Chapter 2
A Survey on Attacks and Defences on LoRaWAN Gateways

Olof Magnusson
Gothenburg University, Sweden

Rikard Teodorsson
Chalmers University of Technology, Sweden

Joakim Wennerberg
Chalmers University of Technology, Sweden

Stig Arne Knoph
Chalmers University of Technology, Sweden

ABSTRACT

LoRaWAN (long-range wide-area network) is an emerging technology for the connection of internet of things (IoT) devices to the internet and can as such be an important part of decision support systems. In this technology, IoT devices are connected to the internet through gateways by using long-range radio signals. However, because LoRaWAN is an open network, anyone has the ability to connect an end device or set up a gateway. Thus, it is important that gateways are designed in such a way that their ability to be used maliciously is limited. This chapter covers relevant attacks against gateways and potential countermeasures against them. A number of different attacks were found in literature, including radio jamming, eavesdropping, replay attacks, and attacks against the implementation of what is called beacons in LoRaWAN. Countermeasures against these attacks are discussed, and a suggestion to improve the security of LoRaWAN is also included.

DOI: 10.4018/978-1-7998-7468-3.ch002

INTRODUCTION

Nowadays, more and more devices are being connected to the Internet. The term Internet of Things (IoT) is used to describe this phenomenon. These devices are typically small with a very specific purpose. They range from sensors in homes, to infrastructure, agriculture, and more. In 2019, there were 26 billion active IoT devices, and this number is expected to increase to 35 billion by 2021 (Maayan, 2020).

As IoT devices become increasingly more common, so does the need to facilitate their connection to the Internet, especially when placed in remote locations with limited access to conventional methods of Internet connections (such as 4G, Wi-Fi, or similar). To enable connection of IoT devices in these circumstances, multiple technologies have been developed, which serve devices in a wide area using low power, but with limited bandwidth. These technologies go under the umbrella acronym LPWAN, which stands for Low-Power Wide-Area Network (Wedd, 2020).

One such technology is called LoRa (**Lo**ng **Ra**nge) and is a physical-layer network protocol which enables communication with IoT devices over a wide area (10+ km) with low power consumption and low bandwidth. There are several upper-layer protocols on top of the LoRa physical layer, one of which is LoRaWAN. The physical layer protocol enables access, while the upper-layer protocols define how the network is accessed and secured.

The first version of LoRaWAN, version 1.0, was released in 2015 (LoRa Alliance, 2015). Much research has been done regarding this version and it has been discovered that it suffers from several security vulnerabilities, concerning data confidentiality, message integrity and network availability. Many of these issues were fixed when version 1.1 of the protocol was released in 2017 but, as this paper will show, not all of them.

Emerging network protocols require thorough analysis to guarantee their security. Flaws in network protocols enable attacks on connected devices, which can include extraction of poorly secured data, impersonation of devices, usage of botnets in distributed denial-of-service (DDoS) attacks, etc. It is therefore of paramount importance to secure network protocols against attacks like these.

In (Lambrinos, 2019) the author shows that a LoRaWAN network can be used to gather information from different sensors for a Decision Support System (DSS) in agriculture and smart farming. Similarly, (Cui et al, 2018) uses LoRaWAN to monitor a lake brine pump with the help of a DSS as a method to detect pump failures. In both cases the transmitted information, including weather, crop and pump voltage data, needs to be reliably and securely transmitted to facilitate quality decisions in order to, for example, optimise harvests and detect pump failures.

This paper surveys research done on attacks and defences against LoRaWAN gateways, i.e. connection points for IoT devices to the Internet, and is structured as