LoRaKeY

Secret Key Generation for Low Power Wide Area Networks

Programm / Ausschreibung	Bridge, Bridge_NATS, Bridge_NATS 2016	**Status**	abgeschlossen
Projektstart	01.09.2017	**Projektende**	30.09.2019
Zeitraum	2017 - 2019	**Projektlaufzeit**	25 Monate
Keywords	Secret Key Generation, LoRaWAN, Low-Power, Physical Layer Security		

Projektbeschreibung

Drahtlose Niedrigenergieweitverkehrnetzwerke (englisch: Low-Power Wide-Area Network, Kurzform: LPWAN) ermöglichen einen energieeffizienten Datenaustausch für verschiedene Kommunikationsanwendungen im Bereich Internet der Dinge (IdD). Jedoch ist in solchen Netzwerken der Aufbau von starker Kommunikationssicherheit durch regelmäßige Schlüsselerneuerung herausfordernd aufgrund der hohen Anzahl an drahtlosen Endgeräten (> 1000) und strenger Ressourcenbeschränkungen. An dieser Stelle bietet das Projekt LoRaKeY starkes Verbesserungspotential. Unter Verwendung von drahtlosen Physical Layer Sicherheitskonzepten werden neue Schlüsselerzeugungsalgorithmen gezielt für zentralisierte LPWAN entwickelt. Das erfordert, sich den neuen Herausforderungen wie etwa Schlüsselerzeugung unter hoher Netzwerkbelastung, während der Präsenz von Störsignalen oder bei Einschränkungen aufgrund von Hardware-Voraussetzungen zu stellen. Die angestrebten Ergebnisse zeigen starke Bedeutung: Erstens, Physical Layer Schlüsselerzeugung über weite Distanzen (> 10km) kombiniert mit niedrigem Energieverbrauch wird realisierbar. Zweitens, Kommunikationssicherheit zwischen drahtlosen Geräten und der Basisstation kann auf ein mit kryptographischen Protokollen, wie sie beispielsweise in IoT Backend Systemen (Cloud-/Web-Services) Verwendung finden, vergleichbares Niveau erhöht werden. Daher hat dieses vorgeschlagene Projekt das Potential, Physical Layer Schlüsselerzeugungsmethoden in einen Einsatzbereich zu bringen, wo diese hohe Relevanz aufweisen.

Abstract

Wireless Low-Power Wide-Area Networks (LPWAN) enable energy efficient data exchange for several light-weight Internet of things applications. However in such networks, establishment of strong communication security via periodic secret key refreshment becomes non-trivial due to high number of wireless nodes (> 1000) and strict resource constrains. This is where the project LoRaKeY aims to make a change. By utilizing wireless physical layer security concepts, novel secret key agreement methods customized for centralized LPWAN will be developed. This nessecitates to tackle challenges such as key agreement in dense communication scenarios, presence of interfering signals or restrictions due to ultra-light hardware implementations. The anticipated results show strong impact: Firstly, wide range physical layer key agreement (> 10 km) combined with ultra low energy consumption becomes feasible. Secondly, the communication security between the wireless nodes and the base-station can be lifted to comparable levels with the cryptographic protocols utilized, e.g., in IoT Backend systems (cloud/Web-services). Thus, the proposed project has the potential to bring physical layer key agreement

techniques to a domain where they are highly relevant.

Projektkoordinator

- Hochschule für Angewandte Wissenschaften St. Pölten Forschungs GmbH

Projektpartner

- Microtronics Engineering GmbH