Mercator

Florian Hartmann
Betreuer: Johann Schlamp, Dirk Haage
Hauptseminar - Innovative Internettechnologien und Mobilkommunikation SS2010
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: hartmanf@in.tum.de

KURZFASSUNG

Netzwerke, insbesondere das Internet, unterstehen einer ständigen Veränderung. Die Übersicht über ein Netzwerk zu behalten, ist schwierig. Programme sind in der Lage, Karten eines Netzwerkes durch Messungen zu erstellen. Diese können in diversen Anwendungsgebieten hilfreich sein. In dieser Arbeit wird das Programm Mercator beschrieben, das durch Traceroute-Messungen im Internet Daten liefert, mit denen später eine Internet-Karte erstellt werden kann. Es werden die genutzten Techniken erklärt, die zum Auffinden von Routern und Verbindungen, sowie zum Zuordnen von Interfaces zu Routern nötig sind. Darüber hinaus wird auf Ergebnisse von Testmessungen eingegangen und mögliche Verbesserungen der Techniken aufgezeigt.

Schlüsselworte

Internet-Karten, Netzwerktopologie, Mercator, Traceroute, Source-Routing, Alias-Auflösung, hop-limited probes, informed random address probing

1. EINLEITUNG

Das Internet besteht aus vielen untereinander verbundenen Computernetzwerken. Zu diesen Netzwerken gehören hauptsächlich Provider-, Firmen- oder Universitäts- bzw. Forschungsnetzwerke. Jedes dieser Netzwerke steht unter einer eigenen administrativen Verwaltung. Da die Infrastrukturen der einzelnen Netzwerke unabhängig voneinander sind, kann jede Verwaltung eigene Regeln und Richtlinien festlegen. Dies hat zur Folge, dass Netzwerke unterschiedlich aufgebaut sein können und daher oftmals unterschiedliche Netzwerktopologien besitzen. Des Weiteren unterstehen Netzwerke einem stetigem Wandel. Teilnehmer und Verbindungen kommen hinzu, werden entfernt oder Eigenschaften ändern sich.

Den Überblick über ein Netzwerk zu behalten, ist eine schwierige Aufgabe. Zum einen ist es eine zeitaufwändige Angelegenheit, eine Netzwerktopologie per Hand zu pflegen, und zum anderen geben die Verwaltungen oftmals keine detaillierten Informationen über ihr Netzwerk preis. Dennoch können genaue Informationen über Netzwerktopologien, wie in Kapitel 3.2 beschrieben, in vielerlei Hinsicht hilfreich sein. In Kapitel 3 wird erläutert, was Internet-Karten sind und wie diese aussehen können.

Das Programm Mercator ist in der Lage, die Topologie eines Netzwerkes herauszufinden, ohne dabei Informationen über das entsprechende Netzwerk zu benötigen. Durch die dabei entstehenden Daten lassen sich Internet-Karten generieren. In Kapitel 4 wird dieses Programm, sowie dessen Techniken vorgestellt. Weiterhin wird auf die bei Messungen entstandenen Ergebnisse eingegangen und diese bewertet. In Kapitel 5 wird ein Ausblick auf weitere Techniken gegeben, die ebenfalls zur Generierung einer Internet-Karte genutzt werden können.

2. VERWANDTE TOOLS

Neben Mercator gibt es noch weitere Tools, die Internet-Karten erstellen können.

Rocketfuel [13], ein Tool der Universität von Washington (USA), ist darauf ausgelegt, die Netzwerktopologie eines gegebenen Internet Service Providers abzubilden. Rocketfuel läuft auf knapp 300 Servern in Europa, Australien und der USA.

Ein weiteres Tool ist Skitter [7]. Skitter wird von der Cooperative Association for Internet Data Analysis, kurz CAIDA, betrieben und hat innerhalb der letzten zehn Jahre über vier Terabyte Daten gesammelt, die Grundlage vieler Visualisierungen sind.

Auch scamper [11] ist ein Tool zur Erstellung von Internet-Karten. Es wird von der WAND group der Universität von Waikato (Neuseeland) entwickelt. Scamper nutzt aktuellere Techniken als Mercator und unterstützt unter anderem auch IPv6. Es wird von CAIDA in einer neuen Mess-Infrastruktur genutzt, die Skitter ablösen soll.

3. INTERNET-KARTEN

Von einem Netzwerk können Karten generiert werden. Dabei wird in der Regel zwischen drei verschiedenen Arten von Karten unterschieden [8].

- Geografische Karten zeigen die geografische Position der Teilnehmer auf einer Landkarte. Solche Karten können genutzt werden um Netzwerkprobleme geografischer oder klimatischer Natur zu lösen.
- Konzeptionelle Karten hingegen betrachten nicht den physikalischen Aufbau, sondern die Verteilung der Informationen im Netzwerk. Diese Karten können genutzt werden, um Informationen im Netzwerk zu finden. Generiert und genutzt werden solche Karten vor allem von Suchmaschinen wie Google oder Yahoo. Durch Verbindungen zwischen verschiedenen Informationen lässt sich die Relevanz der Daten bemessen.

- Eine weitere Art von Karten sind die Infrastrukturkarten. Bei diesen Karten handelt es sich um die Darstellung einzelner Netzwerkteilnehmer, Knotenpunkte und deren Verbindungen untereinander. Entsprechende Anwendungsgebiete solcher Karten werden im Kapitel 3.2 betrachtet.

3.1 Definition

Im Folgenden wird mit Internet-Karte immer eine Infrastrukturkarte, wie im Kapitel 3 beschrieben, bezeichnet.

Eine Internet-Karte besteht aus einem ungerichtetem Graphen. Die Knoten dieses Graphens entsprechen den Routern bzw. Hosts im Internet. Dabei kann ein Router mehrere Interfaces besitzen. Jedes Interface ist einer IP-Adresse zugeordnet, wobei diese Adresse im Netzwerk eindeutig ist. Die Knoten sind über Kanten miteinander verbunden. Eine Kante entspricht einer logischen Verbindung zweier Interfaces. Ein Interface ist immer mit einem oder mehreren Interfaces verbunden. Die Verbindung ist auf IP Ebene zu sehen - Repeater, Bridges, Hubs oder Switches werden vernachlässigt. Abbildung 1 zeigt eine mögliche graphische Darstellung einer Internet-Karte.

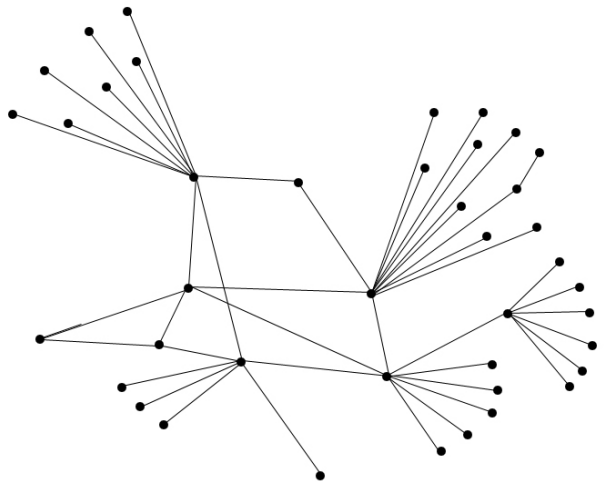

Abbildung 1: Darstellung einer Internet-Karte

3.2 Anwendungsgebiete

Internet-Karten können in vielen Szenarien hilfreich sein. Zur Simulation von Netzwerken können Internet-Karten die benötigten Daten liefern. Der Vorteil besteht darin, dass die Informationen auf realen Netzwerken basieren und somit realistische und praxisnahe Simulationen zulassen [5]. Beispielsweise werden in Referenz [12] simulierte Netzwerke genutzt, um Annahmen über die Skalierung von Multicast-Netzwerken zu bestätigen.

Karten eines Netzwerkes sind ebenfalls für dessen Verwaltung nützlich. Die Netzwerktopologie kann bei der Platzierung neuer Knotenpunkte helfen. Zudem können Probleme und Flaschenhälse identifiziert und entsprechend aufgelöst werden [1].

Nicht nur für die Netzwerkbetreiber bzw. die Verwaltung ist es interessant, ihre Netzwerktopologie zu kennen. Auch Teilnehmer des Netzwerkes können anhand der Karte entscheiden, wo sie sich im Netzwerk platzieren wollen und welcher Internetprovider dafür gewählt wird. Besonders im Internet ist es wichtig, Server richtig aufzustellen und somit die Latenzzeit zur Zielgruppe zu minimieren und die verfügbare Bandbreite zu maximieren [1].

Ist in einem Netzwerk die komplette Topologie bekannt, können spezielle Protokolle und Algorithmen angewandt werden. Es existieren Routingprotokolle, die anhand der Netzwerktopologie den kürzesten Weg zum Ziel berechnen können (beispielsweise das Optimized Link State Routing Protokoll, kurz OLSR). Allerdings sind solche Routingprotokolle nur für kleine bzw. statische Netzwerke nützlich. Für große, stark fluktuierende Netze wie das Internet, sind solche Algorithmen kaum einsetzbar.

Es gibt demnach vielfache Anwendungsmöglichkeiten für Internet-Karten. Im folgenden Kapitel wird das Programm Mercator vorgestellt, das die für Internet-Karten benötigten Informationen durch Messungen herausfinden kann.

4. MERCATOR

Mercator ist ein Programm, das 1998 von Ramesh Govindan und Annop Reddy am Information Sciences Institute an der University of Southern California (USA) entwickelt wurde. Das Programm ist in der Lage, Informationen durch Messungen im Internet zu liefern, die für die Erstellung von Internet-Karten vonnöten sind. Genau genommen sucht Mercator Router im Netzwerk und Verbindungen zwischen den Routern. Des Weiteren kann Mercator Aliasse auflösen, also Interfaces zu Routern zuordnen.

4.1 Anforderungen

Da Mercator Informationen über die Infrastruktur des Internets liefern soll, gibt es bestimmte Einschränkungen, die das Programm beachten muss. Im Allgemeinen bietet das Internet nur wenige Funktionen zur Infrastrukturbestimmung. Protokolle zur Netzwerkverwaltung, wie zum Beispiel das Simple Network Management Protocol, sind in der Regel nicht verfügbar. Für Mercator wurden demnach die drei folgende Anforderungen gewählt [9].

- Die Anforderungen an das Netzwerk sollen minimal sein. Das bedeutet, Mercator nutzt zur Informationsgewinnung nur Techniken, die standardmäßig jeder Router im Internet unterstützt. Im Grunde basieren Mercators Messungen nur auf Paketen, deren time-to-live begrenzt ist, wie auch beim Programm Traceroute.
- Die Messungen sollen von einem einzelnen, frei wählbaren Knoten im Netzwerk ausgeführt werden können. Durch eine einzelne Instanz des Programmes auf einem Knoten wird die Programmierung und der Betrieb vereinfacht. Ein komplexes, verteiltes System ist nicht nötig. Mercator soll außerdem auf einem beliebigen Host im Netzwerk installiert werden können. Denn eine Platzierung auf Transit- oder Hauptknotenpunkten ist oftmals nicht möglich oder durch die Netzwerkverwaltung nicht gewünscht.

- Router und deren Verbindungen werden von Mercator durch Messungen bestimmt. Diese Messungen werden zu bestimmten Ziel-Adressen ausgeführt. Die Ziele könnten durch Adresstabellen definiert werden. Adresstabellen müssten dann allerdings aufwändig per Hand gepflegt werden und könnten dementsprechend fehlerhaft und nicht immer aktuell sein. Die Wahl der Ziele muss deshalb vom Programm selbst getroffen werden.

4.2 Ziele

Neben dem Hauptziel, Daten für eine Internet-Karten zu beziehen, wurden noch weitere Ziele für Mercator definiert. So soll das Programm seine Messungen möglichst effektiv durchführen. Das bedeutet, dass die Anzahl der Pakete, die gleichzeitig und insgesamt gesendet werden, möglichst klein sein soll. Somit soll eine geringe Netzwerkbelastung erreicht werden [9].

Weiterhin sollen die Messungen schnell durchgeführt werden. Dies steht aber in Konkurrenz zur geringen Netzwerkbelastung. Denn schnelle Messungen erfordern eine große Menge an parallel versendeten Paketen. Ziel ist es also, die richtige Balance zwischen Effektivität und Geschwindigkeit zu erzielen.

Die gefundenen Informationen über das Netzwerk sollen darüber hinaus vollständig und fehlerfrei sein. Wie in Kapitel 4.3.4 beschrieben, können aber möglicherweise nicht alle Router und Verbindungen gefunden werden, wenn die Messungen nur von einem Knotenpunkt im Netzwerk ausgeführt werden.

4.3 Techniken

Um die festgelegten Ziele zu erreichen, setzt Mercator verschiedene Techniken ein. Dabei werden Messungen, so genannte „Traceroutes“, zu bestimmten IP-Adressen durchgeführt. Die Messungen entdecken und speichern Router und Verbindungen zwischen den Routern. Genau genommen werden allerdings keine Router gefunden, sondern nur einzelne Interfaces mit den dazugehörigen IP-Adressen. Zusätzlich zu den genannten Messungen führt Mercator weitere Tests durch, die die gefundenen Interfaces zu ihren Routern zuordnen sollen. Letztendlich ergeben sich Router, ihre zugehörigen Interfaces sowie die Verbindungen zwischen den Routern. Mit diesem Ergebnis ließe sich dann eine Internet-Karte generieren. Dies ist aber nicht Teil von Mercator.

4.3.1 Traceroute

Die Mercator zu Grunde liegende Technik nennt sich „Traceroute“. Bei einem Traceroute wird der Pfad vom Messknoten zu einem Zielknoten herausgefunden. Das heißt, alle Knoten zwischen Start und Ziel werden nacheinander durchlaufen. Dabei werden sogenannte „hop-limited probes“ genutzt, dies sind Pakete deren time-to-live, folgend als TTL abgekürzt, begrenzt ist. Die TTL bezeichnet die Anzahl an Knotenpunkten, folgend als Hop bezeichnet, die ein Paket traversieren darf, bevor es verworfen wird. Jeder Hop dekrementiert die TTL um eins. Sobald der Wert auf Null sinkt, sendet der aktuelle Hop eine ICMP-time-exceeded-Fehlermeldung an den Sender zurück. Sollte der aktuelle Hop das Ziel des Paketes sein, wird eine ICMP-echo-reply-Meldung zurück gesendet. ICMP-Meldungen (Internet Control Message Protocol) sind Bestandteil von IPv4 und werden zum Austausch von Informations- und Fehlermeldungen genutzt. Die hier beschriebene Technik wird auch vom Programm Traceroute genutzt, das auf gängigen System verfügbar ist (Unix/Mac: traceroute, Windows: tracert.exe).

Bei „traceroute“-Messungen können TCP-, UDP- oder ICMP-Pakete verwendet werden. Als erstes wird ein Paket von Mercator zum Zielknoten versendet dessen TTL = 1 gesetzt ist. Der erste Hop (A) auf der Route zum Ziel verringert die TTL, somit ist die TTL = 0, der Hop verwirft das Paket und sendet eine ICMP-time-exceeded-Fehlermeldung an den Startknoten zurück. Anhand der Quelladresse der ICMP-Fehlermeldung kennt Mercator nun die Adresse von A und weiß außerdem, dass A direkt mit ihm verbunden ist.
Jetzt wird ein zweites Paket mit der TTL = 2 versendet. Hop A verringert die TTL auf 1 und sendet das Paket weiter. Diesmal dekrementiert Hop B die TTL auf Null. B antwortet nun ebenfalls mit einer ICMP-time-exceeded-Fehlermeldung. Mercator kann dann wiederum anhand der Quelladresse des ICMP-Paketes B identifizieren und weiß, dass A mit B direkt verbunden ist.
Mercator versendet nun so lange neue Pakete, jedes mal mit höherer TTL, bis eine ICMP-echo-reply-Meldung zurück kommt. In diesem Fall weiß Mercator, dass der Zielpunkt erreicht wurde und die Messung abgeschlossen ist. Das Ergebnis ist der komplette Pfad von Mercator bis zum Endpunkt inklusive aller Hops und deren IP-Adressen. Mercator verschickt immer nur ein Paket pro Traceroute-Messung gleichzeitig. Parallele Messungen sind jedoch möglich.

Mit dieser Technik kann Mercator Knotenpunkte und deren Verbindungen untereinander in einem Netzwerk herausfinden und schafft somit die Grundlage für Internet-Karten.

4.3.2 Adresswahl

Im letzten Kapitel wurde erläutert, dass Mercator seine Traceroute-Messungen zu bestimmten Zielknoten durchführt. In Kapitel 4.1 wurde an Mercator die Anforderung gestellt, die Adressen der Zielknoten selbstständig zu generieren. Des Weiteren ist gefordert, dass die entstehende Karte vollständig ist. Der einfachste Weg wäre eine Messung zu allen mögliche IP-Adressen zu starten. Allerdings umfasst der IPv4-Adressbereich über vier Milliarden mögliche Ziele. Eine Messung zu jeder IP-Adresse auszuführen würde viel zu lange dauern. Außerdem sind viele dieser IP-Adressen nicht erreichbar und eine Messung zu diesen Adressen würde wenig neue Informationen bringen. Folglich kann nur eine begrenzte Anzahl an Messungen durchgeführt werden. Ziel ist es deshalb, nur Teilnetze zu wählen und diese dafür vollständig abzudecken.

Mercator nutzt dafür eine Technik namens „informed random address probing“. Dabei wird anhand von zwei Annahmen der Adressbereich eingeschränkt. Der Bereich wird so gewählt, dass er große Mengen an adressierbaren, also erreichbaren IP-Adressen enthält. Ein Adressbereich bzw. Block wird durch ein Präfix dargestellt (z.B.: 128.10/16). Alle IP-Adressen aus einem Block haben ein gemeinsames Präfix. Mercator wählt 8, 16 oder 19 Bit als Länge des Präfixes. Diese Längen wurden so gewählt da Netzwerkbetreiber oftmals diese Längen für ihre Präfixe verwenden [9].

Die erste Annahme geht davon aus, dass IP-Registrierungs-

stellen ihre IP-Adressen immer in Blöcken verteilen [9]. Der Besitzer eines solchen Adressblockes wird also zuerst einen Großteil der IP-Adressen in diesem Block vergeben, bevor er einen neuen Adressblock anfordert. Mercator geht daher davon aus, dass wenn in einem Adressblock eine erreichbare IP-Adresse vorhanden ist, noch weitere adressierbare IP-Adressen in diesem Block existieren. Beim Programmstart wählt Mercator den Adressblock, in dem es sich selbst befindet, als Initialblock. Dann werden so lange zufällige IP-Adressen aus diesem Block gewählt bis über eine Zeitspanne von drei Minuten keine neuen erreichbaren IP-Adressen gefunden werden können.

Wenn in einem Adressblock keine neuen IP-Adressen mehr gefunden werden, muss Mercator einen neuen Block wählen. Dazu wird die zweite Annahme verwendet. Diese besagt, dass IP-Registrierungsstellen ihre Adressblöcke sequentiell vergeben. Existieren also in einem Block adressierbare IP-Adressen, so werden höchstwahrscheinlich auch in den Nachbarblöcken erreichbare IP-Adressen existieren [9]. Beispielsweise sind Block 128.9/16 und 128.11/16 Nachbarblöcke von 128.10/16. Um einen neuen Block aus allen Nachbarblöcken zu wählen, wird ein Lotterie-Scheduling-Verfahren angewandt. Dabei ist die Anzahl an Lottoscheinen proportional zu der gefundenen Anzahl an IP-Adressen im jeweiligen Nachbarblock.

Beide Annahmen helfen Mercator, weniger Messungen zu nicht erreichbaren IP-Adressen durchzuführen und ermöglichen letztendlich eine schnellere Erforschung des Netzwerkes. Außerdem liegen die gefundenen Adressen sehr nahe beieinander, was zu einem relativ kompletten Teilnetz führt.

4.3.3 Reduzierung benötigter Pakete

Auf Grund der Wahl der Ziele (Kapitel 4.3.2) werden sehr viele Traceroute-Messungen pro Block ausgeführt. Wie in Abbildung 2 zu sehen, ist der Pfad zum Block 128.10/16 immer der selbe. Bei jeder Messung den gesamten Pfad zu traversieren, würde keine neuen Informationen liefern. Daher reicht es, wenn Mercator die TTL des ersten Paketes so wählt, dass dieses den ersten Knoten im Block erreicht. Kommt die resultierende ICMP-time-exceeded-Fehlermeldung von dem erwarteten Knoten, führt Mercator seine Messung von dort an fort [9].

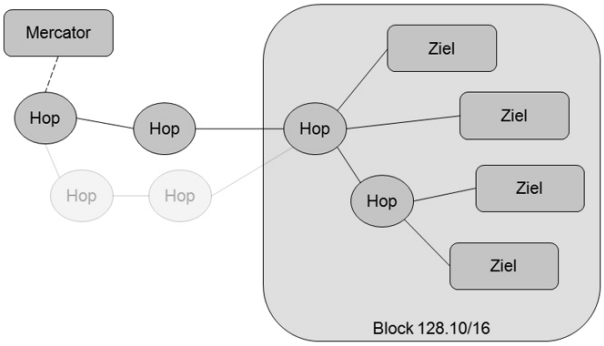

Abbildung 2: „traceroute“-Messung zu einem Adressblock

Unter Umständen kann sich der Pfad zum ersten Knoten im Block verändern, siehe Abbildung 3. Dies geschieht zum Beispiel durch alternative Pfade oder durch Ausfall von Verbindungen und Routern. In diesem Falle merkt Mercator aber anhand der Quelladresse der ersten ICMP-Fehlermeldung, ob der Knoten dem erwarteten entspricht. Sollte dies nicht der Fall sein, prüft Mercator den Pfad rückwärts bis es zum ersten Knoten stößt, der ihm bekannt ist. Von diesem Knoten an kann es dann seine Traceroute-Messung ganz normal weiterführen. Durch diese Technik wird die Gesamtanzahl benötigter Pakete verringert.

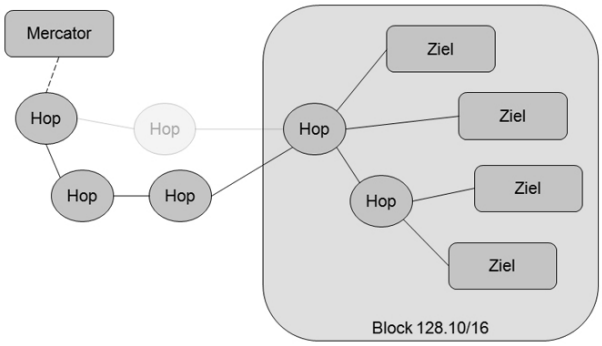

Abbildung 3: Änderung des Pfades zum Block

4.3.4 Source-Routing

Mit den bisher vorgestellten Techniken lassen sich viele Knotenpunkte und Verbindungen zwischen Knoten herausfinden. Doch können trotzdem Pfade unbekannt bleiben. Wie in Abbildung 4 zu sehen kann es passieren, dass durch Messungen zwar die Hops A und B gefunden werden, Pakete aber nie die Verbindung zwischen A und B passieren. Dies liegt an der Entscheidung, Mercator nur auf einem einzigen Knoten im Netzwerk laufen zu lassen (siehe Kapitel 4.1). Könnte eine weitere Instanz von Mercator auf Hop B betrieben werden und würde von dort aus eine Messung zum Ziel A durchgeführt werden, könnte die fehlende Verbindung gefunden werden.

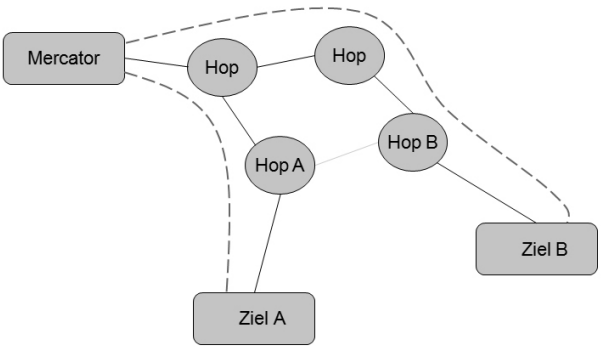

Abbildung 4: Verbindungen werden nicht immer gefunden

Um dieses Problem zu lösen, setzt Mercator auf Router, die „Source-Routing“ unterstützen. Diese Technik basiert auf dem Internet Protokoll (IP). Dabei kann ein IP Paket über einen vorgegebenen Router gesendet werden (siehe Abbildung 5). Dafür wird im IP Header des Paketes der Pfad eingefügt, den das Paket ablaufen soll. Das Paket wird dann zum ersten Knoten im angegebenen Pfad gesendet. Unterstützt dieser Knoten die Source-Routing-Technik, wird er das Paket zum

nächsten Knoten im angegebenen Pfad weiterleiten. Mercator nutzt diese Technik und führt zusätzlich zu seinen normalen Messungen, weitere Messungen über jeden bekannten Source-Routing-Router durch [9]. Bei einer Messung über einen Zwischenpunkt wählt Mercator die Initial-TTL so, dass das erste Traceroute-Paket beim Source-Routing-Router ankommt. Dann wird die TTL wieder pro Schritt um eins erhöht und somit der Pfad vom Zwischenpunkt zum Zielpunkt herausgefunden.

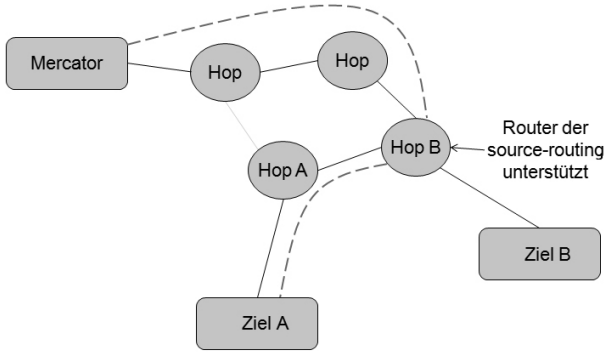

Abbildung 5: Traceroute mit Hilfe von „Source-Routing“

Source-Routing stellt jedoch ein Sicherheitsrisiko dar und ist deswegen auf den meisten Routern deaktiviert [2]. Die Entwickler haben herausgefunden, dass zum Zeitpunkt der Messungen etwa 8% aller Router im Internet Source-Routing unterstützen. Dies liegt zum Teil daran, dass Betreiber von Routern vergessen haben, Source-Routing in ihren Routern zu deaktivieren oder es nutzen, um ihr eigenes Netzwerk zu testen. Die Mercator Entwickler haben mit Simulationen berechnet, dass bei rund 5% Source-Routing-Routern bis zu 90% aller Knoten und Verbindungen in einem Netzwerk entdeckt werden können [9].

Mercator besitzt bei Programmstart noch keine Information über Router, die Source-Routing unterstützen. Daher muss es zur Laufzeit Router testen, ob bei diesen Source-Routing aktiviert ist. Hierfür sendet Mercator über einen Router A ein UDP-Paket an einen zufälligen Port eines beliebigen Routers B. Ist Source-Routing auf Router A aktiviert, leitet dieser das Paket weiter. Da das Paket an einen zufälligen Port adressiert ist, antwortet Router B sehr wahrscheinlich mit einer ICMP-port-unreachable-Fehlermeldung. Durch diese Fehlermeldung erfährt Mercator, dass Router A das Paket erfolgreich weitergeleitet hat, und Router A wird zur Liste der Source-Routing-Router hinzugefügt. Diesen Test führt Mercator mehrfach mit jedem gefundenen Router im Netzwerk aus, da möglicherweise Router A gerade nicht erreichbar ist oder Router B keine ICMP-port-unreachable-Fehlermeldung versendet, da ein existierender Port adressiert wurde.

4.3.5 Alias-Auflösung

Wie bereits in Kapitel 3.1 erwähnt, können Router mehrere Interfaces besitzen. Zur Erstellung von Internet-Karten ist es allerdings wichtig, den Router, zu dem das Interface gehört, zu kennen. Dieser Router könnte schließlich noch weitere Interfaces besitzen, die auf der Karte als ein Knotenpunkt dargestellt werden sollen.

Wie in Abbildung 6 zu sehen, führt Mercator mehrere Messungen aus. Beispielsweise könnte bei einer Messung Interface A gefunden werden und bei einer weiteren Messung Interface B. Für Mercator stellen beide Interfaces zwei eigenständige Knotenpunkte auf der Karte dar. Jedoch könnten beide Interfaces zu einem physikalischem Gerät gehören, siehe Abbildung 7. Mercator muss also in der Lage sein, mehrere Interfaces einem Router zuordnen zu können. Ansonsten würde die entstehende Internet-Karte fehlerhaft sein und das gegebene Netzwerk nicht korrekt wiedergeben werden.

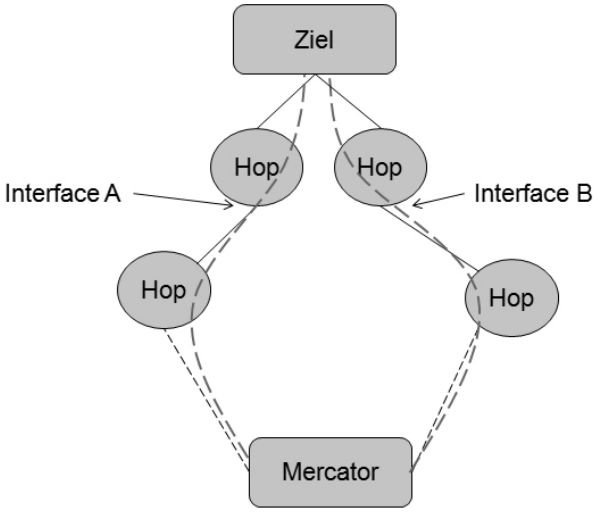

Abbildung 6: Netzwerk aus Sicht Mercators

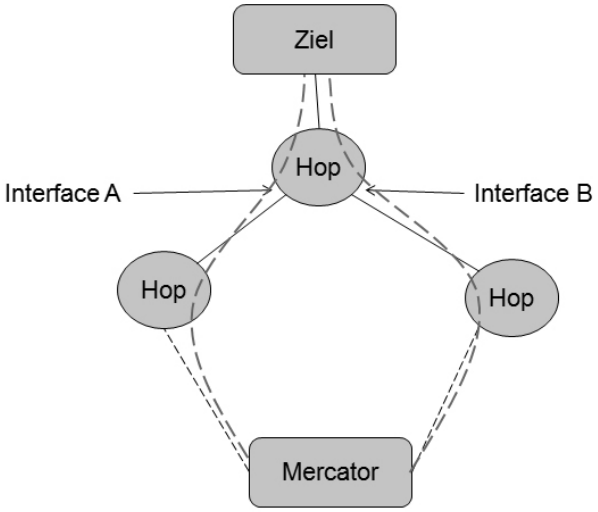

Abbildung 7: tatsächlich gegebenes Netzwerk

Um dieses Problem zu lösen, nutzt Mercator eine Eigenschaft vieler Router aus [9]. Empfängt ein Router ein Paket und möchte darauf antworten, versendet er die Antwort nicht immer über das Eingangsinterface, sondern über ein vorgegebenes Ausgangsinterface. Ein- und Ausgangsinterface sind also nicht immer gleich. Um diese Eigenschaft zu nutzen, sendet Mercator eine so genannte „alias-probe“ an ein Interface A, siehe Abbildung 8. Eine alias-probe bezeichnet ein UDP-Paket, das an einen zufälligen Port adressiert

ist. Erreicht dieses Paket den Router von Interface A, und existiert dieser Port nicht an dem Router, sendet dieser eine ICMP-port-unreachable-Fehlermeldung zurück an Mercator. Wie bereits erwähnt, kann diese Antwort möglicherweise über ein anderes Interface B versendet werden. Sendet Mercator also eine alias-probe an Adresse A und bekommt die Antwort von Adresse B zurück, so geht Mercator davon aus, dass Interface A und B zu einem physikalischem Gerät gehören [9].

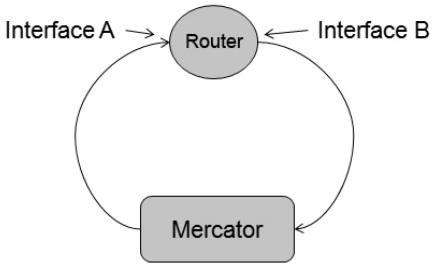

Abbildung 8: Auflösung von Alias durch „alias-probes“

Wie bei der Suche nach Source-Routing-Routern versendet Mercator wiederholt an jedes bekannte Interface eine alias-probe, um somit Alias-Interfaces aufzulösen. Jedoch kann auf Grund von vorgegebenen Netzwerkregeln und Richtlinien nicht jedes Interface direkt adressiert werden. Deswegen sendet Mercator zusätzlich noch alias-probes über Source-Routing-Router, um somit eine größere Anzahl an Interfaces zu erreichen.

4.4 Ergebnisse und Bewertung

Um Mercator zu testen, ließen die Entwickler das Programm drei Wochen lang laufen. Bei maximal 15 gleichzeitigen Traceroute-Messungen wurden knapp 150.000 Interfaces und 200.000 Verbindungen gefunden. 16% der Verbindungen wurden durch Source-Routing gefunden. 20.000 Interfaces konnten zu ihren zugehörigen Router aufgelöst werden (3.000 davon über Source-Routing-Router) [9].

Obwohl mit Traceroute-Messungen viele Interfaces gefunden werden konnten, hat Traceroute einige Probleme. So können zum Beispiel, wie in Referenz [4] erläutert, durch Load-Balancer falsche Pfade entstehen, und diese verfälschen somit die Messdaten. Weiterhin ist nicht zugesichert, dass durch Traceroute entstehende ICMP-Fehlermeldungen bei Mercator ankommen. Teilweise sind Firewalls so eingestellt, dass sie diese Meldungen verwerfen und somit der adressierte Router für Mercator als unerreichbar erscheint.

Um den Adressbereich für die Messungen einzuschränken, verwendet Mercator die Technik „informed random address probing“. Um die Effizienz dieser Technik zu messen, haben die Entwickler von Mercator die gefundenen Adressblöcke mit den Adressblöcken eines Backbone Routers verglichen. Dabei wurden nur 8% der Präfixe im Backbone Router von Mercator nicht gefunden. Wohingegen 20% Präfixe gewählt wurden, die wiederum nicht im Backbone Router vorhanden waren. Dies ist jedoch nicht verwunderlich, da durch Annahme zwei, siehe Kapitel 4.3.2, immer Nachbarblöcke hinzugenommen wurden. Diese enthalten aber möglicherweise gar keine erreichbaren Adressen.

Um die resultierende Internet-Karte zu validieren, haben die Mercator-Entwickler die Daten mit dem Netzwerk eines lokalen Internet-Service-Providers verglichen. Dabei konnten alle Router und alle Verbindungen, bis auf eine, gefunden werden [9]. Obwohl diese Ergebnisse sehr gut sind, bleibt es fraglich, ob auch in größeren, komplexeren Netzwerken ein ebenso gutes Resultat erzielt werden kann.

Mercator ist jedenfalls nicht in der Lage, von jedem Netzwerk eine komplette Internet-Karte zu erstellen. Es können Router oder Verbindungen existieren, die nicht entdeckt werden. Außerdem können Zusammenhänge, wie zum Beispiel zwei Router, die im selben Rechenzentrum platziert sind, aber nie Daten austauschen, nicht herausgefunden werden. Allerdings kann Mercator die wichtigsten Transit- und Backbone-Router finden und somit den wichtigsten Teil eines Netzwerkes darstellen.

Die resultierende Karte kann auch nicht als Momentaufnahme des Netzwerkes gesehen werden. Die Messungen vollstrecken sich über mehrere Wochen, und in dieser Zeit kann sich das Netzwerk verändern. Somit ist die Karte nur als Zeitdurchschnitt zu sehen [9].

5. VERBESSERTE METHODEN

Die Entwicklung Mercators ist bereits einige Jahre her. In dieser Zeit wurden verschiedene Techniken und Programme entwickelt, die bestehende Techniken Mercators verbessern.

Zum Standard-Traceroute-Programm, wie es auch Mercator in einer ähnlichen Form implementiert, gibt es bereits Alternativen. Paris-Traceroute ist eine Traceroute-Implementierung, die die Probleme mit Load-Balancern umgehen kann [3, 4]. Um die zunehmende Problematik mit Firewalls zu vermeiden, kann das Tool tcptraceroute [14] eingesetzt werden. Dieses verwendet anstatt ICMP-Pakete TCP Pakete. Diese sind an Port 80 adressiert, der bei fast allen Webservern geöffnet ist.

Mercators Alias-Auflösung basiert nur auf dem Fakt, dass viele Router Pakete über ein Standard-Ausgangsinterface versenden. Sollte ein Router dieser Regel nicht folgen, kann Mercator diesem Router Interfaces nicht zuordnen. Alternativ kann das Tool RadarGun [6] Alias auflösen, in dem es das Identification Feld des IP Headers betrachtet. RadarGun ist somit nicht auf das Verhalten der Router angewiesen.

6. ZUSAMMENFASSUNG

Internet-Karten bieten eine gute Möglichkeit, die Übersicht über die Struktur des Internets zu behalten. Die Daten für solche Karten können durch einfache Traceroute-Messungen generiert werden. Allerdings sind diese Karten niemals vollständig und fehlerfrei. Zusätzlich sind die Messungen sehr aufwändig und zeitintensiv, weshalb diese immer über einen längeren Zeitraum hinweg durchgeführt werden müssen.

Mercator bietet einfache Techniken, um möglichst effizient Internet-Karten zu erstellen. Bei kleinen, lokalen Teilnetzwerken gelingt dies Mercator sehr gut, ob es auch bei größeren Teilen des Internets eine relativ vollständige Karte liefert, bleibt fraglich.

Durch neuere, verbesserte Techniken könnte Mercator kor-

rektere Ergebnisse liefern. Es gibt einige aktuellere Tools, die bereits solche Techniken einsetzen. Derzeit wird auch am Lehrstuhl für Netzarchitekturen und Netzdienste der TU München eine Mess-Infrastruktur namens IStruktA entwickelt, die der Generierung von Internet-Karten dient. IStruktA bietet zu den normalen Traceroute-Messungen noch die Möglichkeit an, Messungen von beliebigen Rechnern zu starten. Somit können Internetbenutzer rund um den Globus selbstständig Messungen von ihrem Rechner aus durchführen. Dieser neuartige Ansatz verspricht zusätzliche Daten, die zu einem verbesserten Ergebnis bei Internet-Karten führen können [10].

7. LITERATUR

[1] S. S. Ands. Discovering internet topology.

[2] R. Atkinson. Security architecture for the internet protocol. Technical report, 1998.

[3] B. Augustin, X. Cuvellier, B. Orgogozo, F. Viger, T. Friedman, M. Latapy, C. Magnien, and R. Teixeira. Avoiding traceroute anomalies with paris traceroute. In *In Proc. Internet Measurement Conference*, 2006.

[4] B. Augustin, T. Friedman, R. Teixeira, U. Pierre, and M. Curie. Multipath tracing with paris traceroute. In *in Proc. Workshop on End-to-End Monitoring (E2EMON*, 2007.

[5] S. Bajaj, L. Breslau, D. Estrin, K. Fall, S. Floyd, P. Haldar, M. Handley, A. Helmy, J. Heidemann, P. Huang, S. Kumar, S. McCanne, R. Rejaie, P. Sharma, K. Varadhan, Y. Xu, H. Yu, and D. Zappala. Improving simulation for network research. Technical Report 99-702b, University of Southern California, March 1999. revised September 1999, to appear in IEEE Computer.

[6] A. Bender, R. Sherwood, and N. Spring. Fixing ally's growing pains with velocity modeling.

[7] CAIDA. Skitter. Online verfügbar unter http://www.caida.org/tools/measurement/skitter; besucht 24. Juni 2010.

[8] A. Danesh, , A. Danesh, L. Trajkovic, S. H. Rubin, and M. H. Smith. Mapping the internet, 2001.

[9] R. Govindan and H. Tangmunarunkit. Heuristics for internet map discovery, 2000.

[10] T. M. Lehrstuhl für Netzarchitekturen und Netzdienste. Istrukta. Online verfügbar unter http://istrukta.net.in.tum.de; besucht 24.Juni 2010.

[11] W. g. Matthew Luckie. scamper. Online verfügbar unter http://www.caida.org/tools/measurement/scamper; besucht 24.Juni 2010.

[12] G. Phillips, S. Shenker, and H. Tangmunarunkit. Scaling of multicast trees: Comments on the chuang-sirbu scaling law, 1999.

[13] N. Spring, R. Mahajan, and D. Wetherall. Measuring isp topologies with rocketfuel. In *In Proc. ACM SIGCOMM*, pages 133–145, 2002.

[14] M. C. Toren. tcptraceroute. Online verfügbar unter http://michael.toren.net/code/tcptraceroute; besucht 24. Juni 2010.