Technische Universität München

Informationsveranstaltung zum Seminar Sensorknoten: Betrieb, Netze und Anwendungen

SS 2009

Prof. Baumgarten, Prof. Carle, Dipl.-Inf. (Bioinf.) Schmitt

Technische Universität München

Ablauf

- Organisation und Betreuer
- Hinweise zur Themenbearbeitung
- Bewertung
- Vorstellung der Themen
- Themenvergabe

Organisation und Betreuer

- **Organisation:** Prof. Baumgarten, Prof. Carle, Dipl.-Inf. (Bioinf.) Schmitt
- **Ort und Zeit:** 29. KW, 14./15.7.09, 9-17 Uhr, MI tba
  Es wird eine Anwesenheitsliste geführt.

Jedes Vortragsthema ist fest mit einem Termin verknüpft.
Das Konzept des Seminars setzt voraus, dass die Teilnehmer die Termin einhalten.

- **Weitere Vorbesprechung mit Themenvergabe findet am 20.4.09 um 16 Uhr in Raum 03.07.023 statt**
- Anmeldung und weitere Informationen sind zu finden auf der Seminarhomepage und werden auch per Mailingliste kommuniziert
- **Web:** http://www.net.in.tum.de/en/teaching/ss09/seminars/

Wichtige Termine - Deadlines

- Folien: **01.07.2009**
- Ausarbeitung: **01.07.2009** (elektronisch)
- Reviews:
  - Verteilung am 02.07.2009 (elektronisch)
  - **Rückgabe am 14.07.2009** (elektronisch)
- Überarbeitete Ausarbeitung: **31.7.2009** (elektronisch)

Auf der Seminarhomepage werden Templates für die Folien, die Ausarbeitung und die Reviews zur Verfügung gestellt.

Hinweise zur Themenbearbeitung - allgemein

- Frühzeitige Kontaktaufnahme mit dem Betreuer
- **Literatur:**
  - Material vom Betreuer
  - Zusätzlich meist **selbständige Recherche** gefordert!
- **Recherchemöglichkeiten:**
  - Katalog der Bibliothek
  - Suche über Google und Citeseer
  - Webseiten von Konferenzen, Workshops, Standardisierungsorganisationen,...
- **Ziel:**
  - nicht einfach nur Informationen anlesen und wiedergeben, sondern
  - **eigenes Verständnis entwickeln** und **Verstandenes mit eigenen Worten erklären**
  - **Neutrale Bewertung des Themas**
    - Die eigene Meinung kann – wenn gewünscht – in einem extra gekennzeichneten Abschnitt vermittelt werden

Technische Universität München

Hinweise zur Themenbearbeitung - Vortrag

- Dauer: 20 - 30 Minuten
- Stil (Layout) nach Vorlage

- **Die anderen Seminarteilnehmer sollen möglichst viel mitnehmen!**
- verständliche Aufbereitung des Stoffes, z.B. durch (eigene) Abbildungen
- Einbeziehen der Zuhörer, Interaktion
- Quellen von Fremdmaterial (Bilder etc.) angeben!

- Geplant: Videoaufzeichnung zur eigenen Nachbetrachtung!

Hinweise zur Themenbearbeitung - Ausarbeitung

- Längenvorgabe: 5 - 8 Seiten im IEEE-Paper-Format (zweispaltig)
- Ausarbeitung wird korrigiert und ggf. zur Verbesserung zurückgegeben
- Gliederung wissenschaftlicher Artikel einhalten:
  - Kurzfassung
  - Einleitung
  - ...
  - Vergleiche und Bewertungen
  - Zusammenfassung/Fazit/Ausblick
  - Literaturangaben
  - korrekte Literaturangaben

➔ mehr Hinweise zur Ausarbeitung werden auf der Webseite bereitgestellt

Reviews

- Betreuer verteilen Reviews, jeder Student bekommt 2 Reviews, der Betreuer ist 3. Reviewer
- Für den Reviewer sind seine geschriebenen Reviews Teil der Note
  → bitte auch kritische Reviews schreiben
- Auf der Seminarseite wird ein Reviewformular zur Verfügung gestellt
- Teile des Review-Formulars:
  - Titel
  - Autor
  - Worum ging es in dem Paper? Hauptpunkte des Themas?
  - Stärken der Ausarbeitung:
  - Schwächen der Ausarbeitung:
  - Fragen an den Autor (Offene Punkte, Fragen die sich beim Lesen gestellt haben):
  - Sachliche Korrektheit (zb. im Bezug auf die genannten Quellen) (mind. 1 Fehler finden!):
  - Form (Quellen, Bilder, Fußnoten, Rechtschreibung, Zeichensetzung, Grammatik etc.)
    Referenz ist die Vorlage von der Webseite:

Bewertung

- **Bewertung:**
  - Vortragsfolien und Vortragsinhalt (nicht der Vortragsstil)
  - Ausarbeitung (Version 1 und Version 2)
  - Geschriebene Reviews
  - regelmäßige Anwesenheit bei den Vortragsterminen (Abzug von 0,3 Notenpunkten oder umfangreichere Ausarbeitung bei unentschuldigtem Fehlen!)
  - Das Seminar wird benotet.

- **Kein Schein bei Plagiarisums!**
  - wörtliche Übernahme von existierenden Texten sind unter Angabe der Quelle als Zitate zu kennzeichnen
  - Nichtbeachtung erfüllt den Tatbestand des Plagiarismus
  - Lehrstuhl testet die Ausarbeitungen mittels Software

- **Ausschluß vom Seminar sobald gegen eine der Deadlines oder Regeln verstoßen wird oder Plagiarismus vorliegt.**

Technische Universität München

Themenvorstellung

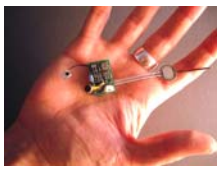
Übersicht der Themenbereiche

1. Sensorknoten
   - Smart-Its Technologie
   - Mica Technologie
   - Scatterweb Technologie
2. Netztechnologien (Ansprechpartner Prof. Baumgarten)
   - Bluetooth
   - ISO/OSI Modell
   - Management selbstorganisierter Systeme
3. Betriebssysteme
   - TinyOS
   - Weitere Themen von Prof. Baumgarten
4. Middleware-Konzepte
   - Sicherheit in WSNs (u.a. SPINS, TinySec, TinyPK, MiniSec, IPv6, ISA, secFleck)
   - Weitere Themen von Prof. Baumgarten
5. Anwendungen
   - Habitat Monitoring – Wild Life Tracking, Great Duck Island
   - Structural Health Monitoring – Golden Gate Bridge Project
   - Condition Monitoring

Technische Universität München

Smart-Its Technologie

- Zählt zu den „Embedded“ Technologien
- Kleine kontextspezifische Computer
- Können an alle möglichen Objekte angebracht werden
- Projektpartner:
  - Lancaster Universität (UK)
  - Universität Karlsruhe
  - ETH Zürich



Augenmerk auf:

- Hardwarebeschreibung und Analyse im Vergleich zu anderen bekannten Technologien
- Limitierende Faktoren & Herausforderungen
- Einsatzgebiete

http://www.smart-its.org/

http://www.viktoria.se/fal/exhibitions/smart-its-s2003/index.html

Mica Technologie

- Plattform für „Smart Sensors“
- Speziell entwickelt für tiefgreifende embedded Sensornetze
- Entwickelt in Berkeley, Californien (USA)

Augenmerk auf:

- Hardwarebeschreibung und Analyse im Vergleich zu anderen bekannten Technologien
- Limitierende Faktoren
- Herausforderungen
- Einsatzgebiete

`http://csc.lsu.edu/sensor_web/facilities.html/`

`http://www.xbow.com/`

`http://tinyos.millenium.berkeley.edu/`

Scatterweb Technologie

- Entwickelt an der FU Berlin
- Zählt zu den „Embedded“ Technologien
- Unabhängig von Infrastruktur
- Low-Power Design
- Einsatzgebiete: Lehre, Forschung und kommerzielle Anwendungen

Augenmerk auf:

- Hardwarebeschreibung und Analyse im Vergleich zu anderen bekannten Technologien
- Limitierende Faktoren
- Herausforderungen
- Einsatzgebiete

`http://cst.mi.fu-berlin.de/projects/ScatterWeb/`

Themenstellung - Sensorknoten

Titel: Technologievergleich – Smart-Its, Mica, Scatterweb

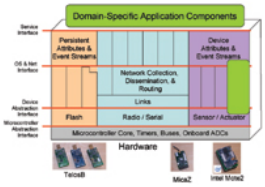
- Charakterisierung von Smart-Its, Mica-Technologie und Scatterweb
- Vergleich hinsichtlich:
  - Hardwareausstattung
  - Kommunikation
  - Limitierenden Faktoren
  - Optimierungsmöglichkeiten
  - Einsatzgebieten

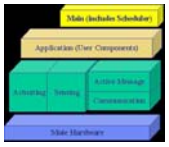
- TinyOS Motes und IPv6

Bereits vergeben !

TinyOS

- Open-source-Betriebssystem
- Speziell entwickelt für drahtlose Sensornetzwerke (Berkeley Motes)
- Entwickelt an der Universität Berkeley von Dr. D. Culler
- Komponentenbasierte Architektur
- Ereignisbasiertes Ausführungsmodell
- ZigBee-Alliance



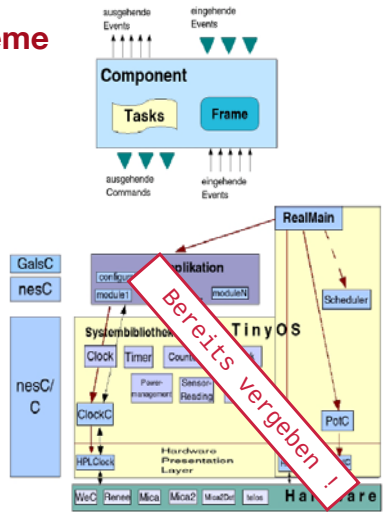


http://blog.csdn.net/lybra/archive/2008/04/05/2253628.aspx/

Themenstellung - Betriebssysteme

Titel: TinyOS

- Charakterisierung der Architektur:
  - Modularer Aufbau
  - Ereignisbasiertes Ausführungsmodell
- Welche Knotentechnologien werden unterstützt?
- Welchen Einfluß nehmen die limitierenden Faktoren der Sensorhardware auf die Anwendung von TinyOS?
- Erklärung der Funktionalität der Architektur anhand eines einfachen Beispiels (bsp. Blink)



http://www.teco.edu/~cdecker/pub/sayer_tinyos.pdf

Sicherheit in WSNs

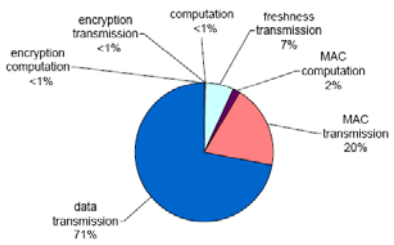
- Sensorknoten haben zahlreiche limitierende Faktoren
- Optimale Ausnutzung der Ressourcen, und gleichzeitig Sicherheit zu gewährleisten, ist eine große Herausforderung

Sicherheitsfragen:

- Data Confidentiality
- Data Authentication
- Data Integrity
- Data Freshness

Lösungsansätze:

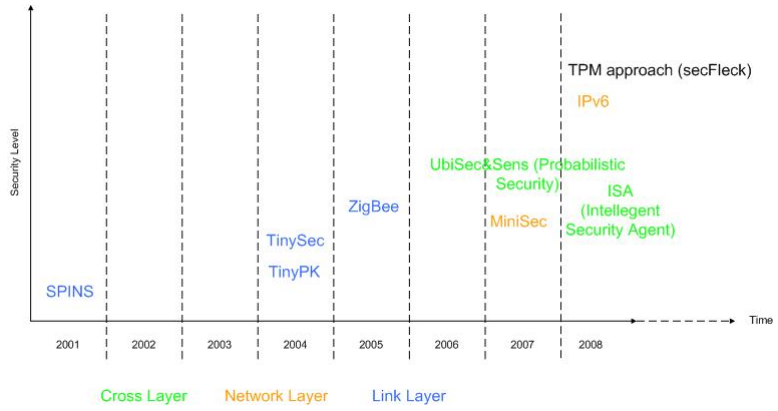
- Schicht 2: TinyPK, SPINS, TinySec
- Schicht 3: IPv6, MiniSec



Overview of Energy costs

Perrig et al „ SPINS: Security Protocols for Sensor Networks“

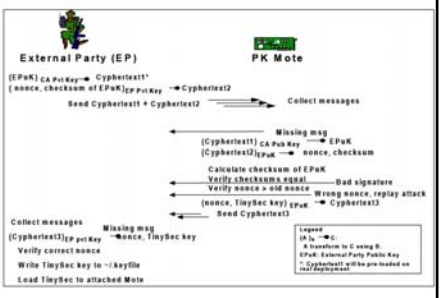
Sicherheit in WSNs - Projekte



TinyPK

- Public Key Technologie
- Key Exchange
  - **Idee:** Diffie-Hellmann Protokoll ← hat keinen authentication check
  - **Innovation:** Abwandlung – semi-static Diffie-Hellmann – ermöglicht authentication check der Knoten
    → Knoten benutzt ein static Diffie-Hellmann Schlüsselpaar mit einem Textstring processed durch einen CA Private Key als Credential

Zusätzliches entwickeltes Tool Auth-XNP ermöglicht Knotenprogrammierung „on the fly“ !

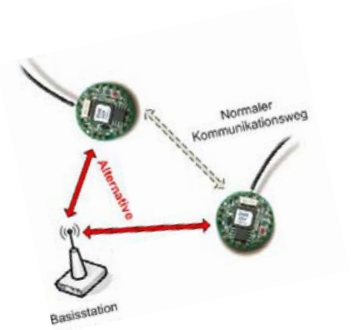


TinyPK EP Protocol Exchange Diagram, Watro et al „TinyPK:Security Sensor Networks with Public Key Technology“

SPINS

= Security Protocols for Sensor Networks

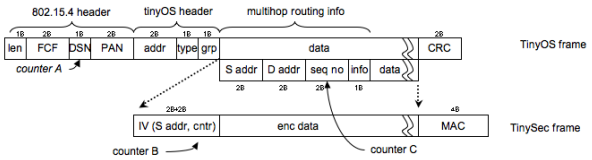
Technologie: Smart Dust
Problem: 4500 bytes Speicherkapazität auf Knoten



- Gibt eine Auslieferungswahrscheinlichkeit > 0 für Nachrichten an
- Software besteht aus 2 Teilen:
  - *Secure Network Encryption Protocol* (SNEP)
    → Confidentiality, Authentication, Integrity und Freshness
  - „micro“ Version von *Timed, Efficient, Streaming, Loss-tolerant Authentication Protocol* (µTESLA)
    → Authentication für Data broadcast
- **Ideen:**
  - Masterkey zwischen Basisstation und Knoten, weitere werden davon abgeleitet.
  - Basisstation soll die meiste Arbeit machen!

TinySec

- Voll implementierte Link-Layer Security Architektur speziell für WSNs
- Portabel zu vielen Hardware und Radio Plattformen
- **Idee:** Paketstruktur ändern
- Software besteht aus 2 Teilen:
  - Authentication encryption (TinySec-AE) – TinySec verschlüsselt die Data-Payload und authentisiert das Paket mit dem MAC
  - Authentication only mode (TinySec-Auth.) – Tiny Sec authentisiert das ganze Packet mit dem MAC, wobei die Data-Payload nicht verschlüsselt ist

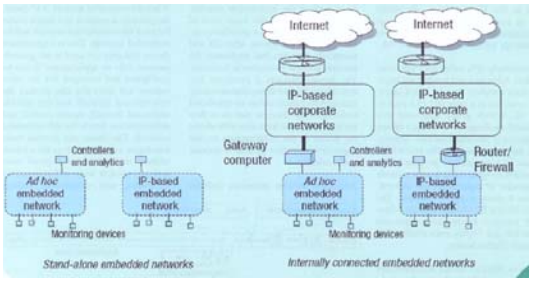


http://www.lightbluetouchpaper.org/2007/10/02/counters-freshness-and-implementation/

IPv6

Vorteil: 132-bit Adressraum im Internet

Anforderungen:
- Spezifikation von IPv6 an Sensorknotentechnologien
- Ad-hoc Netzwerke
- Autokonfiguration
- Mobilitätsmanagement
- Sicherheitsfragen



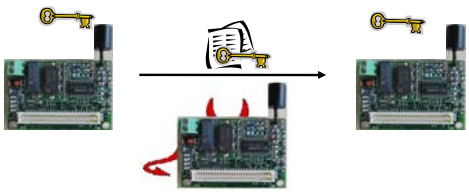
Lösungsansatz: 6LoWPAN
→ AES-128 Encryption
→ „pay only for what you use“ Header compression scheme

http://www.archrock.com/downloads/resources/ArchRock.Sum07.pdf

MiniSec

Baut auf die Ansätze TinySec und ZigBee auf und kombiniert das Beste.

Anforderungen:
- Data Secrecy
- Data authentication
- Replay protection



Lösungsansatz:
- Single-source communication
- Multi-source broadcast communication

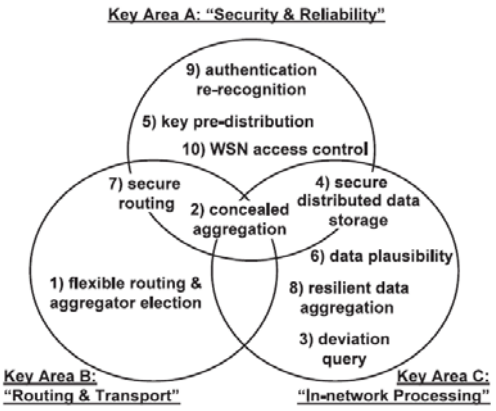
http://sparrow.ece.cmu.edu/group/projects/minisec/minisec-ipsn07.ppt

UbiSec&Sens

„Probabilistic Approach“

Anforderungen abhängig von der Applikation:

- Scalability
- Security
- Reliability
- Self-healing
- Robustness



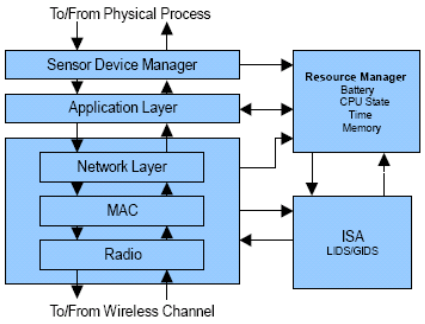
http://www.nec.co.jp/techrep/en/journal/g06/n03/t060322.pdf

Intellegent Security Architecture

Sicherheits-Framework

Eigenschaften:

- Verwendung von Cross-Layer Interaktionen
- Schichtabstraktion
- Verwendung minimaler Inter-Layer-Interaktionen



Lösungsansatz:

- Vordefiniertes Wissen
- Entsprechende Sicherheitsmaßnahmen für einzelne Knoten

http://www.cs.umanitoba.ca/~adcom08/StudentsForum/PDFs/S019.pdf

TPM-Approach - secFleck

Verwendung eines „Trusted Platform Modules“ (TPM) entwickelt durch die Trusted Computing Group (TCG)

Ziel: Authentication

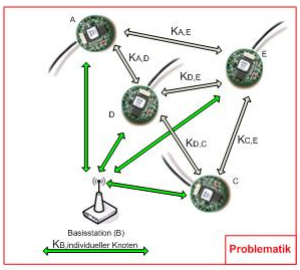
Leistungen:
- Ver-/Entschlüsselung
- Signierung
- Verifikation der Signatur

Lösungsansatz:
- PK Technologie
- Fleck OS module

http://www.cse.unsw.edu.au/~wenh/hu_ewsn09.pdf
http://doi.acm.org/10.1145/1460412.1460496

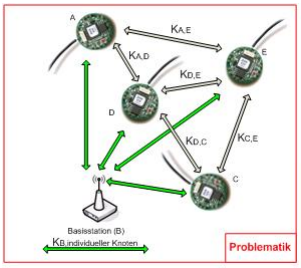
Themenstellung: Link- vs Network-Layer Security

- Charakterisierung der Herausforderungen bedingt durch die limitierende Faktoren der Sensorknoten
- Warum funktionieren herkömmliche Sicherheitsalgorithmen nicht?
- Charakterisierung, Vergleich und Bewertung der Lösungsansätze:
  - Schicht 2
  - Schicht 3
- Welche Angriffspunkte gibt es?



Themenstellung: Cross-Layer Security & TPM Approach

- Warum sind Cross-Layer Ansätze viel versprechend?
- Warum herkömmliche Sicherheitsalgorithmen haben Einfluß?
- Charakterisierung, Vergleich und Bewertung der Lösungsansätze:
  - UbiSec&Sens
  - ISA
  - secFleck
- Welche Problematiken bei der Umsetzung können entstehen?
- Welche Technologien werden angewendet?



Habitat Monitoring – Wild Life Tracking

- Bekanntestes Projekt ZebraNet
- University Princeton – Prof. Martonosi

Herausforderungen:
- Großes Überwachungsgebiet
- Knoten Mobil
- Geringer Einfluß
- Langlebig

Augenmerk auf:
- Charakterisierung des Projektes
- Eingesetzte Hardware
- Herausforderungen
- Ergebnisse

http://www.peizhang.com/research/research/research.htm/

Habitat Monitoring – Great Duck Island

- Maine, USA (44.09N, 68.15W)
- Kooperationspartner:
  - Nature Conservancy
  - College of the Atlantic (COA)

- 5000 Leach's Storm Petrels brühten in sog. „Patches“ in 3 unterschiedlichen Umgebungen
- Sensoren außerhalb und innerhalb der Bruthölle

Augenmerk auf:

- Charakterisierung des Projekts
- Anforderungen an die Hardware
- Ergebnisse

http://www.wired.com/wired/archive/11.12/network.html/

http://www.coa.edu/html/greatduckisland.htm/

Technische Universität München

Themenstellung – Habitat Monitoring

Ziel: Projektvergleich

- Was versteht man unter Habitat Monitoring?
- Welche Ziele verfolgen Informatiker und Biologen?
- Charakterisierung der Projekte ZebraNet und Great Duck Island
- Vergleich hinsichtlich:
  - Hardwareeinsatz und Hardwareanforderungen
  - Netzstruktur
  - Limitierenden Faktoren
  - Optimierungs Möglichkeiten
  - Einsatzgebieten und Ergebnisse
  - Vergleich zu ähnlichen Projekten

Structural Health Monitoring

Ziel: Entdeckung von strukturellen Schäden an Bauwerken

Bisheriger Ansatz:
Prüfung der Bauten zu bestimmten Zeitpunkten

Aktueller Ansatz:

- Anwendung von WSNs
- Ständige Überwachung von mehreren Bedingungen
- Schnelle Datenauswertung
- Kaum Einsatz von Menschen nötig

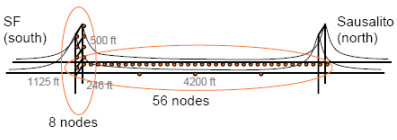
http://www.cse.polyu.edu.hk/rcuhm/damage.html

Structural Health Monitoring – Golden Gate Bridge Project

- San Francisco Bay
- University of Berkeley
- Messung von „ambient structural vibrations“

Augenmerk auf:

- Charkterisierung des Projekts
- Anforderungen an die Hardware
- Herausforderungen
- Ergebnisse



http://doi.acm.org/10.1145/1236360.1236395/
http://www.cs.berkeley.edu/~binetude/ggb/

Structural Health Monitoring – weitere Ansätze u.a. in Asien

- Vibration monitoring of Lautau Fixed Crossing
- Lantau Fixed Crossing and Ting Kau Bridge wind and structural health monitoring masterplan task 7.12
- Field tests under agreement No. CE76/97: Investigation for rehabilitation of Tsing Yi South Bridge
- Structural damage detection of cable-supported bridges by vibration measurement
- Experimental study on seismic damage detection of tall building structures
- Innovative optical fibre sensors for structural health monitoring of Tsing Ma Bridge

Condition-Monitoring

- Überwachung von Maschinen

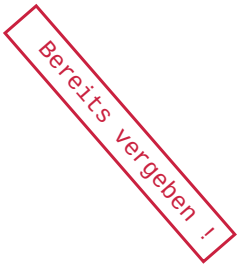
Ziele:
- Sicherheit → Notabschaltung
- Maschineneffizienz → Zustandsorientierte Instandhaltung

Anforderungen:
- Sensorik
- Meßdatenverarbeitung
- Anlagespezifische Kenntnisse

Themenstellung – Structural Health Monitoring

Ziel: Structural Health Monitoring

- Was versteht man unter Structural Health Monitoring?
- Welche Ziele werden verfolgt?
- Unterschied zu Condition Monitoring
- Charakterisierung des Golden Gate Bridge Projektes
- Vergleich zu anderen Ansätzen
- Charakterisierung hinsichtlich:
  - Hardwareeinsatz und Hardwareanforderungen
  - Netzstruktur und Herausforderungen
  - Limitierenden Faktoren
  - Optimierungsmöglichkeiten
  - Einsatzgebieten und Ergebnisse
  - Vergleich zu ähnlichen Projekten



Themen von Prof. Baumgarten

- Weitere Betriebssysteme
- Vernetzung
- Selbstorganisation und Middleware

Themenstellung – Weitere Betriebssysteme

Ziel: Vorstellung weiterer Betriebssysteme

- Welche Eigenschaften haben Betriebssysteme für Sensorknoten?
  - Embedded OS ?!
  - Realtime OS ?!
- Welche Ziele sind wichtig?
  - Energiesparsam !?
  - Mobilität !?
  - IT-Sicherheit !?
- Beispiele
  - Genode
  - L4

Bereits vergeben !

Themenstellung – Vernetzung

Ziel: Vorstellung der Konzepte und Technologien zur Vernetzung

- Wie kommunizieren Sensorknoten untereinander?
- Drahtlose Technologien
  - Bluetooth
  - Weiterentwicklungen von Bluetooth (3.0)
  - ZigBee
- Einordnung in Modelle (ISO/OSI)
  - Layer 1
  - Layer 2
  - Weitere Layer für die oben genannten Technologien
- Beispiele
  - …

Bereits vergeben !

Themenstellung – Selbstorganisation und Middleware

Ziel: Vorstellung der Organisation der Sensorknoten zum Informationsaustausch

- Wie organisieren sich die Sensorknoten untereinander?
- Konzepte und Eigenschaften
  - Master/Slave
  - Adhoc
  - Mobil, …
- Einordnung in Modelle (ISO/OSI)
  - Layer 3: Routing
  - …
- Middleware zur Vorbereitung der Anwendungen
  - Kommunikations-Middleware
  - Java, Virtuelle Maschinen
- Beispiele
  - …

Technische Universität München

Technische Universität München

Themenreservierung – Blockseminar Sensorknoten

Betreuerin: schmitt@net.in.tum.de

1. Sensorknoten – Technologievergleich (TinyOS und Anwendungen, soweit es für das Verständnis benötigt wird !) - **Korbinian Mögele**
2. Anwendung: Structural Health Monitoring (mit Technologievorstellung Mica und TinyOS, soweit es für das Verständnis benötigt wird !) - **Marco Antonio Volbracht**
3. Betriebssystem TinyOS – **Thomas Kothmayr**

Technische Universität München

Themenreservierung – Blockseminar Sensorknoten

Betreuer: uwe.baumgarten@in.tum.de

1. Vernetzung – **Kamal Najib**
2. Weitere Betriebssysteme – **Zlatina Cheva**