Taxonomy of Attacks on LoRaWAN Devices

Kieran Scanlon, Felipe Trinidad Pilier, Armando Flores Munos, Delray Frierson

I. Problem Background

LoRaWan is a Media Access Control Layer Protocol that is used for long-range low-power communication released in 2015. And is separated between three modes of operation class A,B and C. Since its conception and implementation, it has seen many attempts at exploitation. According to Statistica [19], there are more than 470 million LoRa devices implemented in the Internet of Things. This number is expected to grow to 730 million by the end of this year. This leaves the infrastructure a particular area of interest to threat actors. Here, we want to discuss the different types of attacks on these devices. To do this, we must have an outline and description of the types of attacks and the LoRaWan Devices that these attacks are deployed against. Given that LoRa Wan is a protocol, the number of types of devices ranges in the hundreds and would extend the length of this paper exponentially. These devices are usually regulated by infrastructure and monitoring tools. Weather monitoring and smart water meters. For example, in the case of Smart water meters, these devices are susceptible to, Physical Tampering, Wireless Interception and Eavesdropping, Denial of Service (DoS) Attacks, Man-in-the-Middle (MITM) Attacks, Firmware Tampering, Replay Attacks, and Spoofing Attacks. These different devices will have overlap in the attacks that are deployed against them. In Figure 1, these are categorized, and we will discuss most of these different attacks and the danger they impose on some of these devices.

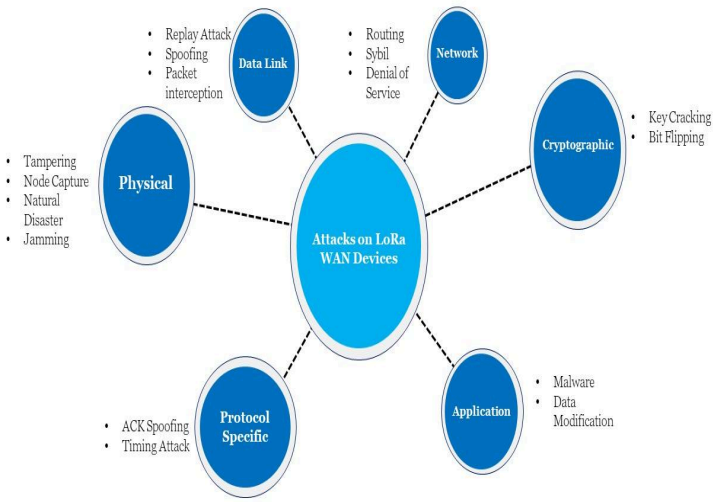

Figure: 1 LoRa Device attack types

II. Physical Attacks on LoRa Devices

LoRa devices offer an advantage compared to other forms of long-range wireless connection, such as 5G and LTE by resolving the encumbering issue of battery consumption. Low power wide area networks are versatile in usability. For example, health-related tests such as temperature, blood pressure, and weight can be sent in small packets and sent to healthcare centers. In this section, we will be discussing vulnerabilities within the physical layer of LoRa devices.

One of the major security issues with LoRa devices is its susceptibility to eavesdropping. Sniffing, the process of monitoring and collecting data packets, is possible with a single LoRa modem. This is due to a smaller number of receivers being needed to intercept communication. This puts Low-power WAN devices at a detrimental disadvantage in comparison to other wireless communication methods. The packets sent from a device are not encrypted and an attacker can intercept these messages. Low-power WAN technology very typically uses symmetric encryption when cryptography is applied. The AppKey is directly integrated into the program's code. An attacker may be able to extract the private key through the use of a firmware dump. Due to the nature of the method, the private key can be obtained under the radar to decrypt any sensitive data.

LoRa devices, like any other IoT system, contain vulnerabilities in their different components. These components include the hardware itself, the operating system, as well as leaving room for human error. In particular, hardware vulnerabilities are difficult to detect because of the many possibilities there are. A component could be damaged or corrupted or could be incompatible with another component. According to "Security Vulnerabilities in LPWANs," LoRa technology uses end-to-end security using network and application keys. An attack to bypass this may be through the use of an external device. If a flash drive with malware were installed onto the device, the payload, if developed correctly, can extract the symmetric key.

LPWAN devices are used to gather a plethora of information in different fields. Earlier, we gave an example of its potential use in the medical field. They have also provided a helping hand in the agriculture setting. As per a press

release, ICT International and Definium have implemented a set of LoRa-enabled sensors across a large avocado farm in New South Wales, Australia. The goal is to pinpoint the ongoing factors contributing to low crop yield. By utilizing soil moisture sensors, sap flow sensors, vapor-pressure deficit sensors, and weather stations, the collected data precisely identified instances of low soil moisture and elevated plant water stress, correlating them with increased fruit drop. LoRa devices prove beneficial in smart agriculture applications, providing farmers and ranchers with advantages such as extensive network coverage, reaching up to 30 miles from a single LoRaWAN gateway in rural areas. In a field of work where there could be many non-visible influences, LoRa devices have the ability to give exact answers to broad inquiries. However, especially in nature-based settings, they are vulnerable to natural threats from harsh weather conditions. Natural threats encompass earthquakes, energy vulnerabilities, hurricanes, floods, and fires, all posing significant risks to computer systems. While security measures can be put in place to mitigate the impact of these threats, preventing them entirely is challenging. To be effectively ready for potential damages, implementing a loss-expectancy plan can prove valuable.

Lastly, we would like to discuss the susceptibility to jamming. Jamming is a notorious denial-of-service attack that blocks a wireless channel with a powerful RF signal. In wireless communication, a jammer emits signals that overpower or interfere with the normal communication signals, causing disruption. This interference can take various forms, including continuous wave signals, noise, or signals that mimic legitimate communication but with the intent to disrupt. It can be used against specific devices. LoRaWAN operates in unlicensed frequency bands, making it easier for attackers to access and interfere with the communication. Additionally, being a low-power system inherently makes the system weaker, allowing it to be more vulnerable to jamming attacks as it may lack the power to counteract strong interference. To mitigate jamming attacks, LoRaWANs can implement an intrusion detection system to identify jamming attempts.

III. Attacks Against LoRa Software

Since LoRa devices can operate on low power and communicate long distances, they have become a standard in many industries. However, LoRa devices are so widespread and cheap that companies are only sometimes inclined to incorporate security into their LoRa devices. This lack of protection leaves many LoRa devices vulnerable to outside threats. In this section, we will review some of the different types of application and protocol attacks LoRa devices can face when unprotected.

In 2018, a report was released by researchers in the Netherlands about a DDoS being found in the ABP mode of LoRaWAN devices. The researchers found that the FRMPayload protocol in version 1.0 of LoRa could overflow, allowing a packet request to be sent repeatedly. After the counter overflow, the system stopped functioning as it kept trying to send the request, resulting in a DDoS exploit. The session keys will remain the same until they have been updated manually or a firmware update happens. This DDoS exploit is just one problem LoRa devices face, and another is when the message can be captured by a threat actor, such as in Ack Spoofing.

One change LoRaWAN made to save on the battery life of LoRa devices was the creation of the acknowledgment mechanism. This mechanism change was introduced to reduce the time it took for radios to power up. However, this change also brought along a critical flaw, and it was discovered by Xueying Yang, Evgenios Karampatzakis, Christian Doerr, and Fernando Kuiper. These researchers found that the ACK messages do not know which devices they send confirmation messages to. When the confirmation message can not reach its desired endpoint, it will repeatedly send the confirmation request. The attacker can then intercept this request, effectively hijacking the confirmation.

It is worth noting what class these attacks take place on since they work slightly differently depending on your target class. The most common setups use LoRaWAN class A mode, which specifies that the download traffic has to follow the uplink. Class B, on the other hand, reduces the needed power by telling the end devices to wake up periodically to check for any incoming messages. The duration for how long these devices stay awake is determined by a beacon broadcast message consisting of the PHY layer header followed by a beacon payload. With the information that is known, an attacker can drain the battery life of the LoRa device over time by sending crafted frames with extreme wake-up time. An attacker can also extract the position of the LoRa device since the GPS coordinates are in the information description of the GwSpecific field.

Security tools for LoRa devices only come out sometimes, and when they do, they are few and far between each other. New frameworks such as LAF (LoRaWAN Auditing Framework) and ChirpOTLE are being made to try and deal with some of the problems LoRa devices face when dealing with attackers. However, these new tools and frameworks still have their limitations as they are still in testing. For example, LAF can only listen for uplink packets. Another example of framework limitation can be found in ChirpOTLE, as it can only operate on a select few channels. Still, even with these limitations, new tools and frameworks are being developed to secure LoRa devices better.

IV. Application and protocol specific attacks

Application and software have a number of vulnerabilities that can be exploited. Since LoRaWAN devices are apart of the IOT infrastructure this is no exception. This makes it particularly susceptible to Malware, specifically code injection attacks. Unsecure software, Debug ports and unreviewed insecure code are all particular pain points for these devices. For example, LoRaWAN Gateways allow for firmware updates and support physical interface for connection. If properly done an attacker can exploit this device and inject code. According to [20] LoRaWAN devices are vulnerable to

DevEUI, JoinEUI, and Home_NetID. DevEUI identifies end devices for LoRaWAN and can be exploited during the OTAA procedure as a join request message is sent to the designated network. Considering the message hijacking can occur and malicious code can be injected/ exfiltrated through the header field of the frame. Receiving the message the instructions are executed separately from the device's CPU evading antivirus software. Join EUI identifies the Join server and Like the DevEUI the header field can be exploited via code injection. Attackers will use code injection in the DevEUI and JoinEUI header fields to produce a better nesting quality. And finally the Home_NetID uses the header field sent by the server and acts upon the end device. This similarly affects the Join-accept message since it's not encrypted.

V. CRC and MIC in LoRaWAN Devices

Integrity checking the payload of a packet is important during the transmission. A big factor in specific class attacks carried out by an adversary is frame modification. A frame modification is when an attacker is looking to attempt with the originators packet in order to battery exhaust or location spoof. A beacon is a packet with a payload that is sent out to the devices by the network operator for management services. A MIC is used in order to integrity check through the use of cryptography value checking of the MAC payload. Another integrity checking mechanism is CRC in the physical layer. message authentication code on Universal hashing is a standard for MIC. UMAC is a secretive selection process of a hash function from a list. That digest is then encrypted to hide the hash function. There are some attacks like Bit flipping that are detected by CRC but there are a wide range of Class attacks that can be detected through the use of Mac layer MIC. The bit flipping attack is carried from the network server to the application server. Being able to distinguish when an attacker is able to eavesdrop during the transmission of data is extremely important. The most effective way to distinguish integrity is through MIC or CRC at different layers. A big contribution to the lack of the implementation of a MIC is the public key infrastructure cost. When implementing an IoT system the devices are very small and cost effective to implement in a wide range of land. The cost of implementation of a public key infrastructure to use in an MIC is a factor in risk.

VI. Conclusion

With the rise of LoRAWAN devices being implemented there are more than 470 million LoRa devices implemented in the Internet of Things. This number is expected to grow to 730 million by the end of this year. . Security is a big concern and a risk when implementing them for the use in Health Care, Agriculture and Security equipment. LoRAWAN devices are separated between three modes of operation class A,B and C. Since its conception and implementation, it has seen many attempts at exploitation. This leaves the infrastructure a particular area of interest to threat actors. Throughout this paper we effectively discuss the different types of attacks on these devices. With Physical Tampering, Wireless Interception and Eavesdropping, Denial of Service (DoS) Attacks, Man-in-the-Middle (MITM) Attacks, Firmware Tampering, Replay Attacks, and Spoofing Attacks being our talking points. These different devices will have overlap in the attacks that are deployed against them. A very important implementation of LoRa devices is in smart agriculture applications, providing farmers and ranchers with advantages such as extensive network coverage, reaching up to 30 miles from a single LoRaWAN gateway in rural areas. With food shortages around the world effectively implementing LoRa devices will positively impact production of agricultural goods. Even though there are huge benefits to LoRA devices implementation, physically allocating them in rural regions and damage the device. Especially in nature-based settings, they are vulnerable to natural threats from harsh weather conditions. Natural threats encompass earthquakes, energy vulnerabilities, hurricanes, floods, and fires, all posing significant risks to computer systems. Jamming is a notorious denial-of-service attack that blocks a wireless channel with a powerful RF signal. In wireless communication, a jammer emits signals that overpower or interfere with the normal communication signals, causing disruption. This interference can take various forms, including continuous wave signals, noise, or signals that mimic legitimate communication but with the intent to disrupt. With the vulnerabilities mentioned throughout our paper the taxonomy is portrayed and concerning. The attack surface at large there is a big security concern. With bug bounty programs allowing ethical hackers to attempt to ethically penetration test an IoT device. Security in depth, physical security controls, encryption, and integrity implementation is needed to improve the security posture.

References

[1] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] https://www.mdpi.com/1424-8220/22/9/3127

[4] https://www.trendmicro.com/en_no/research/21/a/Low-Powered-but-High-Risk-Evaluating-Possible-Attacks-on-LoRaWAN-Devices.html

[5] https://www.cyber-threat-intelligence.com/publications/IoTDI2018-LoraWAN.pdf

[6] https://www.sciencedirect.com/science/article/abs/pii/S2542660520301359

[7] https://dl.acm.org/doi/10.1145/3561973

[8] Torres, Nuno, et al. “Security Vulnerabilities in LPWANs—An Attack Vector Analysis for the IoT Ecosystem.” Applied Sciences, vol. 11, no. 7, Apr. 2021, p. 3176. Crossref, https://doi.org/10.3390/app11073176. https://www.mdpi.com/2076-3417/11/7/3176

[9] "Semtech: LoRa Devices Boosting Crop Yield on Connected Avocado Farms." Professional Services Close-Up, 19 Sept. 2020, p. NA. Gale Business:Insights,link.gale.com/apps/doc/A635879345/GBIB?u=nysl_me_fordham&sid=bookmark-GBIB&xid=3c27d0c6

[10] Torres, Nuno & Pinto, Pedro & Lopes, Sérgio. (2021). Security Vulnerabilities in LPWANs—An Attack Vector Analysis for the IoT Ecosystem. Applied Sciences. 11. 3176. 10.3390/app11073176.

[11] Kovacs, Eduard. “Millions of Devices Using Lorawan Exposed to Hacker Attacks.” SecurityWeek, 28 Jan. 2020, www.securityweek.com/millions-devices-using-lorawan-exposed-hacker-attacks/

[12] X. Yang, E. Karampatzakis, C. Doerr and F. Kuipers, "Security Vulnerabilities in LoRaWAN," 2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI), Orlando, FL, USA, 2018, pp. 129-140, doi: 10.1109/IoTDI.2018.00022. https://ieeexplore.ieee.org/abstract/document/8366983

[13] E. Aras, G. S. Ramachandran, P. Lawrence and D. Hughes, "Exploring sthe Security Vulnerabilities of LoRa," 2017 3rd IEEE International Conference on Cybernetics (CYBCONF), Exeter, UK, 2017, pp. 1-6, doi: 10.1109/CYBConf.2017.7985777. https://ieeexplore.ieee.org/abstract/document/7985777

[14] Basu, Debraj, et al. “Security Issues of Low Power Wide Area Networks in the Context of Lora Networks.” arXiv.Org, 30 June 2020, arxiv.org/abs/2006.16554

[15] Jiang, Xingbin, et al. “An Experimental Analysis of Security Vulnerabilities in Industrial IOT Devices.” ACM Transactions on Internet Technology, 1 May 2020, https://dl.acm.org/doi/abs/10.1145/3379542

[16] Adefemi Alimi, Kuburat Oyeranti, et al. “A Survey on the Security of Low Power Wide Area Networks: Threats, Challenges, and Potential Solutions.” *Sensors*, vol. 20, no. 20, Oct. 2020, p. 5800. *Crossref*, https://doi.org/10.3390/s20205800.

[17] K. C. Wiklundh, "Understanding the IoT technology LoRa and its interference vulnerability," *2019 International Symposium on Electromagnetic Compatibility - EMC EUROPE*, Barcelona, Spain, 2019, pp. 533-538, doi: 10.1109/EMCEurope.2019.8871966.

[18] Physical Attacks Mentioned: Key Extraction, Eavesdropping, Human Error, Natural Threat, Jamming

[19] Taylor, Petroc. “Lpwan Connections by Technology 2017-2023.” *Statista*, 18 Jan. 2023, www.statista.com/statistics/880822/lpwan-ic-market-share-by-technology/

[20] Noman, Haitham Ameen, and Osama M F Abu-Sharkh. “Code Injection Attacks in Wireless-Based Internet of Things (IOT): A Comprehensive Review and Practical Implementations.” *Sensors (Basel, Switzerland)*, U.S. National Library of Medicine, 30 June 2023, www.ncbi.nlm.nih.gov/pmc/articles/PMC10346793/.

---------- **********----------