Security threats of LoRaWAN and countermeasures.

G. D. H. P. Gamage, Reg. No: MS21908538
Subject Code: IE5022 [2021/JAN]
Subject Name: Applied Network Security

February 2021

The aim of this research is to conduct a comparative security analysis in LoRaWAN, based on the layered approach for identifying major vulnerabilities. And it is proposed the different possible attacks and their countermeasures. Other than this analysis, it is developed a software-based security testing framework as a proof-of-concept, which helps to execute vulnerability test in existing LoRaWAN network.

In the last decade, the growth of the Internet of things (IOT) and the low power wide area (LPWA) technology transformation is happening at a rapid pace. Due to LoRaWAN's long-range and high energy-efficient characteristics, it is becoming a popular choice for wireless smart devices manufacturer. Academic institutions and researchers have researched on the problem related to LoRaWAN network's signal strength, transferring protocol optimization and energy constraints, but it opens the door for security issues. In this research as a first part, it performs the security analysis on selective attack types, as an example it is focused on energy exhaustion type attack, selective device-based Denial-of-Service attack, middleman attack (related to message modification), Brute-force attack.

As a second objective of this research, it discussed about the existing LoRaWAN security techniques and countermeasures and how they can be used to prevent the attacks or minimize the impact of attacks. As an example, it focused on existing security features like mutual authentication, counter management, key management, and message integrity checking techniques.

Develop a vulnerability testing framework is the third and key objective of this research. This is a software defined framework, and it can be executed on established LoRaWAN network for identifying major security vulnerabilities. According to this research, this framework is designed as a proof-of-concept, so this framework is only supported to identify selected set of security vulnerabilities.

References

[1] Ismail Butun, Patrik Österberg, and Houbing Song. Security of the internet of things: Vulnerabilities, attacks, and countermeasures. *IEEE Communications Surveys & Tutorials*, 22(1):616–644, 2019.

[2] SeungJae Na, DongYeop Hwang, WoonSeob Shin, and Ki-Hyung Kim. Scenario and countermeasure for replay attack using join request messages in lorawan. In *2017 international conference on information networking (ICOIN)*, pages 718–720. IEEE, 2017.

[3] John Thomas, Season Cherian, Saranya Chandran, and Vipin Pavithran. Man in the middle attack mitigation in lorawan. In *2020 International Conference on Inventive Computation Technologies (ICICT)*, pages 353–358. IEEE, 2020.

[4] Xueying Yang, Evgenios Karampatzakis, Christian Doerr, and Fernando Kuipers. Security vulnerabilities in lorawan. In *2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)*, pages 129–140. IEEE, 2018.