Universität Karlsruhe (TH)

Institut für Theoretische Informatik
Lehrstuhl Prof. P. H. Schmitt

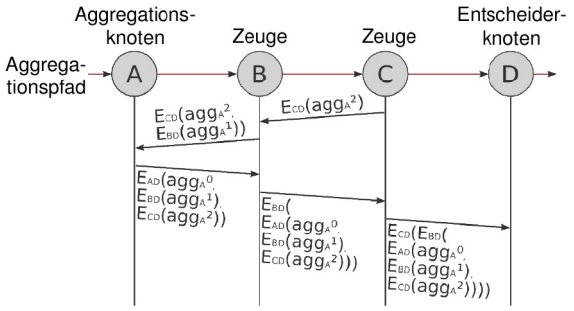
Frank Werner

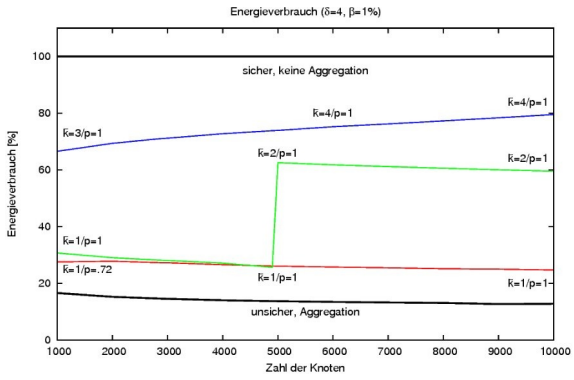
Geb. 50.34, Raum 308
frank.werner@kit.edu

Diplomarbeit

Verifikation von Protokollen zur abstufbaren Authentifizierung in Sensornetzen

Abstufbare Authentizität und non-repudiation (nicht Abstreitbarkeit) sind wichtige Eigenschaften moderner Datentransportprotokolle in drahtlosen Sensornetzen. Da Sensorknoten in solchen Netze oft stark-beschränkten Ressourcen unterliegen, lässt sich durch die Verwendung von Datenaggregation ein beachtliches Maß an Energie einsparen. Zusätzlich verlangt man von solchen Protokollen, dass sie authentisch arbeiten und Knoten, die falsche Daten einschleusen, nicht-abstreitbar identifiziert werden, d.h. sie können ihr Verhalten nicht leugnen.





In der vorliegenden Diplomarbeit sollen bestehende Protokolle wie z.B. ESAWN (Extended secure aggregation for wireless networks) [Blaß, Wilke, Zitterbart: A Security-Energy Trade-Off for Authentic Aggregation in Sensor Networks] auf Korrektheit untersucht werden. Hierzu wird das Problem in einer geeigneten Abstraktion modelliert und mit Hilfe formaler Methoden und Model-Checking Algorithmen untersucht. Praktische Erfahrung in Verifikations-Tools z.B. Spin und Uppaal sind von Vorteil, aber nicht erforderlich.