A LoRaWAN Security Assessment Test Bench

T. Claverie, J. Lopes Esteves
Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)
Paris, France

Abstract

LoRaWAN is a recent protocol and despite having been already studied from a security perspective, several attacks have not been reproduced in practice mostly due to a lack of details regarding the test benches used. After presenting previous work on the LoRaWAN protocol and the various platforms described, we present an environment based on hardware, software and SDR to study the radio layer of the protocol. The efficiency of this architecture is demonstrated by reproducing theoretical attacks on LoRaWAN 1.0.

1 Introduction

LoRaWAN is a protocol dedicated to Low Power IoT devices; its current version (1.1) was released in October, 2017 [5]. It is built upon the LoRa (Long Range) modulation patented by Semtech.

In [4] a *replay and decrypt* attack is detailed on LoRaWAN 1.0 and the authors provide a very accurate and complete overview of the state of the art up to late 2017. A formal verification of the security of the LoRaWAN handshake has been proposed in [8]. In [19], the biasing of a random number generator in presence of electromagnetic interferences is demonstrated. Session cryptographic material desynchronisation between a device and the network has been discussed in various articles [4, 19, 14, 11, 12]. The possibility of spoofing LoRaWAN gateways in order to provide fake time and position references appeared in [12, 20]. Message modification and forgery in order to attack the network has been suggested in [15, 10].

Several LoRaWAN security testing environments have already been mentioned in previous work. However, none have been described precisely enough to allow reproductibility of the results and some do not involve instrumentation of the radio layers.

In [17, 18], the author describes using a LoRaWAN gateway, two test end devices and an open-source LoRaWAN server to emulate a complete infrastructure. However, these tests concerned only the communication in the core network, beyond the gateway. A testing platform is mentioned in [12]; it is able to capture and analyze messages, however no information on its exact capabilities and building blocks are provided. In [11], hardware attacks on devices and radio attacks are mentioned. In particular, eavesdropping of LoRaWAN communications, replay attacks, and various denial of service by flooding an object with messages are described. Again, the test infrastructure description does not allow reproducing the setup.

Even when specific radio testing has been investigated, the information regarding the test setup were left aside: no details on the jamming methods [3, 6], nor on how a LoRaWAN device is perturbated by electromagnetic interference [7] were given.

2 Experimental setup

In this section, the different components used for our test bench are introduced.

LoRaWAN Evaluation kit In order to rapidly deploy a LoRaWAN 1.0 network without having to develop the core network services, a Microchip LoRaWAN development kit [13] has been set up. This development kit includes two LoRa Mote (based on the SX1276 chipset) and a LoRa gateway (SX1301) which can be connected via ethernet to core network services packaged in a ready-to-use docker container. The administration interface allows to manage gateways, applications, devices, encryption keys and some radio parameters (frequency, modulation). It constitutes a ready-to-use LoRaWAN infrastructure but is intended only for high level interaction with the protocol and thus lacks low layer flexibility.

LoRa programmable dongle A PyCom FiPy board has been used to act as a malicious LoRa node. It is a MicroPython development board supporting LoRa modulation and including a LoRaWAN stack. With this tool one can send and receive LoRa MAC frames with a better timing accuracy and lower latency than the LoRa Mote and act as both a gateway and a device.

GNU Radio In order to also have physical layer instrumentation, the GNU Radio framework was used along with a software defined radio (SDR) USB dongle based on a Realtek RTL2832U and a R820T2 tuner. Several SDR-based LoRa receivers are available, with varying completion rates [16, 2, 1].