Sicherheitsmechanismen in Protokollen für drahtlose Sensornetze

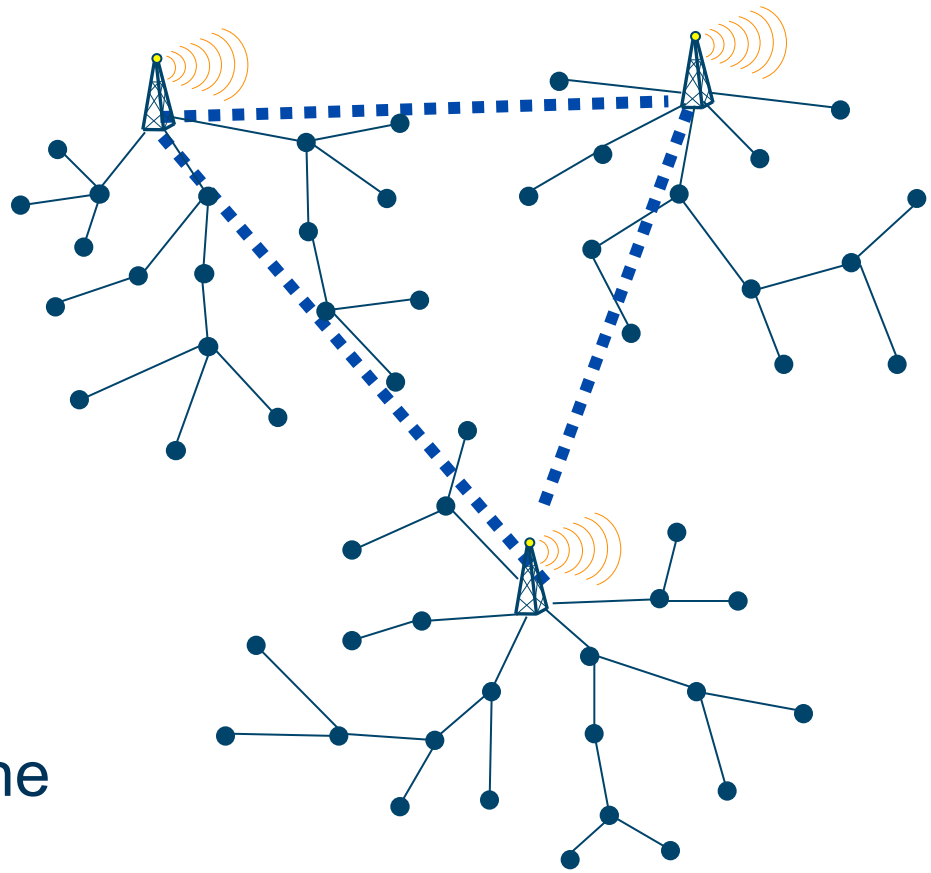
Dr.-Ing. Michael Roßberg
FG Telematik/Rechnernetze
Technische Universität Ilmenau

Übersicht

- Herausforderungen durch Sensornetze an sichere Protokolle
- Umsetzung sicherer Kommunikation
  - Probabilistische Schlüsselverteilung
  - Multicast-Authentisierung mit TESLA
  - Sichere Schätzung von Koordinaten
- Zusammenfassung & Fazit

Herausforderungen durch Sensornetze

- Mangelnde Energie & Rechenleistung
- Gleichzeitig höheres Angreiferpotential
- Selbstkonfiguration & Multi-Hop-Kommunikation
- Vorherrschend: Gruppenkommunikation
- Content-Centric, d.h. oft auch applikationsspezifische Anforderungen



Probabilistische Schlüsselverteilung – Kernidee

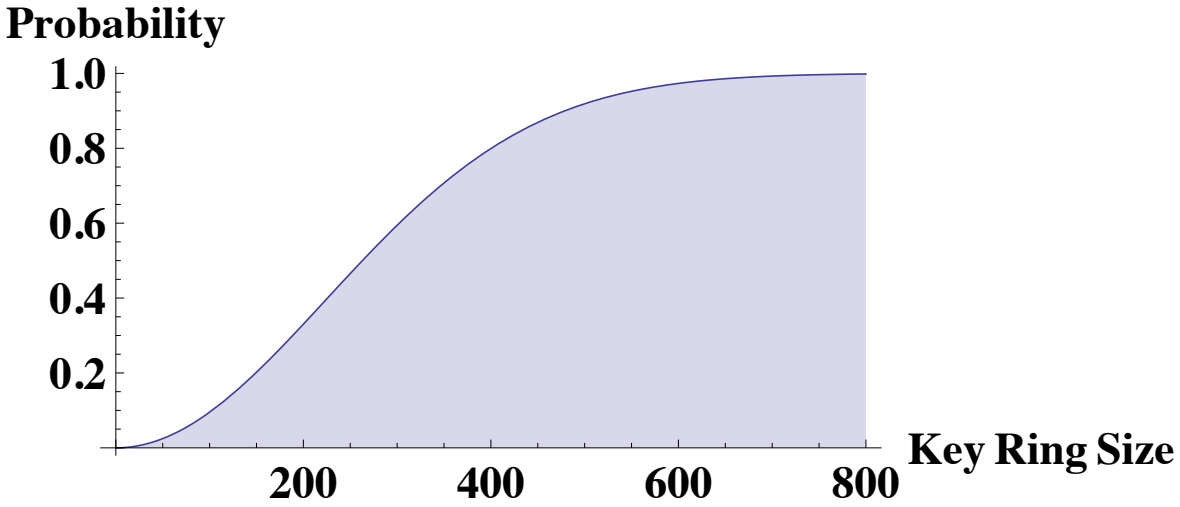
- Motivation:
  - Ein einziger Schlüssel K zwischen allen Knoten unsicher
  - Individuelle Schlüssel zwischen allen Knoten aufwendig, insgesamt $O(n^2)$
- Idee:
  - Vor Netzinstallation Erzeugung eines *Schlüssel-Pools*
  - Jeder Knoten erhält Auswahl (*Schlüsselring*)
  - Nachbarknoten tauschen sich über vorhandene Schlüssel aus und verwenden einen Schlüssel den sie sich teilen
  - Die Größe von Pool und Ring erlaubt Abwägen zwischen Konnektivität, Sicherheit und Speicherbedarf (abhängig von Knotengrad und Anzahl der Knoten)

Probabilistische Schlüsselverteilung – Parameter

- Für wie viele Links ist ein Schlüssel vorhanden?

$$P(\text{gemeinsamer Schluessel}) = 1 - \frac{((P-k)!)^2}{P!(P-2k)!}$$

- Beispiel für #Pool = 100 000



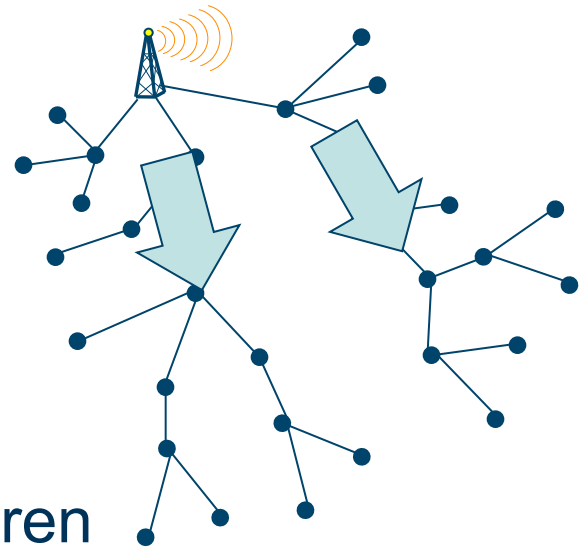
Probabilistische Schlüsselverteilung – Sicherheit

- Vorteil: Angreifer kann immer nur Teil des Key Pools rekonstruieren
  - Erlaubt Key Revocation
  - Aber: Knoten sollten nicht im Klartext Key-IDs austauschen!
- Verbleibendes Problem: Einige Knotenpaare könnten gleichen Schlüssel verwenden
  - →Schlüssel nur Verwenden um Session Key zu etablieren
  - →Mehrere gemeinsame Schlüssel können gleichzeitig verwendet werden
  - Verwendung mehrerer Schlüssel kann forciert werden (dann kleinerer Pool oder größerer Ring)

Probabilistische Schlüsselverteilung – Unterarten

- Absicherung von Multi-Hop-Kommunikation
- Speziellere Konstruktionen der Key Rings erlauben Garantie von λ-Sicherheit
  - λ Knoten können kompromittiert werden ohne das Sicherheit anderer Links betroffen ist
- Andere Verfahren können mit Zusatzwissen (z.B. in welchem Bereich Knoten ausgebracht werden) Sicherheit und Effizienz steigern

Sicherer Broad- & Multicast



- Häufig Gruppenkommunikation
  - Bsp.: Basisstation sendet an einige oder alle Sensoren eine Information
  - Vertraulichkeit in Sensornetzen i.d.R. über sichere Links zu realisieren
- Problem: Authentisierung nicht direkt über symmetrische Kryptographie zu realisieren
- Idee: Asymmetrie durch verzögertes Offenlegen von Schlüsseln

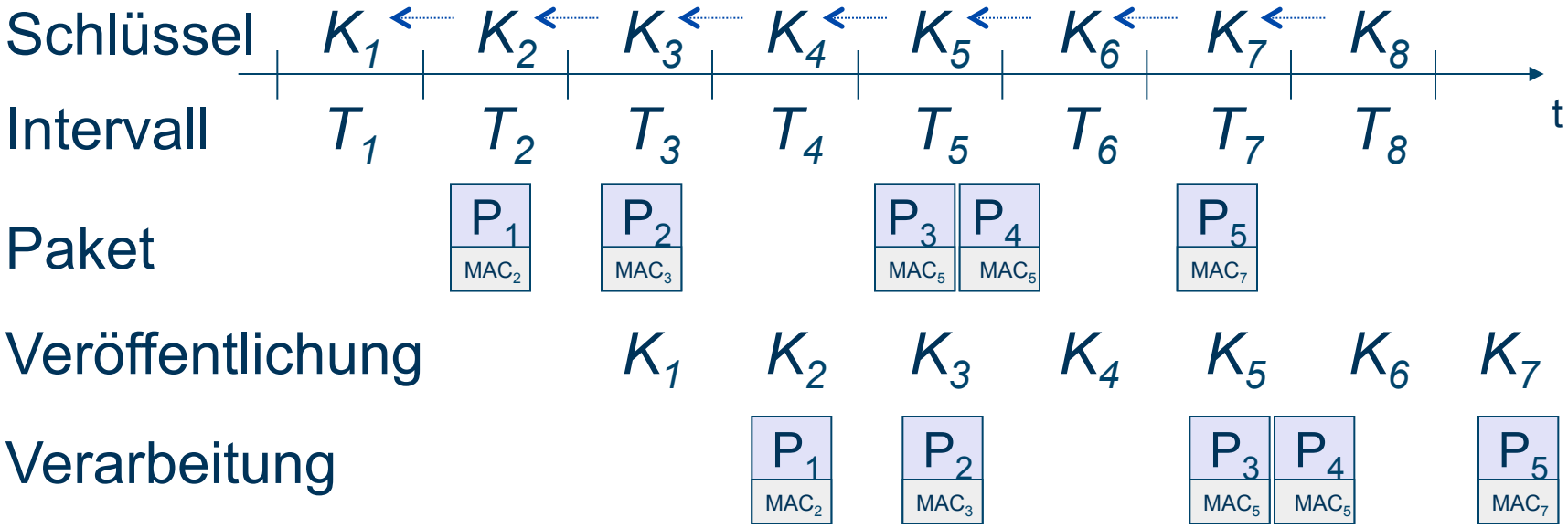
Multicast-Authentisierung mit TESLA – Initialisierung

- Beim Sender:
  - Generiert Hash-Kette der Länge n (z.B. 10^6) aus einem zufälligen Schlüssel K_n
  - Rekursive Berechnung und Speicherung einer Hash-Kette: $K_{n-1} := H(K_n)$
  - Wobei H(x) eine kryptographische Hash-Funktion ist (wie SHA-1), leicht zu berechnen, $H^{-1}(x)$ schwer
  - Gibt K_0 auf sicherem Weg bekannt
    - asymmetrisch gesichert (TESLA)
    - per Unicast (µTESLA)
    - oder fest eingespeichert

Multicast-Authentisierung mit TESLA – Kommunikation

- Versenden von authentisierten Paketen:
  - Zeit wird in Intervalle T_i fester Länge aufgeteilt
  - Im Intervall T_i werden Pakete mit K_i authentisiert
  - Der Schlüssel K_i während des Intervalls $T_{i+\delta}$ (z.B. $\delta = 2$) im Netz bekannt gegeben
  - Jeder Knoten authentisiert K_i durch Vergleich von $H(K_i)$ mit K_{i-1}
  - Erst dann werden zwischengespeicherte Pakete authentisiert

Multicast-Authentisierung mit TESLA – Ablauf

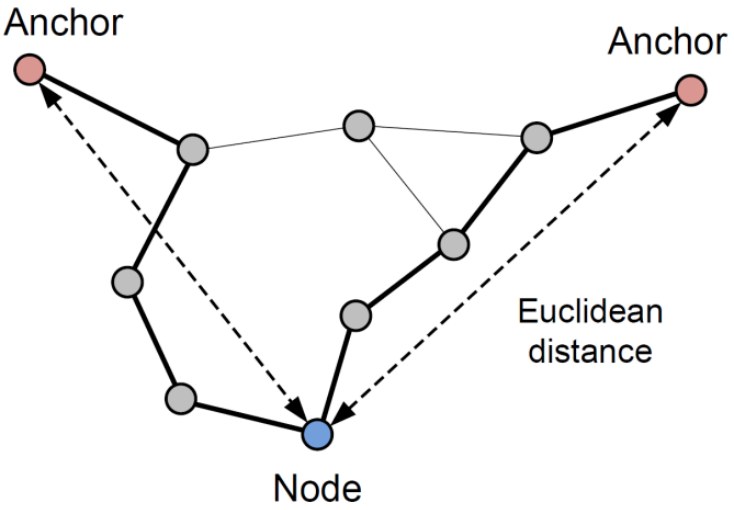


Multicast-Authentisierung mit TESLA – Eigenschaften

- Vorteil: Verwendet ausschließlich kryptographische Hash-Funktionen (schnell zu berechnen)
- Nachteile:
  - Benötigt eine Form der Zeitsynchronisation
  - Eignet sich nur für periodische Kommunikation mit konstanter Datenrate
  - Verzögerung u.U. groß (je nach Wahl von T_i)
- Aber: Sollte für viele Sensornetze ausreichen!

Sichere Schätzung von Knotenpositionen mit DV-Hop (I)

- Funktionsweise DV-Hop:
  - Einige Knoten (Anchor) kennen ihre Position
  - Fluten regelmäßig Beacons durch das Netz
  - Knoten inkrementieren Hop-Zähler bei der Weiterleitung
- Knoten schätzen Funkreichweite und eigene Position durch Hop-Anzahl sowie anhand der Anchor-Positionen
  - z.B. 4 Hops x 80 m = 320 m

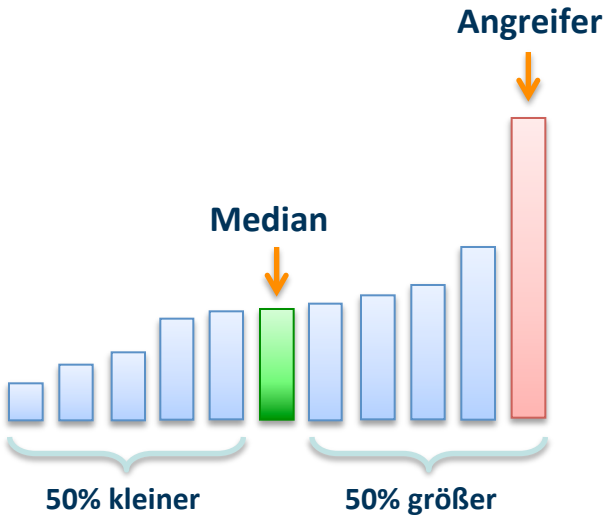


Sichere Schätzung von Knotenpositionen mit DV-Hop (II)

- Zwei Schätzungen:
  - Schätzung der durchschnittlichen Distanz zwischen Knoten (über Mittelwert)
  - Schätzung der eigenen Knotenposition durch Multilateration (anhand kleinster Fehlerquadrate)
- Aber was, wenn Angreifer:
  - Einige Knoten kompromittiert,
  - Einige Knoten physisch verschiebt oder
  - Signale oder Pakete aus einer Region an anderer Stelle wiedereinspielt (Wormhole-Angriff)?

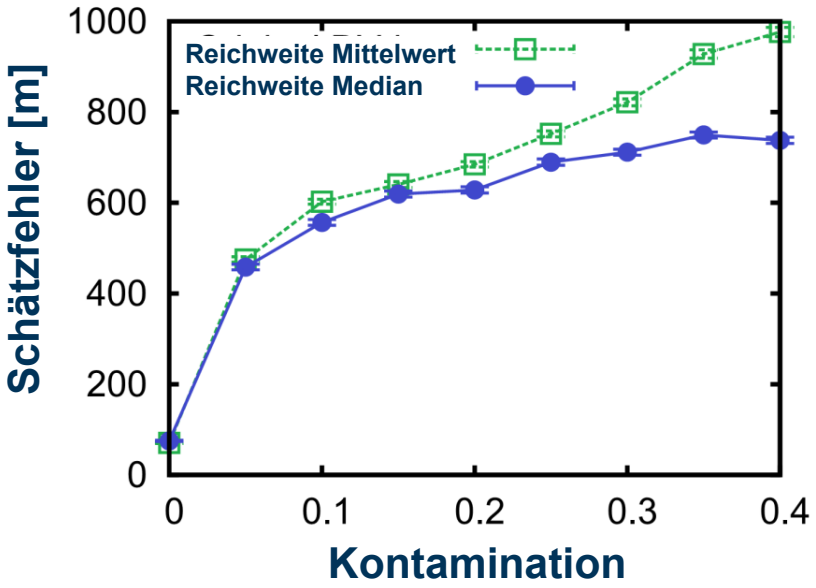
Sichere Schätzung von Knotenpositionen mit DV-Hop (III)

- Idee: Robustere Schätzungsmethoden erlauben es Angreifer als Ausreißer zu klassifizieren
- Anschließend kaum Einfluss (bis zu gewisser Prävalenz)
  - Bei Schätzung der Funkreichweite z.B. Median
  - Bei Positionsschätzung z.B. Least Median of Squares (LMS), Schätzung durch Untermengen-bildung

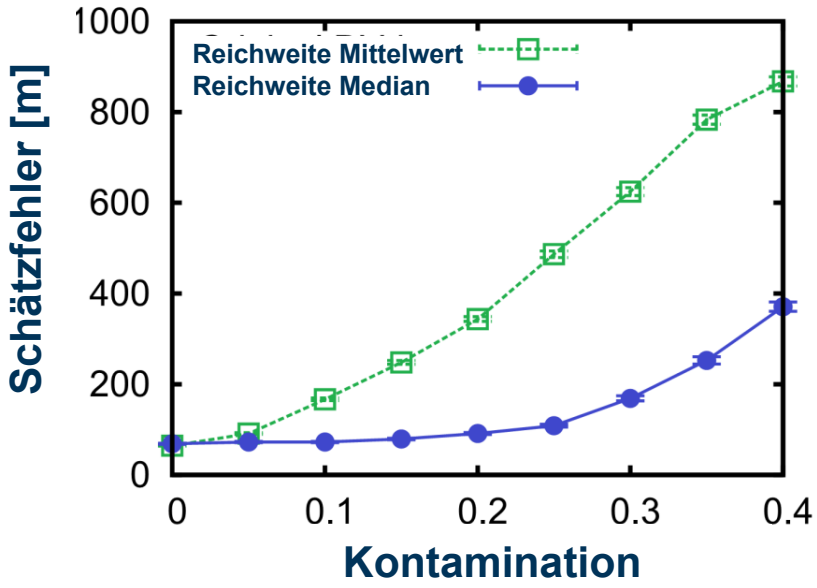


Sichere Schätzung von Knotenpositionen mit DV-Hop (IV)

Kleinste Fehlerquadrate



Least Median of Squares (LMS)



Sichere Schätzung von Knotenpositionen mit DV-Hop (V)

- Bereits erste robuste Schätzung erlaubt Ausschluss von Angreifern
- Mehrfaches Schätzen von Knotenuntermengen erlaubt weitere Steigerung der Genauigkeit
- Aber: LMS benötigt aufwendigere Berechnung

→ Aktuell werden Heuristiken entwickelt, die auf das Problem angepasst sind

Zusammenfassung & Fazit

- Optimierung von Sicherheitsmechanismen für Sensornetze
  - Oft vertretbarer Mehraufwand für ein erhebliches Steigern der Sicherheit ☺
  - Teilweise sogar Steigerung der Robustheit insgesamt

- Aber oft auch Sicherheitsmechanismen mit wenig Gewinn durch falsches Optimieren ☹
  (hier nicht gezeigt)

Vielen Dank für Ihre Aufmerksamkeit!

Dr.-Ing. Michael Roßberg
FG Telematik/Rechnernetze
Technische Universität Ilmenau

+49 3677 69-4553
michael.rossberg@tu-ilmenau.de

Literatur

[PS+02a] A. Perrig, R. Szewcyk, J. Tygar, V. Wen, D. Culler. *SPINS: Security Protocols for Sensor Networks.* Wireless Networks, vol. 8, pp. 521-534, Kluwer, 2002.

[EG02] L. Eschenauer, V. D. Gligor. *A Key Management Scheme for Distributed Sensor Networks.* CCS'02, Washington, DC, USA, November 2002.

[CPS03] H. Chan, A. Perrig, D. Song. *Random Key Predistribution Schemes for Sensor Networks.* IEEE Symposium on Security and Privacy, May 2003.

[HD05] Huang, C., Du, D.: *New constructions on broadcast encryption and key pre-distribution schemes*. In: *Proceedings of the IEEE INFOCOM'05*, 2005.

[YG05] Z. Yu and Y. Guan. A robust group-based key management scheme for wireless sensor networks. In *Wireless Communications and Networking Conference*, pages 1915–1920. IEEE, 2005.

[Sch09] Schaefer, Guenter Sensor Network Security, Book chapter in R. Zurawski (ed.) „Embedded Systems Handbook, Second Edition: Networked Embedded Systems", CRC Press, 2009.

[WGS11] Wozniak, Sander; Gerlach, Tobias; Schäfer Günter: *Optimization-based Secure Multi-hop Localization in Wireless Ad Hoc Networks*, Kommunikation in Verteilten Systemen 2011 (KiVS '11), Kiel, Germany, March 2011.