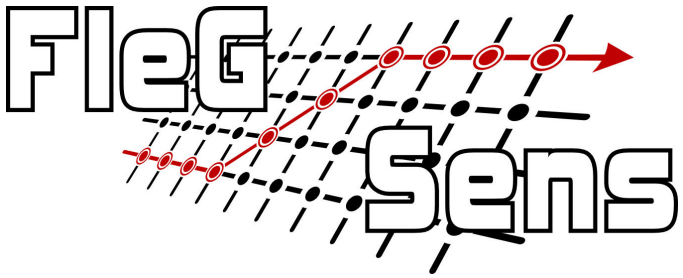
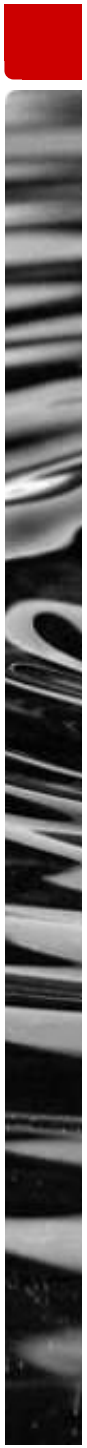
Sicherheit in einem Sensornetz zur Grenzüberwachung

Dipl.-Inf. Peter Rothenpieler
Institut für Telematik, Universität zu Lübeck

04.12.2009, Universität der Bundeswehr München





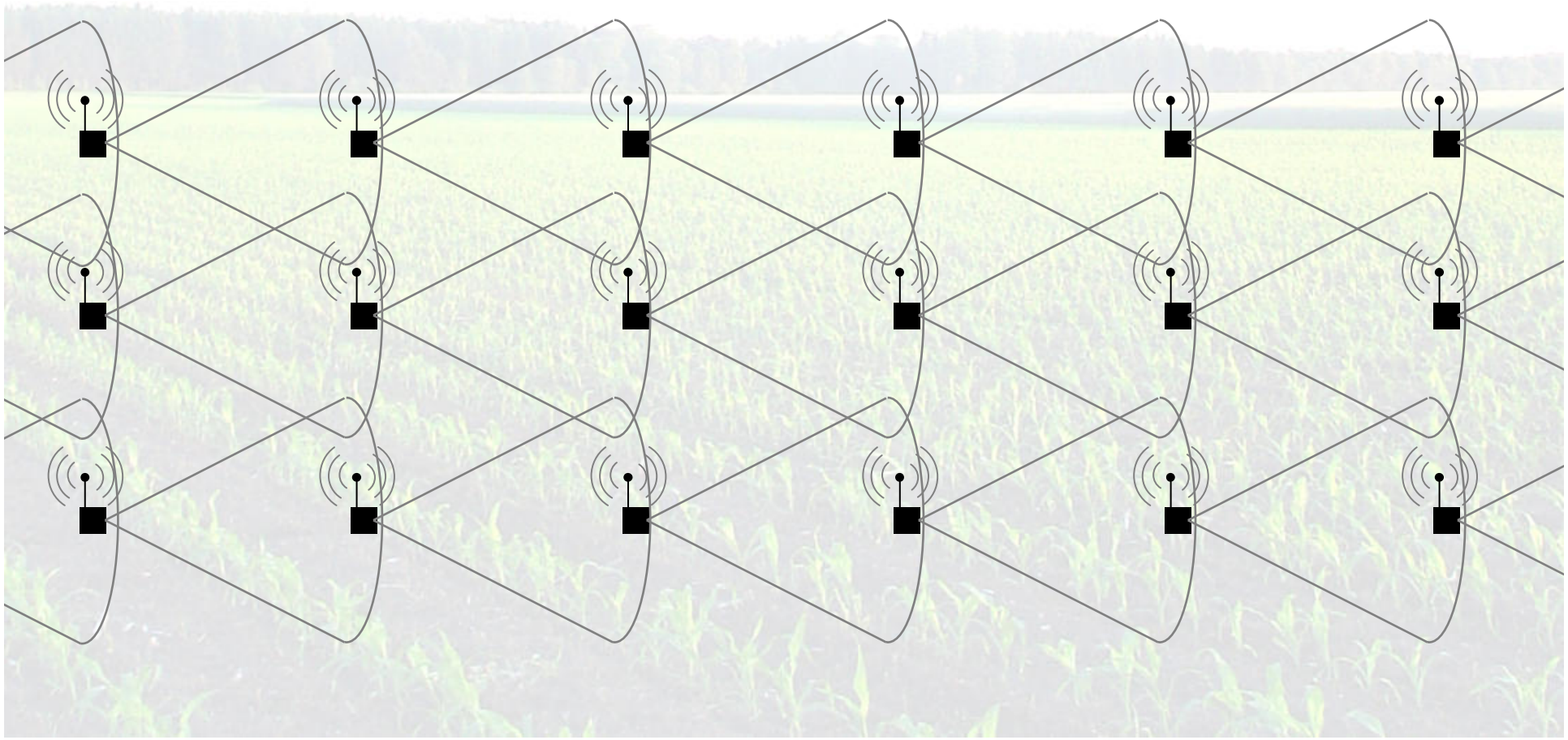
Inhalt

- Über FleGSens
- Anforderungen & Sicherheitskonzeption
  - Angreifermodell
  - Angriffs- und Schutzziele
  - Sicherheitsmechanismen
- Protokolle
  - Trackingprotokoll
  - Knotenausfallprotokoll
- Demonstratorsystem
- Diskussion und Demonstration

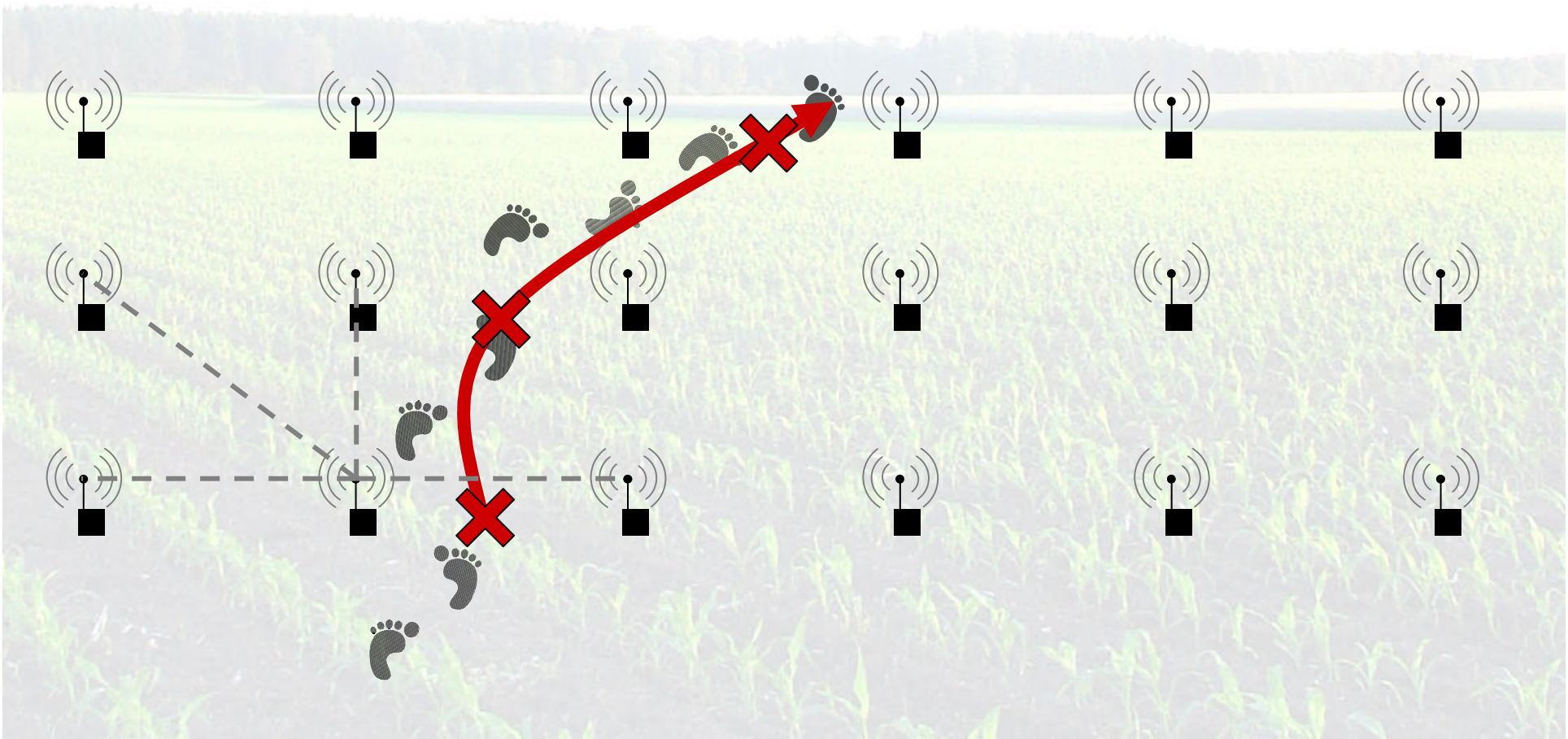
Über FleGSens

- Sichere Grenz- und Liegenschaftsüberwachung durch drahtlose Sensornetze
  - Erkennung von Übertritten an einer grünen Grenze
  - Fokus auf Informationssicherheit, nicht Sensorik
  - Demonstratorsystem mit >150 Sensorknoten
  - Simulation von Sensornetzen mit bis zu 2000 Knoten
- Partner
  - Institut für Telematik, Universität zu Lübeck
  - Institut für Telematik, Universität Karlsruhe
  - coalesenses GmbH, Lübeck
- Auftraggeber
  - Bundesamt für Sicherheit in der Informationstechnologie
- Bearbeitungszeitraum
  - Dezember 2007 – Juli 2009

Grenzüberwachung mittels drahtloser Sensornetze



Grenzüberwachung mittels drahtloser Sensornetze



Anforderungen & Sicherheitskonzeption

- Anforderungen
  - Meldung von Eindringlingen innerhalb von 5 Sekunden
  - Lebensdauer: 7 Tage
  - 10% Knotenausfallrate
  - 5% korrumpierte Knoten
- Sicherheitskonzeption
  - Angreifermodell
  - Angriffe und Schutzziele
  - Sicherheitsmechanismen
  - Sichere Protokolle der Anwendung
    - Erkennung der Grenzverletzung
    - Weitere Protokolle
      - Schlüsselverteilung, Knotenausfallerkennung, Lokalisierung, Zeitsynchronisation, Partitionserkennnung, DoS-Erkennung

Angreifermodell

- Dolev-Yao / „Man-in-the-middle Angreifer“
  - Abhören jeglicher Kommunikation im Netz
  - Erzeugen, Modifizieren von Nachrichten und Maskerade
  - Kann kryptografische Algorithmen nicht effizient berechnen
    - Kann Schlüsselmaterial nicht erraten

- Erweiterungen in FleGSens
  - Angreifer kennt alle Protokollabläufe und Nachrichtenformate
  - Auslesen und Neu-Programmierung der Sensorknoten (auch über Funk) → Korrumpierte Knoten

Angriffs- und Schutzziele

- Ein Angreifer wird versuchen, Alarme zu
  - Verhindern
  - Verzögern
  - Verfälschen
  - Fehlalarme erzeugen

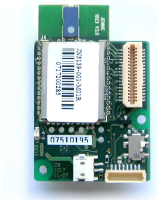
- Angriffsmöglichkeiten
  - Zerstörung von Knoten
  - Korrumpieren von Knoten
  - Denial of Service
    - Angriffe basierend auf Fluten von Nachrichten
  - Partitionierung des Netzes

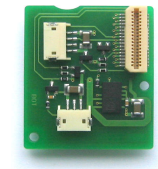
Sicherheitsmechanismen

- Einsatz von symmetrischer Kryptografie
  - Asymmetrische Kryptografie „zu teuer“
    - Symmetrisches Verschlüsseln (AES/128Bit): <350µs
    - Asymmetrisches Verschlüsseln (ECC/160Bit): ca. 3s
  - Nutzung des AES-Coprozessors auf den Sensorknoten
  - Paarweise symmetrische Schlüssel für Kommunikationspartner
    - Schlüsselaustauschprotokoll notwendig (HARPS)
- Einsatz von Broadcast-Authentifikationsprotokollen
  - Authentifikation von Basisstation und Senken (µTESLA)
- Nutzung von Message Authentication Codes (MACs)
  - CCM*-MAC des AES-Coprozessors

FleGSens Hardwarekonfiguration

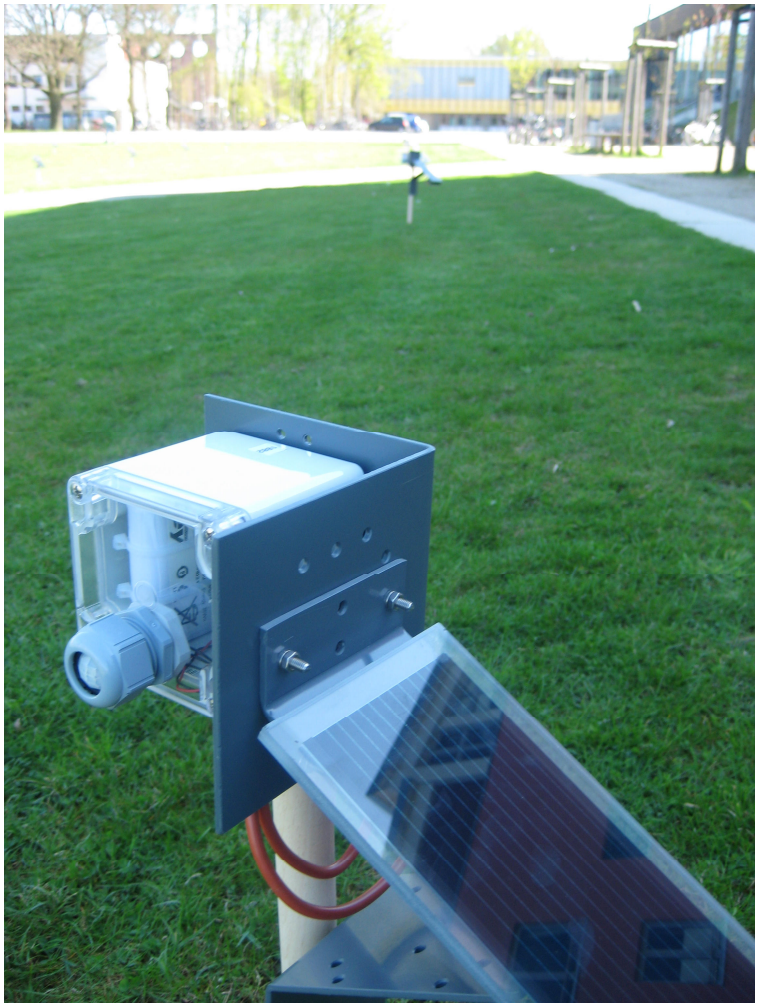
- iSense Core Module
  - 32 Bit RISC, 16MHz, 96kB RAM, 128KB Flash
  - IEEE 802.15.4 (2.4GHz) Funkschnittstelle
    - Datenrate: 250 kBit/s
    - Hardware AES-Verschlüsselung
- GPS (10% der Knoten)
- PIR Sensor
  - ca. 10m Reichweite (110° Winkel)
  - Detektion von Bewegungen
    - Seitlich >10m
    - Frontal ca. 5-7m
- Energieversorgung
  - Li-Ionen Akku (6750 µAh)
    - Dauerbetrieb: ca. 3 ½ Tage
    - 35 % Duty Cycle: ca. 10 Tage
  - Ladung durch Solarzellenmodul


+

+

+

+


Hardware



Protokolle

- Sicherheit
  - Schlüsselverteilungsprotokoll: HARPS
  - Broadcast Authentication: µTESLA
- Zeitsynchronisierung
- Lokalisierung
- Tracking-Protokoll
- Knotenausfallerkennung
- Partitionserkennung
- Duty Cycling
- Denial-of-Service-Erkennung

Tracking-Protokoll

- Ziel: Sichere Erkennung von Grenzverletzungen
  - Sensorknoten sind mit einem PIR Bewegungsmelder ausgestattet
  - Nach Auslösen des Sensors sendet der Knoten ein *PIR-Event*
    - beinhaltet Knoten-ID, Zeitstempel und Ort
    - abgesichert durch CCM*-MAC
      - Gemsamer Schlüssel zwischen Senke und Sensorknoten
  - PIR-Events werden lokal aggregiert, bevor sie mit Hilfe einer *PIR-Message* ins Netz geflutet werden
    - Resistenz gegen Fehl-Events durch Umwelteinflüsse (z.B. Wind)
  - Übertrittspfad wird an den Gateways grafisch dargestellt
    - Gateway kann gefälschte oder veränderte PIR-Messages erkennen
    - Zusätzlich Anzeige des Orts und der Zeitinformation der PIR-Events

Knotenausfallprotokoll

- 2 Protokollphasen:
  - Buddy Election:
    - Sensorknoten bilden Überwachungsbeziehungen (Buddys)
    - Hierfür sucht sich jeder Knoten Buddys aus den Knoten in Funkreichweite
  - Operationsphase
    - Knoten senden regelmäßig Heartbeat Nachrichten (alle 4 Sekunden)
    - Knotenausfall wird gemeldet, sobald 10 Heartbeat Nachrichten in Folge nicht empfangen wurden
- Sicherheitsmechanismen
  - Nachrichten enthalten einen Zeitstempel zum Schutz vor Replay Angriffen und sind durch CCM*-MAC Prüfsummen abgesichert (gemeinsamer Schlüssel beider Knoten)
  - Gültigkeitsdauer der Zeitstempel: 20 Sekunden

Demonstratorsystem

- 152 Sensorknoten (4 Reihen, 38 Spalten)
- 7m Abstand zwischen den Knoten
- Carlebachpark im Lübecker Hochschulstadtteil

>250m

Video: Sensornetz

http://www.youtube.com/FleGSens

Grenzübertritt Beispiel

Ablauf der Demonstration

- Im Vorfeld
  - Programmieren der Sensorknoten
  - Ausbringung vor Ort
  - Initialisierungsphase
    - Synchronisierung der Uhren
    - Buddy Election Phase
- Operationsphase
  - Duty Cycle: 30 % (300ms Wachphase, 700ms Schlafphase)
  - PIR Sensoren überwachen die Umgebung
  - Tracking Protokoll generiert Events und Alarme
  - Knoten senden Heartbeats, überwachen Heartbeats ihrer Buddys und melden Ausfälle

Demonstration und Diskussion

- Vielen Dank für Ihre Aufmerksamkeit
- Fragen und Antworten während und nach der Demo

Zusätzliche Informationen

Weitere Informationen finden Sie unter:

http://www.itm.uni-luebeck.de/projects/flegsens/

Dipl.-Inf. Peter Rothenpieler
Institute of Telematics, University of Lübeck
http://www.itm.uni-luebeck.de/users/rothenpieler
Ratzeburger Allee 160, 23538 Lübeck, Germany
Phone: +49 451 500 5392