

Sensornetzwerke

Raphael Hahn, Oliver Neukum

Hauptseminar "Dienste & Infrastrukturen mobiler Systeme"
Wintersemester 03/04
Institut für Informatik
Ludwig Maximilians Universität München
raphael@schokoladenbaum.de, oliver@neukum.org

Zusammenfassung. Sensornetzwerke sind eine stark wachsende Technologie, die immer mehr bei Umweltbeobachtungen, in medizinischen Systemen oder in der Robotik eingesetzt werden. Die Anwendungsgebiete sind vielfältig und spiegeln die immer größer werdende Bedeutung dieser Netzwerke wieder. Im Folgenden soll anhand mehrerer konkreter Anwendungen ihre Vielseitigkeit und Zukunftsträchtigkeit herausgestellt werden. Nach einer genaueren Untersuchung der Voraussetzungen und spezifischen Anforderungen besonders an den Energiebedarf werden verschiedene MAC-Protokolle vorgestellt sowie das Routing in Sensornetzwerken betrachtet.

I. Einführung

Biologen des James San Jacinto Mountains Reservat in Süd-Californien gelang vor einiger Zeit eine überraschende und unerwartete Entdeckung. Es stellte sich heraus, dass die sich üblicherweise von Nüssen und Beeren ernährenden Eichhörnchen der Feuchtigkeit wegen Moos zerkauen, was bisher vollkommen unbekannt war. Dies gelang mit Hilfe eines 7.5 Quadratmillimeter großen Bewegungssensors, der eine Miniaturkamera auslöste, von der die Aufzeichnungen stammen. Die Geräte sind Teil einer 12 Hektar großen Anlage südwestlich von Palm Springs, USA, auf der neben den Tierbeobachtungen auch Pflanzen- und Umweltveränderungen durch eine große Anzahl von weit verteilten Sensoren gemessen werden [1].

Drahtlose Sensornetzwerke sind in der Tat eine stark wachsende Technologie, die immer mehr bei Umweltbeobachtungen, in medizinischen Systemen oder in der Robotik eingesetzt werden. Charakteristisch ist der Gebrauch von batteriebetriebenen Sensoren, die drahtlos miteinander in Verbindung treten und so ad-hoc-Netze bilden können. Typisch sind auch verhältnismäßig lange Horch- und Wartephasen der einzelnen Sensoren, sowie deren Einschränkungen in den Hardwaremöglichkeiten und damit verbundenen Problemen in der Energieversorgung. Um die Sendeleistung der Funkmodule gering zu halten, wird für lange Übertragungstrecken meist ein Multi-Hop-Verfahren angewendet.

Ziel eines solchen Sensornetzwerkes ist es, mit Hilfe von vielen sehr kleinen und billigen Knotenpunkten ein möglichst anpassungsfähiges und selbstorganisierendes Netzwerk einzurichten, das zudem über lange Zeiträume hinweg funktionsfähig bleiben soll.

Im Folgenden sollen einige Beispiel-Applikationen das weite Feld der Sensornetzwerke charakterisieren und die besonderen technischen Anforderungen aufgezeigt werden, die vor allem den MAC-Layer und das Routing betreffen.

Verwandt mit den Sensornetzwerken ist auch der RFID Media Access, der ein Mehrfachzugriffsverfahren auf Basis von Radiofrequenz-Identifikationstechnologie darstellt [2]. Dies ist besonders häufig im Alltag zu finden, wie auch erste Testläufe in Supermärkten zeigen. Hier werden alle Waren mit Tags ausgezeichnet, die der Einkaufswagen lesen und so jederzeit den aktuellen Gesamtpreis errechnen kann. Auch für die Logistik von Großhandelsunternehmen ist diese Technik schon lange interessant. Aber auch beim Skiverleih mit elektronischen Zeitstempeln an den Skiern oder Wegfahrsperren bei Autos wird schon heute RFID Media Access eingesetzt.

Trotz vieler Gemeinsamkeiten müssen diese Verfahren aber von den Sensornetzwerken abgegrenzt werden. Während bei den Sensornetzwerken meist eine Knoten-zu-Knoten-Kommunikation stattfindet, wird hier stets ein Lesegerät benötigt, das unter anderem auch den Tags die benötigte Energie berührungslos zur Verfügung stellt. Somit stellt der Energiebedarf kein besonderes Kriterium mehr dar. Auch haben die wenigsten RFID-Tags eigene Sensoren, sondern vielmehr stellen ihre IDs die zu lesenden Daten selber dar.

Weitere interessante Themen, die in Verbindung mit Sensornetzwerken betrachtet werden könnten, sind die Zeitsynchronisation, die Systemsoftware, Speicher und Datenbanktechniken, Collaborative Processing, Lokalisierungsverfahren sowie die Sicherheit. Diese Themen werden jedoch weitestgehend in anderen Zusammenhängen diskutiert und sind weniger spezifisch auf Sensornetzwerke zu beziehen.

II. Applikationen

Militärische Anwendungen:

Eine besondere Stellung nehmen militärische Sensornetze ein, da sie zurzeit die größte finanzielle Unterstützung erhalten und damit wie bei den meisten hochtechnisierten Anwendungen den zivilen Forschungen weit voraus sind. Die U.S. Department of Defense's Advanced Research Projects Agency (DARPA) legt große Hoffnungen auf die Entwicklung von Sensornetzwerken und hat 160 Millionen Dollar für die Forschung bereitgestellt. Hinzu kommen 500 Millionen Dollar von anderen U.S. Regierungsbehörden.

In Zusammenarbeit mit der University of California, Berkeley, wurde so unter anderem ein Experiment durchgeführt, in dem von Drohnen Sensoren zur Aufzeichnung von Bewegungen von Fahrzeugen abgeworfen wurden [3].

Die Abbildungen 1 und 2 zeigen die Entwicklung von anfangs großen und klobigen Sensoren hin zu sehr kleinen und vielseitigen Modulen. Die unauffälligen Motes können in vielen Situationen eingesetzt werden, ohne die Aufmerksamkeit der zu beobachtenden Ziele zu erregen und entdeckt zu werden.

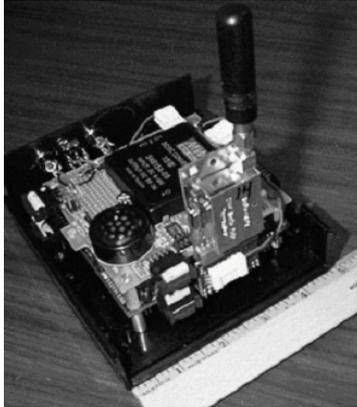


Fig. 1. Prototyp eines Sensor Nodes



Fig. 2. 'COTS Mote', entwickelt an der University of California, Berkeley

Einen ersten Eindruck vermittelt das 'Frisbee'-Modell zur Lokalisierung von Objekten, dargestellt in Abbildung 3. Die einzelnen weit verteilten Sensoren befinden sich die meiste Zeit in einem Schlafmodus. Entdeckt ein Sensor ein Objekt, weckt er die anderen Knoten seiner Gruppe auf, um genauere Informationen wie Bewegungsrichtung, Geschwindigkeit und Typ des Fahrzeuges sammeln zu können. Bewegt sich das Objekt weiter, schicken die Sensoren in Richtung der Bewegung einen Wake-up-call und wecken so die nachfolgenden Gruppen. Durch diese Zusammenarbeit kann der Pfad des Fahrzeuges aufgezeichnet werden.

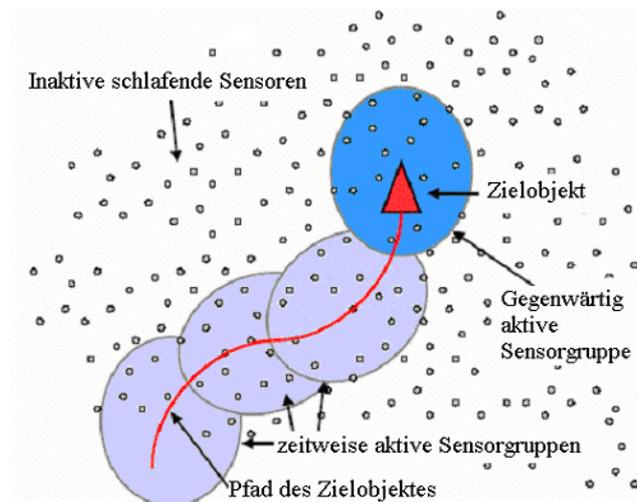


Fig. 3. Das 'Frisbee'-Modell. Das Dreieck stellt das zu beobachtende Objekt dar. Die schattierten Regionen kennzeichnen die Gruppen von Sensoren, die nacheinander aufgeweckt werden ('Frisbees')

Das Anwendungsbeispiel ist allgemeiner auch unter dem Begriff 'Smart Dust' bekannt geworden, da die Sensoren mittlerweile eine Größe erreicht haben, die einem Staubkorn nahe kommt, und so problemlos in den Einsatzgebieten verstreut werden können (siehe Abbildung 4). Erweiterbar ist dieses System mit unzähligen Funktionen wie die Kommunikation mit intelligenten Minen, die auf diese Weise nicht nur das erste Fahrzeug einer Kolonne treffen, sondern durch die Ausnutzung des gesamten Minenfeldes einen vielfach höheren Wirkungsgrad erzielen können.

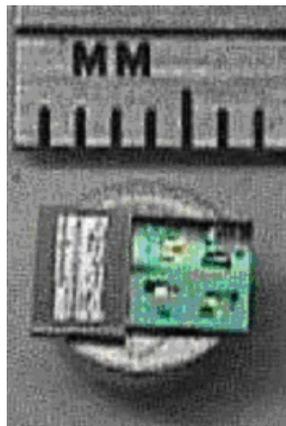


Fig. 4. Mote der University of California, Berkeley. Stand: Juli 1999. Zurzeit sind auch Entwicklungen an Sensoren von nur 1-2 mm Größe weit fortgeschritten, die neben einer Softgel-Batterie sogar eine Solarzelle besitzen

Diese Art von Sensorik findet heutzutage auch in zahlreichen zivilen Anwendungen Verwendung, ist aber nach wie vor besonders für das Militär interessant.

Der Mobile Patient:

Eine weitere Klasse sind medizinische Sensornetzwerke. Hier werden Sensoren zur Prävention von Krankheiten, Überwachung von Patienten, und Ersetzen von eigenen Sinnen wie z.B. bei einem künstlichen Auge gebraucht. Bauer, Sichertiu, Istepanian und Premaratne stellen in ihrer Forschungsarbeit das Konzept des 'Mobilen Patienten' vor [4]. Mit Hilfe eines mehrschichtigen Netzwerkes, das aus Sensoren zur Messung von Vitalfunktionen und einem überwachenden Prozessor am Körper des Patienten sowie einem Root-Rechner im Krankenhaus besteht, soll Patienten eine höhere Mobilität und damit eine bessere Lebensqualität gewährleistet werden. So müssen schwerkranke oder pflegebedürftige Personen nicht ständig unter ärztlicher Aufsicht sein, sondern können sich frei im Klinikgelände oder in Parks bewegen, was auch im Bezug auf den Genesungsprozess sehr positive Auswirkungen haben kann.

Great Duck Island:

Bei der Lebensraumüberwachung geht es um eine möglichst lückenlose Aufzeichnung eines bestimmten Gebiets. Hier wird vor allem Wert auf eine lange Betriebsdauer und den unauffälligen Betrieb gelegt. Das College of the Atlantic (COA) betreibt in Zusammenarbeit mit der University of California, Berkeley, und

der Intel Research Laboratory, Berkeley, einige solcher Anwendungen. Eine davon ist das Great Duck Island (GDI) (44.09N, 68.15W) [5], eine kleine Insel etwa 15 km südlich der Mount Desert Island, Maine, USA. Hier wird eine seltene Sturmschwalbenart beobachtet, die in den ausgewaschenen Felsen der Insel nistet. Besonders in das bisher unerforschte Brutverhalten dieser Vögel kann die Technik der Sensornetzwerke tiefere Einblicke gewähren, als dies auf herkömmlichem Wege möglich ist. So kann das Wissen um die Bedeutung der Fels- und Erdlöcher bei der Nutzung als Brutstätten oder das unterschiedliche Verhalten der Vögel in kleinen oder großen Populationen insbesondere beim Schutz der seltenen Vogelart dienlich sein. Zu diesem Zweck werden Messungen wie Temperatur und Belegung in unterschiedlichen Brutlöchern, in denen sich erwachsene Tiere, Jungtiere oder Eier befinden oder die auch leer sein können, durchgeführt.

Da sich die Insel weit ab von jeglicher Zivilisation befindet, ist eine Basisstation notwendig, die den Zugriff vom Internet aus bewerkstelligt. Einzelne feste Knotenpunkte bilden die Kommunikationsbrücken zwischen dieser Basisstation und den einzelnen mobilen Sensoren. Obwohl sich im Sommer immer wieder Wissenschaftler auf der Insel befinden, muss das Monitoring und das Management vollständig über das Internet möglich sein, um Eingriffe in das empfindliche Ökosystem so gering wie möglich zu halten und ausschließlich auf den Austausch und die Neuinstallation von Knotenpunkten und Sensoren zu beschränken. Der Energievorrat der nicht auswechselbaren Batterien ist auf 9 - 12 Monate ausgelegt, da mit den Jahreszeiten, die ja direkte Auswirkungen auf die Pflanzen- und Tierwelt haben, auch die Messergebnisse stark unterschiedlichen Charakter haben können. Einige Teile des Netzwerkes können dank Solarstrom längerfristig in Betrieb bleiben.

Die typischen Messdaten wie Temperatur, Helligkeit, Luftdruck und Luftfeuchte werden durch spezielle Sensoren zur Messung von Beschleunigung, Vibration, Gewicht, chemischen Gasen und Gaskonzentrationen, pH-Werten und Lärmpegeln sowie Infrarotsensoren erweitert. Dadurch können sehr komplexe und aussagekräftige Ergebnisse erzielt werden.

Im Juli 2003 wurde bereits die zweite Generation des Netzwerkes mit 105 Knoten installiert und nur einen Monat später um 60 Brutloch-Sensoren und 25 Wettersensoren erweitert. Einige davon sind bis zu 3 km weit im Wald verteilt.

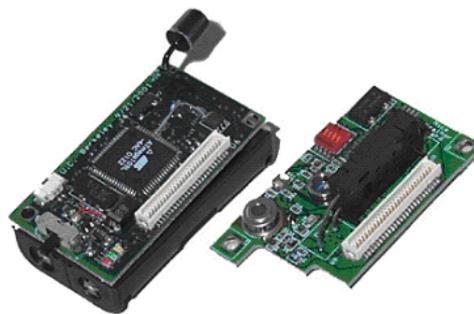


Fig. 5. Mica Hardware Plattform: Mica Sensor Node (*links*) und Mica Weather Board (*rechts*)



Fig. 6. Schutzhülle aus Acryl zum Aussetzen der Mica Mote

Unter <http://www.greatduckisland.net> können jederzeit aktuelle Informationen über das Projekt sowie die neuesten Messdaten und Live-Bilder abgerufen werden. Nach Auswahl von gewünschten Sensoren, deren Lage und Status auch auf einer Karte angezeigt werden, sowie von Messdaten und Zeitintervallen werden die Ergebnisse in Diagrammen dargestellt und dem Benutzer zur Verfügung gestellt.

Ähnliche Projekte sind auch in der Nähe von Palm Springs [1] oder vor der Küste von Los Angeles im Pazifik zu finden, wo eine mikrobiologische Kontrolle des Wassers durchgeführt wird [6].

Smart Kindergarten:

Beim Beobachten von Verhaltensmustern geht es mehr um das Verhalten einzelner Individuen und wie sie spontan miteinander reagieren. Der 'Smart Kindergarten' ist ein Beispiel hierfür [7]. Ziel ist die Schaffung einer sich weiterentwickelnden Umgebung zur Problemlösung für frühe Kindererziehung. Kinder lernen anhand von Interaktionen mit Spielzeugen und dem Entdecken ihrer Umgebung. Durch die angestrebte Technik sollen den Kindern individualisierte Lernmöglichkeiten gegeben werden, die an verschiedene Kontexte angepasst sind, Aktivitäten von mehreren Kindern koordinieren und dem Lehrer eine kontinuierliche und vor allem unaufdringliche Einschätzung der Lernfortschritte ermöglichen. Umgesetzt wird dies durch mit Sensorik ausgestattete Spielzeuge und andere Objekte im Klassenraum.

Ein Professor der University of California, Los Angeles, Mani Srivastava, will versuchsweise ab dem Frühjahr 2004 ein komplettes Klassenzimmer einer ersten Klasse mit Sensoren ausstatten, vom Raum selbst bis hin zu den Schülern. Diese sollen spezielle Mützen tragen, die mit sog. 'IBadges'-Sensoren ausgestattet sind, die ihre genaue Position und die Ausrichtung des Kopfes bestimmen sowie die Stimme über kleine Mikrophone aufnehmen. Zusätzlich zeichnen weitere Mikrophone und Kameras im Raum alle Aktivitäten auf. Das Projekt wird von der National Science Foundation mit 1.8 Millionen Dollar unterstützt [8]. Trotz vieler Proteste wird das Projekt von anderen Professoren und Wissenschaftlern als Meilenstein im Data Mining gerechtfertigt.

Industrie:

Zahlreiche Firmen wie Dust-Inc bieten schon seit geraumer Zeit Anwendungen auf Basis von Sensornetzwerken an [9]. Die Bandbreite geht vom industriellen Monitoring über Tracking von Objekten bis hin zur Umsetzung von Sicherheitsaspekten. So können die weit verbreiteten Alarmanlagen in Häusern verbessert und ausgebaut, aber auch zusätzlich mit Sensorik zur Messung von Vitalfunktionen von Personen wie Herzschlag und Körpertemperaturen oder anderen relevanten Funktionen erweitert werden. Die Firma verspricht eine Lebensdauer der Sensoren von über 5 Jahren mit einer einzigen Batterie.

Die Firma Crossbow [10] bietet eine Vielzahl verschiedener Sensoren für alle erdenklichen Anwendungen an. Die Chips können je nach Einsatzzweck unterschiedlich ausgestattet werden und sind in der Größe oft sogar kleiner als die Batterie, die sie betreibt. Abbildung 7 zeigt die Spezifikationen eines angebotenen Motes, der dieselbe Größe wie ein 25-Cent-Stück besitzt und durch den Einbau in eine spezielle Hülle sogar als Geldstück getarnt werden kann. Ähnliche Modelle werden auch von der Firma MicroStrain [11] angeboten.

Processor/Radio Board	MPR500CA	MPR510CA	MPR520CA	Remarks
Processor Performance				
Program Flash Memory	128K bytes	128K bytes	128K bytes	
Measurement (Serial) Flash	512K bytes	512K bytes	512K bytes	>100,000 Measurements
Configuration EEPROM	4 K bytes	4 K bytes	4 K bytes	
Serial Communications	UART	UART	UART	0-3V transmission levels
Analog to Digital Converter	10 bit ADC	10 bit ADC	10 bit ADC	6 channels, 0-3Vin
Other Interfaces	DIO	DIO	DIO	9 channels
Current Draw	8 mA	8 mA	8 mA	active mode
	< 15 uA	< 15 uA	< 15 uA	sleep mode
Multi-Channel Radio				
Center Frequency	868/916 MHz	433 MHz	315MHz	ISM bands
Number of Channels	> 8, > 100	> 8	> 8	programmable, country specific
Data Rate	38.4 Kbaud	38.4 Kbaud	38.4 Kbaud	manchester encoded
RF Power	-20 - +5 dBm	-20 - +10 dBm	-20 - +10 dBm	programmable, typical
Receive Sensitivity	-98 dBm	-101 dBm	-101 dBm	typical, analog RSSI at AD Ch. 0
Outdoor Range	500 ft	1000 ft	1000 ft	1/4 Wave dipole, line of sight
Current Draw	27 mA	25 mA	25 mA	transmit with maximum power
	10 mA	8 mA	8 mA	receive
	< 1 uA	< 1 uA	< 1 uA	sleep
Electromechanical				
Battery	3V Coin Cell	3V Coin Cell	3V Coin Cell	
External Power	2.7 - 3.3 V	2.7 - 3.3 V	2.7 - 3.3 V	connector provided
User Interface	1 LED	1 LED	1 LED	user programmable
Size (in)	1.0 x 0.25	1.0 x 0.25	1.0 x 0.25	excl. battery pack
(mm)	25 x 6	25 x 6	25 x 6	excl. battery pack
Weight (oz)	0.11	0.11	0.11	excl. batteries
(grams)	3	3	3	excl. batteries
Expansion Connector	18 pins	18 pins	18 pins	all major I/O signals

Fig. 7. Spezifikationen eines von Crossbow angebotenen Motes

III. Der MAC-Layer

Medium Access Control (MAC) ist besonders bei Netzwerken über die Luftschnittstelle eine wichtige Komponente. Die grundlegende Aufgabe eines MAC-

Layer Protokolls besteht darin, den Zugriff auf das gemeinsame Medium zu regulieren und damit die Kommunikation zwischen den verschiedenen Knoten im Netzwerk zu ermöglichen.

1) Designüberlegungen:

In drahtlosen Sensornetzwerken sind aufgrund der speziellen Voraussetzungen wie die beschränkten Hardwaremöglichkeiten oder die typischen Verkehrsmuster die Anforderungen an ein MAC-Protokoll stark unterschiedlich zu herkömmlichen Protokollen.

Limitierte Energieressourcen:

Besonders zum Tragen kommen hierbei die extrem limitierten Energieressourcen. Allgemein gilt zu beachten, dass aufgrund der meist nur kurzen Übertragungsdistanz und damit der geringen Sendeleistung der Funkmodule das Empfangen von Nachrichten ähnlich viel Energie verbraucht wie das Senden.

Der größte Energieverbrauch kann so den folgenden Faktoren zugeordnet werden:

- Aufgrund der meist hohen Korrelation des Netzverkehrs treten vermehrt Kollisionen auf, so dass die entsprechenden Pakete wiederholt gesendet werden müssen. Eine Vermeidung von Kollisionen spart diesen Aufwand ein.
- Als Overhearing bezeichnet man das Mithören von fremden Übertragungen benachbarter Knoten. Da jeder Knoten einer Nachbarschaft alle Nachrichten empfängt, auch wenn sie nicht für ihn selber bestimmt sind, wird unnötig Energie verbraucht.
- Das Senden und Empfangen von Kontrollpaketen kostet ebenfalls Energie und sollte daher möglichst gering gehalten werden.
- Idle listening bezeichnet das Horchen am Medium zum Zweck des Carrier Sense oder um auf eine Nachricht zu warten. Dies kostet ca. 50 - 100 % soviel Energie wie das Empfangen selbst. Es ist somit ineffizient, horchend auf eine Nachricht zu warten, wenn keine gesendet wird. Ideal wäre es also, die Knoten so oft wie möglich auszuschalten.

Skalierbarkeit und Anpassungsfähigkeit:

Zudem erfordern die Knoten ein hohes Maß an Selbstorganisation. Typischerweise fallen immer wieder einzelne Sensoren nach Aufbrauchen ihrer Energieressourcen oder wegen Defekten aus. Je nach Anwendung können ebenso wieder neue Knoten zum Netzwerk hinzugefügt werden. Die generell sehr hohe Dynamik resultiert auch aus möglicherweise andauernden Positionswechseln der einzelnen Sensoren. So unterliegt die Netzwerktopologie ständigen Veränderungen.

Diese Probleme werden dadurch verschärft, dass es sich meist um eine sehr große Anzahl von verteilten Knoten handelt. Da die Sensoren immer kleiner und billiger werden, sind Netzwerke mit mehreren tausend Knoten keine Seltenheit.

Verkehrscharakteristik:

Auch das typische Verkehrsmuster in Sensornetzwerken unterscheidet sich von dem in herkömmlichen drahtlosen Netzen. Der Datenaustausch ist häufig stark korreliert

und variabel. Lange Ruhephasen mit nur wenig Verkehr wechseln sich ab mit kurzen, intensiven Phasen mit hoher Netzlast. Dies resultiert aus dem meist gleichzeitigen Detektieren desselben Ereignisses von mehreren Sensoren.

Vergleich mit existierenden Protokollen:

Herkömmliche Protokolle sind für diese Anwendungsgebiete aufgrund der unterschiedlichen Anforderungen und Ziele weitestgehend ungeeignet. Bezüglich des Energieverbrauchs sind diese sehr ineffizient, was deutlich am Beispiel von 802.11 zu sehen ist. Bei dem hier verwendeten CSMA-Verfahren mit Collision Avoidance verbringen die Knoten fast die gesamte Zeit im Idle mode. Auch das bekannte PAMAS-Protokoll [12] bietet nur ungenügende Lösungsansätze. Zwar wird hier das Funkmodul ausgeschaltet, solange keine Übertragung empfangen oder gesendet wird, und damit auch das Overhearing vermieden, jedoch geschieht keine Verringerung des Idle listening. Zusätzlich werden zwei getrennte Funk-Kanäle benötigt, was bei den immer kleiner werdenden Sensoren sicherlich ein Problem darstellt. TDMA-basierende Ansätze haben den entscheidenden Nachteil, dass die Skalierbarkeit aufgrund der festen Slot-Belegung relativ schlecht ist. Schwer zu handhaben ist auch die physische Clusterbildung und damit die Interferenzen und die Kommunikation über die Cluster Grenzen hinaus.

Bei der Entwicklung entsprechender Protokolle für Sensornetze sind daher besondere Designüberlegungen zu beachten. Bei einem Netzwerk mit mehreren unabhängigen Benutzern möchte bekanntermaßen jeder die gleichen Rechte zum Senden und Empfangen besitzen sowie einen gewissen Grad von Quality of Service gewährleistet wissen. Da dies bei Sensornetzen nicht der Fall ist, sondern vielmehr alle Knoten einer gemeinsamen Anwendung dienen, treten die üblicherweise betrachteten Aspekte wie Latenz, Durchsatz und Fairness in den Hintergrund.

2) MAC-Protokolle für Sensornetze:

Lösungsvorschläge bieten unter anderem die vier Protokolle S-Mac, Berkeley-MAC, CSMA-PS, sowie DE-MAC, die allerdings auf unterschiedlichen Voraussetzungen aufbauen und somit schon relativ anwendungsspezifisch sind.

Die Vorteile des S-MAC beruhen auf periodischen Wach- und Schlafzyklen der einzelnen Knoten sowie dem Prinzip des Message Passing, das zudem auch dem Hidden-Terminal-Problem entgegenwirkt. Berkeley-MAC geht von einer eindeutigen Basisstation aus und setzt sehr erfolgreich die Idee des Parenting auf Grundlage eines Spannbauums um. Während hier jedoch das Problem des Idle listening nicht gelöst wird, zielt CSMA-PS besonders auf dessen Vermeidung ab. Hier wird das klassische CSMA, das auch bei 802.11 eingesetzt wird, mit Preamble Sampling kombiniert. DE-MAC betrachtet den Energieverbrauch eher auf Netzwerkebene als für jeden einzelnen Knoten und realisiert dies durch ein Ausbalancieren des Energiebedarfs zwischen energiekritischen und unkritischen Sensoren.

a) S-MAC (Sensor-MAC)

Entwickelt wurde S-MAC von Wei Ye und John Heidemann, beide vom Information Science Institute der University of Southern California, sowie von Deborah Estrin vom Computer Science Department der University of California, Los Angeles [13].

Gefördert wurde diese Arbeit nicht zuletzt aus militärischem Hintergrund durch das Space and Naval Warfare Systems Center San Diego.

Eine der Besonderheiten dieses MAC-Protokolls ist die Möglichkeit, die Latenzzeit und den Energieverbrauch in Abhängigkeit von den Netzbedingungen gegeneinander abzustimmen.

Eine Implementierung erfolgte bisher nur auf Testebene mit sehr wenigen Knoten, zeigt jedoch schon hier die spezifischen Vorteile und die Überlegenheit gegenüber herkömmlichen Protokollen. Um aussagekräftige Vergleiche ziehen zu können, implementierten Ye, Heidemann und Estrin auch ein vereinfachtes IEEE 802.11 MAC auf Basis derselben Plattform. Benutzt wurden zu diesem Zweck die sog. 'Motes', entwickelt von der University of California, Berkeley (siehe Abbildung 8).

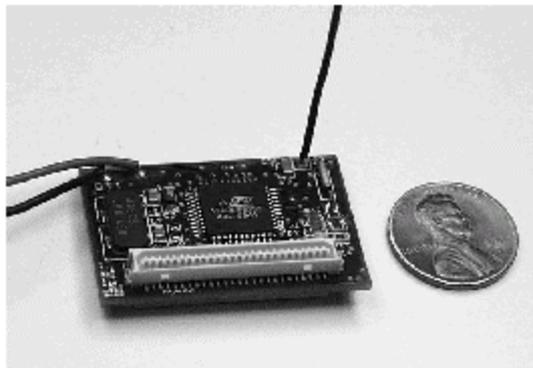


Fig. 8. Mote, Entwickelt an der University of California, Berkeley. Ein Mote besitzt einen 8-bit Microcontroller mit 4Mhz, sowie 8kB programmierbaren Flashspeicher und 512 Bytes Datenspeicher. Der Funk-Transceiver arbeitet auf einer Frequenz von 916.5 MHz und stellt eine Übertragungsrate von 19.2 Kbps zur Verfügung. Das Betriebssystem TinyOS ist rein event-gesteuert

Überblick:

S-MAC geht von einem ad-hoc-Netzwerk mit vielen sehr kleinen Knoten aus, die untereinander ohne Hilfe einer Basisstation kommunizieren. Zusätzlich sollen sie ein hohes Maß an Selbstkonfigurierbarkeit besitzen.

Als ein Hauptkriterium wird, wie schon aufgeführt wurde, der Energieverbrauch der einzelnen Knoten betrachtet. Das Ergebnis ist eine sehr energieeffiziente Lösung, die auf Basis von ausgefeilten Schlaf- und Wachintervallen und dadurch verbundener virtueller Cluster-Bildung, Multi-Hop-Übertragung mit Message Passing, sowie Vermeidung von Kollisionen und Overhearing den Anforderungen eines Sensornetzwerkes gerecht zu werden versucht.

Der Anspruch an die Fairness ist in keinster Weise mit den Bedingungen bei traditionellen drahtlosen Netzen zu vergleichen. Während hier jeder Benutzer gleiche Rechte und Möglichkeiten fordert, dienen die Knoten eines Sensornetzwerkes alle derselben Aufgabe. So kann das Konzept des Message Passing wieder eingeführt werden, dessen Grundidee eine Aufteilung langer Nachrichten in kleinere Fragmente und das Versenden in einem Burst ist. Andere Knoten, die nur eine kurze Nachricht

senden wollen, müssen so unter Umständen lange warten. Dies erscheint unfair, spart aber Energie durch die Verringerung von Kontrollpaketen und Overhearing.

Besonders drastisch ist die Energie-Ersparnis durch das periodische Versetzen der Sensoren in einen Schlafmodus und dem Horchen am Medium. Die Idee dazu wurde von PAMAS [12] übernommen. Schon ein halb-sekündiges Ausschalten während einer ein-sekündigen Periode senkt den Verbrauch um 50 %. Während der Schlafphase wird das Funkmodul abgeschaltet und ein Timer gesetzt, der als ein Wecker fungiert. Die Dauer der einzelnen Phasen können der jeweiligen Anwendung angepasst werden, um den spezifischen Anforderungen gerecht zu werden. Der Einfachheit halber sollten diese Parameter jedoch für alle Knoten eines Netzes übereinstimmen.

Die Latenzzeiten werden allerdings insgesamt erhöht, da durch die periodischen Schlafmodi die Sensoren teilweise mit dem Senden einer Nachricht warten müssen, bis der Empfänger aufgewacht ist.

Zum Ausgleichen der zeitlichen Ungenauigkeiten muss natürlich auch eine regelmäßige Synchronisation der Knoten untereinander gewährleistet werden. Hierzu werden erstens durchweg Zeitstempel mit relativen statt absoluten Zeitangaben verwendet. Zweitens sind die aktiven Zeiten des Horchens am Medium deutlich länger als die typischen Zeitabweichungen. Dadurch ist eine sehr viel lockerere Synchronisation möglich als dies z.B. beim klassischen TDMA mit seinen kurzen Zeitschlitzten der Fall ist. Die einzelnen Knoten können ihren Schlaf- und Wachrhythmus zunächst frei wählen, sollten sich dann jedoch mit den direkten Nachbarn synchronisieren, auch wenn das nicht immer möglich ist.

Die Synchronisation erfolgt durch einen Broadcast des Zeitplans an alle benachbarten Knoten. Direkte Nachbarknoten formen so durch die Autosynchronisation virtuelle Cluster. Dies ermöglicht einen Datenaustausch ohne Rücksicht auf eventuelle Schlafzeiten, ohne jedoch die üblicherweise bei Clusterbildung entstehenden Probleme wie Inter-Cluster-Kommunikation oder Interferenzen mit sich zu führen.

Infolge der virtuellen Cluster werden allerdings bei der Multi-Hop-Übertragung über längere Wege die Latenzzeiten stark erhöht. So wirken sich die spezifischen Anforderungen der Anwendung auf die Latenzzeit direkt auf die Länge der Schlafzeiten aus.

Auswählen der Zeitpläne:

Die einzelnen Knoten verwalten jeweils eigene Tabellen mit den Zeitplänen der bekannten direkten Nachbarn. Um einen eigenen Schlaf- und Wachrhythmus zu wählen, werden drei Schritte durchlaufen:

1. Der Knoten horcht eine bestimmte Zeit lang, ob er einen Zeitplan eines anderen Knoten empfangen und übernehmen kann. Ist dies nicht der Fall, wählt er einen zufälligen Rhythmus aus und verbreitet diesen sofort mittels einer SYNC Nachricht. Darin enthalten ist auch die Zeitdauer, bis er in den Schlafmodus geht. Dieser Knoten wird nun 'Synchronizer' genannt, da sich die Nachfolgenden nach ihm richten.
2. Falls der Knoten einen Zeitplan empfängt, übernimmt er diesen und wird daher 'Follower' (Nachfolger) genannt, da er sich nach dem Synchronisierer richtet. Nach einer zufälligen Verzögerung sendet nun auch dieser Knoten eine SYNC Nachricht, in der die Zeitdauer bis zum Schlafmodus enthalten ist. Die Verzögerung dient zur

Vermeidung von Kollisionen, so dass mehrere Follower, die demselben Synchronisierer folgen, nicht gleichzeitig den Zeitplan weitersenden.

3. Wenn ein Knoten einen Zeitplan empfängt, nachdem er einen eigenen gewählt und weiterverbreitet hat, übernimmt er beide Zeitpläne. Vor dem Schlafmodus versendet er seinen eigenen Zeitplan. Normalerweise sollten nur wenige Knoten mehrere Rhythmen übernehmen, da sie sich stets zuerst nach anderen umhören, bevor sie einen eigenen wählen. Aufgrund von Kollisionen kann es dennoch dazu kommen.

In einem Netzwerk synchronisieren sich also alle mit dem ersten Knoten, dessen Timer abläuft und der einen Broadcast verschickt. Sollten dies zwei Knoten gleichzeitig tun, weil sie sich nicht hören können, übernehmen die Knoten in der Grenzzone beide Zeitpläne. Der Nachteil ist, dass diese dadurch weniger Zeit im Schlafmodus verbringen und so mehr Energie verbrauchen.

Als Alternative dazu könnten die Grenzknoten auch nur die erste Synchronisation übernehmen und den zweiten Plan speichern. So können sie mit allen anderen kommunizieren, müssten jedoch beim Broadcast zwei Pakete entsprechend der Zeitpläne verschicken.

Regelmäßige Synchronisation der Zeitpläne:

Obwohl die Wach-Zeiten relativ lang sind und so auch Abweichungen tolerieren können, müssen die Knoten sich in regelmäßigen Abständen miteinander synchronisieren. Hierzu reichen nach den Versuchen von Ye, Heidemann und Estrin Zeiten von 10 und mehr Sekunden aus. Die Synchronisierung geschieht mittels einer SYNC-Nachricht, die die Adresse des Absenders sowie die Zeitdauer bis zur nächsten Schlafphase enthält. Dieser Zeitabstand ist in allen Paketen enthalten und wird in Relation zum Ende der Übertragung angegeben, so dass die Nachbarknoten aufgrund der kurzen Ausbreitungsverzögerung direkt ihren Timer danach einstellen können.

Damit die Knoten sowohl SYNC- als auch Daten-Pakete empfangen können, wird die Wachphase wiederum in zwei Phasen unterteilt. Der erste Teil ist für SYNC bestimmt, der zweite für RTS-Pakete. Eine weitere Unterteilung in kleine Zeitschlitze ermöglicht den Sendern das Medium abzuhören. Wie in Abbildung 9 dargestellt beginnt also der Sendeknoten beim Senden eines Paketes mit dem Carrier Sense zu dem Zeitpunkt, zu dem der Empfänger anfängt zu horchen, und startet in einem zufällig gewählten Zeitschlitz mit dem Senden.

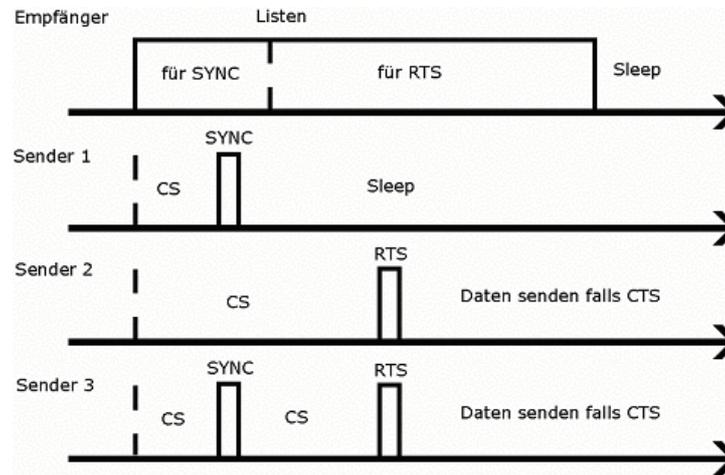


Fig. 9. Verschiedene Phasen mehrerer Sender und eines Empfängers. CS: Carrier Sense

Jeder Knoten broadcastet in regelmäßigen Abständen seine SYNC-Nachricht, auch wenn er keine Nachfolger besitzt, so dass sich neue Knoten anschließen können.

Vermeidung von Kollisionen und Overhearing:

Zur Vermeidung von Kollisionen übernimmt S-MAC die grundlegenden Prinzipien von 802.11, besonders das virtuelle und physische Carrier Sensing sowie den Austausch von RTS/CTS Nachrichten. Jedes Nachrichtenpaket enthält unter anderem die Länge der verbleibenden Übertragung, so dass andere Knoten, die die Nachricht mithören, stets wissen, wie lange sie noch im Schlafmodus verbleiben müssen.

Broadcastnachrichten werden ohne RTS/CTS versendet, alle anderen Pakete folgen jedoch der Abfolge von RTS/CTS/DATA/ACK zwischen Sender und Empfänger. Die beteiligten Knoten werden bis zum Ende der Datenübertragung nicht wieder in den Schlafmodus versetzt und bleiben im Wachzustand.

Während in 802.11 die Knoten alle Übertragungen ihrer Nachbarknoten mithören, um ein effizientes virtuelles Carrier Sensing durchzuführen, werden in S-MAC die Knoten in den Schlafzustand versetzt, nachdem sie ein fremdes RTS oder CTS empfangen haben. So wird sichergestellt, dass alle direkten Nachbarn sowohl des Senders als auch des Empfängers inaktiv sind und so einerseits die Übertragung nicht stören können und andererseits selber Energie sparen.

Message Passing:

Ziel des Message Passing ist, lange Nachrichten möglichst effizient im Hinblick auf Energie und Latenzzeit zu versenden. Das Versenden einer Nachricht am Stück als ein Paket hat den Nachteil, dass selbst bei kleineren Übertragungsfehlern die gesamte Nachricht wiederholt werden muss. Bei Fragmentierung in kleinere Pakete ist aufgrund von RTS/CTS für jedes einzelne Paket mit einem verstärkten Aufwand für Kontrollpakete und somit größeren Verzögerungen zu rechnen.

S-MAC löst dieses Problem durch eine Fragmentierung und dem Versenden der so entstandenen Pakete in einem Burst. Hierfür wird nur eine RTS- bzw. CTS-Nachricht

benötigt, die das Medium für die Dauer der Übertragung reserviert. Nach jedem Paket wartet der Sender auf die Bestätigung (ACK) und wiederholt notfalls das aktuelle Paket.

Da das Umschalten von Schlaf- auf Empfangsmodus technisch bedingt einige Zeit in Anspruch nimmt, sollte die Umschaltfrequenz stets gering gehalten werden. Das Prinzip des Message Passing setzt die Knoten so lange wie möglich in den Schlafzustand und vermeidet so zu großen Overhead.

Die Verwendung von ACK nach jedem Fragment wirkt zugleich dem Hidden-Terminal-Problem entgegen. Ein Nachbarknoten des Empfängers, der erst während der Übertragung aufwacht oder neu hinzukommt, hört unter Umständen die Pakete des Senders nicht und geht so nach seinem Carrier Sense von einem freien Medium aus und verursacht eine Kollision beim Empfänger. Durch die ACK-Nachrichten des Empfängers wird dies verhindert. Diese enthalten wie jedes andere Paket auch die Länge der restlichen Übertragung, so dass stets alle mithörenden Knoten ihren Timer korrekt stellen können, auch wenn die Länge wegen der Wiederholung eines Paketes oder anderer Fehler vom Sender erhöht wurde.

Obwohl auch 802.11 die Fragmentierung unterstützt, gibt es doch entscheidende Unterschiede. Hier reserviert das erste RTS / CTS das Medium nur für das erste Datenpaket und das ACK. Diese reservieren das Medium weiter für das zweite Datenpaket und das ACK und so weiter. Dies geschieht aus Gründen der Fairness, da der Sender bei einem ausbleibenden ACK die Übertragung abbrechen und erneut das Senderecht erwerben muss. Da infolgedessen die Nachbarknoten immer nur bis zum nächsten Fragment im Schlafmodus bleiben können, ist der Energieverbrauch deutlich höher als bei S-MAC, bei dem die Fairness auf Anwendungsebene wichtiger ist als zwischen einzelnen Knoten.

Zusammenfassung:

S-MAC bietet einen je nach Netzbedingungen 2-6-fach geringeren Energieverbrauch als 802.11. Die gute Skalierbarkeit und Kollisionsvermeidung sprechen ebenfalls für dieses Protokoll. Nachteilig sind die eventuell recht große Multi-Hop-Latenz und der höhere Energieverbrauch der Grenzknoten eines Clusters.

Umfassendere Tests in konkreten Anwendungsfällen in größeren Umgebungen sowie genauere Untersuchungen der Skalierbarkeit und der Auswirkungen der verschiedenen Parameter bleiben abzuwarten und werden feststellen, ob sich S-MAC auch in der Praxis bewähren kann.

b) Berkeley-MAC

Das Berkeley-MAC-Protokoll wurde von Woo und Culler [14] von der University of California, Berkeley, auf der Basis von CSMA entwickelt. Auch dieses Protokoll zielt auf einen möglichst geringen Energieverbrauch ab. Als Voraussetzung werden kurzfristig hohe Verkehrsaufkommen mit kurzen Paketen, die um die 30 Bytes groß sind, angenommen.

Berkeley-MAC geht von einer eindeutigen Basisstation aus, zu der alle Daten der einzelnen Knoten geschickt werden. Dies erfolgt mit einem Spannbaum, der von einer übergeordneten Schicht erstellt wird. Jeder Knoten kennt hier seinen Vaterknoten und weiß so stets, wohin er seine Nachrichten senden muss.

Neben der Optimierung des Energieverbrauchs steht die Ausnutzung der Bandbreite von den Knoten zur Basisstation im Vordergrund. Insbesondere sollen die

Knoten in der Nähe der Basisstation nicht mehr senden können als weiter entfernte. Zu diesem Zweck schlägt Berkeley-MAC einen *Adaptive Rate Control Mechanismus* vor, der diese Fairness sicherstellt. Dieser wird jedoch nicht im MAC-Layer realisiert.

Das CSMA-Prinzip wird um zufällig lange Wartezeiten im Schlafmodus vor dem eigentlich Carrier Sense erweitert. Diese sollen vor allem Kollisionen verhindern, die beim gleichzeitigen Detektieren derselben Ereignisse vermehrt auftreten, sowie Energie einsparen. Außerdem ermöglicht die Technik des *Parenting* den gänzlichen Verzicht auf Kontrollpakete.

Das *Parenting* nützt den zugrunde liegenden Spannbaum aus. Im in Abbildung 10 dargestellten Beispiel sendet der Knoten B eine Nachricht zum Zeitpunkt t an Knoten C. Der Knoten A weiß zusätzlich, dass C das Paket innerhalb der Zeit $(t + t')$ an D weitersenden wird, und wartet genau diese Zeit ab, bevor er selbst sendet, um eine Kollision in B zu verhindern. Jedoch können nicht alle Kollisionen auf diese Art und Weise vermieden werden, wie das Szenario weiter zeigt. Ein Knoten E, der außerhalb der Reichweite von A liegt, kann eine Übertragung an C starten. A bemerkt davon nichts, beginnt seinerseits mit dem Senden und verursacht somit eine Kollision in B.

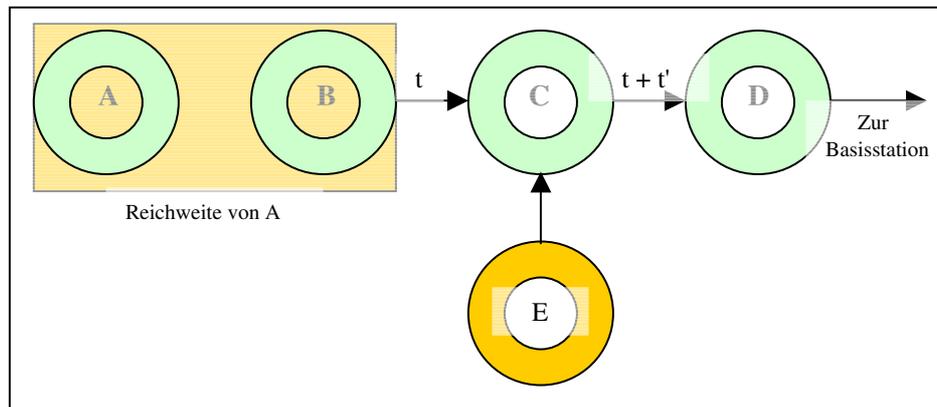


Fig. 10. Parenting im Berkeley-MAC

Auch die ACK-Pakete können dank des Parenting eingespart werden, da die Weiterleitung der Nachricht von B nach C wie ein implizites Acknowledgement wiederum von A empfangen werden kann.

Ein Hauptkritikpunkt am Parenting ist die Notwendigkeit der ständigen Überwachung des Mediums seitens der einzelnen Knoten, so dass durch Idle listening unnötig Energie verbraucht wird.

Implementiert und getestet wurde das Berkeley-MAC wie auch S-MAC auf den Berkeley-Motes und zeigte ebenfalls eine deutliche Energieeinsparung gegenüber 802.11. Aufgrund der ungelösten Problematik des Idle listening eignet sich dieses Protokoll jedoch allenfalls für Netzwerke mit durchschnittlich sehr hohem Verkehrsaufkommen, bei dem dieses weniger akut zum tragen kommt.

c) CSMA-PS

Das Carrier Sense Medium Access Preamble Sampling (CSMA-PS) wurde 2002 von El-Hoiydi entwickelt [15, 16]. Unter der Annahme, dass bei Sensornetzwerken der

Nachrichtenverkehr meist sehr gering ist, zielt dieses Protokoll hauptsächlich auf die Verhinderung von Idle listening ab.

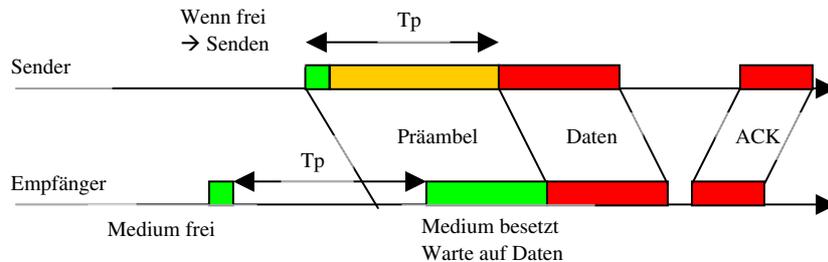


Fig. 11. Übertragung bei CSMA-PS

Abbildung 11 zeigt den Ablauf einer Übertragung in CSMA-PS. Alle Knoten befinden sich in einem periodischen Wach- und Schlafzyklus. Die Länge des Intervalls wird mit T_p bezeichnet. Zum Senden verschickt der Sender nach einem Carrier Sense zuerst eine Präambel der Länge T_p , die den Empfänger identifiziert, und dann erst die Daten selbst. Durch die gewählte Länge der Präambel ist gewährleistet, dass der Empfänger genau einmal aufwacht, während die Präambel gesendet wird. Wacht nun ein Knoten auf, horcht er zunächst, ob das Medium besetzt ist. Falls das Medium frei ist, kann er weiter im Schlafmodus verbleiben. Erkennt er jedoch eine Präambel, horcht er weiter, bis er die Daten empfängt und bestätigt die erfolgreiche Übertragung durch ein ACK.

Gegenüber S-MAC müssen die Knoten für dieses Verfahren nicht synchronisiert sein.

Nachteilig wirkt sich bei CSMA-PS jedoch der erhöhte Energieverbrauch beim Senden aus, der seine Ursache in der langen Präambel findet. Zusätzlich wird auch die Wahrscheinlichkeit von Kollisionen erhöht.

Ein verbessertes Protokoll, Synchronized-CSMA-PS (S-CSMA-PS), behebt diese Probleme durch die Speicherung der Aufwachzeitpunkte der direkten Nachbarn, so dass genau zu diesen Zeitpunkten Nachrichten gesendet werden können. Die Präambel muss dadurch nur noch lang genug sein, um die eventuellen Zeitabweichungen ausgleichen zu können.

Zusammenfassend stellt S-CSMA-PS ein sehr viel versprechendes Protokoll dar, das bei einem Übertragungsintervall von 10 Sekunden zumindest rein rechnerisch eine Lebensdauer von mehreren Jahren gewährleistet.

d) DE-MAC

Eine sehr neue Entwicklung stellt das Distributed Energy-Aware MAC-Protokoll (DE-MAC) der Louisiana State University dar [17]. Entwickelt von R. Kalidindi, L. Ray, R. Kannan und S. S. Iyengar und erst vor wenigen Monaten erstmals vorgestellt, basiert dieser Lösungsansatz auf einem TDMA-Prinzip und vermeidet so vor allem Kollisionen und verringert den Overhead an Kontrollpaketen. Es benutzt auch die schon bekannte Idee der periodischen Wach- und Schlafzyklen um Idle listening und Overhearing zu minimieren.

Die Besonderheit dieses Protokolls besteht jedoch in einer lokalen Auswahl-Prozedur, die schwachen und kritischen Knoten Vorrechte zuteilt und längere Zeit schlafen lässt. Dieser Mechanismus ist vollständig in die TDMA-Zeitschlitzvergabe integriert und benötigt so keine zusätzliche Bandbreite.

Kriterien, anhand derer Knoten als schwach oder kritisch ausgewählt werden, können lokale Statusinformationen sein oder durch eine Funktion des Standortes eines Sensors innerhalb dynamischer Routing-Bäume dargestellt werden.

Zu Beginn wird jedem Knoten dieselbe Anzahl von Time-Slots zugeordnet. Wenn nun bei einem Knoten der Energievorrat unter einen bestimmten Schwellwert fällt, kann er eine Wahl auslösen, bei der alle Knoten ihren Energielevel an die regelmäßigen Übertragungen innerhalb ihres Zeitschlitzes anhängen und so den kritischsten Knoten bestimmen. Dieser ist nun der neue Leiter und sein Energielevel wird zum neuen Schwellwert für weitere Wahlen. Alle anderen Knoten verringern nun die Anzahl der ihr zugeordneten Zeitschlitzte um einen konstanten Wert und stellen sie dem Leiter zur Verfügung. Durch dieses Verfahren wird die Zeit für Idle listening der schwachen Knoten stark verkürzt.

Die Schlafzeiten eines Knoten sind also ausschließlich innerhalb der eigenen Timeslots, in denen nichts gesendet werden muss. Während der übrigen Zeit hört jeder Knoten alle Nachrichten der anderen mit. Die jeweils schwächsten Sensoren haben mehr Zeitschlitzte zur Verfügung, so dass ihr Energieverlust durch Idle listening verringert wird.

Ein relativ groß angelegter Versuchsaufbau mit 100 Sensoren in einem Gebiet von einem Quadratkilometer zeigt deutliche Vorteile gegenüber herkömmlichen TDMA-Verfahren ohne das dargestellte Auswahlverfahren der schwächsten Knoten und deren Bevorzugung. Abbildung 12 zeigt die Energieersparnis in Abhängigkeit von der Zeit.

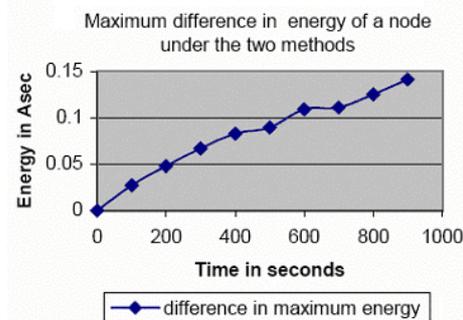


Fig. 12. Maximale Energiedifferenz zwischen TDMA mit und ohne Auswahlverfahren

Die Vorteile des DE-MAC sind die durch die Verwendung von TDMA resultierende Kollisionsvermeidung sowie das nicht notwendige Bewerben um Senderechte, was Carrier Sensing überflüssig macht und Kontrollpakete minimiert.

Nachteilig wirkt sich sicherlich der weiterhin sehr hohe Aufwand für Idle listening aus. Ein Knoten muss stets auf Nachrichten anderer Knoten warten, auch wenn keine gesendet werden. Der Schlafzyklus beschränkt sich auf die eigenen Timeslots. Die für das Umschalten zwischen den Modi benötigte hardwarebedingte Zeit kann sich beim häufigen Hin- und Herschalten in Abfolge der eigenen Timeslots zu einem störenden Faktor aufsummieren. Weiterhin wird bei TDMA eine Synchronisation der Knoten

untereinander notwendig, die zusätzlichen Aufwand bedeutet. Auch die Skalierbarkeit ist bei diesen Verfahren sehr schlecht.

Insgesamt ist die Idee der Unterstützung von schwächeren Knoten zwar als sehr positiv anzusehen, die Umsetzung bringt jedoch vielfältige Probleme mit sich, die es noch zu lösen gilt.

3) Zusammenfassung

Die Entwicklung der MAC-Protokolle für Sensornetzwerke zeigt deutliche Fortschritte und macht mit innovativen Ideen und Strukturen auf sich aufmerksam. Leider ist eine genauere Bewertung anhand von realen Einsätzen nicht ohne weiteres möglich, da für die meisten Anwendungen eigene Versionen und Variationen oder auch völlig neue Ansätze entwickelt und eingesetzt werden. So wird im Netzwerk des Great Duck Island ein eigenes Protokoll auf FDMA-Basis benutzt.

Auch gibt es bisher keine vergleichenden Messungen zwischen den verschiedenen bekannten Lösungsansätzen.

Diese Tatsachen resultieren aus den stark unterschiedlichen Voraussetzungen und Zielen der Applikationen, die eine Festlegung auf ein einheitliches MAC-Protokoll für Sensornetzwerke unmöglich machen. Eine Standardisierung erscheint nur schwer möglich und auch nur für verschiedene Anwendungen getrennt realisierbar. So werden bei Forschern, Wissenschaftlern, beim Militär und bei Privatunternehmen auch weiterhin eine Vielzahl verschiedener Systeme mit unterschiedlichen Charakteristiken zu finden sein.

IV. Routing

1) Allgemeine Betrachtungen

Routingprotokolle gibt es bereits viele. Dennoch betrachtet man sie im Allgemeinen als für Sensornetzwerke schlecht oder gar nicht geeignet. Warum?

Sensornetzwerke stehen speziellen Problemstellungen gegenüber, die andere, herkömmlichere Netzwerktypen nicht oder nur in Ansätzen lösen müssen. Das bedeutet allerdings nicht, dass Routingprotokolle für Sensornetzwerke nicht mit ausfallenden Routen zurechtkommen müssten. Sensornetzwerke müssen sich selbst organisieren und haben in der Regel kleine und nicht erneuerbare Energiereserven in den einzelnen Sensoren. Ausfallende Sensorknoten und damit auch Routen, da die Knoten die einzige Netzwerkinfrastruktur sind, sind von Anfang an sicher. Sensornetzwerke haben gewöhnlich, außer wenn die Knoten z. B. mit genügend Solarzellen ausgerüstet sind, durch Energiemangel begrenzte Lebensdauern.

Andere Anforderungen, wie maximaler Durchsatz, sind hingegen von sekundärer Bedeutung.

Diese Anforderungen wiederum prägen die Protokolle. Dazu müssen einige Erklärungen gegeben werden.

a) Selbstorganisation

Alle Knoten sind gleich aufgebaut. Daher unterscheiden sie sich am Anfang nur durch ihre geographische Lage. Im Laufe der Zeit können sie sich durch die in ihren Batterien verbliebene Energie unterscheiden.

Daher ergibt es keinen Sinn vor dem Einsatz Rollenfestlegungen, wie zum Beispiel einen Routingbaum, zu treffen. Die Rollen der Knoten beim Routing und die eigentlichen Routen können erst nach Erreichen der Einsatzposition festgelegt werden. Der extrem komplexe Fall beweglicher Knoten soll hier nicht betrachtet werden.

Die sinnvollen Kriterien zur Festlegung der Rollen und Routen sind, wie gesagt, Energieinhalt und Position im Verhältnis zum Empfänger und zu anderen Knoten. Unglücklicherweise sind diese Informationen nicht immer und überall vorhanden, beziehungsweise, sie zu übermitteln wäre zu aufwändig. In solchen Fällen muss man zu heuristischen Lösungen greifen oder zu Algorithmen mit Zufallselementen (probabilistische Algorithmen).

b) Sparsamer Umgang mit Energie

Konventionelle Routingprotokolle haben die Aufgabe, Kosten zu minimieren. Kosten sind hierbei entweder wörtlich, im monetären Sinne, oder als Latenzzeiten oder Bandbreitenverbrauch zu verstehen. Routingprotokolle für Sensornetzwerke verstehen Kosten als Energieverbrauch. Hier muss man sich vor Augen führen, wodurch Energie in der Kommunikation verloren geht.

Natürlich und am leichtesten einzusehen ist der Energieaufwand in Form der eigentlichen Sendeenergie. Sie hängt von verschiedenen Faktoren ab. Jedoch kann das Routingprotokoll davon in einem Knoten nur die Entfernung des Empfängers wählen, indem es den Empfänger auswählt. Dieser Teil der Kosten einer Route entsteht durch die Addition der Sendeenergien.

Weiterer Energieverbrauch entsteht durch den Betrieb der Sendeelektronik. Deswegen hängt der Energieverbrauch beim Senden nicht nur von der Sendeenergie ab, sondern hat auch einen entfernungsunabhängigen Teil, der davon abhängt, wie lange Sendungen dauern.

In einem gegebenen Knoten kann ein Routingprotokoll nicht beeinflussen, wie lange die Übertragung einer Nachricht dauert. Dies ist tiefer liegenden Schichten vorbehalten. Die Energiekosten im gesamten Netzwerk hängen allerdings davon ab, wie oft eine Nachricht übertragen wird. Die Länge einer Route, im Sinne der Anzahl der teilnehmenden Knoten, nicht im geometrischen Sinne, bestimmt diesen Anteil des Energieverbrauchs.

Zusätzlicher Energieverbrauch entsteht aus drei weiteren Aktivitäten, nämlich dem Initialisieren des Senders, dem Initialisieren des Empfängers und dem Betrieb der Empfangselektronik. Protokolle, die ständige Empfangsbereitschaft voraussetzen, haben also einen erhöhten Energiebedarf.

Zusammenfassen kann man dies in folgenden Formeln:

$$E_{\text{Knoten}} = E_{\text{Betrieb}} + f \cdot E_{\text{Sendung}} = P_{\text{Sender}} \times t + f \cdot P_{\text{Sendung}} \times l \times d^a \quad (1)$$

P Elektrische Leistung

l Länge der Nachricht
 a Ausbreitungskoeffizient
 d Entfernung
 Nachrichten Knoten

$$E_{\text{Netzwerk}} = \uparrow \quad \uparrow \quad E_{\text{Knoten}} \quad (2)$$

Die Aufgabe eines Routingprotokolls besteht darin, mit heuristischen Mitteln ein Minimum des Energieverbrauches des Systemes zu finden.

2) Flooding

a) Grundidee

Unter Flooding versteht man eine Technik, eine Nachricht im ganzen Netzwerk zu verbreiten. Jeder Knoten sendet eine erhaltene Nachricht einfach allen Knoten in seiner Reichweite. Diese Technik steht auch zur Verfügung, bevor komplexeren Protokollen notwendige Information verfügbar sind. Daher wird diese Technik gerne bei der Initialisierung eines Netzwerkes benützt. In gewisser Weise ist Flooding ein Routingprotokoll ohne Routen. Bei probabilistischen Routingprotokollen kann Flooding auch als Hilfsverfahren im Versagensfalle dienen.

Dabei kann man zwischen zwei Verfahren unterscheiden. Einerseits kann man Anfragen in das Sensornetzwerk hineinfluten, und andererseits kann man Nachrichten über Ereignisse hinausfluten. Welches Verfahren zu bevorzugen ist, hängt davon ab, welcher Anteil der Ereignisse, die die Knoten beobachten, im Augenblick von Interesse sind.

b) Implikationen

Flooding stellt sehr große Anforderungen an die unteren Schichten des Kommunikationssystem, weil es viele unkoordinierte Broadcasts einsetzt. Selbst im günstigsten Falle skaliert der Energieaufwand linear mit der Anzahl der Knoten und Nachrichten.

c) Verbesserungsmöglichkeiten

Wenn die Knoten über geographische Informationen über ihre eigene Lage und die Lage des Zieles verfügen, können sie bei vorausgesetzter homogener Verteilung der Knoten die Skalierung verbessern, indem sie die Nachricht nur wiederholen, wenn sie zwischen Ziel und Quelle liegen. Die Skalierung erfolgt mit der Wurzel der Anzahl der Knoten.

3) Shortest Hop First

a) Einführung

Hier betrachten wir erstmal, sozusagen als schlechtes Beispiel, ein sehr einfaches Routingprotokoll - Shortest Hop First.

Es handelt sich dabei um ein nur wenig abgewandeltes Protokoll aus der Welt der konventionellen, leitungsgebundenen Kommunikation. Dabei verhält sich jeder Knoten egoistisch und benutzt geographische Informationen um den Weg zu wählen. Dies setzt voraus, dass die Knoten wissen, wo sie sind und wo das Ziel liegt. Die Frage, wie sich Knoten diese Informationen verschaffen, ist nicht Aufgabe eines Routingprotokolls, also nehmen wir sie hier als gelöst an.

b) Grundidee

Ein Knoten wählt den nächsten Knoten einer Route danach aus, wie weit, in Sendeenergie ausgedrückt, die anderen Knoten vom Ziel und vom aktuellen Knoten entfernt sind. Als Kandidaten für das nächste Zwischenziel kommen nur Knoten in Frage, die dem Ziel näher sind als der aktuelle Knoten. Von all diesen Knoten wird der, der dem aktuellen Knoten am nächsten ist, ausgewählt.

Um die Leichtigkeit der Implementierung zu zeigen, hier in leicht vereinfachtem Pseudocode:

```

FÜR alle Knoten
    WENN Knoten.distanz(ziel) < selbst.distanz(Ziel)
        DANN Kandidaten.aufnehmen(Knoten)
entfernung = unendlich
zwischenziel = NULL
FÜR alle Kandidaten
    WENN entfernung > Kandidat.distanz(ziel)
        DANN
            entfernung = Kandidat.distanz(ziel)
            zwischenziel = Kandidat

```

c) Aufbau der Datenstrukturen

Das Protokoll arbeitet mit geographischen Informationen. Nachdem sie ermittelt worden sind, müssen sie zumindest den Nachbarn übermittelt werden. Gibt es nur ein Ziel, dessen Standort bekannt ist, genügt es, nur den Nachbarn den eigenen Standort mitzuteilen. Sonst müssen die Standorte weiter verbreitet werden.

Eine alternative Methode zum Aufbau eines Routingbaumes besteht darin, das Ziel den Aufbau des Baumes einleiten zu lassen, indem eine Nachricht durch Flooding weiterverbreitet wird. Entfernung lässt sich in diesem Falle direkt als Signalstärke beim Empfang messen. Dies ist, weil der Verlust an Signalstärke nicht linear und auch nicht vorhersagbar von der geometrischen Entfernung abhängt, ein Verfahren

mit geringerem Energieverbrauch. Allerdings gibt es, vor allem militärische, Anwendungen, bei denen es unakzeptabel ist, dass das Ziel anpeilbare Signale von sich gibt.

d) Mängel der Selbstorganisation

Bei diesem Verfahren können sich Sackgassen bilden. Das Verfahren blickt nicht voraus und kann nicht abschätzen, ob ein aus rein geographischen Gründen ausgewählter Knoten oder seine Nachfolger Routen, die zum Ziel führen, haben.

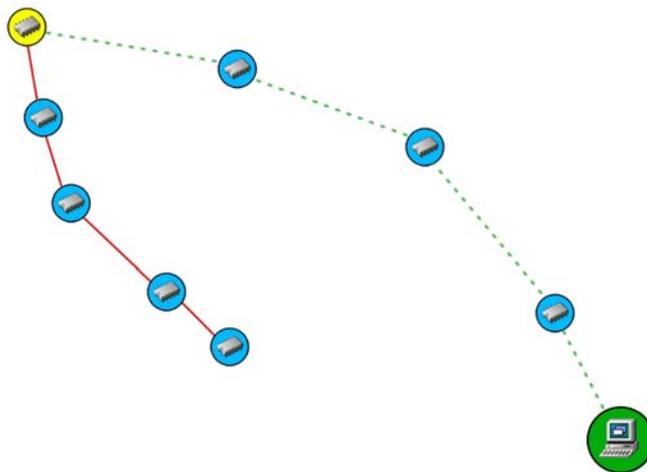


Fig. 13. Pathologische geografische Verteilung. Der vom egoistischen Algorithmus gewählte Weg in rot. Der ideale Weg grün-gestrichelt. Quelle in gelb. Ziel in grün.

Um in solch einem Falle die Nachricht zustellen zu können, muss man die Technik des Backtracking benutzen. Das führt zu vielen eigentlich vermeidbaren Übertragungen. Die alternative Aufbaumethode bildet am Anfang natürlich keine Sackgassen. Sie können sich nur nachträglich durch Ausfall von Knoten bilden.

e) Zeitlich ungleichmäßige Entwicklung der Energievorräte der Knoten

Unter der Annahme, dass es ein einheitliches, unbewegliches Ziel der überwiegenden Anzahl aller Nachrichten gibt und eine zufällige Verteilung der überwiegenden Anzahl aller Datenquellen gibt, stellt sich ein charakteristisches Muster des Datenverkehrs ein. Nachrichten laufen auf einem Zickzackkurs eine Hyperfläche hinab, deren tiefsten Punkt das Ziel darstellt.

Eine sehr kleine Anzahl (Nähe ist richtungsabhängig) oder auch nur ein Knoten muss dem Ziel am nächsten liegen. Über ihn oder sie laufen alle Nachrichten. Das belastet die dem Ziele nächsten Knoten überdurchschnittlich. Ihre Batterien werden zuerst erschöpft. Dadurch läuft eine "Sterbefront" vom Ziel aus durch das Netzwerk. Sie beschleunigt sich sogar, weil der Abstand, den die dem Ziele nächsten Knoten überwinden müssen, immer weiter ansteigt und damit auch der Energieverbrauch durch nötig werdende höhere Sendeleistungen.

Es kann auch zu einem abrupten Tode des ganzen Netzwerkes kommen, wenn die Maximalreichweite des dem Ziele nächsten Knoten nicht ausreicht.

f) Vorteile

Der wesentliche Vorteil dieses Routingprotokolles ist sein einfaches und daher leicht zu implementierendes Prinzip.

Weiterhin bedingt diese Einfachheit, dass außer bei der Initialisierung nur Nachrichten mit Nutzlast übertragen werden.

4) Selbstorganisiertes Baumverfahren mit wechselnden Astknoten

a) Grundidee

Die Knoten organisieren sich selbst in Gruppen und mindestens zwei Ebenen, die aus Blattknoten und Astknoten gebildet werden. Die Astknoten dienen als Zwischenstationen in der Nachrichtenübertragung. Eine Gruppe besteht aus einem Astknoten und benachbarten Blattknoten, beziehungsweise Astknoten einer tieferen Ebene.

b) Initialisierung

Zuerst werden Gruppen gebildet. Dazu ernennt sich ein gewisser Prozentsatz der Knoten nach dem Zufallsprinzip zu Astknoten. Ein Blattknoten wählt den sendeenergetisch nächstgelegenen Astknoten und schließt sich seiner Gruppe an.

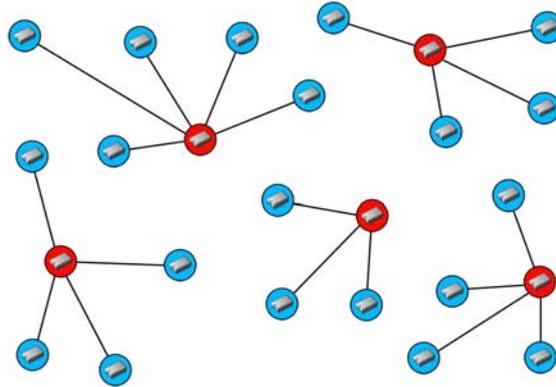


Fig. 14. In Gruppen aufgeteiltes Sensornetzwerk. Astknoten in rot.

c) Auswahl der Astknoten

Während die geometrischen Informationen in Form der geringsten Sendeenergie, die benötigt wird, um einen Astknoten zu erreichen, benutzt werden, um Gruppen zu bilden, werden Informationen über die Energievorräte benutzt, um die Astknoten neu auszuwählen.

Ergibt sich aus irgendeinem Grunde die Notwendigkeit einen neuen Astknoten zu wählen, so entscheidet sich ein Knoten zufällig, mit einer vom Energievorrat im Verhältnis zur bisherigen Betriebsdauer des Sensornetzwerkes abhängigen Wahrscheinlichkeit, ob er die Rolle eines Astknoten ausfüllen will.

d) Ablauf der Kommunikation

Kommunikation mit Nutzlasten läuft strikt hierarchisch ab.

Nachrichten laufen von einem Blattknoten oder einem Astknoten zu einem höher liegenden Astknoten, bis sie einen Astknoten der höchsten Ebene erreicht hat, der direkt mit dem Ziel kommuniziert.

e) Kontrolle der Kommunikation

In einer Gruppe wird die gesamte Kommunikation nach einem zeitlichen Schema, das der Astknoten festlegt, durchgeführt. Dabei werden jedem Blattknoten Sende- und Empfangszeitintervalle zugeteilt. So sind die Blattknoten in der Lage, außerhalb des ihnen zugeteilten Zeitintervalls ihre Kommunikationssysteme vollständig abzuschalten. Nur innerhalb eines Empfangszeitintervalls muss der empfangende Teil des Kommunikationssystems eingeschaltet sein. Auf diese Weise kann der

Energieverbrauch reduziert werden, wie man am Term E_{Betrieb} der Formel (1) ersehen kann.

Außerdem gestattet eine zentralisierte Weiterleitung der Nachrichten eine Bündelung mehrer Nachrichten, die nach oben weitergeleitet werden sollen, in einen Sendezeitschlitz. Dies reduziert den Energieaufwand auf zweifache Weise.

Einerseits wird der Protokollaufwand niedriger Schichten des Kommunikationsprotokolls auf den Aufwand einer Nachricht reduziert, obwohl mehrere Nachrichten so übertragen werden. Andererseits muss die zur Initialisierung der Sendeelektronik aufzuwendende Energie nur einmal aufgebracht werden, statt für jede Nachricht einzeln.

Wenn man bereit ist, die Trennung der Schichten des Kommunikationssystems aufzuweichen, sind noch weitere Einsparungen möglich. Dazu müssen höhere Protokollschichten die empfangenen Nachrichten analysieren und zusammenfassen. Dabei können auch Verluste an Genauigkeit der Messdaten in Kauf genommen werden. Danach müssen nur noch geringere Datenmengen über große Entfernungen übertragen werden.

f) Neuauswahl der Astknoten

In der bisher vorgestellten Form führt das Routingprotokoll zu einer energetischen Schonung der Blattknoten auf Kosten der Astknoten, die die ganze Bürde der Kommunikation auf weite Entfernungen tragen und ihre Empfangselektronik dauernd betreiben müssen.

Die Energiereserven des Astknoten wären bald verbraucht und nachdem die Blattknoten bemerkten, dass der Astknoten ausgefallen ist, würde eine Neuauswahl der Astknoten durchgeführt. Dabei fiel allerdings der Sensor des früheren Astknotens, der aus Energiemangel den Betrieb eingestellt hat, weg. Außerdem führte dieses Verfahren, da normalerweise nur ein Astknoten gleichzeitig ausfiel, zu einer Aufsplitterung der Gruppen.

Deswegen gibt der alte Astknoten seine Eigenschaft, nachdem er einen gewissen Energiebetrag verbraucht hat, einem Nachfolger höherer Energiereserven ab. Leider ist es ungünstig, direkt den verbleibenden Energievorrat als Kriterium zu verwenden. In diesem Falle entschiede der Astknoten jeder Gruppe unabhängig von anderen Astknoten, wann er seine Rolle aufgeben möchte. Damit müsste sich gewöhnlich jede Gruppe alleine reorganisieren, weil es unwahrscheinlich ist, dass Astknoten benachbarter Gruppen innerhalb der kurzen Zeitspanne der Neuorganisation den kritischen Punkt ihres Energievorrates erreicht.

Da die Anzahl der innerhalb einer Gruppe neu auftretenden Astknoten zufällig ist und in dem Falle, dass sich 0 neue Astknoten bilden, eine neue Runde stattfindet, bilden sich im Durchschnitt mehr als 1 neuer Astknoten. Das Sensornetzwerk splitterte in immer mehr Gruppen auf, wodurch der Anteil der Astknoten auf ungünstige Höhen anstiege.

Um das zu vermeiden, zwingt man alle Astknoten, ihre Rollen aufzugeben, indem man festlegt, dass die Rollen nach einer bestimmten, für alle Knoten gleichen Zeit aufgegeben werden müssen. So organisiert sich das ganze Sensornetzwerk neu.

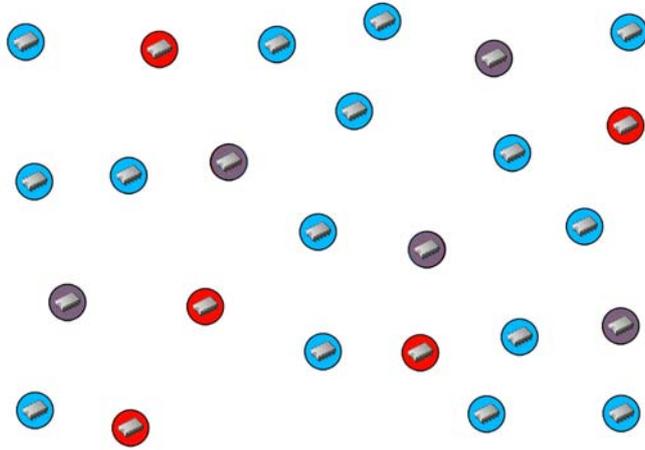


Fig. 15. Zur Neuwahl geben die alten Astknoten ihre Funktion ab und neue Astknoten werden zufällig ausgewählt. Alte Astknoten in purpur. Neue Astknoten in rot.

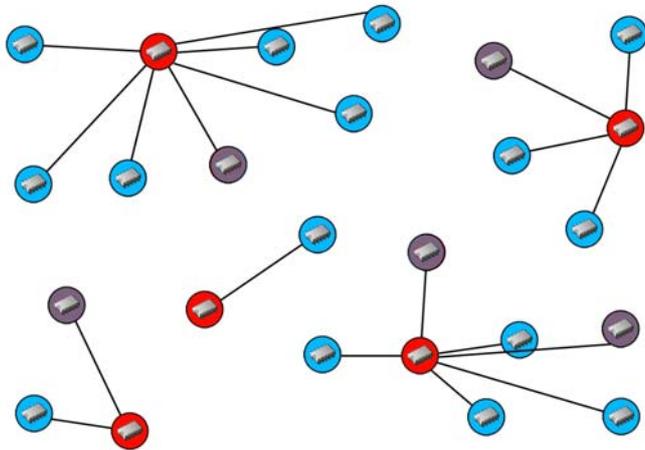


Fig. 16. Neubildung von Gruppen um die neuen Astknoten. Neue Astknoten in rot. Alte Astknoten in purpur.

Es ist auch nicht sinnvoll, die Betriebsdauer des Sensornetzwerkes als absolute Zeit zu benutzen. Wichtig für die Zwecke des Routingprotokolls ist nur, wie oft ein Knoten bereits Astknoten gewesen ist. Man kann auch, wenn man davon ausgeht, dass Kommunikation der Hauptenergieverbraucher eines Knoten ist, den Energievorrat durch die Zeitdauer, die ein Knoten Astknoten gewesen ist, annähern.

Dadurch kommt man auf folgende Formeln für die Wahrscheinlichkeit, das ein Knoten sich entscheidet Astknoten zu werden:

$$S=0, \text{ falls es in der Gruppe Knoten gibt, die seltener Astknoten waren} \quad (3)$$

$$S=P/1 \checkmark P \times r \bmod \frac{1}{P} \checkmark, \text{ sonst} \quad (4)$$

P Anteil der Astknoten
r Aktuelle Runde

So kann man erreichen, dass ein Knoten kein weiteres Mal Astknoten wird, solange es Knoten gibt, die seltener Astknoten gewesen sind.

g) Parameter

Das Routingprotokoll hat drei vor dem Einsatz festzulegende Parameter.
Die Anzahl der Routingebenen.
Die Dauer der Rolle eines Astknotens.
Der Anteil der Astknoten.

Eine analytische Methode, optimale Parameter festzulegen, ist nicht bekannt.
Im praktischen Einsatz greift man zu Simulationen und Faustregeln.

h) Nachteile

Das Verfahren setzt voraus, dass jeder Knoten die Fähigkeit besitzt, Astknoten zu werden. Es ist also nicht möglich, dieses Routingprotokoll einzusetzen, wenn das Ziel der Nutzdaten nur von einem Teil der Knoten direkt erreicht werden kann, sei es, weil es Hindernisse im Einsatzfeld gibt, oder weil das Sensornetzwerk zu groß ist.

Eine Aggregation der Nutzdaten in den Astknoten ist nicht in jedem Falle möglich, entweder weil kein Verlust der Genauigkeit vertretbar ist, oder auch wenn die Übertragungszeit so klein gehalten werden muss, dass Daten nicht zwischengespeichert werden können.

Durch den Wechsel der Rolle als Astknoten tritt Kontrolldatenverkehr auf. Das Protokoll wird ineffizient, wenn der Energieverbrauch durch Kontrolldatenverkehr gegenüber dem Energieverbrauch durch Datenverkehr nicht mehr als klein betrachtet werden kann.

i) Vorteile

Das Protokoll kommt gut mit ungleich verteiltem Nachrichtenaufkommen zurecht.

Mit einer Wahrscheinlichkeit von $1-a/n$ (a/n : Anteil der Astknoten) muss nur die Sendeenergie für eine Übertragung über eine kurze Entfernung aufgewendet werden. So kann die Belastung auf viele Batterien verteilt werden.

5) Routing auf Basis von Ereignissen mit Gerüchten

a) Einführung

Bis jetzt haben wir Protokolle betrachtet, die eine wichtige Eigenschaft mit konventionellen Protokollen leitungsgebundener Systeme gemein haben: Die grundlegenden Subjekte dieser Protokolle sind einzelne Knoten, die einzeln als solche adressiert werden können.

Es ist jedoch auch möglich, ein Sensornetzwerk als ein großes Messgerät zu betrachten, das beauftragt werden kann, bestimmte Messgrößen zu liefern. Die grundlegende Einheit der Adressierung ist in diesem Falle nicht ein einzelner Knoten, sondern Messdaten, die interessant sind, werden als solche beschrieben und dem Netz übergeben.

b) Grundidee

Knoten, die ein Ereignis beobachten erzeugen Gerüchte, die Informationen über Routen zu Ereignissen weiterverbreiten.

Ziele, im Folgenden Beobachter genannt, bringen Anfragen, die sich wie Gerüchte verhalten, ins Sensornetzwerk. Eine funktionierende Route entsteht, wenn sich die Wege passender Gerüchte und Anfragen kreuzen. Es handelt sich hierbei um ein heuristisches Verfahren. Es gibt keine Garantie, dass eine Anfrage eine Route hervorbringt. In solch einem Falle muss der Beobachter auf ein anderes Verfahren, in der Regel Flooding der Anfrage, zurückgreifen.

Das Protokoll hat entfernte Ähnlichkeiten mit Shortest Hop First, funktioniert aber ohne feste Routen oder Ziele (Beobachter) und ohne geographische Informationen.

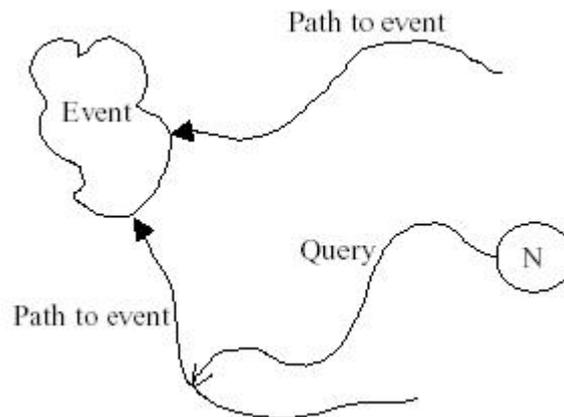


Fig. 17. Grundlegende Funktionsweise des Routings auf Basis von Gerüchten. N markiert das Ziel, von dem die Nachfrage ausgeht, welche einen der Pfade trifft, die zu dem Gebiet, in dem ein Ereignis beobachtet wird, führen.

c) Initialisierung

Jeder Knoten muss seine Nachbarn kennen. Dazu macht er sich am Anfang seinen Nachbarn durch eine Sendung bekannt. Jeder Knoten unterhält eine Liste seiner Nachbarn.

d) Routen

Eine potentielle Route existiert in einem Knoten als Reihe in einer Tabelle von Anfragen und Gerüchten mit Spalten für den nächsten Knoten und die Anzahl der Übertragungen von Knoten zu Knoten. Bei sehr vielen Anwendungen kommt noch ein Verfallsdatum hinzu.

e) Anfragen

Eine Anfrage beinhaltet eine Beschreibung des gesuchten Ereignisses und eine Lebensdauer in Schritten, die bei jeder Weitergabe verringert wird. Die Beschreibung eines Ereignisses ist anwendungsabhängig und kann meistens als Bitstring aufgefasst werden.

Leider ist das nicht immer möglich, denn es muss entschieden werden, ob ein Gerücht und eine Anfrage zueinander passen. Bei manchen Anwendungen kann dies geschehen, indem man die Beschreibungen der Anfrage und des Gerüchts als Bitstrings vergleicht. Bei anderen Anwendungen ist das nicht möglich und die Schichtung des Kommunikationssystemes muss verletzt werden, um Beschreibungen zu interpretieren.

f) Gerüchte

Gerüchte haben wie Anfragen eine Lebensdauer.

Im Unterschied zu Anfragen enthalten Gerüchte die Beschreibung aller Ereignisse, denen das Gerücht auf seinem Wege durch das Sensornetzwerk begegnet ist, mit den dazugehörigen Routen in Form ihres nächsten Knotens.

In jedem Knoten wird die Tabelle der Ereignisse im Gerücht mit der Tabelle des Knotens abgeglichen. Dabei werden fehlende Ereignisse hinzugefügt und die bessere Route doppelt vorhandener Ereignisse ausgewählt.

Je nach verwendeten unteren Schichten des Kommunikationssystemes hören Knoten einige Nachrichten, also auch Gerüchte, die nicht direkt ihnen geschickt werden, mit. Solche Gerüchte werden genutzt, indem ihnen in der Tabelle des Knotens fehlende Ereignisse und bessere Routen, entnommen werden. Natürlich dürfen sie nicht weitergegeben werden, um keine exponentielle Vermehrung von Gerüchten auszulösen.

g) Wegewahl

Die Wahl des Weges einer Antwort, zu der immer eine Beschreibung vorliegt, und einer Anfrage, zu der ein passendes Ereignis in der Tabelle vorliegt, ist trivial. Der Knoten, dem die Nachricht zu senden ist, ist in der Tabelle verzeichnet.

Die anderen Fälle, ein Gerücht und eine Anfrage, zu der kein passendes Ereignis vorliegt, sind komplexer. Sie müssen auf zufälliger Basis weitergegeben werden. Da alle Knoten eines Sensornetzwerkes gleich sind, ist es nicht trivial, einen günstigen nächsten Knoten auszuwählen.

Die Grundlage der Wegewahl beruht hier auf theoretischen geometrischen Überlegungen. Zwei Geraden in einer Fläche schneiden sich entweder oder sind parallel. Die Wege hier sind keine Geraden. Erstens haben sie durch die Lebensdauer eine begrenzte Länge und, da Knoten nur durch einen unwahrscheinlichen Zufall in gerader Linie liegen, sind sie auch krumm und machen Kurven. Das stellt die Funktionstüchtigkeit des Verfahrens nicht in Frage. Im Gegenteil, Kurven erhöhen die Wahrscheinlichkeit, dass Routen optimiert werden.

Trotzdem muss man darauf achten, dass sich Kurven nicht zu Schleifen oder, noch schlimmer, Spiralen entwickeln, denn diese Wege haben geringe Wahrscheinlichkeiten, sich zu schneiden.

Wenn die Knoten ihre geographische Lage kennten, wäre das kein Problem. Da man die damit verbundenen, hohen, durch Einbau eines GPS-Empfängers in die Knoten bedingten Kosten scheut, benutzt man die bei der Initialisierung aufgebauten Nachbarschaftslisten. Jeder Knoten sendet seinen Nachbarn, entweder bei der Initialisierung oder mit Gerüchten verbunden, die eigene Nachbarschaftsliste. Der empfangende Knoten wählt aus seiner Nachbarschaftsliste einen Knoten, der nicht in der erhaltenen Nachbarschaftsliste enthalten ist, wenn es möglich ist. Am Rande des Sensornetzwerkes ist es nicht möglich und die Nachricht muss "reflektiert" werden.

h) Gerüchte erzeugen

Ein Knoten, der ein Ereignis misst, ist nicht gezwungen, sofort ein Gerücht zu erzeugen. Er kann warten, bis ein Gerücht bei ihm eintrifft und es dann mitbenutzen.

Deswegen kann man einen zufallsgesteuerten Erzeugungsalgorithmus benutzen, wobei man eventuell mit einer Zeitschranke, die nicht überschritten werden darf, und Gewichtungen nach Anzahl und Alter neuer Ereignisse arbeitet.

i) Parameter

Es gibt lediglich zwei Parameter.

Die Kriterien, nach denen Gerüchte erzeugt werden. Sie hängen in hohem Maße von den Anforderungen der Anwendung ab.

Die Lebensdauer der Anfragen und Gerüchte. Hier hat sich gezeigt, dass länger lebende Gerüchte effizienter sind als mehr Gerüchte.

j) Nachteile

Das Verfahren ist probabilistisch. Es kann nicht garantiert werden, dass eine Anfrage beantwortet wird.

Auch ohne Anfragen werden Gerüchte erzeugt. Dieser Verkehr kann unnützen Energieverbrauch bedeuten.

k) Vorteile

Das Verfahren arbeitet auch in Sensornetzwerken, deren Größe die Maximalreichweite eines Knoten überschreitet.

Mehrere Beobachter bedeuten keinerlei Komplikation.

6) Bewertungen

a) Allgemeines

Kein Protokoll kann alle Wünsche erfüllen, noch ist jedes Protokoll für jeden Einsatzzweck geeignet.

Man kann die Eignung eines Protokolls am ehesten aus den Charakteristiken des Datenverkehrs ablesen. Insbesondere ist wichtig, ob die Resultate einer Anwendung als Ereignisse beschrieben werden können. Wenn nicht, verbietet sich der Einsatz eines ereignisorientierten Protokolls.

Sind die Daten zusammenfassbar oder auf andere Weise noch im Sensornetzwerk vorverarbeitbar, so dass sich das Datenvolumen oder die Anzahl der Nachrichten verringern, sollte man diese Möglichkeit unbedingt nutzen.

b) Abhängigkeiten vom Datenverkehr

Grundsätzlich gibt es immer ein Mindestmaß Datenverkehr, unterhalb dessen Flooding das günstigste Protokoll ist. Allerdings ist Flooding natürlich nur bei ereignisorientierten Anwendungen oder Anweisungen an die Knoten möglich.

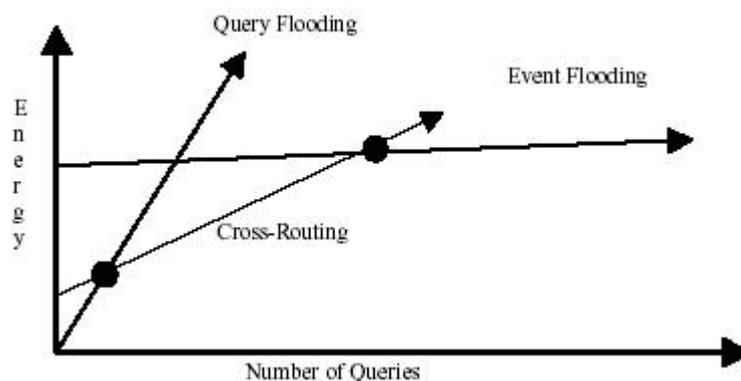


Fig. 18. Gegenüberstellung der Effizienz einzelner Protokolle in Abhängigkeit der Anzahl zu versendender Anfragen. Query Flooding: Anfragen fluten. Event Flooding: Ereignisse fluten. Cross-Routing: Routing mit Gerüchten

Auch ist die Beziehung von Quelle und Ziel der Datenübertragungen wichtig. Bei Anwendungen, bei denen Broadcast oder Multicast an größere Gruppen einen bedeutenden Teil des Verkehrsaufkommens ausmachen, sind hierarchische Verfahren nahezu unschlagbar.

V. Ausblick

Die Entwicklungen zeigen, dass sich das Bild der Sensornetze ändern wird. Manche Sensoren sind schon jetzt so klein und effizient, dass sie mit einer Leistung von 100 Mikrowatt laufen können. So könnten sie sich bald Energiequellen wie Temperaturschwankungen oder kinetische Energie zu Nutze machen, so dass sie unabhängig von eigenen Batterien ungeahnte neue Möglichkeiten zur Anwendung in sich tragen.

Ohne Frage werden die Sensornetzwerke auch in Zukunft ein bedeutsames Thema bleiben, und in kaum einem anderen Gebiet wurden in den letzten Jahren wohl vergleichbare Fortschritte gemacht. Dass dies so ist, verdanken wir vor allem dem Militär. Doch schon längst hat diese Technik ihren Weg in das Zivilleben und sogar in die Privatsphäre vieler Menschen gemacht. Bald werden viele dieser Anwendungen selbstverständlich werden und nicht nur Thema der Forschung sein, sondern auch einen großen Markt darstellen. Bleibt zu Hoffen, dass es der Wissenschaft gelingt, trotz fließender Übergänge diese Grenzen so eindeutig wie möglich zu ziehen, so dass sich nicht die Menschen selber zu Zielobjekten wandeln und sich plötzlich an der Stelle des eingangs erwähnten Eichhörnchens wieder finden.

References

- [1] Benjamin Fulford, "Sensors gone wild", The Forbes Magazine, <http://www.forbes.com/global/2002/1028/076.html>, 28.10.2002
- [2] K. Finkenzeller, RFID-Handbuch, Tibbett & Britten, Sainsbury's RFID Trial, Hanser-Verlag, ISBN 3-446-22071-2, 2002.
- [3] Schwiebert, Gupta, Weinmann, "Habitat Monitoring: Application Driver for Wireless Communications Technology", First ACM SIGCOMM Workshop on Data Communications in Latin America and the Caribbean, San Jose, Costa Rica, 3-5 April 2001. Auch in UCLA Computer Science Technical Report 200023, Dezember 2000.
- [4] P. Bauer, M. Sichertiu, R. Istepanian, K. Premaratne, "The Mobile Patient: Wireless Distributed Sensor Networks for Patient Monitoring and Care", Proc. of the IEEE Conference on Information Technology Applications in Biomedicine (IEEE ITAB 2000), pp. 17-21, Arlington, Virginia, Nov. 2000.
- [5] Mainwaring, Alan. Polastre, Joseph. Szewczyk, Robert. Culler, David. Anderson, John, "Wireless Sensor Networks for Habitat Monitoring", First ACM Workshop on Wireless Sensor Networks and Applications, Atlanta, GA, USA, 28. September 2002.

- [6] Requicha, Caron, Estrin, Sukhatme, Zhou, "Monitoring of Marine Microorganisms", <http://cens.ucla.edu/Research/Applications/momm.htm>
- [7] M. Srivastava, R. Muntz, M. Potkonjak, "Smart Kindergarten: Sensor-based Wireless Networks for Smart Developmental Problem-solving Environments" in "Mobile Computing and Networking", pp. 132-138, in The Seventh Annual International Conference on Mobile Computing and Networking, 2001.
- [8] National Science Foundation Award Abstract #0085773
<https://www.fastlane.nsf.gov/servlet/showaward?award=0085773>
- [9] <http://www.dust-inc.com>
- [10] http://www.xbow.com/Products/Wireless_Sensor_Networks.htm
- [11] http://www.microstrain.com/wireless_sensors.htm
- [12] S. Singh, C.S. Raghavendra, "PAMAS: Power aware multi-access protocol with signalling for ad hoc networks", ACM Computer Communication Revue, vol. 28, no. 3, pp. 5-26, Juli 1998.
- [13] Ye, Heidemann, Estrin, "An Energy-Efficient MAC Protocol for Wireless Sensor Networks", USC/ISI Technical Report ISI-TR-543, 2001.
- [14] Woo, Culler, "A Transmission Control Scheme for Media Access in Sensor Networks", Proc. ACM MobiCom '01, Rom, Juli 2001.
- [15] A. El-Hoiydi, "Aloha with Preamble Sampling for Sporadic Traffic in Ad Hoc Wireless Sensor Networks", in Proc. IEEE International Conference on Communications (ICC 2002), New York, 2002.
- [16] A. El-Hoiydi, "Spatial TDMA and CSMA with Preamble Sampling Aloha with Preamble for Low Power Ad Hoc Wireless Sensor Networks", in Proc. IEEE International Conference on Computers and Communications (ISCC 2002), Italien, 2002.
- [17] R. Kalidindi, L. Ray, R. Kannan, S. S. Iyengar, "Distributed Energy-Aware MAC Protocol for Wireless Sensor Networks", International Conference on Wireless Networks, Las Vegas, Nevada, Juni 2003.
- [18] Wendi Rabiner Heinzelman, Anantha Chandrakasan, Hari Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks", Proceedings of the 33rd Hawai'i International Conference on System Sciences-2000