A Systematic Review of Security in the LoRaWAN Network Protocol

POLIANA DE MORAES, Federal University of São Paulo, Brazil
ARLINDO FLAVIO DA CONCEIÇÃO, Federal University of São Paulo, Brazil

The age of the Internet of Things is adding an increasing number of new devices to the Internet and is expected to have fifty billion connected units by 2021. These form an extensive network that may have multiple points where there is a risk of attacks that can compromise the entire system. This paper has conducted a systematic review of security in LoRaWAN protocol specification versions 1.0 and 1.1 by locating its vulnerabilities and determining what measures can be taken for improvement and how they can be checked or tested. The review identifies nineteen areas of vulnerability in the LoRaWAN protocol and shows that the current studies focus on specification version 1.0, key management, and authentication procedures.

CCS Concepts: • **Security and privacy → Security protocols**.

Additional Key Words and Phrases: systematic review, Internet of Things, LoRaWAN

ACM Reference Format:
Poliana de Moraes and Arlindo Flavio da Conceição. 2021. A Systematic Review of Security in the LoRaWAN Network Protocol. *ACM Comput. Surv.* 30, 3, Article 102 (March 2021), 20 pages. https://doi.org/XX.XXXX/XXXXXXX.XXXXXXX

1 INTRODUCTION

The age of the Internet of Things is adding an increasing number of new devices to the Internet and is expected to have 50 billion connected units by 2021. In this context, LoRaWAN protocol is a wireless wide-area network in which the architecture and operation implement system-defined properties. The first LoRaWAN specification was released in October 2015, and the second and most recent one was released in October 2017. It is characterized by low operational costs, optimal power consumption, a high number of connected devices, and long-range communication. LoRaWAN is an attractive option for Internet of Things applications because of the following features: open standards, the provision of off-the-shelf and low-cost platforms, operating services in unlicensed industrial, scientific and medical frequencies, and a private network alternative [25].

Since the LoRaWAN protocol is an Internet of Things application, it forms part of an extensive interconnected system that has multiple points that are vulnerable to attacks. These attacks aim to access, block, modify, and corrupt data or services. They can cause significant disruption to businesses and companies that do not have suitable security mechanisms in place. In addition, successful attacks can harm the reputation of a company, as well as cause a loss of sensitive data or a violation of intellectual property. Because of this, security is currently considered a crucial issue. The objective of this paper is to conduct a systematic review of security in LoRaWAN protocol specification versions 1.0 and 1.1 by locating its vulnerabilities and determining what measures can be taken for its improvement and how they

Authors' addresses: Poliana de Moraes, poliana.moraes@embraer.com.br, Federal University of São Paulo, São José dos Campos, São Paulo, Brazil; Arlindo Flavio da Conceição, arlindo.conceicao@unifesp.br, Federal University of São Paulo, São José dos Campos, São Paulo, Brazil.

Manuscript submitted to ACM