Abstufbare Authentizität und Non-Repudiation bei aggregierendem Datentransport in WSN

Joachim Wilke

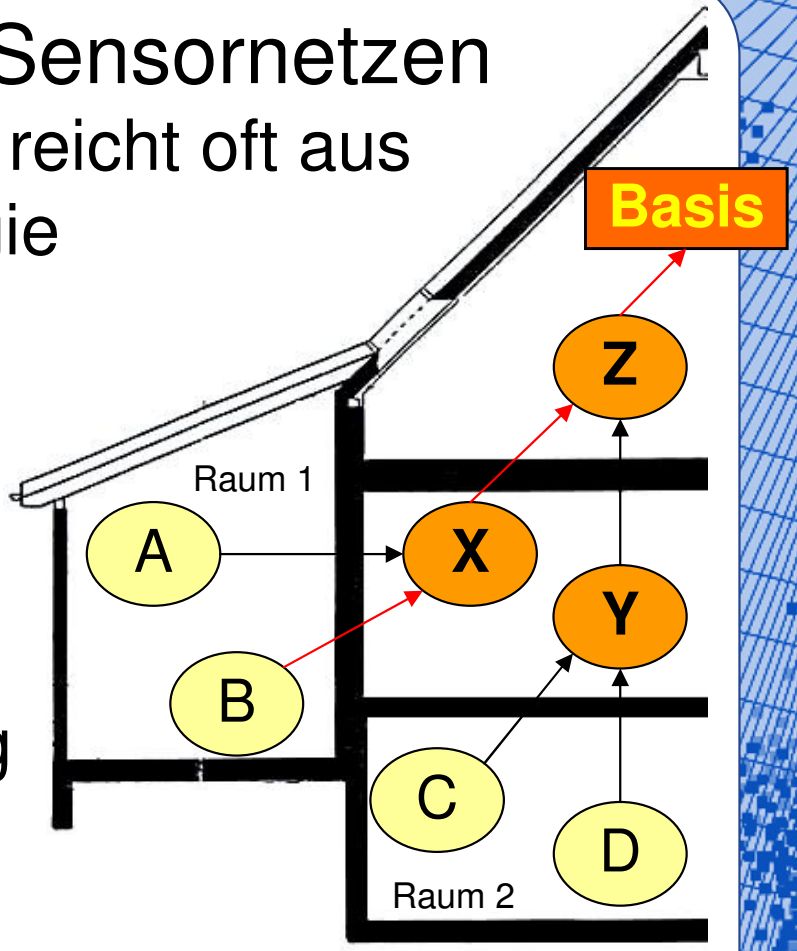
Diplomarbeit am

Institut für Telematik

Motivation: „sichere Aggregation“

- Beschränkte Ressourcen in Sensornetzen
  - Zusammenfassung der Daten reicht oft aus
  - Datenaggregation spart Energie
- Sicherheitsrelevante Applikationen
  - Sensorknoten vor physischem Zugriff nicht geschützt
  - Authentizität der Daten wichtig

➔ „sichere Aggregation“ verbindet beide Anforderungen



Problemstellung

- Anforderungen an eine „sichere Aggregation“ =
  - Aggregation liefert authentisches Aggregat
  - jeder Manipulationsversuch führt zu einer Alarmmeldung („Vollständigkeit“)
  - jeder Alarmmeldung liegt ein Manipulationsversuch zu Grunde („Korrektheit“)
  - Ursprung des Manipulationsversuchs nachvollziehbar („Non-Repudiation“)

- Bisher nur teilweise gelöst, offen bleibt „Korrektheit“ und Non-Repudiation

Überblick über die Arbeit

- Zwei neue Protokolle:
  - ESAWN-2: „Korrektheit“ durch Mehrheitsentscheide
  - ESAWN-NR: Non-Repudiation durch Datenprotokollierung und Schlüsselaufdeckung
  - Aufwand O(1) bezüglich Speicher- und Energieverbrauch
- Bisherige Forschungsarbeiten:
  - Girao, Westhoff, Schneider: „*Concealed Data Aggregation for Reverse Multicast Traffic in Wireless Sensor Networks*“, IEEE ICC, Mai 2005
    - „privacy homomorphisms“ (nur lineare Aggregationsfunktionen)
  - Blaß, Wilke, Zitterbart: „*A Security-Energy Trade-Off for Authentic Aggregation in Sensor Networks*“. IEEE Secon, September 2006
    - ESAWN – Extended secure aggregation for wireless networks
    - teilweises Aufheben der Aggregation (durch k Zeugen) und probabilistische Authentizitäts-Garantien
    - „Wahrscheinlichkeit korrekter Aggregation“ ≤ 100%
    - nur „Vollständigkeit“
- ESAWN ≤ ESAWN-2 ≤ ESAWN-NR

Systemmodell

- Angreifer
  - „aktiv“: Angreifer erlangt physischen Zugriff
  - „statisch“: Menge der korrumpierten Knoten B ist fest und ändert sich nicht
  - „gobal“: Angreifer kann beliebige Knoten korrumpieren, festes Budget, wählt |B| Knoten zufällig ➔ Wahrscheinlichkeit β
- Aggregationsbaum
  - stellt die Aggregationsbeziehungen in Netzwerk dar
  - Verzweigungsgrad δ, normalverteilt
- Sonstiges
  - zuverlässige Kommunikation
  - „Routing“ entlang der Aggregationspfade möglich (siehe „directed diffusion“)

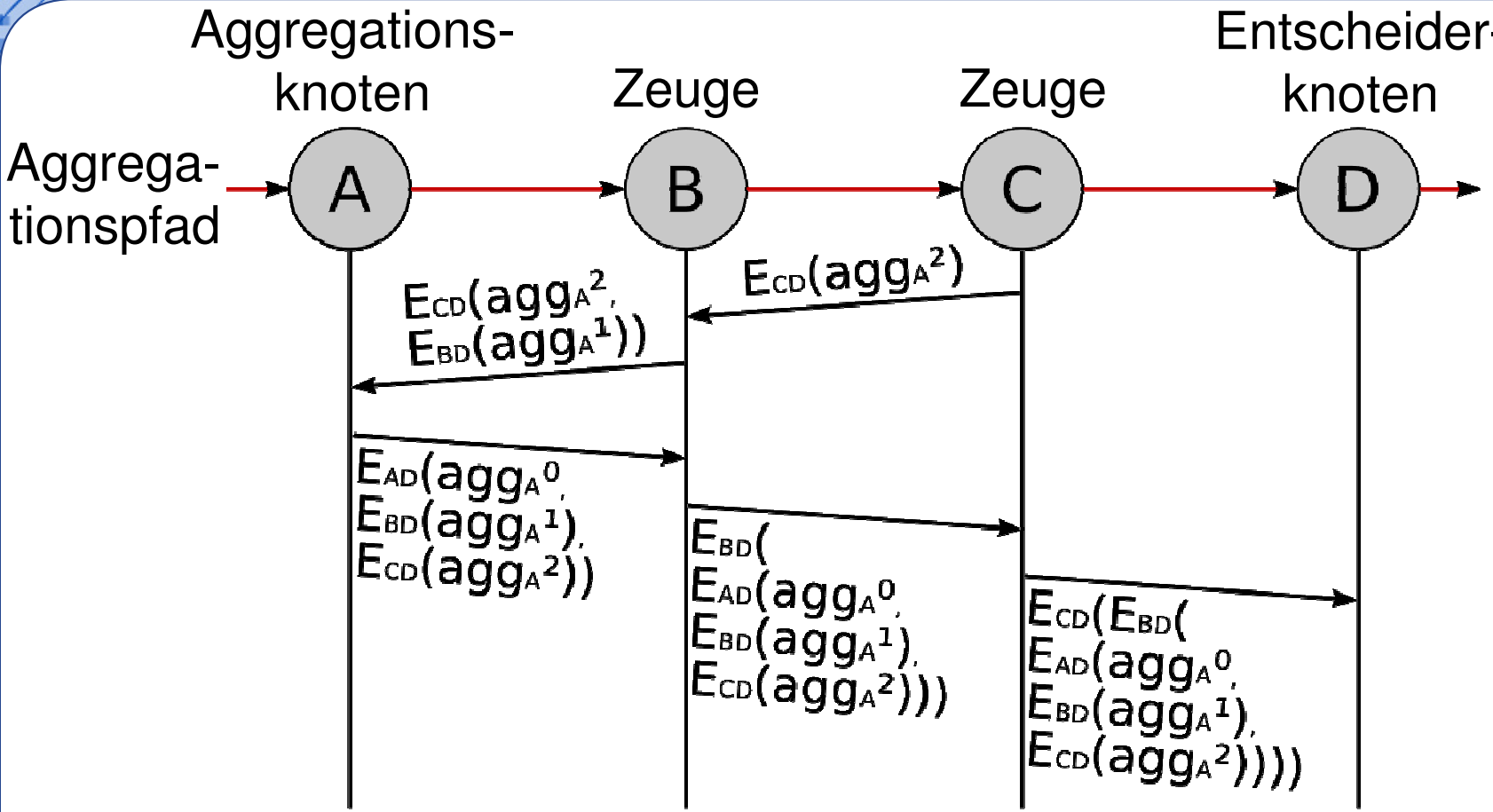
ESAWN-NR im Detail (I)

- Prinzip
  - induktiver Protokollaufbau
  - jedes Aggregat wird mit Wahrscheinlichkeit p zusätzlich durch $2\bar{k}$ Zeugen (Vorgänger des Aggregationsknoten) berechnet
  - Mehrheitsentscheid liefert korrektes Aggregat
- Ablauf
  - IV: Aggregationsknoten und Zeugen liegen Daten des vorangegangenen Aggregationsschritts vor
  - IS: $(2\bar{k}+1)$-fache Berechnung des Aggregats, Mehrheitsentscheid, Datenprotokollierung
- Insgesamt hoher Aufwand: aufgrund der Randbedingungen jedoch nicht vermeidbar

ESAWN-NR im Detail (II)

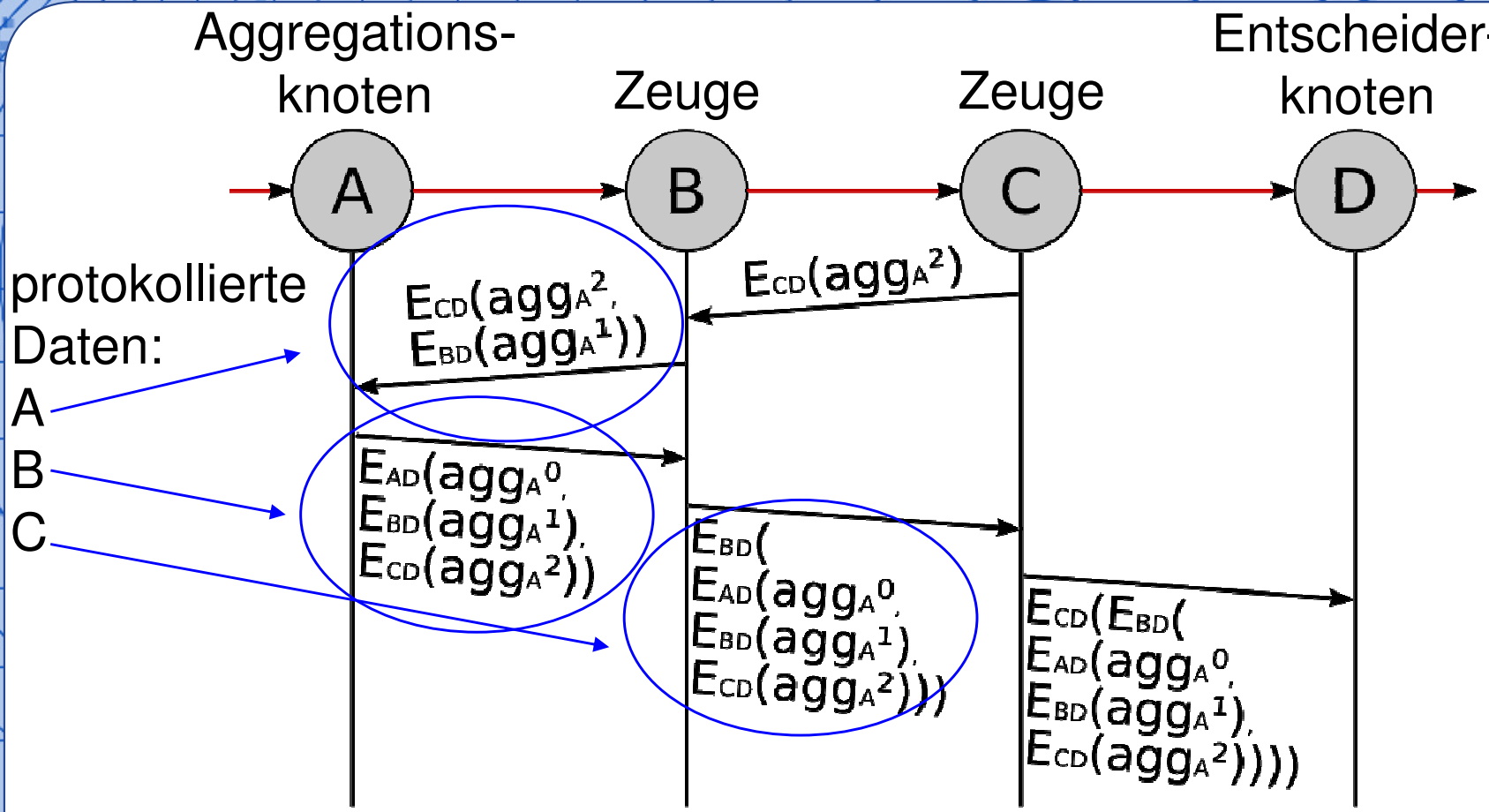
- Induktionsschluss im Detail
  - Aggregationsknoten und Zeugen berechnen Aggregat, senden es an den Entscheiderknoten.
  - Kommunikationsweg: jeder Knoten kann die verschlüsselten Daten der anderen Knoten protokollieren
  - Mehrheitsentscheid des Entscheiderknoten
  - Unterschiedliche Aggregate:
    Alarm, Schlüsselaufdeckung als Beweis
- Ergebnis
  - höchstens $\overline{k}$ korrumpierte Knoten in $2\overline{k}+1$ auf Aggregationspfad hintereinanderliegende Knoten
    ➔ ESAWN-NR liefert Non-Repudiation
  - formal in Ausarbeitung bewiesen

ESAWN-NR: Beispiel, $\bar{k}$=1 (I)



IV: A, B und C liegen die Daten zur Berechnung von agg_A vor

ESAWN-NR: Beispiel, $\bar{k}$=1 (II)

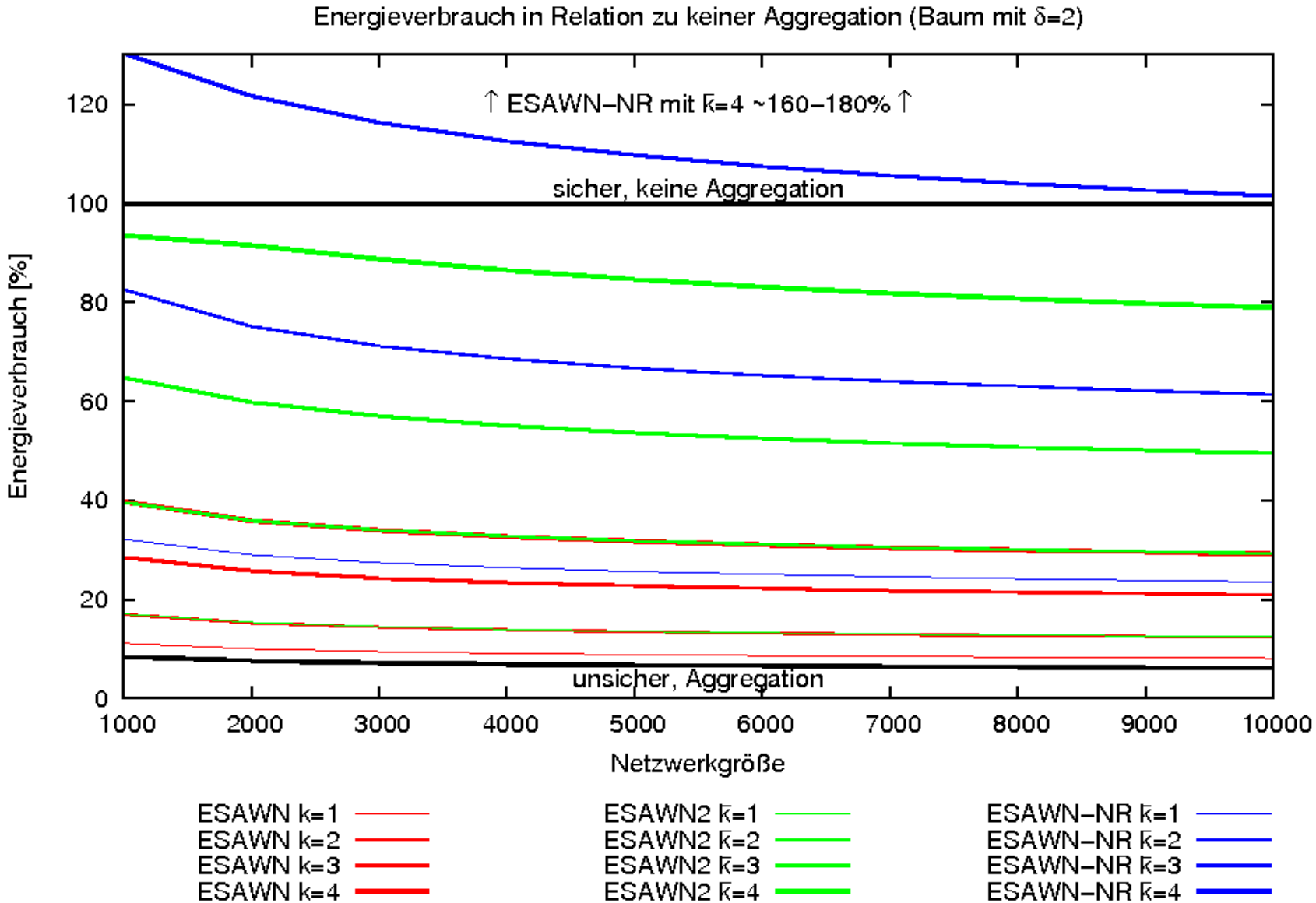


Im Betrugsfall: D legt K_{AD}, K_{BD}, K_{CD} (je nach Bedarf) auf.

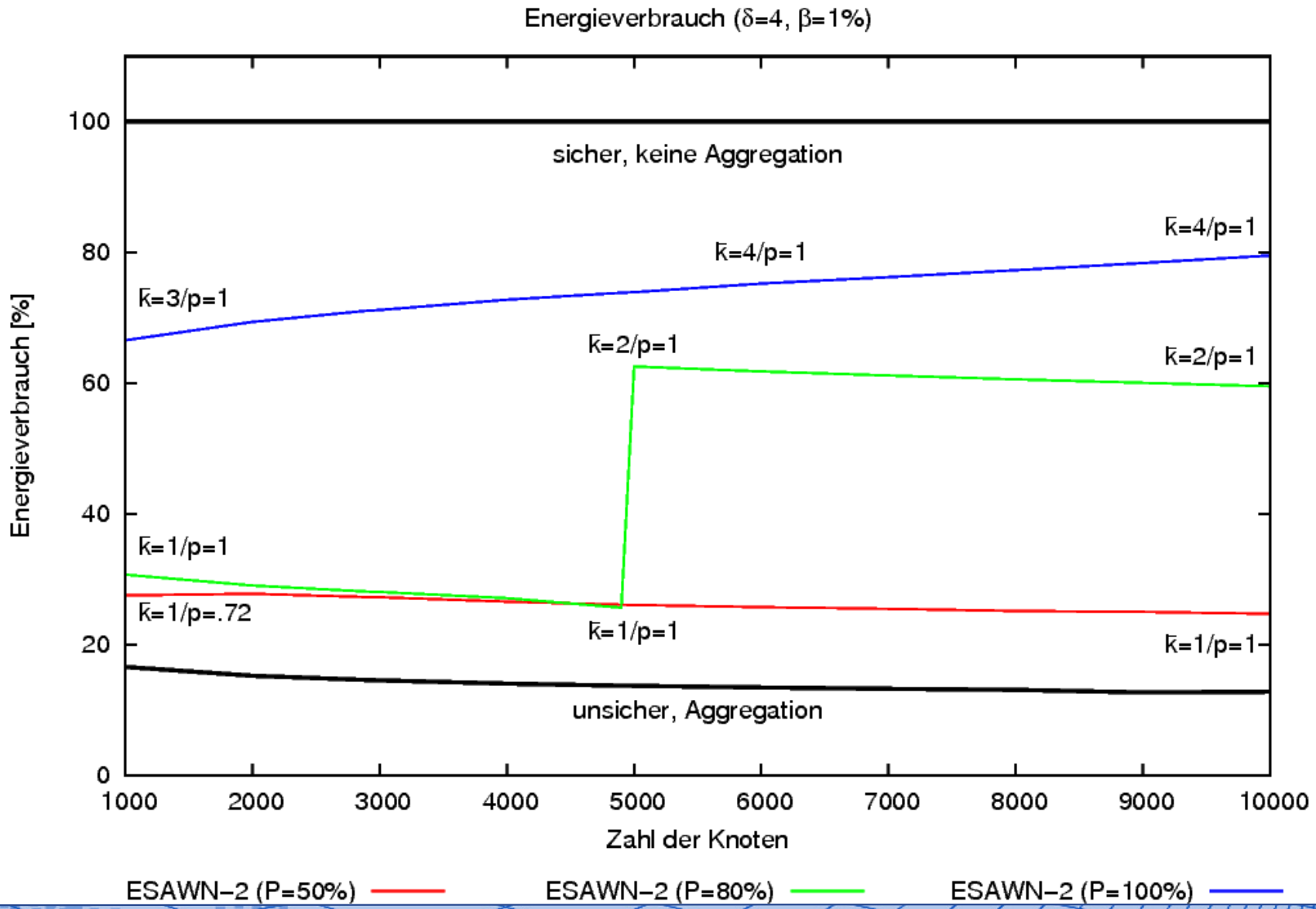
Implementierung & Evaluierung

- in GloMoSim
  - Zufälliges Generieren von Sensornetzen und Aggregationsbäumen
  - Sensornetze: n=1.000…10.000, δ=2…4
  - Routingprotokoll: precalc
  - Protokollieren der Zahl der
    - durchgeführten Aggregationen
    - Verschlüsselungsvorgänge
    - versendeten Pakete
  - daraus Berechnung der Energiekosten (MICA2, RC5)
- in TinyOS
  - zu Test- (praktische Realisierbarkeit) und Demonstrationszwecken, Verwendung im ZEUS-Projekt
  - ca. 22.000 Byte ROM / 410 Byte RAM

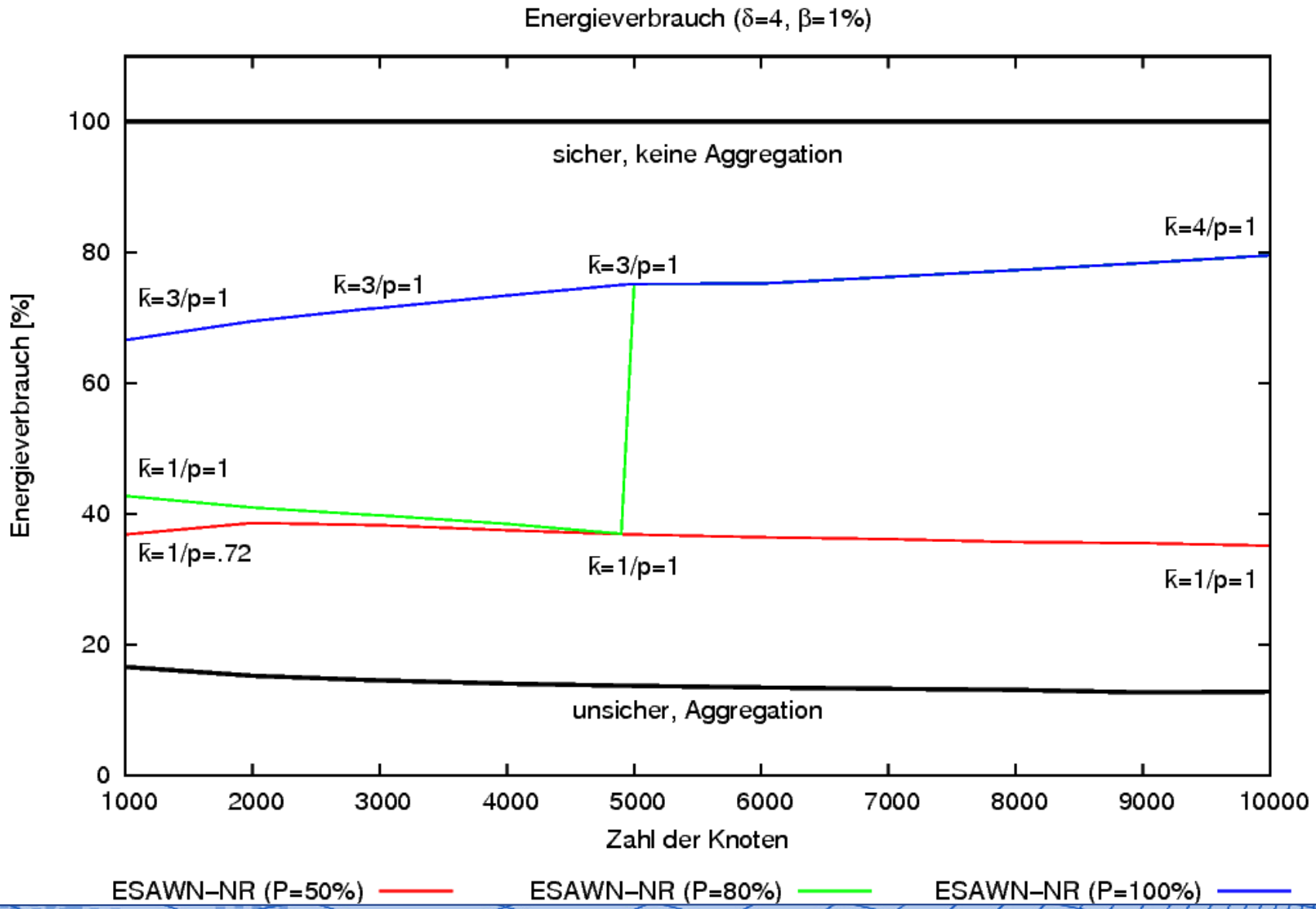
Energieverbrauch im Vergleich



Mindestwahrscheinlichkeit (I)



Mindestwahrscheinlichkeit (II)



Zusammenfassung

- Eigenschaften der ESAWN-Protokolle
  - beliebige Aggregationsfunktionen
  - Speicher- und Energieverbrauch in O(1) bezüglich Netzwerkgröße
  - ESAWN realisiert „Vollständigkeit“
  - ESAWN-2 zusätzlich „Korrektheit“
  - ESAWN-NR zusätzlich „Non-Repudiation“
    - Schlüsselaufdeckung erfordert neue Schlüssel
- Energie-Sicherheit-Tradeoff
  - Nutzer kann Tradeoff flexibel bestimmen
  - Wahl von Protokoll, k/$\overline{k}$ und p