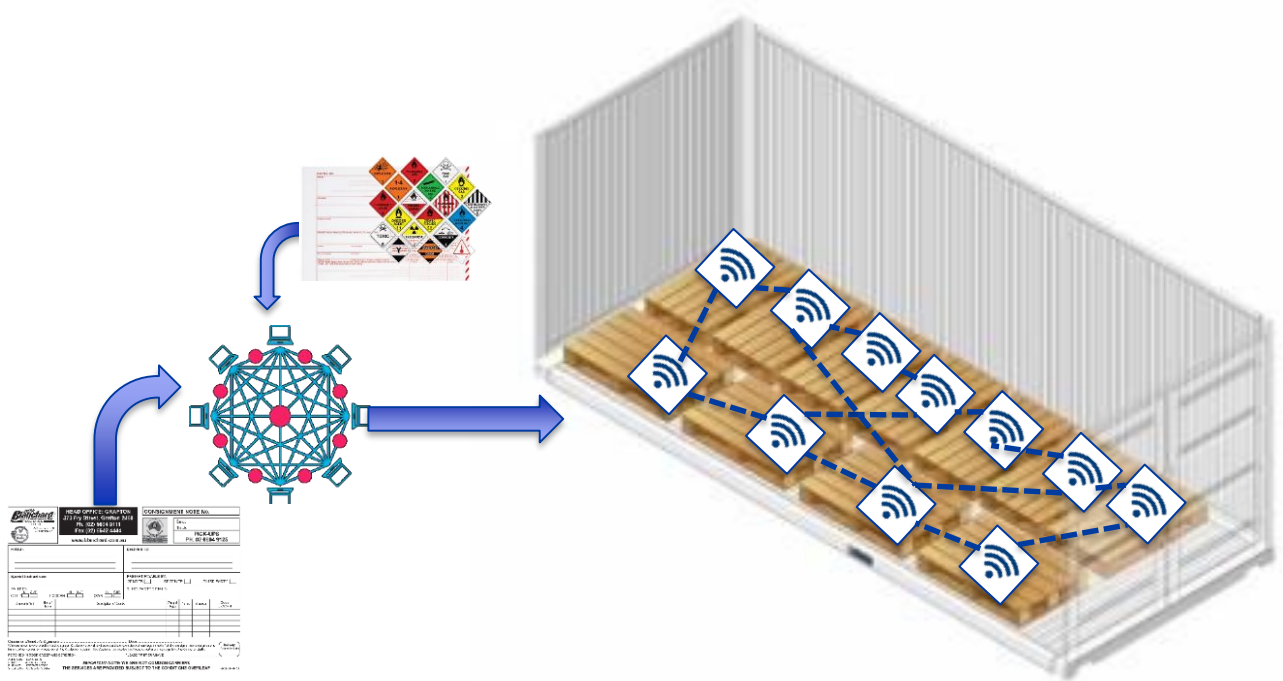
PROOF-OF-LOCATION

A Byzantine fault tolerant method for securing sensor-data-communication

Lorenz Bornholdt (B.Sc.)
Hochschule für Angewandte Wissenschaften Hamburg
Mai 2019

NEUE DIGITALE ÖKOSYSTEME

- Zunehmende Digitalisierung von Prozessen in Industrie 4.0, Smart-X (Smart-City, Smart-Grid, Smart-Health...)
- Drahtlose Sensornetzwerke: Reduzierter Speicher, Bandbreite, verteilte Systeme, keine zentrale Instanz
- Wie kann Vertrauen hergestellt werden?



TRUST PROBLEM IN EINEM VERTEILTEN SYSTEM

Vertrauen (engl. Trust)

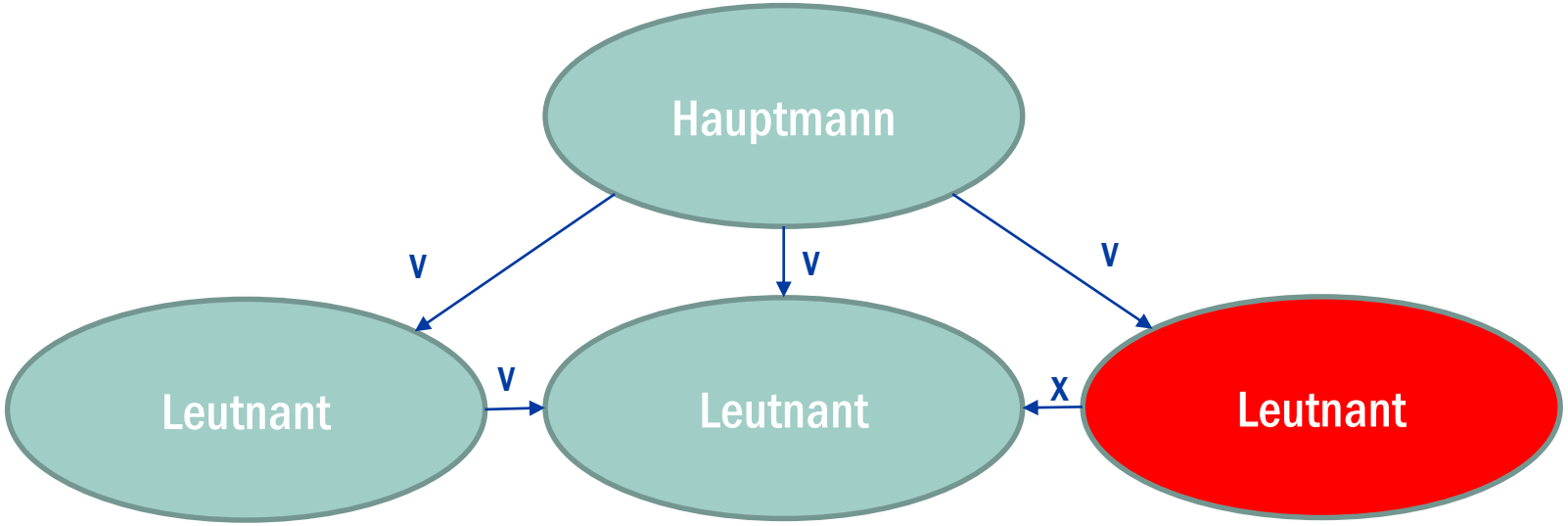
Integrität

„property that data has not been altered or destroyed in an unauthorized manner" ISO/IEC 27000:2014

Authentizität

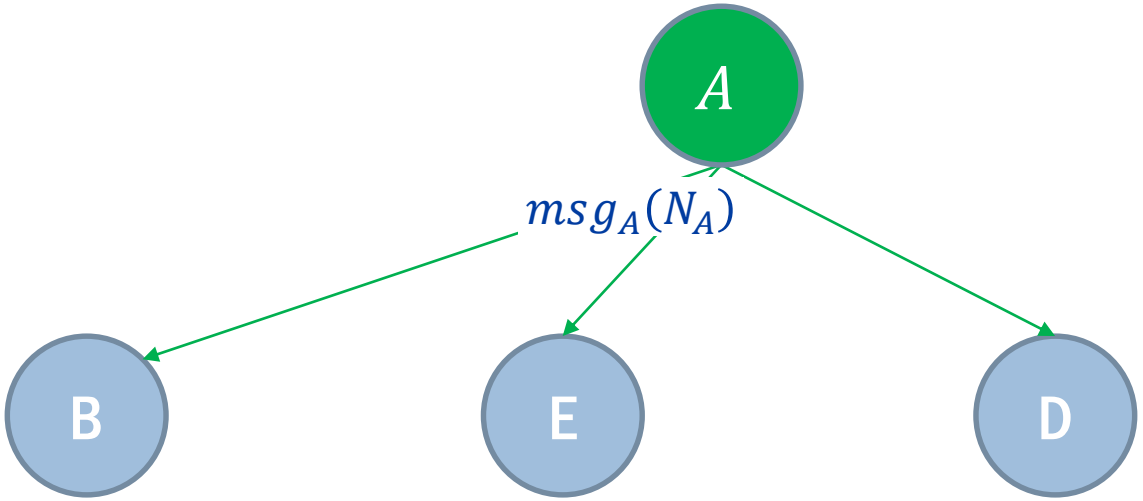
„Property that an entity is what it claims to be" ISO 7498-2:1989

KURZFASSUNG BYZANTINISCHES GENERALSPROBLEM

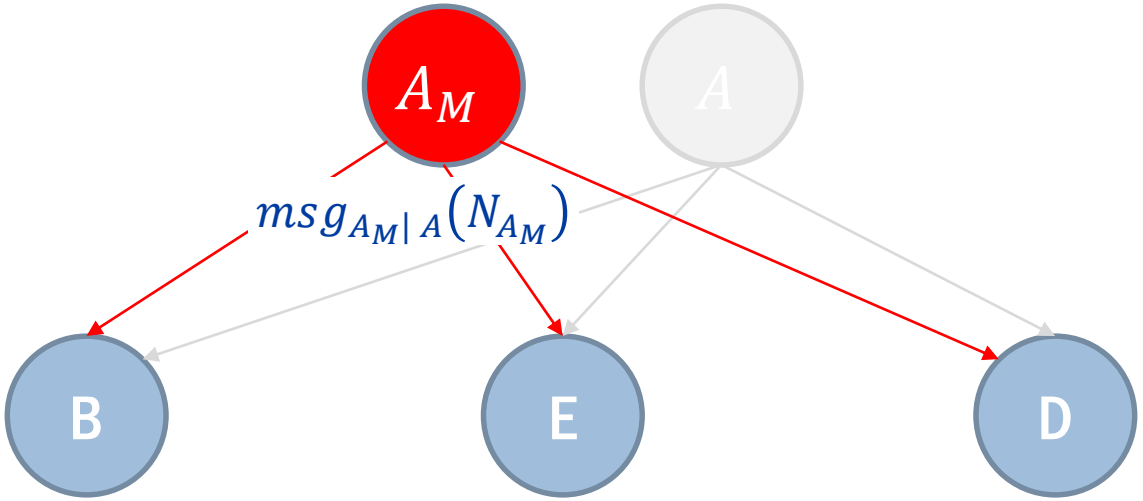


→Problem für $3m + 1$ Generäle bei m Verrätern lösbar

ANGRIFFSSZENARIEN IN DRAHTLOSEN SENSORNETZWERKEN MITTELS FALSCHER IDENTITÄTEN



ANGRIFFSSZENARIEN IN DRAHTLOSEN SENSORNETZWERKEN MITTELS FALSCHER IDENTITÄTEN

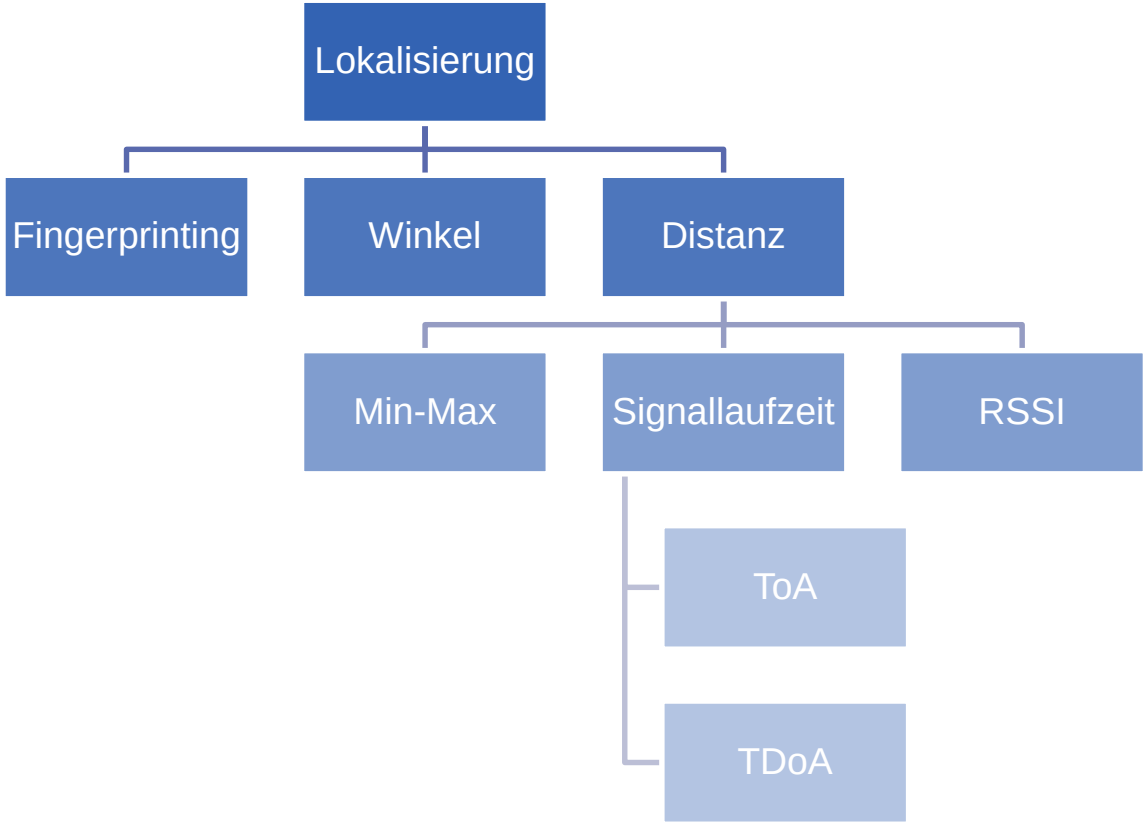


PROOF-OF-LOCATION

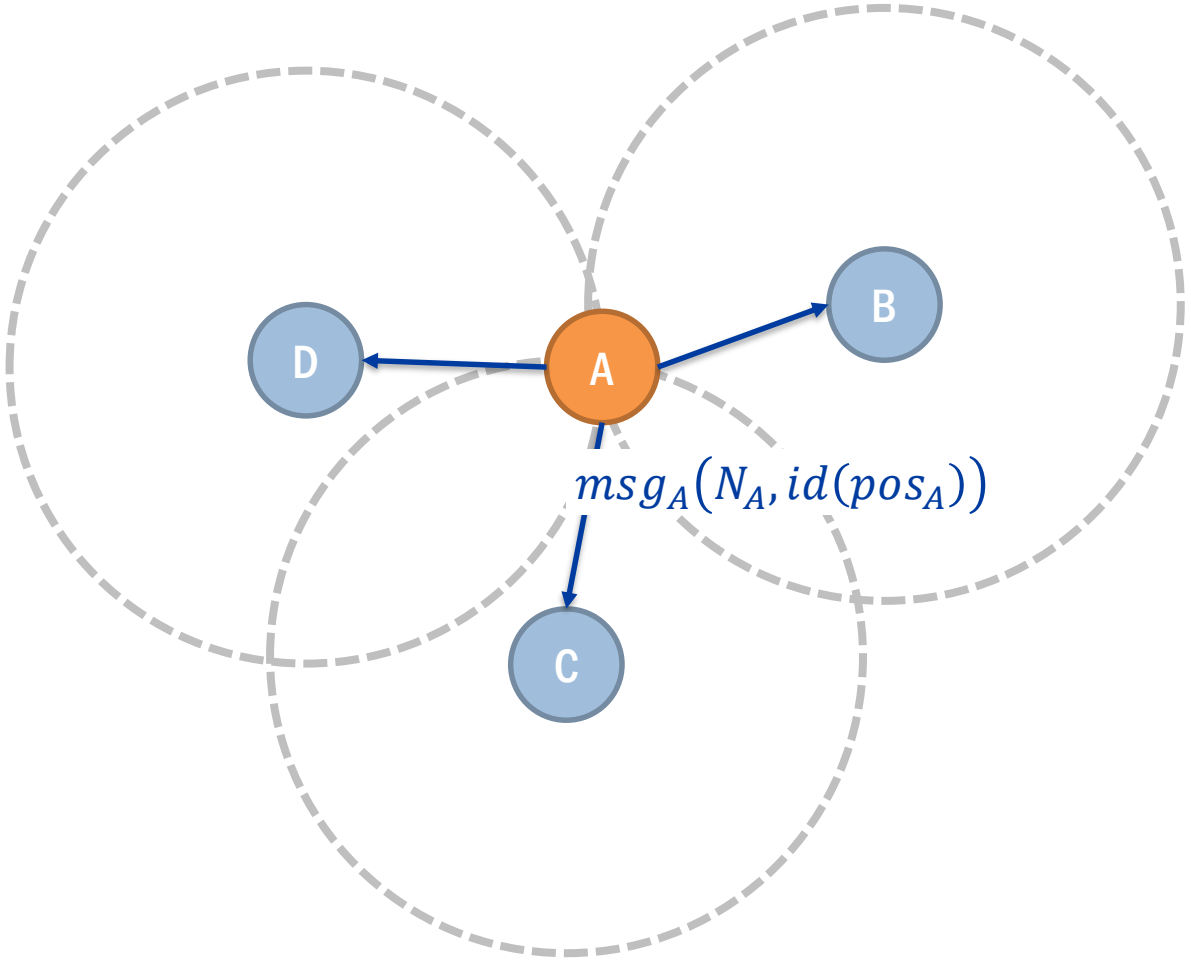
- Grundüberlegung: Position eines Knotens wird Teil seiner Identität $id_{node}(pos_{node})$
- Zu Beginn einer Messkampagne ortet sich jeder Knoten zu festgelegten Ankerpunkten
- Im Laufe der Messkampagne wird diese Position durch andere Netzwerkteilnehmer verifiziert

PROOF-OF-LOCATION

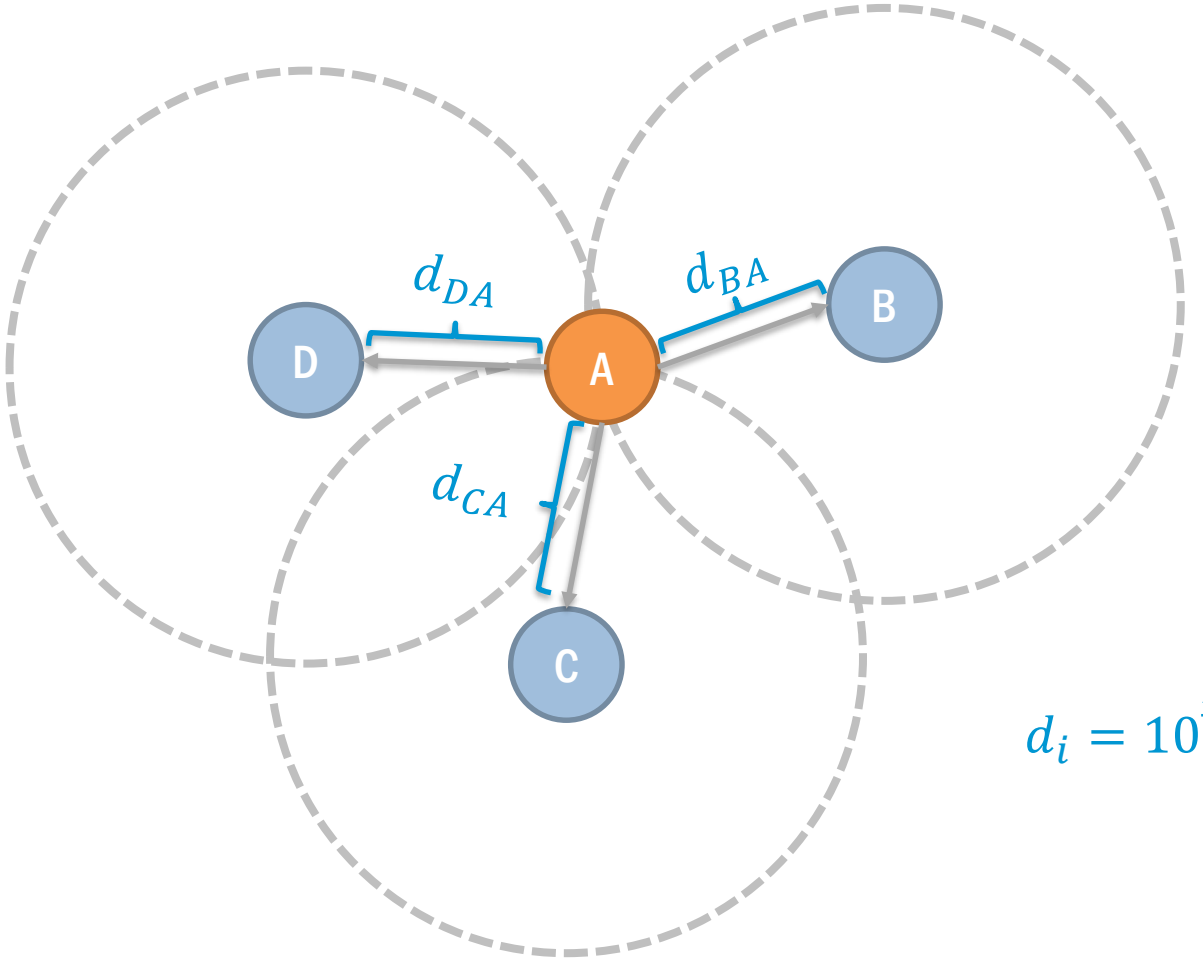
- Grundüberlegung: Position eines Knotens wird Teil seiner Identität $id_{node}(pos_{node})$
- Zu Beginn einer Messkampagne ortet sich jeder Knoten zu festgelegten Ankerpunkten
- Im Laufe der Messkampagne wird diese Position durch andere Netzwerkteilnehmer verifiziert



PROOF-OF-LOCATION: SENDEN EINER NEUEN NACHRICHT

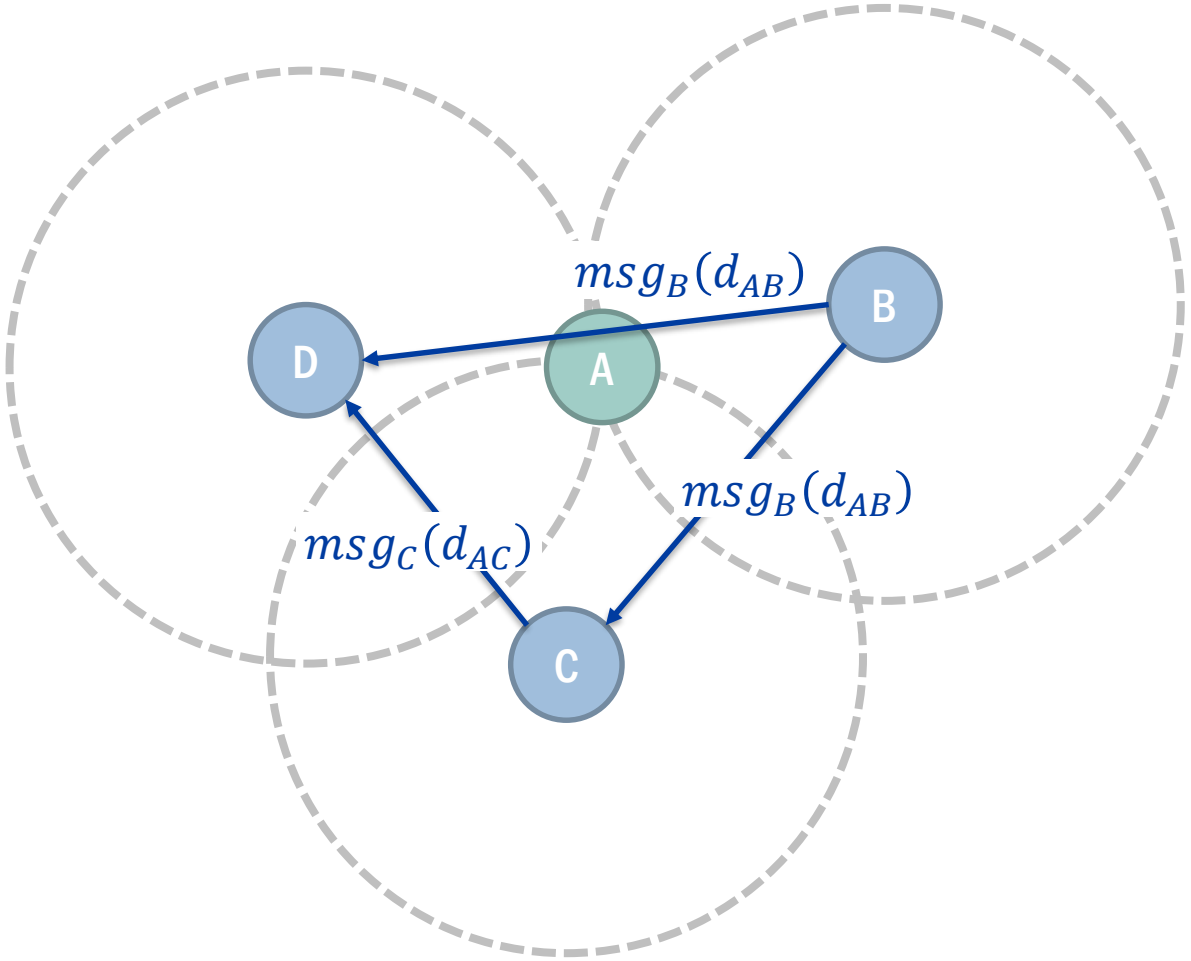


PROOF-OF-LOCATION: DISTANZEN ZU DER DATENQUELLE

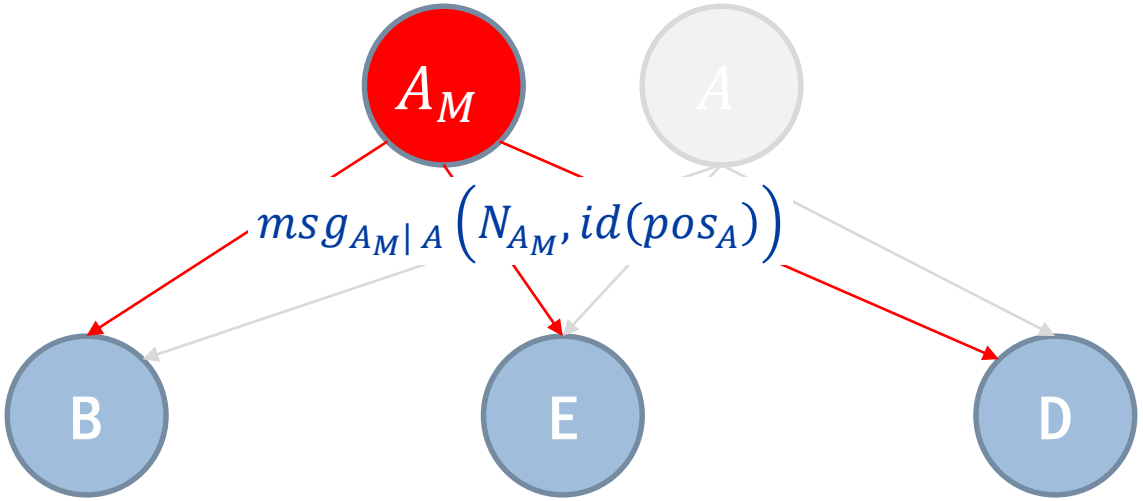


$$d_i = 10^{\frac{RSSI_i - A}{-10n}}$$

PROOF-OF-LOCATION: BFT-ÄHNLICHER DATENABGLEICH



ANGRIFFSSZENARIEN IN DRAHTLOSEN SENSORNETZWERKEN MITTELS FALSCHER IDENTITÄTEN



ZUSAMMENFASSUNG UND AUSBLICK

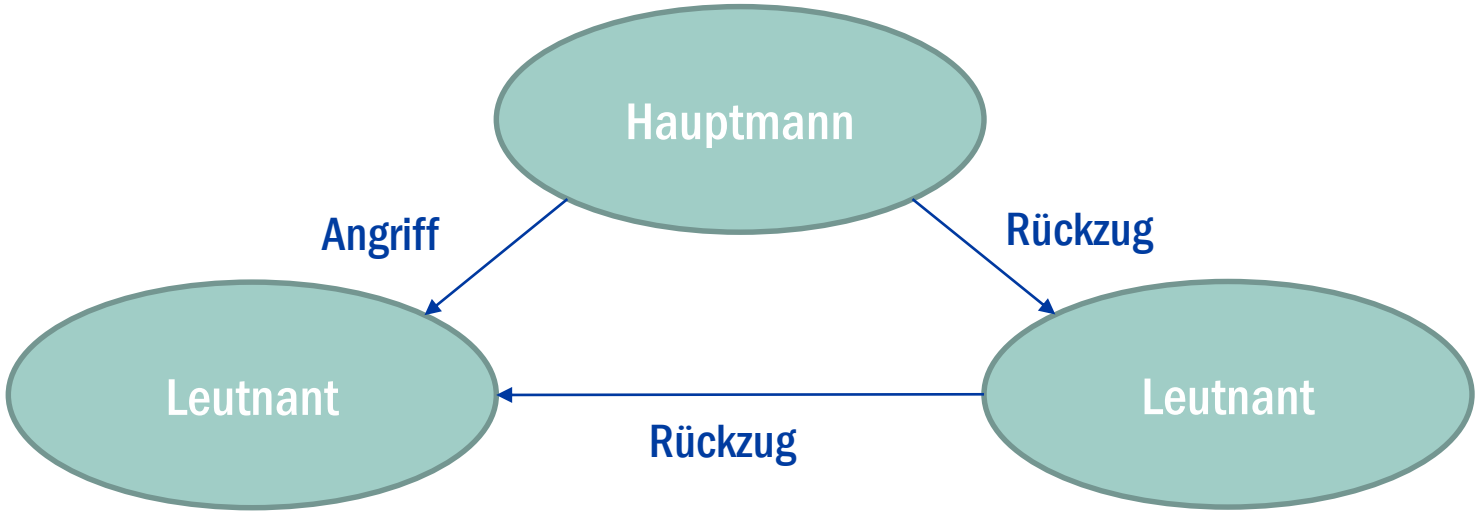
- Ein vertrauensbildendes Verfahren, welches auf BFT-ähnlichen Prinzipien basiert, wurde vorgestellt
- Die relative Position eines Sensorknotens wird hier als identitätsbildendes Merkmal verwendet

- Das Protokoll soll im Zuge weiterer Forschung verbessert werden mit Fokus auf:
  - Berücksichtigung geometrischer Spezialfälle
  - Fehlerminimierung der signalstärkebasierten Ortung
  - Aufbau einer fälschungssicheren Historie unter Berücksichtigung von Blockchain Prinzipien

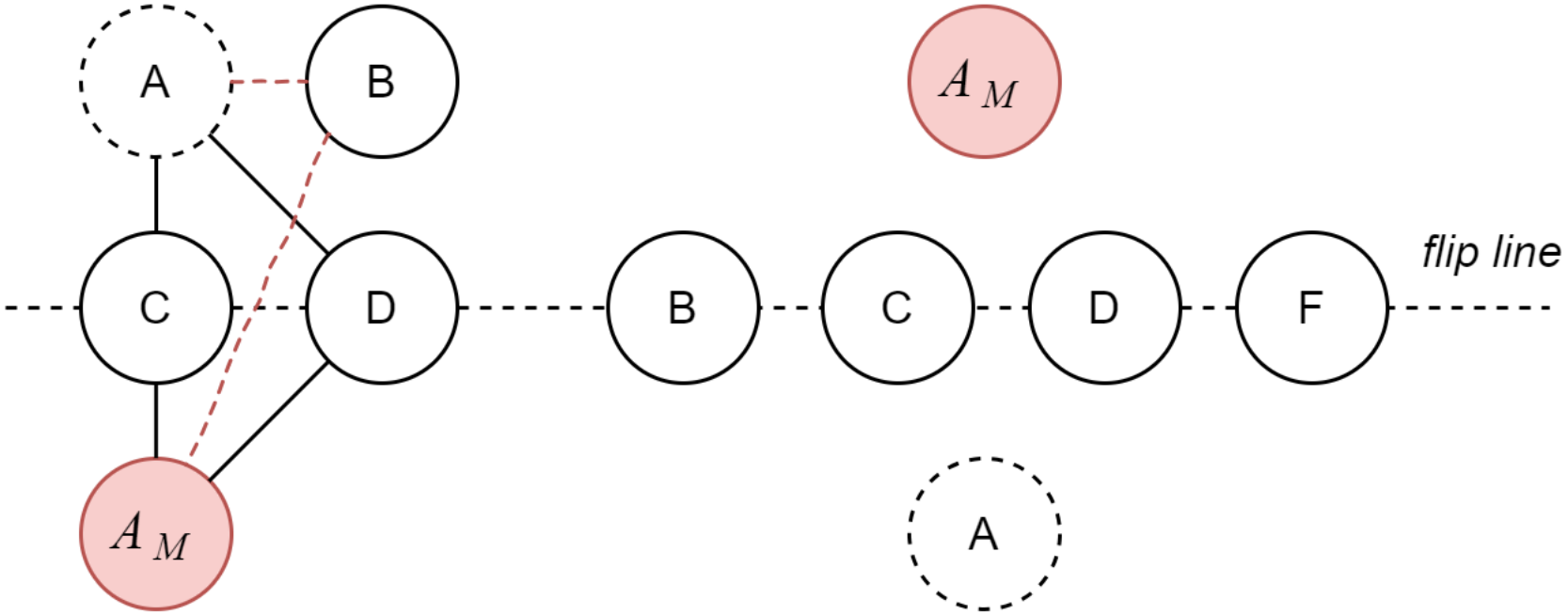
VIELEN DANK FÜR IHRE AUFMERKSAMKEIT

HAW HAMBURG

BACK-UP: BYZANTINISCHES GENERALSPROBLEM



BACK-UP: FLIP LINE



BACK-UP: PROOF OF LOCATION DATAGRAM