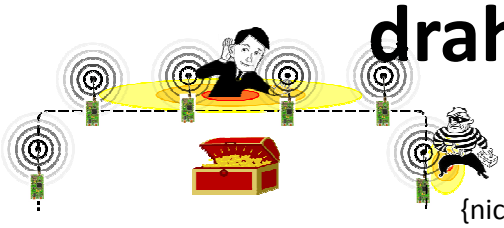
Telematics
Computer Systems

Freie Universität Berlin

Sicherheit in ereignisorientierten, drahtlosen Sensornetzen



Nicolai Schmittberger und Norman Dziengel
Freie Universität Berlin
Computer Systems and Telematics Group
{nicolai.schmittberger, norman.dziengel}@fu-berlin.de

Warum Sicherheit?

Motivation

- Alle drahtlosen Sensornetze sind mit geringem technischen Aufwand kompromittierbar.
- Besonders sicherheitsrelevant sind z.B. Geländesicherung, Medizin und Militär.
- In ereignisorientierten, drahtlosen Sensornetzen kann der Datenverkehr reduziert [Wit] und dadurch erstmals realistisch gesichert werden.
- Sicherheit muss Kommunikation schützen und Funktion des Sensornetzes gewährleisten.

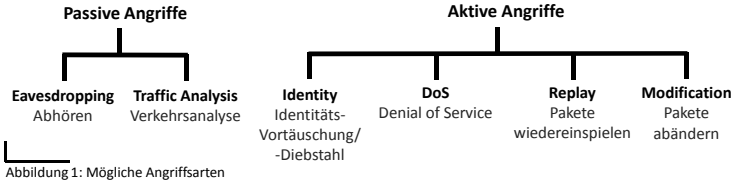


Abbildung 1: Mögliche Angriffsarten

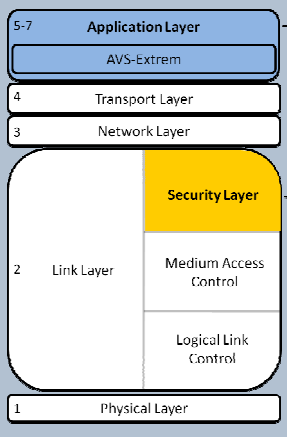
Was ist Sicherheit?

Kriterien und Umsetzung für ein sicheres Sensornetz

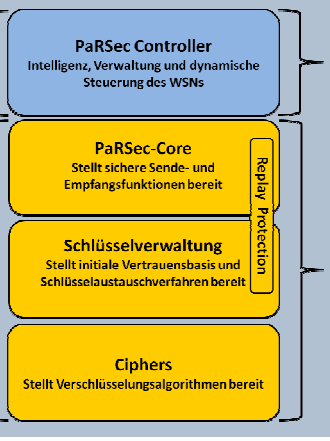
✓ **Vertraulichkeit:**	Symmetrisches Blockverschlüsselungsverfahren im Cipher-Block-Chaining (CBC) Modus - derzeit SkipJack, AES, RC5, TwoFish, 3DES
✓ **Authentizität:** ✓ **Integrität:**	Message Authentication Code (MAC)
✓ **Aktualität:**	16-Bit (2-Byte) Counter
✓ **Semantische Sicherheit:**	8-Byte Initialization Vector (IV) inkl. Counter
✓ **Zugangskontrolle:**	Paarweise und globale Schlüssel mit 20-Byte Schlüssellänge
! **Verfügbarkeit:**	Dynamische Anpassung des Sicherheitslevels, Angriffserkennung

Realisierung

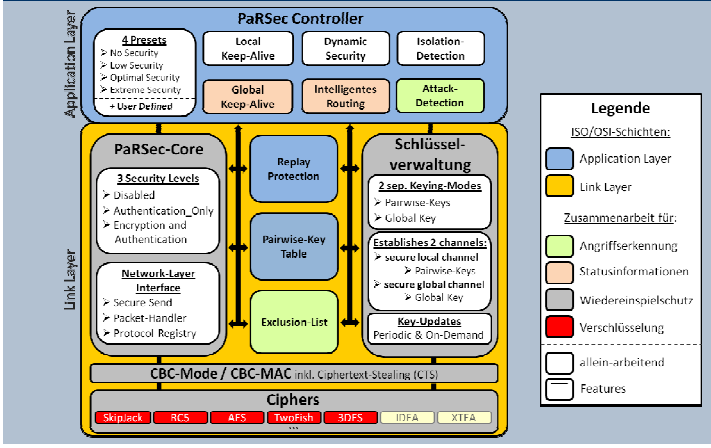
Integration in ISO/OSI-Modell



Sicherheitskonzept



Software-Architektur



Umsetzungsdetails

Sicheres Schlüsselaustausch-Verfahren

- Baut auf Basis sicherer initialer Gruppenschlüssel **sichere paarweise-Verbindungen** auf.
- Gewährleistet sicheren Austausch neuer Schlüssel für alle Knoten
- **Austausch-Intervalle** sind beliebig wählbar und garantieren Sicherheit vergangener Daten im Falle einer Kompromittierung des aktuellen Schlüssels
- Kompromittierte Knoten können mittels **Exklusions-Liste** ausgeschlossen werden.

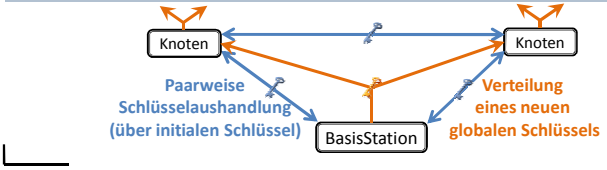
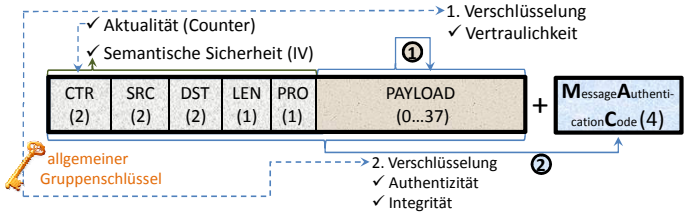


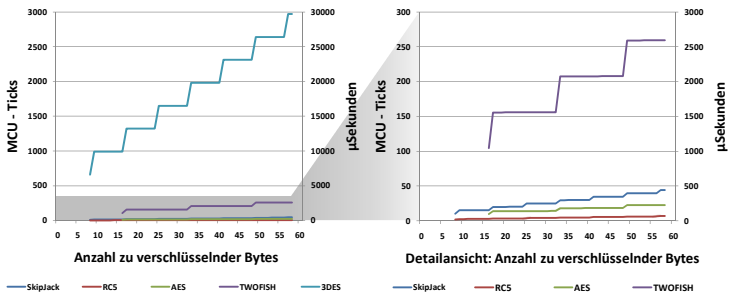
Abbildung 2: Schlüsselaustauschverfahren

Absicherung eines Netzwerkpakets

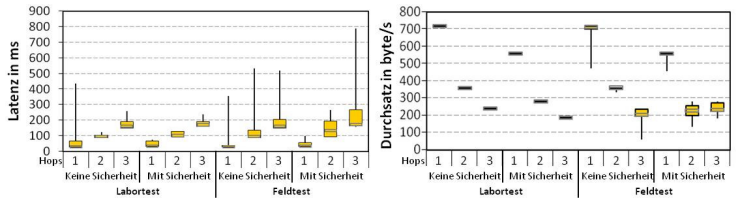


Auswertung

Rechenzeitbedarf der einzelnen Verschlüsselungsalgorithmen



Latenz – und Durchsatz-Veränderung durch Sicherheitsschicht



[Wit]: Georg Wittenburg, Norman Dziengel, Christian Wartenburger and Jochen Schiller. A System for Distributed Event Detection in Wireless Sensor Networks. Proc. of 9th ACM/IEEE Conf., IPSN, Stockholm (Apr 2010)