Poster: Impact of Energy Consumption Attacks on LoRaWAN-Enabled Devices in Industrial Context

Muhammad Nouman Nafees[1], Neetesh Saxena[1], Pete Burnap[1], and Bong Jun Choi[2]
[1]Computer Science and Informatics, Cardiff University, Cardiff, United Kingdom
{nafeesm, saxenan4, burnapp}@cardiff.ac.uk
[2]School of Computer Science & Engineering, Soongsil University, Seoul, South Korea
davidchoi@soongsil.ac.kr

ABSTRACT

Successful deployment of Long-Range Wide Area Network (LoRaWAN) technology in several Industrial Internet of Things (IIoT) scenarios, such as Outage Management System (OMS) in smart metering, rely on low energy consumption of the end device. In this work, we conducted an experiment to demonstrate an on/off Denial-of-Service (DoS) attack to analyze the impact on the energy consumption of the LoRaWAN end device. We implemented the attack that manipulates the end device to remain in packet retransmission mode for several seconds. The conducted experiments show that the configurable parameters of LoRaWAN that are required for applications, like OMS, are susceptible to energy consumption attacks. In summary, our results show that when an on-off DoS attack is performed, the end device utilizing the Spreading Factor (SF) 12 consumes 92 times more energy due to packet retransmissions as compared to the end node using SF 7 under no attack.

CCS CONCEPTS

•Security and privacy~Network security~Denial-of-service attacks • Networks~Network protocols~Network layer protocols~Routing protocols

KEYWORDS

IIoT; Energy consumption; DoS attack; LoRaWAN

ACM Reference format:

Muhammad Nouman Nafees, Neetesh Saxena, Pete Burnap, and Bong Jun Choi. 2020. Poster: Impacts of Energy Consumption Attacks on LoRaWAN Devices. In *Proceedings of 2020 ACM CCS.* ACM, New York, NY, USA, 3 pages.

1 INTRODUCTION

Low-Power Wide Area Networks (LPWANs) have emerged as an essential part of the Industrial Internet of Things (IIoT) infrastructure for applications that require low mobility and short communication messages [1]. Long-Range Wide Area Network (LoRaWAN) is a promising technology in LPWAN, which has received significant attention lately. In the context of the smart grid, LoRaWAN appears to be quite suitable for the Outage Management System (OMS) in smart metering applications [2]. Centrally located single LoRaWAN gateway can provide long-range communication for geographically dispersed devices in the smart metering infrastructure. However, the vision of deploying LoRaWAN in aforesaid application relies on the low power consumption of the end devices. The OMS requires continuous functioning of the devices for automatic meter reading and also during the power outages [2]. The battery-powered LoRaWAN devices of Class A have a finite battery lifetime; therefore, the energy consumption of such devices holds paramount importance.

In smart metering, the escalation method is usually employed to determine if there is a problem in a single transformer or if it is affected by a large-scale outage using the outage notifications messages from smart meters [2]. In this direction, the utility needs to ensure the successful packet transmission rate for power consumption reading and outage alert notifications. LoRaWAN provides retransmission of packets in acknowledged mode to ensure fair packet delivery. However, packet collision probability also increases with the retransmission of packets that can cost more energy consumption as the end device is now required to transmit more packets. Moreover, LoRaWAN protocol does not employ algorithms such as Carrier-Sense Multiple Access for collision avoidance. Consequently, the adversaries can exploit vulnerabilities to perform energy consumption attacks in order to deplete the energy of the battery-powered LoRaWAN devices.

In this work, we conduct an experiment to perform an on/off DoS attack to manipulate the packet retransmission of the LoRaWAN end device in acknowledged transmission mode. To this end, we analyze the impact of the attack on energy consumption of the LoRaWAN end device utilizing the Spreading Factor (SF) values of 7 and 12. Most importantly, our work demonstrates the impact through observed results of energy consumption of the packet transmission under on/off DoS against the energy consumption of the transmitted packets under no attack.

2 RELATED WORK

Until recently, most of the existing research focused on the reliability and low bandwidth issues of LoRaWAN in the Internet of Things (IoT) network. There are only a few works that highlight the potential threats of energy consumption attacks on the battery-powered LoRaWAN devices. Mikhaylov et al. [3] considered the deployment of LoRaWAN nodes for the wind turbine monitoring in smart grid infrastructure. However, the work only provides a high-level discussion on the suitability of the LoRaWAN network in energy infrastructure. To maximize battery exploitation, Sisinni et al. [4] proposed an Adaptive Data Payload (ADP) as an alternative to the Adaptive Data Rate (ADR) algorithm to equalize the message

time duration for the whole smart metering lifetime. The work, however, does not address the impact of built-in parameters of LoRaWAN on its power consumption. Samuhasilp et al. [2] analyzed the applications of LoRaWAN technology in the smart grid. In this context, they explained how LoRaWAN devices can be incorporated into smart metering for OMS. This work does not discuss the energy consumption attacks and the influence of LoRaWAN parameters.

Like our work, Nguyen et al. [5] and Mikhaylov et al. [6] focused on the energy depletion attacks on the low power wireless network. Nguyen et al. [5] presented a systematic overview of other LPWAN technologies but did not analyze the LoRaWAN technology concerning energy depletion attacks, whereas, Mikhaylov et al. [6] experimentally validated the feasibility of the energy attacks on LoRaWAN end devices. The experiments, however, do not cover the energy attacks in the acknowledged transmission mode of the end device. Therefore, the influence of the retransmission of packets on energy consumption was ignored. Our work specifically focuses on the impact of spreading factors and retransmission attempts of the packets on energy consumption of the LoRaWAN under an on/off DoS attack. We realize that most applications in IIoT require the retransmission of packets for fair packet delivery. In addition, these applications may utilize different SFs according to the environmental conditions between the end device and the gateway. In this context, frequent packet retransmissions and high values of SF can account to more transmission time, therefore, both parameters are quite significant with respect to energy consumption of LoRaWAN end devices.

3 APPROACH

Our main goal of this work is to examine the overall impact of energy consumption attacks on LoRaWAN devices. In this direction, energy consumption attacks often entail manipulation of configurable parameters of LoRaWAN to keep the end-device in a longer period of energy-consuming tasks such as transmission mode. To find the influence of such parameters, we briefly explain the key parameters of LoRaWAN that can influence the power consumption of the end device under the energy consumption attack.

Spreading Factor (SF). It is a key variable in Long-Range (LoRa) and has a significant impact on power consumption and the range of LoRaWAN communication. Each SF has an orthogonal signal and LoRa uses the SF values ranged from 7 to 12 (that correspond to data rates from DR5 to DR0, respectively). The greater value of SF increases the sensitivity of the signal, however, time-on-air for the message transmission also gets increased [7]. To this end, airtime of the messages directly impacts the energy consumption of the LoRaWAN devices, since the devices spend more time in the energy-consuming tasks of transmitting the signal.

Receive Windows. All end-devices open two receive windows after every uplink transmission. LoRaWAN uses this feature for the downlink messages from the gateway to the LoRaWAN end-devices. The uplink spreading factor is used for the first receive window (RX1) by default, while the second receive window (RX2) uses a fixed spreading factor of 12. To this end, the duration of each receive window depends on the time required to detect the downlink preamble. Receive window is a critical parameter with respect to energy consumption since the time spent waiting for the downlink transmission can directly impact the lifetime of battery-powered LoRaWAN devices.

Energy Consumption Attacks. These attacks aim to significantly reduce the lifetime of battery-powered devices [6]. The adversaries can scan the radio channel to see receive window configurations that are publicly available. Next, messages from the rogue gateway can be sent using the same SF as of the RX1 configuration of the victim's device with high transmitting power. In turn, the packets received in the RX1 can account for more time in detecting the full packet until the valid preamble is detected since the Message Integrity Check (MIC) bit is located at the end of the LoRaWAN's packet [6].

To extend this attack scenario, we run an experiment to demonstrate an on/off Denial-of-Service (DoS) attack on sensor nodes by flooding the device with unauthenticated messages for short intervals (wisely striking on/off attack waveforms that cause a denial of service). The adversary can opportunistically execute this attack without being detected. If the device is enabled with acknowledged transmission mode for reliable packet delivery, the on/off DoS attack can manipulate the end device to attempt to retransmit the packet several times (up to 8). The adversary can execute this attack for short intervals that can potentially pose a stealthy threat to the energy consumption of the end device due to the retransmission of packets. We argue that this attack can significantly increase the energy consumption of the end device. Nevertheless, the adversaries can execute the attack persistently to drain the energy of the batteries. Consequently, such attacks can incur high financial losses due to interruption of related operations such as outage notification and polling algorithm in OMS.

4 EXPERIMENTAL EVALUATION

Experimental Setup. We use the Libelium LoRaWAN microcontroller with the events sensor board. We use the 12CXL-MaxSonar ultrasonic sensors for the demonstration of a LoRaWAN application. For downlink transmissions, we use Multitech Conduit gateway since it is programmable and employs the Node-Red visual development tool. Moreover, the aforementioned gateway logs all the packets' transmission history. We program the LoRaWAN microcontroller to join the gateway using Over-the-Air Activation (OTAA) method. We configure the transmit power to 14 dBm, maximum payload to 51 bytes, and bandwidth to 125 kHz for all set of experiments. To this end, we configure these parameters by considering the extreme requirements of the IIoT OMS application. The distance between the gateway and the end device is 45 meters. We use an oscilloscope to measure power fluctuations during an experiment.

Execution. We power on the LoRaWAN end device using the external power source of 3.3 Volts as per the vendor's recommendations. Following initialization, the microcontroller connects to the LoRaWAN module using the Universal Asynchronous Receiver-Transmitter (UART) 0. For the first two sets of experiments, we configure the end device with

acknowledged transmission mode and measure the energy consumption for the SF value of 7 and 12 under no energy attack.

To emulate the attack scenario for the next two sets of experiments, we use another LoRaWAN gateway as a rogue device to execute an on/off DoS attack by configuring the same RX1 configuration as of the victim's device. We enable the acknowledged transmission mode and execute the on/off DoS attack for a few seconds for the SF value of 7 and 12. We execute the attack until several retransmissions of packets are done. We use the experimental results to evaluate the impact of an on/off DoS attack on energy consumption utilizing different SF values.

Results. The results from our experiment are summarized in Table 1 and Table 2. The first two sets of experimental results compare the impact of the spreading factor on energy consumption in acknowledged transmission mode. Under no energy attack, the results show that in order to facilitate 51 bytes of payload, the end device configured with SF 12 consumes approximately 18 times more energy than the end devices configured with SF 7. More airtime of the packet transmission keeps the end device in the energy-consuming task of transmitting, therefore, SF 12 caused significantly more energy consumption. It is worth noting that the significant difference between the energy consumption for both values of SF is also attributed to the receive windows parameter. Nevertheless, RX2 uses the highest SF for the downlink acknowledgment as opposed to RX1, which uses the uplink SF. In the case of SF 12, both RX1 and RX2 utilize the highest SF which also corresponds to the lowest data rates and more airtime.

Table 1. Energy consumption under no attack

Spreading Factor	Sensitivity (dBm)	Payload (Bytes)	Energy (mJ)
7	-123.0	51	41.4
12	-137.0	51	760

Table 2. Energy consumption under on/off DoS attack

Spreading Factor	Sensitivity (dBm)	Payload (Bytes)	Energy (mJ)
7	-123.0	51	210
12	-137.0	51	3830

The second set of two experimental results show the impact of on/off DoS attack**s** on the energy consumption of the end device. The on/off DoS attack was executed frequently for the duration of a few seconds to keep the end device in retransmitting mode until the message is finally transmitted. For SF 7, the demonstrated attack increased the energy consumption of a single successful transmission of the packet to 210 mJ, 5 times more than the result for the same SF under no attack. To this end, the LoRaWAN device utilizing SF 12 shows the significant energy consumption of 3830 mJ for a single packet successful transmission after various retransmission attempts. The results clearly show that the retransmission of packets due to the on/off attack has a significant impact on the device utilizing higher SF which can be attributed to the packets airtime, packets collision factor, and receive windows parameter.

5 CONCLUSION AND FUTURE WORK

In this study, we briefly discussed the efficacy of LoRaWAN for OMS in smart metering. Particularly, we discussed the energy consumption attacks that how an adversary can manipulate the parameters of LoRaWAN to significantly diminish the battery lifetime of the end device. Our results show that the end device using acknowledged transmission for fair packet delivery can be susceptible to on/off DoS attacks. The end node utilizing SF 12 under an on/off DoS attack can consume approximately 92 times more energy as compared to the end node using SF 7 under no attack in acknowledged transmission mode. To this end, the applications that require retransmission of packets for fair packet delivery must ensure the avoidance of using high spreading factors. In the future, we aim to further investigate the impact of energy attacks for different sizes of data payload in accordance with the spreading factors. In this direction, we believe that robust analysis is needed to evaluate the vulnerability of LoRaWAN end devices against various types of energy attacks.

ACKNOWLEDGMENTS

This research was supported by Cardiff University HEFCW GCRF Project (SP113) and the National Research Foundation (NRF), Korea (2019R1C1C1007277) funded by MSIT, Korea.

REFERENCES

[1] Saba Al-Rubaye, Ekhlas Kadhum, Qiang Ni and Alagan Anpalagan. 2019. Industrial internet of things driven by SDN platform for smart grid resiliency. *IEEE Internet Things J.* 6, 1, 267–277.

[2] Jittiwat Samuhasilp and Wanchalerm Pora. 2018. Development of an automatic meter reading and outage management system using LoRaWAN technology. In *Proceedings of the 5th IEEE International Conference on Smart Instrumentation, Measurement and Application (ICSIMA)*, 1-4.

[3] Konstantin Mikhaylov, Abdul Moiz, Ari Pouttu, José Manuel Rapún and Sergio Gascon. 2018. LoRaWAN for Wind turbine monitoring: prototype and practical deployment. In *Proceedings of the 10th International Congress on Ultra Modern Telecommunications and Control Systems (ICUMT)*, 1–6.

[4] Emiliano Sisinni et al. 2020. A new LoRaWAN adaptive strategy for smart metering applications. In *Proceedings of the IEEE International Workshop on Metrology for Industry 4.0 IoT*, pp. 690-695.

[5] Van-Linh Nguyen, Po-Ching Lin and Ren Hwang. 2019. Energy depletion attacks in low power wireless networks. *IEEE Access* 7, 51915-51932.

[6] Konstantin Mikhaylov et al. 2019. Energy attack in LoRaWAN: Experimental validation. In *Proceedings of the 14th International Conference on Availability, Reliability and Security*, Article 74, 1-6.

[7] N. Sornin et al. *LoRa Specification 1.0*, LoRa Alliance Std Spec. [online] Available: https://lora-alliance.org/resource-hub/lorawanr-specification-v10.