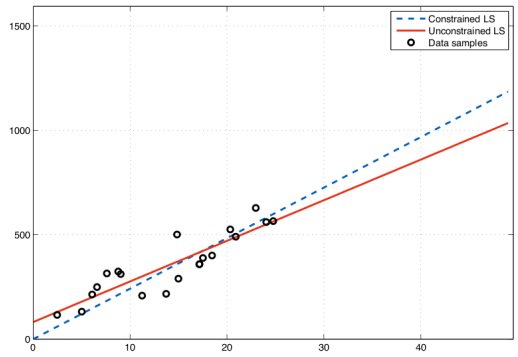


Figure 5: A random constrained least square example.

We can describe the problem with the standard form:

$$\begin{array}{ll} \text{minimize} & f_0(x) = ||Ax - d||_2^2 \\ \text{subject to} & g^T x \leq 0, \qquad g = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \end{array}$$

$$A = \begin{bmatrix} x_1 & 1 \\ x_2 & 1 \\ \vdots & \vdots \\ x_n & 1 \end{bmatrix} \qquad d = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} \qquad x = \begin{bmatrix} m \\ t \end{bmatrix}$$

The parameters m, t of the linear function are the optimization variables. They have to be determined such that the objective function is minimized. The objective function represents the sum of the squares of errors in the Euclidian norm. This can be easily proven:

$$Ax - d = \begin{bmatrix} x_1 & 1 \\ x_2 & 1 \\ \vdots & \vdots \\ x_n & 1 \end{bmatrix} \begin{bmatrix} m \\ t \end{bmatrix} - \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} mx_1 + t - y_1 \\ mx_2 + t - y_2 \\ \vdots \\ mx_n + t - y_n \end{bmatrix}$$

$$\begin{aligned} \Rightarrow ||Ax - d||_2^2 &= \sum_{i=1}^{n} \sqrt{(mx_i + t - y_i)^2}^2 \\ &= \sum_{i=1}^{n} (mx_i + t - y_i)^2 \end{aligned}$$

The inequality constraint $t \leq 0$ is expressed by $g^T x \preceq 0$.

For simplicity, it is advisable to replace the norm:

$$\begin{aligned} f_0(x) &= ||Ax - d||_2^2 \\ &= (Ax - d)^T (Ax - d) \\ &= x^T A^T Ax - x^T A^T d - d^T Ax + d^T d \end{aligned}$$

Let us define $B = A^T A$. B plays an important role for the solvability of the problem. If the problem is well formed, then B is invertible.

Fortunately this problem is convex. The sum of squares of errors is apparently convex and the inequality constraint is even linear. Thus Slater's condition is fulfilled and strong duality holds. Therefore it is a good choice to consider the dual function to solve the problem.

The Lagrangian of this problem is:

$$L(x, \lambda) = f(x) - \lambda g^T x$$

As the problem is convex and meets Slater's condition, the KKT conditions apply and we can determine the infimum of the Lagrangian over x by setting its gradient to 0:

$$\begin{aligned} g(x, \lambda) &= \inf_x L(x, \lambda) \\ \Longleftrightarrow &\nabla L(x, \lambda) = \frac{\partial L}{\partial x^T} = 2Bx - 2A^T d - \lambda g \stackrel{!}{=} 0 \\ \Longleftrightarrow &x = B^{-1} \left(A^T d + \frac{1}{2} \lambda g \right) \end{aligned}$$

This result can now be inserted into the dual function, which leads to the dual problem:

$$\begin{array}{ll} \text{maximize} & g(\lambda) \\ \text{subject to} & \lambda \geq 0 \end{array}$$

The solution can be obtained by solving this problem and maximizing the objective function. However, this is not advisable as it leads to cumbersome calculations. An easier approach is to consider optimality conditions. Because of strong duality, we can use the complementary slackness constraint:

$$\lambda^\star > 0 \Rightarrow g^T x^\star = 0$$

If $g^T x^\star < 0$ holds, then the inequality constraint $t \leq 0$ is inactive ($\lambda^\star = 0$), that means it does not determine the solution. Consequently the problem reduces to an unconstrained least squares problem. The second case is that $\lambda^\star > 0$ applies, that means that the constraint is active and determines the solution. Then you can determine λ since $g^T x^\star$ must be 0:

$$\begin{aligned} g^T x^\star = g^T B^{-1} \left(A^T d + \frac{1}{2} \lambda g \right) &\stackrel{!}{=} 0 \\ \Rightarrow \lambda = -2 \frac{g^T B^{-1} A^T d}{g^T B^{-1} g} & \end{aligned}$$

doi: 10.2313/NET-2011-07-2_20

Now one can obtain the solution of the constrained problem by determining x by the use of λ.

To put it all in a nutshell, here is the complete solution:

$$x = (A^T A)^{-1}(A^T d + \frac{1}{2}\lambda g),$$
$$\text{with } \lambda = \begin{cases} -2\frac{g^T B^{-1} A^T d}{g^T B^{-1} g} & \text{if } g^T x \leq 0 \, active \\ 0 & otherwise \end{cases}$$

Whether the constraint is active or inactive depends on the problem. By determining the solution of the unconstrained problem ($\lambda = 0$), one can easily check if $t \leq 0$. If this is the case, then the problem is solved. Otherwise the solution of the constrained problem with the active inequality constraint has to be calculated.

5.3 Water-filling

Let us consider a practical problem from information theory. It's about capacity optimization in multiple-input and multiple-output (MIMO) communication systems. These systems are characterized by the use of multiple antennas on the transmitter and receiver side to improve performance. A common problem is to allocate the power available to the transmitter, so that the overall throughput is maximized. For a detailed description see [10].

Allocating power to a transmitter increases its throughput, as it increases its signal-to-noise ratio. However, it depends on the specific transmitter and its damping how useful an allocation is. According to [11] when allocating the power x_i to the channel i of the n communication channels, the mutual information transmitted by the MIMO system can be calculated as followed:[5]

$$I = \sum_{i=1}^{n} \log_2(1 + \frac{x_i}{\varrho^2}\lambda_i)$$

Here ϱ^2 is the mean-square error of the noise and x_i is the power assigned. Furthermore λ_i describes the damping and its value is between 0 and 1. The formula can be derived from Shannon.

For simplicity we rewrite the formula for the information throughput.

$$\begin{aligned} I &= \sum_{i=1}^{n} \log_2 \left(1 + \frac{x_i}{\varrho^2}\lambda_i\right) \\ &= \sum_{i=1}^{n} \log_2 \left(\frac{1}{\varrho^2 \frac{1}{\lambda_i}} \left(\frac{\varrho^2}{\lambda_i} + x_i\right)\right) \\ &= \sum_{i=1}^{n} \left(\log_2 \left(\frac{\varrho^2}{\lambda_i} + x_i\right) - \log_2 \left(\varrho^2 \frac{1}{\lambda_i}\right)\right) \\ &= \sum_{i=1}^{n} \left(\log_2 \left(\frac{\varrho^2}{\lambda_i} + x_i\right)\right) - \sum_{i=1}^{n} \left(\log_2 \left(\varrho^2 \frac{1}{\lambda_i}\right)\right) \\ &= \sum_{i=1}^{n} \left(\log_2 \left(\alpha_i + x_i\right)\right) - c \end{aligned}$$

[5]We assume that there is no interference between channels

Now we can derive a simple optimization problem. Given a set of n communication channels, we want to allocate power to these communication channels in order to maximize the total communication rate. We define x_i as the transmitter power allocated to the i-th communication channel. Its resulting communication rate is $log_2(\alpha_i + x_i)$. Note that α_i is always positive. Furthermore we limit the total amount of power by 1, i.e. 100%. As the objective function $\sum_{i=1}^{n} \log_2(\alpha_i + x_i)$ is concave, we can transform this problem to a convex minimization problem by taking the negation of the objective function (see [5], p.254):

$$\begin{array}{ll} \text{minimize} & -\sum_{i=1}^{n} log_2(\alpha_i + x_i) \\ \text{subject to} & x \succeq 0, \qquad 1^T x = 1 \end{array}$$

As we have to derive the objective function later, we replace the dual logarithm by the natural logarithm.

$$\begin{aligned} f_0(x) &= -\sum_{i=1}^{n} \log_2(\alpha_i + x_i) \\ &= -\sum_{i=1}^{n} \frac{\ln(\alpha_i + x_i)}{\ln(2)} \\ &= -\frac{1}{\ln(2)} \sum_{i=1}^{n} \ln(\alpha_i + x_i) \end{aligned}$$

A positive factor in front of the objective function doesn't change its solution and convexity. Therefore we leave it out and consider the following problem.

$$\begin{array}{ll} \text{minimize} & -\sum_{i=1}^{n} \ln(\alpha_i + x_i) \\ \text{subject to} & x \succeq 0, \qquad 1^T x = 1 \end{array}$$

Apparently this problem satisfies again Slater's condition. Therefore we can again use the KKT conditions to determine the solution. First we have to determine the Lagrangian:[6]

$$L(x, \lambda, \nu) = -\sum_{i=1}^{n} \ln(\alpha_i + x_i) - \lambda^T x + \nu(1^T x - 1)$$

Then we can apply the KKT conditions to find the optimum.

$$x^\star \succeq 0, \qquad 1^T x^\star = 1, \qquad \lambda^\star \succeq 0, \qquad \lambda_i^\star x_i^\star = 0 \quad (i = 1, ..., n)$$

$$\nabla L(x^\star, \lambda^\star, \nu^\star) = \frac{\partial L}{\partial x} = 0$$

For the gradient, we get:

$$\begin{aligned} &\frac{\partial L(x, \lambda_i, \nu)}{\partial x_i} \\ &= \frac{\partial}{\partial x_i} \left(\sum_{i=1}^{n} (-\ln(\alpha_i + x_i) - \lambda_i x_i) + \nu \left(\sum_{i=1}^{n} (x_i) - 1\right)\right) \\ &\Leftrightarrow \frac{-1}{\alpha_i + x_i^\star} - \lambda_i^\star + \nu^\star = 0 \\ &\Leftrightarrow \lambda_i^\star = \nu^\star - \frac{1}{\alpha_i + x_i^\star} \end{aligned}$$

[6]Note that the minus before λ arises because the inequality constraint not a less-equal constraint. Furthermore the equality constraint is also not in the standard form. The 1 has to be taken to the other side.

doi: 10.2313/NET-2011-07-2_20

To solve these equations in order to find $x^\star$, $\lambda^\star$ and $\nu^\star$, we can start by eliminating $\lambda^\star$, which acts as slack variable.

$$x \succeq 0, \qquad 1^T x = 1,$$

$$x_i^\star \left(\nu^\star - \frac{1}{\alpha_i + x_i^\star} \right) = 0 \quad (i = 1, ..., n)$$

$$\nu^\star \geq \frac{1}{\alpha_i + x_i^\star} \quad (i = 1, ..., n)$$

Let us assume $\nu^\star < \frac{1}{\alpha_i}$, then $x_i^\star$ must be positive as a result of the last inequality. Consequently, the third condition implies $\nu^\star = \frac{1}{\alpha_i + x_i^\star}$, which leads to $x_i^\star = \frac{1}{\nu^\star} - \alpha_i$.

On the other hand, if $\nu^\star \geq \frac{1}{\alpha_i}$ holds, $x_i^\star$ cannot be positive, as this would violate the complementary slackness condition: $\nu_i^\star \geq \frac{1}{\alpha_i} > \frac{1}{\alpha_i + x_i^\star}$. Thus, $x_i^\star$ must be non-positive and, because of the first condition, this results in $x_i^\star = 0$.

All in all, we get:

$$x_i^\star = \begin{cases} \frac{1}{\nu^\star} - \alpha_i & \nu^\star < \frac{1}{\alpha_i} \\ 0 & \nu^\star \geq \frac{1}{\alpha_i} \end{cases}$$

This can be summarized to:

$$x_i^\star = \max \left\{ 0, \frac{1}{\nu^\star} - \alpha_i \right\}$$

Taking the second condition into account leads to:

$$\sum_{i=1}^{n} \max \left\{ 0, \frac{1}{\nu^\star} - \alpha_i \right\} = 1$$

The lefthand side can be interpreted as a piecewise linear increasing function of $\frac{1}{\nu^\star}$ with breakpoints at α_i. As a result the equation has a unique solution, which can be easily obtained as the function is monoton increasing.

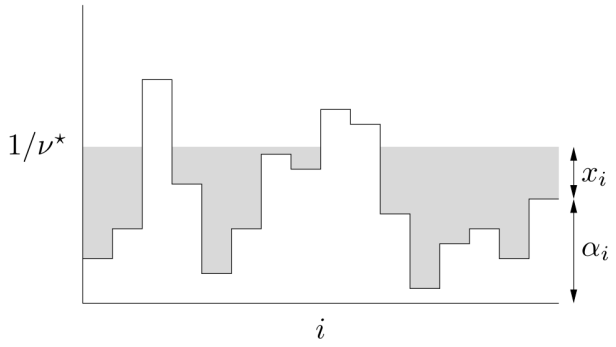


Figure 6: Illustration of the water filling algorithm. The water is shown shadowed and the patches white. (From [5], p.246)

In practice this solution method is known as *water filling* because it has an intuitive interpretation. the default transmitter power α_i of each channel is represented by the height of the patch i in figure 6. We flood the region with water to a depth of $\frac{1}{\nu^\star}$ and calculate the amount of used water: $\sum_{i=1}^{n} \max \left\{ 0, \frac{1}{\nu^\star} \right\}$. Then we increase or decrease the water level until the amount of used water is equal to 1. As a result the water level above patch i denotes the optimal value $x_i^\star$.

6. CONCLUSION

Convex optimization problems are prevalent in practice. Fortunately, many practical problems meet the requirements for strong duality. Here, the theory of Lagrangian duality offers a powerful tool to determine the exact solution of convex problems. By describing the constraints within the objective function, it enables us to tackle the problem analytically. Especially optimality conditions can be very useful for determining the solution of the primal problem, as demonstrated in the examples.

Furthermore, the theory of strong duality is in particular the basis for efficient and distributed algorithms for convex problems. As the last example shows, the insights gained from duality can be easily transformed to algorithms. Although this example was very problem specific, it is also possible to come up with more general algorithmic approaches for convex problems, for example by considering the ϵ-suboptimality (see [5], p. 241f). In addition to that, strong duality offers the opportunity for perturbation and sensitivity analysis (see [5], p. 249ff).

Besides the theory of strong duality, Lagrangian duality has also a lot of applications. First it can be used to determine lower bounds for non-convex problems. The main advantage of this is, no matter how complex the primal problem is, the dual problem is a concave maximization problem and therefore easy to solve. So duality enables us to determine efficiently a lower bound. Furthermore it can be applied to determine feasibility of a system of equalities or inequalities (see [5], p.258ff).

All in all, duality is a comprehensive theory with a lot of applications and totally worth a deeper look. For more intensive reading, I can recommend the following books: [3], [5], [9] as well as [6] and [7] cover the Lagrangian duality in detail. For a German book about optimization in general, I recommend [8]. In [2] numerous applications of convex optimizations can be found.

7. REFERENCES

[1] Rosenbrock function. Website, April 2011. http://en.wikipedia.org/w/index.php?title=Rosenbrock_function&oldid=426154114 (May 25th 2011).

[2] A. Ben-Tal and A. S. Nemirovskiaei. *Lectures on Modern Convex Optimization: Analysis, Algorithms, and Engineering Applications*. Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 2001.

[3] D. Bertsekas, A. Nedi, and A. Ozdaglar. Convex Analysis and Optimization. 2003.

[4] J. Borwein and A. Lewis. *Convex Analysis and Nonlinear Optimization: Theory and Examples*, volume 3. Springer Verlag, 2000.

[5] S. Boyd and L. Vandenberghe. *Convex Optimization*. Cambridge University Press, New York, NY, USA, 2004.

[6] J.-B. L. C. Hiriart-Urruty. *Convex Analysis and Minimization Algorithms I*. Springer, 1993.

[7] C. Hiriart-Urruty, Jean-Baptiste Lemarechal. *Convex Analysis and Minimization Algorithms II*. Springer,

doi: 10.2313/NET-2011-07-2_20

1993.

[8] F. Jarre and J. Stoer. *Optimierung*. Springer, 2003.

[9] R. T. Rockafellar. *Convex Analysis*. Princeton University Press, 1997.

[10] G. Scutari, D. P. Palomar, and S. Barbarossa. The MIMO Iterative Waterfilling Algorithm. *IEEE Transactions on Signal Processing*, 57(5):1917–1935, 2009.

[11] M. Wennström, M. Helin, A. Rydberg, and T. Öberg. On the Optimality and Performance of Transmit and Receive Space Diversity in MIMO Channels. In *IEE Technical Seminar on MIMO Communication Systems: From Concept to Implementation*, London, 2001.

doi: 10.2313/NET-2011-07-2_20

Patente: Von der Erfindung zum Patent

Thomas Grass
Betreuer: Andreas Müller, Tobias Bandh
Hauptseminar - Innovative Internettechnologien und Mobilkommunikation SS2011
Lehrstuhl Netzarchitekturen und Netzdienste, Lehrstuhl Betriebssysteme und Systemarchitektur
Fakultät für Informatik, Technische Universität München
Email: thomas.grass@in.tum.de

KURZFASSUNG

Auf der ganzen Welt stellen Patente eine wichtige Grundlage zur Sicherstellung eigener Erfindungen vor der Nachahmung Dritter dar. Nicht jede Erfindung kann als solche patentiert werden. Wichtig ist dabei, dass es sich bei der Erfindung um eine technische Erfindung handelt, die es in dieser Art und Weise noch nicht gegeben hat und auf einer erfinderischen Tätigkeit beruht.

Liegt eine solche Erfindung vor, so beginnt der eigentliche Weg zum Patent mit der Patentanmeldung und seinen einzelnen Bestandteilen, und endet nach einigen Zwischenschritten im positiven Fall mit der Erteilung des Patents vom zuständigen Patentamt. Um ein positives Resultat aus diesem mehrmonatigem Prozess zu ziehen, kommt es vor allem auf die korrekte Formulierung der Patentansprüche und auf das richtige Reagieren auf Prüfungsbescheide an.

In dieser Arbeit wird ausführlich der oft steinige Weg beschrieben, der zwischen der eigentlichen Erfindung und der Erteilung eines Patentes zu bewältigen ist.

Schlüsselworte

Patent, Erfindung, Patentgesetz, PatG, Patentansprüche

1. EINLEITUNG

In der heutigen globalisierten und modernen Welt werden jeden Tag dutzende Erfindungen getätigt, die Menschen dabei helfen sollen, durch einfachere Vorgehensweisen oder durch Hilfsprodukte effektiver und effizienter durchs Leben zu kommen. Der Erfinder selbst versucht dabei natürlich selbst Vorteile für sich zu erwirken. Die gewünschten Vorteile können hierbei sowohl materiell, also durch das Erwirtschaften von Gegenständen oder Geld, als auch immateriell, also zum Beispiel durch das Erlangen eines guten Rufes, auftreten.

Dabei ist es unvermeidlich, dass durch die Vielzahl von Menschen auf dieser Welt und durch die Anzahl der möglichen Erfinder, Erfindungen oft mehrfach (aber nicht zwangsläufig gleichzeitig), sei es aus Zufall oder Vorsatz, entwickelt werden. Jeder Erfinder oder Imitator versucht für sich einen Vorteil aus der Erfindung zu erzielen.

Aus diesem Grund gibt es das sogenannte 'Patent'. Mit einem Patent kann sich der Eigner einer Erfindung vor der vorsätzlichen oder zufälligen Nachahmung durch Dritte schützen lassen und somit selbst und privilegiert die Vorteile aus seiner Erfindung ziehen.

Da der Weg von der Erfindung zum Patent oft sehr steinig und undurchsichtig ist, wurde diese Arbeit geschrieben. Sie behandelt zunächst in Kapitel 2 die Grundbegriffe und erklärt dann in Kapitel 3 den Ablauf von der Erfindung zum Patent. In Kapitel 4 wird dann Anhand eines Beispiels aus der Informatik gezeigt, wie eine Erfindung sich konkret in der Patentschrift wiederfinden lässt.

Die Arbeit basiert auf dem deutschen Recht und den aktuell gültigen deutschen Gesetzen (10. Patentgesetz PatG). Da sich die europäischen und internationalen Gesetze im Bezug auf das Patentrecht jedoch nur gering unterscheiden, kann diese Arbeit auch als Hilfestellung im europäischen und internationalen Fall dienen.

2. GRUNDBEGRIFFE

Im folgenden Abschnitt werden zum allgemeinen Verständnis die wichtigsten zwei Begriffe, die im Rahmen der Arbeit behandelt werden, erläutert: Die Erfindung und das Patent.

2.1 Die Erfindung

Der Begriff 'Erfindung' ist heutzutage in aller Munde, und jeder würde wahrscheinlich auch von sich behaupten, dass er auch genau weiß, was dieser Begriff auch bedeutet.

Doch wenn man genauer nach der Bedeutung des Begriffs 'Erfindung' nachfragt wird man sehr schnell feststellen, dass viele versuchen werden, den Begriff 'Erfindung' mit dem Begriff 'Entdeckung' zu umschreiben.

Dass dieser oft gebrauchte Schluss jedoch falsch ist, zeigt ein Blick in das 10. Patentgesetz ('PatG'). Das PatG definiert in §1 Abs. 1 genau, was eine Erfindung im Sinne des PatG ist: 'Patente werden für Erfindungen auf allen Gebieten der Technik erteilt, sofern sie neu sind, auf einer erfinderischen Tätigkeit beruhen und gewerblich anwendbar sind.' Außerdem schließt der Gesetzgeber den Begriff der 'Entdeckung' explizit zwei Absätze danach in §1 Abs. 3 mit '[...] Als Erfindungen [...] werden insbesondere nicht angesehen: 1. Entdeckungen sowie wissenschaftliche Theorien und mathematische Methoden; [...]' aus.

Dies bedeutet, dass eine 'Entdeckung' einer Sache oder eines Problems noch keine Erfindung im Sinne des PatG darstellt. Erst die Lösung eines Problems mit Hilfe der Zusammensetzung verschiedener Materialien, oder das Verfahren der Zusammensetzung verschiedener Materialien kann als 'Erfindung' gelten.

doi: 10.2313/NET-2011-07-2_21

Dabei wird im PatG nach §9 Abs. 1-3 genau die kurz oben angesprochene Thematik behandelt: So kann eine Erfindung entweder ein 'Erzeugnis' sein oder ein 'Verfahren' zum Herstellen eines Erzeugnisses. [1]

2.2 Das Patent

Wenn man eine Erfindung gemacht hat (wie im Kapitel zuvor definiert), kann man dieses Erzeugnis oder das Verfahren gesetzlich vor Nachbauten oder Nachahmungen Dritter schützen lassen. Dabei stellt das 'Patent' neben dem 'Gebrauchsmuster' und dem 'Geschmacksmuster' die populärste Form des Rechtsschutzes dar.

Dabei muss beachtet werden, dass die 'Erfindung' selbst noch nicht reicht. Die Erfindung muss neu, im Sinne des PatG sein und wird vom Gesetzgeber im PatG §3 Abs 1. wie folgt definiert: 'Eine Erfindung gilt als neu, wenn sie nicht zum Stand der Technik gehört. Der Stand der Technik umfasst alle Kenntnisse, die vor [...] der Anmeldung [...] durch schriftliche oder mündliche Beschreibung [...] der Öffentlichkeit zugänglich gemacht wurden.'

Somit gilt der Schutz des Patentes für neue technische Erfindungen und verleihen dem Patentinhaber das räumlich und zeitlich befristete Privileg, allein über die Erfindung zu verfügen. Der Patentinhaber erhält somit mit der Anmeldung ein Exklusivrecht für die Verwertung seiner Erfindung. [2]

Eine patentierte Erfindung garantiert dem Patentinhaber, dass ausschließlich er diese Erfindung weiterentwickeln und vermarkten darf. Dies ist insbesondere daher wichtig, da das Erfinden immer ein langwieriger Prozess ist, der in den meisten Fällen sehr viel Zeit in Anspruch nimmt und daher extrem hohe Kosten verursacht.

Ein sehr gutes Beispiel für die Wichtigkeit des Patentschutzes in Bezug auf die hohen Ausgaben bei der Erfindung lässt sich in der Pharmazeutischen Industrie finden. Die Firma Eli Lilly & Company entwickelte ein bekanntes Antidepressivum mit dem Namen 'Prozac'. Dieses Medikament wurde seit Frühling 1988 verkauft und brachte dem Unternehmen in den Jahren 1988-2001 rund 21 Millarden USD Umsatz. Im Jahr 2000 konnte das Unternehmen alleine mit Prozac 2,6 Millarden USD Umsatz erzielen und war dadurch für das Unternehmen Eli Lilly & Company zu einer Art 'Cashcow' geworden.

Im Jahre 2002 erlosch der Patentschutz. Noch im gleichen Jahr entwickelten andere Hersteller eine Imitation des Produkts. Dadurch sank der Umsatz auf rund 570 Millionen USD im Jahr 2002. [3]

Die Kosten, die für Forschung und Entwicklung einer Erfindung in der pharmazeutischen Industrie anfallen, liegen bei rund 400 Millionen USD und dauern rund 10 bis 12 Jahre. Die Zeit und die Kosten fallen dabei für die Isolierung der Wirkstoffe, für klinische Tests und Tests mit Patienten an. Im Gegensatz dazu können Imitatoren das selbe Produkt nach nur 1 bis 2 Jahren und Kosten von 1 bis 2 Millionen USD auf den Markt bringen. Die Kosten fallen lediglich zum Nachweis der Bioäquivalenz an.[4]

Das war auch der Grund, weshalb die Firma Eli Lilly & Company mit ihrem Produkt nach Ablauf der Patentschutzzeit scheiterte: Sehr viele kleinere Pharmaunternehmen sahen die Chance, in kurzer Zeit eine 'Cashcow' zu züchten und nahmen diese Chance auch wahr. Am Beispiel des Antidepressivums 'Prozac' lässt sich gut abschätzen, wie hoch die Kosten für die Entwicklung sein können und wie wichtig daher auch der Schutz gegen Imitation sein kann.

Als Erfinder muss man sich aber auch immer im Klaren sein, dass das Anmelden eines Patentes auch immer gesetzliche Verpflichtungen mit sich bringt. So stimmt man mit der Patentanmeldung zu, dass eine Erfindung veröffentlicht wird. Das Patent steht somit auch anderen Erfindern zur Verfügung und kann diesen als Maßstab und Basis für Weiterentwicklungen auf dem betreffenden Gebiet dienen.[2]

Dies stellt einerseits einen Vorteil für die betreffende Technikbranche dar, andererseits öffnet man so aber auch eine Pforte zur möglichen Produktpiraterie in Ländern, in denen der Patentschutz nur teilweise oder gar nicht existiert.

Als Beispiel kann man hier einen Fall der Firma 'Doppelmayr' nennen. 'Doppelmayr' ist eine österreichische Produktionsfirma für Seilbahnen und Technologieführer im Seilbahnwesen. Bis heute hat 'Doppelmayr' mehr als 14.000 Seilbahnsysteme für Kunden in über 83 Staaten realisiert.

Um das Jahr 2005 kam ans Licht, dass zumindest zwei chinesische Firmen in über 200 Fällen die Technologie der Doppelmayr Lifte kopiert und in China an vielen Orten aufgestellt haben. Teilweise haben sich die chinesischen Firmen nicht einmal die Mühe gemacht, ein eigenes Firmenlogo anzubringen. Stattdessen wurde sogar das Doppelmayr-Logo angebracht. Dies führte auch dazu, dass sich Mitarbeiter und Betreiber der gefälschten Lifte bei der echten Firma Doppelmayr gemeldet haben, um Wartungen zu beantragen. Dadurch wurde diese großangelegte Produktpiraterie überhaupt erst bekannt. Da der Patenschutz jedoch in China nicht greift, ist Doppelmayr bis heute machtlos, und kann dem ganzen Treiben nur zuschauen.[5]

3. DER WEG ZUM PATENT

Im Kapitel 2 dieser Arbeit wurden die Begriffe 'Erfindung' und 'Patent' beschrieben. Wie der Weg von der Erfindung zum Patent aussieht, wurde noch nicht behandelt.

Ein Patent entsteht nicht automatisch mit der Anmeldung einer Erfindung bei der zuständigen Stelle (in Deutschland, das Deutsche Patent- und Markenamt (DPMA)). Eine Erfindung kann erst dann tatsächlich patentiert werden, wenn ein gesetzlich vorgeschriebenes Verfahren mit positivem Ergebnis durchlaufen wurde. Erst mit der Patenterteilung setzt das Schutz- und Verbietungsrecht ein.[2]

3.1 Die Anmeldung

Die Anmeldung einer Erfindung zum Patent erfolgt in Deutschland über das Deutsche Patent- und Markenamt (DPMA). Zunächst muss ein Antrag auf Erteilung eines Patentes gestellt werden. In den Anmeldeunterlagen muss die Erfindung so deutlich wie möglich und vollständig offenbart werden, dass ein Fachmann sie ohne weiteres nachvollziehen kann. Deshalb legt das DPMA den Erfindern nahe, folgende Bestandteile dem Antrag auf Erteilung beizufügen:

doi: 10.2313/NET-2011-07-2_21

1. Technische Beschreibung
2. Patentansprüche
3. Zeichnungen
4. Zusammenfassung
5. Erfinderbenennung

Die Bestandteile 1, 2 und 3 müssen zusammen mit der Anmeldung eingereicht werden. Die anderen Bestandteile 4 und 5 können aber auch noch innerhalb von 15 Monaten ab dem Anmeldetag nachgereicht werden. [6]

3.1.1 Technische Beschreibung

Die technische Beschreibung ist ein wesentlicher Bestandteil der Patentanmeldung und soll dem DPMA Aufschluss darüber geben wie die Erfindung heißt und zu welchem technischen Gebiet diese Erfindung gehört. Des Weiteren muss dem DPMA vorgelegt werden, wie der aktuelle Stand in diesem technischen Gebiet ist und welche Mängel in diesem Gebiet vorliegen (also die Beweggründe für die Erfindung).

Die Problemlösung ist ebenfalls Bestandteil der technischen Beschreibung. Sie muss genau beschreiben, welches technische Problem mit welchen Mitteln gelöst wurde. Das DMPA schreibt außerdem vor, dass die technische Beschreibung ein Ausführungsbeispiel der Erfindung enthält, sowie die Vorteile, die mit der Erfindung erzielt werden, aufzählt. [7]

3.1.2 Patentansprüche

Mit den Patentansprüchen wird in der Patentanmeldung der Schutzumfang des Patents festgelegt. Alle unter Schutz zu stellenden Merkmale müssen in den Ansprüchen exakt wiedergeben werden. Die richtige Formulierung der Patentansprüche ist von größter Bedeutung, da ausschließlich durch diese der Schutzgegenstand und Schutzumfang eindeutig festgelegt wird. Dabei kann man bei mehreren Patentansprüchen für eine Erfindung zwischen Anspruch und Unteranspruch unterscheiden und die Ansprüche entweder in einer zweiteiligen oder auch in einer einteiligen Fassung wiedergeben. Mindestens ein Patentanspruch ist jedoch erforderlich.[8]

Beispiel 1: 'Streuscheibe für eine Signallaterne' [9]
Zweiteilige Fassung:

1. *Streuscheibe für eine Signallaterne mit vorgegebener Lichtstärkeverteilung in der Umgebung der optischen Achse insbesondere für Eisenbahn- und/oder Straßenverkehrs Lichtsignale, dadurch gekennzeichnet, dass die Streuscheibe aus einem Halterahmen und mehreren Scheibenausschnitten, die je für sich hergestellt sind und jeweils einen bestimmten Teil der Lichtstreuung hervorrufen, zusammengesetzt ist.*
2. *Streuscheibe nach Patentanspruch 1, dadurch gekennzeichnet, dass die Streuscheibenausschnitte und der zugehörige Halterahmen mit Passstücken zum unverwechselbaren Aneinanderfügen der Scheibenausschnitte versehen sind.*

Einteilige Fassung:

1. *Streuscheibe für eine Signallaterne mit vorgegebener Lichtstärkeverteilung in der Umgebung der optischen Achse insbesondere für Eisenbahn- und/oder Straßenverkehrs Lichtsignale, wobei die Streuscheibe aus einem Halterahmen und mehreren Scheibenausschnitten, die je für sich hergestellt sind und jeweils einen bestimmten Teil der Lichtstreuung hervorrufen, zusammengesetzt ist.*
2. *Streuscheibe nach Anspruch 1, bei dem die Streuscheibenausschnitte und der zugehörige Halterahmen mit Passstücken zum unverwechselbaren Aneinanderfügen der Scheibenausschnitte versehen sind.*

Das *Beispiel 1* zeigt ein Beispiel für eine ordentliche Formulierung der Patentansprüche in einer zweiteiligen Fassung und einer einteiligen Fassung. *1.* formuliert bei beiden Fassungen den 'Anspruch', *2.* analog den Unteranspruch. Bei der einteiligen Fassung werden die Merkmale in sinnvoller Reihenfolge aneinander gereiht.

Bei der zweiteiligen Fassung werden die Merkmale entweder dem Oberbegriff oder dem Kennzeichen zugeordnet. Die Merkmale, die aus dem Stand der Technik bereits bekannt sind, kommen in den Oberbegriff, die neuen Merkmale in das Kennzeichen. Die Trennung erfolgt mit den Worten 'dadurch gekennzeichnet, dass' oder 'gekennzeichnet durch'.[8]

3.1.3 Zeichnungen

Bei Bedarf können der Beschreibung Zeichnungen beigefügt werden.[8] Die Zeichnungen sollen das Zusammenwirken der Merkmale der Erfindung klar erkennen lassen und das Wesentliche hervorheben. Fotos werden als Ersatz für Zeichnungen nicht zugelassen.[7]

3.1.4 Zusammenfassung

Die Zusammenfassung ist der Anmeldung beizufügen und ist daher nicht Bestandteil der Anmeldung. Sie dient ausschließlich der Information und hat keine rechtliche Bedeutung.[8] Die Bestandteile der Zusammenfassung beinhaltet die Bezeichnung der Erfindung, eine verständliche Kurzfassung der technischen Offenbarung und eine Zeichnung, falls diese in der Kurzfassung erwähnt wird.[7] Die Zusammenfassung muss innerhalb von 15 Monaten ab Anmeldung eingereicht werden. Wird diese nicht eingereicht, so wird die Anmeldung zurückgewiesen.[8]

3.1.5 Erfinderbenennung

Der Anmelder des Patents und der oder die Erfinder müssen nicht zwangsläufig identisch sein. Deshalb muss der Anmelder innerhalb von 15 Monaten (analog zur Zusammenfassung) nach dem Anmeldetag der Erfindung, den oder die Erfinder benennen.[7]

Aufgrund der Erfinderbenennung nennt das DPMA den oder die Erfinder in der Offenlegungsschrift und Patentschrift. Der Erfinder kann jedoch, falls gewünscht, einen Antrag auf Nichtnennung stellen, und bleibt dadurch anonym.[8]

3.2 Das Verfahren

Hat der Patentanmelder seine Anmeldung beim zuständigen Patentamt, wie zum Beispiel dem DPMA abgegeben, so startet nach Zahlung der gegebenen Anmeldegebühr das

doi: 10.2313/NET-2011-07-2_21

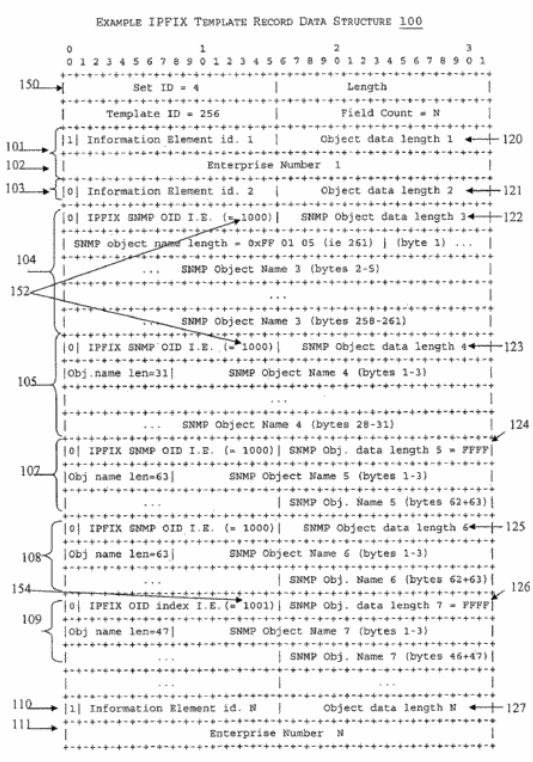


Abbildung 1: Technische Zeichnung 'IPFIX Template Record Data Structure' [10]

Prüfungsverfahren. Ab diesem Zeitpunkt hat sich der Patentanmelder den Zeitrang der Anmeldung gesichert. Im Prüfungsverfahren stellen Patentprüfer des DPMA sicher, dass die eingereichte Erfindung die folgenden Kriterien erfüllt:

1. Neuheit
2. gewerbliche Anwendbarkeit
3. erfinderische Tätigkeit

Zudem muss es sich um eine technische Erfindung handeln. [11]

3.3 Vorprüfung

Der Ablauf des Patentprüfungsverfahren startet zunächst mit einer Vorprüfung. Dabei werden die eingereichten Unterlagen auf Einhaltung der Formvorschriften und auf offensichtliche Patentierungshindernisse analysiert (auch 'Neuheit', 'gewerbliche Anwendbarkeit' und 'erfinderische Tätigkeit').[13] Außerdem wird die Erfindung nach ihrem sachlichen Gehalt in ein international geltendes Klassifikationsschema eingeordnet. [11]

3.4 Eigentliche Prüfung

Um tatsächlich ein Patent auf seine Erfindung zu erhalten, muss nach erfolgreich bestandener Vorprüfung ein Prüfungsantrag gestellt werden. Dieser ist in Deutschland mit einer Prüfungsgebühr verbunden. Erst ab diesem Zeitpunkt kann das DPMA die für die eigentliche Patenterteilung notwendige Prüfung der Anmeldung durchführen.[11]

Der Prüfungsantrag selbst muss innerhalb von 7 Jahren, ab dem Anmeldetag eingereicht werden. Ist dies nicht der Fall, so wird die Anmeldung zurückgenommen. Der Prüfungsantrag selbst läuft schriftlich ab und unterteilt sich im Normalfall in:

1. Prüfungsbescheid
2. Reaktion des Anmelders[8]

3.4.1 Prüfungsbescheid

Wurde ein Prüfungsbescheid gestellt, so wird von den Patentprüfern zunächst der für die Erfindung aktuelle relevante Stand der Technik ermittelt und überprüft, ob vor dessen Hintergrund ein Patent für den Gegenstand erteilt werden kann oder nicht.

Sollte der Patentprüfer feststellen, dass die Erfindung sowohl neu ist ('Sind alle Merkmale des Anmeldegegenstands in noch keinem Beispiel beschrieben?' [12]), auf einer erfinderischen Tätigkeit beruht ('Kommt ein Fachmann im Wissen des Stands der Technik nicht ohne Weiteres auf den Anmeldegegenstand?' [12]), gewerblich anwendbar ist, als auch die Anmeldung alle sonstigen formalen Voraussetzungen erfüllt, so erteilt er ein Patent. [11]

Wenn vom Patentprüfer Mängel in der Anmeldung oder den Erfordernissen festgestellt wurden, so wird dies von ihm in einem Prüfungsbescheid mitgeteilt. Auf den Prüfungsbescheid erfolgt dann die 'Reaktion des Anmelders'.

3.4.2 Reaktion des Anmelders

Der Anmelder kann zu den Prüfungsbescheiden Stellung nehmen, wobei er verschiedene Reaktionsmöglichkeiten hat:[8]

- keine Reaktion: sollten Mängel vorliegen wird die Anmeldung zurückgezogen
- Anmeldung zurückziehen: Die Rücknahme kann als Prozesshandlung nicht widerrufen werden
- Anmeldung teilen (gem. PatG §39): dies kann jederzeit erfolgen. Aus der ursprünglichen Anmeldung werden ein oder mehrere Teilanmeldungen.
- Anmeldung verbinden: mehrere Anmeldungen, die im selbem Verfahrenstand sind, können miteinander verbunden werden.
- Teile entfernen: Sofern vom DPMA Teile als unheitlich angesehen werden, können Teile aus der Patentanmeldung entfernt werden.
- Umformulieren: Der Anmelder ändert den Schutzgegenstand durch Umformulierung der Patentansprüche oder deren Streichung. Der Anmelder kann geänderte oder völlig neue Ansprüche einreichen. Deren Inhalt muss jedoch in den ursprünglichen Anmeldeunterlagen als Erfindung offenbart sein. Grundsätzlich ist die Änderung der Patentansprüche im Erteilungsverfahren unproblematisch, da deren Formulierung als Versuch angesehen wird, mit dem Ziel, gemeinsam mit dem DPMA eine optimale Fassung der Patentansprüche zu erreichen.
- Änderung der sonstigen Anmeldeunterlagen
- Verteidigen: Der Anmelder kann den Anmeldegegenstand auch verteigen und versuchen, das DPMA zu überzeugen, dass die im Prüfungsbescheid aufgeführten Mängel nicht vorliegen

doi: 10.2313/NET-2011-07-2_21

- Mündliche Verhandlung beantragen: Der Anmelder kann eine Anhörung beantragen (PatG §46): Das DPMA muss bei Sachdienlichkeit (eine Anhörung ist sachdienlich, wenn sie das Verfahren fördern kann) einen Antrag auf Anhörung stattgeben. In der mündlichen Verhandlung können direkt die verschiedenen Punkte des Prüfungsbescheides besprochen und an Lösungen gemeinsam gearbeitet werden.

3.5 Offenlegung

Wenn eine Erfindung beim DPMA angemeldet wurde ist diese für die ersten 18 Monate ab Anmeldung nicht für die Öffentlichkeit zugänglich. Während dieser Zeit läuft in der Regel das Prüfungsverfahren mit den im Kapitel zuvor beschriebenen Prüfungsbescheiden und Reaktionen, an denen nur der Patentanmelder selbst und die Patentprüfer beteiligt sind. Nach den 18 Monaten folgt in jedem Fall, auch bei noch nicht Fertigstellung des Patents, die Veröffentlichung der Patentanmeldung in Form einer Offenlegungsschrift. Die Offenlegungsschrift ist die schriftliche Darlegung der Erfindung, wie sie am Anmeldetag beim DPMA eingereicht worden ist.

Während der 18 Monate kann der Patentanmelder auch entscheiden, ob er seine Anmeldung weiterverfolgen möchte, oder ob er sie zurückzieht, um zum Beispiel zu Verhindern, dass Details seiner Erfindung an die Öffentlichkeit gelangen.[14]

Ziel der Offenlegung ist es, die Öffentlichkeit über den aktuellen Stand der Technik zu informieren [11] und somit zum Beispiel auch weitere Erfindungen in dem Bereich möglich zu machen, aber auch Erfinder davon abzuhalten, Energie in eine Erfindung und Patentanmeldung zu stecken, die schon erfunden wurde.

3.6 Entscheidung, Zurückweisung oder Patenterteilung

Sobald alle Formalitäten der Patentanmeldung beidseitig durchgeführt wurden und somit die Patenanmeldung entscheidungsreif ist, erlässt das DPMA einen Beschluss, durch den die Anmeldung entweder zurückgewiesen wird oder ein Patent erteilt wird.[8]

Die Erteilung erfolgt in der Regeln dann, wenn die Patentprüfung erfolgreich bestanden wurde. Dabei erfolgt analog zur Offenlegung die Bekanntmachung der Erteilung im Patentblatt und ist ab dann in den Datenbanken der DPMA oder der zuständigen Patentverwaltungsbehörde für die Öffentlichkeit recherchierbar.[11]

3.7 Einspruch

Gegen eine Patenterteilung kann sich jedermann, also zum Beispiel mögliche andere Erfinder oder Menschen die durch eine Patentanmeldung Schaden befürchten, innerhalb von drei Monaten nach Veröffentlichung der Patentschrift Einspruch einlegen.

Mit dem Einspruch hat der Einsprechende die Möglichkeit, Gründe anzuführen, die gegen eine rechtmäßige Erteilung des Patents sprechen. Im Einspruchsverfahren wird kostenpflichtig erneut geprüft, ob notwendige Voraussetzungen für die Erteilung oder Aufrechterhaltung eines Patents fehlen.

Dies geschieht in der Regel nicht durch einzelne Patentprüfer, sondern durch ein Gremium aus Mitgliedern einer Patentabteilung des DPMA. Nach der Prüfung des Einspruchs kann das Patent widerrufen, teilwiderrufen oder aufrechterhalten werden. Der Patentanmelder kann vor dem Bundespatentgericht auch gegen einen Einspruchsbeschluss Beschwerde einlegen.

Wird kein Einspruch innerhalb von drei Monaten eingelegt, so gilt das Patent als rechtskräftig und gilt ab diesem Zeitpunkt für maximal 20 Jahre.[11]

4. ERFINDUNG UND PATENT IM BEISPIEL

In den Kapiteln zuvor wurde beschrieben, was eine Erfindung und was ein Patent ist. Des weiteren wurden die einzelnen Bestandteile der Patentanmeldung gezeigt und erläutert. In diesem Kapitel wird nun anhand eines Beispieles aus dem Informatikbereich gezeigt, wie eine Erfindung als solches, sich zum Patent verhält, wie der zeitliche Ablauf der Patentanmeldung von statten geht, und wie eine Erfindung in der Patentanmeldung, beziehungsweise konkret in den Patentansprüchen wiederfindet.

Als Beispielsgrundlage dient das 'Internet Protocol Flow Information Export' (IPFIX). Das IPFIX ist ein Push-Protokoll, dass zum standardisiertem Austausch von Netzüberwachungsinformationen entwickelt wurde. Es arbeitet auf der Anwendungsschicht im TCP/IP-Protokollstapel. Entwickelt wird IPFIX von der Internet Engineering Task Force (IETF). Als Basis diente das 'Netflow'-Protokoll der Firma Cisco Systems. IETF ist ein Standardisierungsgremium für Internetstandards. Internetstandards sind Regelwerke für die technische Kommunikation im Internet. [15]

4.1 Entwicklungsprozess von IPFIX

Das IPFIX im folgenden Abschnitt als Beispielsgrundlage gewählt wurde liegt daran, dass IPFIX wie schon oben erwähnt ein von der IETF entwickeltes Protokoll ist. Die IETF publiziert, im Gegensatz zu anderen Entwicklern oder Herstellern, sämtliche Dokumente zu deren Entwicklungen frei zugänglich auf ihrem Webportal. [16]

Zu den veröffentlichten Dokumenten zählen dazu unter anderem die Mailinglist und die sogenannten 'Request for Comments' (RFC). In der Mailinglist werden sämtliche E-Mails, die zwischen den einzelnen Projektteilnehmern zum Thema IPFIX geschrieben wurden, chronologisch online zugänglich gemacht. Bei den RFC's handelt es sich um eine Reihe von beschreibenden technischen Dokumenten, welche die Öffentlichkeit über den aktuellen Stand der Entwicklungen detailliert informiert. RFC's bekommen bei der Veröffentlichung eine eindeutige Nummer zugeteilt, und können ab dem Zeitpunkt nicht mehr verändert werden, sondern nur noch durch ein neueres RFC abgelöst werden.

Mit den publizierten Informationen der IETF lässt sich somit der Entwicklungsprozess von IPFIX sehr gut nachvollziehen, und in einem Zeitstrahl, wie in Abbildung 3 ersichtlich.

Wie aus dem Zeitstrahl in Abbildung 3 ersichtlich, starte-

doi: 10.2313/NET-2011-07-2_21

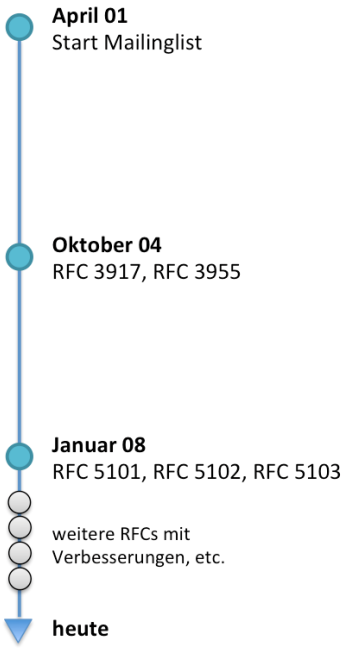


Abbildung 2: Entwicklungsprozess IPFIX als Zeitstrahl

te der Entwicklungsprozess von IPFIX im April 2001 mit der Einrichtung der Mailinglist und einem ersten Aufruf an andere Entwickler, sich dieser Mailinglist, beziehungsweise diesem Projekt anzuschließen. Anschließend wurde innerhalb der Mailinglist über die verschiedensten Anforderungen, Zielsetzungen und Lösungsansätze diskutiert, zu mehreren realen Treffen eingeladen und später über die Ergebnisse dieser Treffen berichtet.

Im Oktober 2004, also mehr als vier Jahre nach dem offiziellen Start des Projektes, wurden die ersten zwei RFC's mit dem Titel 'Requirements for IP Flow Information Export' (RFC 3917) [17] und 'Evaluation of Candidate Protocols for IP Flow Information Export' (RFC 3955) [18] von der IETF publiziert. Im RFC 3917 werden die von der IETF im Zeitraum April 2001 bis Oktober 2004 erarbeiteten Anforderungen dargestellt, die von IPFIX erwartet werden. Im RFC 3955 werden dann eine Auswahl von fünf verschiedenen Protokollen dargestellt, auf welchen IPFIX aufsetzen könnte, und dessen Vor- und Nachteile im Bezug auf die im anderen RFC (RFC 3917) gestellten Anforderungen untersucht.

Nach knapp vier weiteren Jahren, etlichen E-Mails und etlichen Treffen später wurde im Januar 2008 dann das wohl wichtigste RFC im Bezug auf die Entwicklung von IPFIX veröffentlicht: 'Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information' (RFC 5101) [19]. Dieses RFC ist eine komplette technische Beschreibung von IPFIX und dessen Bestandteile. Der Aufbau des RFC ist klar strukturiert: Zunächst folgt eine Einleitung, in welcher beschrieben wird, warum IPFIX benötigt wird, und was es können muss. Der Schreibstil ist grundlegend erklärend, benötigt jedoch ein Grundwissen um richtig verstanden zu werden. Der folgende Auszug aus der Einleitung stellt den Schreibstil des gesamten RFC relativ gut dar:

Beispiel 2:
'A data network with IP traffic primarily consists of IP flows passing through the network elements. It is often interesting, useful, or even required to have access to information about these flows that pass through the network elements for administrative or other purposes. The IPFIX Collecting Process should be able to receive the flow information passing through multiple network elements within the data network. [...]'

Nach dem Konkretisieren des Problems und dem Festlegen der grundlegenden Begriffe wird in den darauf folgenden Kapiteln erklärt, wie die einzelnen Komponenten von IPFIX funktionieren und wie das Zusammenspiel dieser Komponenten IPFIX funktionstüchtig macht. Interessant ist auch hier, besonders im Blick auf das nächste Kapitel, die Beobachtung des Schreibstils: Wie schon in der Einleitung findet auch hier die Beschreibung ausschließlich erklärend und ohne das Umschreiben des Problems statt. Dies wird auch aus dem kurzen Auszug klar ersichtlich:

Beispiel 3:
'[...] One of the essential elements in the IPFIX record format is the Template Record. Templates greatly enhance the flexibility of the record format because they allow the Collecting Process to process IPFIX Messages without necessarily knowing the interpretation of all Data Records. A Template Record contains any combination of IANA-assigned and/or enterprise-specific Information Elements identifiers.[...]'

Zeitgleich mit der Veröffentlichung des RFC 5101 wurden auch zwei weitere RFCs veröffentlicht (RFC 5102, RFC 5103), in denen zum einen das 'Information Model' von IPFIX näher erläutert wird und zum anderen ein weiteres Verfahren, das 'Bidirectional Flow Export' im Bezug auf IPFIX erklärt.

IPFIX war somit im Jahre 2008 nach acht Jahren Entwicklungszeit 'fertig', jedoch dauern die Entwicklungen in diesem Bereich bis heute an: Ein Blick auf die Seite der IETF belegt, dass hinter den Kulissen in der Mailinglist eifrig weitergearbeitet wird. So entstanden in der Zeit bis Juli 2011 noch ganze elf weitere RFC's. Diese beschäftigen sich unter anderem mit Verbesserungen einzelner Teile von IPFIX, aber auch mit Richtlinien für das effiziente Testen des Protokolls.

4.2 Patentprozess von IPFIX

Neben der Veröffentlichung von sämtlichen Dokumenten von IPFIX ist ein weiteres interessantes Merkmal, dass auch der Patentprozess relativ gut nachvollziehbar ist. Besonders informationsreich ist es hierbei, wenn man sich den Zeitstrahl des Patentprozesses im direkten Vergleich mit dem Zeitstrahl des Entwicklungsprozesses in Abbildung 4 ansieht.

Wie aus dem Zeitstrahl ersichtlich, wurde im März 2007 IPFIX beim 'United States Patent and Trademark Office', also dem amerikanischen Pendant zum DPMA, zum Patent angemeldet. [10] Die Anmeldung von IPFIX zum Patent erfolgte durch die Firma 'Cisco Technology, Inc.'. Ab diesem Zeitpunkt lief das Patentverfahren.

doi: 10.2313/NET-2011-07-2_21

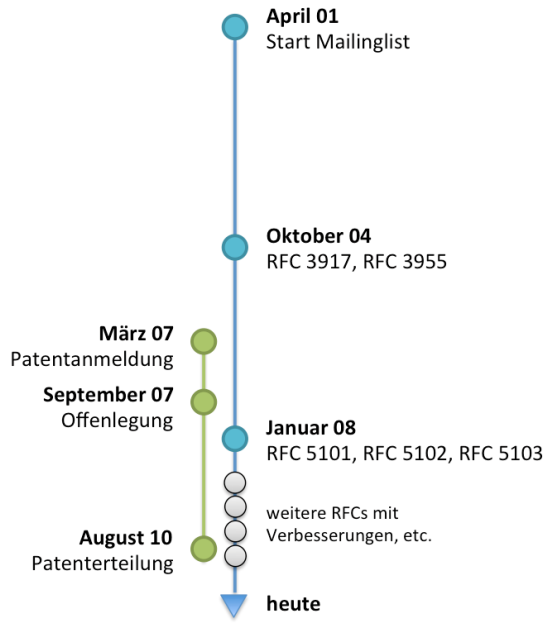


Abbildung 3: Patentprozess vs. Entwicklungsprozess IPFIX als Zeitstrahl

Im Gegensatz zum deutschen Recht, erfolgt in den USA die Offenlegung des Patents, bzw. des Patentantrages, nicht nach 18 Monaten, sondern schon nach sechs Monaten. So war es auch bei IPFIX der Fall: Am 20. September 2007 wurde der aktuelle Stand (zu diesem Zeitpunkt noch der Patentantrag), der Öffentlichkeit zugänglich gemacht.

Die Erteilung des Patents erfolgte dann erst über drei Jahre später, am 31. August 2010. Am Beispiel IPFIX lassen sich jetzt zwei wesentliche Informationen zum Thema 'Von der Erfindung zum Patent' ablesen: Zum einen lässt sich sehr gut erkennen, dass eine Erfindung, bzw. eine Entwicklung ein fortlaufendes Verfahren ist, welches oft durch die Patentanmeldung noch lange nicht abgeschlossen ist. Gerade im Falle von IPFIX sieht man, dass die Patentanmeldung noch im laufenden Entwicklungsverfahren abgegeben worden ist, und zwar über zehn Monate vor der Veröffentlichung des wesentlichen RFC 5101.

Zum anderen lässt sich erahnen, dass die Anmeldung einer Erfindung zum Patent nicht nur Vorteile mit sich bringt: Problematisch ist vor allem die zeitlich gebundene Offenlegung. Gerade bei der Offenlegung werden der Konkurrenz oft schon wichtige und intime Neuerungen verraten, noch bevor man als Erfinder die Möglichkeit hat, selbst von seiner Erfindung zu profitieren. Der 'Überraschungseffekt', mit denen man sich Raum in dem jeweiligen Konkurrenzumfeld schaffen könnte, ist dadurch quasi geplatzt. Die Konkurrenz hat dann oft genügend Zeit sich darauf vorzubereiten.

Im Kapitel zuvor wurden einige Auszüge aus den einzelnen RFC's wiedergegeben, um einen groben Einblick in die Art und Weise der Beschreibung einer technischen Erfindung zu erhalten. Eine Frage die sich jetzt noch aufdrängt ist, wie sich eine technische Erfindung, wie IPFIX, in der Patentschrift wiederfinden lässt. Im folgenden werden nun einige Auszüge aus der Patentschrift von IPFIX (Patent US 7,788,371 B2) präsentiert, an denen sich sowohl die einzelnen in den Kapiteln zuvor beschriebenen Teilfragmente der Patentanmeldung, als auch die technische Erfindung IPFIX an sich, wiederfinden lassen.

Die Patentschrift zu IPFIX wird gestartet mit dem Titel des Patents: 'EXPORTING MANAGEMENT INFORMATION BASE DATA USING IPFIX'. Anschließend folgen hier die wichtigsten Eckdaten zur Patentanmeldung, wie zum Beispiel der Patentanmelder ('Cisco Technology, Inc., San Jose, CA (US)') und der kompletten Erfinderbenennung. An dieser Stelle wird auch wieder deutlich, dass der Anmelder des Patents nicht immer gleich den Erfindern des Patents sein muss.

Nach den wichtigsten Eckdaten und der Kurzfassung folgen eine Reihe von technischen Zeichnungen, auf die innerhalb der Patentanmeldung zurückgegriffen wird. Im Falle IPFIX wurde als technische Zeichnung eine Aufstellung der einzelnen Header-Felder, und mehrere Ablaufdiagramme abgegeben.

Im nächsten Abschnitt der Patentanmeldung steht nun die technische Beschreibung im Vordergrund. Hier wird zunächst angegeben, in welches technische Gebiet diese Erfindung gehört. Anschließend wird IPFIX kurz aber sehr ähnlich den RFC's technisch beschrieben.

Beispiel 4:
'TECHNICAL FIELD: The present disclosure relates generally to network management.

BACKGROUND: The approaches described in this section could be pursued, but are not necessarily approaches that have been previously conceived or pursued. Therefore, unless otherwise indicated herein, the approaches described in this section are not prior art to the claims in this application and are not admitted to be prior art by inclusion in this section.

IP (Internet Protocol) Flow Information eXport (IPFIX) is a protocol based on Cisco NetFlow version 9, which is defined in the Internet Engineering Task Force (IETF) Request for Comment (RFC) 3954. IPFIX is currently at the final phase of standardization at the IETF. IPFIX could be considered as NetFlow version 10. The Working Group home page is accessible at http://www.ietf.org/html.charters/ipfix-charter.html

The IPFIX protocol defines how IP Flow information can be exported from routers, measurement probes or other devices. IP Flow information can be used as input to various applications. IPFIX is a general data transport protocol, easily extensible to suit the needs of different applications. IPFIX provides appropriate Information Elements (IEs) for various IP versions. A text-based draft of the IPFIX Information Element draft is accessible at (http://www.ietf.org/internet-drafts/draft-ietf-ipfix-info-13.txt [...]'

An dem obigen Beispiel lässt sich sehr gut erkennen, dass technische Beschreibung sehr kurz gehalten ist und für nähere Details, die nicht unbedingt die Patentanmeldung betreffen, auf andere Quellen verwiesen wird.

doi: 10.2313/NET-2011-07-2_21

Bis hier her kann ein Experte des technischen Gebiets die Patentanmeldung verstehen. Das eigentliche Herzstück einer Patentanmeldung sind die Patentansprüche. Wie beschrieben, werden erst mit diesen geklärt, was eigentlich und in welchem Zusammenhang geschützt ist. Die Ausführung der Patentansprüche ist, wie im nächsten Beispiel sichtbar wird, sehr juristisch formuliert und deshalb ab diesem Teil auch für Experten, die sich zwar in dem technischen Gebiet aufhalten, jedoch nur wenig juristisches Fachwissen besitzen, sehr schwer zu verstehen:

Beispiel 5:
'Hauptanspruch:
1. A networking apparatus, comprising: a network interface; a processor coupled to the interface; logic coupled to the processor and encoded in one or more tangible storage media [...]
a Simple Network Management Protocol (SNMP) MIB variable or table that corresponds to the MIB object; creating an Internet Protocol Flow Information Export (IPFIX) template record data structure that includes the object identifier; [...]

Nebenansprüche:
[...] 6. The apparatus as recited in claim 1 wherein the strings compromise NULL terminated strings. [...]'

Zusammengefasst lässt sich gerade im Beispiel IPFIX sagen, dass die Patentanmeldung selbst im Prinzip aus zwei Teilen besteht: Der technischen Beschreibung für die Experten auf dem jeweiligen technischen Gebiet, und den sehr juristischen Patentansprüchen, welche die Erfindung vor der unautorisierten Nachahmung durch Dritte schützen soll.

5. ZUSAMMENFASSUNG

Eine Erfindung alleine reicht noch nicht aus, um als Erfinder oder Inhaber aus dieser Vorteile zu ziehen. Eine Erfindung ist wertvoll und braucht in jedem Fall Schutz vor der unautorisierten Nachahmung Dritter. Das Patent ist dabei die wohl wertvollste Methode, einen wirksamen Schutz zu erreichen. Erst eine geschützte Erfindung ist in den meisten Fällen eine ertragreiche Erfindung.

Wichtig ist sowohl den richtigen Zeitpunkt für die Patentanmeldung zu finden (im Bezug auf die Offenlegung), als auch die Patentansprüche richtig zu formulieren. Oft ist es hilfreich, sich andere Projekte oder Produkte anzusehen, die im selben technischen Gebiet erfolgreich und bereits patentiert sind.

Da der Weg von der Erfindung zum Patent nicht immer einfach ist, lohnt es sich auf jeden Fall auch Experten, wie zum Beispiel Rechtsanwälte oder Juristen zu Rate ziehen. Sind zum Beispiel die Patentansprüche lückenhaft oder lassen Spielraum für andere Produkte offen, die als Endergebnis das Gleiche produzieren, ist eine Patentanmeldung quasi gescheitert.

6. LITERATUR

[1] Dipl.-Ing. Volker Ilzhöfer / Rainer Engels: *Patent-, Marken und Urheberecht 8. Auflage*, Der Begriff Erfindung, Seite 53, Verlag Franz Vahlen, München, Deutschland, 2010

[2] *DPMA - Patent, Patente fördern Innovationen*, `http://www.dpma.de/patent/index.html`, abgerufen: 18.05.2011

[3] *Pharmabranche: Mit Zähnen und Klauen*, `http://www.rpoth.at/pastwork/pharma.shtml`, abgerufen: 20.05.2011

[4] Prof. Dr. Joachim Henkel: *Grundlagen der Betriebswirtschaftslehre 2*, Modul 2: Innovation -Marktaspekte, Seite 3-4, Lehrstuhl für Technologie- und Innovationsmanagement, TU München, Deutschland, SS 2010

[5] *200 nachgemachte Doppelmayr-Lifte in China*, `http://vorarlberg.orf.at/stories/57435/`, abgerufen: 18.05.2011

[6] *DPMA - Anmeldung*, `http://www.dpma.de/patent/anmeldung/index.html`, abgerufen: 18.05.2011

[7] *DPMA - Patent FAQ*, `http://www.dpma.de/patent/faq/index.html`, abgerufen: 18.05.2011

[8] Dipl.-Ing. Volker Ilzhöfer / Rainer Engels: *Patent-, Marken und Urheberecht 8. Auflage*, Kapitel 2. Patentgesetz (PatG), Seite 81-90, Verlag Franz Vahlen, München, Deutschland, 2010

[9] Deutsches Patent- und Markenamt: *Merkblatt für Patentanmelder*, Beispiel für Patentansprüche und Beschreibung, Seite 12-13, DPMA, 80297 München, Deutschland, 2009

[10] United States Patent, Claise et. al: *Exporting Management Information Base Data Using IPFIX*, Patent Nr..: US 7,788,371 B2, Seite 11-13, Anmelder: Cisco Technology Inc., San Jose, CA, US, 2010

[11] *DPMA - Verfahren*, `http://www.dpma.de/patent/verfahren/index.html`, abgerufen: 18.05.2011

[12] *Patent - Wikipedia*, `http://de.wikipedia.org/wiki/Patent`, abgerufen: 19.05.2011

[13] *Service BW - Patentanmeldung*, `http://www.service-bw.de/zfinder-bw-web/processes.do?vbid=1263162&vbmid=0`, abgerufen: 20.05.2011

[14] *Universität Regensburg, Erfinderberatung, Patente von A bis Z*, `http://www.uni-regensburg.de/Einrichtungen/FUTUR/html/patenteaz.html`, abgerufen: 20.05.2011

[15] Network Working Group: *Request for Comments (RFC) 2026*, Kapitel 1.1 - 1.2, s. Bradner, Harvard University, 1996

[16] *IP Flow Information Export (ipfix) - Charter*, `http://datatracker.ietf.org/wg/ipfix/charter/`, abgerufen: 17.07.2011

[17] Network Working Group: *Request for Comments (RFC) 3917*, J. Quittek NEC Europe Ltd., T. Zseby Fraunhofer FOKUS, B. Claise Cisco Systems, S. Zander Swinburne University, 2004

[18] Network Working Group: *Request for Comments (RFC) 3917*, S. Leinen, SWITCH, 2004

[19] Network Working Group: *Request for Comments (RFC) 5101*, B. Claise, Ed., Cisco Systems, Inc., 2008

doi: 10.2313/NET-2011-07-2_21

ISBN 3-937201-22-X
DOI 10.2313/NET-2011-07-2

ISSN 1868-2634 (print)
ISSN 1868-2642 (electronic)