Sicherheit in ereignisorientierten, drahtlosen Sensornetzen

Nicolai Schmittberger, Norman Dziengel

Freie Universität Berlin
Computer Systems & Telematics Group
nicolai.schmittberger@fu-berlin.de
norman.dziengel@fu-berlin.de

Art der Arbeit: Diplomarbeit
Betreuer/in der Arbeit: Prof. Dr.-Ing. Jochen H. Schiller

Abstract: Bestehende Sicherheitssysteme können in drahtlosen Sensornetzen (WSNs) entweder nicht alle Sicherheitsanforderungen abdecken und/oder sind zu aufwendig, als dass sie realistisch eingesetzt werden können. Diese Arbeit stellt ein eigenes Sicherheitssystem, *PaRSec*, für WSNs vor, das mit adäquatem Aufwand alle Sicherheitsanforderungen abdeckt. Zu diesem Zweck wird eine Definition der Sicherheitsanforderungen auf Basis der aktuellen Literatur gegeben und die vorhandenen Sicherheitssysteme auf ihre diesbezügliche Leistung hin untersucht. Es wird ein Konzept präsentiert, dass die Problempunkte der vorhandenen Systeme – Schlüsselverwaltung, Vollständigkeit und Aufwand – löst und eine dynamische Anpassung des Sicherheitslevels einführt. PaRSec wurde in einem Labor- und Feldtest untersucht. Die Evaluation der Latenz und des Durchsatzes zeigt, dass trotz der Abdeckung aller Sicherheitsanforderungen ein derart geringer Mehraufwand benötigt wird, dass die Praxistauglichkeit von PaRSec gegeben ist.

1 Motivation und Problemstellung

Drahtlose Sensornetze (WSNs) [Aky02] bestehen aus einzelnen Sensorknoten, die mittels Sensoren Daten der unmittelbaren Umwelt erfassen und diese per drahtloser Kommunikation mit ihren Nachbarn und/oder einer Basisstation austauschen können. Ereignisorientierte WSNs überwachen die unmittelbare Umgebung auf den Auftritt bestimmter Ereignisse und melden diese an eine zentrale Basisstation. Sie finden in immer mehr Bereichen wie z.B. Frühwarnsysteme für Naturkatastrophen [Sch07], [Rud06], zur Patientenüberwachung [Han06] oder beim Grenzschutz [Dzi10] Einsatz. Der Bedarf an Sicherheit für ereignisorientierte WSNs, der durch die Übertragung sicherheitsrelevanter Informationen und für die Aufrechterhaltung der Funktionalität des WSNs entsteht, kann bisher nur ungenügend abgedeckt werden. Aktuell verfügbare Sicherheitssysteme erfüllen entweder nicht alle Anforderungen oder sind durch ihren hohen Aufwand nicht realistisch einsetzbar. Bereits das Schlüsselaustauschverfahren, das die Grundlage jedes Sicherheitssystems darstellt, ist ein bis heute noch nicht zufriedenstellend gelöstes Problem [Liu05]. Aufgrund der bekannten und für WSNs typischen Ressourcenbeschränkung

		SPINS	SSNfPP	TinySec	PaRSec
Anforderungen	➢ Vertraulichkeit	✓	✓	✓	✓
	➢ Authentizität	✓	✓	✓	✓
	➢ Integrität	✓	-	✓	✓
	➢ Aktualität	✓	✓	-	✓
	➢ Sem. Sicherheit	✓	✓	✓	✓
	➢ Schlüsselverwalt.	✓	✓	-	✓
Aufwand	➢ Kommunikation	⬆	⬇	➡	⬈
	➢ Speicherbedarf	⬆	➡	➡	➡
	➢ Synchronisierung	⬆	⬆	⬇	⬇
Umsetzg.	➢ Konzept	✓	✓	✓	✓
	➢ Simuliert	✓ (teilw.)	✓	✓	✓
	➢ Implementiert	-	-	✓	✓

Abb. 1: Vergleich der Ansätze mit PaRSec

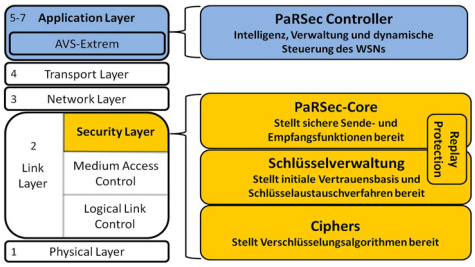

Abb. 2: Konzept der Sicherheitsschicht

kann die Vereinbarung eines gemeinsam geteilten Geheimnisses nicht über die in kabelgebundenen Netzen gängigen Public-Key Verfahren bzw. das Diffie-Hellmann Verfahren stattfinden [Per01].

2 Sicherheit in Drahtlosen Sensornetzen

Zur genaueren Analyse der vorhandenen Ansätze und ihrer Sicherheitsleistung bedarf es einer Definition der Sicherheit in drahtlosen Sensornetzen. Nach der aktuellen Literatur [Çay09], [Kar04], [Dut04], [Ava03], [Per01] und [Car00] lassen sich die folgenden Anforderungen benennen: **Vertraulichkeit, Integrität, Authentizität, Aktualität und Semantische Sicherheit.** Können alle Anforderungen gewährleistet werden, ist ein System als sicher zu bezeichnen. Die Erfüllung aller Anforderungen bewirkt jedoch bisher eine derartige zusätzliche Ressourcenbelastung der Sensorknoten durch Kommunikation, Speicherauslastung und Synchronisierung, dass die Praxistauglichkeit der Systeme nicht gezeigt werden konnte.
Der vorhandene Ansatz *SPINS* [Per01] wurde für eine universelle Einsetzbarkeit entwickelt, unterstützt jedoch die allgemeine Broadcastkommunikation nicht. Für die Abdeckung aller Sicherheitsanforderungen werden neben einer Zeitsynchronisierung ebenfalls eine Counter-Synchronisierung und eine Counter-Statushaltung benötigt. Dadurch entsteht ein in der Praxis vermutlich nicht mehr realisierbarer Mehraufwand der oben beschriebenen und in Abb. 1 dargestellten Ressourcen. Mangels einer Implementierung lässt sich dies allerdings nicht überprüfen.
Der Ansatz *Secure Sensor Networks for Perimeter Protection (SSNfPP)* [Ava03] ist ein speziell auf die Geländesicherung ausgelegtes Sicherheitssystem. Die hohe Spezialisierung auf diese Aufgabe ermöglicht ein relativ leichtgewichtiges System, das nur durch die nötige Zeitsynchronisierung belastet wird. Es beschränkt die universelle Einsetzbarkeit u.a. auf zwei Hops und vernachlässigt zudem die Abdeckung der Integritätsanforderung. Für die Kommunikation mit der Basisstation werden paarweise und globale Schlüssel eingeführt. Hierbei wird der paarweise Schlüssel jedes Sensorknotens immer mit der Basisstation geteilt und der globale Schlüssel nur für die Weiterleitung von Paketen verwendet. Dieses Prinzip wird in der hier vorgestellten Arbeit weiterentwickelt.
TinySec [Kar04] wurde für TinyOS entwickelt und ist auf eine universelle Einsetzbarkeit ausgerichtet. TinySec präsentiert eine leichtgewichtige Sicherheitsschicht, die durch ihre quelloffene Implementierung anpassbar ist. Die Aktualitätsanforderung und die Schlüsselverwaltung bleiben dem Benutzer zur Implementierung offen, wodurch jedoch ein Kernproblem der Sicherheit in WSNs ungelöst bleibt.

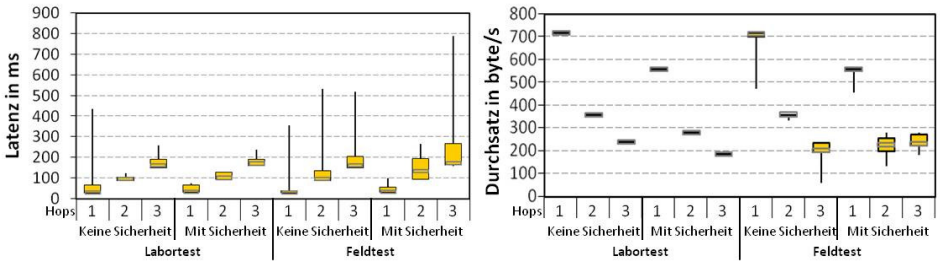

Abb. 3: Ergebnisse der Latenz- und Durchsatz-Tests mit und ohne Sicherheitssystem

3 Konzept und Umsetzung

Die für das hier vorgestellte Sicherheitssystem, *PaRSec*, entwickelte Schlüsselverwaltung beruht auf dem in [Dut04] vorgestellten Prinzip der Vereinbarung sicherer paarweiser Schlüssel auf der Basis eines nur kurzzeitig gültigen, gemeinsam geteilten, globalen Geheimnisses. Aufgrund der kurzen Gültigkeit dieses Geheimnisses kann es als sicher betrachtet werden. Auf den sicheren paarweisen Verbindungen aufbauend wird ein neuer sicherer globaler Kanal erstellt, über den die Kommunikation im Regelfall stattfindet.
Für die Umsetzung der Sicherheitsanforderungen kommt ein symmetrisches Blockverschlüsselungsverfahren im CBC-Modus [NIS98] für die Vertraulichkeit, ein Message Authentication Code (MAC) für die Authentizität und Integrität, ein Counter für die Aktualität und ein Initialisierungsvektor für die Semantische Sicherheit zum Einsatz. Dies ist in Abb. 2 durch die gelb gefärbten Komponenten dargestellt. Des Weiteren kommt mittels des in Abb. 2 dargestellten, blau markierten Controllers eine dynamische Anpassung des Sicherheitslevels an die aktuelle Sicherheitssituation zum Einsatz. Eine ebenfalls im Controller vorhandene Angriffserkennung liefert die dafür notwendigen Informationen über die aktuelle Sicherheitssituation. Verschiedene Sicherheitsvoreinstellungen bieten dem Anwender die Möglichkeit die Sicherheitsschicht an den individuellen Sicherheitsbedarf anzupassen
Trotz der Abdeckung aller Sicherheitsanforderungen werden keinerlei Synchronisierungs- oder Statushaltungsverfahren eingesetzt, wodurch das System leichtgewichtig und in der Praxis einsetzbar bleibt. Dies wird erreicht indem das eingesetzte Schlüsselaustauschverfahren sowie der Paketwiedereinspielschutz bewusst ohne derartige Mechanismen entwickelt wurden. Das Streaming von Sensordaten kann aufgrund des im Vergleich zur Ereignisorientierung starken Datenverkehrs nicht berücksichtigt werden.

4 Auswertung

Für die hier vorgestellte Arbeit werden derzeit die Verschlüsselungsalgorithmen SkipJack, RC5, AES, TwoFish und 3DES unterstützt. Eine Analyse der Algorithmen zeigte, dass der AES-Verschlüsselungsalgorithmus die beste Performance bietet. Lediglich der RC5 Algorithmus konnte eine noch bessere Performance zeigen, ist aber aufgrund von Sicherheitsmängeln [Kel00] und eines Patentschutzes für den Einsatz nicht zu empfehlen. Ein Labortest mit 10 und ein Feldtest mit 28 ARM7-basierten AVS-Extrem-

Sensorknoten [Sch10] haben gezeigt, dass die Sicherheitsschicht die Abdeckung aller Sicherheitsanforderungen mit adäquatem Mehraufwand realisieren kann. Wie in Abb. 3 dargestellt, wird die Performance des Gesamtsystems in Hinblick auf die Netzwerklatenz und den Datendurchsatz nur um ca. 10% bzw. ca. 25% negativ beeinflusst. Im Vergleich zu den hier aufgeführten verwandten Arbeiten SPINS, SSNfPP und TinySec kann sich PaRSec durch Vollständigkeit und Praxistauglichkeit hervorheben. Das System ist damit die erste vollständig implementierte, dynamisch reagierende und alle Sicherheitsanforderungen mit adäquatem Aufwand abdeckende Sicherheitsschicht, die für drahtlose Sensornetze entwickelt wurde und stellt damit neben einem wissenschaftlichen Mehrwert ein in der Realität einsetzbares System dar.

Literaturverzeichnis

[Aky02] Akyildiz, I., Su, W., Sankarasubramaniam, Y., Cayirci, E.; *Wireless Sensor Networks: A Survey*. Computer Networks., 2002.

[Ava03] Avancha, S., Undercoffer, J., Joshi, A., Pinkston, J. 2003. *Secure sensor networks for perimeter protection.* s.l. : Elsevier B.V., 2003.

[Car00] Carman, D., Kruus, P., Matt, B. 2000. *Constraints and Approaches for Distributed Sensor Network Security.* [Technical Report] Glenwood, MD, USA : NAI Labs, 2000.

[Çay09] Çayırcı, E., Rong, C. *Security in Wireless Ad Hoc and Sensor Networks.* Chichester, West Sussex, United Kingdom : John Wiley & Sons, Ltd., 2009.

[Dut04] Dutertre, B., Cheung, S., Levy, J. *Lightweight Key-Management in Wireless Sensor Networks by Leveraging Initial Trust.* [Technical Report] Menlo Park, CA, USA : System Design Laboratory - SRI International, 2004.

[Dzi10] Dziengel, N., Ziegert, M., Kasmi, Z., Hermans, F., Adler, S., Wittenburg, G., Schiller, J. *A Platform for Distributed Event Detection in Wireless Sensor Networks.* Proc. of CONET 2010.

[Han06] Hande, A., Polk, T., Walker, W., Bhatia, D. *Self-Powered Wireless Sensor Networks for Remote Patient Monitoring in Hospitals*. Sensors. 6, 2006.

[Kar04] Karlof, C., Sastry, N., Wagner, D. *TinySec: a link layer security architecture for wireless sensor networks.* SenSys '04: Proc. of the 2nd international conference on Embedded networked sensor systems, Baltimore, MD, USA : ACM, 2004.

[Kar05] Karl, H., Willig A. *Protocols and Architectures for Wireless Sensor Networks.* West Sussex, England : John Wiley & Sons Ltd., 2005.

[Kel00] Kelsey, J., Ferguson, N., Schneier, B., Stay, M. *Cryptanalytic Progress: Lessons for AES.* Gaithersbourg, PA, USA : National Institute of Standards and Technology, 2000.

[Liu05] Liu, D., Ning, P., Li, R. *Establishing Pairwise Keys in Distributed Sensor Networks.* NC, USA : North Carolina State University, 2005.

[NIS98] NIST, National Institute of Standards and Technology. *SKIPJACK and KEA Algorithm Specifications.* [FIPS 185] Gaithersbourg, PA, USA, 1998.

[Per01] Perrig, A., Szewczyk, R., Wen, V., Culler, D., Tygar, J. *SPINS: security protocols for sensor networks.* MobiCom '01: Proc. of the 7th annual international conference on Mobile computing and networking, Rome, Italy, 2001.

[Rud06] Rudloff, A., Lauterjung, J., Zschau, J. *Der Deutsche Beitrag zur Einrichtung eines Tsunami-Frühwarnsystems*. Notfallvorsorge (Walhalla-Verlag). 1/2006, 2006.

[Sch07] Schmidt, M. *SLEWS - A Sensorbased Landslide Early Warning System*. Department of Engineering Geology and Hydrogeology, RWTH Aachen University, 2007.

[Sch10] Schmittberger, N. *Security in Event-Driven Wireless Sensor Networks* [Diplomarbeit], Freie Universität Berlin, 2010.