Sicherheitsmechanismen für CAN-basierte Dienstlokalisierung in Sensornetzen

Ingmar Baumgart
Hans-Joachim Hof
Prof. Dr. M. Zitterbart
Institut für Telematik, Universität Karlsruhe (TH)

“Neue Herausforderungen in der Netzsicherheit”
Essen, 6.10.2005

Motivation

- Neue Herausforderungen durch Sensornetze
  - Stark beschränkten Ressourcen der Sensorknoten
  - Hohe Knotenanzahl und multi-hop Kommunikation
  - Keine bestehende Infrastruktur ➔ Selbstorganisation
- Anwendungsszenarien
  - Gebäudeautomation
  - Gesundheitswesen ➔ Hohe Sicherheitsanforderungen
- Dienstorientierte Sensornetzen:

  Dynamische Erzeugung neuer komplexer Dienste möglich

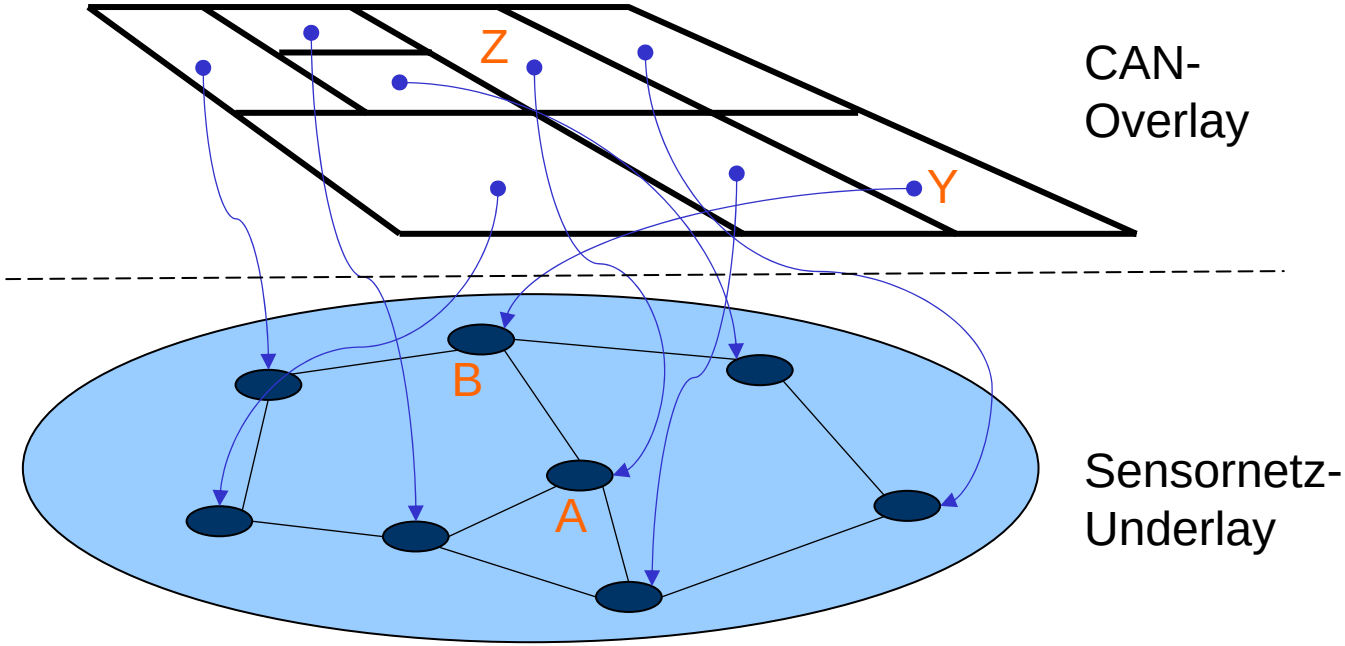
  ➔ Dienstverzeichnis

Überblick

- Content Addressable Networks (CAN)
- Dienstverzeichnis SCAN
- Sicherer Knotenbeitritt
- Sicheres Einfügen und Auffinden von Diensten
- Simulationsergebnisse
- Ausblick

CAN: a content addressable network

- DHT (distributed hash table)
- Verteiltes Speichern von (*Schlüssel, Wert*)-Paaren
- Schlüssel wird durch Hashfunktion auf ID abgebildet (Punkt im Koordinatenraum)
- Koordinatenraum: d-dimensionaler Torus
- Operationen: Join, Insert und Lookup



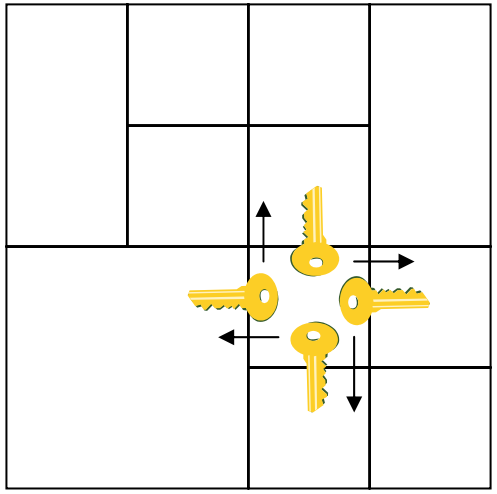
Das Dienstverzeichnis SCAN

- Dynamisches Auffinden von Diensten in Sensornetzen
- CAN-Overlay + Sicherheitsarchitektur:
  - symmetrische Schlüssel zwischen Overlay-Nachbarn
  - *Master-Device* als Vertrauensanker
- Eignung für Sensornetze:
  - dezentral
  - Keine Verwendung von Public-Key-Kryptographie
- Schutzziel:
  - Bei Outsider-Angreifern: vollständiger Schutz
  - Bei Insider-Angreifern: Schaden lokal begrenzen
  - Insider durch physische Manipulation der Knoten

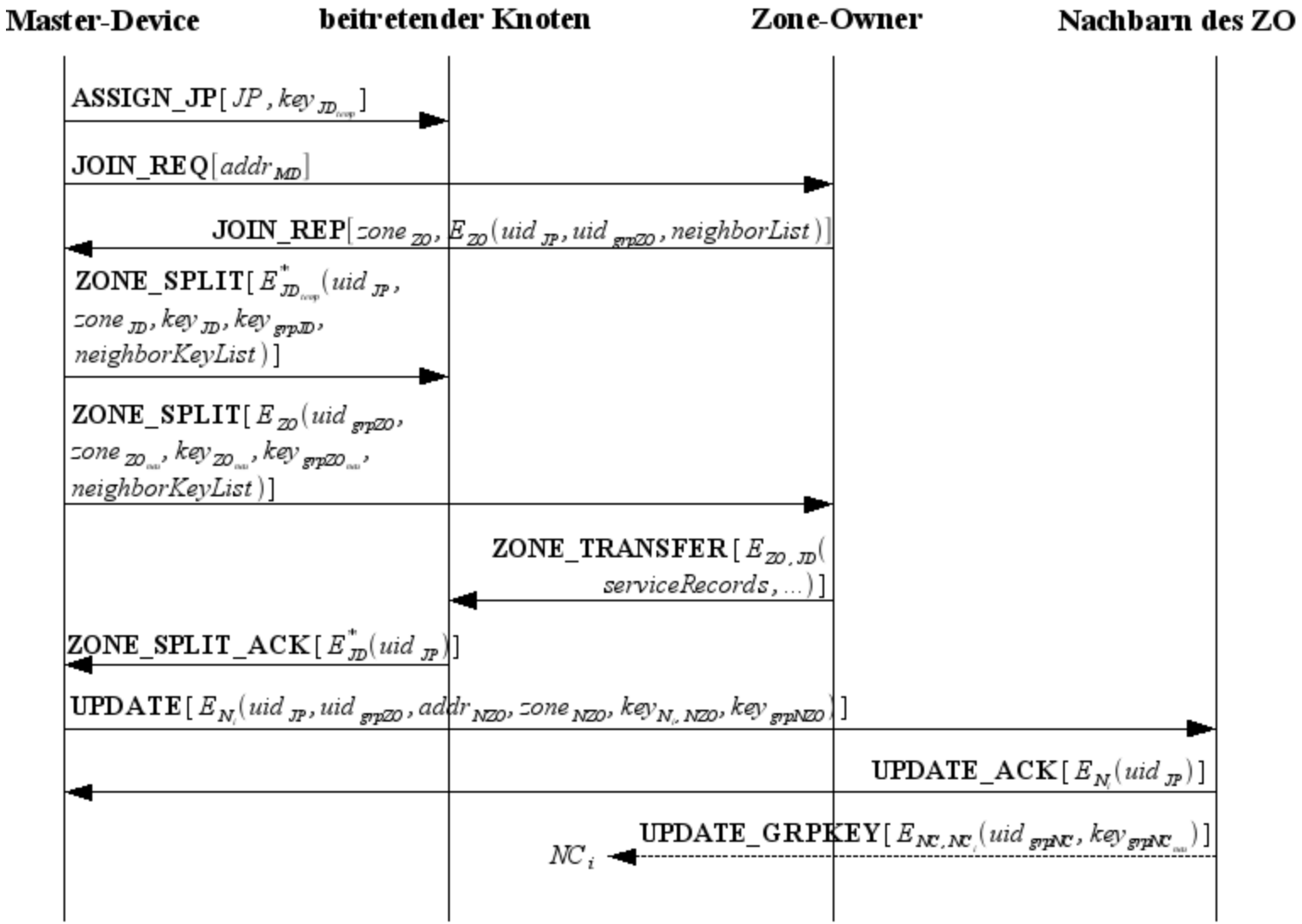
Sicherer Knotenbeitritt (Join)

- Sicherer Knotenbeitritt durch *Master-Device*
  - Kleines und leichtes Gerät
  - Speichert einen zentralen Master-Schlüssel
  - Ansonsten zustandslos ➔ leicht ersetzbar
- Master-Device als Vertrauensanker
  - Knotenbeitritt erfordert einmaligen Kontakt mit Master-Device
  - Verteilt symmetrische Schlüssel zwischen Overlay-Nachbarn nachdem eine Zone geteilt wurde

iButton



Sicherer Knotenbeitritt: Protokollablauf



Sicheres Einfügen und Auffinden von Diensten

Problem:

- gemeinsame Schlüssel nur zwischen Overlay-Nachbarn

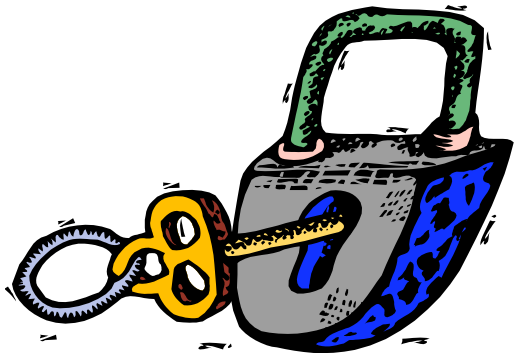
Ansatz für sicheres Einfügen und Auffinden:

- Austausch eines gemeinsamen Sitzungsschlüssel über das Overlay
- Sitzungschlüssel ➔ sichere direkte Kommunikation
- Zwei Schlüsselaustauschverfahren: SPX und MPX
  - SPX = Single Path key eXchange
  - MPX = Multiple Path key eXchange

Schlüsselaustausch in Sensornetzen

Warum neue Ansätze für Schlüsselaustausch?

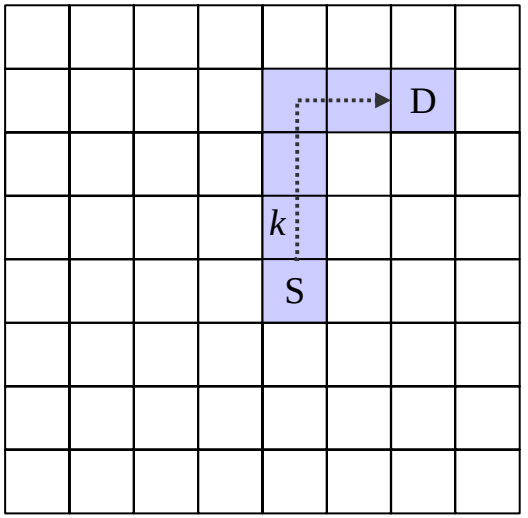
- public-key Verfahren nicht praktikabel
- Alternativen mit symmetrischen Schlüsseln:
  - Ein gemeinsamer Schlüssel für allen Knoten
  - Eigener Schlüssel für jedes Knotenpaar
  - Eigener Schlüssel zwischen Knoten und Basisstation
  - Neue Ansätze: *random-key predistribution (Chan et al.)*



➔ Schlüsselaustausch mit SPX und MPX: Übertragung der "random-key predistribution"-Idee auf ein CAN-Overlay

Schlüsselaustauschverfahren SPX

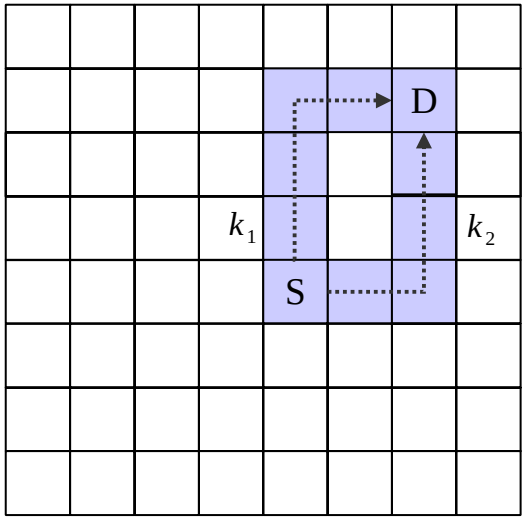
- S erzeugt zufälligen Schlüssel *k*
- *k* wird im Overlay zu D geroutet
- *k* kann nur von Knoten auf dem Weg zu D mitgelesen werden
- Alle Knoten auf dem Weg zu D gutartig
  ➔ sicherer Sitzungsschlüssel zwischen Knoten S und D
- Erhöhung der Dimensionalität *d* führt zu
  - Kürzeren Overlay-Pfaden
  - ➔ Verbesserter Schutz vor Insider-Angreifern



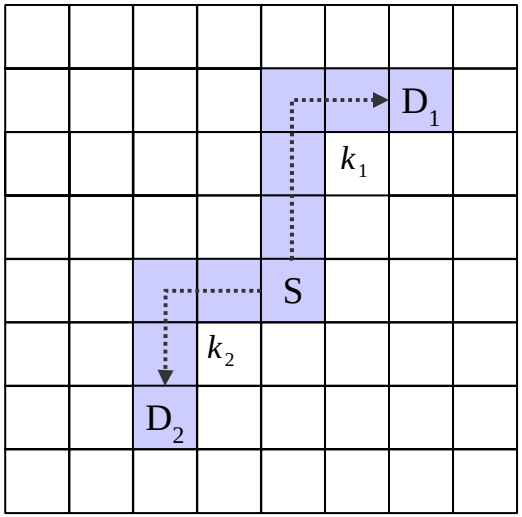
Schlüsselaustauschverfahren MPX

- S erzeugt zufälligen Schlüssel *k*
- verteilte Geheimnisse: $k = k_1 + k_2 + \ldots + k_d$
- k_i über disjunkte Pfade zu D
- *d* disjunkte Pfade in *d-dimensionalen CAN*
- Erhöhung der Dimensionalität *d* führt zu
  - Kürzeren Overlay-Pfaden
  - Größeren Anzahl disjunkter Pfade

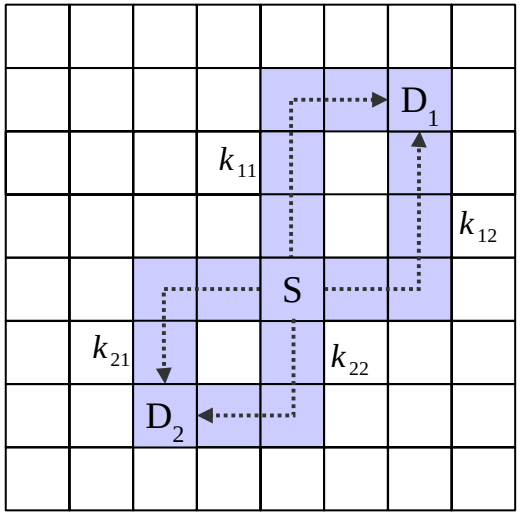
  ➔ Verbesserter Schutz vor Insider-Angreifern



SPX und MPX mit Replikaten



SPX

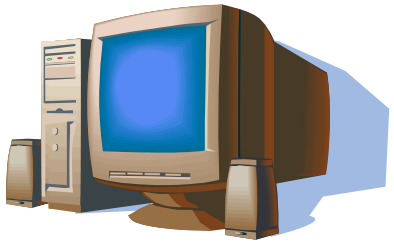


MPX

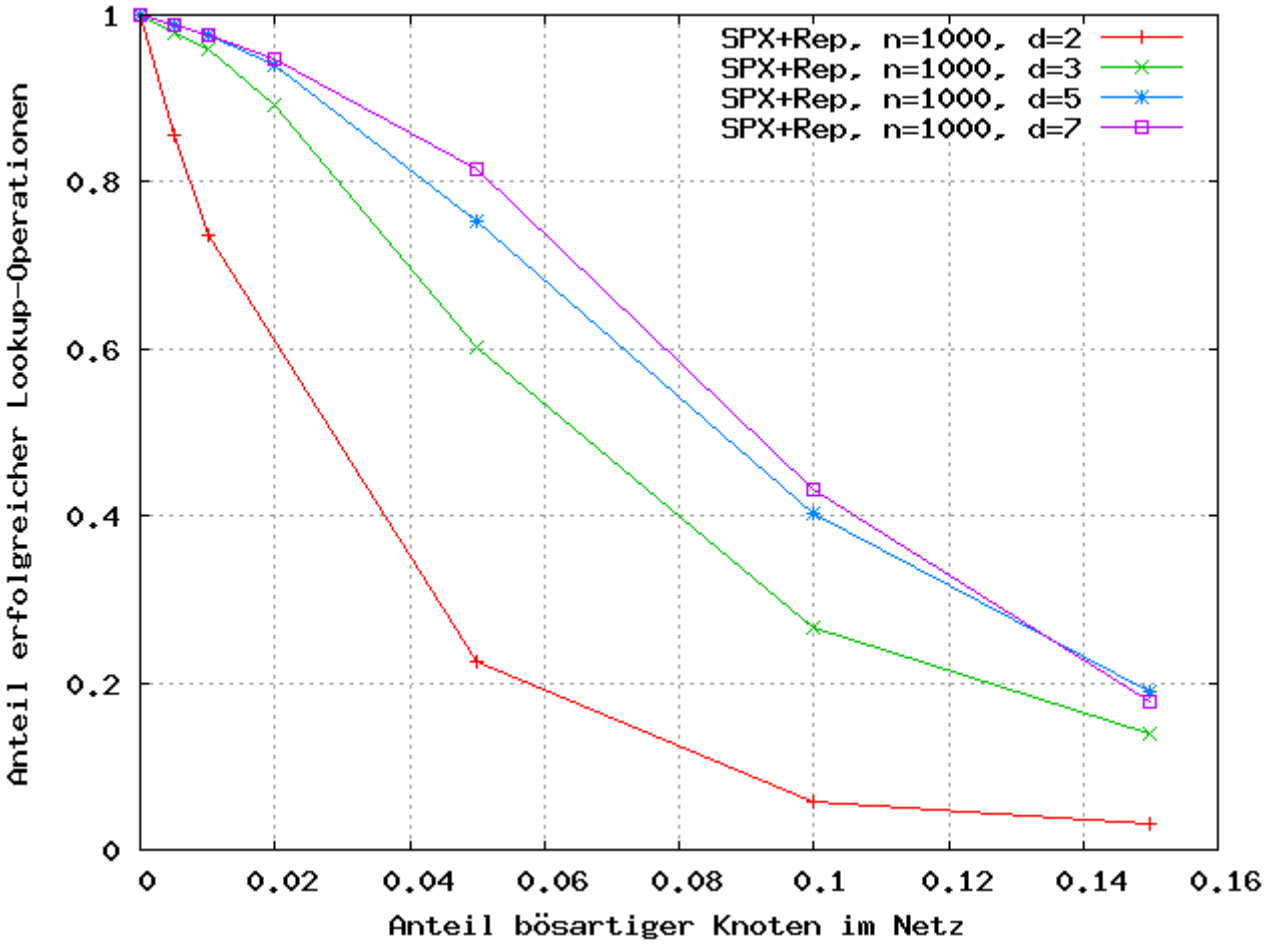
- Replikate: Gleichen Datensatz auf verschiedenen Knoten speichern
- Gleichzeitiges Abfragen mehrerer Replikate erhöht Wahrscheinlichkeit für korrektes Auffinden von Diensten
- Erkennung ungültiger Einträge durch Mehrheitsentscheid

Evaluierung des Dienstverzeichnisses SCAN

- Implementierung von SCAN im Simulator GloMoSim
- Bösartige Knoten: Typischer Insider-Angriff simuliert
- Simulationsparameter:
  - 1000 Sensorknoten
  - Simulationsgebiet 500m x 500m
  - 158m Senderadius
  - 250 kbit/s Datenübertragungsrate
- Messung Anteil erfolgreicher Lookup-Operationen abhängig vom Anteil bösartiger Knoten im Netz

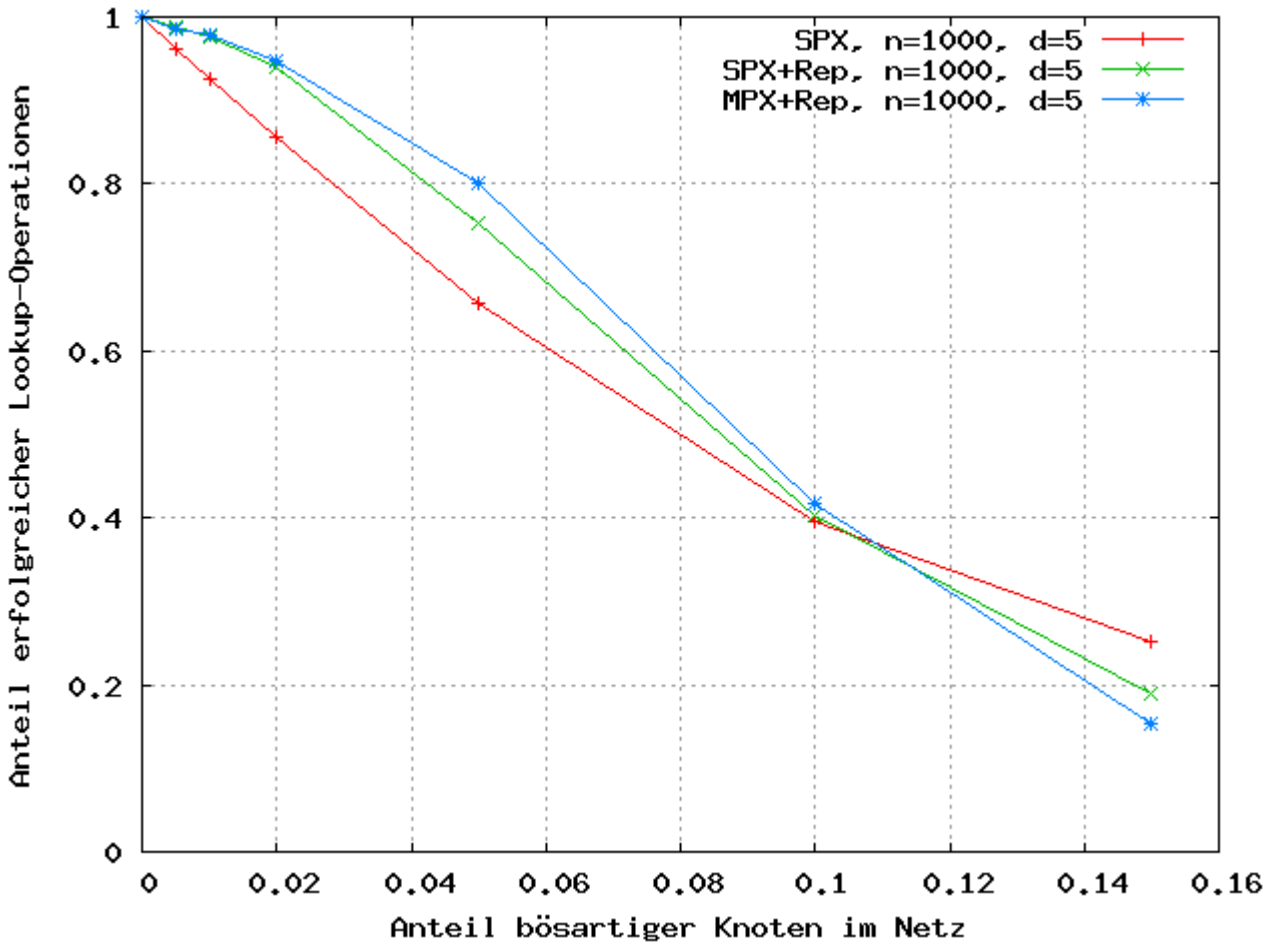


Simulationsergebnisse: Lookup-Erfolg (I)



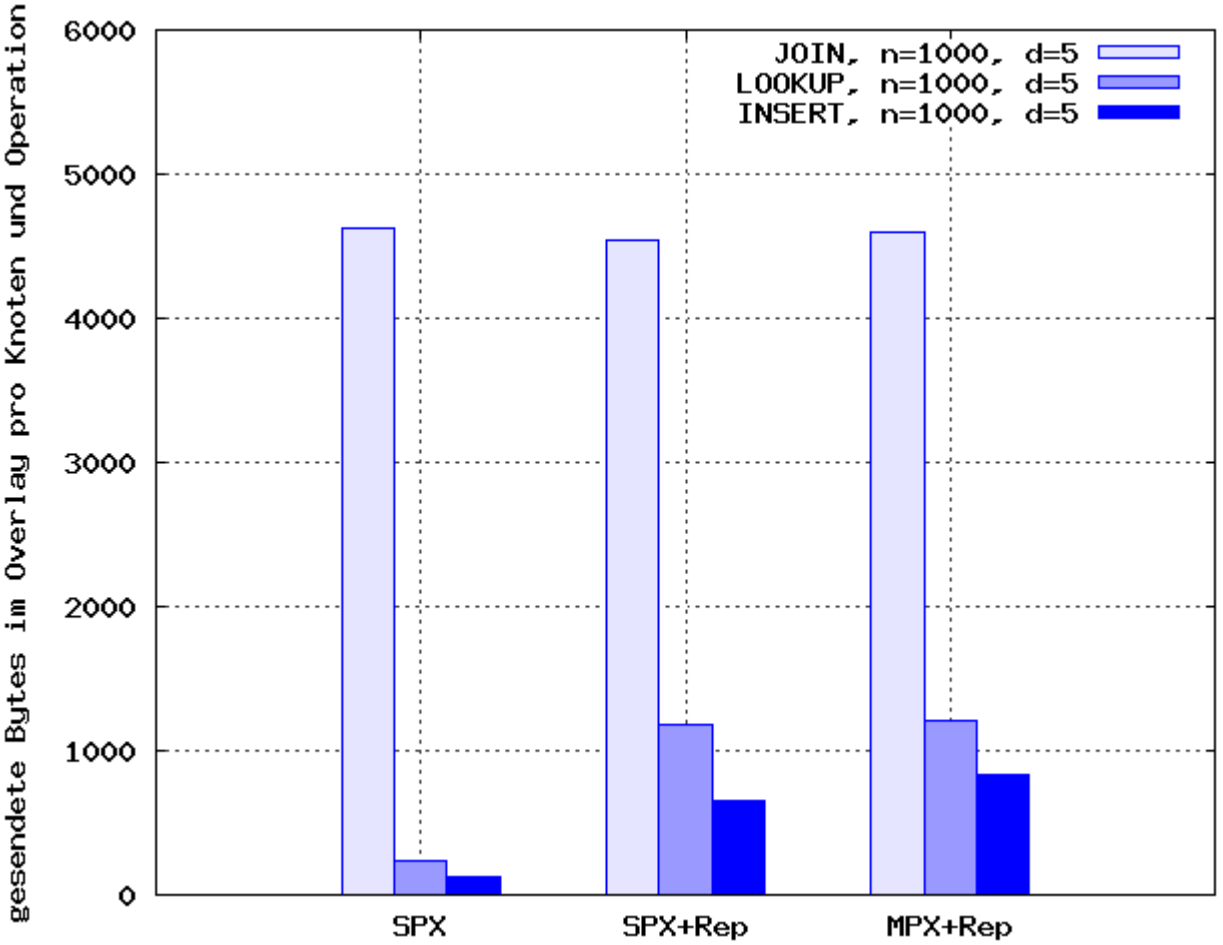
Anteil erfolgreicher Lookup-Operationen abhängig von CAN-Dimensionalität

Simulationsergebnisse: Lookup-Erfolg (II)



Anteil erfolgreicher Lookup-Operationen abhängig vom Schlüsselaustauschverfahren

Simulationsergebnisse: Kommunikationsaufwand



Kommunikationsaufwand abhängig vom Schlüsselaustauschverfahren

Zusammenfassung / Ausblick

- Dienstverzeichnis SCAN ermöglicht sicheres Einfügen und Auffinden von Diensten
- Speziell für Sensornetze geeignet:
  - dezentrale Overlaystruktur
  - keine aufwändigen kryptographische Verfahren
- Variables Sicherheitsniveau und Kommunikationsaufwand

Ausblick:

- Cluster-basierte Variante des Dienstverzeichnisses
- Schichtenübergreifende Sicherheitsarchitektur

Fragen?