

Drahtlose Sensornetze

Friedemann Mattern und Kay Römer
Institut für Pervasive Computing
ETH Zürich

Der technische Fortschritt ermöglicht es in zunehmendem Maße, Sensoren, Prozessoren, drahtlose Kommunikationseinheiten und autarke Energiequellen in so genannten Sensorknoten auf kleinstem Raum zu integrieren. Netze aus vielen solchen Knoten gestatten die weiträumige Beobachtung von Phänomenen der realen Welt mit großer Genauigkeit, ohne dabei die physischen Prozesse wesentlich zu beeinflussen. Sensornetze sollen daher in vielen Anwendungsgebieten einen hohen Nutzen stiften.

So wollen beispielsweise Biologen das Verhalten von Tieren in ihrem natürlichen Lebensraum besser erforschen; Umweltforscher erhoffen sich umfassendere und genauere Möglichkeiten zur Überwachung der Ausbreitung von Verschmutzungen in Luft und Wasser; durch Einbringen von Sensornetzen in Gebäude und Brücken will man den Einfluss von seismischen Aktivitäten auf deren strukturelle Integrität besser erkennen; und Militärs sind stark daran interessiert, Aktivitäten in unzugänglichem Gelände durch den Einsatz von Sensornetzen zu überwachen (vgl. [1]).

In gewisser Weise handelt es sich bei der Verwendung der so genannten „Wireless Sensor Networks“ um einen Paradigmenwechsel im Einsatz von Computern: Verarbeitete man früher mit der „EDV“ Daten, die typischerweise manuell eingegeben wurden, so erfasst man jetzt – automatisch, online und in Realzeit – die physischen Phänomene selbst, was in einem viel größeren Umfang möglich ist und eine ganz neue Qualität von Resultaten ermöglicht [4]. Tatsächlich sendet die Umwelt ständig eine Vielzahl unterschiedlicher Signale aus; messen oder beobachten kann man beispielsweise akustische und visuelle Phänomene oder aber einfach nur Helligkeit, Beschleunigung, Temperatur, Feuchtigkeit und andere nützliche Parameter.

Die Funktion eines einzelnen Sensorknotens ist für sich

genommen relativ einfach (Auslesen von Sensordaten, Vorverarbeitung und Weiterleitung der Daten). Die vergleichsweise komplexe Funktionalität eines Sensornetzes ergibt sich erst durch das Zusammenwirken vieler Sensorknoten in einem oft hochgradig dynamischen System. So ist es erst durch die Kooperation vieler evtl. unterschiedlicher Sensorknoten möglich, gewisse Eigenschaften eines Umweltphänomens (wie Aufenthaltsort, räumliche Orientierung, Bewegungsrichtung- und Geschwindigkeit, Größe, Form von Objekten) zu erkennen und über die Zeit hinweg zu beobachten.

Aus den Anforderungen an einzelne Sensorknoten und an ein Sensornetz als Ganzes ergibt sich eine Vielzahl von konzeptionellen und technischen Herausforderungen, die ein weites Themenspektrum innerhalb der Informatik und Elektrotechnik, aber auch der Energie-, Material- und Mikrosystemtechnik betreffen. So sollen die individuellen Sensorknoten möglichst klein (wenige Kubikmillimeter), langlebig, billig und robust gegenüber Umwelteinflüssen sein. Die beschränkte Größe führt naturgemäß zu knappen Energieressourcen. Um trotzdem Langlebigkeit zu garantieren, müssen einerseits Hardware (Sensorik, Prozessoren, Kommunikationstechnik) und Software (Betriebssystem, Kommunikationsprotokolle) konsequent auf Energieeffizienz hin optimiert werden, andererseits müssen auf kleinstem Raum effiziente Techniken zur Energiespeicherung oder -gewinnung untergebracht werden.

Heute verfügbare Prototypen funkbasierter Sensorknoten, wie die an der Universität Berkeley entwickelten Motes¹, die μ AMPS-Knoten² des MIT oder die an der ETH Zürich entstandenen BTnodes³, haben noch ein Volumen von einigen Kubikzentimetern, verfügen über ei-

¹ www.xbow.com/Products/Wireless_Sensor_Networks.htm

² www-mtl.mit.edu/research/icsystems/uamps/

³ www.inf.ethz.ch/vs/res/proj/smart-its/btnode.html

nige MIPS Rechenleistung, mehrere 100 kB Programmspeicher und bis zu 100 kB RAM, können drahtlos über wenige Meter mit bis zu einigen 100 kbit/s kommunizieren und benötigen zwischen 50 μ W im Schlafzustand und 200 mW im vollen Betrieb.

Während diese Prototypen aus kommerziell verfügbaren Standardkomponenten aufgebaut sind, erfordert eine weitere signifikante Verkleinerung die Verwendung speziell gefertigter Hardwarebausteine und teilweise sogar völlig anderer Technologien. So wurden an der Universität Berkeley erste Prototypen von „Smart Dust“ [8] entwickelt, die eine Solarzelle, einen Helligkeitssensor, Möglichkeiten zur bidirektionalen Kommunikation mit einer Basisstation und eine einfache Kontrolllogik in 16 Kubikmillimeter unterbringen. Da die heutige Funktechnologie noch zu groß und energieaufwendig ist, verwendete man hier eine laserbasierte Methode zur Kommunikation mit dem „schlaun Staub“. Diese Art von optischer Kommunikation kann mehrere hundert Meter überwinden und kommt mit sehr wenig Energie in den Sensorknoten aus. So wird der Prototyp mit einer Solarzelle betrieben, die eine Leistung von etwa 2 mW abgibt.

Auf Sensornetz-Ebene ist ebenfalls eine Vielzahl von Problemen zu lösen. Auch hier steht die Energieeffizienz im Vordergrund, da die Kommunikation den Energieverbrauch eines Sensorknotens bei weitem dominiert. Protokolle und verteilte Algorithmen sollten aber nicht nur die pro Knoten aufgewendete Energie minimieren, sondern auch die Energiebelastung so auf die Knoten verteilen, dass eine lange Lebenszeit des Sensornetzes als Ganzes garantiert wird. Sensornetze unterliegen einer starken Dynamik: Knoten fallen aufgrund erschöpfter Batterien oder schädlicher Umwelteinflüsse häufig aus, neue kommen hinzu, um ausgefallene Knoten zu ersetzen, und manche Knoten sind aufgrund von Umwelteinflüssen wie Wind und Wasser sogar mobil. Trotz dieser Dynamik sollen Sensornetze ihre Aufgabe in robuster Weise erfüllen. In lebenswichtigen Anwendungen ist darüber hinaus Verlässlichkeit und Fehlertoleranz gefordert, d.h. ein Sensornetz sollte möglichst auch bei Ausfall einzelner Komponenten oder beim Auftreten zu erwartender Fehler noch bestimmte Funktionsgarantien erfüllen. Aufgrund der anvisierten Einsatzgebiete müssen Sensornetze ohne Infrastruktur auskommen, Sensorknoten müssen sich also spontan vernetzen – Techniken aus dem gegenwärtig intensiv erforschten Bereich der Ad-hoc-Netze spielen da-

her eine bedeutende Rolle. Ebenso ist Skalierbarkeit eine wichtige Anforderung, da Sensornetze Tausende oder gar Millionen von Knoten umfassen können. Die Größe der Netze und die Unzugänglichkeit der Knoten selbst verhindert, dass einzelne Knoten gezielt von menschlicher Hand konfiguriert oder administriert werden können, Sensornetze haben daher selbstkonfigurierend und selbst-administrierend zu sein. Nicht zuletzt müssen Sensornetze abhängig vom Anwendungsgebiet gewissen Echtzeit-Anforderungen genügen, beispielsweise um bestimmte Maximalzeiten zwischen dem Auftreten eines Ereignisses und der Meldung durch das Sensornetz zu garantieren. Sicherheitsrelevante Anwendungsbereiche erfordern den Schutz des Sensornetzes vor störenden Einflüssen und bössartigen Angriffen; neben eher traditionellen Sicherheitsmechanismen sind auch Lösungen für neue Probleme wie beispielsweise das Einschleusen von fremden Knoten in ein Sensornetz oder das Überschwemmen des Sensornetzes mit physischen Stimuli gefordert.

Da es sich bei den in Sensornetzen verarbeiteten Daten letztlich um physikalische Messgrößen handelt, spielt die Signalverarbeitung eine wichtige Rolle. Anstatt unter hohem Energieaufwand reine Sensorwerte im Netz zu verschicken, werden die Messwerte typischerweise lokal vorverarbeitet, um für die Problemstellung relevante Ereignisse zu extrahieren (beispielsweise das Erkennen eines Fahrzeugs anhand seines typischen Audio-Frequenzspektrums), die dann effizienter kommuniziert werden können. Daten verschiedener Sensorknoten müssen dann geeignet aggregiert bzw. verschmolzen werden, um die eingangs erwähnte komplexe Funktionalität eines Sensornetzes zu realisieren. Dabei wird aus einer relativ großen Menge von Rohdaten auf niedrigem Informationsniveau (beispielsweise eine Menge von Sichtungen eines Objektes durch verschiedene Sensorknoten) eine eher kleine Datenmenge auf relativ hohem Informationsniveau (beispielsweise die Durchschnittsgeschwindigkeit und Bewegungsrichtung des beobachteten Objektes) generiert. Aufgrund der damit verbundenen Datenkompression sollte idealerweise diese Informationsverarbeitung schon inkrementell „auf dem Weg“ im Sensornetz erfolgen, um nicht unter wesentlich höherem Energieaufwand die umfangreichen Rohdaten zunächst an einem zentralen Punkt sammeln zu müssen. Darüber hinaus werden oft zusätzlich auf den Datentyp abgestimmte Kompressionstechniken benötigt, um das Kommuni-

kationsaufkommen weiter zu reduzieren. All diese Informationsveredelungstechniken müssen mit den relativ beschränkten Ressourcen (Speicher, Rechenleistung, Kommunikationsbandbreite) der Sensorknoten auskommen.

Die genannten Aspekte können vielfach nur dann sinnvoll angegangen werden, wenn man bestimmte Annahmen klassischer Modelle verteilter Systeme überdenkt: Während in einem traditionellen verteilten System bei der Kommunikation meist gezielt Knoten mit bestimmten Adressen oder Namen angesprochen werden, ist in Sensornetzen die Identität eines Knotens weniger von Interesse. Im Extremfall verfügen Sensorknoten über gar keine Identifikationen; man „adressiert“ die Knoten dann über ihren Aufenthaltsort oder den Typ und Inhalt der von ihnen lieferbaren Informationen. Das hat wichtige Konsequenzen, unter anderem kann dadurch relativ einfach die Funktion eines ausgefallenen Knotens durch einen nahe gelegenen anderen Knoten mit gleicher oder ähnlicher Sensorik übernommen werden. Ein weiterer Unterschied zu klassischen verteilten Systemen betrifft die Eigenschaften der in einem Sensornetz ausgetauschten Daten: Daten von nahe gelegenen Knoten sind oftmals stark korreliert, was beispielsweise für Kompression (Elimination der Redundanz), Robustheit (benachbarte Knoten müssen ähnliche Daten liefern) oder Sicherheitsmechanismen (Erkennung von eingeschleusten Fehlinformationen) genutzt werden kann. Auch der Verlust von Nachrichten kann vielfach toleriert und durch eine spätere „Messung“ ausgeglichen werden, so dass klassische Kommunikationsprotokolle wie TCP/IP mit Ende-zu-Ende-Garantien bezüglich Zustellung von Nachrichten oftmals nicht notwendig bzw. wegen des erhöhten Aufwands sogar unerwünscht sind.

Neben diesen eher prinzipiellen Aspekten stellt sich auch die Frage nach Konzepten und Architekturen für Programmierung und Betrieb von Sensornetzen. Erste Ansätze wie TinyOS⁴ zeigen, dass sich beispielsweise Betriebssysteme für Sensorknoten deutlich von bisher bekannten Systemen unterscheiden müssen, um den Ressourcenbeschränkungen und den spezifischen Erfordernissen von Applikationen gerecht zu werden. Darüber hinaus sollten Anwendungen geeignet durch Infrastruktur („Middleware“) unterstützt werden. Dabei stehen unter anderem Sprachen und Techniken zur einfachen und

effizienten Programmierung von Sensornetzen, dynamische Reprogrammierbarkeit während des Betriebs und die gleichzeitige Nutzung eines Netzes für mehrere Aufgaben im Vordergrund. Auch hier gibt es erste Ansätze, die u.a. auf Datenbank-Sichtweisen basieren oder Anleihen bei Agentensystemen oder Event-Diensten nehmen. So interpretiert beispielsweise der TinyDB-Ansatz⁵ das Sensornetz als eine verteilte Datenbank, die durch Sensoren dynamisch mit Daten der realen Welt gefüllt wird. Mittels SQL-ähnlicher Konstrukte kann man dann Anfragen an das Sensornetz stellen.

Durch die Einbettung der Sensornetze in die reale Welt gewinnen die Kategorien Raum und Zeit eine besondere Bedeutung und müssen geeignet unterstützt werden. So ist es vielfach von Interesse, wo und wann ein physisches Ereignis stattgefunden hat. Darüber hinaus erfordert das oben erwähnte Verschmelzen der von verschiedenen Sensorknoten gelieferten Daten häufig ein gemeinsames räumliches und zeitliches Bezugssystem unter den Sensorknoten – es sind daher den neuen Anforderungen angemessene Mechanismen zur Lokalisierung und zeitlichen Synchronisierung der Knoten eines Sensornetzes notwendig [3, 6]. Ferner ist oftmals eine Einbindung von Sensornetzen in bestehende Infrastrukturen und eine Anbindung an das Internet sinnvoll, beispielsweise um weltweiten Zugriff auf ein Sensornetz zu ermöglichen oder Sensornetzen die Nutzung Internet-basierter Dienste und Ressourcen zu erlauben.

Hinsichtlich der oben genannten Aspekte und Konzepte, die für einen großflächigen Einsatz vernetzter Sensoren notwendig sind, zeichnet sich die Machbarkeit inzwischen ab, auch wenn noch eine Vielzahl von Problemen zu lösen bleibt, bevor Sensornetze einfach angewendet werden können. Letztendlich erwartet man von Sensornetzen Gewaltiges: Statt Experimente in einem Labor voller Instrumente durchzuführen, soll es dann – quasi umgekehrt – oft möglich sein, die extrem miniaturisierten Beobachtungsinstrumente am Vorgang in der Natur selbst anzubringen. Ökosysteme beispielsweise sollten sich so viel leichter und umfassender überwachen lassen – auch wenn man von schwimmenden Sensoren in Planktongröße zur Beobachtung von Fischschwärmen vorerst höchstens träumen darf. Sensornetze stellen damit eines der wichtigsten Instrumentarien dar, um die Visionen des

⁴webs.cs.berkeley.edu/tos

⁵telegraph.cs.berkeley.edu/tinydb

Ubiquitous Computing [9] zu realisieren [5].

Erste Feldversuche mit prototypischen Sensornetzen wurden bereits erfolgreich durchgeführt⁶. Allgemein dürften die stark sinkenden Kosten zur Überwachung und Informationsgewinnung viele Anwendungen ermöglichen, die bisher unwirtschaftlich gewesen wären, vor allem auch im industriellen Bereich. Die US-amerikanische DARPA-Förderinstitution hat im Jahr 2002 Sensortechnik und Sensornetze zu einem Thema höchster Priorität erklärt, dagegen steht die konzertierte europäische Forschung auf dem Gebiet der drahtlosen Sensornetze erst am Anfang – ein Pionier stellt hier das EU-Projekt EYES⁷ dar.

Die generische „Killerapplikation“ von Sensornetzen ist das feinmaschige und umfassende Monitoring. Werden damit nicht Ökosysteme, Produktionsprozesse oder physische Infrastrukturen überwacht, sondern in indirekter oder gar direkter Weise Menschen, dann zieht eine solche einfach anzuwendende und nahezu unsichtbare Technik massive gesellschaftliche Probleme nach sich: Sensornetze könnten letztendlich die delicate Beziehung zwischen Freiheit und Sicherheit aus dem Gleichgewicht bringen, indem sie die qualitativen und quantitativen Möglichkeiten zur Überwachung derart ausweiten, dass auch Bereiche erfasst werden, die einer dauerhaften und unauffälligen Überwachung bisher nicht zugänglich waren [2, 7].

Literatur

- [1] AKYILDIZ, I. F., W. SU, Y. SANKARASUBRAMANIAM und E. CAYIRCI: *Wireless Sensor Networks: A Survey*. Computer Networks, 38(4):393–422, März 2002.
- [2] CAS, J.: *Privacy in Ubiquitous Computing Environments?* In: *13th ITS-Europe Regional Conference*, Madrid, Spain, September 2002.
- [3] ELSON, J. und K. RÖMER: *Wireless Sensor Networks: A New Regime for Time Synchronization*. In: *Hotnets-I*, Princeton, USA, Oktober 2002.
- [4] ESTRIN, D., D. CULLER, K. PISTER und G. SUKHATME: *Connecting the Physical World with Pervasive Networks*. IEEE Pervasive Computing, 1(1):59–69, Januar 2002.
- [5] MATTERN, F.: *Vom Verschwinden des Computers - Die Vision des Ubiquitous Computing*. In: MATTERN, F. (Herausgeber): *Total vernetzt*. Springer-Verlag, 2003.
- [6] RÖMER, K.: *The Lighthouse Location System for Smart Dust*. In: *MobiSys 2003*, San Francisco, USA, Mai 2003.
- [7] SHEPHERD, D.: *Networked Microsensors and the End of the World as We Know It*. IEEE Technology and Society Magazine, 22(1):16–22, 2003.
- [8] WARNEKE, B., M. LAST, B. LEIBOWITZ und K. S. J. PISTER: *Smart Dust: Communicating with a Cubic-Millimeter Computer*. IEEE Computer Magazine, 34(1):44–51, Januar 2001.
- [9] WEISER, M. D.: *The Computer for the 21st Century*. Scientific American, 265(3):94–104, September 1991.

⁶www.greatduckisland.millennium.berkeley.edu/29Palms.htm

⁷eyes.eu.org