S-CAN: Sicheres Overlay für Sensornetze

Erik-Oliver Blaß, Hans-Joachim Hof, Martina Zitterbart
Institut für Telematik
Universität Karlsruhe
[blass|hof|zit]@tm.uni-karlsruhe.de

Motivation

Kleinst-Computer begleiten uns heute mehr und mehr im Alltag und in gewöhnlichen Gegenständen: „Wearables“ stecken an oder sogar in unserer Kleidung, Büroräume verwalten sich selbstständig, Helligkeits-Sensoren regeln automatisch die Beleuchtung und Temperatur-Fühler steuern Heizungen. Solche Sensoren können drahtlos miteinander kommunizieren und Ad-Hoc Netze bilden. Problematisch sind allerdings klassische Sicherheits-Anforderungen wie Vertraulichkeit und Authentizität an diese Kleinst-Computer. Ihre Ressourcen sind in Bezug auf Speicher und Rechenleistung extrem limitiert, ihre Bandbreite beschränkt, asymmetrische Kryptographie teuer und Batteriestrom allgemein kostbar. Traditionelle Sicherheits-Architekturen sind daher in Sensor-Netzen nur schwer einsetzbar. In dieser Arbeit wird ein Protokoll, „S-CAN“ (Secure Content Addressable Network), zum sicheren Aufbau eines Overlay-Netzes für Sensoren präsentiert, das ermöglicht, Dienste von Sensoren sicher anzubieten, sicher aufzufinden und sicher zu verwenden. Dabei muss der Benutzer in der Lage sein, die Sensoren vor ihrem Einsatz zu personalisieren, ein Anwendungs-Beispiel wäre die Heim-Automatisierung durch Sensoren.

Das Content Addressable Network ist ein P2P-Overlay-Netz, das beispielsweise in File-Sharing Umgebungen oder zur Verwaltung eines verteilten Verzeichnisses Verwendung finden kann. Am Institut für Telematik wird das CAN[1] als Overlay-Netz auf Sensoren eingesetzt und um das S-CAN Protokoll erweitert, so daß abgesicherte Kommunikation zwischen den einzelnen Sensor-Knoten möglich wird.

Die grundsätzliche Idee von S-CAN besteht aus der induktiven Erweiterung des Netzes um zusätzliche Sensoren. Ist das Netzwerk zu einem bestimmten Zeitpunkt mit gewissen Knoten in einem „sicheren“ Zustand, dann muss nach dem Hinzufügen eines weiteren Knotens dieser Zustand erhalten bleiben. Das als Grundlage verwendete CAN-Overlay-Netzwerk enthält Dienst-Namen (wie „Temperatur von Raum A“) sowie zugehörige Adressen von Dienst-Anbietern, den Sensoren. Die in diesem Beitrag vorgestellten neuen Ideen im Kontext von S-CAN sind die Integration eines *Zeugenverfahrens* sowie eines *Mehrheitsentscheids*. Die Nachbarn des neu ins Netz hinzuzufügenden Knotens beweisen ihre Authentizität über ein Zeugenverfahren, Anfragen nach Diensten werden durch Redundanz und Mehrheitsentscheide abgesichert.

Überblick: Content Addressable Network (CAN)

Ein CAN ist eine auf alle am Netz teilnehmenden Knoten verteilte Hash-Tabelle. Jeder Knoten verwaltet eine sog. Zone, einen Teilbereich des kompletten Hash-Wertebereichs einer

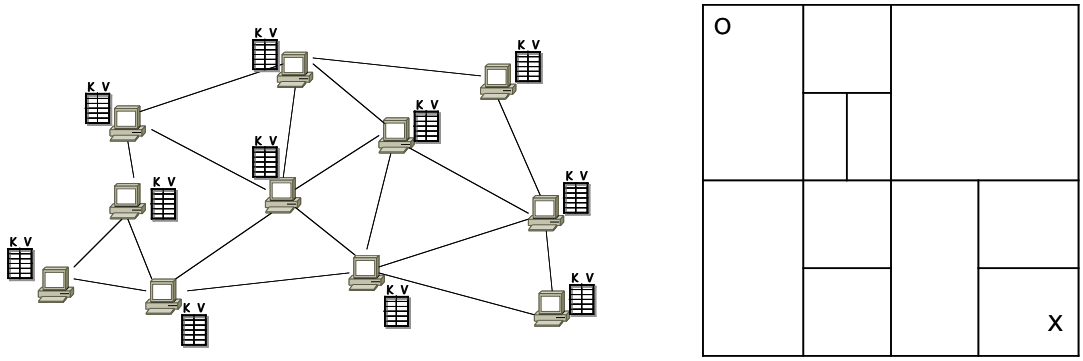

Abbildung 1: a) Verteilte Hash-Tabelle, b) 2-dimensionales CAN

Hash-Funktion *H*. Dies zeigt Abbildung 1a. Die jeweiligen Besitzer einer Zone sind zuständig für das Aufbewahren von (*Schlüssel*, *Wert*)-Tupeln, deren *Schlüssel* in ihrer Zone liegt. Möchte ein Teilnehmer ein (*Schlüssel*, *Wert*)-Tupel im CAN ablegen, so kontaktiert er denjenigen Zonen-Verwalter, der für die Zone, in dem *H*(*Schlüssel*) liegt, verantwortlich ist. CAN beinhaltet ein Routing-Verfahren, das diese Kommunikation ermöglicht. Genauso kontaktiert ein Knoten auf der Suche nach dem zum *Schlüssel* passenden *Wert* den Zonen-Verwalter, der *H*(*Schlüssel*) verwaltet.
Die Hash-Wertebereich wird dabei in d-Dimensionen eingeteilt, Abbildung 1b zeigt ein Beispiel für zwei Dimensionen. Knoten `o` und Knoten `x` verwalten zwei unterschiedliche Zonen der Hash-Funktion. Sie sind über Nachbarn miteinander verbunden. Benachbarte Knoten im CAN verwalten aneinander anliegende Hash-Zonen. Kommt ein neuer Knoten ins Netz, so wird eine vorhandene Zone in zwei Teile aufgebrochen („*split*“). Der alte Zonen-Verwalter und der neue Knoten verwalten dann jeweils die Hälfte der alten Zone.

Die CAN-Funktionalität wird verwendet, um zu Dienste-Beschreibungen Netzwerk-Adressen abzulegen, beispielsweise IP-Adressen oder für Sensor-Netze geeignetere Bluetooth Scatter-Netz-Adressen. Ein Sensor, der einen bestimmten Dienst anbietet, speichert im CAN unter dem Hash-Wert seiner Dienstebeschreibung seine Netzwerk-Adresse ab.

Konzepte von S-CAN
Das Protokoll S-CAN funktioniert induktiv, ausgehend von einem sicheren Zustand wird ein neuer Knoten in das Netz eingefügt („join“), so daß das Netz nach dem „join“ immer noch sicher ist. Das Protokoll verzichtet dabei auf zeitaufwendige Public-Key Operationen, die auf Ressourcen-schwachen Sensoren sehr teuer sind[3].

Die Grundlage für das sichere „join“ in unserem Protokoll ist das sog. „Master-Device“ (MD). Dieses zustandslose Gerät verwendet der Benutzer ausschließlich dafür, um neue Sensoren bewußt in das Netzwerk hinzuzufügen. Das MD ist physikalisch klein, z.B. ein Teil am Schlüsselanhänger des Benutzers. Das MD ist deshalb zustandslos, damit es der Benutzer bei Beschädigung durch ein äquivalentes Gerät von einem sicheren Aufbewahrungsort ersetzen kann. Will der Benutzer seinem Netz einen neuen Sensor hinzufügen, so wird dieser mittels des MD personalisiert. Dies geschieht durch einen „location limited channel“, einen sicheren Übertragungskanal, beispielsweise physikalischer Kontakt. Im Moment des Kontaktes kann das MD Geheimnisse auf dem neuen Sensor sicher abspeichern: jeder Sensor bekommt eine zufällige ID und einen nur vom MD direkt aus der ID ableitbaren symmetrischen Schlüssel S_{ID}. Da kein Zustand auf dem MD vorgehalten werden muß, bedeutet dies niedrige Anforderungen an dessen Hardware, eine Batterie ist nicht zwingend notwendig: Strom kann im Moment der physikalischen Berührung vom Sensor aus übertragen werden.

Nach dem Personalisierungs-Vorgang initiiert das MD nun den „join“-Vorgang. Es wählt eine zufällige Position im CAN-Netz, dessen zugehörige Zone aufge-*splittet* werden soll. Der zugehörige Zonen-Verwalter wird gebeten sich zu authentifizieren. Um Mißbrauch zu verhindern, muß der Zonen-Verwalter Zeugen vorweisen, die dem MD bestätigen, daß der Zonen-Verwalter tatsächlich für die gesuchte Zone zuständig ist. Dies sind üblicherweise die direkten Nachbarn des Zonen-Verwalters. Die Sicherheit der Kommunikation zwischen MD und den Nachbarknoten ist durch ihre gemeinsamen geheimen Schlüssel S_{ID} gewährleistet. Die alte Zone wird aufgeteilt und deren Nachbarn entsprechend über die neue Verwaltung informiert. Zudem werden sicher Schlüssel zwischen den Nachbarn und dem neuen Zonen-Verwalter ausgetauscht. Diese beschützen die direkte Kommunikation zwischen zwei Nachbarn im CAN. Zu diesem Zeitpunkt ist das CAN wieder in einem sicheren Zustand: der neue Knoten ist Teil des Netzes, seine direkten Nachbarn können vertraulich mit ihm kommunizieren. Er ist an einer zufälligen Stelle im Netz Zonen-Verwalter, kein Angreifer hat das beeinflusst.

Es ist allerdings noch ein weiterer Schritt notwendig, um Dienste im Netz sicher abzulegen und sicher danach zu suchen. Zunächst gilt, dass kein Verwalter einer Zone bewußt Änderungen an seinem Datenbestand durchführen kann. Da die Hash-Funktion nicht umkehrbar ist, kann er den einzelnen Hash-Werten und den damit verbundenen Adressen keine Dienst-Namen zuordnen. Problematisch ist jedoch, wenn auf dem Rückweg einer Anfrage das Ergebnis der Anfrage, der *Wert*, verfälscht wird. Dies ist aufgrund fehlender Ende-zu-Ende-Sicherheit prinzipiell allen auf dem Antwort-Pfad liegen-

den Knoten möglich. Ein Angreifer-Knoten könnte das Ergebnis so verändern, dass beispielsweise seine eigene Adresse in der Antwort enthalten ist. Wir schlagen daher vor, Redundanz im CAN zu erzeugen und darauf basierend Mehrheits-Entscheide durchzuführen. Anstatt einer einzelnen Hash-Funktion *H* sollten zwei (oder mehr) zusätzliche Hash-Funktionen *H'* und *H''* Verwendung finden. Ein Sensor, der seine Dienste im CAN Netz propagieren möchte, legt seine Adresse nun nicht nur in der Zone ab, in der *H(Dienst-Name)* liegt, sondern auch in den Zonen, in denen *H'(Dienst-Name)* und *H''(Dienst-Name)* verwaltet werden. Da die einzelnen Hash-Werte auf unterschiedlichen Knoten im CAN verwaltet werden, ist die Wahrscheinlichkeit groß, das nicht alle Wege vom anfragenden Dienst-Nutzer zu den Zonen-Verwaltern über einen bösartigen Knoten laufen. Der Dienst-Nutzer sucht analog nicht nur nach dem *Wert* von *H(Dienst-Name)*, sondern auch nach denen von *H'(Dienst-Name)* und *H''(Dienst-Name)*. Über die ihn erreichenden Antworten führt der Dienst-Nutzer dann einen Mehrheitsentscheid durch und verbindet sich zu dem in den Antworten meistgenannten Knoten oder aber schlägt bei nicht Übereinstimmung aller drei Ergebnisse bei einer zentralen Stelle Alarm.

Prototyp-Implementierung

Am Institut für Telematik werden Sensor-Prototypen („BlueNodes“[2]) basierend auf einem 8-Bit ATMEGA 128 Mikrokontroller mit 4 MHz eingesetzt. Als Hauptspeicher stehen 4 KByte RAM zur Verfügung, die drahtlose Kommunikation geschieht derzeit über Bluetooth.

Das S-CAN Protokoll benötigt auf den eingesetzten Sensoren nicht mehr als 900 Byte Hauptspeicher. Es verzichtet darüber hinaus komplett auf rechenintensive und Batterie-belastende Public-Key Operationen. Zur zeit werden am Institut für Telematik Experimente mit Java IButtons für den Einsatz als Master-Device durchgeführt. Die BlueNodes-Prototypen können über physikalischen Kontakt mit einem IButton Daten austauschen.

Fazit und Ausblick

Das S-CAN Protokoll leistet ein sicheres Anbieten und Abfragen von Diensten in Sensor-Netzen. Dafür wird ein Overlay-Netzwerk aufgebaut, das Dienst-Informationen und dazu passende Adressen von Dienst-Anbietern vorhält. Um Mißbrauch vorzubeugen, müssen die zukünftigen Nachbarn eines neu hinzuzufügenden Knotens über ein Zeugenverfahren beweisen, daß sie bestimmte Eigenschaften innehaben. Die sicherheits-relevanten Daten werden im Netzwerk redundant an verschiedenen Positionen abgelegt und die Antworten auf Dienst-Anfragen durch Mehrheitsentscheide auf Richtigkeit überprüft.

Das Protokoll kann allerdings nur in den Szenarien eingesetzt werden, bei denen der Benutzer die Möglichkeit hat, neue Sensoren vor ihrem Einsatz durch ein Master-Device zu personalisieren. Klassische Beispiele hierfür sind die Verwendung im Home- oder Office-Bereich. In anderen Umgebungen, wie dem Abwerfen vieler Sensoren aus dem Flugzeug heraus über einem Zielgebiet, ist dies nur eingeschränkt möglich.

Zur weiteren Absicherung der Kommunikation im Anschluß an die Dienst-Anfrage, den eigentlichen Nutz-Daten-Austausch, könnte als Teil der Adresse beispielsweise ein Public-Key-Zertifikat des Dienst-Erbringer-Sensors mitgeliefert werden. Inwieweit Zertifikate als gemeinsamer Ankerpunkt in den spontanen und ressourcen-beschränkten Sensor-Netzen sinnvoll sind, ist hingegen noch offen. Dies ist jedoch völlig unabhängig vom hier behandelten Registrieren von Diensten bzw. Abfragen von Diensten im CAN.

Literaturverzeichnis

[1] Sylvia Ratnasamy, Paul Francis, Mark Handley, Richard Karp und Scott Schenker: „A scalable content-addressable network“, Proceedings of the 2001 conference on applications, technologies, architectures, and protocols for computer communications, 2001

[2] Erik-Oliver Blaß, Hans-Joachim Hof, Bernhard Hurler, Martina Zitterbart: „Erste Erfahrungen mit der Karlsruher Sensornetz-Plattform“, GI/ITG KuVS Workshop Sensornetze, Berlin, 2003

[3] Yee Wei Law, Sandro Etalle und Pieter H. Hartel: „Assessing Security In Energy-Efficient Sensor Networks“, Small Systems Security, 2003