Sicherheit in DTN-basierten ÖPNV-Netzen

Johannes Morgenroth und Lars Wolf

IBR, Technische Universität Braunschweig
Mühlenpfordtstraße 23, Braunschweig, Germany
{morgenroth|wolf}@ibr.cs.tu-bs.de

1 Einleitung

Eine flächendeckende Erfassung verschiedener Sensordaten im städtischen Bereich ist in vielerlei Hinsicht von großem Nutzen. Beispielsweise lassen sich so Schadstoffe in der Luft feingranular messen, um die Bevölkerung umfassender zu informieren und das Verkehrsmanagement zu optimieren. Öffentliche Verkehrsmittel verkehren regelmäßig und annähernd im gesamten Stadtgebiet, wodurch sie sich sehr gut für diesen Zweck eignen. Gleichzeitig können so auch Betriebsdaten von technischen Anlagen entlang des Streckenverlaufs erfasst werden.

Das Konzept eines Delay Tolerant Network (DTN) [2] bietet die Möglichkeit zur Realisierung einer leistungsfähigen Vernetzung zur zeitnahen Auswertung der gesammelten Daten, ohne dabei auf die Nutzung von kostenaufwändigen Mobilfunklösungen angewiesen zu sein. Da einzelne Knoten in Bewegung sein können, wird in einem DTN davon ausgegangen, dass eine ununterbrochene Ende-zu-Ende Kommunikation, wie sie in stationären Computernetzen vorhanden ist, grundsätzlich nicht gegeben ist. Mit Hilfe von intelligenten Wegewahlmechanismen [1], können Datenpakete (Bündel) bei einem sporadisch stattfindenden Kontakt gezielt weitergegeben werden bis diese schließlich ihr Ziel erreichen.

In einem Kooperationsprojekt zwischen der Firma BBR Verkehrstechnik und dem Institut für Betriebssysteme und Rechnerverbund der TU Braunschweig wird im Rahmen des Projekts OPTraCom[1] ein neuartiges, unterbrechungstolerantes Kommunikationssystem auf WLAN-Basis entwickelt, welches Daten mit Hilfe des Öffentlichen Personen Nahverkehrs (ÖPNV) transportiert.

2 Anwendungsszenarien

Die Knotenbewegungen und die sporadischen Kontakte führen zwangsläufig zu Latenzen bei der Ende-zu-Ende Übertragung. Dabei kann es sich um Sekunden, Minuten oder sogar Stunden handeln. Nicht jedes Szenario ist für ein derartiges Netz geeignet, aber bei bestimmten Anwendungen können solche Verzögerungen toleriert werden. Für zeitkritische Anwendungen ist eine ergänzende Bereitstellung von alternativen Übertragungskanälen denkbar.

Ein mögliches Szenario stellt die flächendeckende Aufnahme von Messwerten dar [3]. Dabei sollen an Fahrzeugen angebrachte Sensoren in regelmäßigen Abständen Messwerte mit Positionsdaten verknüpfen und dadurch eine sehr hohe Abdeckung mit nur wenigen Sensoren erzielen. Die gesammelten Daten werden mit Hilfe des DTNs zeitnah zur Auswertung an eine Senke übertragen.

Als weiteres Szenario in diesem Projekt ist die Vernetzung von Fahrgastinformationssystemen geplant. Diese Systeme bedürfen regelmäßiger Versorgung mit neuen Fahrplänen, Multimediainhalte, Werbeanzeigen und Softwareaktualisierungen. Derartige Daten sind zeitunkritisch und enthalten potenziell größere Mengen an Daten.

3 Architektur / Plattform

Im wesentlichen besteht ein DTN aus mobilen Netzknoten, die sich in diesem Fall auf Fahrzeugen befinden. Unterstützend können noch stationäre Netzknoten, an strategisch interessanten Punkten aufgestellt werden, um die Netzkapazität zu steigern oder die Latenz zu verringern. Stationäre Knoten können dabei optional über eine kabelgebundene Vernetzung verfügen, welche einen Transport zu einem Datenzentrum (z.B. Senke) oder in einen anderen Teil des Netzes ermöglicht.

Die Hardware eines Netzknotens besteht aus einer eingebetteten Plattform (Ubiquiti Routerstation Pro), welche mit einem Wifi Modul (IEEE 802.11a/b/g) ergänzt worden ist. Zukünftig sollen die Knoten zusätzlich mit einer Zigbee Schnittstelle erweitert werden, um auch mit energiereduzierten Geräten kommunizieren zu können. Als Softwareplattform wird die OpenWRT Distribution verwendet. Diese basiert auf dem Linux Kernel und einer schlanken Standard-Bibliothek (uclibc), welche für eingebettete Systeme gut geeignet ist. Als Basissoftware wurde IBR-DTN [4] entwickelt, ein für eingebettete Plattformen optimierter Netzwerkstack für DTNs basierend auf dem Bundle Protocol (RFC5050).

Netzknoten für Fahrzeuge und stationäre Netzknoten

[1] http://www.optracom.de/

unterscheiden sich nicht wesentlich bezüglich ihrer Ausstattung. Lediglich die äußeren Komponenten wie das Gehäuse, die Art der Stromversorgung und die Auswahl der Antenne, wurden an die Gegebenheiten angepasst.

4 Sicherheit

Neben Vandalismus ist ein derart exponiertes Netz durch den Einsatz von drahtlosen Kommunikationstechnologien einer Vielzahl von Angriffsmöglichkeiten ausgesetzt, welche das Netz kurzzeitig stören oder sogar auf Dauer schädigen können. Eine Analyse hat neben Jamming des Funkkanals auch DDoS-Attacken und Softwarelücken als besonders kritisch eingestuft. Um den Knoten vor böswilligen Attacken zu sichern wurden Penetrationstests und Werkzeuge entworfen mit denen das System während der Entwicklung bezüglich des Risikos klassifiziert werden kann.

Zum Schutz der drahtlosen Netzwerkschnittstelle eines Netzknotens sollen Verschlüsselungsverfahren verwendet werden, welche das Netz gegenüber unbefugten Dritten unzugänglich macht. Bei der Betrachtung der gängigen Verfahren für IEEE 802.11 wurde festgestellt, dass diese entweder unsicher oder nicht für den Betrieb im Ad-Hoc Modus geeignet sind. Daher wurde eine Kombination aus Wired Equivalent Privacy (WEP) und einem Virtual Private Networking (VPN) Ansatz gewählt. WEP gilt zwar als unsicher, bietet aber dennoch eine Hürde, die eine unbeabsichtigte Störung des Netzes verhindert. Für den Fall dass ein Angreifer die WEP Verschlüsselung überwindet, wird zwischen den Knoten ein Ad-Hoc-fähiges VPN eingesetzt, welches die gesamte Netzwerkkommunikation auf Ebene der Vermittlungsschicht schützt. Durch den zusätzlichen Einsatz einer Firewall reagiert der Netzknoten lediglich auf Verbindungsanfragen zum VPN.

Über den Grundschutz hinaus bietet das als Erweiterung spezifizierte Bundle Security Protocol weitere Sicherheitsfunktionen, welche unter anderem eine Ende-zu-Ende Kommunikation absichern können. Für die übertragenen Bündel gibt es die Möglichkeit diese mittels eines symmetrischen Schlüssels zu authentifizieren und je nach Richtlinie Bündel zu akzeptieren oder zu verwerfen. Weiterhin existieren Möglichkeiten die zu transportierenden Daten für ein bestimmtes Ziel zu verschlüsseln oder vor dem Versand zu signieren. Dabei werden Kombinationen aus symmetrischen und asymmetrischen Verfahren verwendet, um eine hohe Sicherheit bei gleichzeitig hoher Leistung zu gewährleisten.

4.1 Aktualisierungsstrategie

Alle bisherigen Sicherheitsverfahren basieren auf statischen Schlüsseln und Zertifikaten. In einem DTN stellt die Aktualisierung und der Widerruf von Zertifikaten eine besondere Herausforderung dar, denn ein Zertifikat kann nicht bei jeder Verwendung auf Widerruf geprüft werden. Zur Verteilung von neuen Zertifikaten und Widerrufslisten ist daher ein mehrstufiges System gefragt, welches die Integrität des Netzes sicherstellt.

Zur Behebung von Fehlern in der Software oder Ergänzung von neuen Funktionen, ist ebenfalls eine Aktualisierungsstrategie notwendig. Mittels eines 4-Stufen-Systems sollen neue Softwarerevisionen auf bereits im Betrieb befindliche Netzknoten verteilt werden. Dazu wird in einem Testbed der Aktualisierungsvorgang zuerst mit einer Teilmenge der Netzknoten erprobt. Dabei soll sichergestellt werden, dass ein Mischbetrieb von Netzknoten mit der neuen und der vorhergehenden Revision zu keiner Störung führt. Ist eine solche Erprobung erfolgreich, wird die Aktualisierung auf eine Teilmenge des Produktivnetzes ausgeweitet und bei Erfolg alle Netzknoten aktualisiert.

5 Ausblick

Alle bisherigen Sicherheitsmechanismen schützen das Netz bereits vor unbefugtem Zugriff. Sollten jedoch vertrauliche Informationen oder sogar ein ganzer Netzknoten in die Hände Dritter gelangen, dann könnte das Netz zumindest in begrenztem Umfang gestört werden.

Derzeit wird ein möglicher Sink-Hole Angriff auf das Netzwerk untersucht. Dabei gibt sich ein Netzknoten für den Empfänger von bestimmten Bündeln aus und verwirft diese anschließend, so dass die Bündel niemals ihr Ziel erreichen. Da das Bundle Protocol selbst bisher keinen Mechanismus bietet einen solchen Angriff zu verhindern, wird für diesen Fall in einer anderen Arbeit ein präventiver Mechanismus entwickelt.

Literatur

[1] M. Doering, T. Pögel, and L. C. Wolf. DTN routing in urban public transport systems. In *ACM MobiCom 2010 Workshop on Challenged Networks (CHANTS 2010)*, Chicago, USA, 9 2010.

[2] K. Fall. A delay-tolerant network architecture for challenged internets. 2003.

[3] S. Lahde, M. Doering, W.-B. Pöttner, and G. Lammert. Mobile and Distributed Measurement of Air Pollution in Metropolitan Areas Using Car2X Techniques. In *Proceedings of 3nd Symposium on Informationssysteme für mobile Anwendungen (IMA)*, Braunschweig, October 2006.

[4] S. Schildt, J. Morgenroth, W.-B. Pöttner, and L. Wolf. Ibr-dtn: A lightweight, modular and highly portable bundle protocol implementation. *Electronic Communications of the EASST*, 37:1–11, Jan 2011.