Freie Universität Berlin

An overview on Wireless Sensor Networks

Proseminar Technische Informatik

Fabian Nack

WS 08/09

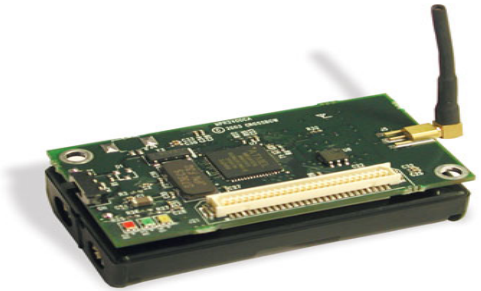
30. 01. 2009

Gliederung

1. Einführung
    1. Was versteht man unter einem DSN (I)
    2. Was versteht man unter einem DSN (II)
    3. Anwendungsgebiete
    4. Herausforderungen
2. Komponenten, Topologie und Routing
    1. Hardwarekomponenten
    2. Softwarekomponenten
    3. Netzwerktopologie
    4. Routingprotokolle
3. Stärken und Schwächen
    1. Stärken von DSN
    2. Schwächen von DSN (I)
    3. Schwächen von DSN (II)
    4. Gegenüberstellung
4. Zusammenfassung

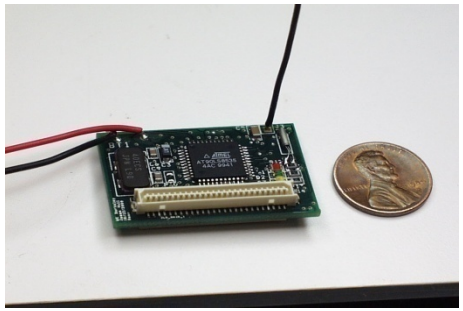
Was versteht man unter einem DSN (I)

- Ein Drahtloses Sensornetzwerk (DSN)
  - ist bestehend aus mehreren, **räumlich verteilten**, **autonomen** Geräten
  - ist dabei **selbst-organisierend**
  - kommt **ohne vorhandene Infrastruktur** aus.

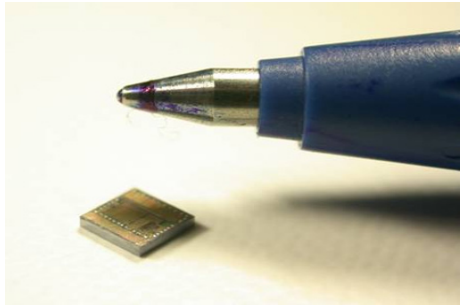


Crossbow MICAz 2.4GHz

Crossbow Cricket



UCB Rene Mote

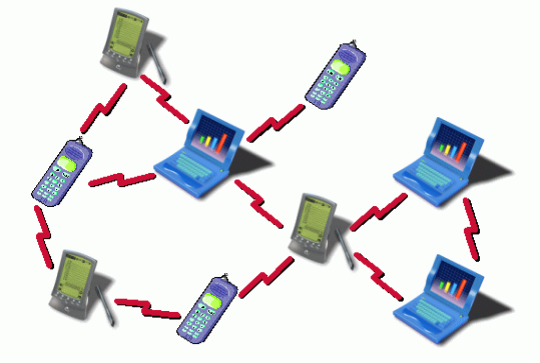


Spec Mote

Was versteht man unter einem DSN (II)

Spezielle Form von Ad-hoc-Netzwerken

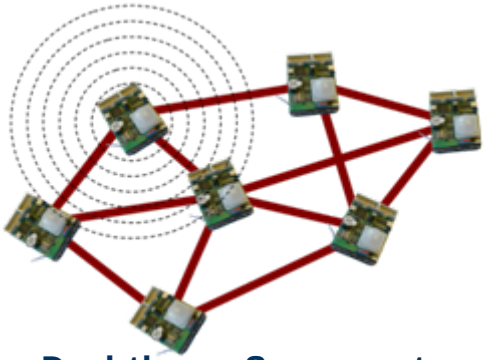
=> Jeder Knoten besitzt einen Transceiver



Typisches Ad-hoc-Netzwerk

- Fokus bei üblichen Ad-hoc-Netzen
  - Kommunikation / Austausch von Informationen
  - Geräte nah am menschlichen Nutzer
  - Interaktion mit dem Nutzer

- Fokus bei Drahtlosen Sensornetzwerken
  - Interaktion mit der Umwelt
  - Messen und Aufzeichnen von physik. / chem. / biol. Größen
  - Überwachung der Umgebung



Drahtloses Sensornetz

Anwendungsgebiete

- Hohe Vielfalt an Applikationen, z.B.:
  - Militäranwendungen
  - Umweltanwendungen
  - Anwendungen im Gesundheitsbereich
  - Kommerzielle Anwendungen
  - Heimanwendungen
  - Viele mehr…

Herausforderungen

Um in diesen, teils stark sicherheitsrelevanten Gebieten einsatzfähig zu sein, müssen DSN natürlich einige Voraussetzungen erfüllen:

Herausforderungen

Um in diesen, teils stark sicherheitsrelevanten Gebieten einsatzfähig zu sein, müssen DSN natürlich einige Voraussetzungen erfüllen:

- Zuverlässigkeit

Herausforderungen

Um in diesen, teils stark sicherheitsrelevanten Gebieten einsatzfähig zu sein, müssen DSN natürlich einige Voraussetzungen erfüllen:

- Zuverlässigkeit
- Energieeffizienz

Herausforderungen

Um in diesen, teils stark sicherheitsrelevanten Gebieten einsatzfähig zu sein, müssen DSN natürlich einige Voraussetzungen erfüllen:

- Zuverlässigkeit
- Energieeffizienz
- Mobilität

Herausforderungen

Um in diesen, teils stark sicherheitsrelevanten Gebieten einsatzfähig zu sein, müssen DSN natürlich einige Voraussetzungen erfüllen:

- Zuverlässigkeit
- Energieeffizienz
- Mobilität
- Sicherheit

Herausforderungen

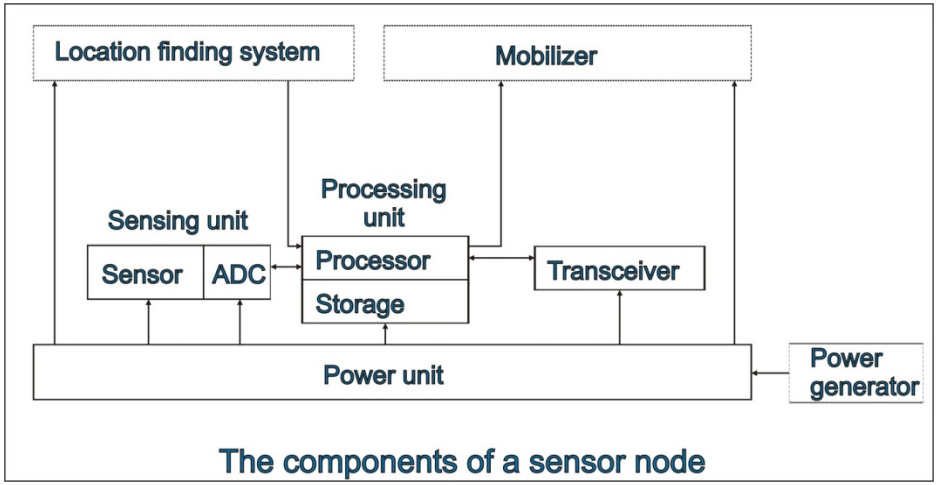
Um in diesen, teils stark sicherheitsrelevanten Gebieten einsatzfähig zu sein, müssen DSN natürlich einige Voraussetzungen erfüllen:

- Zuverlässigkeit
- Energieeffizienz
- Mobilität
- Sicherheit
- Geringe Größe der einzelnen Komponenten

Hardwarekomponenten

Ein typischer Sensorknoten besteht **primär** aus folgenden Bestandteilen:

- Low-power Prozessor
- Memory / Storage
- Radio Transceiver
- Sensor mit ADC-Einheit
- Energiequelle
- Häufig: System zur Standortlokalisierung



The components of a sensor node

Softwarekomponenten

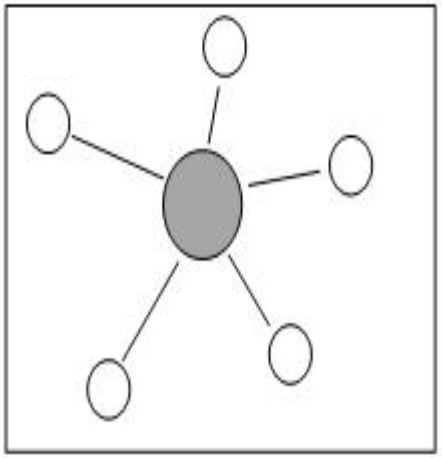
Die Softwarebestandteile eines Sensorknotens können typischerweise in **5 Untergruppen** eingeteilt werden:

- Microcode des OS
- Sensortreiber
- Software zur Abwicklung der Kommunikation
- Treiber für die Kommunikationskomponenten
- Mini-Applikationen, z.B. zur Datenweiterverarbeitung

Netzwerktopologie

1. Single-Hop Star-Topologie

- Alle Knoten **kommunizieren direkt** mit Gateway
- Vereinfacht viele schwierige Netzwerk-Fragen, z.B. Routing
- Probleme, unter anderem: Knoten mit höherer Entfernung zum Gateway erleben schlechte Verbindungsqualität => **Kaum Mobilität**

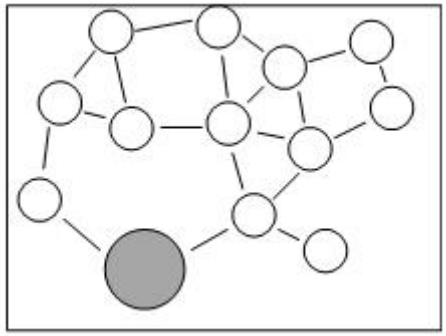


Star-Netzwerk

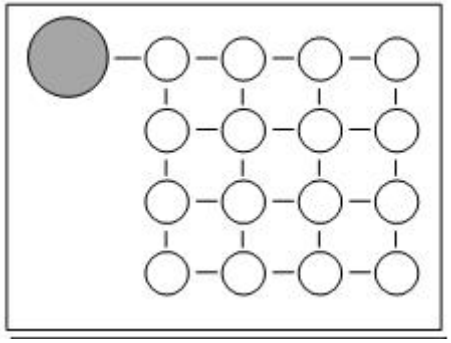
Netzwerktopologie

2. Multi-Hop Maschen- und Gitter-Topologie

- **Multi-Hop** nötig um größere Gebiete abzudecken
- Signal springt von Knoten zu Knoten bis zum Erreichen des Gateways
- Notwendigkeit eines Routing-Protokolls zum Bestimmen des Weges



Maschen-Topologie

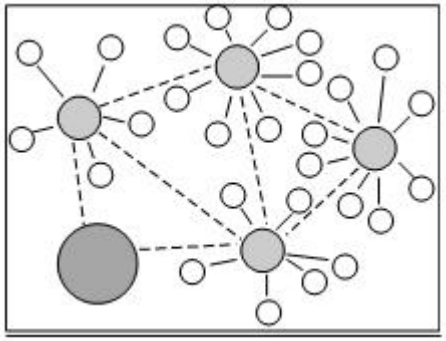


Gitter-Topologie

Netzwerktopologie

3. Hierarchische Topologie

- Wird normalerweise **für große DSN** verwendet
- Die Sensorknoten eines Bereichs schicken ihre Daten an einen sogenannten Clusterhead für ihr Region
- Die Clusterheads bilden wiederum ein Netz
- Netzwerk ist **in Zonen geteilt**



Two-Tier Hierarchie

Routingprotokolle

- Energieeffizientes Routing notwendig

- Herausforderungen an ein effizientes Protokoll:
  - Nicht zuviele Hops
  - Balancierte Nutzung der Knoten
  - Delay
  - Balancierung der vorhergehenden Aspekte

- Aufteilbar in **3 Arten**:
  - **Proaktiv**
    - Konstant => Hoher Datenaufwand
    - Table-Driven
  - **Reaktiv**
    - On-Demand => Höheres Delay
    - Route-Discovery Strategien
  - **Hybrid**
    - Mix aus beidem

Proaktive Protokolle	Hybrid Protokolle	Reaktive Protokolle
DSDV	ZRP	SSR
OLSR		AODV
GSR		ABR
CGSR		CHAMP
OSPF		SMR
WRP		DSR
TBRPF		TORA

Populäre Routing-Protokolle und ihre Einteilung

Stärken von DSN

- Funktionsfähigkeit, auch in weiten und gefährlichen Gebieten
- Robustheit und Unauffälligkeit der Knoten
- Selbst-Organisation
- Meistern von Knotenfehlern
- Knoten-Mobilität
- Kaum Wartungsaufwand
- Keine Homogenität der einzelnen Sensoren nötig

Schwächen von DSN

Grob in **2 Untertypen** aufteilbar: Schwächen, die **allgemein** für drahtlose Netzwerke gelten und **DSN-spezifische** Schwächen.

Allgemeine:

- Geringere Datenraten
- Kommunikationsfehler
- Sicherheit

DSN-Spezifische:

- Limitierte Energieressourcen
- Limitierte(r) Rechenpower/Speicher
- Sicherheit

Gegenüberstellung

DSN - Komponenten	Vorteile	Nachteile
Prozessor	- Energieeffizient - Günstig	- Für gewisse Anwendungen zuwenig Rechenpower - Kann keine komplizierten Funktionen durchführen
Memory / Storage	- Günstig - Schnell	- Zwischenspeicherung eingeschränkt
Transceiver	- Schlaffunktion - Kleine energy-per-bit Kosten	- Meist Low-Rate - Short-Range - Radio-Kommunikation am kostenintensivsten

Zusammenfassung

Wir haben uns also einen Überblick verschafft über:

- Generelle Definition
- Typische Anwendungsgebiete
- Hardware- und Softwarekomponenten
- Übliche Topologien und Routingprotokolle
- Stärken und Schwächen des Netzes und der Knotenhardware

Quellen

- M. W. Chiang, Z. Zilic, J.-S. Chenard, and K. Radecka, “Architectures of increased availability wireless sensor network nodes,” Test Conference, International, vol. 0, pp. 1232–1241, 2004.
- A. E. Kateeb, A. Ramesh, and L. Azzawi, “Wireless sensor nodes processor architecture and design,” Advanced Information Networking and Applications Workshops, International Conference on, vol. 0, pp. 892–897, 2008.
- M. A. Taleghan, A. Taherkordi, M. Sharifi, and T.-H. Kim, “A survey of system software for wireless sensor networks,” Future Generation Communication and Networking, vol. 2, pp. 402–407, 2007.
- H. Chen, C. K. Tse, and J. Feng, “Impact of topology on performance and energy efficiency in wireless sensor networks for source extraction,” IEEE Transactions on Parallel and Distributed Systems, vol. 99, no. 1, 5555.
- D. J. Vergados, N. A. Pantazis, and D. D. Vergados, “Energy-efficient route selection strategies for wireless sensor networks,” Mob. Netw. Appl., vol. 13, no. 3-4, pp. 285–296, 2008.
- R. S. Bhuvaneswran, J. L. Bordim, J. Cui, and K. Nakano, “Fundamental protocols for wireless sensor networks,” Parallel and Distributed Processing Symposium, International, vol. 3, p. 30137a, 2001.
- N. N. Pham, J. Youn, and C. Won, “A comparison of wireless sensor network routing protocols on an experimental testbed,” Sensor Networks, Ubiquitous, and Trustworthy Computing, International Conference on, vol. 2, pp. 276–281, 2006.
- E. Sabbah, A. Majeed, K.-D. Kang, K. Liu, and N. Abu-Ghazaleh, “An application-driven perspective on wireless sensor network security,” in Q2SWinet ’06: Proceedings of the 2nd ACM international workshop on Quality of service & security for wireless and mobile networks. New York, NY, USA: ACM, 2006, pp. 1–8.

Quellen

- G. de Meulenaer, F. Gosset, F.-X. Standaert, and O. Pereira, “On the energy cost of communication and cryptography in wireless sensor networks,” Wireless and Mobile Computing, Networking and Communication, IEEE International Conference on, vol. 0, pp. 580–585, 2008.
- H. Chan and A. Perrig, “Security and privacy in sensor networks,” Computer, vol. 36, no. 10, pp. 103–105, 2003
- Z.-Y. Cao, Z.-Z. Ji, and M.-Z. Hu, “An image sensor node for wireless sensor networks,” Information Technology: Coding and Computing, International Conference on, vol. 2, pp. 740–745, 2005.
- D. Gra?anin, M. Eltoweissy, S. Olariu, and A. Wadaa, “On modeling wireless sensor networks,” Parallel and Distributed Processing Symposium, International, vol. 13, p. 220b, 2004.
- M. Hempstead, N. Tripathi, P. Mauro, G.-Y. Wei, and D. Brooks, “An ultra low power system architecture for sensor network applications,” Computer Architecture, International Symposium on, vol. 0, pp. 208–219, 2005.
- B. Hurler, H.-J. Hof, and M. Zitterbart, “A general architecture for wireless sensor networks: Fisrt steps,” Distributed Computing Systems Workshops, International Conference on, vol. 3, pp. 442–444, 2004.
- B. Krishnamachari, Networking Wireless Sensors. Cambridge University Press, 2005.
- S. Mahfoudh and P. Minet, “Survey of energy efficient strategies in wireless ad hoc and sensor networks,” International Conference on Networking, vol. 0, pp. 1–7, 2008.
- J. A. Stankovic, “Wireless sensor networks,” Computer, vol. 41, no. 10, pp. 92–95, 2008.

Danke für eure Aufmerksamkeit!

Fragen?