LoRaWAN Performance Evaluation and Resilience under Jamming Attacks

Vaia Kalokidou, Manish Nair and Mark A. Beach
Communication Systems and Networks Group
University of Bristol, UK,
{Vaia.Kalokidou, Manish.Nair, M.A.Beach}@bristol.ac.uk

2022 Sensor Signal Processing for Defence Conference (SSPD) | 978-1-6654-8348-3/22/$31.00 ©2022 IEEE | DOI: 10.1109/SSPD54131.2022.9896225

***Abstract*— There is an increasing deployment of Internet-of-Things (IoT) networks, from smart meters and smart lighting to humidity soil sensors and medical wearable devices. Long Range (LoRa) is one such over-the-air (OTA) transmission IoT standard, having a wide range of applications in smart cities, agriculture and health. It facilitates the inter-connection of services and smooth exchange of information. However, owing to its wireless interface, it is susceptible, as all wireless networks are, to OTA attacks. In this paper, we initially obtain the Bit Error Rate (BER) and Packet Error Rate (PER) of LoRa, in order to investigate the impact of continuous and reactive jamming attacks on it. We show that overall, LoRa can achieve a good performance even under a jamming attack, subject to parameters such as the transmit power, the Spreading Factor (SF) and the Coding Rate (CR). Moreover, it is proven that the impact on BER and PER is similar irrespective of whether the attack occurs with total frame synchronization or is synchronized to after the preamble transmission. Lastly, we apply a detection scheme, based on previous values of Received Signal Strength Indicator (RSSI) and PER to successfully identify malicious attacks.**

Keywords—LoRa, LoRaWAN, PHY Security, Jamming.

I. INTRODUCTION

There is a wide deployment of Internet of Things (IoT) networks in smart cities/buildings, healthcare, and industrial applications. However, wireless networks in general are susceptible to cyber-attacks. Therefore, it is crucial to "build" secure and agile future networks by developing detection and defense mechanisms.

A well-known IoT technology is the Long Range (LoRa) standard, developed by Semtech. It has wide ranging use cases such as smart parking, waste management, smart meters, lighting, agriculture, healthcare, smart industrial control, supply chain and logistics [1]. In the UK, The Things Network (TTN) has been initially deployed in Cambridge and is expanding elsewhere. TTN is based on Long Range Wide Area Network (LoRaWAN) [2], a Low Power Wide Area Network (LPWAN) technology that operates on top of the proprietary LoRa protocol stack (originally developed to connect battery and low-power devices wirelessly to the internet) [2]. It constitutes a STAR network topology that uses gateway devices for receiving data from nodes and forwarding it onto LoRaWAN servers [3]. LoRaWAN allows geographically spread devices connectivity, securing bi-directional communication, mobility, and localisation services, and provides open-source software for hardware gateways and backend services [4].

LoRa features low-power operations, long range communications and low data rates. Table I provides an overview of LoRa specifications in Europe. Ten channels are defined in total, with eight having multi data-rate of 250bps-5.5Kbps, a single channel with high data rate (11Kbps), and a single Frequency Shift Keying (FSK) channel at 50kbps [3]. As LoRa is an over-the-air (OTA) transmission standard, it is susceptible to cyber-attacks. There are two levels of security in LoRa: (a) network level security (authentication of node, providing integrity between the device and the network server - NwkSKey), and (b) application layer security (confidentiality with end-to-end encryption between the device and the application server - AppSKey) [4]. Most important identified LoRa vulnerabilities are related to the encryption keys, which are the key to attack the network once compromised [3,4].

Table I. LoRa Specifications (Europe).

Parameter	Values (approx.)
Frequency	868-870 MHz
Bandwidth	(UL) 125/250 kHz
	(DL) 125 kHz
EIRP	max 20dBm
Link Budget	155 dB
Spreading Factor	7-12
Data Rate	250bps – 50kbps
Battery Life	106 months (2000mAh)
Coverage	(urban) up to 5km
	(rural) up to 15km

State-of-the-art research has shown that additional security can be attained by employing physical layer (PHY) security. In general, PHY security entails: information-theoretic security, artificial noise aided security, security-oriented beamforming techniques, diversity-assisted security approaches, and physical-layer secret key generation [1,2]. The latter has gained a lot of attention in the LoRa standard. In [3], authors investigate the employment of different algorithms based on PHY key generation to a LoRaWAN network, looking at both static and mobile scenarios, achieving 13Mbit/s and 21Mbits/s key establishment rates. Moreover, [4] presents indoor and outdoor LoRa network experiments on secure key generation achieving higher key establishment rate of 31Mbits/s in mobile scenarios. In [5], the authors show that wireless key refreshment is feasible even in cases where an eavesdropper is close to the legitimate

978-1-6654-8348-3/22/$31.00 ©2022 IEEE

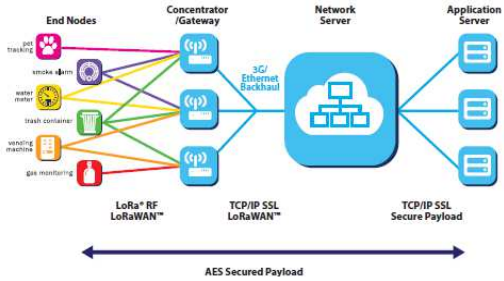

Fig. 1 LoRaWAN Architecture [6].

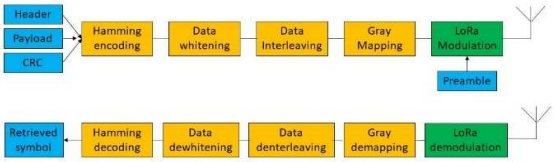

Fig. 2 LoRa PHY.

Fig. 3. LoRa frame format.

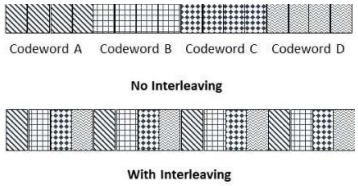

Fig. 4. Example of Bit Interleaving.

nodes. Interestingly enough, [3] presents a Machine Learning approach on generating security keys by converting wireless signals into structured datasets. In [4], PHY key generation is employed to LoRaWAN by using differential equations to achieve a great degree of randomness.

In this paper, we aim to initially evaluate the performance of LoRa, by building a LoRa-like Matlab simulator. Performance results are benchmarked to published results [5] to ensure the correct operation of our simulator. Then, we investigate the impact of various jamming attacks on the performance for different Spreading Factors (SF) and Coding Rates (CR). A detection mechanism is then applied, based on setting a threshold, related to Packet Error Rate (PER) and Received Signal Strength Indicator (RSSI), that provides the LoRa-like simulator with the opportunity to correctly identify a potential threat, i.e., jamming attack.

This paper is organised as follows: Section II presents the generic LoRa architecture, the PHY and the frame format, as well as the working specifications of the LoRa simulator developed in the University of Bristol. Section III gives an overview of performance results, starting from mean Bit Error Rate (BER) and PER under normal operation, and then analysing the performance impact of different jamming attacks. Finally, Section IV discusses the results of our research along with recommendations for future work.

II. LoRa PHY

A. Architecture

In a LoRa-LoRaWAN network, as depicted in Fig. 1, the end nodes, for e.g., smart meters, communicate with the gateways via the LoRa PHY. The gateways are connected to the network server via 3G/Backhaul Ethernet, and the network server communicates with the application server based on the TCP/IP SSL secure payload. Our focus in this paper falls on the connectivity between the end-nodes and the gateways, as we investigate LoRaWAN from the PHY layer perspective (LoRa).

LoRaWAN uses three different classes of devices to trade off network downlink (DL) communication latency against battery duration and optimise performance [3]. Class A entails bi-directional end-devices, whose UL transmission is followed by two short DL receive windows [3], based on ALOHA-type of protocol. This is the lowest required power class for applications that only require DL communication from the server shortly after the UL transmission. Class B comprises of bi-directional end-devices that require scheduled receive slots, allowing the server to identify active end-devices that are listening. Finally, bi-directional end-devices with maximal receive slots fall into the Class C category, with devices almost constantly opening receive windows [3]. In this Section, we focus on the LoRa PHY standard, discussing the frame format, the encoding and decoding process, and the modulation/demodulation employed by the standard. Since LoRa is a proprietary standard, the description of LoRa architecture and operation is based on research papers, online available material and reverse engineering results.

Overall, the LoRa PHY architecture is depicted in Fig. 2. It should be noted that some sources [6] define that data-whitening proceeds Hamming encoding. As shown in Fig. 2, there are four distinct operations comprising the LoRa encoding: (a) Hamming encoding, which adds parity bits, (b) data-whitening, which provides de-correlation of data, removing DC-bias in the transmitted data, (c) bit-interleaving, which scrambles bits to provide better immunity to burst errors (fading), and (d) gray-mapping, which reduces errors in adjacent bits by making adjacent symbols in the original representation only differ by one bit in the gray representation [6].

Encoding is followed by modulation. The LoRa standard uses Chirp Spread Spectrum (CSS) modulation. CSS modulation uses wideband frequency modulated chirp pulses to encode data. A chirp refers to a sinusoidal signal that increases/decreases in frequency over time.

The input symbol is spread on different frequencies and different time instances. The value of the SF, which takes values from 7 to 12, denotes the number of raw bits that can be encoded by the symbol and all the possible chip values (2^{SF}). The number of samples for every input symbol is given by the sampling frequency divided by the symbol rate, and for each sample the symbol value is cyclically shifted. To encode a LoRa symbol S in a chirp, a starting offset is added to the frequency sweep. The starting offset is given by [6]:

$$f_{offset} = \left({Bwth}/{2^{SF}}\right) S, \text{ where } \quad S \in [0, 2^{SF} - 1]. \qquad (1)$$

The bandwidth is restricted to $\left(f_c - {Bwth}/{2}, f_c + {Bwth}/{2}\right)$, and thus, the instantaneous frequency is linearly increased to the maximum frequency ($f_c + {Bwth}/{2}$), and then wrapped to the minimum frequency ($f_c - {Bwth}/{2}$). The instantaneous

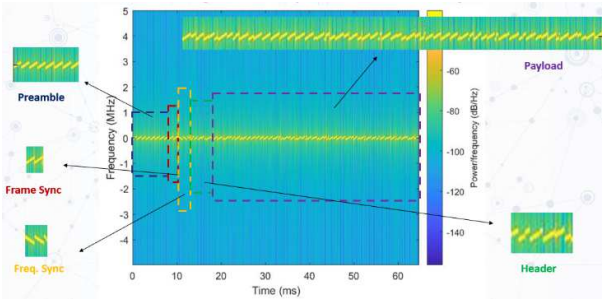

Fig 5. LoRa I/Q symbols for SF=7 and CR=4.

Fig. 6: LoRa network with one jammer attempting to attack the network.

frequency of the LoRa symbol S at time t, with $t \in [0\ T_s]$ and T_s denoting the symbol period, is given by [10]:

$$f_s(t) = S\frac{Bwth}{2^{SF}} + \mu\frac{Bwth}{T_s}t \ \ (mod\ Bwth), \qquad (2)$$

where μ defines if we have an upchirp ($\mu = 1$) or a downchirp ($\mu = -1$).

Demodulation and extracting symbols in a LoRa packet requires: (a) channelising and resampling the signal to the chirp bandwidth, (b) de-chirping with a locally generated signal, (c) taking the Fast Fourier Transform (FFT) of the de-chirped signals (where the number of FFT bins equals the spreading factor), and (d) extracting the maximum value from each FFT to obtain the symbol. Accurate synchronisation on the Start Frame Delimiter (SFD) is essential for demodulation. This is because incorrect synchronisation can spread the symbol energy between adjacent FFTs, resulting in incorrect demodulation. Lastly, the receiver performs synchronisation and frequency-offset estimation and compensation prior to demodulation. More details on the operation of the aforementioned blocks are given in Section II.B, with regards to the LoRa simulator developed in Matlab. Lastly, Fig. 3 depicts the LoRa frame format.

B. LoRa-Like Simulator

A LoRa-like simulator is developed using Matlab, partially based on the work presented in [5]. The frame consists of 8 symbols in the preamble, 2 symbols in the frame synchronisation field and 2.25 symbols in the frequency synchronisation field, 7 symbols in the header, variable length payload filed (depending on the simulation), and a 2-byte CRC field.

1) LoRa Encoding

The input data is randomly generated in binary format and converted to decimal (and back) depending on the stage of the encoding:

a) Hamming Encoding: Hamming codes (HC) belongs to the family of cyclic redundancy codes that check the integrity of the received message. A hamming encoder adds a number

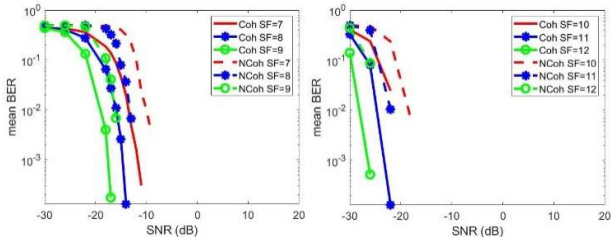

Fig. 7: Mean BER for CR=1 and (left) SF=7,8,9, (right) SF=10,11,12.

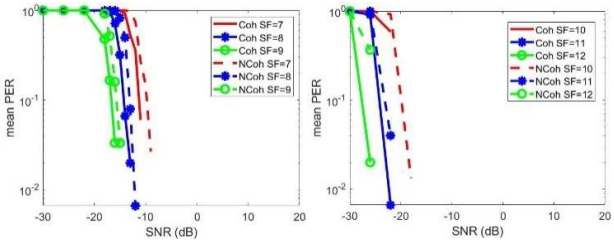

Fig. 8: Mean PER for CR=1 and (left) SF=7,8,9, and (right) SF=10,11,12.

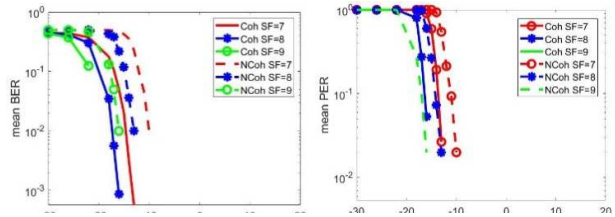

Fig. 9: Performance for SF=7,8,9 and CR=4 and (left) BER, (right) PER.

of parity bits that helps to detect and/or correct errors at the receiver during decoding. In LoRa, four CRs are available: a) 4/5 (simple parity check), b) 4/6 (shortened HC), c) 4/7 (common HC), and d) 4/8 (extended HC), with the first two CRs providing only error detection and the last two able to support error correction as well.

b) Data Whitening: During the data whitening, the transmitter XORs the transmit frame with a pseudorandom sequence, and the receiver XORs the received frame with the same sequence. Randomising data in this way attains receiver synchronisation similar to Manchester coding. However, unlike Manchester coding, it provides the advantage of keeping the same data rate at the cost of not having the guarantee of removing any DC-bias albeit with a very high probability of removing it [6].

c) Bit-Interleaving: Interleaving is a very-well known process in communications systems. The aim is to spread the bits comprising a codeword between multiple symbols. There are several ways of scrambling data during interleaving. Most sources in LoRa are not specific on the kind of interleaving employed. In our simulator, we perform simple interleaving by taking the transpose of the original data whitened matrix and mixing bits as shown in the Fig. 4. Reverse engineering work performed claims to have identified a special way of interleaving data in LoRa, based on using diagonals to scramble the bits [6].

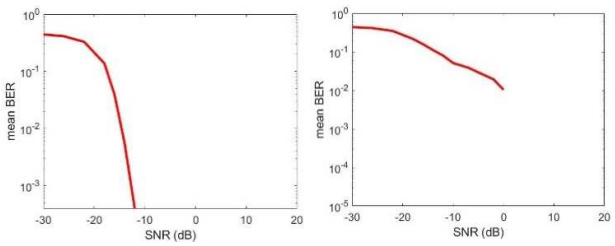

Fig. 10. BER (left) no jamming, and (right) with CW jamming.

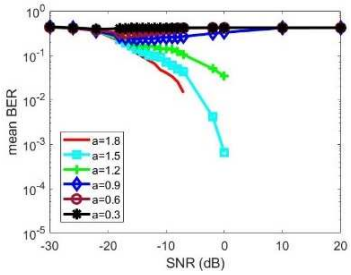

Fig. 11. Reactive jamming: Mean BERs for SF=7 and CR=1

d) Gray Mapping: In general, gray-mapping entails the mapping between a symbol, in any numeric representation, to a binary sequence. The input to the gray-mapper is XOR'd with a shifted version of itself. The Gray code we apply is given by $C_n = B_n \; XOR \; (B_n \gg 1)$ where B_n is the left most significant bit binary representation of n. On top of the mapping, a shift of -1 is used. At the receiver, a reverse to the encoding process is applied in order to retrieve the original symbols.

2) LoRa Modulation/Demodulation

The input to the modulator is a vector containing decimal values from $[0, \cdots, 2^{SF} - 1]$. The modulation process follows the steps defined in Section IIB. For every symbol (decimal value), there are N_s samples. Once the instantaneous frequency is chosen (2), the instantaneous phase of the LoRa symbol S at time t ($t \in [0\ Ts]$) is calculated:

$$\theta_s(t) = 2\pi f_s(t)t \tag{3}$$

Lastly, the complex LoRa symbol at time t ($t \in [0\ Ts]$) is given by:

$$s(t) = cos\theta_s(t) + jsin\theta_s(t) \tag{4}$$

At the demodulator, a default sequence of all zeros is CSS modulated and multiplied by the received sequence, separately for the preamble, and separately for the header/payload field. Then, having a choice between non-coherent and coherent detection, the data is demodulated. In the case of non-coherent detection, the maximum of the FFT window is taken. When coherent detection is active, then the resulting data is convolved with an ideal FSK signal, and the maximum real value is chosen. As shown in Section III, coherent detection offers a better performance. The I/Q LoRa, for the case of SF=7 and CR=4, are depicted in Fig. 5.

3) LoRa Cyclic Redundancy Code (CRC)

CRC is available only at the UL and has a size of 2 bytes. It belongs to the family of block codes and is applied to detect changes (errors) to the transmitted data. It entails a binary

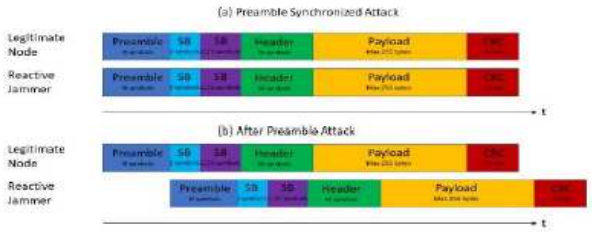

Fig. 12. Schematic of a preamble related attack.

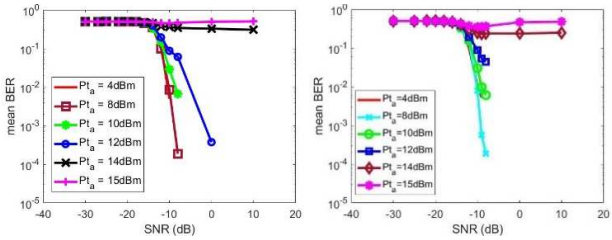

Fig. 13. Jamming Preamble BER (SF=7, CR=1), (left) total sync, (right) attack after preamble.

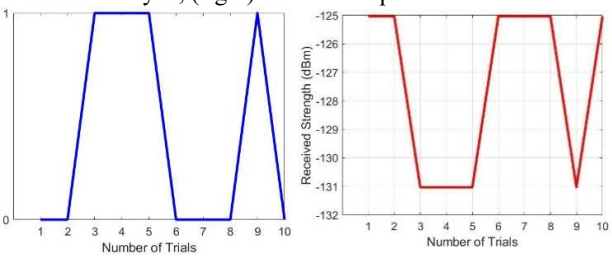

Fig. 14. Reactive jamming detection with RSSI and PER threshold. A set of attack-sessions denoted by 1 (left) mixed with no attack-sessions denoted by 0 (left) are simulated.

division of the actual data by a predetermined divisor, generated using polynomials. Based on [6], the polynomial used in LoRa is given by

$$x^{16} + x^{12} + x^5 + 1. \tag{5}$$

Moreover, findings in [3] show that the CRC bytes in the payload are not taken into account in the CRC calculation, but they are used as the final XOR value.

III. LoRa System Performance

LoRaWAN performance results are captured from several Matlab simulations in terms of the Bit Error Rate (BER) and Packet Error Rate (PER). The length of the payload is set to 17 bytes with all other fields in the frame having a pre-fixed length according to simulator definition parameters given in Section IIB. We consider one LoRa sensor transmitting to a gateway, and one jammer attempting to intrude the network, as depicted in Fig. 6. Unless stated otherwise, the transmit power at the legitimate node is set to 12dBm.

A. LoRa General Performance

We consider transmission over an Additive White Gaussian Noise (AWGN) channel

$$y(t) = s(t) + z(t) \tag{6}$$

where $y(t)$ is the received signal at the gateway, $s(t)$ is the CSS modulated LoRa signal transmitted by the LoRa sensor, and $z(t)$ represents the AWGN, with $z \in \mathcal{CN}(0, \sigma^2)$. We consider both coherent and non-coherent detection. Fig. 7 (left) presents the BER for a rate code ($RC = \frac{CR}{CR+1}$, where CR

is the coding rate) of 4/5 (i.e., CR=1), and all available SFs, i.e., SF=7-12. For the same specifications, Fig. 7 (right) depicts the respective PER. Fig. 8 depicts the mean BER and PER for a coding rate 4/8 (i.e., CR=4) and SF=7,8,9. Overall, it can be observed that the higher the SF, the better the BER and PER. This is because higher SFs attain higher symbol energy. Moreover, as we switch from CR=1 to CR=4, an improved BER performance can be observed, as expected. It should be noted that our results are aligned with published results in [5], thus validating the accuracy of our LoRa-like simulator, using similar parameters. It can be observed that Fig. 8 (left) attains similar PER as in Fig. 9 for SF=7,8,9 as in [5].

B. LoRa Performance Under Attack

There are various types of attacks that can be anticipated in a LoRa network. Investigation is performed on two types of jamming: (a) continuous jamming, where the jammer continuously transmits independently of whether a legitimate transmission takes place or not, and (b) reactive jamming, where the jammer attempts an attack only when they sense a legitimate transmission [2]. Initially, the case of having a continuous jammer is simulated. Assuming that the attacker transmits an asynchronous continuous wave (CW) signal at 868MHz over an AWGN channel for SF=7 and CR=1, the degradation in performance is depicted in Fig. 10. As compared to the case without jamming, for asynchronous jamming, a much higher SNR is required to maintain the same BER. For example, whilst a mean BER of 10^{-3} is attained at an SNR of -10dB under normal LoRa operation (Fig. 10 left), at similar SNRs, the BER degrades by two orders of magnitude to 10^{-1}) under asynchronous CW jamming (Fig. 10 right). Moreover, considering reactive jamming, the received signal at the gateway is given by

$$y(t) = s_l(t) + s_\alpha(t) + z(t) \quad (8)$$

where $y(t)$ is the received signal at the gateway, $s_l(t)$ is the CSS modulated LoRa signal transmitted by the legitimate LoRa sensor, $s_\alpha(t)$ is the CSS modulated LoRa signal transmitted by the attacking node and $z(t)$ represents the AWGN. For SF=7, Fig. 11 shows the mean BER for the case of CR=1. The ratio of the legitimate node's transmit power over the power of the attacker is denoted by α. It can be observed that for $\alpha < 0.9$, the system breaks, i.e., packets cannot be transmitted correctly.

Lastly, we consider the case that a reactive jamming attack is performed either in total frame synchronisation between the attacker and the legitimate node, or right after the end of the preamble transmission from the legitimate node's end, as described in Fig. 12. For SF=7 and CR=1, the comparison between the two cases is depicted in Fig. 13. Taking Pt_a as the transmit power of the attacker varying from 4dBm to 15dBm, with the legitimate node having a transmit power of 12dBm, we can observe that when the attacker transmits at 13dBm or lower, a good BER can be achieved. Furthermore, no major difference, on the performance, is observed if there is no total synchronisation between the transmissions of the attacking and the legitimate node.

C. LoRa Detection of Attacks

One of the most popular detection mechanisms against cyber-threats is the establishment of a threshold, typically related to RSSI and PER, based on their values from previous observations. This method is particularly suitable for networks in environments that are highly static or with slow changes (e.g., static sensor in a rural area) where severe changes in the environment are not anticipated allowing the setting of a threshold to detect any threats on the network.

We have chosen to set both an RSSI and a PER threshold. For SF=7 and CR=1, the values of the thresholds, based on previous observations (i.e., extensive simulations), were taken as -126dBm for the RSSI case, and 0.001 for the PER case. Again, for a payload length of 17 bytes and reactive jamming on the network, a set of attack-sessions (denoted by 1) mixed with no attack-sessions (denoted by 0) are simulated (10 trials overall) to observe if attacks can be identified on both metrics. The sequence of events was 0011100010. As shown in Fig. 14, attacks were correctly detected. Moreover, for each event the corresponding RSSI value is depicted.

IV. CONCLUSIONS

In this paper, we modeled transmissions between LoRa nodes and gateways. BER/PER under normal operation is assessed. Multiple jamming attacks were performed to study the networks' performance under their impact. Asynchronous continuous jamming had an impact on the performance, however, transmissions were still possible. It was shown that the performance variation between attacking the network with total synchronisation and attacking it after the preamble transmission was not substantial. In the case of reactive jamming, if the transmit power of the jammer was not considerably higher than that of the legitimate node, good BERs were attained. An RSSI and PER threshold were employed to successfully detect any possible threats. For future investigation, we propose using RSSI values to 'train' the LoRa network and apply PHY key generation exchange between the legitimate nodes to secure the network against malicious attacks

ACKNOWLEDGMENT

This research is funded through the UKRI/EPSRC Prosperity Partnership in Secure Wireless Agile Networks (SWAN), (EP/T005572/1), https://www.swan-partnership.ac.uk/

REFERENCES

[1] E. Aras, et. al., "Exploring The Security Vulnerabilities of LoRa", IEEE Conference on Cybernetics, June 2017

[2] Y. Zen, X. Wang, L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances and Future Trends", Proceedings of the IEEE, vol. 104, no. 9, pp. 1727-1765, Sept. 2016.

[3] T.M. Hoang, et. Al., "Physical Layer Security: Detection of Active Eavesdropping Attacks by Support Vector Machines" IEEE Access, vol. 9, pp. 31595-31607, Feb. 2021.

[4] J. Zhang, A. Marshall, L. Hanzo, "Channel-Envelope Differencing Eliminates Secret Key Correlation: LoRa-Based Key Generation in Low Power Wide Area Networks", IEEE Transactions on Vehicular Technology, vol. 67, no. 12, pp. 12462-12466, Dec. 2018.

[5] [B. Al Homssi, et. Al., "IoT Network Design using Open-Source LoRa Coverage Emulator", IEEE Access, vol. 9, pp. 53636-53646, April 2021.

[6] T, Joachim, "Complete Reverse Engineering of LoRa", EPFL, Telecommunications Circuits Laboratory, Lausanne.

[7] M. Chiani, A. Elzanaty, "On the LoRa Modulation for IoT: Waveform Properties and Spectral Analysis", IEEE Journal on Internet of Things, vol. 6, no. 5, pp. 8463-8470, May 201