LoRaWAN Security

Olivier Seller

Technical Fellow, Semtech, and LoRa Alliance® Technical Committee Vice-Chair, Fremont, CA, United States
E-mail: oseller@semtech.com

Received 19 December 2019; Accepted 10 March 2020;
Publication 30 April 2021

Abstract

The LoRaWAN security design adheres to state-of-the-art principles: use of standard, well-vetted algorithms, and end-to-end security. The fundamental properties supported in LoRaWAN security are mutual end-point authentication, data origin authentication, integrity and replay protection, and confidentiality. The use of symmetric cryptography and prior secret key sharing between a device and a server enables an extremely power efficient and network efficient activation procedure.

Keywords: LoRaWAN, security, authentication, encryption, Join Server, activation, personalization, provisioning.

1 Introduction

The LoRaWAN protocol is optimized for low power consumption wide area networks. It supports low-cost, mobile, and secure bi-directional communication for Internet of Things applications. LoRaWAN networks can handle millions of devices. Security is a fundamental need in all IoT applications, it is therefore an important aspect of the LoRaWAN specification. LoRaWAN security fits the general LoRaWAN design criteria: low power consumption, low implementation complexity, low cost and high scalability. As devices are deployed in the field for long periods of time (years), security must

Journal of ICT, Vol. 9_1, 47–60. *River Publishers*
doi: 10.13052/jicts2245-800X.915