Integration von Sensornetzen ins Internet

Ingmar Kessler
Betreuerin: Corinna Schmitt
Seminar Future Internet WS2010/2011
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: kesslein@in.tum.de

KURZFASSUNG

Menschen und Maschinen benötigen Informationen, um Entscheidungen zu treffen, weshalb die Computerisierung und Automatisierung des Sammelns von Informationen durch Sensornetze großes Potential bietet. Sensornetze sind WLAN-Netzwerke aus mit Sensoren bestückten, günstigen, batteriebetrieben Mikro-Computern. Mit Hilfe von mehr und besseren Informationen können bessere Entscheidungen getroffen werden, sei es in Umweltfragen, im Krankenhaus oder zu Hause im Intelligenten Haus. Die gesammelten Informationen werden umso wertvoller, wenn man sie nicht nur an einem lokalen Rechner einsehen kann, sondern global über das Internet auf sie zugreifen kann. In Bezug auf Sensornetze ergeben sich durch die Anbindung an das Internet einige spezifische Herausforderungen in Sachen Effizienz, Zuverlässigkeit und Sicherheit. Im Folgenden sollen einige Ansätze und Techniken vorgestellt werden, die zeigen dass die genannten Herausforderungen überwindbar sind.

Schlüsselworte

Drahtloses Sensorsystem, Internet, 6LoWPAN, Sicherheit

1. EINLEITUNG

Die von Sensornetzen gelieferten Informationen lassen sich für vielerlei Zwecke nutzen. So können in einem Intelligenten Haus zum Beispiel Temperatur- und Lichteinstrahlungsdaten genutzt werden, um die Energieeffizienz des Hauses zu steigern, Sensoren können als Alarmanlage fungieren und ältere Menschen können von der Automatisierung des Hauses und dem Sammeln von gesundheitsrelevanten Informationen profitieren. Es macht Sinn, solche Sensornetze nicht nur in einem lokalen Netzwerk zu betreiben, sondern mit dem Internet zu verbinden. Zum Beispiel können ältere Menschen länger alleine, selbst bestimmt und sicher in ihrem eigenen Zuhause wohnen, wenn ihre Ärzte, Krankenhäuser und Verwandten global Zugriff auf diese häuslichen und gesundheitsrelevanten Informationen haben.

Der globale Zugriff auf Sensornetze und ihre Informationen stellt eine neue Herausforderung in Sachen Technik, Standardisierung, Benutzerfreundlichkeit und Zuverlässigkeit dar. Aber das wohl essentiellste Problem stellen die Fragen der Datensicherheit, Zugriffskontrolle und des Schutzes vor böswilligen Angriffen dar, denn umso wichtiger die Daten sind, die von Sensornetzen gesammelt werden, desto wichtiger ist es, sie vor unbefugtem Zugriff zu schützen.

In den folgenden Kapiteln soll gezeigt werden, wie diese Ziele trotz der technischen Einschränkungen von Sensornetzen erreicht werden können. Im nächsten Kapitel werden zuerst die grundlegenden Eigenschaften von Sensornetzen betrachtet und im Kapitel 3 werden mögliche Arten der Internetanbindungen vorgestellt. Im 4. Kapitel wird es um eine IPv6-Implementation für den Gebrauch innerhalb von Sensornetzen gehen und das 5. Kapitel wird auf einige Sicherheitsaspekte in Bezug auf Sensornetze und ihre Internetanbindung eingehen. Kapitel 6 soll einen Ausblick auf eigenständige Sensoren liefern, die direkt an das Mobilfunknetz angeschlossen werden. Anschließend folgt eine Zusammenfassung der Ergebnisse.

2. EIGENSCHAFTEN VON SENSORNETZEN

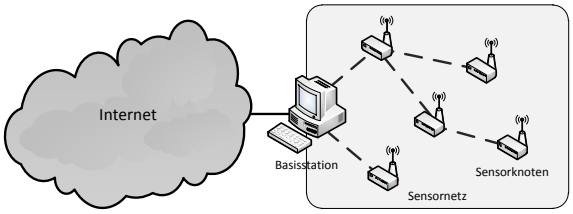

Abbildung 1: Aufbau eines Sensornetzes [1][3]

Sensornetze bestehen aus zwei Arten von Geräten: Einer Vielzahl von Sensorknoten, die Umweltdaten messen, und einer oder mehreren Basisstationen, an welche die gesammelten Daten übermittelt werden und die gegebenenfalls die zentrale Konfiguration übernimmt.

Sensorknoten sind kleine, leistungsschwache und günstige Geräte, die im Wesentlichen nur aus einem frei programmierbaren Rechenbaustein, einer WLAN-Antenne, einer Batterie und mindestens einem Sensor bestehen und von ihren Ressourcen her hauptsächlich der Klasse II aus Tabelle 1 zugeordnet werden können [1]. Ihr Zweck, als Datenquellen im Sensornetz, besteht allein darin die Sensordaten aufzunehmen und zu speichern, bis sie erfolgreich an die Basisstation übertragen wurden. Dabei können die Sensorknoten dauerhaft und in Echtzeit ihre Umwelt messen und so kontinuierliche Messreihen erstellen oder auch nur das Einhalten von bestimmten Schwellenwerten überprüfen und gegebenenfalls Alarm schlagen. Ebenso können sie nur bei Bedarf Messungen einholen oder sogar über ihre eigentliche Messfunktion hinausgehen und mit Aktuatoren statt Sensoren aktiv in ihre Umwelt eingreifen. Für die Datenübertragung müssen die Sensorknoten dabei nicht direkt mit der Ba-

doi: 10.2313/NET-2011-05-2_02

Tabelle 1: Klassifizierung von Sensorknoten [1]

Klasse	Taktrate	RAM	ROM	Energie
I	4 Mhz	1 kB	4-16 kB	1.5 mA
II	4-8 Mhz	4-10 kB	48-128 kB	2-8 mA
III	13-180 Mhz	256-512 kB	4-32 MB	∼40 mA

sisstation verbunden sein, sondern sie können mittels eines WLAN-Netzwerkes (meistens IEEE 802.15.4) über mehrere andere Knoten hinweg eine Verbindung mit der Basisstation aufbauen, was ihre Reichweite erhöht bzw. den Energiebedarf ihrer WLAN-Antennen senkt. Ein großer Vorteil von Sensorknoten ist, dass sie weder auf ein Daten- noch auf ein Stromkabel angewiesen sind und deshalb leicht überall platziert werden können, einschließlich entlegenen, unzugänglichen oder gefährlichen Orten. Die freie Platzierung im Raum bedeutet natürlich auch, dass sie über keine dauerhafte Stromquelle verfügen und dementsprechend auf Batterien angewiesen sind. Aufgrund der Arbeitskosten, die mit dem Batteriewechsel verbunden sind [8], und den giftigen bzw. schwierig zu entsorgenden Altbatterien wird auch an kleinen Stromquellen geforscht [2], die den Batteriewechsel überflüssig machen sollen. Momentan jedoch ist es notwendig nach einigen Tagen bis einigen Jahren [1] die Batterien der Sensorknoten auszutauschen, was natürlich entgegen des Ziels der automatischen Messung durch Sensornetze ist. Um diese Energieeffizienz, die ein ständiges Forschungsgebiet ist, überhaupt erst zu erreichen, sind einige Einschränkungen an die Rechenleistung notwendig. Außerdem werden aufgrund des hohen Strombedarfs einer WLAN-Antenne beim Senden, Empfangen und selbst nur beim passiven Lauschen die Antennen oft die meiste Zeit ausgeschaltet und nur sporadisch aktiviert um die gesammelten Daten zu senden bzw. weiter zu senden [3].
Basisstationen, die der Klasse III aus Tabelle 1 entsprechen, werden üblicherweise am Stromnetz betrieben und fungieren als Datensenke für das Sensornetz und als Router, die bei der Installation oder beim Ausfall eines Sensorknotens das Netzwerk automatisch konfigurieren. Diese automatische Konfiguration, welche die Sensorknoten auch teilweise selbstständig durchführen können, ist ein weiterer Reiz von Sensornetzen. Durch sie wird die Benutzerfreundlichkeit und die Redundanz des Netzes beim Ausfall einzelner Knoten gesteigert und damit auch die mit einer Sensornetz-Installation verbunden Personalkosten gesenkt. Die Basisstation kann wiederum an das Internet angeschlossen werden oder der Nutzer kann an ihr direkt die Messdaten ablesen.

3. ARTEN DER INTERNETANBINDUNG

Die Integration von Sensornetzen in das Internet kann Sinn machen, um mehr Menschen Zugriff auf die Daten zu gewähren oder um an Orten zu messen, an denen sich keine Menschen befinden. So werden Sensornetze in Island zur Gletschermessung und Klimaforschung verwendet [10] und in Nationalparks können sie bei Waldbränden die Reaktionszeiten der Löschkräfte senken [4]. Aufgrund der Beschränkungen von Sensornetzen und des Fehlens von Standards bietet die Internetanbindung von Sensornetzen einige spezielle Herausforderungen und Lösungen.

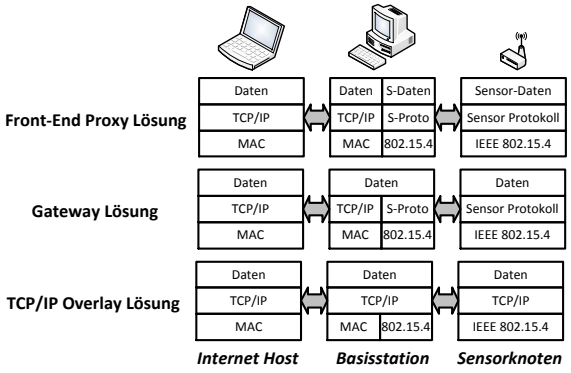

Abbildung 2: Integrationsstrategien von Sensornetzen ins Internet [1]

3.1 Front-End Proxy Lösung

Bei der Front-End Proxy Lösung gibt es keine direkten Verbindungen zwischen dem Internet und den Sensorknoten, sondern die Basisstation arbeitet als Interface und interpretiert die Kontrollbefehle und schickt sie dann an die Sensorknoten weiter. In der Gegenrichtung arbeitet die Basisstation zudem als Cache-Server und speichert die Sensorinformationen, die sie zum Beispiel als Web-Server dem Internet zur Verfügung stellt. Der große Vorteil daran ist, dass das Sensornetz damit nicht Teil des Internets ist und eigene Protokolle und Algorithmen verwenden kann. Zudem wird durch die strikte Trennung zwischen Internet und Sensornetz das Sicherheitsproblem auf das eines gewöhnlichen Web-Servers reduziert [1].

3.2 Gateway Lösung

Bei der Gateway Lösung kann das Sensornetz weiterhin eigenständige und anwendungsoptimierte Protokolle verwenden, aber eine Daten-Verbindung zwischen Internet-Hosts und Sensorknoten wird ermöglicht. Dies geschieht, indem die Basisstation auf der Anwendungsebene als Gateway fungiert und mittels einer Übersetzungstabelle Nachrichten und Adressen der darunterliegenden Schichten zum Beispiel von TCP/IP in ein spezialisiertes Protokoll übersetzt [1].

3.3 TCP/IP Overlay Lösung

Bei der TCP/IP Overlay Lösung verwenden die Sensorknoten TCP/IP, weshalb die Basisstation fast nur noch als gewöhnlicher Router fungieren muss und die Sensorknoten Teil des Internets werden und somit direkt mit Internet-Hosts Pakete austauschen können [1]. Da die Sensorknoten nur über geringe Ressourcen verfügen, wird das Sensornetz zwar IP-kompatibel betrieben, aber es werden sparsamere Protokolle wie 6LoWPAN verwendet, weshalb es notwendig ist, dass die Basisstation Standard-IPv4- bzw. Standard-IPv6-Pakete übersetzt. Ein weiterer Vorteil der TCP/IP Overlay Lösung, neben der direkten Kommunikation zwischen beliebigen Internet-Hosts und Sensorknoten, ist die Verwendung eines standardisierten und optimierten Protokolls wie IPv6, aus dem sich hoffentlich eine standardisierte und kompatible Art der Internetanbindung von Sensornetzen entwickelt.

doi: 10.2313/NET-2011-05-2_02

4. IP-BASIERENDE SENSORNETZE

Es macht für Sensornetze offensichtlich Sinn ein IP-Protokoll für die Kommunikation zwischen Knoten zu verwenden, wenn das Sensornetz mittels einer TCP/IP Overlay Lösung Teil des standardisierten und allumspannenden Internets werden soll. Aber auch Sensornetz-intern kann es gute Gründe geben, ein standardisiertes Protokoll wie IPv6 zu verwenden. So können die Entwicklungskosten gesenkt oder die Kompatibilität zwischen den Modellen verschiedener Generationen bzw. Hersteller verbessert werden. Zusätzlich handelt es sich bei IPv6 um ein ausgereiftes und sauber entworfenes Protokoll, dessen Leistungsfähigkeit sich auch mit anwendungsspezifischen Protokollen im Bereich der Sensornetze messen kann [3].

4.1 Gründe für IPv6

Hersteller und Anwender von Sensornetzen haben lange Zeit IPv4 und IPv6 zu Gunsten von anwendungsspezifischen Protokollen gemieden [3], was sich auf die geringen Ressourcen von Sensorknoten und den Wunsch nach anwendungsspezifischen Optimierungen zurückführen lässt. Auch spielte die große Anzahl an Knoten und der damit verbundene, nicht vertretbare Aufwand bei einer manuellen Konfiguration eine wichtige Rolle. Der Vorteil von IPv6 gegenüber IPv4 ist natürlich der größere Adressraum, der es theoretisch erlaubt, an jeden Sensorknoten eine eigene IP zu vergeben. Zudem wurden Protokolle wie ARP und DHCP Teil von IPv6 und erlauben zusammen mit Autoconf und ICMPv6 eine sparsame, automatische Konfiguration des Sensornetzes [3]. IPv6 bietet eine generalisierte, funktionsreiche Struktur um viele Anforderungen eines Sensornetzes zu erfüllen und wo Sensornetz-spezifische Lösungen notwendig sind, bietet es auch die notwendige Erweiterbarkeit beispielsweise über ein flexibles Header-Format.

4.2 IPv6 für Sensornetze

Obwohl IPv6 grundlegend für Sensornetze geeignet ist, ist es dennoch notwendig IPv6 für Sensornetze anzupassen, um ihr volles Potential auszuschöpfen. Deshalb soll hier die IPv6-Implementation namens 6LoWPAN vorgestellt werden, das von einer herstellerunabhängigen IETF Working Group entwickelt wird. Mit einem ROM-Bedarf von 24 kB und einem RAM-Bedarf von 4 kB [3] ist es auch auf Geräten mit geringen Ressourcen lauffähig ist und bietet trotzdem einen Grad an Zuverlässigkeit, Energieeffizienz und Allgemeinheit, der sich durchaus mit Sensornetz-spezifischen Protokollen messen kann [3]. Die Verwendung einer angepassten IPv6-Implementation ist nicht allein wegen den Header- und MTU-Größen notwendig, wird dort aber wohl am deutlichsten: Sensorknoten verwenden den WLAN-Standard 802.15.4, der nur Pakete mit maximal 127 Bytes unterstützt, und bei einem MAC-Header von maximal 25 Bytes, einer 128-Bit AES-Verschlüsselung, die 21 Bytes benötigt, einem IPv6-Header mit standardmäßig 40 Bytes und einem UDP-Header mit 8 Bytes bleiben nur 33 Bytes für die eigentlichen Daten übrig [5]. Nebenbei wird von IPv6-fähigen Geräten erwartet, dass sie eine Paketlänge von mindestens 1280 Bytes unterstützen, weshalb (IPv6-)Pakete, die länger als (81 bzw.) 127 Bytes sind, im Sensornetz ankommen können und auf der Sicherungsschicht fragmentiert werden müssen [5]. Das Header-Kompressionsverfahren von 6LoWPAN verwendet keinen expliziten Kontext, d.h. die Verbindungspartner müssen vor der Datenübertragung nicht erst die Art der Kompression aushandeln. Stattdessen ist die Kompression kontextfrei bzw. sie verwendet einen impliziten Kontext, indem angenommen wird, dass alle Knoten im Sensornetz ausschließlich 6LoWPAN verwenden. Damit kann der Overhead eines UDP/IP-Pakets von 48 Bytes auf 6 bis 25 Bytes reduziert werden. Dies geschieht, indem im IPv6-Header nur häufig verwendete Werte erlaubt werden, wie zum Beispiel dass Version "6" und Traffic Class und Flow Label "0" sein müssen und der nächste Header nur UDP, TCP oder ICMPv6 sein darf [3]. Zudem werden redundante Daten wie die Länge des Paketinhalts aus dem IPv6-Header entfernt und aus dem MAC-Header errechnet. Es werden außerdem, wenn möglich, kürzere IP-Adressen verwendet, die nur lokal gültig sind.

Neben der Header-Kompression wird das Router Advertisement im IPv6-Standard so modifiziert, dass Konfigurationsinformationen von Routern, d.h. Basisstationen, nicht nur an direkte Nachbarn sondern über mehrere Knoten hinweg verbreitet werden. Um einen hohen Netzwerk-Overhead zu vermeiden, werden in einem Trickle-Verfahren bei Änderungen bzw. neuen Informationen Router-Advertisement-Pakete häufiger (weiter-)verschickt und seltener wenn die Netzwerk-Konfiguration lange unverändert bleibt. DHCPv6 erlaubt eine automatische Adresskonfiguration für alle Sensorknoten, indem die Knoten ihre Anfragen an den zentralen Router verschicken und über mehrere anderen Knoten hinweg ihre Antwort erhalten.

Um eine möglichst hohe Energieeffizienz und Netz-Robustheit zu erreichen, werden Nachrichtenübertragungen auf einer Knoten-zu-Knoten-Basis behandelt. Dies bedeutet, dass die Vermittlungsschicht bei jedem Paketverlust neu evaluieren kann, ob wieder an den gleichen Knoten weitergesendet werden soll oder ob eine neue Route gewählt werden soll. Zudem wird ein Streaming-Prinzip verwendet, bei dem ein Sender auf dem ersten Datagramm kennzeichnen kann, ob sofort weitere Pakete folgen, weshalb nicht erneut die Verbindungskonditionen ausgehandelt werden müssen. Dadurch wird eine höhere Übertragungsrate erreicht, die es den Knoten erlaubt, mehr Zeit im Schlafmodus zu verbringen und so Energie zu sparen. Eine Stau-Kontrolle wird wiederum durch ein 'additive-increase and multiplicative-decrease'-Verfahren und indem Pakete nie fallen gelassen werden erreicht, wodurch bei einer vollen Warteschlange ein Rückstau über alle Knoten hinweg entsteht [3].

Das Routing in einem Sensornetz stellt eine besondere Herausforderung dar, da die Verbindungsqualität zwischen den Knoten und selbst ihre Positionen im Raum sehr variabel sein können. Zudem verfügen die Knoten nicht über genug Rechenleistung für komplexe Vermessungsverfahren und Extra-Traffic zum Auskundschaften des Netzwerkes ist zu vermeiden. Da man sich den damit verbundenen Energieverbrauch nicht leisten kann, werden die optimalen Routen oft nur mit eingeschränkten Informationen geschätzt. Die Basisstation unterhält eine Route zu jedem Sensorknoten, während die Knoten selbst nur die direkten Nachbarn kennen und eine Default-Route für die Basisstation und alle anderen Ziele unterhalten. Die Knoten und die Basisstation speichern dabei zu jedem Zeitpunkt nicht nur eine Route, sondern testen mehrere Alternativ-Routen gleichzeitig. Dabei senden sie einen Großteil ihrer Pakete über die Default-Route, die am billigsten ist und bei der die Zuversicht über die Kostenabschätzung am höchsten ist. Die restlichen Pakete werden über die Alternativ-

doi: 10.2313/NET-2011-05-2_02

Routen versendet, um ihre Zuversicht zu erhöhen und wenn möglich eine bessere Default-Route zu finden. Da das Sensor-Netzwerk nicht statisch ist, werden mit den Paketen die erwartete Anzahl der Hops und die benötigten Übertragungsversuche mit versandt. Eine Abweichung in der Anzahl der Hops kann auf eine Schleife hindeuten, während eine Abweichung in der Anzahl der benötigten Übertragungsversuche bedeuten kann, dass es sich um eine (in)effiziente Route handelt.
Da dem Sensornetz ein kompatibles IPv6-Protokoll zur Verfügung gestellt wird, können bis auf die Header-Komprimierung standardmäßige Transportprotokolle wie TCP und UDP verwendet werden.

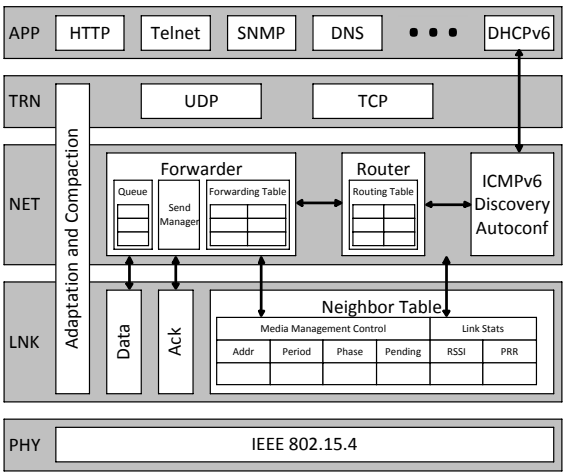

Abbildung 3: IP-Stack der Sensorknoten [3]

5. SICHERHEITSASPEKTE

Wenn Sensornetze mit oder ohne Internetanbindung in Zukunft eine tragende Rolle in militärischen bzw. zivilen Anwendungen spielen sollen, ist es notwendig sie vor störenden Umwelteinflüssen und Angriffen zu schützen. So sind zum Beispiel Sensornetze, die bei der Koordination von Rettungskräften helfen sollen, nutzlos oder sogar gefährlich, wenn sie keine Erdbeben oder Stürme überstehen können. Gleiches gilt für sicherheitskritische Sensornetze, die zur Kontrolle von Fahrzeugen, Produktionsanlagen, der Infrastruktur oder als Sicherheitssysteme für wichtige Gebäude verwendet werden und von Angreifern leicht ausgeschaltet werden können. Es ist schwierig, wenn auch nicht unmöglich, Sensornetze zu schützen, bei denen Angreifer physikalischen Zugriff zu einem oder mehreren Sensorknoten besitzen. Aber auch gegenüber Angreifern, die keinen physikalischen Zugriff besitzen, ist es wichtig einige Sicherheitsmaßnahmen zu treffen.
Für den sicheren Betrieb eines Sensornetzes sind innerhalb und außerhalb des Netzes vier wesentliche Punkte wichtig: Verschlüsselung gegen Abhörversuche, Authentifizierung gegen Angreifer, die sich als legitime Nutzer, Sensorknoten oder Basisstationen ausgeben, Autorisierung gegen unberechtigten oder für eingeschränkten Zugriff und Protokollierung um die Verantwortlichkeit von Nutzern zu garantieren. Selbst mit den geringen Ressourcen eines Sensorknotens ist eine 128-Bit AES-Verschlüsselung im WLAN bzw. eine SSL-Verschlüsselung zwischen einem Internet-Host und dem Sensornetz möglich [1], auch wenn dadurch natürlich der Rechen-, Speicher- und Energieverbrauch in einem gewissen Rahmen erhöht wird. Innerhalb des Sensornetzes kann die Authentifizierung und Autorisierung durch Public Key Kryptographie bzw. Zertifikate zumindest in kleinen Netzen sichergestellt werden. Dabei stößt man aber schon an die Grenzen der Leistungsfähigkeit von Klasse II Sensorknoten [1] und zudem wird die automatische Konfiguration durch den Austausch von Zertifikaten erschwert.
Die sichere Kommunikation zwischen Sensorknoten und dem Internet ist dagegen schwieriger herzustellen, da einerseits leichter größere Angriffe gestartet werden können, weshalb stärkere Verfahren notwendig sind und andererseits sehr viel mehr Authentifizierungs-, Autorisierungs- und Protokollierungsdaten gespeichert werden müssen, was die Speichergrenzen von typischen Sensorknoten sprengt. Aus diesem Grund kann es Sinn machen, die Leistungsfähigkeit und den zur Verfügung stehenden Speicher von Sensorknoten zu erhöhen, was auch anderen Funktionen und anderen Sicherheitsaspekten zu Gute kommen würde. Dadurch würden aber allerdings einige Vorteile von Sensorknoten wie ihr geringer Preis und ihre lange Batterielaufzeit, die sie durch ihren geringen Ressourcenbedarf erlangen, wieder verschwinden. Eine andere Alternative wäre zum Beispiel die Schlüssel dezentral unter den Knoten im Sensornetz zu verteilen [1], was allerdings kompliziert und wenig robust gegenüber dem Ausfall anderer Knoten ist und dem Gedanken von Sensorknoten als eigenständigen Internet-Hosts wiederum entgegen läuft.
Da sparsame Sensorknoten in jedem Fall den Betrieb einer leistungsfähigeren Basisstation notwendig machen, sei es auch nur zur Umwandlung von IPv4- oder IPv6-Paketen in 6LoWPAN-Pakete, macht es Sinn die schon gegebene Abhängigkeit weiter auszunutzen. So können aufwendige Aufgaben auf die Basisstation ausgelagert werden [1] und die Basisstation kann gegebenenfalls auch Funktionen weiter auf einen zentralen Web-Server auslagern. Die Gefahr einer Single-Point-of-Failure in der Basisstation wird damit zwar nicht nur aus technischer sondern auch aus sicherheitsrelevanter Sicht erhöht, aber andererseits kann die Basisstation mit ihrer Leistung eine stärkere, zentrale Sicherheit implementieren und unter den gegebenen Umständen erscheint die Lösung als guter Kompromiss. Außerdem ergeben sich weitere Vorteile, wie zum Beispiel dass die Basisstation historische Messdaten der Sensorknoten speichern kann, welche von den Knoten aufgrund des Speichermangels entweder gelöscht, zusammengefasst oder anderweitig komprimiert werden müssten [1]. Zusätzlich kann die Basisstation als Cache-Server agieren und so bei häufigen Anfragen schnelle Antworten liefern und den Sensorknoten so Energie sparen oder auch beim Ausfall eines Sensorknotens zumindest historische Daten und Fehlerdiagnoseinformationen liefern.
Diese Art der zentralen Sicherung eines Sensornetzes ist bei der Front-End Proxy Lösung besonders einfach, da die Basisstation auf standardmäßige und lange Zeit im Internet erprobte Verfahren für die sichere Kommunikation zwischen zwei gleichwertigen Internet-Hosts setzen kann und das Internet und das Sensornetz streng getrennt werden [1]. Aber auch bei der Gateway und der TCP/IP Overlay Lösung sind Hybrid-Verfahren denkbar, welche die Basisstation als 'Gatekeeper' einsetzen.

doi: 10.2313/NET-2011-05-2_02

5.1 DoS-Angriffe

Denial of Service (DoS) bedeutet, dass das Sensornetz seine zugewiesene Funktion nicht mehr erfüllen kann, was zum Beispiel durch eine zu große Anzahl gleichzeitiger, legitimer Nutzer oder durch den Ausfall von zu vielen Knoten durch Umwelteinflüsse passieren kann. Hier sollen aber bewusste Angriffe betrachtet werden, die darauf abzielen die Funktion eines Sensornetzes zu mindern oder komplett zu stören.

DoS-Angriffe können auf mehreren Schichten stattfinden, wobei ein Angriff auf physikalischer Ebene aus einem simplen Radiostörsender bestehen kann [6]. Die Existenz eines Störsenders ist leicht durch hohe und unablässige Aktivität auf der entsprechenden Frequenz zu erkennen. Die Knoten innerhalb des Störgebietes können nur versuchen, auf anderen, hoffentlich ungestörten Frequenzen oder auf mehreren Frequenzen gleichzeitig zu senden, was für Sensorknoten mit ihren geringen Ressourcen schwierig ist. Der Störsender kann auch nur kurze Störimpulse senden, was zu Übertragungsfehlern und somit zum erneuten Versenden von Paketen führt, wodurch die Batterien der Sensorknoten schnell geleert werden. Durch die kurzen Störimpulse spart der Störsender auch Strom und kann damit länger senden bzw. kleiner gebaut werden. Auch hier können die Sensorknoten die Störung nicht beseitigen, sondern nur mittels bestimmter Verfahren mindern [6]. Falls das Störgebiet nicht das gesamte Sensornetz umfasst, können Knoten außerhalb des Gebietes versuchen um das Gebiet herumzusenden und so den Ausfall des Sensornetzes möglichst gering zu halten. Da die Sensorknoten also nur eingeschränkt gegen das Störsignal vorgehen können, muss die endgültige Beseitigung des Störsignales erfolgen, indem man den Störsender findet und ausschaltet.

Auf der Transportschicht kann ein Sensorknoten oder eine Basisstation gestört werden, indem ihre Ressourcen durch einen Angreifer aufgebraucht werden, der unzählige Verbindungen aufbaut, sie aber nicht nutzt. Falls der Angreifer und das Opfer über ähnliche Leistung verfügen, kann das Opfer von potentiellen Kommunikationspartnern verlangen, ein Puzzle zu lösen, das leicht zu erstellen, aber schwer zu lösen ist, bevor eigene Ressourcen für den Verbindungsaufbau verwendet werden [6]. Legitime Kommunikationspartner verfügen über ausreichend Ressourcen um einige Puzzle zu lösen, was den Overhead zwar ein wenig erhöht, aber Angreifer, die versuchen hunderte bis hunderttausende Verbindungen aufzubauen, stoßen bald an ihre eigenen Leistungsgrenzen. Die Stärke des Puzzles kann auch mit dem Ausmaßdes Angriffs wachsen und so einerseits unnötigen Overhead vermeiden und andererseits stärkeren Angriffen widerstehen.

5.2 Firewalls

Firewalls können Computern, besonders solchen mit Internetanschluss, helfen sich vor ungewollter Kommunikation und Einbruchsversuchen zu schützen, weshalb Hardware- und Software-Firewalls Teil jedes Computers mit Internetanschluss sein sollten. Basisstationen von Sensornetzen bieten aufgrund ihrer ausreichenden Ressourcen eine Plattform, auf der Firewalls ein Sensornetz effektiv schützen können. Der Einsatz von Firewalls, die oft eine beträchtliche Menge an Rechenzeit benötigen, auf Sensorknoten scheint dagegen aufgrund der geringen Rechenleistung und Stromversorgung der Knoten als unrealistisch. Dennoch würden sie eine weitere Mauer zum Schutz der Sensorknoten bieten, falls die Firewall auf der Basisstation versagen sollte oder falls der Angriff nicht über das Internet sondern direkt über das WLAN erfolgen sollte. Diese Art des Angriffs ist damit zwar nicht spezifisch für Sensornetze mit Internetanbindung, aber es wird sie dennoch genauso betreffen und in unkontrollierbaren ländlichen und urbanen Gebieten werden wohl insbesondere Sensornetze mit Internetanschluss eingesetzt werden.

Die geringen Ressourcen von Sensorknoten sind zwar ein Hindernis für den Einsatz von Firewalls, aber die Entwicklung der AEGIS-Firewall [9] hat gezeigt, dass man die Vorteile von Firewalls auch auf beschränkten Geräten nutzen kann. Die AEGIS-Firewall ist in der Lage den ein- und ausgehenden Traffic eines Sensorknotens mit Hilfe einer kontextfreien Regelbasis zu filtern, welche die Sender- und Empfängeradresse, die Richtung und das sendende und empfangende Modul umfasst. Sie ist auf Sensorknoten lauffähig, da die entworfenen Regeln nicht in einer Datei auf dem Sensorknoten gespeichert werden und bei jedem Filtervorgang aufwendig geladen und ausgewertet werden müssen. Stattdessen erfolgt zuerst auf einem PC ein aufwendiger Optimierungsvorgang, bei dem die Regeln zuerst auf Konfliktfreiheit hin untersucht werden und dann als Ganzes zusammen mit der Firewall in speziell optimierten Bytecode kompiliert werden, der, nur als Beispiel, die Verschwendung von Rechenzeit durch redundante Regeln vermeidet. Eine erste Version der Firewall wurde schon erfolgreich in einem Sensornetz getestet, wobei sie nur 2.9 kB ROM-Speicher [9] benötigte. Sie verfügt zwar noch nicht über die Funktionen moderner Firewalls und IP-Spoofing stellt noch eine Schwachstelle dar, aber sie zeigt, dass Sensorknoten aufgrund ihrer geringen Ressourcen nicht kategorisch auf moderne Sicherheitstechniken verzichten müssen.

6. GPRS-SENSOREN

Mit Hilfe von Basisstationen können Sensorknoten viele Aufgaben und Funktionen eines Sensors bzw. Sensornetzes auslagern, wodurch sie mit geringen Ressourcen auskommen. Dadurch erreichen sie eine geringe Größe, geringe Kosten, eine lange Laufzeit der Batterie und zusammen mit der Basisstation ein bestimmtes (automatisches) Konfigurationsschema für das Sensornetz. Durch die Teilnahme eines Sensorknotens an einem solchen Sensornetz geht er jedoch auch eine geographische und funktionale Abhängigkeit zu einer Basisstation ein, die zu einem Single-Point-of-Failure wird. Zudem ist er für die Übertragung seiner Daten auch an das korrekte Funktionieren anderer räumlich naher Sensorknoten angewiesen. Auch aus Sicht der Konfiguration kann es Sinn machen, viele unabhängige, möglicherweise identische Sensoren, die direkt mit dem Internet verbunden sind, statt einem komplexen Sensornetz zu betreiben.

Beispielsweise bei mobilen und räumlich stark getrennten Sensoren kann es deshalb Sinn machen, sie eigenständig zu verwenden. Wie in den vorangegangen Kapiteln, insbesondere bei der TCP/IP Overlay Lösung, gezeigt wurde, reichen die beschränkten Ressourcen von typischen Sensorknoten aus, um sie als eigenständige Internet-Hosts zu betreiben. Außerdem sind auch geringe Erweiterungen der Ressourcen für weitere Funktionalitäten insbesondere in Anbetracht des ständigen technischen Fortschritts in der Computerbranche realistisch. Da die Sensoren und Rechenbausteine der Sensorknoten damit also weitgehend identisch zu denen in typischen Sensornetzen sein können, ist noch die Kommunikation

doi: 10.2313/NET-2011-05-2_02

mit dem Internet zu betrachten. Eine Internetanbindung über WLAN scheint aufgrund der großen Entfernungen bzw. des Mangels an Wireless Hotspots unrealistisch, weshalb die Verwendung des Mobilfunknetzes, das insbesondere in urbanen Umgebungen praktisch überall verfügbar ist, als passende Alternative erscheint. In der Tat wird GPRS schon als Alternative für die Festnetzanbindung von Sensornetzen an das Internet verwendet [4] und es gibt schon erfolgreiche Implementationen von eigenständigen Sensoren, die per GPRS mit einem zentralen Server im Internet kommunizieren und mit Hardware arbeiten, die ähnlich zu derer von gewöhnlichen Sensorknoten ist [7].
Eine offene Frage bleibt jedoch, ob sich die Kommunikation solcher Sensoren mit Hilfe eines GPRS-Modems energieeffizient genug gestalten lässt, um mit der von Sensorknoten erreichten Batterielaufzeit mithalten zu können. Dies ist besonders relevant, da es einige Anwendungsgebiete von Sensornetzen gibt, für die eine Batterielaufzeit von bis zu mehreren Jahren dringend erforderlich ist. Es ist außerdem klar, dass für die Mobilfunknetze eine geringe Anzahl von GPRS-Sensoren unerheblich ist, aber es ist fraglich, ob sie mehrere Millionen wenn nicht gar mehr verkraften können. Auch stellt sich die Frage, ob die Mobilfunkbetreiber willig sind passende Entgeltungspläne für Geräte mit einem geringen Datenaufkommen wie GPRS-Sensoren zu erstellen. Insbesondere für sicherheitskritische Sensoren, die zum Beispiel die Infrastruktur einer Stadt überwachen, ist es außerdem fraglich, ob Mobilfunknetze, die bei Großereignissen oder Katastrophen oft überlastet sind, eine ausreichende Zuverlässigkeit bieten können.
Bedingt durch diese Hindernisse macht es Sinn sich aufgrund einer Anforderungsanalyse für ein Sensornetz oder GPRS-Sensoren zu entscheiden. Natürlich können beispielsweise durch technische Entwicklungen, die eine höhere Batteriekapazität bzw. sparsamere GPRS-Modems ermöglichen, oder durch die Integration von Energiequellen wie zum Beispiel Solarzellen in die GPRS-Sensoren die möglichen Laufzeitprobleme gelöst werden. Die Belastung der Mobilfunknetze könnte auch gesenkt werden, indem die Sensoren auf eine GPRS-Verbindung verzichten und sich falls möglich in einem ad-hoc WLAN-Sensornetz zusammenschließen.
Die grundsätzliche Eignung von GPRS-Sensoren für bestimmte Anwendungen wurde schon gezeigt [7] und so können die Nützlichkeit und die Anwendungsgebiete von GPRS-Sensoren durch technische Entwicklungen und weitere Forschungen nur erweitert werden.

7. ZUSAMMENFASSUNG

Das große Interesse an Sensornetzen in der Forschung und in der technischen Entwicklungsgemeinde zeugen von der wichtigen Rolle, die Sensornetze im Alltag, in der Wirtschaft und in der Wissenschaft spielen werden. Aber schon heute gibt es weitreichende Produkte und Standards für Sensornetze im Heim- und Büroeinsatz für das Energiemanagement, im medizinischen Einsatz, für die Sicherung von ziviler Infrastruktur wie Brücken, für die Prozesssteuerung in der Fertigungstechnik, in der Automobilindustrie und in der Rohstoffförderung [8].
Ein Teil der wachsenden Bedeutung von Sensornetzen ist ihre Anbindung an das Internet und wie hier verdeutlicht wurde, ist die Umsetzbarkeit schon durch praktische Implementationen gezeigt worden, die auch schon teilweise im Produkteinsatz sind [8]. Es wurden ebenso durchaus relevante Implementierungs- und vor allem Sicherheitsaspekte angesprochen, die zwar schon Teillösungen besitzen, aber immer noch einigen Forschungs- und Entwicklungsbedarf besitzen. Aufgrund des anhaltend großen Volumens an Forschung im Bereich von Sensornetzen und des Marktwertes, ist zu erwarten, dass es keine größeren Hindernisse bei der Verbreitung von Sensornetzen mit Internetanbindung geben wird und dass alle Probleme mittelfristig zufriedenstellend gelöst werden können.

8. LITERATUR

[1] Rodrigo Roman, Javier Lopez, (2009) "Integrating wireless sensor networks and the internet: a security analysis", Internet Research, Vol. 19 Iss: 2, pp.246 - 259

[2] Robert Bogue, (2009) "Energy harvesting and wireless sensors: a review of recent developments", Sensor Review, Vol. 29 Iss: 3, pp.194 - 199

[3] Hui, J. W. and Culler, D. E. 2008. IP is dead, long live IP for wireless sensor networks. In Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems (Raleigh, NC, USA, November 05 - 07, 2008). SenSys '08. ACM, New York, NY, 15-28. DOI= http://doi.acm.org/10.1145/1460412.1460415

[4] Santos, Jorge and Santos, Rodrigo and Orozco, Javier, (2009) "On the Feasibility of Early Detection of Environmental Events through Wireless Sensor Networks and the Use of 802.15.4 and GPRS", GeoSensor Networks, Vol. 5659, pp.122 - 130, Springer Berlin / Heidelberg

[5] Montenegro, et al., "IPv6 over IEEE 802.15.4", RFC 4944, IETF, September 2007

[6] A. D. Wood and J. Stankovic, (2002) "Denial of Service in Sensor Networks", IEEE Computer, Vol. 35 Iss: 10, pp.54 - 62

[7] A. R. Al-Ali, Imran Zualkernan, Fadi Aloul, (2010) "A Mobile GPRS-Sensors Array for Air Pollution Monitoring", IEEE Sensors Journal, Vol. 10 Iss: 10, pp.1666 - 1671

[8] Robert Bogue, (2010) "Wireless sensors: a review of technologies, products and applications", Sensor Review, Vol. 30 Iss: 4

[9] Hossain, Mohammad and Raghunathan, Vijay, (2010) "AEGIS: A Lightweight Firewall for Wireless Sensor Networks", Distributed Computing in Sensor Systems, Vol. 6131, pp.258-272

[10] Martinez, Kirk and Hart, Jane and Ong, Royan, (2009) "Deploying a Wireless Sensor Network in Iceland", GeoSensor Networks, Vol. 5659, pp.131 - 137

doi: 10.2313/NET-2011-05-2_02