

Selbstorganisierende Netzwerke

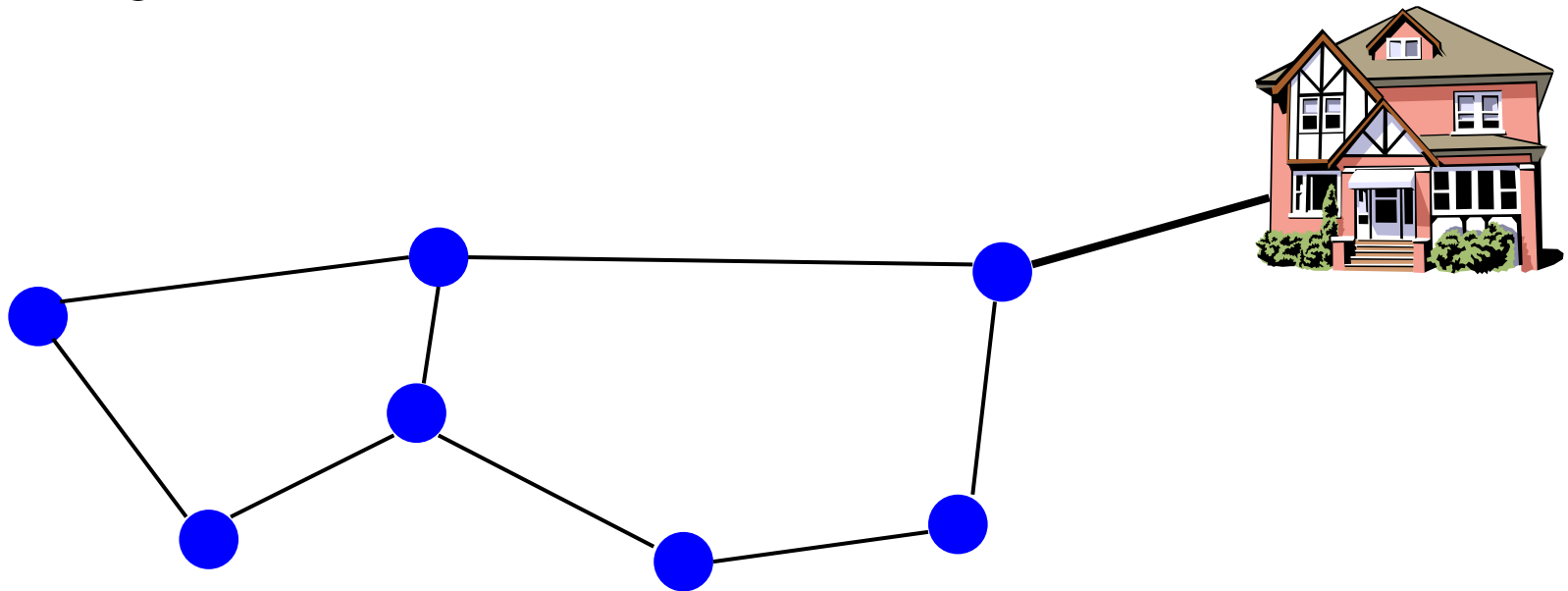
Chance oder Sicherheitsrisiko in der Logistik?

Security Forum 2008
Prof. Birgit Wilkes, TFH Wildau



Selbstorganisierende Netze

- Knoten werden auf einer Fläche verteilt.
- Sie organisieren sich selbständig zu einem Netzwerk.
- Sie geben Informationen weiter.



Selbstorganisierende Netze kommen überall dort zum Einsatz, wo

- keine Möglichkeit besteht, statische Funk- oder Sensorknoten zu installieren.
- die Gegebenheiten des Umfelds statische Funklösungen nicht zulassen und Multihop-Verfahren notwendig sind.
- das zu überwachende Umfeld sich ständig dynamisch ändert.

Selbstorganisierende Netze eignen sich hervorragend in vielen Anwendungen der Logistik

- Besonderheiten und Herausforderungen
 - **Beschränkte Ressourcen (Energieversorgung)**
 - Dynamische Netzwerktopologie
 - Unbeaufsichtigte mobile Sensorknoten
 - **Offenes Netzwerk**
 - Fehlverhalten von Knoten


Aus diesen Besonderheiten ergeben sich völlig neue Verhaltensweisen und damit Sicherheitsprobleme in den Netzwerken.

Neue Funkknoten sollen in das Netz integriert werden.


- Wie vermeide ich die Integration feindlicher oder kompromittierter Knoten?
- Wie kann ich feindliche Knoten erkennen?
- Wie kann ich die Authentifizierung sicherstellen, wenn es keine übergeordnete Instanz gibt?
- Wie realisiere ich ein Schlüsselmanagement, wenn die übertragenen Daten verschlüsselt werden sollen?

**Sicherheitskonzepte für offene Netze sind ein
Forschungsthema und stehen noch am Anfang**


Aus der Abhängigkeit der Knoten von einer Batterie resultieren neue Verhaltensweisen:



Normaler
Multihop-
Funkknoten



egoistischer
Funkknoten



feindlicher
Funkknoten

Knoten in der Mitte eines Netzes oder in der Nähe von Datensinken werden stark belastet, verlieren Energie und fallen als erste aus.

In den Netzwerken ist die Implementierung von Verfahren erforderlich, die in der Lage sind, Egoismus auszugleichen.

Bestrafung

- Beurteilung von Knoten durch andere.
- Festsetzen einer Grenze zur Feindseligkeit.
- Ausschluss eines feindseligen Knotens bei Mehrheit.

Anreiz

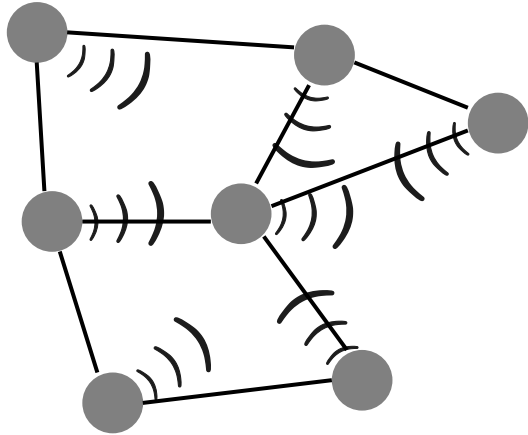
- Knoten erhalten Credits, wenn sie Daten für andere transportieren.
- Knoten müssen Credits zahlen, wenn sie selbst Daten schicken wollen.

Aus der beschränkten Energieversorgung ergibt sich eine Gruppe völlig neuer Angriffe, die darauf ausgerichtet sind, Knoten Energie zu entziehen

- Herbeiführen von Kollisionen
- Vernichtung von Quittungen
- Überflutung mit Nachrichten

oder sie bei anderen Knoten zu diskreditieren.

- Greyhole Attacks
- Blackhole Attacks
- Sinkhole Attacks

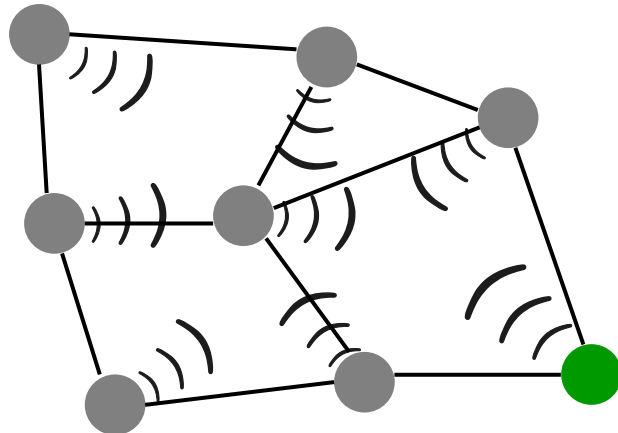


Annahme:

- Alle Knoten sind gleichberechtigt, es gibt keine Sonderstellungen.

Problem:

- Sicherheit des Systems kann nicht gewährleistet werden.



Erkenntnis:

- Es gibt immer einen ausgezeichneten Knoten z.B. eine Datensenke.

Lösung:

- Es gibt einen Knoten, der eine Stromversorgung hat und sicherheitsrelevante Aufgaben übernimmt.

Danke für
Ihre Aufmerksamkeit!