# Sicherheit in Sensornetzen am Beispiel von SWARMS

Stefan Schmidt, Carsten Buschmann und Stefan Fischer
TU Braunschweig, Institut für Betriebssysteme und Rechnerverbund
Mühlenpfordtstr. 23, D-38106 Braunschweig
{schmidt|buschmann|fischer}@ibr.cs.tu-bs.de

Viele Forschungsarbeiten über Sicherheit in Sensornetzen gehen von recht unterschiedlichen Prämissen aus. Für generischere Ansätze muss man auf spezifische Forderungen wie Geräte mit besonderen Fähigkeiten (z.B. leistungsfähige Prozessoren) oder Basisstationen verzichten und auf gleichwertige Geräte setzen, die dynamisch unterschiedliche Aufgaben übernehmen können, wobei jedwede Kommunikation zwischen den Knoten drahtlos geschieht. Die Vermeidung komplexer und zerbrechlicher logischer Hierarchien wie netzweite Baumstrukturen oder zentrale Instanzen verbessert Skalierbarkeit und Robustheit. Um die Kosten pro Gerät niedrig zu halten, muss momentan auch auf physikalisch manipulationssichere Geräte verzichtet werden.

In dieses Umfeld ist auch das SWARMS-Projekt einzuordnen. In diesem wird untersucht, inwieweit die Programmierung von problemorientierten Anwendungen für gemeinsam operierende Schwärme von mobilen, funkvernetzten Sensorknoten auf der Basis eines Read/Write-Kooperationsparadigmas unterstützt werden kann [2]. Die Lösung vieler Anwendungsprobleme setzt eine globale oder mindestens regionale Sicht auf die eigene Umgebung voraus. Daher fußt die Kooperation der Knoten in SWARMS auf einem *Virtual Shared Information Space* (VSIS), in dem der Zustand der Umwelt und des Schwarmes selbst beschrieben ist und der in einer Middleware implementiert wird. Dabei verfügt kein System über die gesamte Information des Schwarmes, vielmehr repräsentiert jedes Gerät einen Teilausschnitt des VSIS. Über Mechanismen zur Informationsverbreitung mittels adressenloser Kommunikation (Broadcast) sowie zum Verbergen der Verteiltheit durch Selbstorganisation hinaus soll die Middleware die transparente Programmierung verteilter Anwendungen durch semiautomatische Bewertung und Kontextuierung von Informationen, Informationsaggregation sowie dynamische Aufgabenverteilung unterstützen.

Sensornetze kommen im Allgemeinen in einem unkontrollierbaren, nicht vertrauenswürdigen Umfeld zum Einsatz, woraus sich ein erhöhter Bedarf an Sicherheit ableitet. Hierfür können die gebräuchlichen Sicherheitsprimitive Authentifizierung, Integrität, Vertraulichkeit und Verfügbarkeit auch in Sensornetzen angewendet werden. Ihr Einsatz ist generell auf das Absichern des Netzes gegenüber dem Zugriff Dritter ausgerichtet. Unerlässlich sind Sicherheitsmaßnahmen beispielsweise zum verlässlichen Austausch von Daten, der sicheren Datenaggregation innerhalb des Sensornetzes oder beim Einsatz von mobilem Code. Generell muss dabei beachtet werden, dass durch Sicherheitsmaßnahmen aufgrund der Berechnung immer Latenzzeiten und Energieverbrauch erhöht und eventuell auch zusätzliche Nachrichten zur Koordination der Sicherheitsmaßnahmen im Netz benötigt werden.

Im Bereich mobiler Ad-hoc-Netze werden zahlreiche vielversprechende Sicherheitsansätze diskutiert, die unter anderem die Risiken der inherent unsicheren, drahtlosen Kommunikation und der Probleme, die durch das Fehlen einer Infrastruktur entstehen, betrachten. Grundsätzlich sind in Sensornetzen die gleichen Problemstellungen wie in Ad-hoc-Netzen zu berücksichtigen. Darüber hinaus müssen jedoch weitere wichtige Randbedingungen berücksichtigt werden, was Sicherheitslösungen aus Ad-hoc-Netzen nur bedingt auf Sensornetze übertragbar macht. Vor allem die extrem geringe Leistungsfähigkeit der Sensorknoten hinsichtlich vorhandenem Speicher, Rechenleistung und Energie schließt etliche Sicherheitslösungen aus. So sind zum Beispiel Verfahren, die auf asymmetrischer Kryptographie beruhen, in vielen Sensornetzen nicht nutzbar, da sie hohe Ansprüche an Rechenleistung und Speicherplatz stellt. Weiterhin liegen Sensornetzen dynamische Topologien mit potenziell extrem vielen Knoten zu Grunde. Eine Sicherheitslösung muss somit extrem skalierbar und möglichst selbstadministrierend sein, da beispielsweise das manuelle Einführen eines neuen kryptographischen Schlüssels bei tausenden Sensorknoten nicht effizient gesteuert werden kann. Ebenfalls aus Gründen der Skalierbarkeit und um einen möglichst gleichmäßigen Energieverbrauch der einzelnen Knoten zu erreichen, sollten außerdem Berechnungs- und Verkehrskonzentrationen im Netz vermieden werden. Da weiterhin Messwerte und Ereignisse abhängig von der Anwendung schnell veralten können, müssen sie zeitnah kommuniziert werden, was Sicherheitsmaßnahmen mit langen Berechnungszeiten ausschließt. Schließlich müssen noch Datenaggregation innerhalb des Netzes und der Einsatz mobilen Codes beim Entwickeln einer Sicherheitslösung für Sensornet-

ze berücksichtigt werden.

Obwohl bereits einige Sicherheitsansätze speziell für Sensornetze existieren, berücksichtigt unserer Kenntnis nach kein Ansatz alle der oben genannten Randbedingungen, bzw. es werden Vereinbarungen getroffen, die nicht mit dem SWARMS-Konzept harmonieren. So benötigen manche Ansätze zwingend eine Basisstation, die als zentrale Instanz im Netz sicherheitsrelevante Aufgaben übernimmt [1, 3, 4, 5]. Weiterhin werden teilweise logisch strukturierte Netze gefordert, die dynamisch Hierarchien im Netz bilden [1, 3], oder physikalisch manipulationssichere Geräte [1].

Folglich ist für SWARMS ein generischeres Sicherheitskonzept erforderlich, welches die gegebenen Randbedingungen berücksichtigt. Grundsätzlich müssen immer die spezifischen Einschränkungen von Ad-hoc-Netzen (unsichere Kommunikation, fehlende Infrastruktur, etc.), Sensornetzen (Skalierbarkeit, Echtzeit-Anforderung, etc.) und der einzelnen Knoten (eingeschränkter Speicher, Rechenleistung, Energie, etc.) berücksichtigt werden. Darüber hinaus ist es notwendig, ein flexibles Konzept zu entwickeln, in dem sich der Grad der Sicherheit bei Bedarf variieren lässt. Dies ermöglicht insbesondere einen der Anwendung angepassten Kompromiss zwischen benötigter Sicherheit und dem resultierenden Energieverbrauch. In diesem Zusammenhang differenzieren wir hinsichtlich der beiden Dimensionen *inhaltsbasierte Sicherheit* und *situationsbasierte Sicherheit*. Inhaltsbasierte Sicherheit gründet auf der Prämisse, dass unterschiedliche Inhalte auch unterschiedliche Sicherheitsanforderungen haben. Zum Beispiel hat mobiler Code üblicherweise viel höhere Sicherheitsanforderungen als kommunizierte Messwerte oder Lokationsinformationen. Dies ermöglicht es der Middleware, für unterschiedliche zu kommunizierende Inhalte flexibel verschiedene Sicherheitsgrade festzulegen. Situationsbedingte Sicherheit beschreibt unterschiedliche Sicherheitsanforderungen abhängig vom internen Zustand des Sensornetzes und der Umwelt. Zwei Situationen, in denen für gleiche zu kommunizierende Daten (z.B. Lokationsinformationen der Knoten) verschiedene Grade an Sicherheit wünschenswert sind, sind zum Beispiel die Langzeitüberwachung von Deichen oder die Überwachung der Planung eines terroristischen Anschlages. Hierbei kann die Anwendung den gewünschten Grad der Sicherheit sowohl für anwendungsrelevante Daten, wie auch für Daten, welche die Middleware zur internen Organisation benötigt, festlegen.

Sicherheit in Sensornetzen kommt anwendungsabhängig eine unterschiedlich starke Bedeutung zu. Aus diesem Grund sind wir davon überzeugt, dass aufbauend auf den Basisanforderungen, die immer beachtet werden müssen, ein flexibles Sicherheitskonzept entwickelt werden muss. Denn so kann der optimale Kompromiss zwischen dem benötigten Grad an Sicherheit und dem Energieverbrauch erreicht werden. Zusätzlich sollte dieser Ansatz möglichst generisch sein, um die Anforderungen an ein Sensornetz, bzw. der einzelnen Knoten möglichst gering zu halten.

In dem Vortrag wollen wir zunächst allgemein das Problemfeld der Sicherheit in Sensornetzen beschreiben und Voraussetzungen und Limitationen aufzeigen. Im Hauptteil werden wir dann auf die beiden Paradigmen inhalts- und situationsbedingter Sicherheit eingehen und erste Ideen zu ihrer Umsetzung vorstellen. Dabei soll es sich nicht um die Präsentation fertiger Konzepte handeln. Vielmehr wollen wir erste konzeptionelle Ansätz beschreiben, die im weiteren Projektverlauf simulativ und experimentell evaluiert und weiterentwickelt werden sollen. Auf diese Art und Weise soll eine Diskussion ausgelöst werden, da wir von der Wichtigkeit des Themas überzeugt sind.


[1] Basagni, S. et al., *„Secure Pebblenets"*, MobiHoc 2001.

[2] Fischer, S., Luttenberger, N., *„SWARMS – Software Architecture for Radio-Based Mobile Self-Organizing Systems"*, Projektantrag im Rahmen des DFG-Schwerpunktprogrammes „Basissoftware für selbstorganisierende Infrastrukturen für vernetzte mobile Systeme" (SPP 1140), 2001.

[3] Hu, L., Evans, D., *Secure Aggregation for Wireless Networks*, Workshop on Security and Assurance in Ad-hoc-Networks, 2003.

[4] Perrig, A. et al., *„SPINS: Security Protocols for Sensor Networks"*, MobiCom 2001.

[5] Undercoffer, J. et al., *„Security for Sensor Networks"*, CADIP Research Symposium 2002.