Risk management in the Age of IoT and Lorawan

Ryan Mounir
2144
Portal of Libyan International Medical University
Faculty of Information Technology
Department of Computer Network

Introduction

The Internet of Things is a hot topic with various use cases, which are usually prefixed by the term smart, like smart home, smart city, and smart farming.
Wireless transmission protocols that suit this long range requirement for IoT applications are grouped by the term low power wide area network (LPWAN), covering several network protocols from different vendors, for example, LoRaWAN, SigFox, NB-IoT, LTE-M [1]. Compared to more traditional wireless network protocols like Wi-Fi, LPWAN protocols allow for a much higher transmission distance between devices, up to several kilometers, as well as having a low power consumption [2].

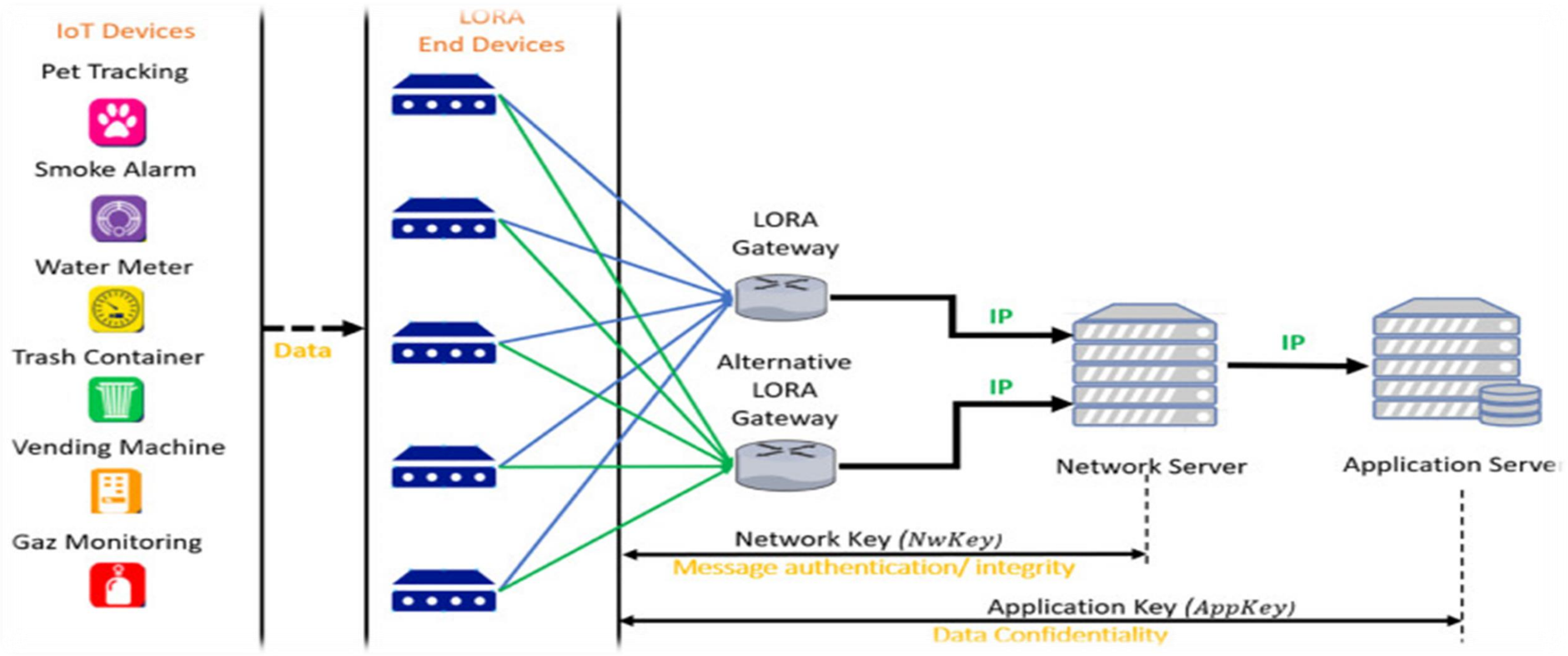

Figure 1: LoRaWAN Topology and encryptions keys[9]

problem statement

The massive growth of the Internet of Things (IoT) has increased facing the number of risks security organizations and increased the risks of network (lpwan) penetration by taking advantage of Lorawan vulnerabilities which represent the most important technology in the Internet of Things, so we need management and solutions to this problems and threats that can threaten institutions and individuals.

research questions

Q1.How can reduce the impact of attacks in iot?
Q2. Which mitigations against the known vulnerabilities should be considered when developing a LoRaWAN-based IoT solution?

Aims and objectives

1.Developing the security of the Internet of things.

2.locating Iot vulnerabilities and risks and determining what measures can be taken for improvement and management..

3.Seek solutions that can improve LoRaWAN security based on the IOT risk management requirements.

4.Study and understanding the security features present in LoRaWAN.

Literature Review

Multiple papers have investigated the security aspects of LoRaWAN and have shown that, while LoRaWAN is a promising technology, it bears multiple issues independent of the application domain. The works by Yang et al [3] and Butun [4] are the most prominent works in this category, while the work of Noura [5] is the most recent survey that covers multiple vulnerabilities we have detected in our literature review. The result of our literature study shows that the newer the LoRaWAN 1.0 version, the fewer attacks are known. But also, the newest 1.0 release (v1.0.4) has more known vulnerabilities compared to v1.1 .
Miller [6] provides a brief overview of LoRaWAN security and outlines how to configure the security features in the protocol to set up a LoRaWAN. The researcher describes the location of the key material in a LoRaWAN setup, and alerts that flaws in key management could compromise a backend.
The work does however not analyze the protocol nor evaluates the security of message exchanges.
A notorious problem in protocol security is the insufficient use of randomness or nonces (“number used once”). Zulian et al. [7] Compare existing key management protocols for IoT, and propose to add proxy nodes that drive a reputation system to enhance the security mechanisms of LoRaWAN. Aras et al.

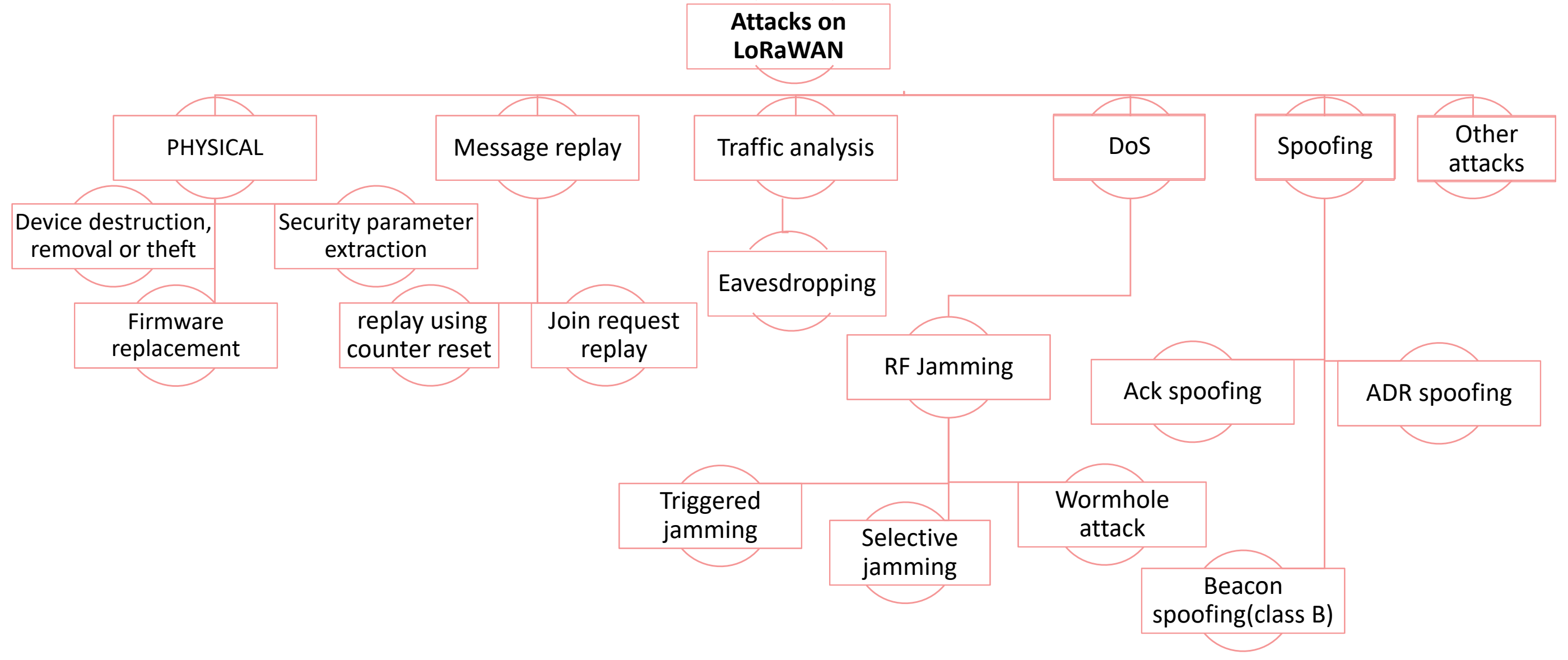

Figure.2 Attack Types of LoRaWAN Vulnerabilities

Methodology

In the research and study of controlling the risks of the Internet of Things, the method of secondary research will be used. Data collection will be done through the internet, reports, and research papers.

Results

1. Is to make people aware of the dangers of the wrong use of the Internet of Things, it will reduce these risks.
2. Periodic updating of IoT applications to correct gaps and defects.
3. As a suggestion, they can be use a third party notarized in the middle, can be used to encrypt the data and take part of the responsibility for the protection.
4. The ability to make the system more secure that can change all default settings will lead to reducing security.
5. At new versions and uses, Potential attacks such as DoS, spoofing can be mitigated by monitoring the amount of traffic sent from each client. A node capable of sending a much larger volume of traffic is identified as a potential fault and blocked.
6. The lack of device management such as the lack of security support on managing the update of devices, and the safe shutdown. There are no developers or programmers who monitor the safety and correctness of the work of devices and applications mainly, which can cause a crisis for users. Therefore, specialized companies or a private sector (third party) can be established to serve Users and follow-up with providers. In addition, that sector must develop plans to control attacks and risks in the event of one of them occurring, and take the necessary measures for crises.

Conclusion

Concluded that obtaining a world of the Internet of things completely free of risks is impossible, and that controlling these risks is difficult due to the expansion of this world and the diversity of services and different devices in it, but we can reduce and control these risks separately.

REFERENCES

[1] Salamai, Abdullah. (2021). Risk Management Techniques on the Internet of Things

[2] Soldatos, John (editor).2020. “Security Risk Management for the Internet of Things”

[3] Rana B, Singh Y, Singh PK. A systematic survey on internet of things: Energy efficiency and interoperability perspective. Transactions on Emerging Telecommunications Technologies. 2021 Aug;32(8):e4166.

[4] Yang, X., Karampatzakis, E., Doerr, C., & Kuipers, F. (2018). Security Vulnerabilities in LoRaWAN. In *2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)* IEEE . https://doi.org/10.1109/IoTDI.2018.00022

[5] Moraes, P.D., & Conceição, A.F. (2021). A Systematic Review of Security in the LoRaWAN Network Protocol. *ArXiv, abs/2105.00384*.

[6] LoRa Technology. Semtech Inc. Available online: http://www.semtech.com/wirelessrf/internet-of-things/what-is-lora / (accessed on 22 August 2018).

[7] LoRaWAN 1.1 Specification. Lora Alliance. 2017. Available online: http://loraalliance.org/lorawan-fordevelopers (accessed on 22 August 2018)

[8] Osorio, A. *et al*. (1970) *Routing in Lorawan: Overview and challenges: Semantic scholar, undefined*. Available at: https://www.semanticscholar.org/paper/Routing-in-LoRaWAN%3A-Overview-and-Challenges-Osorio-Calle/174df9014c9f0cfa8814f9082c2ea7df338fb46a.
[9] Mar 5 2020.Hassan Noura and others published .*Towards Securing LoRaWAN ABP Communication System*