Wireless Personal Communications (2022) 126:3663–3675
https://doi.org/10.1007/s11277-022-09884-8

LoRaWan Sensitivity Analysis and Prevention Strategies Against Wireless DoS Attacks

N. Prasad[1] · P. Lynggaard[2]

Accepted: 29 May 2022 / Published online: 21 June 2022

Abstract
New wireless IoT technology provides smart pseudo intelligent solutions that will have a big impact on the infrastructures and the society in the future to come. In the last decade, many new low power longrange wireless technologies have emerged to support these wireless IoT based solutions. One of the most promising and commonly accepted technologies is LoRaWAN. Unfortunately, the introduction and deployment of a new wireless technology provides new risks and new security challenges. Some of these challenges can be categorized as "critical", which means that if they fail, this will have major consequences for the society's critical infrastructure and the society as a hole. In this paper one of these critical challenges is analyzed in terms of wireless jamming attacks that cause fatale denial-of-services on the LoRaWAN wireless infrastructure and connectivity. This analysis is based on a mathematical simulation model which is described and elaborated. By using this model on a selected societal critical service example, a sensitivity analysis in terms of jamming and DoS attacks is performed, provided, and elaborated. Finally, some selected prevention strategies to avoid and counter-fight these attacks are presented, discussed, and elaborated.

Keywords LoRaWAN · DoS attack · Jamming · Critical infrastructures · IoT sensors

1 Introduction

In the last decade, many new low power long-range wireless technologies have emerged to support the ongoing evolution of the internet in the form of the new Internet of Things (IoT) area. One of the most well-known technologies is LoRaWAN which operates in the unlicensed bands, in contrast to the cellular based (4G, 5G and 6G) technologies that use licensed bands.

LoRaWAN offers high Quality of Service (QoS) capabilities, long-range capabilities, and low power capabilities which makes it an ideal candidate for use in critical applications

✉ P. Lynggaard
plyn@dtu.dk

[1] CTIF Global Capsule (CGC), School of Business and Social Sciences, Aarhus University, Herning, Denmark

[2] Technical University of Denmark, Ballerup, Denmark

such as energy, health, transport, telecommunications, maritime and drinking water supply. In these safety critical applications reliability and security are essential parameters that must be investigated in form of an impact assessment and an examination of the technical and structural security challenges. Such an investigation will potentially save human lives and reduce the huge economic impact a successful attack can cause.

From a future perspective LoRaWAN is expected to take one of the leading roles with respect to long-range wireless IoT communication. Hence, it is expected that 43 percent of the 500 billion IoT devices will be connected by LoRaWAN technology in the year 2030 [1]. Similarly, IoT Analytic expects billion LoRaWAN based IoT connections in 2023 [2], see Fig. 1.

The most important LoRaWAN characteristics are:

- long range (several miles in urban environments, dozens of miles in rural environments).
- deep penetration (especially compared to 5G).
- very long battery life (10 + years).
- low-cost modules.
- low data rate (0.3 bps–50 kbps).
- unlicensed radio frequency spectrum.
- native geolocation.
- bidirectional communication; and open standard.

This paper will further discuss DoS attacks in social critical applications and propose prevention strategies.

2 LoRaWAN DoS Attacks: A Society Critical Service Example

LoRaWAN is becoming one of the key technologies as the COVID-19 outbreak happened worldwide. This solution provides healthcare workers and private people with data and insight into community health, allowing more optimized workflows for the distribution of efficient healthcare services during the ongoing coronavirus (COVID-19) outbreak.

The task of monitoring and managing quarantined and isolated personnel remains a critical challenge. Health services employees, including disease control and prevention

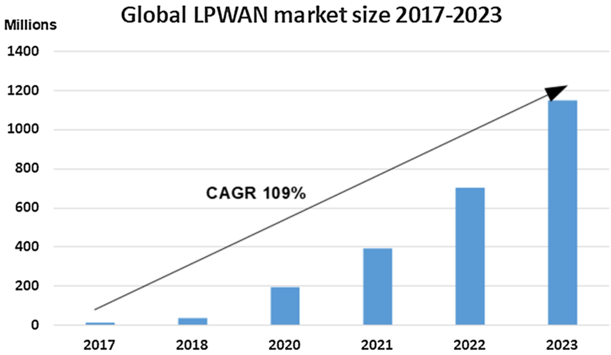

Fig. 1 IoT analytic expects billion LoRaWAN based IoT connections in 2023 [2]. As illustrated, it is expected that more than 1.1 billion IoT devices are connected in 2023. It is noted that a compound annual growth rate (CAGR) of 109 percent is expected over the period 2017 to 2023

teams, are increasingly leveraging smarter applications based on IoT to provide efficient, high-quality care to their communities.

1. *Medical gas valve monitoring* With the increased demand for medical equipment, using LoRaWAN, these valves will contain digital pressure gauges and are equipped with LoRaWAN for data transmission, which allows hospital staff to remotely monitor and control the amount of oxygen remaining in the cylinder.
2. *Asset temperature monitoring* While hospitals focus on treating crucial COVID-19 cases, monitors the temperatures of vaccines and blood in refrigerators as well is in transportation. Maintaining proper temperature is critical to ensure vaccines, medicine, and blood do not spoil, while also helping to relieve the staff from manually having to record temperature readings.
3. *Infection risk reduction in hospitals and healthcare* With the coronavirus outbreak, hospitals are confronted with the challenge of treating patients while preventing the spread of infection. Using LoRaWAN to reduce infection risk through the deployment of sensors that provide a predictive view into cleaning needs, occupancy patterns, air and water quality and more.
4. *Infrared temperature sensor* Using LoRa devices, Polysemes has developed a series of smart human body temperature monitoring products. Real-time data from the temperature sensors enables healthcare workers to efficiently screen individuals with a high temperature. The solution has recently shipped to Italy to help with its coronavirus (COVID-19) response efforts.
5. *Proximity detection and contact tracing for Covid-19* Enhance work-place safety by enforcing social distancing policies! Compact wearable proximity sensors enable easy monitoring of interactions between people in all shared facilities and allow to ensure that people are keeping the safe distance between each other, to avoid temporary shutdowns of operating factories with enhanced safety measures, and to track all the interactions between the infected and healthy people to identify a contamination cluster. The solution allows proximity alert and monitoring, zoning policy enforcement, density policy enforcement, sanitization of shared assets and nurse-call bedside buttons in hospitals.
6. *Nurse call systems for temporary hospitals* With an influx of patients due to COVID-19, temporary hospitals are being set up around the world, but the infrastructure does not exist in temporary locations. LoRa Alliance members are working to provide wireless nurse calling solution that sets up in minutes so patients can push a button to summon the Nurse staff.
7. *Self-service facilities sanitization* This IoT solution helps you to optimize the sanitization of your self-service dispensers, machines, and kiosks so that you can prevent the spread of germs as well as maintain a positive experience with your customers. Thanks to the Switzer cloud, you always know when and how many movements are detected, so that you can react and efficiently plan when to sanitize.
8. *Back to work on premises solution for site managers* Lockdown lift has come and workers are about to get back to work on site be it industrial, commercial or tertiary. To prevent a second COVID-19 wave, a 3 flaps IoT solution to make this process secure and reassuring for people are being brought in place. 3 key issues related to COVID-19 spread are treated: people's temperature, social distancing, and ambient conditions.
9. *Private proximity monitoring* A private proximity monitoring solution is being fast-tracked for use across different industries due to its potential to help workers and com-

munity members maintain social distancing and reduce the spread of the virus without compromising personal privacy.

2.1 Impact of DoS on LoRaWAN Usecases

LoRaWAN usecases are using very low data rate (0.3–50 kbps depending on the frequency band) enabling LoRa to cover long-range communication (1–2 miles). However, it also increases the on-air transmission time in the order of 3 s (depending on the payload). This is a unique feature of LoRa network when the security risks of the nodes in the network are not the same even when these nodes use single hop for communication. Therefore, it makes LoRa network susceptible to different kinds of denial of service (DoS) attacks, including jamming, replay attacks, and eavesdropping and in different variability depending on the distance of the LoRa nodes from the gateway.

DoS attacks are launched to destroy the availability of one or multiple nodes. For example, an adversary may physically tamper an end device to disable its duty or make it transmit interference signals, or it can sniff the packets in wireless channels and selectively jam a particular portion of end devices. DoS attacks disrupt legitimate transmissions and increase the energy consumption of end devices by more re-transmissions.

LoRa can be considered as the WiMAX (IEEE 802.16) of the IoT technology. Several attacks (Distributed Denial of Service and Water Torture attacks) against WiMAX have shown to be dreadful.

In a jamming attack, an example of DoS attack, a high-power transmitter can transmit small packets either continuously or randomly and interfere with legitimate packet transmissions, disrupting the regular network operation [3]. Experiments done with vehicular communication have shown that RF jamming can lead to large communication-blind areas [4]. Not much can be done to mitigate jammers with unlimited resources in terms of transmission power and spectrum efficiency [5]. LoRa works in the frequency band of 26 MHz in the USA (902 to 928 MHz). Such a narrow band is not immune to such kind of wideband jamming attacks. It is, therefore, essential to seek the support of law enforcement to capture the attacker physically. However, a continuous or wide-frequency-band jamming attack is easy to detect. Usually, an attacker would not reveal its presence but only listens to the channel passively.

It selectively jams packets by reading the physical header and go to sleep or in listening mode after jamming the packet [6]. This attack mode is hard to detect and deter. In LoRa, since the on-air time of packets is high, the reaction time of the selective jamming attacker to jam the packet after the header is read is also high. Therefore, this kind of attack is a significant threat to the security of the LoRa network. On the top, LoRa end-devices use random time slots to transmit packets. Therefore, LoRa network cannot distinguish between packet losses due to regular congestion and a jamming attack.

Another unique characteristic of LoRa networks is that the difference between the lowest and highest data rates is vast, resulting in a significant difference between the on-the-air transmission time. The nodes that are close to the gateways can use a high data rate and a short on-the-air transmission time; on the contrary, the nodes that are far away from the gateways have to use a low data rate and a long on-the-air An attacker can make use of the long on-air time to launch a selective jamming attack [7] when the attacker can read the physical message header (which is not encrypted) and jammed based on the jamming policy. Selective jamming not only reads through the preamble but also the message header. Thus, attackers can listen on the channels, target a particular device or traffic class and then jam selected messages [8]. In order to selectively jam LoRaWAN messages, an attacker has to perform the following steps. It first detects a LoRaWAN packet. It aborts receiving if the received content triggers the jamming policy (usually first 5 bytes). If no, it immediately jams the channel. Therefore, the jamming window is smaller than the general triggered jamming. However, selective jamming can prevent critical messages from reaching the gateway, especially for those sensor devices that only transmit when the sensor state change happens (event-driven sensors). Selective jamming is implemented on a real testbed with cheap hardware [9].

3 LoRaWAN—Sensitivity to Wireless DoS Attacks

In general, LoRa is sensitive to wireless jamming attacks where a received uncorrelated signal with a high field strength can degrade the signal-to-noise ratio to a non-decodable level [10]. However, LoRa has a "build in" prevention strategy in the form of using spread spectrum at its physical layer [11].

LoRa uses a proprietary spread-spectrum modulation technique which is based on existing spread-spectrum technologies with a fixed channel-bandwidth (125/500 kHz) and an orthogonal spreading factor. By varying the spreading-factor it is possible to trade bitrate for radio sensitivity and robustness of the transmission channel in relation to interferences and jamming attacks. This robustness is implicitly given by the processing-gain (PG) which is a function of the spreading factor as stated in Eq. (1) [12].

$$PG = \frac{2^{SF}}{SF} \tag{1}$$

The processing-gain enables the receiver to recover a signal, even if it is buried in noise, i.e., the signal-to-noise-ratio (SNR) can be negative. Another important feature of the PG is its ability to suppress interferences and jammers. To elaborate this, the different jamming types will be discussed in the following.

In theory, many jamming-types exist [12]; however, spot-jamming and full-band-noise-jamming represents the two main groups. In the first group (spot-jamming), the attacker attempts to force a DoS attack with one or a collection of unmodulated carrier waves, which LoRa-radio counteracts by spreading these. This counteracting process takes place in the correlation processing step which is performed to de-spread the (wanted) received signal. Hence, the signal from the jammer is reduced by the PG (1). The second group (full-band-noise-jamming) uses a noise form which can be modelled as an uncorrelated wideband Gaussian noise source with a flat power spectral density. This noise source has an impact on the (wanted) received signal because it decreases the receiver's input SNR and thereby reduces the receiver's probability to correctly interpret the received symbol. However, as previously stated the PG needs to be overcome, which means that the noise floor must be larger than the signal needed multiplied by the PG. It is noted that the necessary wideband noise power level requires a considerable amount of energy which the jammer must provide to successfully accomplish a Dos attack. This energy limitation reduces the chances for making successful wireless DoS attacks.

Without loss of generality, a mathematical model has been developed to research, explore, and elaborate the radio-channel conditions needed by a jammer to successfully perform a DoS attack. One of the model's key components is a mathematical description of the pathloss from a (wanted) transmitter or a jammer to the receiver. Such a pathloss model needs to be selected as a function of the context it describes, which in this paper is assumed to be an urban radio channel. One of the better fitting models to urban areas is the Okumura-Hata model [13] (2). In addition, this model covers a frequency range from 150 MHz to 1.5 GHz, which means that the used LoRa communication frequencies fit inside this range.

$$\begin{aligned} &L = 69.55 + 26.16\log_{10}(f) - 13.82\log_{10}(ht) - ahr + (44.9 - 6.55\log_{10}(ht))\log_{10}(R) \\ &\text{Where ahr} = 3.2(\log_{10}(11.75hr)^2 - 4.97) \end{aligned} \tag{2}$$

The model calculates the pathloss (L) in dB based on the parameters ht (transmit antenna height), hr (receiver antenna height), f the frequency in MHz and R the distance from the transmitter to the receiver.

After the signal has passed the channel-model the known signal at the receiver can be found. By combining this signal with an additive white Gaussian noise floor (AWGN) given by Boltzmann's constant, the absolute temperature (in kelvin) and the channel bandwidth the signal to noise ratio (SNR) can be calculated. By using this SNR, the probability for a bit error can be found. A good approximation for the receiver bit-error-rate (BER) can be calculated by using an approximated formula (3) given by Tallal et al. [14].

$$P_b \sim 0.5Q\left(1.28\sqrt{\gamma^{2^{SF+1}} - \sqrt{1.386SF + 1.154}}\right) \tag{3}$$

where γ is SNR, SF is spreading factor and Q(*) is the Q-function. Based on the BER it is possible to calculate the Package-Error-Rate (PER) if the package size is known (4).

$$PER = 1 - (1 - BER)^{N*8} \tag{4}$$

where N is the number of bytes in a LoRaWAN package.

By implementing the discussed formulas ((1) to (4)) in a mathematical program and using the data from Table 1, the PER can be found for different input signals at the LoRaWAN gateway antenna. Nevertheless, it is noted that the model is based on general equations without any dependency to Table 1, i.e., it can be used without loss of generality.

Table 1 Simulation-data used in the mathematical model

LoRaWAN parameters	Value
Noise factor for gateway receiver	6 dB
Transmit frequency	870 MHz
Transmit power	14 dBm
Height gateway antenna	8 m
Height LoRaWAN-node antenna	2 m
Antenna gains	2 dB
Coding rate (CR)	1
Bandwidth	125 kHz
Package length	32 bytes

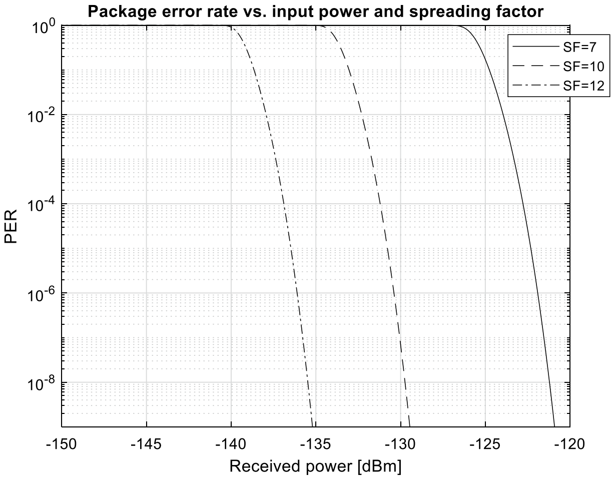

Fig. 2 Package error rate as a function of received input signal to noise ratio, for selected spreading factors (SF = 7,10,12). The x-axis is the received power at the input of the LoRaWAN device and the y-axis is the packet error rate (PER). The graphs show the connection between the received power and the PER for 3 commonly used spreading factors (authors figure)

By using the simulation data (Table 1) the PER as a function of input power can be calculated (Fig. 2). It is noted that the values given by these curves is in good agreement with the results presented in a design note by Semtech Corporation [15].

It can be observed (Fig. 2) that a typical LoRaWAN gateway-receiver is able to receive packages with a very low error rate even if the signal is buried in noise. As an example, it can be observed that using an input signal of -136 dBm with a spreading factor of 12 yields a PER of approximately 10^{-9} (dash-dot curve in Fig. 2). However, the absolute thermal noise floor is approximately at -116 dBm in the used bandwidth, which means that the noise floor is approximately 20 dB larger than the signal. This means that the LoRaWAN signal is submerged 20 dB (100 times) under the surface of the thermal noise floor which makes the signal almost indetectable with radiometer based devices etc. This almost errorfree reception is possible because the frequency components in the spread-spectrum modulation is correlated with the reception key, whereas the noise spectral components are uncorrelated. This gain of 20 dB is provided by the processing gain (1), where it is noted that the processing gain is a function of the spreading factor as stated in Eq. (1). As observed, a low spreading factor (e.g., SF = 7) provides less processing gain, which means that the received input power needs to be higher for a fixed PER compared to a higher spreading factor e.g., SF = 12; nevertheless, the benefit of using a lower processing gain is a higher bitrate, i.e., a SF of 12 yields a bit rate of 293 bps, whereas a SF of 7 yields 5468 bps [16] (Fig. 3).

Focusing on the transmitted distance between the LoRaWAN gateway-receiver and the local LoRaWAN device it turns out that a large spreading factor is required to transmit a package with a small package error rate over a large distance. The reason for this is the processing gain increases with the spreading factor as previously discussed. However, the cost of a large spreading factor is a low bitrate. This clearly illustrates that most parameters in a radio system is based on compromises and trade-offs where package reliability, transmit distance, transmit power, and bitrate need to be negotiated and prioritized.

In relation to intentionally jamming, it is assumed that the jammer uses an additive white gaussian noise-source, which is the worst-case jamming method as discussed previously. By using this jamming method in a service-scenario the received package error rate can be derived as a function of different jamming parameters. One of these parameters is

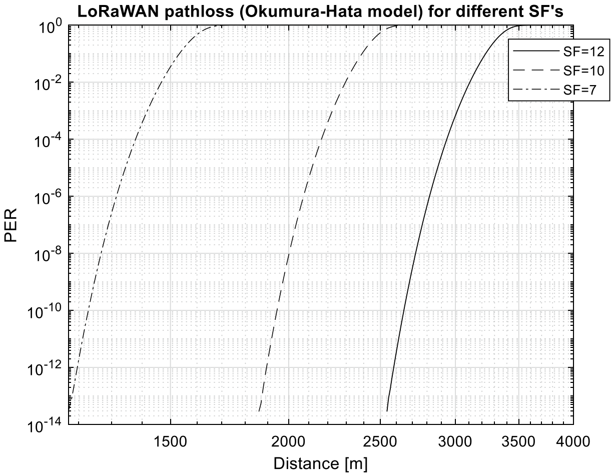

Fig. 3 Package error rate as a function of distance between the transmitting node and the gateway. Three curves are plotted for the spreading factors 7,10 and 12. It is noted that the Okumura-Hata model [13] is used to model the radio channel from a LoRaWAN gateway-receiver to a LoRaWAN local device (authors figure)

the jamming-power needed to overcome the wanted signal in decibel (dB). This parameter is a function of the distance between the wanted transmitting node (TN) and the gateway; and the distance between the transmitting jammer (TJ) and the gateway. By combining these parameters with the parameters in Table 1 an equation that describes the connection between jammer signal to noise ratio, PER and the distance between the jammer and the wanted transmitting node can be established. This equation is plotted in Fig. 4.

Focusing on the left most curve (solid line, Fig. 4) it presents the package error rate given that the distance between the jammer and the gateway is 500 m and the distance between the wanted transmitting node and the gateway is 2000 m (Fig. 5). This packet error rate will be used in the following example.

Assume a service scenario (Fig. 5) where a high PER (larger than 10^{-1}) is considered unacceptable. This could e.g., be a scenario where the streetlight in a smart city is controlled by a LoRa based system. Similarly, it is assumed that the jammers is positioned 500 m from the gateway (see Fig. 5).

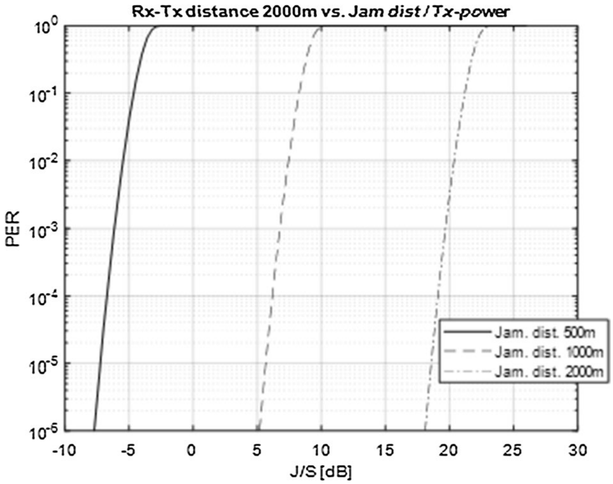

Fig. 4 Package error rate is given as a function of jamming to signal power (J/S) in dB. The three curves illustrate the package error rate as a function of J/S and the distance from jammer to the gateway. Note, it is assumed that the distance from the wanted node to the gateway is set to 2000 m (authors figure)

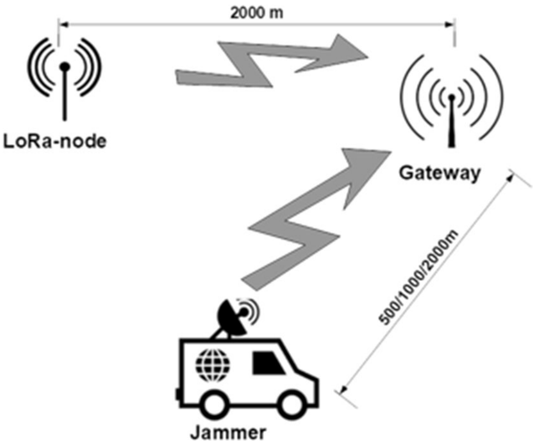

Fig. 5 A lora-node positioned 2000 m from the gateway is jammed by a jammer positioned either 500 or 2000 m away from the gateway (authors drawing)

By using the graph in Fig. 4 a J/S ratio of approximately -4 dB can be found. This means that the jammer only needs 40% (equal to -4 dB) of the power used by the wanted node. If it is assumed that the wanted node transmits with 14 dBm or approximately 25 mW the jammer only needs to transmit with 40 percent of this or approximately 10 dBm (10 mW). Similarly, it is noted that a jammer positioned at the same distance as the wanted node (right most dash-dot curve, Fig. 4) needs 21 dB more power compared to the wanted node. If it is assumed that the wanted node uses 14 dBm (approximately 25 mW) the jammer needs 35 dBm (approximately 3.2 W) to enforce a package error loss of more than 10^{-1}. This amount of power can easily be generated from e.g., a car battery, which means that the jammer can be mobile and thereby have the ability to shift position over time; however, the risk of being detected by an energy-based detector is considerable in this scenario, because the jammer needs to use a pretty high output power (3.2 W).

Another example scenario could be a service which requires a very low PER (less than 10^{-6}). Such a scenario could be a LoRaWAN based fire-alarm system. By using the distance parameters provided in Fig. 5 (jammer and wanted node distance is 2000 m from the LoRaWAN gateway node) it is possible to calculate the jammers probability for having a successful jamming scenario. Assuming that the wanted node transmits with 20 dBm (100mW) the jammer needs 18 dB (Fig. 4, right most curve) more power to jam the wanted node. Thus, the jammer needs 20 dBm + 18 dB which yields 38 dBm (approximately 6.3 W). Still, it is possible to feed the jamming transmitter from a car battery and thereby be able to move the jammer transmitter over time. However, this huge amount of power is easily detectable by an energy based jamming detector.

Without loss of generality, these formulas and figures, which has been derived from a mathematical model can be used to design new LoRaWAN based services which include security requirements such as acceptable package error rates, acceptable distances, and acceptable jamming prevention methods.

4 LoRaWAN—Proposed Prevention Strategies

As previously discussed, it is possible for a jammer with commercial-off-the-shelf (COTS) hardware to perform different types of DoS attacks such as continuous jamming, triggered jamming, and selective jamming [17, 18]. Continuous jamming means that the jammer transmits continuously with sufficient power to jam most of the IoT sensor nodes. This jamming type is easy to detect, spatially locate and prevent by changing the used frequency range or reallocate the gateways. Hence this jamming type will not be discussed further in this paper. Contrary to this, the two other jamming types are more sophisticated and challenging to deal with. The triggered jamming type detects the pre-ample in a frame transmitted from an IoT sensor node and then starts jamming that node. Similarly, selective jamming selects a particular IoT sensor node to be jammed, i.e., by watching the address in the frame transmitted from that IoT sensor node it can start jamming selectively]. This makes it much more difficult to decide if a technical problem has occurred or a jamming session is in play. It is noted that other jamming forms are possible by combining the discussed jamming principles.

Basically, the jammer must consider three elements to have success. These are window of opportunity, jammer signal strength, and channel hopping [19]. Regarding the window of opportunity, the airtime for a LoRa message is long compared with other similar radio systems. This makes the reaction time for the jammer longer, especially when it needs to detect a particular IoT sensor node address and start jamming that one. However, this jamming method leaves a trace, because it starts jamming after the address of the IoT sensor node has been received, i.e., the address is received correctly but the rest of the message is unreadable.

With respect to the jammer signal strength a certain amount of power is needed to overcome and mask the power used by the sending IoT sensor node. A clarification of this challenge is discussed in the previous chapter.

Finally, the jammer needs to overcome the frequency hopping used in the LoRa physical layer. This requires a multi-channel receiver like the ones used in the LoRa gateways. Nevertheless, this type of hardware is COTS and inexpensive, why this is a minor challenge for the jammer to overcome.

To be able to define some prevention strategies in relation to the jamming types discussed tomorrow's technologies need to come into play. One promising technology [14] is an intrusion, detection, and prevention system (IDPS) based on machine learning [20]. The difficulties in implementing such a system are extracting good usable features and getting sufficient training data. Extracting good features requires the LoRa gateways to be equipped with mechanisms/indicators that can provide these. Examples of good features are indicators that signal if:

- Part of a frame is received correctly, but the rest of the frame is unreadable.
- The field strength is abnormally high without any valid demodulation taking place.
- The field strength is above a certain threshold and the radio synchronization circuit is unable to unlock the framing.
- An invalid frame is received.

By using these features in combination with machine learning algorithms like a Neural Network (NN) abnormal situation can be detected with some probability. Another challenge is getting good training data which is a difficult task, however, it is possible to pre-train the NN algorithm by using simulators, where it is noted that the results achieved by pre-training can be improved by using reinforcement learning in the form of online learning.

5 Conclusion

The focus in this paper is on wireless jamming attacks that cause fatale Denial-of-Services on the LoRaWAN wireless infrastructure and connectivity. To set the scene, a highly relevant scenario is presented together with a discussion of the cost and impact of a DoS attack in this setting. In relation to this scenario, a simulation model has been designed and implemented to research and reveal the needed equipment to perform such an attack. Without loss of generality, the simulations performed on this model reveal that a successfully jamming attack can be performed by using cheap-of-the-shell hardware if the distance between the jammer and the LoRa-gateway is limited. Finally, it is concluded that the most optimal countermeasures involve tomorrow's technologies in the form of machine learning algorithms like neural networks. However, it is additionally stressed that this technology has downsides and challenges in the form of providing enough training data. More research is needed to research the optimal training procedure for this type of machine learning algorithm deployed in the settings of detecting jamming attacks.

Funding No external funding.

Data Availability Not applicable.

Code Availability Not applicable.

Declarations

Conflict of interest The authors have not disclosed any Conflict of interest.

References

1. Pégulu, M. (2020) Three 2020 predictions for LPWAN and IoT.
2. Pasqua, E. (2018) LPWAN emerging as fastest growing IoT communication technology – 1.1 billion IoT connections expected by 2023, LoRa and NB-IoT the current market leaders. Available: https://iot-analytics.com/lpwan-market-report-2018-2023-new-report/.
3. Tomic, I., & McCann, J. A. (2017). A survey of potential security issues in existing wireless sensor network protocols. *IEEE Internet of Things Journal, 4*(6), 1910–1923.
4. Pun˜al, O., Aguiar, A. & Gross, J. (2012). In VANETs we trust?: Characterizing rf jamming in vehicular networks. In *9th ACM international workshop on vehicular inter-networking, systems, and applications, ser. VANET '12*. New York, NY, USA: ACM (pp. 83–92). Available: http://doi.acm.org/https://doi.org/10.1145/2307888.2307903
5. Pelechrinis, K., Broustis, I., Krishnamurthy, S.V. & Gkantsidis, C. (2009). Ares: An anti-jamming reinforcement system for 802.11 networks. In *5th international conference on emerging networking experiments and technologies, ser. CoNEXT '09*. New York, NY, USA: ACM (pp. 181–192). Available: http://doi.acm.org/https://doi.org/10.1145/1658939.1658960
6. Shiu, Y.-S., Chang, S. Y., Wu, H.-C., Huang, S.C.-H., & Chen, H.-H. (2011). Physical layer security in wireless networks: A tutorial. *IEEE wireless Communications, 18*(2), 66–74.

7. Aras, E., Ramachandran, G. S., Lawrence, P. & Hughes, D. (2017). Explor- ing the security vulnerabilities of LoRa. In *3rd IEEE international conference on cybernetics (CYBCONF)*, June 2017 (pp. 1–6).
8. Proano, A. & Lazos, L. (2010) Selective jamming attacks in wireless networks. In *ICC. IEEE* (pp. 1–6).
9. Aras, E., Small, N., Ramachandran, G. S., Delbruel, S., Joosen, W. & Hughes, D. (2017). Selective jamming of LoRaWAN using commodity hardware. arXiv preprint arXiv:1712.02141.
10. Butun, I., Pereira, N. & Gidlund, M. (2018). Analysis of LoRaWAN v1.1 security, 2018. In *SMARTOBJECTS'18: 4th ACM MobiHoc workshop on experiences with the design and implementation of smart objects*, June 25, 2018, Los Angeles, CA, USA. ACM, New York, NY, USA.
11. Afisiadis, O., Cotting, M., Burg, A., & Balatsoukas-Stimming, A. (2020). On the error rate of the LoRa modulation with interference. *IEEE Transactions on Wireless Communications, 19*, 1292–1304.
12. Martinez, I., Tanguy, P. & Nouvel, F. (2019). On the performance evaluation of LoRaWAN under Jamming,2019. In *Proceedings of the 12th IFIP wireless and mobile networking conference, WMNC 2019.*
13. Haxhibeqiri, J., De Poorter, E., Moerman, I. & Hoebeke, J. (2018). A survey of LoRaWAN for IoT: From technology to application. *Sensors* (Switzerland).
14. Elshabrawy, T., & Robert, J. (2018). Closed-form approximation of LoRa modulation BER performance. *IEEE Communications Letters, 22*, 1778–1781.
15. Semtech Corporation, SX1272/3/6/7/8 LoRa Modem Design Guide, AN1200.13. (2013). *Semtech technique paper*.
16. Semtech Corporation, LoRa and LoRaWAN A Technical Overview. (2020). *Semtech technique paper*.
17. Areas, E. & Ramachandan, G. (2017). Exploring the security vulnerabilities of LoRa. https://www.researchgate.net/publication/318575428.
18. Yang X., Karampatzakis, E., Doerr, C., & Kuipers, F. (2018). Security vulnerabilities in LoRaWAN. In P*roceedings - ACM/IEEE international conference on internet of things design and implementation, IoTDI 2018*.
19. Aras, E., Small, N., Ramachandran, S. Gowri Sankar, R et al. (2017). Selective jamming of LoRaWAN using commodity hardware. In *ACM international conference proceeding series*.
20. Otoum, S., Kantarci, B. & Mouftah, H. (2018). Adaptively supervised and intrusion-aware data aggregation for wireless sensor clusters in critical infrastructures. In *IEEE international conference on communications*.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Dr. N. Prasad Ph.D., IEEE Senior Member, Director of CTIF-USA, Princeton, USA, leading IoT Test-bed at Easy Life Lab and Secure Cognitive radio network test-bed at S-Cogito Lab and Professor at International Technological University (ITU), San Jose, CA, USA. She received her Ph.D. from University of Rome ''Tor Vergata'', Rome, Italy, in the field of ''adaptive security for wireless heterogeneous network'' in 2004 and M.Sc (Ir.) degree in Electrical Engineering from Delft University of Technology, The Netherlands, in the field of ''Indoor Wireless Communications using Slotted ISMA Protocols'' in 1997. During her industrial and academic career for over 14 years, she has lead and coordinated several projects. At present, she is leading an industry-funded projects on Security and Monitoring (STRONG) and on reliable self-organizing networks REASON, Project Coordinator of European Commission (EC) CIP-PSP LIFE 2.0 for 65 ? and social interaction and Integrated Project (IP) ASPIRE on RFID and Middleware and EC Network of Excellence CRUISE on Wireless Sensor Networks. She is co-caretaker of real world internet (RWI) at Future Internet. She has lead EC Cluster for Mesh and Sensor Networks and Counselor of IEEE Student Branch, Aalborg. She is Aalborg University project leader for EC funded IST IP e-SENSE on Wireless Sensor Networks and NI2S3 on Homeland and Airport security and ISISEMD on telehealth care. She is also part of the EC SMART Cities workgroup portfolio. She joined Libertel (now Vodafone NL), Maastricht, The Netherlands as a Radio Engineer in 1997. From November 1998 until May 2001, she worked as Systems Architect for Wireless LANs in Wireless Communications and Networking Division of Lucent Technologies, Nieuwegein, The Netherlands. From June 2001 to July 2003, she was with TMobile Netherlands, The Hague, The Nether lands as Senior Architect for Core Network Group. Subsequently, from July 2003 to April 2004, she was Senior Research Manager at PCOM:I3, Aalborg, 82 P. M. Pawar et al. Denmark. Her publications range from top journals, international conferences, and chapters in books. She has also co-edited and co-authored two books titled ‘‘WLAN Systems and Wireless IP for Next Generation Communications’’ and ‘‘Wireless LANs and Wireless IP Security, Mobility, QoS and Mobile Network Integration,’’ published by Artech House, 2001 and 2005. Her research interests lie in the area of Security, Privacy and Trust, Management or Wireless and wired networks and Energy-efficient Routing.

P. Lynggaard (male) is a professor in internet-ofthings (IoT) and Artificial Intelligence (AI) at DTU. He holds a M.Sc. in EE and IT and a Ph.D. in artificial intelligence and Internet of Things from Aalborg University, Denmark. Today his research areas are IoT and AI and he is an expert in these areas including the subareas of digital signal processing, wireless sensor networks, wireless communication and security, and advanced analogue and digital electronics. Beyond the academic achievement he has a long track record from a professional industrial career (23 years) with focus on technical-scientific research, development, and implementation. He has received several honours and rewards during this period, and he has been headhunted several times. Over the years he has been involved in numerous research projects funded by the European Commission, the Danish state, etc.