Energy Attack in LoRaWAN: Experimental Validation

Konstantin Mikhaylov
University of Oulu, Oulu, Finland
Brno University of Technology, Brno, Czech Republic
konstantin.mikhaylov@oulu.fi

Radek Fujdiak
Brno University of Technology, Brno, Czech Republic
Technical University of Ostrava, Ostrava, Czech Republic
fujdiak@feec.vutbr.cz

Ari Pouttu
University of Oulu
Oulu, Finland
ari.pouttu@oulu.fi

Voznak Miroslav
Technical University of Ostrava
Ostrava, Czech Republic
Miroslav.voznak@vsb.cz

Lukas Malina
Brno University of Technology
Brno, Czech Republic
malina@feec.vutbr.cz

Petr Mlynek
Brno University of Technology
Brno, Czech Republic
mlynek@feec.vutbr.cz

ABSTRACT

Myriads of new devices take their places around us every single day, making a decisive step towards bringing the concept of the Internet of Things (IoT) in reality. The Low Power Wide Area Networks (LPWANs) are today considered to be one of the most perspective connectivity enablers for the resource and traffic limited IoT. In this paper, we focus on one of the most widely used LPWAN technologies, named LoRaWAN. Departing from the traditional data-focused security attacks, in this study we investigate the robustness of LoRaWAN against energy (depletion) attacks. For many IoT devices, the energy is a limited and very valuable resource, and thus in the near future the device's energy may become the target of an intentional attack. Therefore, in the paper, we first define and discuss the possible energy attack vectors, and then experimentally validate the feasibility of an energy attack over one of these vectors. Our results decisively show that energy attacks in LoRaWAN are possible and may cause the affected device to lose a substantial amount of energy. Specifically, depending on the device's SF (Spreading Factor), the demonstrated attack increased the total energy consumption during a single communication event 36% to 576%. Importantly, the shown attack does not require the attacker to have any keys or other confidential data and can be carried against any LoRaWAN device. The presented results emphasize the importance of energy security for LPWANs in particular, and IoT in general.

CCS CONCEPTS

• **Computer systems organization → Embedded systems**; *Redundancy*; Robotics; • **Security and privacy → Mobile and wireless security**; • **Networks** → Network reliability.

KEYWORDS

IoT, Security, LPWAN, LoRaWAN, LoRa, Energy Attack, Experiment

ARES '19, August 26–29, 2019, Canterbury, United Kingdom

ACM ISBN 978-1-4503-7164-3/19/08…$15.00
https://doi.org/10.1145/3339252.3340525

ACM Reference Format:
Konstantin Mikhaylov, Radek Fujdiak, Ari Pouttu, Voznak Miroslav, Lukas Malina, and Petr Mlynek. 2019. Energy Attack in LoRaWAN: Experimental Validation. In *Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES 2019) (ARES '19), August 26–29, 2019, Canterbury, United Kingdom.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3339252.3340525

1 INTRODUCTION

Today the formation of the Internet of Things (IoT) is actively ongoing, with myriads connected devices taking their place all around us. The statistical reports [12] estimate the number of active IoT devices to exceed 8 billion already today and expect the further increase of their number to over 16 billion by 2025.

Owing to the diversity of the IoT use cases and their specific requirements, the poll of IoT-enabling technologies is very sheer. The current status of the IoT connectivity landscape [2] illustrates this fact. Dozens of wireless communication technologies, ranging from ultra-short-range to terrestrial, are currently on the market.

Of all these versatile technology options, the ones which can jointly be addressed as the Low Power Wide Area Networks (LPWANs) [18] are expected to play the key role in the further development of the massive IoT applications [12]. The conventional LPWANs are characterized by a combination of:

- the low cost of individual devices,
- the low energy consumption,
- the long ranges of communication, and
- the good scalability,

subject to very limited data traffic of each device. To address these goals, the LPWANs are often built in star-of-the-stars network topology, similar to the cellular networks. Also, in an attempt to reduce the costs some of the LPWANs operate in non-licensed frequency bands, typically using the bands below one GHz, to achieve good communication range. Finally, to minimize their energy consumption, the LPWANs often restrict the complexity of their protocols and minimize the signaling. Albeit all these contribute towards improving the performance, as the results the security of the respective solutions might get compromised, and the new kinds of attacks may become possible.

Specifically, in this paper, we focus on the most widely used as of today LPWAN technology [21] named LoRaWAN. Given that a great share of IoT devices is powered by batteries or energy harvesting, the energy is a very important resource for LPWANs. Therefore, in what follows using the real-life experiments we investigate the possibility of launching an energy attack, i.e., the attack aimed at making a device deplete its energy - energy depletion attack (EDA).

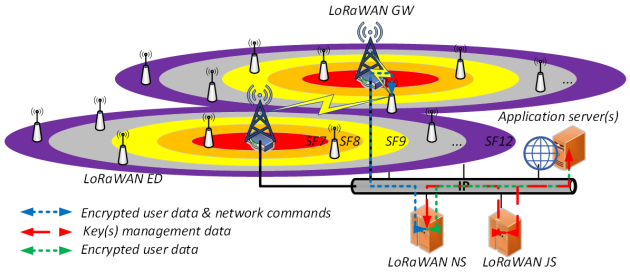

Figure 1: Typical LoRaWAN structure (specification 1.1).

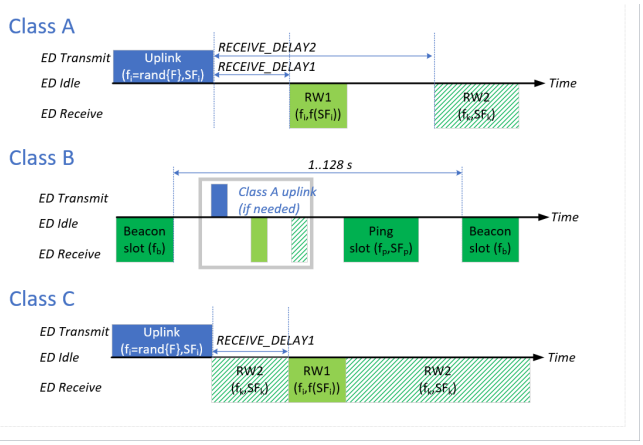

Figure 2: LoRaWAN End-device (ED) classes.

To the best of our knowledge, such types of attacks have not been studied neither theoretically, nor with a practical test bed, yet in the context of LPWAN and LoRaWAN in particular. The most similar work is a survey from Nguyen et al. [16], which defines and puts together high-level theory for energy depletion attacks. Meanwhile, our results decisively show not only the potential possibility of such attacks but also characterize the possible damage (i.e., the energy losses), which can be caused by these. Finally, we also speculate on the potential countermeasures against such attacks. These form the major contributions of the paper.

The structure of the paper is as follows. Section 2 briefly overviews the key aspects of LoRaWAN technology. Section 3 provides a digest of the related works. Section 4 discusses the possibility and potential vectors for energy attacks in LoRaWAN. In Section 5 we detail our experimental setup and present the results of our practical evaluation. Finally, Section 6 summarizes and discusses the obtained results, and lists some of the potential countermeasures for mitigating energy attacks.

2 LORAWAN TECHNOLOGY

The LoRaWAN technical solution is composed of two major components. The former one is the proprietary modulation-coding scheme named LoRa, which is a variation of a chirp-sequence spread spectrum technique, in which the information is encoded into the frequency shift of the beginning of the chirp for each new symbol [24]. By changing the bandwidth, the transmit power and the spreading factor (SF), which denotes the proportion between the data bytes and the radio symbols, the different tradeoffs between the on-air time (linearly related to energy consumption) and the maximum communication range become possible.

The LoRaWAN specification [10] is the second key component of the LoRaWAN solution. The specification defines the link and network layers on top of the LoRa physical layer, and specifies all the key mechanisms. In what follows we briefly discuss them.

The network layer. The structure of a LoRaWAN network is illustrated in Figure 1. The network is built as star-of-stars, having the network server (NS) managing the network in its core. One or several gateways (GW) are connected to the NS, listening to the radio channels and streaming all the legitimate LoRaWAN radio packets received from the end devices (EDs) to the NS over an internet protocol (IP) based connection. The NS manages all the received data (e.g., removes the duplicates received via different GWs) and provides access to these data for the dedicated application servers. Also, the NS may provide to GWs the data to be transmitted to EDs in the downlink. The special join server (JS) might be used to manage the encryption keys and ED connection.

The link layer. A LoRaWAN ED may belong to one of the three classes: A, B or C. The devices of class A may send their data to the NS at any moment of time, given that they obey the duty cycle restrictions imposed by the local radio frequency use regulations. For its uplink transmission, the ED randomly selects one of the frequency channels listened by the GW. At the dedicated times following the end of uplink transmission, the ED is required to open the receive windows (RWs) - RW1 and RW2. RW1 is opened at the same frequency channel, which has been used for uplink transmission and using the SF, which is dependent on the SF used in the uplink. RW2 is opened on a pre-specified frequency channel and SF, common for all EDs in the network. This procedure is illustrated in Figure 2. The class B EDs upkeep the synchronization with the network by listening to the beacons, and open additional RWs for the poll messages of GWs. Finally, class C EDs stay in receive (using RW2 parameters) all the time they do not transmit or receive in RW1. The functionality of class A is obligatory for all LoRaWAN EDs, and these devices are the most common in LoRaWANs. For these reasons in what follows we imply EDs to be class A unless stated otherwise.

Other notable mechanisms. In addition to the ones discussed above, the LoRaWAN solution has several other notable mechanisms:

- For connecting an ED to the network, LoRaWAN defines two procedures, namely the activation by personalization (ABP) and the over-the-air activation (OTAA). The former implies that all the relevant keys and configurations are delivered to an ED offline. The latter enables to generate all the relevant LoRaWAN key online in the process of device connection.

- The adaptive data rate (ADR) mechanism enables effective use of the available resources by the EDs by allowing NS to assign the optimal transmit power and SF to each particular ED.
- The NS may also request an ED to limit its duty cycle to reduce collisions in the network.
- A LoRaWAN ED may send a special link check request, in response to which the NS should give an estimate of the current radio channel condition.
- A LoRaWAN ED may request an acknowledgment for its uplink transmission. In this case, the NS should attempt to provide an acknowledgment, subject to the available resources, in one of the RWs.
- The LoRaWAN does not implement handover. As this is illustrated in Figure 1, if several GWs overhear the ED's transmission - they all forward the received packet to NS. Then this is the task of NS to filter the duplicates out and assign the GW for downlink transmission.

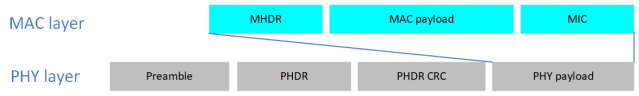

Figure 3: LoRaWAN downlink frame structure.

3 RELATED WORKS: LORAWAN SECURITY

Over the past few years significant efforts have been invested in improving the security of LPWANs in general, and the LoRaWAN in particular. The general-level overview and analyses of the security features of the various LoRaWAN specification releases were carried out, e.g., in [13]-[6]. The security analyses and the enhancements for the LoRaWAN join procedure were provided by the authors of [14],[23] and [7]. The vulnerability of LoRaWAN to jamming and Denial-of-Service(DoS) attacks were investigated by the authors in [3] and [5], respectively. The bit-flipping and replay attacks in the context of LoRaWAN were analyzed in [9] and [22], respectively. The various security-focused enhancements to the LoRaWAN architecture have been proposed by the authors in [17]-[15]. Finally, the specialized security solutions for device-to-device (D2D) and internet protocol (IP) over LoRaWAN have been reported in [8] and [19], respectively. As one can see, the state-of-the-art security studies concerning LoRaWAN focus exclusively on the attacks focused on the data. In the current study, we make a step aside and consider other types of attacks - the energy attacks. We are not aware of any previous practical or theoretical studies of these attacks in the context of LoRaWAN or LPWANs in general.

4 ENERGY ATTACKS IN LORAWAN

Likewise, this is in the Internet; the typical IoT attacks aim at the DoS, or at gaining the unauthorized access and/or compromising the data. Nonetheless, in the context of IoT, there is another critical and vulnerable resource, which is energy. As this is discussed, e.g., in [4], for whatever it does, a LoRaWAN transceiver consumes energy. As can be seen from [4], typically the ED's consumption is maximum while transmitting (TX), is somewhat lower during receiving (RX) and is very low in idle. Thus, as one can easily see, increasing the time spent by a LoRaWAN ED in either TX or RX will compromise the ED's energy utility. Note, that in what follows we do not consider the cases when the LoRaWAN keys are compromised, enabling the attacker to falsify the control (e.g., the ADR) commands. There are two major ways of how an attacker may attempt to increase and ED's TX consumption.

- The former option is through implementing a DoS attack. To ensure the connectivity and handle the ED's mobility, a LoRaWAN ED may periodically issue either a link check request or request an acknowledgment for its data packet. In the case, if no response is received, the ED may presume that channel conditions became more challenging. Consequently, the ED may switch to a higher transmit power or SF. Either of these will increase the ED's energy consumption.
- The latter option is specific to the case when an EDs sends its data in acknowledged mode and is configured to use packet retransmissions. In this case, if an ED does not receive the acknowledgment for its packet (e.g., due to jamming), it will attempt to retransmit the packet several (up to 15) times.

Even though both of the described attacks are feasible, their efficiency is arguable. First, both of them can be detected by the GWs, the ED, or both of these. Second, they have somewhat limited target scope, since they affect only the devices using acknowledged data transfers or using the link check.

Therefore, in what follows we focus on the attacks focused on increasing the ED's RX consumption.

As illustrated in Figure 2, after transmitting data in uplink a LoRaWAN ED must open two RWs. Note that according to LoRaWAN specification the RWs are obligatory and should be present even if the application does not imply any downlink data transfers. Typically, the RWs are rather short (of about five radio symbols only - see [4]) - the ED just checks if it can detect a valid preamble and, if not, switches to the idle state. In the case, if a preamble is detected, the ED proceeds with receiving a packet, the structure of which is depicted in Figure 3. This is worth noting that the physical layer header (PHDR) of a LoRaWAN packet is not encrypted and that the message integrity check (MIC) is located in the very end of the packet. Therefore, after detecting a valid preamble and PHDR, an ED will have to receive the rest of the packet before getting an opportunity to check and validate the packet. Thus, as one can see, the introduction of a radio packet with a valid preamble and PHDR starting during one of the LoRaWAN RWs would increase the time spent by an ED in receive and increase the energy consumption of this ED. Notably, since the functionality of class A is obligatory for all EDs, this attack can be addressed against each and every LoRaWAN ED. Note, that the described attack will typically be undetected - after receiving the whole packet the ED (and the GW, if the attack is carried in RW1) will just dispose of the packet, assuming that it belongs to another network or a non-LoRaWAN system.

As one can see, the LoRaWAN protocol prescribes the use of two receive windows - RW1 and RW2. In a typical LoRaWAN network, the RW1 uses the same SF as was used in the uplink, while for RW2

LoRaWAN network		Victim		Atacker	
Frequency channels, MHz	868.1,868.3, 868.5	TX power, dBm	14	TX power, dBm	0
RECEIVE_DELAY1	1 s	Traffic	Periodic, every few seconds	Traffic	Periodic, every few seconds
RECEIVE_DELAY2	2 s	Uplink payload, bytes	14 or 50	Interf. payload, bytes	30 or 60
RX2 DR	DR0	ADR & ACK	disabled	Frequency, MHz	869.525
RX2 frequency, MHz	869.525				
RX1DROffset	DR7				

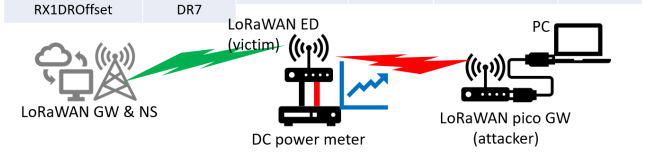

Figure 4: Experiment set-up and key configuration parameters.

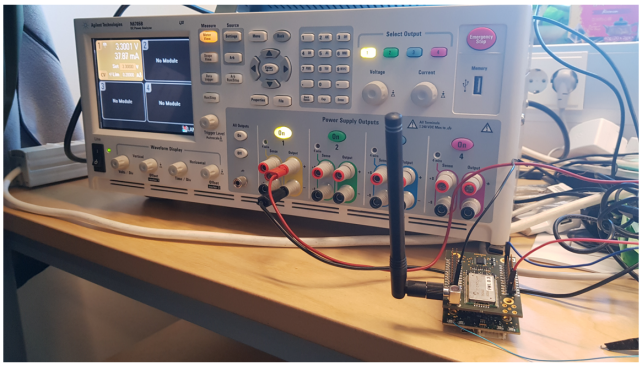

Figure 5: Victim connected to the DC power analyzer.

the maximum SF possible and a dedicated radio channel (e.g., in the 869.5 MHz band in EU, which allows for the maximum transmit power and duty cycle) are used. Note, that the configurations of RW2 are common for all the EDs in a LoRaWAN network. Thus, as one can see, the attacks during the RW2 are likely to take more energy from the victim than in the RW1. Importantly, the RW configurations are often publicly available. And even if not - they can be easily determined by listening to the radio channel.

5 EXPERIMENTAL VALIDATION

5.1 Experimental setup

To validate if the discussed above energy attack is feasible and to characterize the order of the potential energy losses, we have conducted a series of real-life experiments utilizing the commonly-available commercial LoRaWAN hardware chipsets. The structure of our testbed and the key configuration parameters are summarized in Figure 4, while Figure 5 illustrates the victim LoRaWAN ED connected to the DC power analyzer.

As the victim, we have used a single LoRaWAN ED, constructed using the modular IoT hardware platform [11] developed at the Centre for Wireless Communications of the University of Oulu. The test node is composed of the two boards: the core board built around the STM32F217 32-bit ARM microcontroller, and an extension board hosting the Microchip RN2483 radio transceiver, featuring the LoRaWAN radio protocol stack on-board. The special firmware was developed for the experiments on top of the FreeRTOS operation system.

After the initialization, the microcontroller uses the UART interface to initialize and control the radio. First, the radio transceiver is configured as class A LoRaWAN ED and attached to the network using the ABP procedure. Then, the microcontroller starts to periodically generate and forward to the radio the data packets to be transmitted in the uplink. Note, that for the sake of clarity the LoRaWAN ADR functionality is disabled and all the packets are sent in non-acknowledged mode.

The LoRaWAN ED is powered from the Keysight N6705 direct current (DC) analyzer, which also logs the current consumption profile of the ED. The analyzer is configured to output the stable DC voltage of 3.3V and samples the current consumed by the ED at ten kilosamples per second rate. The collected data are further post-processed (e.g., to extract the consumption of the radio by compensating the consumption of the microcontroller core) and visualized with MatLab.

As a LoRaWAN GW we have used the MultiConnect® Conduit™ from MultiTech, which was deployed as the part of the University of Oulu 5GTN [11]. The distance between the ED and the GW was approximately 50 meters.

To emulate the proposed attack, we utilized the SX1308-P868GW Picocell GW [1] from Semtech, which was attached to a computer and controlled by the PicoGW software [20]. We configured (using the HAL_util_TX_test program) the GW to spam the packets in the frequency channel and using the SF matching with that of the victim's RW2. The attacker was placed approximately 2 meters away from the victim. Note that the attacker neither had any of the ED/GW keys, nor any other data except the RW configuration parameters (i.e., the frequency and SF).

5.2 Experimental results

The selected results illustrating the energy consumption profiles of the LoRaWAN ED during normal operation and under energy attack are depicted in Figures 6 and 7, and the respective key numbers measured from the profiles are summarized in Table 1. The presented data illustrate the consumption for the two extreme cases - the ED operating with the minimum (i.e., SF7, EU configuration - CNF1) and the maximum SF (i.e., SF12 - CNF2) and the different payloads. These configurations may be treated as the worst, and the best-case scenarios, respectively, and thus are rather illustrative.

For both these cases, the current consumption was measured for baseline ED operation under no attack, and for the case of energy attack, when a 60-byte RW2 packet from attacker was received by the victim. Additionally, the case of attacker using a 30-byte RW2 packet was measured for ED operating with SF7 (CNF1).

From the presented results one can see that depending on the SF used by the EDs, the attack increases the total amount of energy consumed for one communication event by an ED 36% to 576%. Under the attack, the duration of a communication event also increases by 80-150%. These results decisively demonstrate the vulnerability of the system to the described attack and the devastating effect such an attack might have on the energy utility of the victim ED.

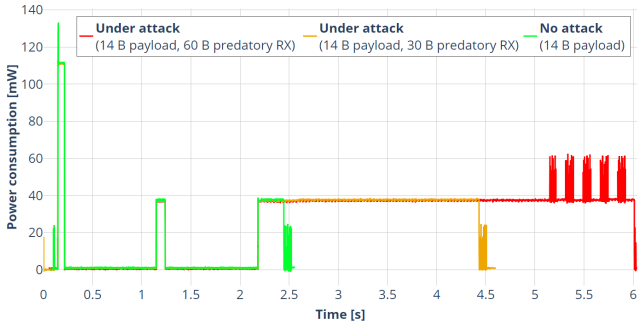

Figure 6: Energy consumption of LoRaWAN ED operating with SF7 - 14 byte uplink payload (normal communication and two different energy attacks.

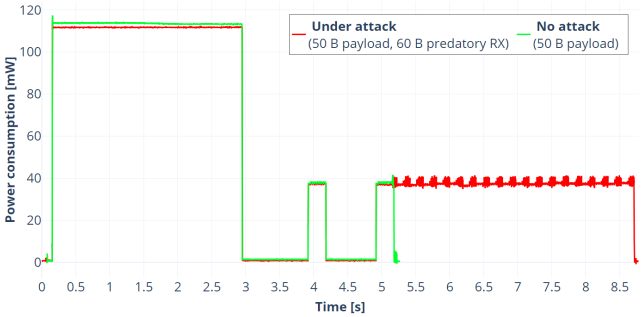

Figure 7: Energy consumption of LoRaWAN ED operating with SF12 - 50 byte uplink payload (normal communication and energy attack).

Finally, Table 2 provides some insight into how the described attack might affect the lifetime of a LoRaWAN ED. As one can see, for the EDs sending once per day, the effect of the attack is very limited. But the more often an ED transmits, the more it gets affected by the attack. For example for an ED operating with SF7 and sending a message approximately every six minutes, an energy attack would reduce the device's lifetime more than three times.

6 DISCUSSION AND CONCLUSIONS

LPWANs in general and the technologies like LoRaWAN will with no doubt play an important role in the future of the IoT. These technologies provide the unique compromise between the cost, consumed energy and scalability, which makes them extremely attractive for resource and traffic limited IoT devices. Still, as we show in this paper, sometimes this might compromise the security.

Departing from the more conventional data-oriented attacks, in this study we have investigated the robustness of LoRaWAN against energy attacks. For many IoT devices, the energy is a limited and very valuable resource, and thus in the near future, it may also become the target of an intentional attack. To the best of our knowledge, the current study is the first to address energy attacks in the context of LPWAN.

Table 1: Energy consumption for communication event in different test cases

Experiment	Energy consumed [mJ]			
	For TX	For CNF1	For CNF2	Total
NATK: ED with DR5	7.4	3.4	9.9	22.9
eATK: ED with DR5 and attacker broadcasts 30-byte predatory RW2 packet	7.4	3.4	84.4	96.8
eATK: ED with DR5 and attacker broadcasts 60-byte predatory RW2 packet	7.8	3.4	112.3	154.9
NATK: ED with DR0	317.2	9.9	9.9	339.5
eATK: ED with DR0 and attacker broadcasts 60-byte predatory RW2 packets	312	9.8	141.2	464.6

*eATK = energy attack, NATK = no attack.

Table 2: Effect of attack on the lifetime (assume node supply from 2 AA batteries with 2850 mAh, 0.1 mW sleep current, linear battery model).

Message per day	Lifetime, years			
	SF7		SF12	
	NATK	ATK	NATK	ATK
1	10.9	10.7	10.5	10.3
10	10.6	9.2	7.8	7.1
100	8.6	3.9	2.2	1.7
250	6.6	2.0	1.0	0.8

*ATK = under attack, NATK = no attack.

In this study, we first analyzed the potential attack vectors, and then experimentally demonstrated the possibility of an energy attack along one of these vectors. Our results decisively show that energy attacks in LoRaWAN are possible and may cause the affected device to lose a substantial amount of energy. Specifically, depending on the ED's SF, the demonstrated attack increased the total energy consumption during a communication event 36 to 576%. Importantly, the shown attack does not require the attacker to have any keys - just the information about the RW2 configuration, which is typically openly available. Also, the shown attack can be carried against any LoRaWAN ED.

Unfortunately, to the best of our knowledge, the state-of-the-art LoRaWAN devices cannot effectively fight against the shown attacks. Specifically, on the one hand, the current specification neither enables the EDs to avoid the RWs nor to control when and in which channels are they opened. Given this, after overhearing an uplink transmission, an attacker may easily predict both the moment of time and the frequency channel in which the ED will receive. On the other hand, this is also very hard to detect such an attack. The ED may detect an attack against it by counting the invalid frames received. The GW may attempt to detect an attack

by listening to the downlink channel when it is not transmitting anything. Unfortunately, to the best of our knowledge, neither of these two mechanisms are readily available in the state-of-the-art LoRaWAN equipment. Finally, an effective countermeasure against the shown attack would be to enable LoRaWAN EDs to check the validity of the packet before it has been received. Nonetheless, this implies substantial, and non-backward-compatible modification of the protocol, and thus is not very likely.

Still, we are certain that the study of the energy-focused attacks need to be continued in order to detect the potential weaknesses and come up with the relevant countermeasures.

7 ACKNOWLEDGMENTS

This work is supported by the Academy of Finland 6Genesis Flagship under Grant no. 318927 and conducted in the context of University of Oulu LPWAN evolution project. Moreover, the National Sustainability Program under Grant no. LO1401 and the Ministry of Interior under Grant no. VI20192022149 financed the research described in this article and, for the research, the infrastructure of the SIX Center was used.

REFERENCES

[1] 5GTN. 2019. 5G Test Network. https://5gtn.fi/. Online; accessed 30 April 2019.
[2] Sergey Andreev, Olga Galinina, Alexander Pyattaev, Mikhail Gerasimenko, Tuomas Tirronen, Johan Torsner, Joachim Sachs, Mischa Dohler, and Yevgeni Koucheryavy. 2015. Understanding the IoT connectivity landscape: a contemporary M2M radio technology roadmap. *IEEE Communications Magazine* 53, 9 (2015), 32–40.
[3] Emekcan Aras, Nicolas Small, Gowri Sankar Ramachandran, Stéphane Delbruel, Wouter Joosen, and Danny Hughes. 2017. Selective jamming of LoRaWAN using commodity hardware. In *Proceedings of the 14th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*. ACM, 363–372.
[4] Lluís Casals, Bernat Mir, Rafael Vidal, and Carles Gomez. 2017. Modeling the energy performance of LoRaWAN. *Sensors* 17, 10 (2017), 2364.
[5] Eef Van Es, Harald Vranken, and Arjen Hommersom. 2018. Denial-of-Service Attacks on LoRaWAN. *Proceedings of the 13th International Conference on Availability, Reliability and Security - ARES 2018* (2018). https://doi.org/10.1145/3230833.3232804
[6] Alexander Gladisch, Simon Rietschel, Thomas Mundt, Johann Bauer, Johannes Goltz, and Simeon Wiedenmann. 2018. Securely Connecting IoT Devices with LoRaWAN. *2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)* (2018). https://doi.org/10.1109/worlds4.2018.8611576
[7] Jaehyu Kim and JooSeok Song. 2017. A simple and efficient replay attack prevention scheme for LoRaWAN. In *Proceedings of the 2017 the 7th International Conference on Communication and Network Security*. ACM, 32–36.
[8] Jaehyu Kim and Jooseok Song. 2018. A Secure Device-to-Device Link Establishment Scheme for LoRaWAN. *IEEE Sensors Journal* 18, 5 (2018), 2153âĂŞ2160. https://doi.org/10.1109/jsen.2017.2789121
[9] JungWoon Lee, DongYeop Hwang, JiHong Park, and Ki-Hyung Kim. 2017. Risk analysis and countermeasure for bit-flipping attack in LoRaWAN. In *2017 International Conference on Information Networking (ICOIN)*. IEEE, 549–551.
[10] LoRa ALLIANCE. 2017. LoRaWAN™ 1.1 Specification. https://lora-alliance.org/resource-hub/lorawantm-specification-v11. Accessed 30 April 2019.
[11] Konstantin Mikhaylov and Juha Petäjäjärvi. 2017. Design and implementation of the plug&play enabled flexible modular wireless sensor and actuator network platform. *Asian Journal of Control* 19, 4 (2017), 1392–1412.
[12] Ministry for Primary Industries. 2018. LPWAN: The fastest growing IoT communication technology. https://www.iot-now.com/2018/10/29/89895-lpwan-fastest-growing-iot-communication-technology/. Online; accessed 30 April 2019.
[13] Thomas Mundt, Alexander Gladisch, Simon Rietschel, Johann Bauer, Johannes Goltz, and Simeon Wiedenmann. 2018. General Security Considerations of LoRaWAN Version 1.1 Infrastructures. In *Proceedings of the 16th ACM International Symposium on Mobility Management and Wireless Access*. ACM, 118–123.
[14] SeungJae Na, DongYeop Hwang, WoonSeob Shin, and Ki-Hyung Kim. 2017. Scenario and countermeasure for replay attack using join request messages in LoRaWAN. In *2017 International Conference on Information Networking (ICOIN)*. IEEE, 718–720.
[15] Sarra Naoui, Mohamed Elhoucine Elhdhili, and Leila Azouz Saidane. 2017. Trusted Third Party Based Key Management for Enhancing LoRaWAN Security. *2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA)* (2017). https://doi.org/10.1109/aiccsa.2017.73
[16] Van-Linh Nguyen, Po-Ching Lin, and Ren-Hung Hwang. 2019. Energy Depletion Attacks in Low Power Wireless Networks. *IEEE Access* 7 (2019), 51915–51932.
[17] Bogdan Oniga, Vasile Dadarlat, Elie De Poorter, and Adrian Munteanu. 2017. A secure LoRaWAN sensor network architecture. *2017 Ieee Sensors* (2017). https://doi.org/10.1109/icsens.2017.8233990
[18] Usman Raza, Parag Kulkarni, and Mahesh Sooriyabandara. 2017. Low power wide area networks: An overview. *IEEE Communications Surveys & Tutorials* 19, 2 (2017), 855–873.
[19] Ramon Sanchez-Iborra, Jesus Sanchez-Gomez, Salvador Perez, Pedro J. Fernandez, Jose Santa, Jose L. Hernandez-Ramos, and Antonio F. Skarmeta. 2018. Internet Access for LoRaWAN Devices Considering Security Issues. *2018 Global Internet of Things Summit (GIoTS)* (2018). https://doi.org/10.1109/giots.2018.8534530
[20] Semtech. 2017. User Guide to the LoRa® PicoCell Gateway V1.0. https://www.semtech.com/uploads/documents/picocell_gateway_user_guide.pdf. Online; accessed 30 April 2019.
[21] Statista. 2018. Share of LPWAN IC module shipments by technology worldwide in 2017. https://www.statista.com/statistics/880822/lpwan-ic-market-share-by-technology/. Online; accessed 30 April 2019.
[22] Woo-Jin Sung, Hyeong-Geun Ahn, Jong-Beom Kim, and Seong-Gon Choi. 2018. Protecting end-device from replay attack on LoRaWAN. In *2018 20th International Conference on Advanced Communication Technology (ICACT)*. IEEE. https://doi.org/10.23919/icact.2018.8323683
[23] Stefano Tomasin, Simone Zulian, and Lorenzo Vangelista. 2017. Security analysis of lorawan join procedure for internet of things networks. In *2017 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*. IEEE, 1–6.
[24] Lorenzo Vangelista. 2017. Frequency shift chirp modulation: The LoRa modulation. *IEEE Signal Processing Letters* 24, 12 (2017), 1818–1821.