FG Simulation & Modellierung
Institut für Systems Engineering
Welfengarten 1, 30167 Hannover

Leibniz Universität Hannover

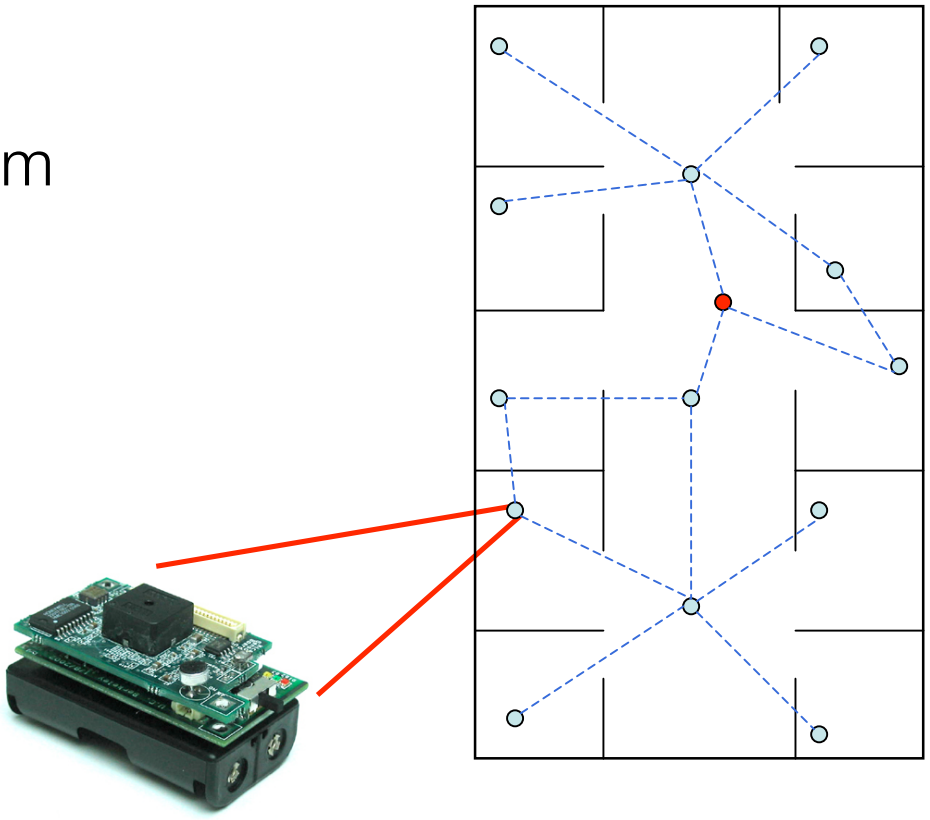
Impact of Misbehaviour and its Detection in Ad-hoc Wireless Sensor Networks using Artificial Immune Systems

Sven Schaust, Leibniz Universität Hannover

3. Fachgespräch KuVS, Berlin

Übersicht

- Motivation
- Künstliches Immunsystem
- Simulationen / Tests
- Ergebnisse
- Fazit



© Crossbow Technology Inc.

Motivation

- Betrachtung von drahtlosen Ad-hoc Sensornetzen
  - Geringe Prozessorleistung, wenig Speicher, variable Topologie

→ Was passiert wenn Knoten sich (un-)absichtlich fehlerhaft verhalten?
Kann man dies Erkennen und Knoten ausgrenzen?

- Eigenschaften Intrusion Detection Systems
  - Basiert auf Netzsensoren, Hostsensoren
  - Signaturdatenbank, heuristische Suche

- Eigenschaften Artificial Immune Systems
  - Lernendes System, „self vs. non-self“ Erkennung mittels Detektoren
  - Auswertung lokalen Datenverkehrs

Intrusion Detection System

- Aufgaben von IDS:
  - Identifizieren und Verhindern von Missbrauch durch bekannte Attacken.
  - Erkennen von Fehlverhalten (Anomalien) für unbekannte Attacken.

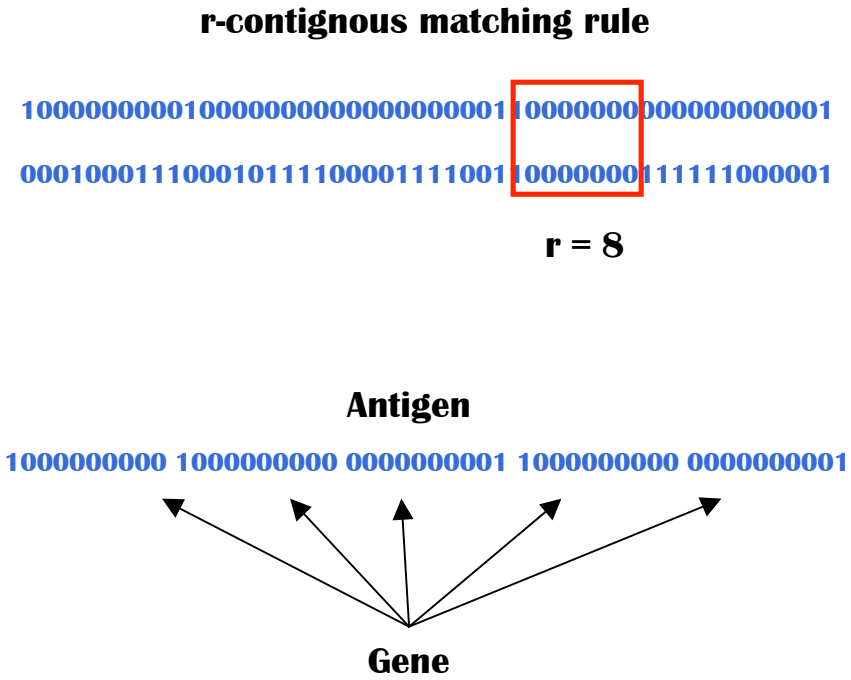
- Vor- und Nachteile:
  - Missbrauchbasiertes IDS: Geringe Rate von Falschmeldungen, aber keine Möglichkeit neue Attacken zu erkennen.
  - Anomaliebasiertes IDS: Hohe Rate von Falschmeldungen, aber Erkennung von neuen Attacken.

Künstliches Immunsystem

- Primär: ein System zur Unterscheidung von „self“ und „non-self“.
- AIS basiert auf Ideen aus der Immunabwehr des Menschen. (Hofmeyr / Forrest [1])
- Arten von IS:
  - Selbstlernend („adaptive immune system“)
  - Vorausgehende Lernphase („innate immune system“)

Wie funktioniert ein AIS?

- Erstelle „self“ Menge.
- Erzeuge Detektorstrings mittels Zufallsprozess.
- Wähle Detektoren mittels negativer Selektion.
- Verwende „überlebende“ Detektoren um vorhandene Antigene zu testen.
- Wenn Detektor auf Antigen reagiert, erzeuge eine Immunantwort. (Fehlverhalten erkannt)
- Klone und mutiere Detektoren um neue Antigene zu erkennen.



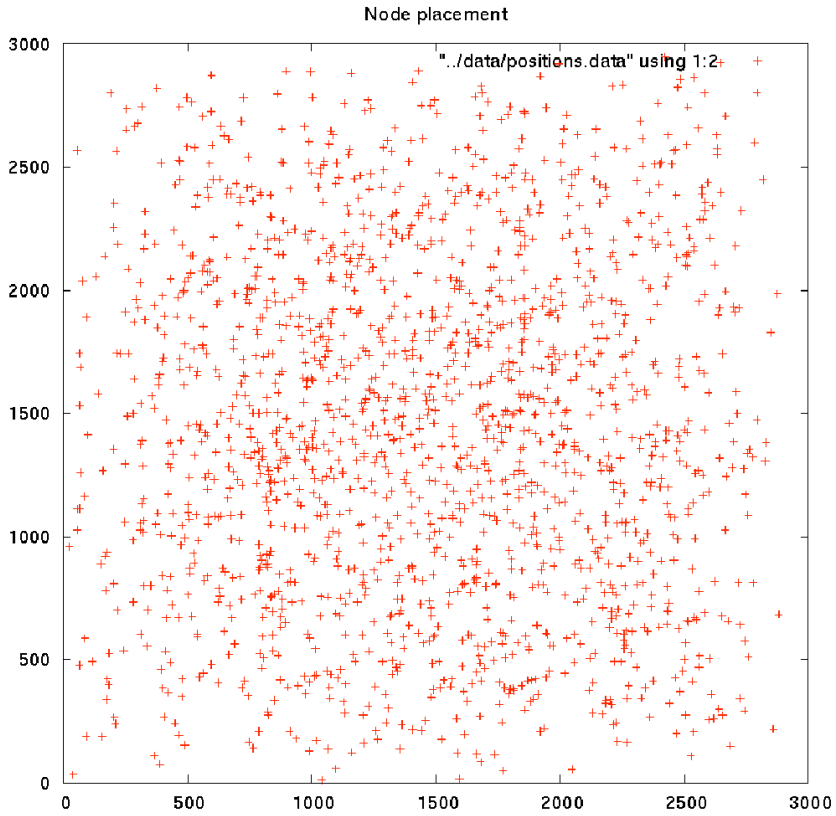
AIS für Sensornetze?

- IDS sind nur bedingt geeignet für Sensornetze
  - Topologieänderungen haben Einfluss auf Netzsensoren
  - Hostsensoren benötigen Speicher, Rechenleistung und betrachten nur Angriffe auf lokales System.
- Überwachung muss leichtgewichtig sein und darf den Knoten nicht übermäßig belasten.
- AIS scheinen besser geeignet zu sein für Sensornetze.
  - Datenverkehr in „Hörweite“ wird zur Analyse genutzt.
  - Datenaufkommen und Verarbeitung vertretbar.
  - Durch geeignete Wahl der Invarianten (Gene) lässt sich eine gute Anomalieerkennung erreichen.

Simulationen / Tests

- Ziel: Untersuchung der Eignung von AIS für Ad-hoc Netze.
- Ad-hoc Netz mit 1718 Knoten
- 10 Verbindungen (CBR)
- MAC: IEEE 802.11b
- Routing: DSR

- Fehlverhalten: Paket wird verworfen (236 Knoten).
- Simulationen für jedes Szenario mit Glomosim 2.03



Gene für AIS

Gen 1:

$$\frac{\text{completeHandshakes}}{\text{numberOfRTSSent}}$$

Gen 2:

$$\frac{\text{numberForwardedData}}{\text{numberdataToBeForwarded}}$$

Gen 3:

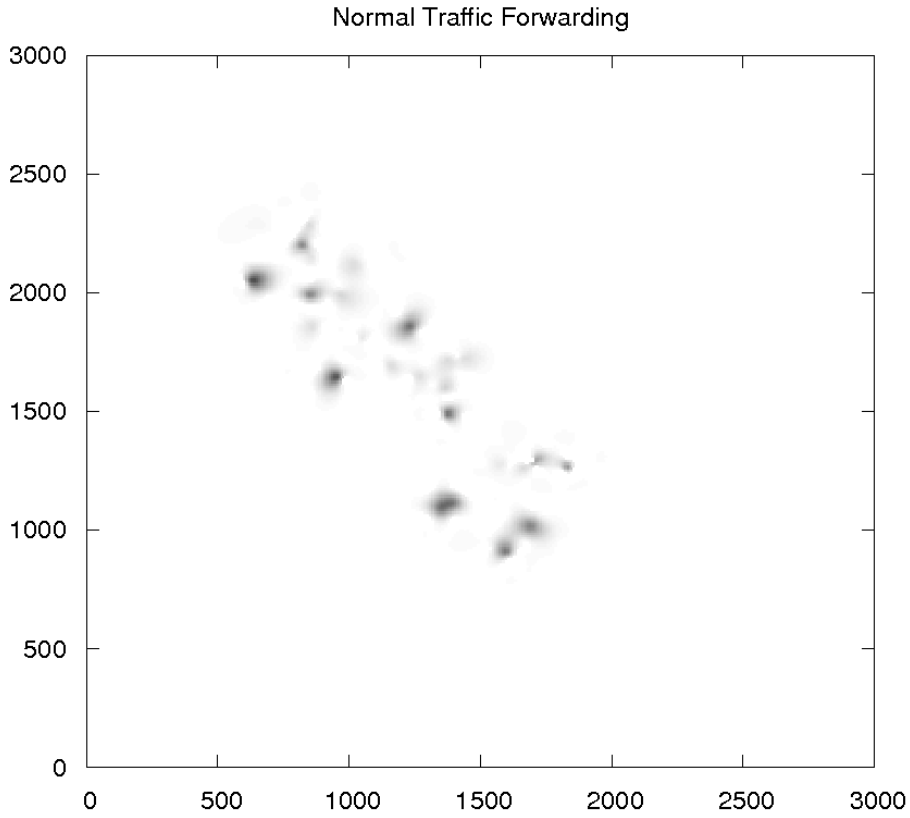
avg delay of forwarded data packets

Gen 4:

$$\frac{\text{numberRERRForwarded}}{\text{numberRERRToBeForwarded}}$$

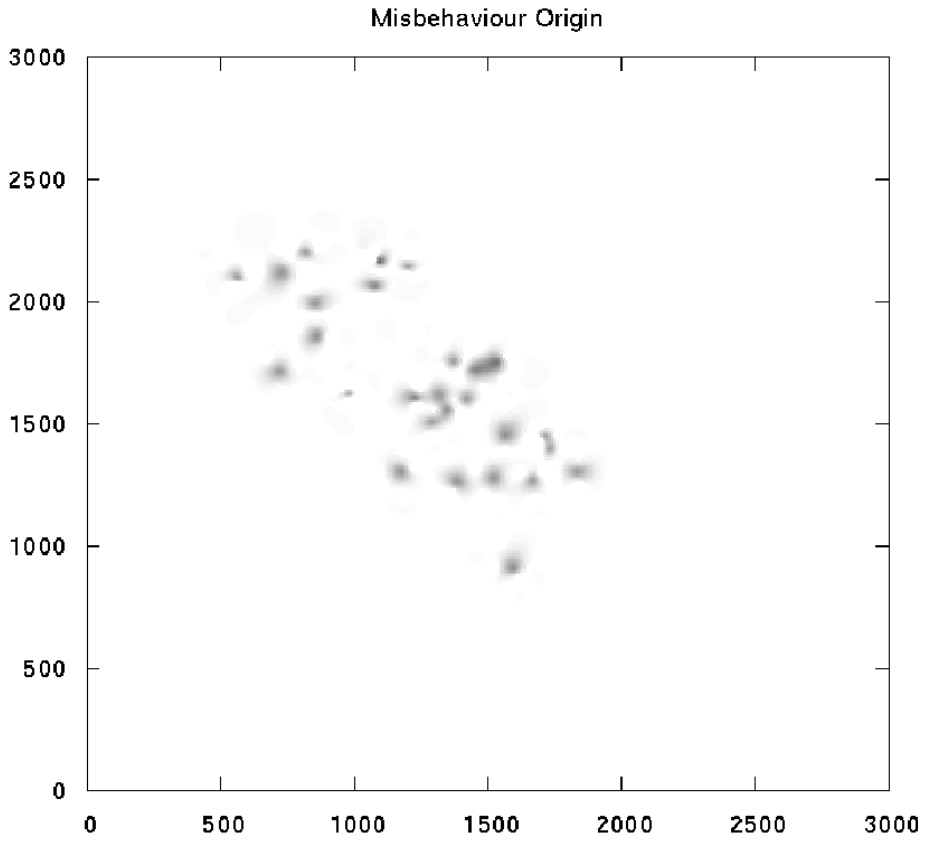
Gen 5:

avg delay of forwarded RERR packets



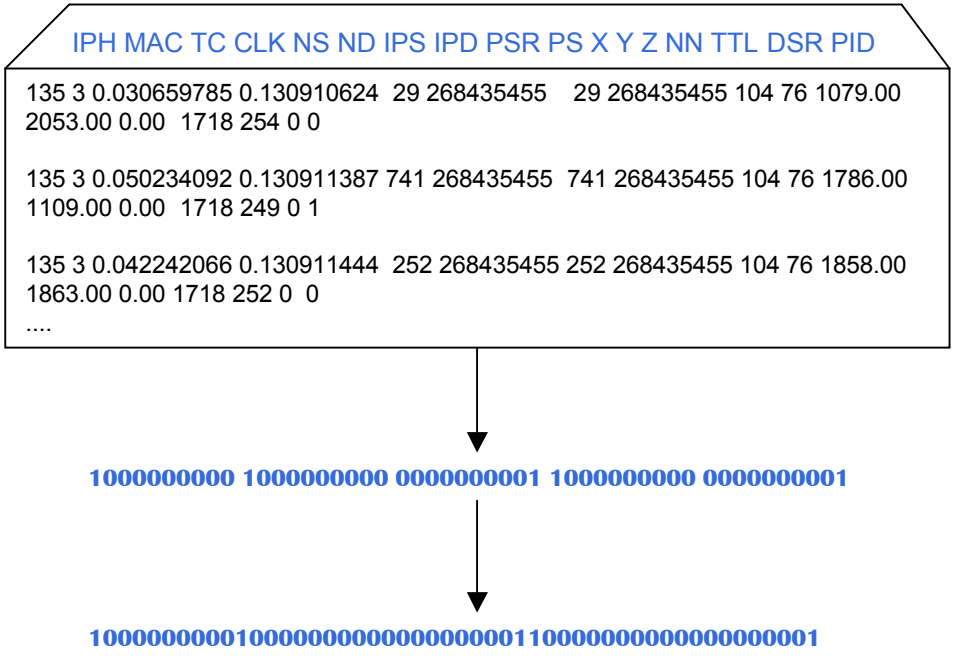
Fehlerhafte Knoten

- Knoten mit Fehlverhalten sind im Bereich der Datenrouten um einen Einfluss auf den Datenverkehr zu haben.
- Getestete Fehlerraten:
  10%, 20%, 30%, 50%



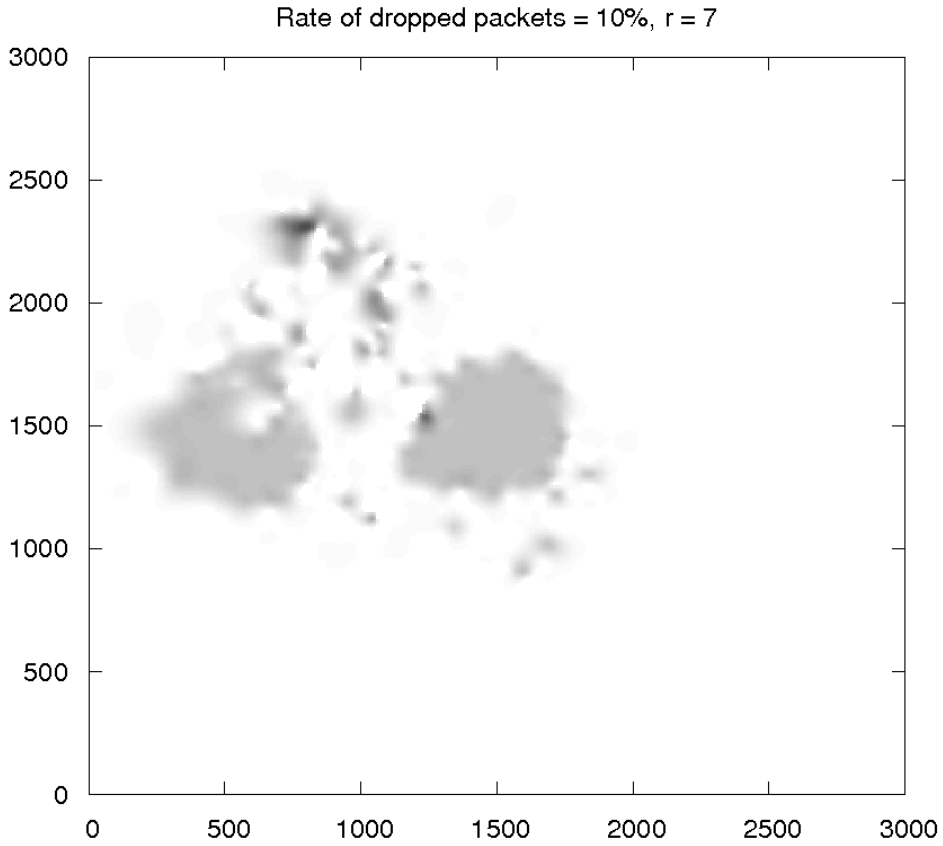
Erzeugen der Antigene

- Antigene wurden für alle Knoten kontinuierlich über ein Zeitintervall generiert.
- Jeweils aus Datenverkehr von 500 Sekunden wurden 5 Gene generiert.
- Aneinanderfügen erzeugte das Antigen.



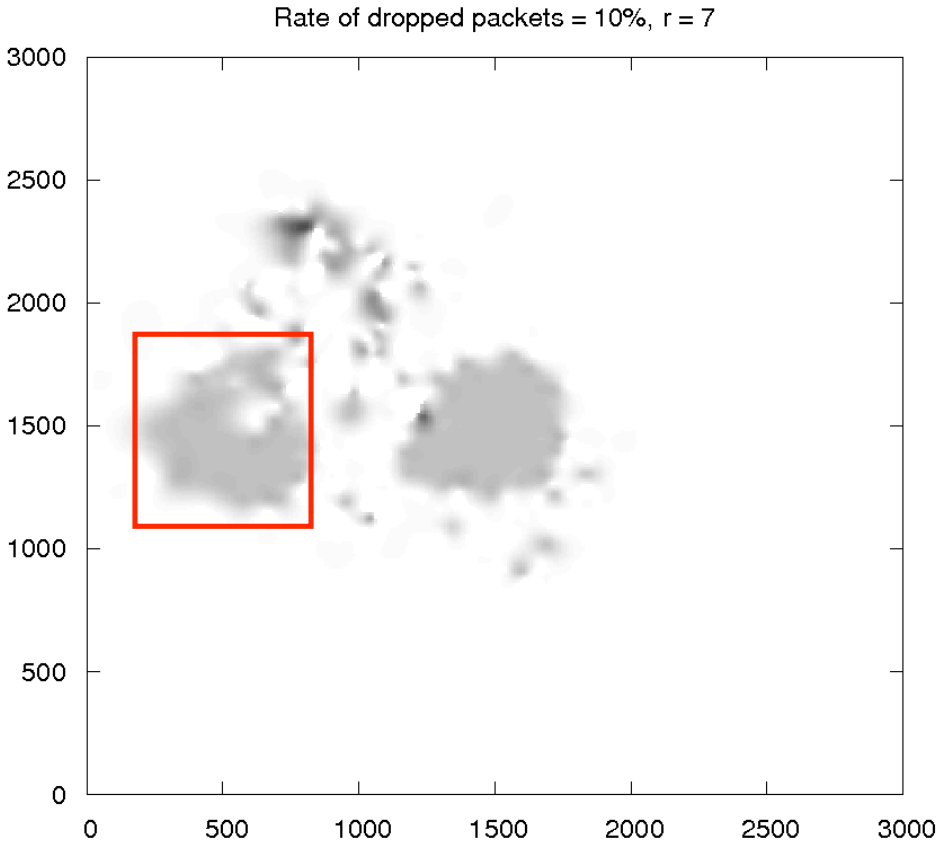
Ergebnisse

- Das AIS ist in der Lage Fehlverhalten zu erkennen.
- Erkennung von Knoten die Pakete verwerfen > 2/3
- Die verwendeten Gene sind aber noch nicht aussagekräftig genug um andere Fehler zu erkennen.
- Es bedarf daher einiger Verfeinerungen und weiterer Suche nach besseren Invarianten für verschiedene Angriffsszenarien.



Anomalie oder Fehlverhalten?

- Das AIS hat neben den Bereichen mit fehlerhaften Knoten auch einen weiteren Bereich entdeckt.
- Dieser Bereich markiert den neuen Datenfluss zwischen Quelle und Senke.
- Mechanismus zur Vermeidung solcher Anomalien in Arbeiten von Le Boudec und Aickelin [3,5]



Fazit

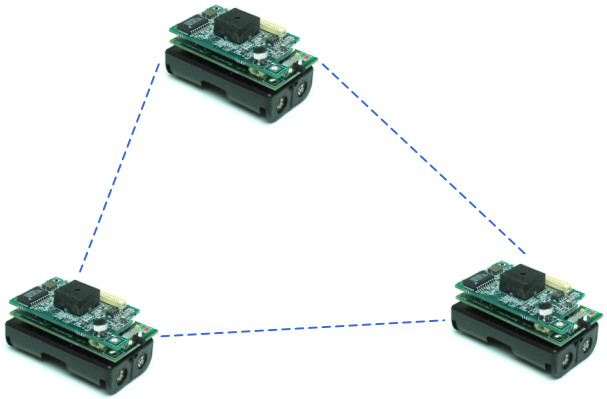
AIS für Sensornetze?

Unsere Simulationen und die Arbeit von Le Boudec [3] deuten darauf hin das ein Einsatz in Ad-hoc Sensornetzen möglich ist.

Nächste Meilensteine:

- Weitere Simulationsstudien
- Verbesserung der Gene (RREQ-, RREP-Pakete, TCP-Schicht).
- Verbesserung / Erweiterung des AIS (Danger theory, Signale).
- Implementierung eines AIS auf einem realen Sensornetz.

Vielen Dank für Ihre Aufmerksamkeit!
Fragen?



© Crossbow Technology Inc.

© www.quarella.co.uk/virus

Referenzen

[1] S. Hofmeyr and S. Forrest. Immunity by Design: An Artificial Immune System. *Proc. Genetic and Evolutionary Computation Conference (GECCO), 1999.*

[2] M. Drozda, H. Szczerbicka, T. Bessey, M. Becker and R. Barton. Approaching Ad Hoc Wireless Networks with Autonomic Computing: A Misbehavior Perspective. *Proc. of Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS*), 2005.

[3] Slavisa Srafijanovic and Jean-Yves Le Boudec. An Artificial Immune System for Misbehavior Detection in Mobile Ad-Hoc Networks with Virtual Thymus, Clustering, Danger Signal and Memory Detectors. *Proc. ICARIS, 2004*.

[4] Uwe Aickelin, Julie Greensmith and Jamie Twycross. Immune System Approaches to Intrusion Detection - A Review. *Proc. The 3rd International Conference on Artificial Immune Systems (ICARIS'04), 2004.*

[5] U. Aickelin, P.Bentley, S.Cayzer, J. Kim, and J. McLeod. Danger theory: The link between ais and ids. *Proc. ICARIS, 2005.*

NS-Algorithmus & non-self Menge