Zwischenvortrag zur Diplomarbeit

10010100100010011110101001000010100101010010011100011010010100101010010011100011010010100100010011110101001010100101010010011100011010010100100010011110101001010100

Analyse leichtgewichtiger kryptographischer Algorithmen für Sensornetzwerke

Holger Krahn

Betreuung: Prof. Dr. S. Fischer
Prof. Dr. D. Wätjen
Dipl.-Wirt.-Inf. S. Schmidt

Gliederung

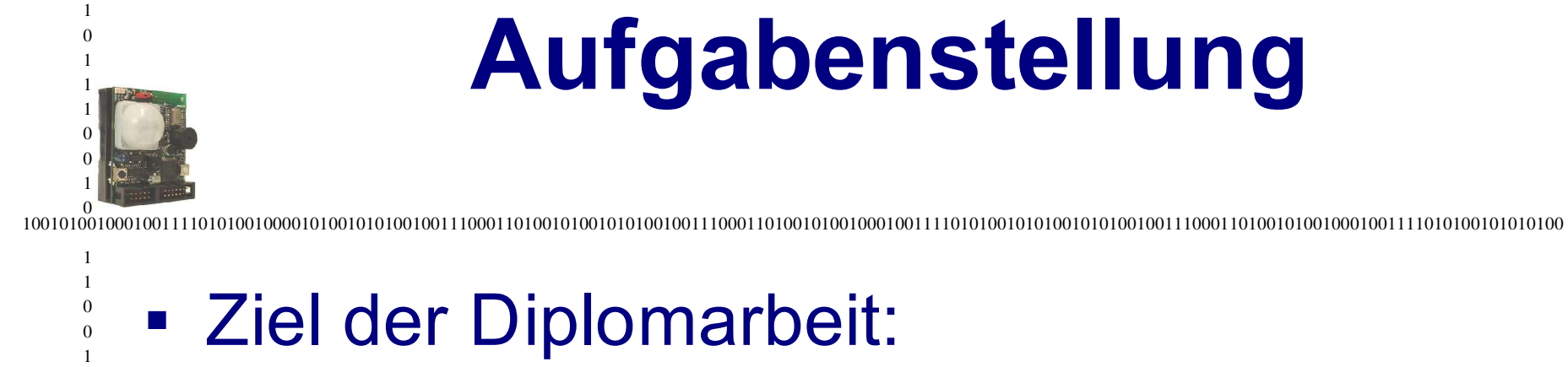
- Definition von Sensornetzwerken
- Aufgabenstellung
- Sensorknoten
- Evaluationsmodell
- Vorschlag für eine Sicherheitsarchitektur
- Ausblick

Sensornetzwerke

- Sensornetzwerke sind drahtlose selbstorganisierte Netze, die durch die Messung von Sensordaten und deren Auswertung gemeinsame Aufgaben erfüllen.

Aufgabenstellung

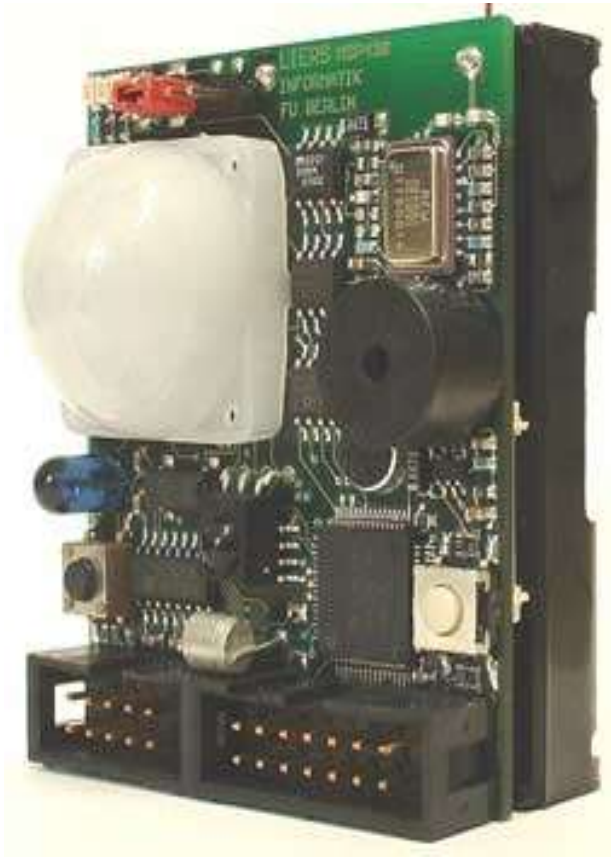
- Die verwendeten Sensornetzwerke
  - kommunizieren über Funk
  - sind dezentral ohne Basisstationen organisiert
  - befinden sich in einer nicht überwachbaren Umgebung
  - haben vor der Verteilung keinerlei Informationen über die Topologie des Netzes
- haben ein erhöhtes Sicherheitsbedürfnis
  - da das Mithören und Einschleusen von Nachrichten einfach ist
  - da die Knoten physikalisch manipuliert werden können.



Aufgabenstellung

- Ziel der Diplomarbeit:
  Erarbeiten einer Sicherheitsarchitektur für Sensornetzwerke
  - Prüfen inwieweit übliche Authentifizierungs-, Integritäts- und Verschlüsselungskonzepte auf Sensornetze übertragbar sind.
  - Implementierung eines Verfahrens

Embedded Sensor Board ESB 430/1



- 1 Mhz MSP430 Prozessor
- Geringer Stromverbrauch
- 2kb RAM, 60kb Flash
- 433/869 MHz Funk:
  19,2 kbit/s
  100m Reichweite
- Programmierung mittels einer Adaption des Gnu-C-Compilers möglich
- www.scatterweb.de

Evaluationsmodell

- Erarbeitung eines Modells anhand dessen sich Algorithmen und Protokolle auf Ihre Eignung für Sensornetzwerke bewerten lassen
  - Laufzeit
  - Speicherbedarf
  - Resistenz gegen Angriffe
  - Adaptivität
  - Mobilität (?)

Evaluationsmodell: Laufzeitanalyse

- Bestimmung der Laufzeit anhand der Auswertung der wichtigsten arithmetischen Operationen
- Kommentierte Ausgabe der Gnu-C-Compiler Adaption für die ESB MSP430 Knoten
- Beispiel: C[i] = C[j] + C[k]

```
0f 4e          mov   r14,   r15        (1 Zyklus)
0f 5f          rla   r15               (1 Zyklus)
0f 51          add   r1,    r15        (1 Zyklus)
2f 4f          mov   @r15,  r15        (2 Zyklen)
2f 5c          add   @r12,  r15        (2 Zyklen)
8d 4f 00 00    mov   r15,   0(r13)     (4 Zyklen)
```

Evaluationsmodell: Laufzeitanalyse

- Zusammenfassung der ermittelten Werte:

	Prozessorzyklen		
Operation	**16bit**	**32bit**	**64bit**
Addition, Subtraktion	11	23	40
Logische Operationen	11	23	40
Multiplikation	28	72	248
Multiplikation (Carry benötigt)	35	248	-
Shift (fest)	11	20	-
Shift (variabel)	54	99	-
Zirkulärer Shift (fest)	21	40	-
Zirkulärer Shift (variabel)	84	226	-

- Ermittlung von Laufzeiten für die Arithmetik von großen Integerwerten

Intuitive Sicherheitsarchitekturen

1 0 1 1 1 0 0 1 0 1001010010001001111010100100001010010101001001110001101001010010101001001110001101001010010001001111010100101010010100100111000110100101001000100111101010010101001001110001101001010010001001111010100101010010100100111000110100101001000100111101010010101001 1 1 0 0 1

- Systemweite Schlüssel
- Asymmetrische Kryptographie mit Zertifikaten

Netzweiter Schlüssel

- Authentizität und Vertraulichkeit durch symmetrische Kryptographie
  - Message Authentication Codes (MAC)
  - Verschlüsselung

  Vorteile:
  - Keine Initialsierungsphase nötig
  - Broadcast-Kommunikation möglich

  Nachteile:
  - Kompromittierung eines Knotens verletzt die Vetraulichkeit des gesamten Netzes und erlaubt das Einschleusen von beliebigen Nachrichten

Kommunikation mittels asymmetrischer Kryptographie

- Authentizität und Vertraulichkeit durch asymmetrische Kryptographie
  - Authentizität durch vorverteilte Zertifikate
  - Verschlüsselung

  Vorteile
  - Kompromittierung eines Knotens verletzt nur die Authenzität eines einzelnen Knotens

  Nachteile
  - Nur individuelle Kommunikation mit zusätzlichem beträchtlichen Overhead möglich
  - Berechnungen sehr aufwendig (Schätzung: 9 Sekunden pro Nachricht)

Anforderungen an eine Sicherheitsarchitektur

- Schlussfolgerung
  - Kommunikation nur über symmetrische Algorithmen praktikabel
  - Verwendung von asymmetrischen Elementen nur zur Etablierung von Schlüsseln
- Idee:
  - Ausgehend von Verfahren zur paarweisen Schlüsselvereinbarung werden in einer Initialisierungsphase Clusterschlüssel etabliert, um Broadcastkommunikation zu ermöglichen

Paarweise Schlüsselvereinbarung

1 0 1 1 1 0 0 1 0 1001010010001001111010100100001010010101001001110001101001010010101001001110001101001010010001001111010100101010010100100111000110100101001000100111101010010101001001110001101001010010001001111010100101010010100100111000110100101001000100111101010010101001 1 1 0 0 1

- Möglichkeiten zur paarweisen Vereinbarung von Schlüsseln:
  - Diffie-Hellman Protokoll mittels elliptischer Kurven
  - Diffie-Hellman Protokoll mittels XTR
  - Blundo-et-al. Schema
  - Zufällige generierte Schlüssel innerhalb einer Initialisierungsphase

Zufällige generierte Schlüssel innerhalb einer Setup-Phase

1
0
1
1
1
0
0
1
0

1001010010001001111010100100001010010101001001110001101001010010101001001110001101001010010001001111010100101010010101001001110001101001010010001001111010100101010100

1
1
0
0
1

- Grundidee:
  Innerhalb einer kurzen Zeit nach Etablierung des Netzes ist ein physikalischer Angriff auf die Knoten praktisch auszuschließen:
- Schlussfolgerung:
  - Symmetrische Kommunikation über vorverteilte Schlüssel kann als gesichert angesehen werden
  - Austausch von Schlüsseln mit benachbarten Knoten innerhalb dieser Phase möglich
  - Anschließendes Löschen des Schlüsselmaterials

Clusterbildung

- Verschiedene Arten von Clusterbildung sind möglich
- Beispiel:
  - Jeder Knoten hat einen Schlüssel, den er mit seinen Nachbarn teilt. Dieser wird von ihm zum Verschlüsseln und Authentifizieren genutzt.
    In einer Setup-Phase teilt er diesen seinen Nachbarn mit.

Zusammenfassung und Ausblick

- Sicherheit in Sensornetzwerken ist mittels symmetrischer Kryptographie zu erreichen
- Weiterhin zu untersuchen sind
  - Möglichkeiten effektiv Cluster in Sensornetzen zu bilden
  - Möglichkeiten bestehende Verfahren auf mobile Sensornetzwerke zu übertragen

1
0
1
1
1
1
0
0
1
0

1001010010001001111010100100001010010101001001110001101001010010101001001110001101001010010001001111010100101010010100100111000110100101001000100111101010010101001001110001101001010010001001111010100101010100

1
1
0
0
1

Vielen Dank für Ihre Aufmerksamkeit!