IEEE INFOCOM 2022 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) | 978-1-6654-0926-1/22/$31.00 ©2022 IEEE | DOI: 10.1109/INFOCOMWKSHPS54753.2022.9798063

Ruling Out IoT Devices in LoRaWAN

Pierluigi Locatelli
Sapienza, Università di Roma
Rome, Italy
pierluigi.locatelli@uniroma1.it

Pietro Spadaccino
Sapienza, Università di Roma
Rome, Italy
pietro.spadaccino@uniroma1.it

Francesca Cuomo
Sapienza, Università di Roma
Rome, Italy
francesca.cuomo@uniroma1.it

***Abstract*—LoRaWAN is certainly one of the most widely used LPWAN protocol. The LoRaWAN 1.1 specification aims at fixing some serious security vulnerabilities in the 1.0 specification, however there still exist critical points that may affect the IoT security. In this demo, we show an attack that can affect LoRaWAN 1.0 and 1.1 networks, which hijacks the downlink path from the Network Server to an End Device, ruling out the target device from the network. The attack exploits the deduplication procedure and the gateway selection during a downlink scheduling by the Network Server, which is in general implementation-dependent. The attack scheme has been proven to be easy to implement, not requiring physical layer-specific operations such as signal jamming, and could target many LoRaWAN devices at once. We demonstrate this attack and its effects by blocking a device under our control by receiving any downlink communication.**

***Index Terms*—LoRaWAN, Security, Denial of Service, Replay Attack, vulnerability analysis**

I. Introduction

In the context of IoT applications, a promising technology for supporting radio connectivity in wide coverage areas with low energy is LoRaWAN [1], [3]. LoRaWAN uses LoRa modulation and forms star topologies where every node, identified as End Device (ED), can reach directly one (or more) internet connected sink nodes named Gateways (GWs) (Fig. 1.) The Network Server (NS) or the Application Server (AS) willing to send downlink messages to an End Device (ED), schedule the transmission on one and only one specific gateway. This downlink gateway selection is not specified in the LoRaWAN standard and it is left to as implementation-dependent. This choice of the downlink gateway opens a potential vulnerability in LoRaWAN as these radio indicators could be indeed manipulated by a malicious third-party and, in this way, an attacker can control the downlink path selection and hijack it as identified in the paper [7]. In this demo, we present a proof of concept of the attack using off-the-shelf hardware and targeting our own device by exploiting the downlink gateway selection of TheThingsNetwork, the largest LoRaWAN open network. As a result of this attack, the target device will not be able to receive any downlink messages, specifically a join accept message, thus it will be ruled out of the network, since it will not be able to derive the encryption keys and join the network.

II. LoRa and LoRaWAN

In this section we describe the critical procedures of LoRaWAN on which a possible hijack attack depends on. For a more complete overview on LoRa and LoRaWAN refer to [3].

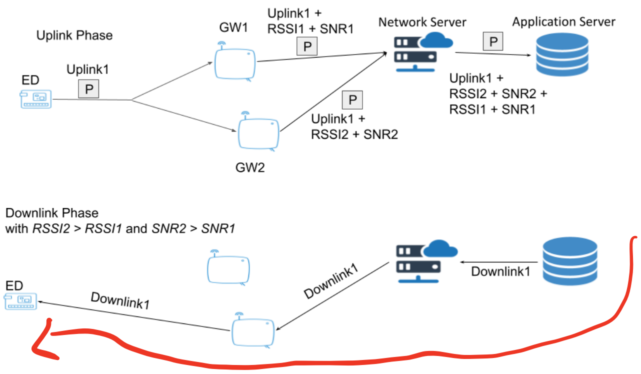

Fig. 1. LoRaWAN Architecture with an uplink, deduplication phase and the following downlink selection

A. Deduplication Procedure

In LoRaWAN, we use the term ”uplink” packet for a LoRaWAN packet sent by an ED which is received by one or more gateways. Instead, we use the term ”downlink” to refer to a packet sent by the NS toward an ED. It may be the case that multiple gateways receive the same uplink packet. In this occurrence, the NS will carry out the deduplication procedure. How the deduplication procedure is carried out is not specified in the standard and it is implementation dependant. The most famous open source implementations, like [2], carry out the deduplication as follows: on the reception of a new packet they open a time window $T_D = 200$ ms. Every copy of the same packet received within T_D is considered as duplicate. The packet that is received with the best radio link quality is kept while the other copies are discarded. This is schematized in the upper part of Fig. 1.

B. Downlink Path Selection

When the AS or the NS want to send a downlink packet to an ED, the NS has to select which gateway to use to transmit the LoRa frame. The gateway selected is the one that received the last uplink u from the ED. If multiple copies of u were received by different gateways, the deduplication step ensures that the gateway which received u with the highest radio link quality is selected to perform the downlink

978-1-6654-0926-1/22/$31.00 ©2022 IEEE

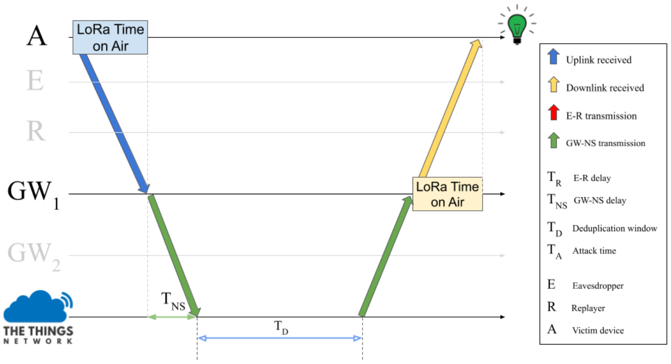

Fig. 2. First step of the demo. The target device performs a full join procedure and at the end, if the procedure ended successfully, it will light a green LED.

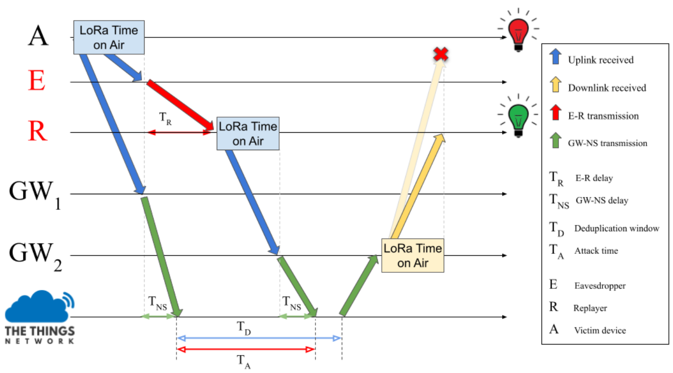

Fig. 3. Second step of the demo, where we exploit the vulnerability. The target device sends a Join Request message, which is replayed by the attacker; the target device will not receive the Join Accept message since it has been hijacked to be sent by the wrong gateway. Therefore, the victim device is ruled out from the network. In this case the target device will light a red LED while the replayer device will light a green LED.

III. Attack Identification

In this section, we describe the attack performed on both LoRaWAN 1.0 and 1.1 in accordance to the Time based Wormhole Replay (TWR) [7].

Device A is the victim device, while E and R are two malicious devices under the attacker control connected by some means to the internet. Moreover, GW_1 and GW_2 are two legitimate gateways connected to the same NS. Let GW_1 be one of the gateway that is able to receive packets generated by A. We place E near A such that the packets sent by A are eavesdropped by E. Moreover, we place R close to a gateway GW_2 such that:

1) The distance between GW_2 and A is large enough to make A unable to receive packets sent by GW_2 and viceversa;
2) $RSSI_2 > RSSI_1$, i.e. the packets sent by R to GW_2 have a RSSI, namely $RSSI_2$, greater than the one of packets sent by A and received by GW_1, namely $RSSI_1$.

The exploitation of the vulnerability goes as the following: The victim A sends an uplink packet p. Gateway GW_1 and E both receives p. E immediately forwards p to R using a traditional IP communication. R replays p as-is via LoRa which is received by GW_2. If the replay process happens before the expiration of the de-duplication window, the NS will select GW_2 as the gateway on which schedule a downlink, if necessary. However, by construction, the downlinks sent by GW_2 won't be heard by A.

IV. Demo

To test the attack we used three Libelium Waspmote PROv1.5 provided with a Microchip RN2483A LoRaWAN extension boards, which acted respectively as the victim A, as the malicious replayer R and as the eavesdropper E which listens for outgoing packets of device A. Finally we used a Raspberry PI 3B as the remote TCP server used to connect E and R. The sniffer implement a custom code (available at [6]) specifically designed to intercept on the default join-request and join-accept frequencies (868.1MHz,868.3MHz and 868.5MHz) and time windows (Rx1 after 5s and Rx2 after 6s). The gateways used to access TheThingsNetwork are RAK7246 which runs the default code for gateways offered in TheThingsNetwork stack.

In the demo we demonstrate the full functionality of the attack. We will start by showing a full, successful join procedure on the target device (Fig. 2). It will send its join request and will receive the corresponding join accept after 5 seconds. This will result in the target device playing a ”success” pattern using a buzzer and it will also light a green led to signal everything completed successfully. In case of a failed join procedure instead the device would play a different ”fail” pattern using the buzzer and it will light a red led to signal the failure of the procedure. Once the device has joined successfully, we will restart the target device which will repeat again its join procedure. This time (Fig. 3) the target device will be near the sniffer device, which will be already connected to the replayer. In this case, using the same approach to signal success and failure, we will demonstrate that by using our architecture, the target device will produce the ”fail” sound and lights, while the replayer device will produce the ”success” pattern, signaling that the join accept message was successfully hijacked and sent by the wrong gateway.

References

[1] ”LoRaWAN v1.1 Specification” LoRa Alliance, Fremont, CA, USA, 2017
[2] The Things Stack, https://www.thethingsindustries.com/stack
[3] J. Haxhibeqiri, E. De Poorter, I. Moerman, and J. Hoebeke, “A Survey of LoRaWAN for IoT: From Technology to Application,” Sensors, vol. 18, no. 11, p. 3995, Nov. 2018
[4] D. Garlisi, I. Tinnirello, G. Bianchi, and F. Cuomo, “Capture Aware Sequential Waterfilling for LoRaWAN Adaptive Data Rate,” IEEE Trans. Wireless Commun., vol. 20, no. 3, pp. 2019–2033, 2020
[5] T. C. M. Dönmez and E. Nigussie, “Security of LoRaWAN v1.1 in Backward Compatibility Scenarios,” Procedia Computer Science, vol. 134, pp. 51–58, 2018
[6] Github repository with code implemented on the boards: https://github.com/rastafaninplakeibol/LoRaWAN-DoS-TWR-Attack
[7] P. Locatelli, P. Spadaccino, F. Cuomo, ”Hijacking downlink path selection in LoRaWAN”, IEEE Globecom 2021, Spain, 2021