Exploring The Security Vulnerabilities of LoRa

Emekcan Aras, Gowri Sankar Ramachandran, Piers Lawrence and Danny Hughes
iMinds-DistriNet, KU Leuven, 3001 Leuven, Belgium.

***Abstract*—Internet-of-Things (IoT) deployments increasingly incorporate long range communication technologies. To support this transition, wide area IoT deployments are employing LoRa as their communication technology of choice due to its low power consumption and long range. The security of LoRa networks and devices is currently being put to the test in the wild, and has already become a major challenge. New features and characteristics of LoRa technology also intorduce new vulnerabilities against security attacks. In this paper, we investigate potential security vulnerabilities in LoRa. In particular, we analyze the LoRa network stack and discuss the possible susceptibility of LoRa devices to different types of attacks using commercial-off-the-shelf hardware. Our analysis shows that the long range transmissions of LoRa are vulnerable to multiple security attacks.**

I. Introduction

Internet of Things (IoT) applications are widely adopted in the context of smart cities and industries. Communication is one of the key requirements for IoT applications. Contemporary applications in the IoT primarily use short range communication protocols such as Bluetooth, Wi-Fi or ZigBee. Although GSM technologies offer long range communication support, it comes at a cost of high resource overhead. Therefore, long range wireless technologies and low power wide area networks (LPWAN) were developed to fill the gap between short range protocols and GSM. LPWAN technologies minimise deployment complexity, while offering long coverages in the order of kilometers. LPWAN technologies such as LoRa and Sigfox are widely used for applications such as smart metering and factory monitoring. In such applications, it is important to ensure that the devices are not vulnerable to security attacks. With the advent of these technologies, each device has the capability to reach distances in the order of several kilometers. This significantly reduces costs by eliminating the need for the deployment of intermediate routing nodes.

LoRa is a proprietary radio modulation technology licensed by Semtech Corporation. LoRa provides long-range connectivity by using the chirp spread spectrum technique, and it operates at 868-900 MHz ISM bands. LoRaWAN MAC protocol specifies the regulations for LoRa and it defines both physical and data link standards for LoRa networking.

Telecom operators around the world are deploying LoRa gateways. Recently in South Korea [1], a nationwide deployment of LoRaWAN has been completed, covering approximately 99% of the population. Countries such as the Netherlands and Germany are also actively deploying LoRa networks. A recent report show that 1.5 million LoRa devices are currently using the network infrastructure throughout the Netherlands[1].

The maintenance and security of such networks has started to become a major hurdle. Securing LoRa end-devices is also a challenging task due to the limited resources and low-cost hardware. In order to ensure the dependability of future deployments of LoRa networks, security measures must be taken that will allow LoRa networks to cope with different types of attack. A detailed analysis exposing security threats for the LoRa technology are important in order to protect these vast number of devices which have recently started to effect daily life all over the world.

LoRaWAN [2] guarantees security for LoRa devices through symmetric-key cryptography. Despite the security features of LoRaWAN. LoRa devices are susceptible to security attacks. For instance, LoRa modulation requires between 900 milliseconds and 1.2 seconds for each LoRa transmission. This wide transmission window provides ample opportunities for attackers.

This paper studies the security vulnerabilities of LoRa and proves that LoRa transmissions are prone to jamming attacks. In addition, it presents a novel attack by combing the selective jamming with off-the-shelf hardware. Lastly, this paper discusses solutions to help the application developers to overcome such security attacks.

The remainder of this paper is organized as follows. Section II provides background information on low power, long range networking, security measures, and presents related work. Section III describes detailed security analysis of LoRa networks. Section IV presents possible weak points and attacks. Section V concludes the analysis and presents possible attacks against the LoRa technology.

II. Background

This section provides background on the key technology and main subject of this paper LoRa and LoRaWAN.

The LoRa Alliance technical workgroup defines both physical and data link standards for LoRa networking [2]. LoRa provides long-range connectivity by utilising a chirped spread spectrum technique with a wide bandwidth. Chirp Spread Spectrum (CSS) was developed for radar applications in the 1940's [3]. The chirp signal is used to spread the transmitted signal and it varies in frequency. CSS modulation schemes are known for low power consumption and robustness against channel degradation challenges such as interference and multi-path fading. This modulation scheme offers a range of data rates for different frequency ranges. In LoRa networks,

978-1-5386-2201-8/17/$31.00 ©2017 IEEE

the data rate is selected based on the range requirement, and there is a trade-off between data rate and communication range. LoRa technology has ability to demodulate several simultaneous signals at the same frequency by using different chirp rates due to their orthogonality. LoRa modulation defines six chirp rates which are called spreading factors, trading throughput for the on-air time. As demonstrated in [3] if a device needs a longer communication range, it uses higher spreading factor. At the highest spreading factor , the time on-air could range between 0.9 to 1.2 seconds, depending on payload length.

On top of LoRa, it is possible to utilise several different networking protocols and topologies (star, mesh, etc.) to support the Internet of Things. LoRaWAN [2] defines the network-layer architecture for LoRa-enabled systems, while the physical layer provides long range communication through LoRa modulation. LoRaWAN is star networking topology which uses gateway devices for receiving data from nodes and forwarding it onto LoRaWAN servers. It is specifically designed for low power networked embedded systems.

The LoRaWAN specification [2] defines the frequency bands for LoRa communication. In Europe, LoRa operates in the 433MHz and 868Mhz ISM frequency bands, while in the USA it operates in the 900MHz band. LoRa frequency bands are controlled by regulatory authorities. In Europe, the European Telecommunication Standards Institute (ETSI) imposes strict guidelines for the use of various frequency bands. According to ETSI regulations, each end-device should follow a duty cycle between 0.1% and 10% depending on the operational sub-band in Europe. In USA, the Federal Communications Commission (FCC) imposes duty-cycling differently: each end-device is restricted from using the operational sub-band for 400 milliseconds after each transmission.

III. Analysis

In this section the LoRa network stack is described and analyzed.

A. Physical Layer

As was mentioned in the previous section, the LoRa physical layer uses Chirp Spread Spectrum. This technique has been commonly used by the military and in secure communication applications. Recently it has started to be adopted by some communications applications due to its relatively low power requirements and robustness against channel degradation challenges such as interference and multi-path fading.

This modulation scheme offers a range of data rates on different frequency ranges. In LoRa networks, the data rate is selected based on range requirements, and there is a trade-off between data rate and communication range. From Table I, it is evident that the maximum range increases the energy consumption of the end-device, while reducing the data rate.

Figure 1 shows the time on air as a function of payload for each different spreading factors. In LoRaWAN, time on air defines the elapsed time on air for a LoRaWAN packet

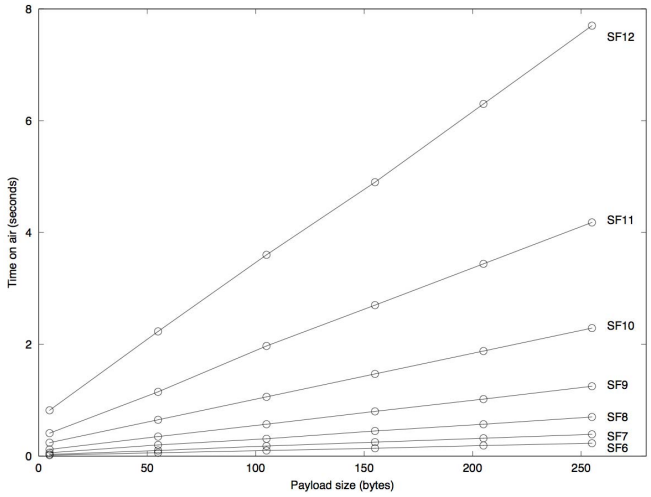

Figure 1: Time on Air of LoRa with code rate 4/5 and a 125 kHz bandwidth.

between end-device and gateway. Time on air for different configurations for each packet can be calculated using a formula provided in LoRaWAN specifications [2]. As can be seen from the Figure 1, low data rates lead to very long transmission times especially when compared with other wireless technologies such as IEEE 802.15.4 [4] and WiFi. In an IEEE 802.15.4 based network over the air time varies between 10-100 ms depending on the payload size [5]. In addition in a WiFi network, packet transmission time over the air is between 0.3 ms & 30 ms [6]. On the other hand, in a basic LoRa network, a device at the edge of the network must communicate with a high spreading factor(i.e. SF12), and can take around 0.9 to 1.5 seconds depending on payload size.

Longer than usual transmission times may be exploited to intercept packets on the air or even corrupt packets before they reach to the gateway. This creates opportunities to perform novel attacks on the LoRa physical layer.

B. LoRaWAN

LoRaWAN defines the networking protocol for LoRa based devices. It specifies different device types, different keys, and encryption capabilities to build a secure wireless network.

According to the LoRaWAN specifications, LoRa end-devices are classified into three different classes. Class A devices support bi-directional communication, in which each end-device has two short down-link receive windows after an up-link transmission. The end-device schedules the transmission slot according to its communication needs (on random time basis i.e. ALOHA-type). Class B end-devices also support bi-directional communication, but have additional receive windows, which are determined by time-synchronized beacons from the gateway. This allows the server to know when the end-device is listening. Finally, Class C devices allow continuous reception of data due to its maximal receive

slots. At the time of writing, only Class A end-devices are available in the market.

LoRaWAN specifies a number of identifiers for devices. All end-devices have a 64-bit unique identifier called Device Identifier (DevEUI) which is set by vendors or developers. In addition, all communication is done using 32 bit device address. Another identifier, called Application Identifier (AppEUI), uniquely identifies the application provider of the end-device.

The cryptographic security is handled using AES-128 operating in CTR mode [7], providing multiple layers of encryption in LoRaWAN. LoRaWAN uses separate device, network, and application keys to secure packets at the network and application level, respectively. This allows intermediate nodes such as gateways and cloud routers to perform routing and network maintenance tasks, while preserving the confidentiality of application data.

A 128-bit AES key known as the Application Key (Appkey) is used to generate two session keys which are called Network Session Key (NwkSKey) and Application Session Keys (AppSKey). The NwkSkey is shared by both the end-device and the network server to generate and verify the message integrity code (MIC). This ensures the integrity of messages, and creates a specific signature for every device. The AppSKey is similar to the NwkSkey, but it is used for encrypting and decrypting the payload of application data. LoRaWAN creates a key stream using NwkSKey, AppSKey, and the up-link or down-link counter of the messages. Therefore, each message is encrypted by using the XOR operation with the corresponding key from the key stream to generate the encrypted payload.

The LoRaWAN protocol ensures the security, and provides encryption capability between the end-device and the gateway. However, the payload length is always the same before and after the encryption. This can be used together with overflowing counters by a malicious entity to restore the key stream from the encrypted messages.

C. Join Procedures and Packet Structure

LoRaWAN defines two joining procedures for end-devices: OTAA and ABP. For an end-device to join a LoRaWAN network, one of the procedures should be followed. Over-the-Air Activation (OTAA) requires DevEUI, the AppEUI, and an AppKey. An end-device must follow this procedure every time it joins a new network or loses the session key information. OTAA is described as the most secure way to authenticate since a network session key ,specifically for that end-device, is generated each time the device joins the network. This allows roaming between networks of different providers. In addition, having two keys makes tampering with or reading application data harder, even if one of the keys are compromised. The end-device initiates the OTAA procedure by a sending join-request message. The message includes the AppEUI, DevEUI, and nonce (DevNonce) of the end device. The DevNonce is a random value which is tracked by the network server and used to reject any join request with an invalid nonce value. This mechanism prevents replay attacks.

The second joining procedure is Activation by Personalization (ABP). This procedure directly connects end-devices to the specified network without initiating a join-request and accept procedure. The device address (DevAddr), NwkSKey, and AppSKey are directly defined and stored in the end-device. Therefore, it does not generate any keys and can directly encrypt messages using these keys. If the keys are compromised, all communication between the device, gateway, and network server can be decrypted by third party entities for the lifetime of the device.

After the join procedure, the end-device starts to send messages to gateways by following the LoRaWAN protocol. There are two types of messages: up-link and down-link message types. Up-link messages are sent by end-devices passing through gateways to the network server. Up-link messages must include a preamble, the physical layer header, header CRC and a physical layer payload and including its own CRC at the end of the message to protect the integrity of entire packet. The physical layer payload is formed by MAC layer headers, frame headers, payload, and message integrity code. The structure of a LoRa packet is shown in Figure 2.

Vulnerability of ABP: One of the potential vulnerability is using ABP for joining, but deriving these keys from publicly available information. This could be worked out through reverse engineering of one device, then all other communications to any device would then be compromised. Therefore, a unique set of NwkSkey and AppSKey must be derived for each device to protect the communication of other devices. In addition, LoRaWAN packet structure does not include any time based data or signature to validate the time of the message, and this might create a vulnerability to perform replay or/and wormhole attacks on LoRaWAN networks.

Table I: Data rate supported by LoRaWAN

Data rate	Spreading Factor	Bandwidth(In kHz)	Radio bit rate(Bytes/sec)	Range/Energy Consumption
0	SF12	125	31	Longest / Highest
1	SF11	125	55	Longer / Higher
2	SF10	125	122	Long / High
3	SF9	125	220	Short / Small
4	SF8	125	390	Shorter / Smaller
5	SF7	125	683	Shortest / Smallest

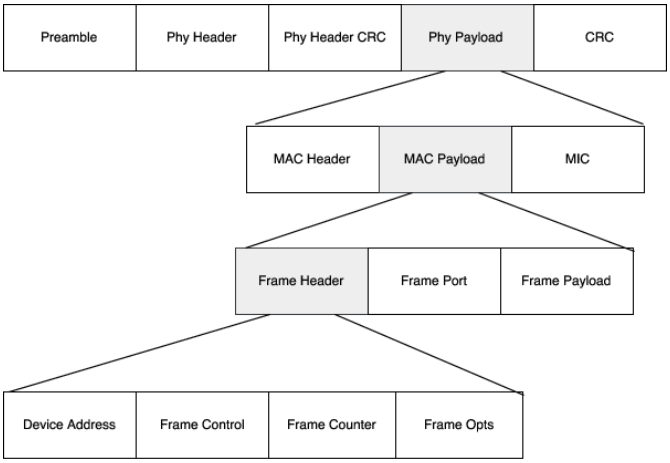

Figure 2: LoraWAN Packet Structure.

D. End devices and Gateways

A typical LoRa network consists of four different components: devices, gateways, a network server, and application service. The hardware setup of LoRa networks are similar to WiFi networks. Devices do not send messages to each other rather they send messages to LoRa gateways. Gateways usually have simple tasks. They scan the spectrum and receive LoRa packets from end-devices and forward their data to a network service which handles the packets if they are valid. The network server or service handles decryption of packets and other LoRaWAN features such as adjusting adaptive data rates. It then forwards to data to the application.

The end-device must have a LoRa transceiver chip which is designed and manufactured by the SemTech Corporation. Right now in the market, all products are based on the SemTech LoRa transceiver. For development purposes, there are integrated circuits with SPI communication and reconfigurable interrupt capabilities such as Semtech SX127x[8] series or with USB communication and easy installation capabilities such as MicroChip Rn2483[9]. Both products are based on Semtech products as explained before, but the RN2483 module provides a command set to configure and control the radio module. However, in all products in the market, firmware has to be developed for the end-device and as it was mentioned in earlier sections, security keys must be implemented by the developer in the firmware.

On the other hand, gateways form and important part of LoRa networks from the security perspective. In the market, many different gateways can be found with different specifications for different needs. Most of the gateway architecture is based on combination of a Semtech Lora Radio Concentrator and an embedded Linux computer such as Raspberry Pi, Beagle Bone and etc. The Radio concentrator has massive digital processing power and it is specifically designed to provide powerful gateway capabilities in the ISM bands. It is usually used with two LoRa transceivers and can listen and receive packets from different channels simultaneously. The gateway usually also runs a network server since it normally contains a powerful embedded computer. The gateway contains valuable information about end-devices and manages security keys for the network.

The gateway in LoRaWAN creates a single failure point for the network which could be used to disconnect hundreds of end-device from application. Moreover, physical access by malicious entities might lead to the security keys and other data to be compromised.Additionally, since the security keys are implemented in the firmware of LoRaWAN end-devices, the development of the firmware is quite important for the whole LoRa network to protect security keys from falling into the hands of malicious entities.

IV. Vulnerabilities and Attacks

We explain the security vulnerabilities and possible attacks in this section.

A. Compromising Device and Network Keys

LoRaWAN provides end-to-end security using application and network keys. However, an attacker with physical access may compromise the LoRa end-devices. If an attacker gains physical access to a device, he/she may extract the keys. Usually, end-devices contain a LoRa radio module and a host microcontroller unit (MCU). The radio module communicates with the host microcontroller via UART or SPI interface. Commands and data exchanges between the host and the radio module can be intercepted using external hardware. For instance, if UART interface is used between two ICs, a basic FTDI interface can be used to extract all the key exchanges. Contemporary radio modules on the market does not provide built-in encryption support to secure the interactions between the host microcontroller and radio module. In such cases, there is no way to understand that the commands sent to the radio module were issued by the host MCU or a malicious entity. Also a malicious entity could intercept all the data exchanges between the host MCU and the radio module and use this intercepted information to create a mock device with the same credentials or manipulate the data payload. Therefore, application developers must not perform sensitive operations such as setting security keys for each data transmissions as it may expose critical informations to malicious entities.

To prove the feasibility of this attack, the Xignal mousetrap [10] was used as a target device. The hardware unit was tampered to expose the UART serial lines between the MCU and the LoRa radio module. A regular FTDI chip was connected to the serial line to read intercept all the transactions between them. We noticed that whenever the mousetrap was reset, the host MCU issues commands to configure the network keys of the radio module. Using these keys and our custom LoRa device, we impersonated a LoRa mouse trap and sent data as if it were coming from the mouse trap. Following this attack we informed the Xignal engineers about the security vulnerability in their devices.

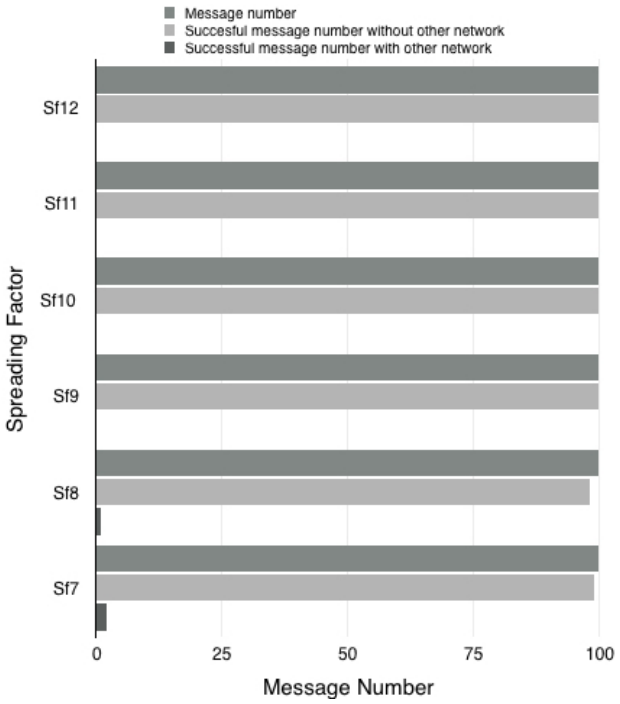

Figure 3: LoRaWAN COTS Jammer Success Rate

B. Jamming Techniques

Radio jamming is one of the serious problems for IoT deployments [11]. Malicious entities can transmit a powerful radio signal in the proximity of application devices, and disrupt the radio transmissions. Typically, such attacks require dedicated hardware, which minimises the possibility of jamming attacks in real-world devices. However, our experimentation reveals that it is possible to jam LoRa devices using commercial-off-the-self LoRa hardware.

CSS modulation is known for its robustness against interferences, but Brecht et al. [12] showed that LoRa devices suffer from coexistence issues. [12] shows that concurrent LoRa transmissions at same frequency and spreading factor can interfere with each other. This vulnerability in LoRa physical layer allows malicious entities or third parties to use commercial-off-the-shelf (COTS) LoRa devices to jam LoRa networks.

Most importantly, this attack requires just an Arduino platform with a LoRa radio module. Anyone with malicious intent can flood LoRa messages at a certain frequency to wipe out all the transmissions in that frequency, and our validation results in Figure 3 shows that roughly 99% of LoRa transmissions are affected by such a jamming approach. For this attack, we used an Arduino Leonardo [13] board and a Semtech LoRa radio module [8] breakout board. The total cost of such a device is around 30 euro. Therefore, it is easy to disrupt LoRa transmissions with a cheat COTS hardware platforms.

Although it is hard to prevent such an attack, there are workarounds to overcome this issue. Firstly, the jamming of the whole network or frequency can be easily detected since all the devices that communicate in that frequency would suddenly start to drop out from the network. By detecting such abnormal behaviours, network administrators can take appropriate action (for instance, by switching the operational frequency) to prevent the impact of jamming.

LoRa transmission on-air times vary from hundreds of milliseconds to 1.5 seconds, depending on the payload size and spreading factor. According to Vanhoef et al. [14], wireless transmissions of specific devices can be selectively selectively by using their device address. Once a jammer receives the initial bytes related with the device address, and if device address matches with the desired device address, a selective jammer could corrupt the rest of the message before it reaches the destination. Such an attack is already performed in WiFi networks [14]. Therefore, selective jamming of LoRa devices are possible using COTS hardware by extending our jammer with additional software to target a specific device address.

C. Replay Attacks

A replay attack is an attack on security protocol, re-sending or repeating the valid data transmission by the malicious entity. The main purpose of this attack is fooling the device or module by using handshake messages or old data from the network. In order to perform the attack in wireless networks, the entity should know the communication frequencies and channels to sniff data from transmission between devices.

In LoRaWAN, it is not possible to decrypt transmissions between end-devices and gateways without AppSKey, since the entire payload of the LoRaWAN message are encrypted by it. Additionally, since tampering with the data will make the MIC check fail, it is not possible to do it without NwkSKey. Although the malicious entity can resend the message consecutively, using frame counters which are defined in LoRaWAN specifications these messages or attacks can be detected and discarded. Once the end-device is activated, these counters are both set to 0 and each message coming from the gateway or the device increments counters. If a message is received with a lower frame counter than the last message, it is ignored. However, the LoRaWAN specification handling off frame counters is specifically left to the application and developer. Therefore, networks which do not track these frame counters could be vulnerable to replay attacks.

In addition, this security measure has consequences for development devices, which often use ABP activation to join networks. Each time the end-device is rebooted, it resets its frame counters to 0. Thus, if a malicious entity is able to reset the end-device, messages which were obtained before by sniffing the transmission between the end-device and gateway could be replayed back to the gateway. As it is described in [15] the effect of this particular attack depends on the application, but in the case of a LoRa based burglar alarm, it might be used to replay an alarm disable message while the actual end-device, in this case it is an burglar alarm, is sending alarm messages. On the other hand, networks such as The Things Network block all the messages coming from

the device until its frame counter reaches the frame counter stored in the gateway. However in this kind of application, if the end-device reboots itself because of its routine or to get rid of technical problems, it will be blocked for a certain amount of time.

D. Wormhole Attacks

As it was mentioned in earlier sections, characteristics of LoRa physical layer might be used to perform novel attacks. Our study shows that, end-devices in LoRaWAN network can be jammed by using off-the-shelf hardware. Together with replay attack, a wormhole attack[16] can be performed against LoRaWAN network. In this type of attack, one malicious device captures the packets from one device and transmits them to other distant located device to replay the captured packet. This can easily be launched by malicious entity without prior knowledge of the network or cryptographic mechanism.

In LoRaWAN network, a wormhole attack could be performed by using two type of device that are sniffer and jammer. The sniffer captures packets and, signals to the jammer to notify that it captured the packet. The captured packet never reaches to the gateway and, validation of captured message stays valid. The captured message can be replayed any time. Gateway and Network server forwards to the packet to the application layer. Therefore, the important alarm messages can be jammed and regular messages which are captured before and never reached to the gateway, could be sent to the gateway as if there is no alarm. Since there is no time-related information in LoRaWAN messages, it is hard to detect this attack in LoRaWAN networks.

V. Conclusion

In this paper, we provide an analysis of the LoRa network stack and introduced possible vulnerabilities. LoRa provides a far greater coverage than prior wireless sensor network technologies with low power consumption. Moreover, LoRa devices and networks are already deployed and widely used in some countries. That might indicate that LoRa is a very promising wireless network technology for IoT devices. On the other hand, providing long range communication, also cause very long transmission times in the networks that is not observed before in other wireless sensor network technologies. In addition, our results indicate that LoRa devices has coexisting problems with other LoRa networks and devices. Devices using lower spreading factors can corrupt signal from devices using higher spreading factor in the same network. Furthermore, most LoRaWAN security measures such as the key management and frame counters need to be implemented and taken care of by developers or manufacturers. Therefore, poor implementation also may put end-devices and gateways in danger. To sum up, our analysis and results shows that long range transmission of LoRa and LoRaWAN has serious security vulnerabilities that can be exploited by malicious third entities.

Acknowledgments

This research is partially funded by the Research Fund KU Leuven and the iMEC IoT research program. The work is conducted in the context of the HI^2-NETSEC Project.

References

[1] J. P. Tomás, "Operators in Korea, Netherlands deploy LoRa networks for IoT," 2016, available at http://www.rcrwireless.com/20160704/carriers/operators-korea-netherlands-deploy-lora-networks-iot-tag23.

[2] *LoRaWAN Specification*, LoRa Alliance, 2015, rev. 1.0.

[3] G. S. Ramachandran, F. Yang, P. Lawrence, S. Michiels, W. Joosen, and D. Hughes, "Micropnp-wan: Experiences with lora and its deployment in dr congo," in *COMSNETS edition:9*, 2017.

[4] *IEEE Standard for Low-Rate Wireless Networks*, IEEE Computer Society Std., 2015.

[5] J. Gutierrez, M. Naeve, E. Callaway, M. Bourgeois, V. Mitter, and B. Heile, "Ieee 802.15.4: a developing standard for low-power low-cost wireless personal area networks," in *IEEE Network*, ser. 5, vol. 15. IEEE, 2001.

[6] T. ElBatt, S. K. Goel, G. Holland, H. Krishnan, and J. Parikh, "Cooperative collision warning using dedicated short range wireless communications," in *Proceedings of the 3rd international workshop on Vehicular ad hoc networks*, 2006.

[7] S. Frankel, R. Glenn, and S. Kelly, "The aes-cbc cipher algorithm and its use with ipsec," Internet Requests for Comments, RFC Editor, RFC 3602, 2003.

[8] *SX1276/77/78/79 - 137 MHz to 1020 MHz Low Power Long Range Transceiver*, Semtech, 2015.

[9] *Low-Power Long Range LoRa Technology Transceiver Module*, MicroChip, 2015, rev. A.

[10] *Xignal Mousetrap*, 2016, avaliable at https://www.xignal.com/products/xignal-mousetrap.

[11] M. Labib, S. Ha, W. Saad, and J. H. Reed, "A colonel blotto game for anti-jamming in the internet of things," in *Global Communications Conference (GLOBECOM)*, 2015.

[12] B. Reynders, W. Meert, and S. Pollin, "Range and coexistence analysis of long range unlicensed communication," in *International Conference on Telecommunications*, 2016.

[13] *Arduino Leonardo*, Arduino, 2017, available at https://www.arduino.cc/en/Main/ArduinoBoardLeonardo.

[14] M. Vanhoef and F. Piessens, "Advanced wi-fi attacks using commodity hardware," in *ACSAC '14 Proceedings of the 30th Annual Computer Security Applications Conference*, 2014.

[15] R. Miller, "Lora security: Building a secure lora solution," MWR Labs, RFC, 2016. [Online]. Available: https://labs.mwrinfosecurity.com/assets/BlogFiles/mwri-LoRa-security-guide-1.2-2016-03-22.pdf

[16] Y.-C. Hu, A. Perrig, and D. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in *22nd Annual Joint Conference of the IEEE Computer and Communications*, 2003.