Erste Erfahrungen mit der Karlsruher Sensornetz-Plattform

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

Die fortschreitende Miniaturisierung von Computer-Hardware erlaubt immer kleinere und leistungsfähigere Geräte. In naher Zukunft werden Kleinstcomputer unsere ständigen Begleiter sein, allgegenwärtig unsere Umgebung bestimmen und uns bei alltäglichen Aufgaben unterstützen. Daraus ergibt sich eine Menge vielfältiger Möglichkeiten auf dem Weg dahin aber vor allem auch Hindernisse, die es zu beseitigen gilt. So eignen sich beispielsweise traditionelle Verfahren aus dem Bereich Sicherheit nur sehr eingeschränkt für die angestrebte Zielplattform kleinster eingebetteter Systeme, da dort meist nur wenig Speicher und Rechenleistung zur Verfügung steht. Auch der sehr eingeschränkte Energievorrat der eingesetzten Geräte stellt ein großes Hindernis für die Übernahme traditioneller Architekturen und Algorithmen dar.

Für erste praktische Versuchen mit solchen autonomen Sensoren bzw. Aktoren wurde eine Einheit entwickelt, welche aus einem Mikrocontroller Atmel Mega 128, einem Bluetooth-Modul und einem oder mehreren Sensoren/Aktoren besteht, die je nach Anwendung direkt auf der Platine oder über eine Drahtverbindung an den Mikrocontroller angeschlossen sind. Zur drahtlosen Kommunikation mit einer Basisstation oder zwischen einzelnen autonomen Sensoren dient das Bluetooth-Modul, für das ein sehr kompakter und effizienter Bluetooth-Stack entwickelt wurde.

Diese flexible Grundeinheit wird am Institut für Telematik für verschiedenste Anwendungen eingesetzt. Ausgestattet mit Beschleunigungssensoren und Gyroskopen wurde im Rahmen des IEEE-Wettbewerbs 2002 der „BlueWand“ entwickelt, welcher Bewegungen und Gesten des Benutzers aufzeichnet. Der Bluewand dient somit als alternatives Eingabegerät, mit dem eine Vielzahl von technischen Geräten bedient werden kann. Ein mit einem Drucksensor ausgestatteter Bürostuhl wurde in ein CSCW-System integriert. Er dient dort zur Übermittlung von Zustandsinformationen an die Teilnehmer einer Session, was non-verbale und intuitive Interaktion zwischen den Teilnehmern ermöglicht. Ein System mit einer größeren Anzahl autonomer Sensoren bzw. Aktoren ist derzeit in der Entstehung. Als Testfall dienen hierzu eine Reihe von Sensoren und Aktoren, welche eine Topfpflanze mit Wasser und geeignetem Licht versorgen sollen, indem Gießanweisungen an den Benutzer und Steuerimpulse an Jalousien übermittelt werden.

Für die oben aufgeführten Anwendungen existiert bisher ein zentraler Punkt, der mit den verschiedenen Geräten über Bluetooth eine Point-to-Point-Verbindung Kontakt aufnimmt und die von den Sensoren ermittelten Daten zentral auswertet. Im weiteren Verlauf der Arbeit am Institut für Telematik ist geplant, mehr und mehr auf Netzwerke von Sensoren hinzuarbeiten, um sowohl räumlich weiter ausgedehnte Szenarien als auch Systeme ohne zentrale Kontrolle realisieren zu können. Die dazu entworfene Architektur besteht unter anderem aus folgenden Bestandteilen:

Sensor Data Replication/Aggregation-Modul:

Im SDR/A-Modul werden Sensordaten vor der Weiterleitung an andere Sensoren aggregiert. Da der mit Abstand Größte Teil der Energie eines Sensor auf das Versenden von Daten entfällt bzw. in Sensornetzwerken auf die Weiterleitung von Paketen, ist es wichtig, möglichst wenig Daten zu übertragen. Dazu werden redundante Daten nicht weiter übermittelt und Sensordaten von verschiedenen gleichartigen Sensoren miteinander kombiniert, um kürzere Datensätze zu erhalten. Diese Reduktion erfolgt applikationsspezifisch. Das Modul koordiniert ebenfalls die Replikation von häufig angefragten Daten an verschiedene Punkten im Sensornetzwerk. Durch intelligente Replikation kann der Kommunikationsaufwand insbesondere bei periodisch anfallenden Daten erheblich eingeschränkt werden. Grundlage für diese applikationsspezifische Aggregation sind die am Institut für Telematik entwickelten Mechanismen aktiver und programmierbarer Netze.

Software-Update-Modul:

Software-Updates sind für eine lange Lebenszeit eines unzugänglichen Netzes wichtig. Die Korrektur von Fehlern, Erweiterung der Funktionalität ebenso wie die Anpassung an Umweltverhältnisse werden dadurch vereinfacht. Software-Updates stellen hohe Anforderungen an die Sicherheit, da die Authentizität und Integrität des zu installierenden Updates eindeutig festgestellt sein muss, bevor es integriert werden kann. Außerdem darf auch ein misslungenes Software-Update einen Sensor nicht völlig unbrauchbar machen. Dazu ist es nötig, gewisse Kernroutinen und Einsprungspunkte zu definieren und diese auch zu schützen. Dabei muss die nötige Flexibilität

für den Update-Programmierer erhalten bleiben. Die Sensoren am Institut für Telematik der Universität Karlsruhe nutzen die Selbstprogrammierungs-Fähigkeiten des Atmel ATMega128 RISC-Prozessors. Zur Zeit ist bereits die Möglichkeit vorhanden, gezielt Speicherbereiche zu beschreiben. Der Software-Update Code selbst liegt in einem besonders geschützten Bereich, der nicht geändert werden kann, so dass auch im Falle einer misslungene Code-Integration die Funktionalität des Sensors wiederhergestellt werden kann.

Verteilte Aktor/Sensor-Interaktion:

Im vorliegenden Netzwerkmodell gibt es neben Sensoren, die Daten liefern, auch Aktoren, die aufgrund anwendungsspezifischer Vorbedingungen ihre Umgebung beeinflussen können. Aktoren verbinden sich zeitweilig oder dauerhaft mit Sensoren, wobei Konflikte bei diesem Bindungsvorgang aufgelöst werden müssen. Dazu wurde ein Konzept entwickelt, mit dem im einfachsten Fall Sensordaten abgefragt und Aktoren direkt angesteuert werden können. Für komplexere Zusammenhänge, die ein Zusammenspiel zwischen verschiedenen Sensoren und Aktoren erfordern, besteht die Möglichkeit, dem Sensornetz Aufträge zuzuteilen. Primitive Aufträge beschränken sich auf oben genannte einfache Abfragen oder Steuerungen. Komplexe Aufträge enthalten wiederkehrende bzw. von gewissen Bedingungen abhängige Aufgaben. Diese Aufträge können wiederum aus einer Reihe von primitiven oder komplexen Aufträgen bestehen. Ein Sensornetz erledigt die ihm gestellten Aufträge autonom, ohne dass weitere Eingriffe von außen notwendig werden. Das Auftragskonzept ermöglicht es, ein Sensornetz schnell und ohne Änderung der bestehenden Sensor-/Aktorkomponenten mit neuen Aufgaben zu belegen. Das Auftragskonzept wird momentan in einer vereinfachten Form für den oben genannten „Intelligenten Blumentopf“ implementiert und eingesetzt.

Secure Content Adressable Network:

Einige Sensoren im Sensornetzwerk bilden ein Overlay-Netzwerk, das sogenannte Secure Content Adressable Network (CAN). Mit Hilfe dieses Overlays wird ein verteiltes Service Directory mit einer Public Key Database realisiert. Das Service Directory dient primär dazu, verfügbare Daten und Dienste des Netzwerks aufzufinden. Es kann auch zur Datenreplikation durch das SDR/A-Modul verwendet werden. Das Service Directory stellt die Grundlage für das A/SI-Modul dar, das einem Sensor die Möglichkeit bietet, einen Aktor aufzufinden. Da das Service Directory von zentraler Bedeutung für die Funktionalität unseres Sensornetzwerks ist, wurde besonderer Wert auf sichere Konstruktion und Erhalt der Strukur des Overlays gelegt. Dabei verzichtet die vorgeschlagene Lösung auf den Sensoren fast komplett auf asymmetrische kryptographische Verfahren und spart so Rechenleistung und Speicherplatz. Bei der Konstruktion des CAN werden jeweils benachbarte Knoten im Overlay dynamisch mit einem gemeinsamen Geheimnis ausgestattet und können damit fortan sicher und ressourcen-effizient mittels symmetrischer Verschlüsselung kommunizieren. Insbesondere die periodischen Update-Nachrichten über Nachbarschaftsbeziehungen werden durch diese Geheimnis geschützt. Somit wird die Struktur des Overlay-Netzes gesichert. Um neue Geräte in das CAN-Netz aufzunehmen wird ein so genanntes „Master Device“ eingesetzt. Dieses Gerät hat eine herausragende Stellung im Sensornetzwerk: Es bildet den Zugangsschlüssel zum Netzwerk, ist in der Lage auch komplexere kryptographische Operationen auszuführen, ist zustandslos und kommuniziert nur zu bestimmten Zeitpunkten mit dem Sensornetzwerk. Der Einsatz des Master Devices erfordert eine Interaktion mit dem Benutzer. Das Master Device sorgt für eine gleichmäßige Verteilung der Knoten im CAN-Space und stellt den einzelnen Geräten des CAN ein Zertifikat für die von ihnen verwaltete Zone aus. Außerdem verfügt jedes Gerät über ein gemeinsames Geheimnis mit dem Master Device. Durch ein spezielles Konstruktionsschema muß dies nicht für jedes Gerät auf dem Master Device gespeichert werden. Der Ausfall eines Geräts und das damit entstehende „Loch“ im CAN-Space kann durch das Master Device mit Hilfe von Bürgschaften der Nachbarn repariert werden. Die im S-CAN zum Einsatz kommenden kryptographischen Algorithmen wurden am Institut für Telematik im Hinblick auf die besonderen Erfordernisse der Zielplattform implementiert. Bisher konnten durch die Algorithmen folgende Leistungsdaten erzielt werden:

- Symmetrische Verschlüsselung über AES, 128 Bit Schlüssellänge: ca. 40 kBit/s
- Asymmetrische Verschlüsselung über Elliptische Kurven Kryptographie, 113Bit Schlüssellänge: ca. 0,06 kBit/s (verschiedene Formen zur erheblichen Optimierung in Arbeit)
- Hash-Algorithmus SHA-1, 4,4 kBit/s (auch hier sind noch einige Optimierungen in Arbeit)

Sämtliche kryptographischen Algorithmen benötigen dabei insgesamt nicht mehr als ca. 900 Bytes RAM.