Detection of Mobile LoRa Jammers

Bleszynski, Bartlomiej Jozef; Orfanidis, Charalampos; Fafoutis, Xenofon

Published in:
Proceedings of the IEEE Virtual Conference on Communications 2023

Link to article, DOI:
10.1109/VCC60689.2023.10474753

Publication date:
2024

Document Version
Peer reviewed version

Detection of Mobile LoRa Jammers

Bartlomiej Jozef Bleszynski, Charalampos Orfanidis, Xenofon Fafoutis
Department of Applied Mathematics and Computer Science, Technical University of Denmark (DTU), Denmark
{s182182, chaorf, xefa}@dtu.dk

***Abstract*—Low Power Wide Area Networks (LPWANs) platforms (LoRa, NB-IoT, Sigfox) came to add a missing piece to the Internet of Things (IoT) ecosystem, namely long range communication in low power. LPWAN platforms are characterized by low data rate and long transmission time. LoRa specifically, has a data rate from 27 to 0.3 kbps and the transmission time of a single packet might be more than 1.5 seconds for some cases. These characteristics render LPWANs vulnerable to jamming attacks as a malicious user can perform a jamming attack from long range and the long transmission time is allowing a large time window to perform the attack. Moreover, if the jamming node is mobile (*i.e.,* attached on a vehicle or an Unmanned Aerial Vehicle (UAV)), the current countermeasures proposed by the literature will not be relevant anymore. In this paper we investigate if it is possible to detect a mobile LoRa jammer based on the impact of the Doppler effect and based on a combination of signal strength and the entropy of the transmitted data. The results, obtained by utilizing commercial hardware, reveal that we could detect a potential mobile jammer that follows a deceptive jamming strategy with random payload, but further investigation is required for more sophisticated jamming attacks.**

***Index Terms*—Internet of Things, LoRa, Mobile Jamming**

I. Introduction

Low Power Wide Area Networks (LPWAN) [1] enriched the Internet of Things (IoT) [2] ecosystem with a feature that was missing so far, namely long-range communication in low power. Platforms like LoRa [3], NB-IoT [4], Sigfox [5] and many more emerged, enhancing the application scenario domain. Smart cities [6], precision agriculture [7], livestock monitoring [8] are some of the most popular applications based on LPWAN.

LoRa is one of the most popular LPWAN platforms due to the fact that it's able to achieve robust, long-range communication in low power [9]. LoRa PHY was designed to be functional even with low levels of sensitivity and be resilient to external interference from other networks [10]. This is achieved by using a chirp spread spectrum modulation, which has been proven robust to noise. Even though the signal modulation of LoRa made it a successful solution for several applications, at the same time the long range transmissions and the long time-on-air, made it a subject for potential jamming attacks [11]. Furthermore, the only feature LoRa has to check the channel before transmitting a packet to avoid collisions is called Channel Activity Detection (CAD), but it is able to detect only modulated LoRa signals. Therefore, any other modulated signal different than LoRa or unmodulated signal can collide with LoRa. Hence, a malicious user may use low cost, commercial hardware, to perform jamming attacks from a long distance. Given the long time-on-air values, it is available a large time window (sometimes longer than 1,5 seconds) to jam a LoRa packet or a part of it. Even though LoRa has been proven robust to noise, however if a large percentage of the transmitted packet is subjected to noise, the packet will be corrupted [10], [12].

The jamming attacks have been investigated already and the conclusions illustrate that LoRa can be vulnerable to jamming attacks [11]. The proposed countermeasures are based on detecting the difference of the transmission power between a legitimate user and a malicious one, using multiple gateways or increasing the SF value of LoRa. All these solutions are not viable when a jamming node is mobile because the transmission power level of the mobile attacker will be variable. Furthermore prior investigations of mobile jamming attacks to other networks [13] should be investigated further because LoRa has different physical characteristics (*i.e.*, lower sensitivity, different modulation). To this end we explore if we can detect mobile LoRa jammers based on the Doppler effect caused by a mobile LoRa transmission and the variable transmission power of the attacker combined with the entropy of the payload.

The rest of the paper is organized as follows: Section II briefly introduces LoRa, LoRaWAN and jamming attacks on LoRa. Section III describes the state of the art, Section IV presents the adversary model and the setup we use. Section V illustrates the Doppler based approach, Section VI shows the approach based on the transmission power and the entropy of the data. Finally Section VII concludes the paper.

II. Background

This section describes the technical details of LoRa and LoRaWAN networks which are relevant to security vulnerabilities and more specifically to jamming attacks. In addition, the section presents available techniques to perform a jamming attack to LoRa.

A. LoRa

LoRa is a long range and low power communication technology, able to achieve robust performance. It is based on a Chirp Spread Spectrum (CSS) modulation technique, developed by Semtech in 2015 [14]. CSS is based on chirp signals which are frequency modulated pulses. The LoRa radio has several configuration parameters which affect aspects like the sensitivity, communication range and the time-on-air of a packet [15].

LoRaWAN is the Media Access Control (MAC) protocol that is used on top of LoRa technology. LoRaWAN implements

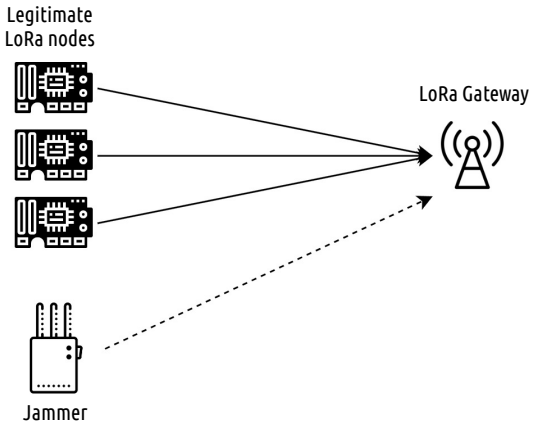

Fig. 1. A deceptive LoRa jammer attacks hampers the communication of legitimate LoRa nodes by transmitting valid LoRa packets continuously.

all the useful features a MAC protocol offers, including addressing, cryptography, transferring data to higher layers and many more. It is organized in star architecture in which all end-devices communicate directly with a LoRa gateway. LoRaWAN classifies the end-devices into Class A, Class B and Class C. We will focus on Class A devices since it has the lowest power consumption and we target more on low power application scenarios.

B. Jamming LoRa

Jamming attacks have been studied extensively for wireless networks and IoT [16], [17] and there are several variations of the jamming attack depending the targeted wireless technology (*i.e.,* Wi-Fi, Bluetooth, Zigbee). LoRa has different characteristics from the previous wireless technologies and it is important to mention which variations of the jamming attack might pose a threat to LoRa networks. For instance, a *constant* jammer might emit demodulated carrier continuously to generate interference and block the communication. This is effective but also easy to detect the attack and identify the location of the attacker, assuming that it is stationary. The *deceptive* jammer is the same with the constant but instead of unmodulated carrier it transmits legitimate packets to pretend that there is a high traffic scenario. An advanced variation is the *random* jamming attack which includes a duty cycle where the attacker sleeps and wakes up to jam the medium with unmodulated carrier to conserve energy. The *reactive* jamming attack is listening to the channel for a potential activity and if if detects a transmission, it emits unmodulated carrier to jam it. In this paper we will focus on the deceptive jamming attack as it is illustrated in Figure 1.

III. Related work

This section presents the current research studies on jamming LoRa networks and their countermeasures. Aras et al. analyzed the LoRa network stack focusing on its vulnerabilities and different types of attacks, a malicious user may perform, using off-the-shelf hardware [18]. The authors are demonstrating that LoRa networks can be susceptible to jamming attacks or selective jamming attacks [12] which are more advanced as the jamming starts only after the legitimate transmission is initiated. The countermeasures proposed, to switch the transmission frequency, use the channel hopping feature and increasing the SF value to increase the sensitivity. Synchronized jamming chirps attack is able to harm the LoRa PHY [11]. More specifically, if a malicious user is able to align jamming chirps with legitimate ones using high signal strength, LoRa gateways are not able to distinguish the jamming from the legitimate ones. The authors also mention that frequency domain and collision recovery solutions are not able to cope with this vulnerability and they propose a countermeasure which is leveraging the difference in signal strength to distinguish the attacker from the legitimate user. The jamming attack on LoRa is also investigated in [19] where the authors focus on the orthogonality property of LoRa. Therefore, the authors use commercial LoRa devices to demonstrate that jamming attacks with specific LoRa Radio Frequency (RF) combinations are able to corrupt LoRa transmissions, even with low power. [20] proposes an Intrusion Detection System (IDS) to detect jamming attacks for LoRaWAN. More specifically, two methods are used to detect a potential jammer during the LoRaWAN joining procedure, one based on Kullback Leiber Divergence and one based on the Hamming distance and both methods achieve over 87% detection rate. [21] takes advantage of the CAD and the channel hopping feature to conduct jamming attacks on LoRaWAN networks using commercial hardware. The authors propose multiple gateways deployment and using the frequency hopping feature for the legitimate transmissions can reduce the success rate of the jamming attacks.

No matter the variation of jamming attack towards LoRa, if the jammer is mobile it would be difficult to be identified. Solutions based on differentiating signal strength assume that the signal power of LoRa chirps from the same packet would remain stable. Detecting mobile jammers for cellular networks based on the Doppler frequency shift has been proposed in [13], but LoRa operates with significantly lower Signal to Noise Ratio (SNR) since it is designed to operate with lower sensitivity. Therefore it is not certain if the same approach applies there. Mobile LoRa jamming is posing new challenges which this paper attempts to identify and tackle.

IV. Adversary Model

System Model: We consider a smart metering application scenario based on LoRaWAN technology [22]. We assume that the end devices are Class A, they are deployed across a city and they are reporting power consumption values in order to allow a power provider to remotely and timely obtain the user consumption and allocate the resources efficiently. We assume that the end-nodes execute LoRaWAN 1.1 [23] and Advanced Encryption Standard (AES). Note that the LoRaWAN duty cycles regulations are not followed (by the legitimate node) for practical reasons.

Attacker model: The deceptive jammer transmits legitimate LoRaWAN packets with random data, at very frequent random

points to corrupt the communication. The attacker is mobile and moves with a car within the allowed speed limits in residential areas (0 - 50 km/h in Denmark). The attacker does not possess any cryptographic keys or other data that is marked as protected in the LoRaWAN specification, thus they are not able to break any cryptographic mechanism. The attacker uses commercial LoRa hardware and its transmissions are within the allowed transmission power described by the radio specifications (20 dBm maximum).

A. Implementation

This section provides an overview of the hardware and software we used to implement a testbed in order to imitate the jamming attacks and store the required data to evaluate our hypothesis.

We use commercial and low-cost hardware to provide a solution for a large scale deployment aligned with the IoT and LoRa ecosystem. More specifically, we used the ESP32 microcontroller with the SX1276 chip as a LoRa node. We also used a Software Defined Radio (SDR), which is a repurposed USB DVBT receiver, based on common baseband IC RTL2832 and IQ mixer Fitipower FC0012. The LoRa nodes are running the FreeRTOS [24] Operating System (OS) in combination with the ESP32 LoRa library [25]. The LoRaWAN features are not supported in the current library but we implemented manually the structure of a LoRaWAN packet to represent the corresponding time-on-air values which are relevant to the evaluation. The SDR used the GNU Radio [26] software to capture the raw base-band signal data.

The testbed consisted of three LoRa nodes in total, the SDR module and a Global Positioning System (GPS) application running on a smartphone. Specifically, a LoRa node is deployed by the window of a campus building, acting as a LoRa gateway (GW) and next to it is deployed the SDR to capture the channel activity. Then in a distance of 20 meters in the same building but in a different room, it is deployed another LoRa node representing the legitimate transmitter. The third LoRa node is deployed on the windshield of a car along with a GPS, to capture speed, location, and distance data. The configuration of LoRa nodes is SF 10, BW 125 kHz and TX power 17 dB. The legitimate transmitter is sending a packet of 18 B every 300 ms and the jammer a packet of 10 B every 60 ms. The different size of packets was used to label the packets accordingly during the evaluation. The frequency span for the SDR is $22 - 948.6$ MHz, the max sampling rate is 3.2 MS/s, the max sampling rate without sample loss is 2.4 MS/s and the ADC resolution is 8 bit I/Q. The car with the jammer was moving within the range of of the gateway with a maximum distance 1.02 km, to imitate the mobile jammer. The duration of the experiment was 30 minutes but we illustrate a part of it in the results for practical reasons.

V. Doppler based detection

This section illustrates the attempt to detect a mobile LoRa jammer based on the Doppler effect generated during its mobilization. Any radio signal that is transmitted from a moving transmitter or received by a moving receiver is susceptible to the effect called Doppler shift. This phenomenon is more visible when the carrier frequency is relatively high. High frequencies are used in radio-location to make the Doppler effect more distinctive and by that to determine whether a signal is reflecting off a static or a moving object. In the case of LoRa transmissions, which are mostly limited to the sub-GHz band, the effect is still present but less visible. A similar principle based on the Doppler shift can be applied to the detection of mobile LoRa jammers.

The aforementioned approach is evaluated both theoretically and then experimentally. An analysis conducted using a motion detection algorithm based on a signal generated in a simulator, to which a Doppler shift was added artificially. Then we tried to verify the theoretical results based on a real radio signal data recorded by the SDR.

Formula 1 shows what Doppler frequency is expected to be for a moving transmitter. V_{object} is a radial speed of a jammer toward a receiver, c_0 is the speed of light and $f_{carrier} = 915$ MHz. Table I shows Doppler shift frequencies for potential vehicle speeds. Observing Table I, we can see that the Doppler frequency for speeds, common in urban traffic, is quite low.

$$f_{doppler} = \frac{V_{object}}{c_0} f_{carrier} \tag{1}$$

To examine if this possible to be detected, we artificially generated a LoRa signal in MATLAB simulator based on [27]. Thus, 200 packets were generated with a period of 8.2 ms, with SF 10 and BW 125 kHz. Then we artificially distort the generated signal to represent the Doppler shift, using Frequency Domain Shift which is a property from the Fourier Transform. The range of the Doppler shift is 0 to 50 Hz which corresponds roughly to a speed range of 0 to 60 km/h. Next we applied a Fast Fourier Transformation to obtain the beat frequency. Figure 2 presents the shifted frequency which is in steps instead of a more linear trend. This is due to the limited frequency resolution of the Fourier transform, which is called a frequency bin. The Δf difference demonstrates that when a LoRa radio is mobile, it generates a Doppler shift which is able to be detected. Another observation is that at the first packet of x axis where the speed is 0 and instead of 0 Hz we get approximately -245 Hz. This is happening because imperfect synchronization between the mixed signals.

$speed\ [\frac{km}{h}]$	$f_{doppler}\ [Hz]$
30	25.4
50	42.4
60	50.9
80	67.8
100	84.78

TABLE I
DOPPLER SHIFT FREQUENCIES $f_{carrier} = 915MHz$

It is important to determine accurately the beginning of the LoRa packet during this process otherwise a phase shift between periodic signals will cause a non zero offset. To achieve this we used a cross-correlation technique which

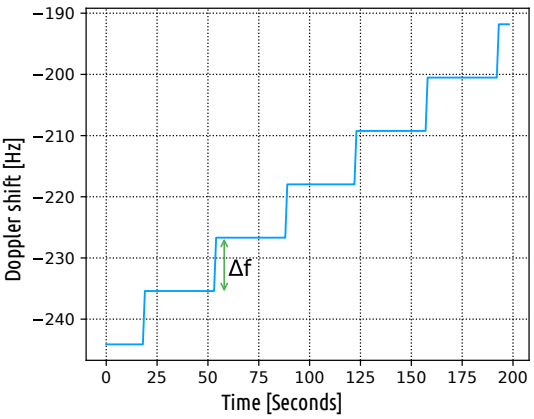

Fig. 2. Detected Doppler shift frequency during simulation of mobile LoRa jammer.

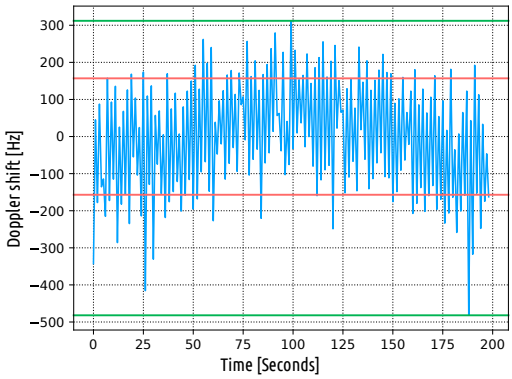

Fig. 3. Detected Doppler shifts for real-life measurements for first 200 packets.

is used to determine the similarity of two signals. Hence, an expected LoRa preamble pattern is correlated with the measured signal to define the exact time point that a LoRa packet begins.

To verify the hypothesis experimentally we set up a scenario where a LoRa mobile jammer was mounted on a car and moves as it is described in Section IV while the SDR was capturing signal data, deployed next to the receiver. In a real word scenario the SDR should be connected to the LoRa gateway where there resources are redundant. Figure 3 shows the results of the experiment of the first 200 jamming packets which were recorded when the jammer was near the receiver and moved with a relatively low speed of 0 to 5 km/h. This corresponds to the time walking to the car with the jammer to start the experiment. It is a good reference to judge whether it is possible to detect movement just by observation of Doppler shift for a real signal recorded by SDR. The expected results would be a relatively flat line with a small deviation but instead we obtained noisy results with high standard deviation, far from the outcome of the simulation.

Although the results obtained from the simulation indicate that it is possible to detect a mobile LoRa jammer from the

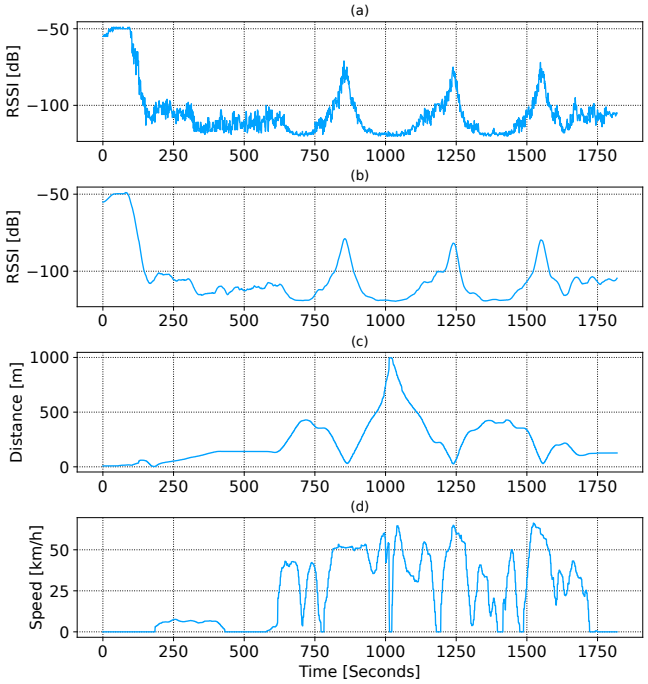

Fig. 4. The signal strength of the mobile LoRa jammer (raw (a) and filtered (b)) captured at the receiver and its regarding distance (c) and speed (d).

Doppler shift, the results from the experimental case do not confirm the hypothesis. There are several reasons to observe this behaviour, low quality hardware, signal clipping or other distortions like instability of the carrier frequency of a signal.

VI. Signal Strength and Entropy Based Detection

This section presents an approach to detect a mobile LoRa jammer which is based on two steps: first, on the transmission power of the signal and second, on the entropy of the received data. Received Signal Strength Indicator (RSSI), is a parameter that indicates the strength of a received radio signal.

First we used a mobile LoRa jammmer attached on a car as it is described in Section IV but without the legitimate LoRa transmitter. The purpose of this attempt was to determine a baseline of the mobile LoRa jammer signal strength, before we include the legitimate LoRa transmitter in the evaluation. The results are illustrated in Figure 4. The first observation is that the RSSI measurements at Figure 4 (a) are very noisy and we used the Savitzy-Golay filter [28] to filter them at Figure 4 (b). Figure 4 (c) and (d) show the distance and the speed of the mobile jammer captured from the GPS. Another interesting observation is that if the distance is 500 m or more, the variation of the signal is very low.

The second part of the evaluation we repeat the same scenario but with the legitimate LoRa transmitter included, to the same setup. The results in Figure 5 (a) and (b) depict the filtered RSSI measurements of the legitimate transmitter and the jammer respectively and (c) the distance of the jammer during its mobility. Figure 5 (a) shows a flat line with slight fluctuations in the RSSI which did not affect the overall

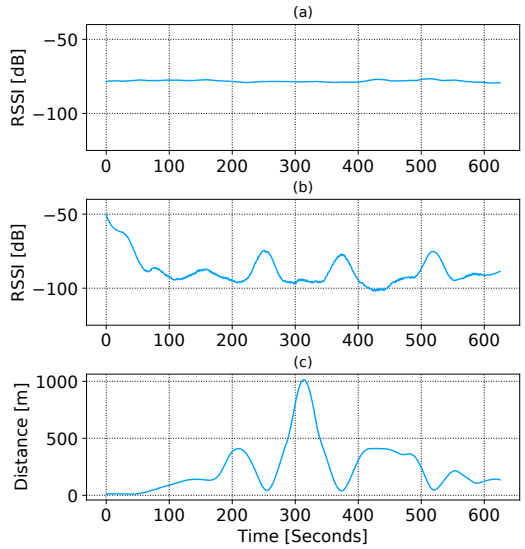

Fig. 5. The filtered signal strength of the legitimate LoRa transmitter (a), the mobile LoRa jammer (b) and its distance while moving (c).

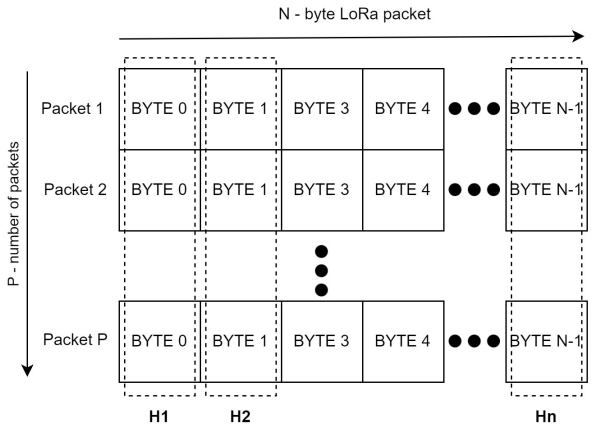

Fig. 6. Data organization for statistical processing during the entropy analysis. H1,H2 to Hn are histograms calculated over columns.

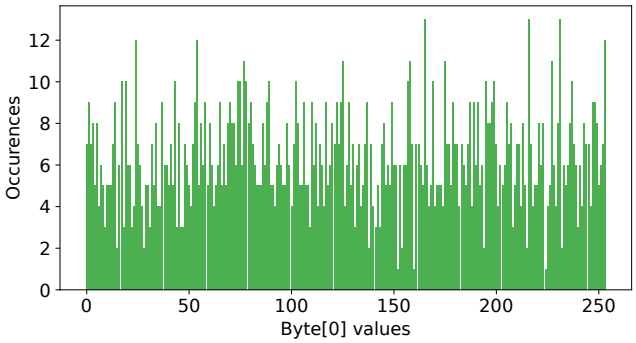

Fig. 7. Histogram of byte[0] values for multiple packets sent by jammer sending random packets

constant value of the RSSI around level of -75 dB. Figure 5 (b) shows that fluctuations correlate inversely, with the changes in the distance between the jamming transmitter and the measuring receiver in an almost inversely proportional way. This is similar to the RSSI measurements collected solely from the mobile LoRa jammer presented in Figure 4 (b). This verifies that observing variations of received LoRa RSSI values can be utilized to determine if the transmitter is stationary or mobile.

To determine if the transmitter is performing a jamming attack or not would require an additional step which is analyzing the entropy of the received data. Entropy can demonstrate the degree of indeterminacy of a random variable. In our case, assuming that the data coming from a jamming attack are generated from a random function, will demonstrate high level of entropy. Given that the data coming from a legitimate transmitter will contain some constants, they will demonstrate low level of entropy.

In order to analyze the data we followed an approach which treats a received LoRa packet as a single horizontal vector of two-dimensional array containing N amount of bytes. The second dimension of the array consists of successive vectors in time as it is illustrated in Figure 6.

To present the results we use histograms which illustrate each vertical vector outlined in Figure 6 with dashed rectangles. To verify that there is high degree of randomness in the packets coming from the jammer, we present the occurrences of the values located at the first bit, in Figure 7 based on 1625 packets. The results in Figure 7 are verifying that the randomness level is high because they were generated from a `rand()` function.

To calculate the entropy we use formula 2, where $count_i$ is the number of occurrences of a given value and N is the total amount of all values. The entropy is calculated based on data from the jammer and the legitimate transmitter respectively based on more than 260 packets respectively. Note that the entropy has been computed for each byte position separately. The entropy in the jammer data is approximately 5.5 for every packet slot and the entropy for the legitimate user is 0 for several packet slots 8, meaning that there is no presence of randomness probably because they are constant values like the address. There are some packet slots that present high level of randomness in Figure 8, we speculate that these are the slots responsible for the encryption or the CRC checksum.

$$H = K \sum_{i=1}^{n} (\frac{count_i}{N}) log_2 (\frac{count_i}{N}) \quad (2)$$

An Intrusion Detection System (IDS) can be based on this two-step approach. First, utilizing the signal power to classify a potential mobile jammer and afterwards analyzing the entropy of the received data to determine if they are transmitted by a jammer or not. Another advantage of this approach is that there is no requirement for additional hardware.

VII. Conclusion

The main focus of this paper was to explore the possibility of detecting mobile LoRa jammers based on two approaches.

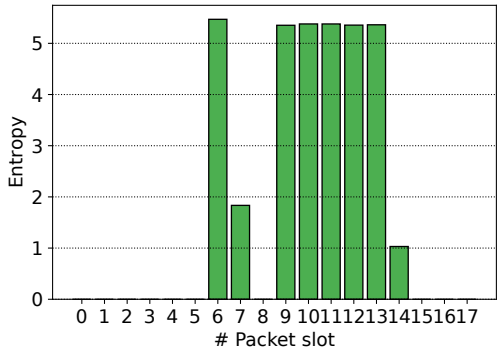

Fig. 8. Entropy calculated based on the data of the legitimate transmitter.

The first one was based on a digital signal processing technique and more specifically on the Doppler effect on mobile communications. The hypothesis that we were able to observe a frequency shift due to the Doppler effect on a mobile LoRa jammer was verified only through a simulation. The second approach was based on analysing the variability of the signal strength as a first step and then examining the entropy of the received data to detect a potential jammer. The results of the second approach show that it is possible to identify a potential mobile LoRa jammer based on the variability of its signal strength and the randomness level in its data. The presented evaluation indicates that it is possible to detect mobile jammers that follow the deceptive jamming strategy with random payload, yet further work is required for more sophisticated jamming attacks, such as jamming with legitimate replayed frames or reactive jamming.

ACKNOWLEDGEMENTS

This work was partially funded by Innovation Fund Denmark, grant 9092-00007B AgroRobottiFleet.

REFERENCES

[1] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low Power Wide Area Networks: An Overview," *IEEE Communications Surveys Tutorials*, vol. 19, no. 2, pp. 855–873, 2017.

[2] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[3] Semtech, "What is LoRa®." https://www.semtech.com/lora/what-is-lora, 2023. [Online; accessed 02/01/2023].

[4] B. Martinez, F. Adelantado, A. Bartoli, and X. Vilajosana, "Exploring the performance boundaries of nb-iot," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5702–5712, 2019.

[5] Sigfox, "Sigfox 0G Technology." https://www.sigfox.com/, 2022. [Online; accessed 02/01/2023].

[6] W. Guibene, J. Nowack, N. Chalikias, K. Fitzgibbon, M. Kelly, and D. Prendergast, "Evaluation of lpwan technologies for smart cities: River monitoring use-case," in *2017 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, pp. 1–5, 2017.

[7] M. C. Vuran, A. Salam, R. Wong, and S. Irmak, "Internet of underground things in precision agriculture: Architecture and technology aspects," *Ad Hoc Networks*, vol. 81, pp. 160–173, 2018.

[8] L. Germani, V. Mecarelli, G. Baruffa, L. Rugini, and F. Frescura, "An iot architecture for continuous livestock monitoring using lora lpwan," *Electronics*, vol. 8, no. 12, 2019.

[9] J. C. Liando, A. Gamage, A. W. Tengourtius, and M. Li, "Known and unknown facts of lora: Experiences from a large-scale measurement study," *ACM Trans. Sen. Netw.*, vol. 15, feb 2019.

[10] C. Orfanidis, L. M. Feeney, M. Jacobsson, and P. Gunningberg, "Investigating interference between lora and ieee 802.15.4g networks," in *2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pp. 1–8, 2017.

[11] N. Hou, X. Xia, and Y. Zheng, "Jamming of LoRa PHY and Countermeasure," in *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications*, pp. 1–10, 2021.

[12] E. Aras, N. Small, G. S. Ramachandran, S. Delbruel, W. Joosen, and D. Hughes, "Selective jamming of lorawan using commodity hardware," in *Proceedings of the 14th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, MobiQuitous 2017, (New York, NY, USA), p. 363–372, Association for Computing Machinery, 2017.

[13] J. A. Jahanshahi, S. A. Ghorashi, and H. Sadreazami, "Jamming detection at base station using fuzzy c-means algorithm," in *2011 International Symposium on Computer Networks and Distributed Systems (CNDS)*, pp. 40–44, 2011.

[14] Semtech, "A Brief History of LoRa®." https://blog.semtech.com/a-brief-history-of-lora-three-inventors-share-their-personal-story-at-the-things-conference, 2020. [Online; accessed 16/01/2023].

[15] M. Bor, J. Vidler, and U. Roedig, "LoRa for the Internet of Things," in *Proceedings of the 2016 International Conference on Embedded Wireless Systems and Networks*, EWSN '16, (USA), p. 361–366, Junction Publishing, 2016.

[16] K. Grover, A. Lim, and Q. Yang, "Jamming and anti-jamming techniques in wireless networks: A survey," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 17, p. 197–215, dec 2014.

[17] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in wsns," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 4, pp. 42–56, 2009.

[18] E. Aras, G. S. Ramachandran, P. Lawrence, and D. Hughes, "Exploring the security vulnerabilities of lora," in *2017 3rd IEEE International Conference on Cybernetics (CYBCONF)*, pp. 1–6, 2017.

[19] C.-Y. Huang, C.-W. Lin, R.-G. Cheng, S. J. Yang, and S.-T. Sheu, "Experimental evaluation of jamming threat in lorawan," in *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*, 2019.

[20] S. M. Danish, A. Nasir, H. K. Qureshi, A. B. Ashfaq, S. Mumtaz, and J. Rodriguez, "Network intrusion detection system for jamming attack in lorawan join procedure," in *2018 IEEE International Conference on Communications (ICC)*, pp. 1–6, 2018.

[21] T. Perković, H. Rudeš, S. Damjanović, and A. Nakić, "Low-cost implementation of reactive jammer on lorawan network," *Electronics*, vol. 10, p. 864, Apr 2021.

[22] Y. Cheng, H. Saputra, L. M. Goh, and Y. Wu, "Secure smart metering based on lora technology," in *2018 IEEE 4th International Conference on Identity, Security, and Behavior Analysis (ISBA)*, pp. 1–8, 2018.

[23] Semtech, "LoRaWAN® Specification v1.1." https://lora-alliance.org/resource_hub/lorawan-specification-v1-1/, 2020. [Online; accessed 12/06/2023].

[24] FreeRTOS, "FreeRTOS Real-time operating system for microcontrollers." https://www.freertos.org/, 2003. [Online; accessed 17/01/2023].

[25] esp32-lora library, "esp32-lora-library." https://github.com/Inteform/esp32-lora-library, 2017. [Online; accessed 17/01/2023].

[26] GNU, "Gnu radio." https://wiki.gnuradio.org, 2001. [Online; accessed 18/01/2023].

[27] B. Al Homssi, K. Dakic, S. Maselli, H. Wolf, S. Kandeepan, and A. Al-Hourani, "IoT Network Design Using Open-Source LoRa Coverage Emulator," *IEEE Access*, vol. 9, pp. 53636–53646, 2021.

[28] R. W. Schafer, "What is a savitzky-golay filter? [lecture notes]," *IEEE Signal Processing Magazine*, vol. 28, no. 4, pp. 111–117, 2011.