

Sichere Nutzung und schnelle Anpassung von Sensornetzen

Dienstorientierte Sensornetze bieten Flexibilität für Benutzer und Entwickler

Einleitung

Der Einsatz von Sensornetzen ermöglicht die Überwachung verteilter Phänomene und ermöglicht es, die Effizienz von Geschäftsprozessen zu erhöhen. So kann ein Sensornetz z.B. zur Verwaltung eines Fuhrparks eingesetzt werden. Es ist möglich, jederzeit Wartungsdaten der Fahrzeuge zu überwachen (z.B. Ölfüllstand, Fehlerprotokolle) bzw. Kilometerstand und Benzinfüllstand zu Fahrtbeginn und Fahrtende automatisch zu erfassen, um eine einfache Abrechnung zu ermöglichen.

Sensornetze können auch dort gewinnbringend eingesetzt werden, wo es notwendig ist, eine Vielzahl von Daten über einen längeren Zeitraum kontinuierlich zu überwachen. Zum Beispiel, können in einem Krankenhaus oder bei der häuslichen Altenpflege Lebenszeichen von Patienten mittels eines Sensornetzes rund um die Uhr überwacht werden. Da Sensornetze drahtlos arbeiten wird die Mobilität der Patienten nicht eingeschränkt.

Aktuelle Sensornetz-Applikationen werden für jeden Anwendungsfall eigens zurecht geschnitten. Dadurch ist die Interoperabilität zwischen verschiedenen Herstellern nicht gegeben. Zudem sind heutige Sensornetzanwendungen schlecht zu warten, schwierig zu erweitern und relativ unflexibel. Der am Institut für Telematik entwickelte dienstorientierte Ansatz bietet eine flexible Architektur für Sensornetze, in der Sensornetz-Applikationen dynamisch aus vorgefertigten Bausteinen, so genannten Diensten, zusammen gesetzt werden können. Mit der dienstorientierten Architektur können Sensornetz-Applikationen einfacher gewartet werden, eine Erweiterung ist dynamisch möglich und die Architektur bietet maximale Flexibilität. Dadurch sind Kostenersparnisse beim Entwurf von Sensornetz-Anwendungen möglich.

Besonderer Schwerpunkt wurde bei der dienstorientierten Architektur auf Sicherheit gelegt, um Sensornetze auch in sicherheitskritischen Szenarien einsetzen zu können.

Hardware

Die in Sensornetzen verwendeten Kleincomputer, auch Sensorknoten genannt, sind üblicherweise nur wenige Zentimeter groß und kommunizieren drahtlos miteinander, z.B. unter Benutzung der Kommunikationsstandards ZigBee oder Bluetooth. Besondere Anforderungen an Entwickler von Applikationen in Sensornetzen entstehen durch die begrenzten Ressourcen der Sensorknoten. Beispielsweise haben die am Institut für Telematik eingesetzten Sensorknoten lediglich eine Taktrate von ca. 7 MHz ($\sim 1/5$ der Taktung eines Gameboys). Ihnen stehen 4 Kilobyte RAM ($\sim 1/8000$ des RAMs eines handelsüblichen PDAs), eine Batterie mit 180 mAh Kapazität ($\sim 1/10$ der Kapazität eines Handy-Akkus), sowie eine

Bandbreite von wenigen kBit/s zur Verfügung. Abbildung 1 zeigt zwei Prototypen von Sensorknoten, die am Institut für Telematik entwickelt wurden. Ein einzelner Sensorknoten findet Platz in der Kapsel von einem Kinder-Überraschung-Ei.

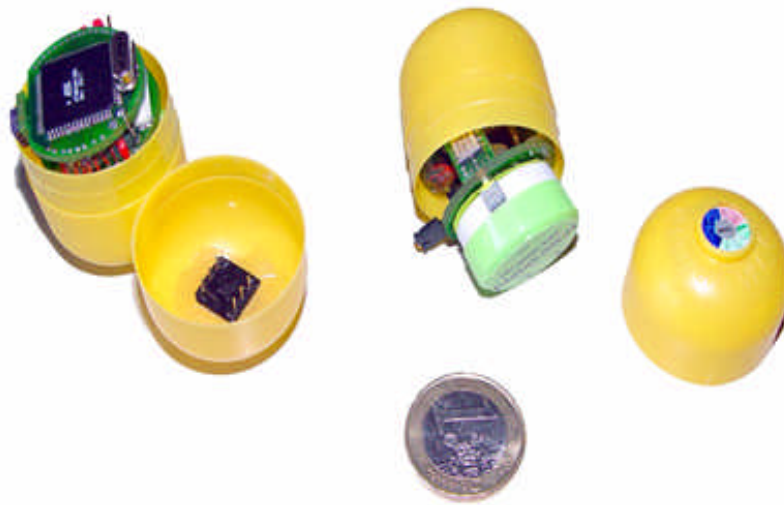


Abbildung 1: Am Institut für Telematik entwickelter Prototyp eines Sensorknotens

Dienstorientierte Sensornetze

Ziel der dienstorientierten Architektur ist es, eine Möglichkeit zu bieten, um Applikationen einfach aus bestehenden Bausteinen zusammen setzen zu können und Applikationen dynamisch umzukonfigurieren. Die Bausteine in dienstorientierten Sensornetzen werden Dienste genannt. Dienste werden von Entwicklern erstellt und zur Laufzeit des Sensornetzes eingespeist. Komplexere Dienste können mit Hilfe einer Beschreibungssprache aus bereits vorhandenen Diensten zusammen gesetzt werden.

Beispielszenario: Patientenversorgung in einem Krankenhaus

Patienten in einem Krankenhaus können mit Körpersensoren versehen werden, die diverse Lebenszeichen des Patienten aufzeichnen. Bedingt durch die geringe Größe und die drahtlose Verbindung der Sensorknoten untereinander wird die Mobilität eines Patienten nicht eingeschränkt. Im Sensornetz stellen die einzelnen Sensorknoten den Zugriff auf die Lebenszeichendaten durch Dienste zur Verfügung: Ein Dienst `Herzfrequenz` liefert z.B. die aktuelle Herzfrequenz. Ein Dienst `Blutdruck` liefert den Blutdruck eines Patienten. Der Dienst `Überwache_Patienten` wird aus den bereits vorhandenen Diensten `Blutdruck` und `Herzfrequenz` durch eine Beschreibungssprache zusammen gesetzt. `Überwache_Patienten` ermittelt über die Dienste `Blutdruck` und `Herzfrequenz` jeweils die entsprechenden Lebenszeichen und löst einen Alarm aus, falls einer der Werte unter einen von einem Arzt definierten Grenzwert fällt. Um den Alarm auszulösen wird der Dienst `Sende_an_Pager` benutzt, der eine Alarmierungs-Nachricht an den Pieper eines Arztes sendet. Abbildung 2 zeigt, wie der Dienst `Überwache_Patienten` in der dienstorientierten Architektur realisiert wird.

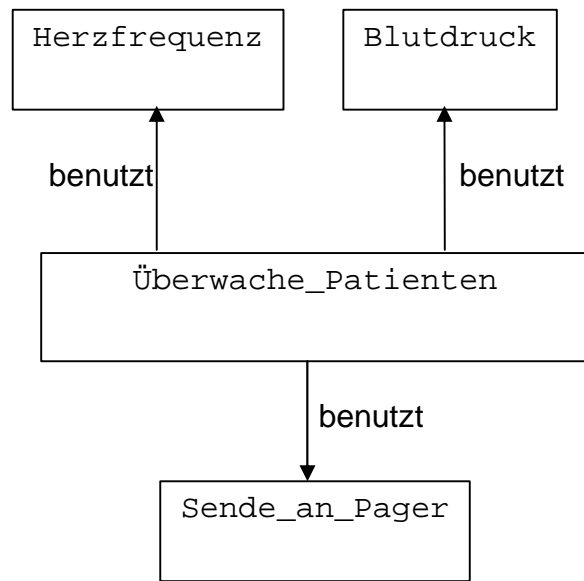


Abbildung 2: Zusammengesetzter Dienst Überwache_Patienten

Beispielszenario: Sensornetz zur Verwaltung eines Fuhrparks

Fahrzeuge eines Fuhrparks verfügen über unterschiedliche Sensoren: Der Dienst Kilometerstand liefert den aktuellen Kilometerstand eines Fahrzeugs und der Dienst Benzinstand stellt den aktuellen Füllstand des Benzintanks zur Verfügung. Die Zufahrt zum Fuhrpark verfügt über einen Sensor, der über die Dienste Anmelden und Abmelden Fahrzeuge registriert, die in den Fuhrpark einfahren oder diesen verlassen. Ein zentraler Server bietet im Sensornetz einen Dienst Fahrtbeginn und Fahrtende an, um Kilometeranzahl und Benzinverbrauch jeweils zum Fahrtbeginn bzw. Fahrtende aus Abrechnungsgründen zu registrieren. Ein Dienst Überwache_Fahrzeug kann aus den obigen Diensten zusammen gesetzt werden: Jedes Mal wenn der Dienst Anmelden oder Abmelden aktiviert wird, greift der Dienst Überwache_Fahrzeug auf die Dienste Benzinstand und Kilometerstand des entsprechenden Fahrzeuges zurück und führt dann entweder den Dienst Fahrtbeginn oder den Dienst Fahrtende aus. Abbildung 3 verdeutlicht, wie der Dienst Überwache_Fahrzeug funktioniert.

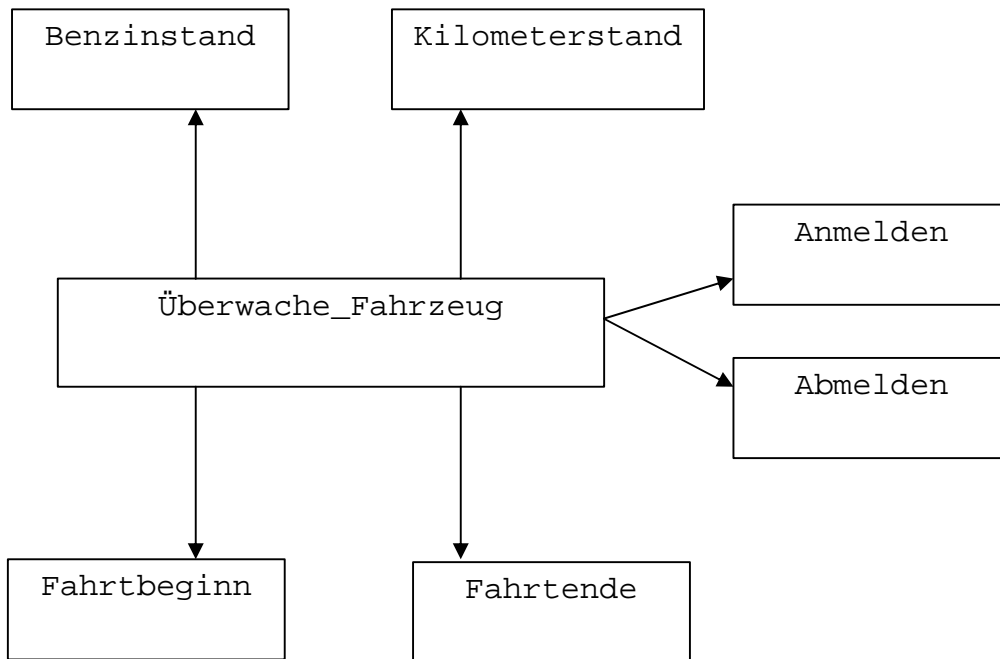


Abbildung 3: Zusammengesetzter Dienst Überwache_Fahrzeug

Sicheres Dienstverzeichnis

Wie bereits oben erwähnt können Dienste aus bereits bestehenden Diensten zusammengesetzt werden. Dazu ist es allerdings notwendig, dass Dienste dynamisch aufgefunden werden können. Dazu existiert in der Middleware von dienstorientierten Sensornetzen ein verteiltes Dienstverzeichnis, in dem Dienste mitsamt einer Beschreibung registriert werden können. Nach der Registrierung können andere Dienste auf den soeben eingespeisten Dienst zugreifen. Offensichtlich ist das Dienstverzeichnis ein zentraler Dienst des Sensornetzes, da nur durch das Verzeichnis zusammengesetzte Dienste möglich werden und Dienste aufgefunden werden können. Deshalb wurde beim Entwurf des Dienstverzeichnisses besonderer Wert auf Sicherheit gelegt. Bei dem sicheren Dienstverzeichnis handelt es sich um eine dezentrale Lösung. Ein virtuelles Overlay-Netz wird verwendet, um die Beschreibungsdaten der Dienste auf eine Menge von Sensorknoten zu verteilen. Sensorknoten, die an dem sicheren Dienstverzeichnis teilnehmen, werden authentifiziert. Weiterhin ermöglicht das verteilte Dienstverzeichnis, dass ein Knoten, der bereits in das Dienstverzeichnis aufgenommen wurde und zu einem späteren Zeitpunkt bösartig wird, nur lokalen Schaden anrichten kann.

Beschreibungssprache

Die Beschreibungssprache ermöglicht es, Dienste neu zu erstellen bzw. bestehende Dienste zu neuen zusammensetzen. Die Wiederverwendbarkeit und mehrfache Nutzung der Basisdienste erlaubt eine flexible, dynamisch änderbare Anwendungsprogrammierung aus bereits vorhandenen Bausteinen. Gleichzeitig ist es möglich bei Problemen oder Ausfall von Diensten diese im laufenden Betrieb zu ändern oder durch Dienste gleicher Funktionalität zu ersetzen. Die Beschreibungssprache erlaubt die Komposition von Diensten auf drei Arten: bedingte Dienste (Conditional Services) aktivieren andere Dienste, wenn gewisse Bedingungen erfüllt sind. Wiederholende Dienste (Repetitive Services) werden mehrmals

ausgeführt, bis eine bestimmte Anzahl oder Zeit erreicht ist. Ereignisdienste (Event Services) werden schließlich durch ein Ereignis von außen angestoßen. Da ein zusammengesetzter Dienst nur aus einer Beschreibung besteht und nicht direkt sondern nur über andere Dienste auf knotenspezifische Sensorhardware zugreift, kann der Ausführungsort eines zusammengesetzten Dienstes beliebig festgelegt werden. Idealerweise geschieht diese Auswahl automatisch durch das Sensornetz, sodass auf den speziellen Anwendungsfall bedarfsgerecht optimiert wird, z.B. auf Energieverbrauch oder Reaktionszeit.

Weitergehende Literatur

Hans-Joachim Hof, Ingmar Baumgart, Martina Zitterbart, *Secure Service Lookup in Service Centric Sensor Networks*, May 2005 (MobiHoc 2005: The Sixth ACM International Symposium on Mobile Ad Hoc Networking and Computing).

Hans-Joachim Hof, Martina Zitterbart, *SCAN: A secure service directory for service-centric wireless sensor networks*, Computer Communications, Jul 2005 (erscheint 2005).

Ingmar Baumgart, Hans-Joachim Hof, Martina Zitterbart, *Sicherheitsmechanismen für CAN-basierte Dienstlokalisierung in Sensornetzen*, Universität Duisburg-Essen, Oct 2005 (Security-Workshop "Neue Herausforderungen in der Netzsicherheit").

Hans-Joachim Hof, Erik-Oliver Blaß, Thomas Fuhrmann, Martina Zitterbart, *Design of a Secure Distributed Service Directory for Wireless Sensornetworks*, First European Workshop on Wireless Sensor Networks, Jan 2004.

Bernhard Hurler, Martina Zitterbart, *A Flexible Concept to Program and Control Wireless Sensor Networks*, First European Workshop on Wireless Sensor Networks, Berlin Germany, Jan 2004.