Reactive Jamming Detection for LoRaWAN Based on Meta-Data Differencing

Henri Ruotsalainen
hruotsalainen@fhstp.ac.at
St. Pölten University of Applied Sciences
St. Pölten, Austria

ABSTRACT

Reactive jamming in LoRaWAN networks is a stealthy way to implement Denial-of-Service attacks against selected devices because the cause of the interference remains hidden from a network operator. In order to make such attacks more detectable this paper proposes a novel algorithm, which is able to expose a jamming attempt from a single LoRaWAN packet. By monitoring deviations in meta-data of LoRaWAN frames, our method can distinguish a jamming attempt from a normal packet collision with up to 99% accuracy. Furthermore, the presented algorithm is also suitable for light-weight implementations on LoRaWAN devices due to its low complexity.

KEYWORDS

LoRaWAN, Denial-of-Service, jamming

ACM Reference Format:
Henri Ruotsalainen. 2022. Reactive Jamming Detection for LoRaWAN Based on Meta-Data Differencing. In *The 17th International Conference on Availability, Reliability and Security (ARES 2022), August 23–26, 2022, Vienna, Austria.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3538969.3543805

1 INTRODUCTION

Low-Power Wide-Area Network (LPWAN) technologies have rapidly gained popularity during the past years. Long communication ranges together with a low energy consumption makes an LPWAN connectivity an optimal data acquisition solution for several applications, where a low data rate between a device and a gateway is sufficient. Example use-cases to this end include e.g. air quality monitoring in a smart city environment, soil quality inspection in smart farming, cold chain monitoring and many more. Out of the several available technologies, i.e. Nb-IoT, Sigfox, mioty, LTE-M, Weightless-N/P/W and LoRaWAN, the latter has drawn considerable interest given the available low-cost LoRa modems, open source back-end software such as Chirpstack [3] and the free channel access on unlicensed RF bands. Recent developments around LoRa/LoRaWAN include also satellite based gatewayless operation [2] for remote deployments and, hence, it is safe to assume that LoRaWAN shall play a significant role also in forthcoming IoT applications.

One of the grand research challenges connected to IoT in general and, hence, also to LoRaWAN is to ensure a similar level of security at all stages starting from physical wireless nodes ranging all the way up to back-end servers. While the fundamental security features such as recurrent security updates, firewalls, intrusion detection systems and public-key infrastructure are ubiquitous in conventional IP networks, compromises to those features need to be made on the front-end side. For example, the limited down-link communication data-rate of LoRaWAN hinders implementations of firmware security updates. Because of the same reason, also secure protocols such as TLS are difficult to implement due to added communication overhead and computation on the LoRaWAN node. Next to the lack of strong security features, the various attacks against LoRaWAN devices pose a serious risk on LoRaWAN use-cases. As an example, the so called key extraction attacks [13] lead to decreased confidentiality and integrity as an attacker is able to, e.g. mount rogue devices to the network. Furthermore, the availability of the LoRaWAN wireless connectivity can be heavily degraded by the so called reactive jamming attacks [7]. Since this kind of Denial-of-Service (DoS) attacks operate on the wireless physical layer, they are more difficult to thwart in comparison to e.g. the classical DoS attacks in IP networks on transport layer.

As a response to the above mentioned challenges, research efforts have been devoted on several fronts concerning system hardening and intrusion detection. For instance the risk of compromised secret keys can be lowered by periodical secret key refreshment techniques. To this end, cryptographic key exchange algorithms [12] as well as wireless physical layer secret key agreement techniques have been proposed [14]. Recently also studies towards jamming attacks and related countermeasures have been conducted. Firstly, performance of a LoRaWAN network including multiple jammers

ARES 2022, August 23–26, 2022, Vienna, Austria
© 2022 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-9670-7/22/08.
https://doi.org/10.1145/3538969.3543805

have been evaluated in [9]. Secondly detection techniques, which shall be able to distinguish jamming attacks from normal LoRaWAN communication have been presented [11]. Finally, novel medium access methods, such as cryptographic frequency hopping [1], being less prone to intentional interference, have been proposed. Despite the advances in LoRaWAN security research to improve wireless availability, up to the authors best knowledge, there is still room for improvement in terms of jamming detection. For instance, the techniques based on machine learning [10] require a training phase with large data sets and computational power to execute classification algorithms.

Motivated by the above mentioned research gaps, this paper aims to present a novel reactive jamming detector which is tailored for LoRaWAN. In particular our contributions include

- Light-weight detector algorithm based on meta data differences
- Investigation of LoRaWAN packet meta-data sensitivity to reactive jamming attacks
- Experimental validation with a LoRaWAN test network

The rest of this paper is organized as follows. At first in Section 2 we present the related work followed by the relevant methods in Section 3. Subsequently, in Section 4 we deliver the experimental results and in Section 5 we compare our work with state-of-the-art. Finally, conclusions and future works are drawn in Section 6.

2 RELATED WORK

Due to chirp spread spectrum LoRa signaling, LoRaWAN links have shown to be robust against fading and difficult RF propagation conditions. Moreover, according to a theoretical analysis given in [4], classical jamming attacks such as single tone jamming or full-band jamming with noise signals shall have only negligible impact on the symbol error rate. On the other hand, reactive jamming attacks with a spreading factor setting set equivalent to that of the victim device, shall achieve much more efficient DoS scenarios. In the following paragraphs we review the recent advances in jamming attack detection techniques.

In [11] the authors considered practical jamming attacks equipped with GNU Radio software defined radio framework and the HackRF transceiver front-end. Their proposed jamming detection method is based on gateway log packet drop analysis. As it turns out, a wide-band noise jamming waveform with a sufficient power (in relation to the victim LoRaWAN waveform power at the receiver) achieves a severe packet loss. Hence, by defining a normal packet loss rate for a device, jamming attacks can be detected if the packet loss rate exceeds a given tolerance bound. However, such detection method might suffer from high latency times as LoRaWAN devices often have to follow strictly limited packet airtime regulations.

A more advanced approach was proposed in [10] where the authors proposed utilization of statistical and machine learning based methods. For the former, the key ingredient involved the exponentially weighted moving average statistical measure, which is useful to detect small deviations in statistical data with relatively low computational complexity. By adjusting the weight parameter, it is possible to tune the sensitivity of the detector for jamming attacks over limited periods of time. For the latter, a recurrent neural network model was proposed, which is claimed to be able to predict higher dimensional anomalies in a data-set more accurately. The feedback nature of such model provides a detection result over a finite time window, similar to the statistical method above. The authors utilized received signal strength indicator (RSSI) and inter arrival time (IAT) as data-sets for model training and evaluation. With large scale simulation data-sets and small scale real-world data-sets, the authors reported true positive rates of ca. 90% for the statistical model and ca. 98% for the machine learning model.

An interesting reactive jamming detection method was proposed in [16], where the authors analyzed RSSI for individual bit errors of a wireless payload. Although the experimental results did not involve LoRaWAN communication, the presented work is relevant as the techniques are closely related to the ones presented in this paper. With the fine-grained RSSI analysis, the authors were able to distinguish jamming attacks from e.g. path-loss/fading and packet collisions. According to conducted experiments, this method achieved ca 100% accuracy for various jamming waveform lengths.

3 METHODS

In this Section we firstly present all the relevant background connected to reactive jamming in LoRaWAN networks and afterwards carry on to explain our detection algorithm.

3.1 LoRaWAN physical layer and packet structure

Wide communication range of LoRaWAN is mainly possible due to the underlying LoRa signaling, which is based on chirp spread spectrum (CSS) modulation. As visible from a spectrogram of several LoRa chirps illustrated in Figure 1, the chirps are effectively RF waveforms with linearly increasing (or decreasing) frequency over time and they occupy the full bandwidth of a LoRaWAN channel. Payload data itself is conveyed to such chirps by phase modulation, where the capacity, i.e. the amount of bits a chirp is able to carry, is defined by the so called spreading factor (SF) parameter. For

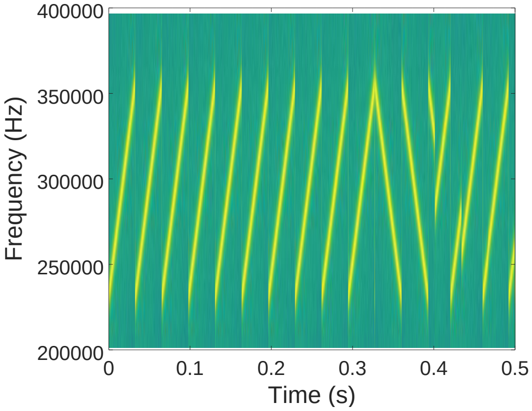


Figure 1: Spectrogram of a LoRa waveform.

LoRaWAN SF can take integer values between 7 and 12. The duration of a LoRaWAN packet is strictly determined by T = 2^{SF}/BW, where BW denotes the signal bandwidth. For example, a LoRaWAN packet with 16 bytes with SF setting of 12 results in an RF waveform with 1646 ms of airtime. As such, LoRa modulation effectively trades achievable datarate for robustness against interference and fading. This is true due to the good correlation properties of the lengthy chirp waveforms, which lead to correct demodulation results even when signal-to-noise ratio at an LoRa receiver is well below zero.

The LoRaWAN up-link packet structure is visible in Figure 2. In the so called explicit header mode, the physical layer parts including preamble, PHY header and PHY header CRC are necessary to synchronize LoRa receiver with the incoming payload and to set correct parameters for LoRa packet decoding. Further within PHY payload, the MAC header field determines the type of the LoRaWAN packet, e.g. join request/accept or up-link/down-link messages. Subsequently, MAC payload contains information on the device (Device address), on the LoRaWAN medium access (Frame control, frame counter, frame options and frame port) as well as the LoRaWAN payload. Finally, integrity of a LoRaWAN packet can be verified by the included cryptographic message integrity code (MIC). A more detailed description of the message types and packet fields can be found in the LoRaWAN specification [8].

3.2 LoRaWAN network

The structure of a LoRaWAN network, as depicted in Figure 3, follows the star-of-stars topology, where a single end-device can be connected to multiple gateways. Additionally network, join and application servers are involved to handle medium access, device commissioning and application data transfers, respectively. A LoRaWAN gateway implements packet forwarding, i.e. it captures LoRaWAN packets and depending on the correctness of a packet (via CRC check) sends them further to a network server. Since multiple gateways might receive an individual LoRaWAN packet, the packet de-duplication is performed on the network server alongside with the frame authentication based on MIC. Given that a packet is successfully authenticated the encrypted payload is forwarded to the application server, where the decrypted payload can be finally accessed, e.g. by a user application. In this paper we consider only single gateway operation with LoRaWAN nodes configured in Class-A mode, which is the medium access method optimized for low energy utilization.

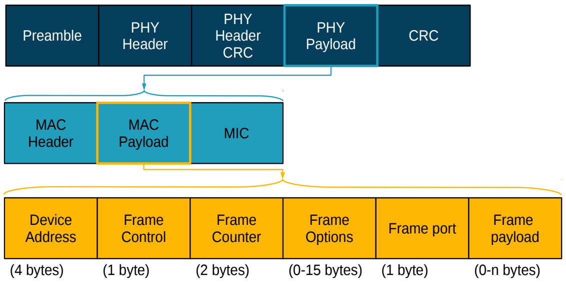


Figure 2: Structure of a LoRaWAN uplink packet.

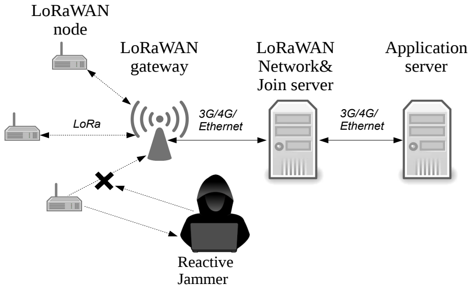


Figure 3: LoRaWAN network components.

3.3 Reactive Jamming with Chirpotle Framework

The DoS attacks we are addressing in this paper involve the so called reactive jamming attacks, in which an attacker, as illustrated in Figure 3, aims to block RF packets only from a selected device. In comparison to classical RF jamming with continuous RF waveforms, such attacks are much harder to detect due to lesser jammer activity. To this end, reactive

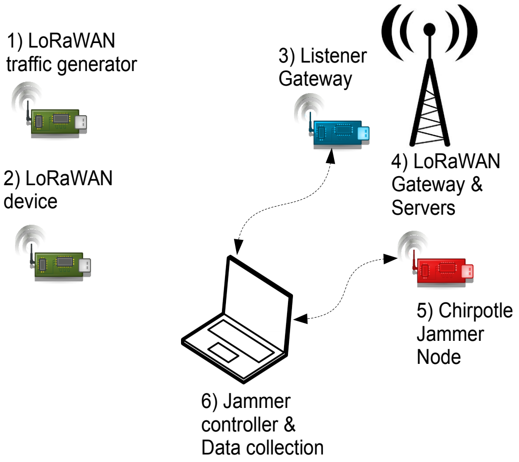

1) LoRaWAN traffic generator
2) LoRaWAN device
3) Listener Gateway
4) LoRaWAN Gateway & Servers
5) Chirpotle Jammer Node
6) Jammer controller & Data collection

Figure 4: Test-bed for LoRaWAN packet collisions and reactive jamming.

jamming is also more energy efficient, which might enable longer jammer activity with mobile, battery driven jammer nodes. The particular toolset we are utilizing to implement reactive jamming attacks in LoRaWAN networks is based on the Chirpotle framework [7], which is originally intended for experimental evaluations for LoRaWAN wormhole attacks. In our work, we adopted the reactive jammer node of the Chirpotle and modified the controller scripts for jamming of LoRaWAN packets stemming from a private LoRaWAN network.

The necessary components to establish reactive jamming with the Chirpotle framework shown in Figure 3 include a controller computer (such as a laptop) and a single jammer node (Raspberry PI computer equipped with a LoRa modem). These two entities are connected via e.g. WLAN/Ethernet/4G network. The jammer node is configured using Linux shell scripts and Jupyter notebooks running on the controller computer. For supported jammer equipment, the firmware sources for reactive jamming are included in the framework. Once a user has entered correct parameters for an intended LoRaWAN device to be jammed (i.e. RF center frequency, SF, Device Address) the jammer node is put onto listening mode, where the LoRa transceiver continuously scans the given RF band for incoming LoRaWAN packets. For each packet, the captured unencrypted device address is compared with the given device address and in case they are equal a jamming waveform is transmitted. According to [6], as the minimum LoRaWAN frame size is 12 bytes, there is a margin of 7 bytes between frame detection and jamming frame transmission. This margin is according to the authors sufficient to jam every LoRaWAN frame type regardless of the SF setting.

3.4 Jamming Detection based on Meta-data differencing

In the following we proceed to propose a simple but efficient technique to detect reactive jamming attacks in LoRaWAN networks.

3.4.1 Receiver Selection. Our method can be implemented on the one hand directly at a LoRaWAN gateway or on the other hand, on an explicit listener gateway. For the former, some modifications to the original LoRaWAN packet forwarder software might be necessary to enable packet and meta-data logging for packets with CRC errors. For the latter, therefore, a readily available packet logging tool, e.g. the one from [15] can be utilized together with a LoRaWAN gateway to capture LoRaWAN communication. In this case, it is important to place the listener gateway antenna as illustrated in Figure 4 as close as possible to the gateway antenna of the selected LoRaWAN network. For this paper, the option with a listener gateway was implemented.

3.4.2 Basic Principle. As soon as LoRaWAN packet logging (with and without CRC errors) is available, the detection algorithm follows the states given in a flow diagram shown in Figure 5. Once a new packet arrives at the gateway, the device id is searched from a local database holding device ids with the latest meta-data information of the device. The stored meta-data include RSSI value, SNR value, frame control byte and frame counter bytes. The stored device ids include those devices for which the jamming detection shall be enabled. In case the received device id is found in the database, the packet CRC error is verified. Given a correctly received packet, the packet meta data is updated in the database and the packet is forwarded towards a network server. Otherwise for a failed CRC check, a meta-data difference is calculated between the received meta-data and meta-data contained in the database for the received device id. In the subsequent step, the meta-data difference (e.g. SNR) is compared with a tolerance bound to detect a jamming attempt.

3.4.3 Detection Rule. Given the multiple meta-data sources, the difference between a correctly received and a jammed/collided packet can be calculated in various ways. The simplest way of detection is based on a comparison with a single meta-data source as

$$d = \begin{cases} jammed & |meta_d - meta_r| > tol_{meta} \\ notjammed & |meta_d - meta_r| <= tol_{meta}, \end{cases} \quad (1)$$

where $meta_d$ and $meta_r$ denote the meta data from the database and the newly recorded meta data, respectively.

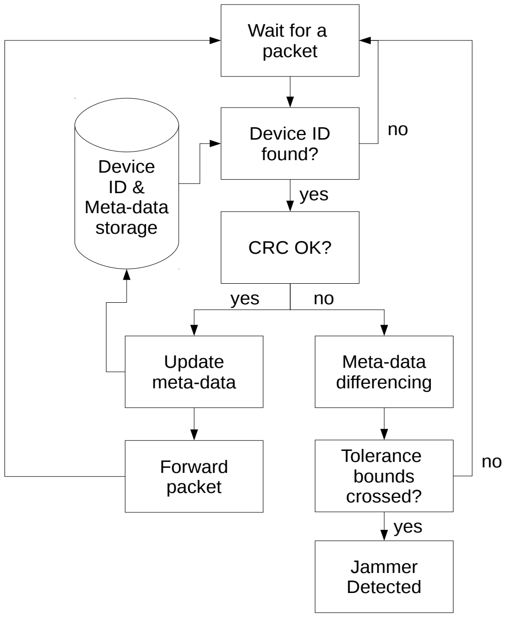


Figure 5: Flow-chart on reactive jamming detection based on meta-data difference.

3.4.4 Meta-data sources. Based on previous results and also on our analysis of LoRaWAN data-sets containing jammed packets, we selected the most promising meta-data sources for jamming prediction. As already mentioned in [16], the overlapping jamming waveform can increase the received RF signal power as the jammer signal power shall be notably higher than that of the legitimate signal. Additionally, since jamming contributes to channel interference, it can be assumed that jamming has an adverse effect on SNR. By evaluating a jamming data-set, it became clear that the SNR of a jammed packet is significantly lower in comparison to a normally received packet. Finally, by inspecting differences in LoRaWAN MAC payload meta-data fields, it was found out that the frame counter value (Fcnt) was affected the most by jamming. Hence, RSSI, SNR and Fcnt were selected as the meta-data sources for jamming detection.

4 EXPERIMENTAL RESULTS

Under this section we present the validation results for our reactive jamming detection method. Additionally, a step on how to determine an optimal detection tolerance bound will be discussed.

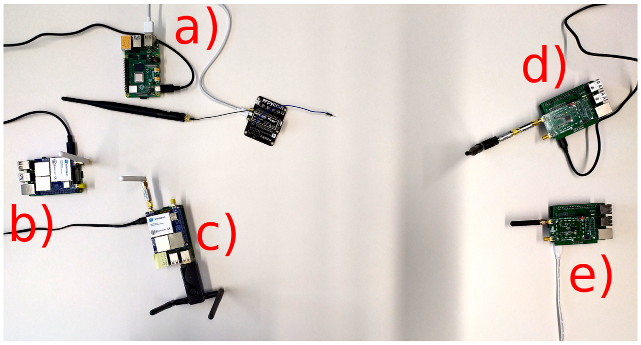
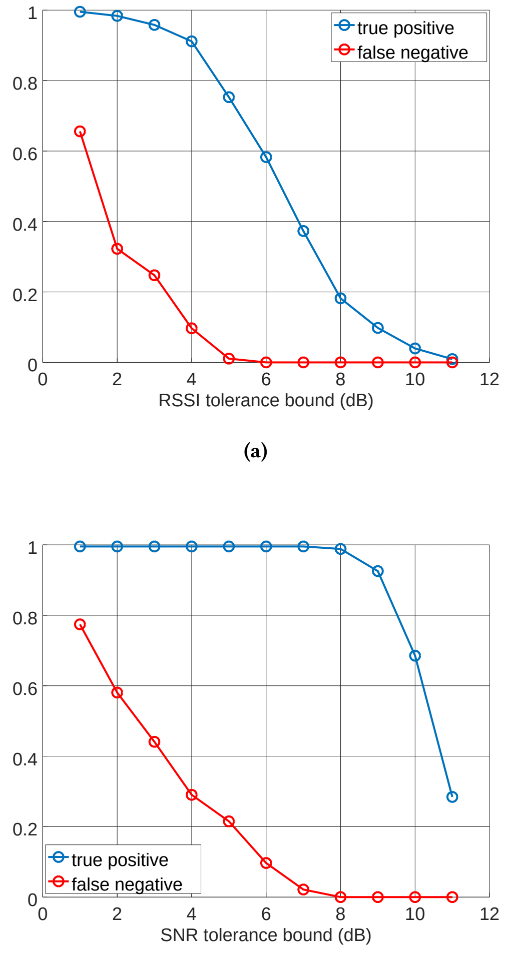


Figure 6: Reactive jamming test-bed including a) Chirpotle jammer node b) Listener LoRaWAN gateway c) LoRaWAN gateway/servers d) LoRaWAN node simulation and e) LoRaWAN traffic generator node.

4.1 Measurement Test-Bed Setup and Data-sets

Figure 6 depicts all the components (excluding the Chirpotle controller PC), which were necessary to collect experimental validation data. All of the nodes are based on Raspberry PI computers, which are controlled remotely over a common WLAN access-point configured on the LoRaWAN gateway e). The Chirpotle jammer node a) is equipped with a Pycom LoPy LoRaWAN module, which embeds a LoRa SX1276 modem with an ESP32 microcontroller. The Raspberry PI and the ESP32 of a) are configured with control scripts and a firmware image of the Chirpotle framework, respectively. The listener LoRaWAN gateway b) is based on a Dragino PG1301 LoRaWAN gateway hat, which runs a packet logger tool from [15] to record the entire LoRaWAN communication (frames with and without CRC errors). Similarly, the LoRaWAN gateway c) is based on the PG1301 and it servers the packet forwarder tool as well as LoRaWAN network and application servers from [5]. Further, the LoRaWAN node simulation d) is implemented with a Semtech SX1276 LoRa development module and an LMIC 1.6 library. Additionally, to emulate path-loss, two 30 dB RF attenuators are mounted between the LoRa module and an 868 MHz antenna. LoRaWAN traffic generation e) is implemented with the same LoRa development module and with the LMIC library. The LoRaWAN communication was configured for the EU868 bands, i.e. 868.1 MHz, 868.3 MHz and 868.5 MHz. Furthermore, the jammer node was configured to block frames only from the LoRaWAN node simulator on 868.1 MHz.

Using the above described test-bed, four distinct data-sets were collected. Firstly, two data-sets containing jammed/not jammed LoRaWAN frames were obtained for $SF = 7$ and $SF = 12$ settings. Afterwards, two further data-sets were collected with the same SF settings with LoRaWAN traffic



(a)

(b)

Figure 7: Detection performance in terms of true positives and false negatives for various tolerance bound settings for a) RSSI based detector and b) SNR based detector.

generation, which resulted in frames with/without packet collisions. As the packet logger tool logs arbitrary LoRaWAN traffic, as the final preparation step only the frames stemming from LoRaWAN node simulator were stored. This resulted in a data-set with 450 meta-data points with jamming and 80 meta-data points with packet collisions.

4.2 Detection tolerance bound optimization

An essential step to improve the detection accuracy, is to find out an optimal tolerance bound setting, i.e. for tol_{meta} in Equation 1. Optimality in this context means selecting a tol_{meta}, which maximizes the true positive rate (jammed packet classified correctly) and at the same time minimizes the false negative rate (normal packet collision classified incorrectly as jammed packet). By evaluating these two figures for different tol_{meta} settings using the both RSSI and SNR based detectors allowed us to determine the optimum settings. As shown in Figure 7, the maximum distance between true positive and false negative rates can be obtained for $tol_{\text{RSSI}} = 4$ and $tol_{\text{SNR}} = 8$ for RSSI and SNR detectors, respectively. In other words, these settings lead to optimum classification performance for the two detectors. Finally, the Fcnt based detector performed equally well for $2 \leq tol_{\text{Fcnt}} \leq 12$.

Table 1: Detector accuracy

Meta-data source	Accuracy (SF7)	Accuracy (SF12)
RSSI	92.9%	86.7 %
SNR	98.0%	99.0 %
Fcnt	93.9%	90.8%

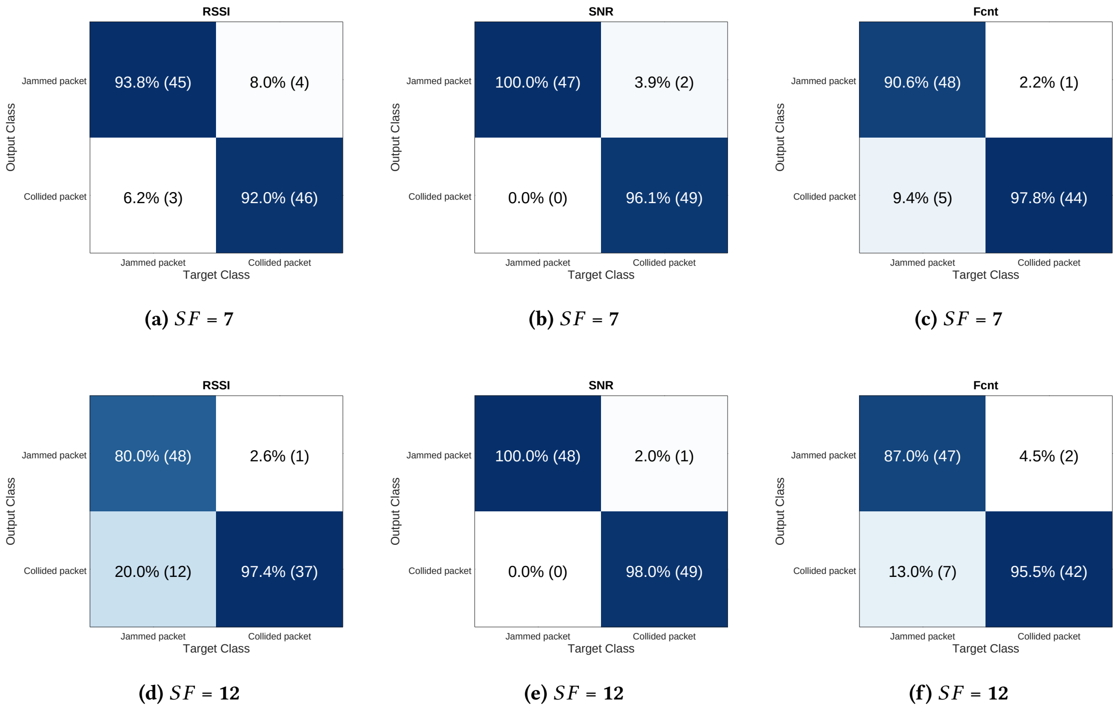
4.3 Single meta-data source

With the determined tolerance bound values, the performance of each detector was measured in terms of confusion matrices and accuracy. Out of these two figures-of-merit, the former expresses true-positive (TP), false-positive (FP), true-negative (TN) and false-negative (FN) rates in a matrix form. The latter is defined as accuracy $= \frac{\text{TP+TN}}{\text{P+N}}$, where P denotes the number of positive conditions and N the number of negative conditions. As indicated by Table 1 and Figure 8, the SNR based detector delivers the best accuracy of 98% and 99% with least amount of false-positives and false-negatives. As it turns out, reactive jamming attacks produced for both SF settings large and constant deviations to SNR, which can be easily distinguished from smaller and more random SNR deviations caused by packet collisions. Interestingly, the variance of jamming based RSSI deviations was higher than that of SNR, which results in some misclassifications particularly for SF = 12. At last the Fcnt based detector performed equally well with RSSI based detector with accuracy of ca. 92%. This can be explained by the art of packet collisions, where the colliding LoRaWAN frame randomly overlaps the original frame. This leads to corrupted Fcnt fields, which increases the number of misclassifications.

5 DISCUSSION

In this Section we compare our work with other jamming detection algorithms listed in Table 2 and subsequently discuss the limitations and the potential applications of our method.

Firstly, although the core functionality of the meta-data differencing based detection draws similarities to the RSSI



(a) $SF = 7$ **(b)** $SF = 7$ **(c)** $SF = 7$

(d) $SF = 12$ **(e)** $SF = 12$ **(f)** $SF = 12$

Figure 8: Confusion matrices calculated for single meta-data jamming detectors, where (a)-(c) and (d)-(f) show results for RSSI, SNR and Fcnt based detectors for two different SF settings, respectively.

analysis based detector in [16], there exist some differences in the detailed implementation. For instance, we investigated several meta-data sources (RSSI,SNR,Fcnt) and argued that for LoRaWAN, the SNR might lead to better performance. Additionally, the results in [16] were collected with short/medium range RF transceivers, whereas our work considers long-range LoRa protocol. Nevertheless, the reported detection performance in [16] is close to the figures given in Section 4. Secondly, while comparing with the packet statistics based detection as presented in [11], the per-packet detectors such as ours shall lead to notably lower detection latency. Since the data-rates in a typical LoRaWAN network become as low as few packets per day, collection of sufficient data (e.g. packet collisions) to build an accurate classification result might lead to severe delays. Hence, we argue that per packet based detectors are better suited for jamming detection in applications where event based signaling is utilized, e.g. in flood/gas/water-leak sensors. Thirdly, the main difference between the presented method and the machine learning based methods given in [10] is the higher computational complexity (e.g. neural network) and the necessity for large training sets.

Despite the encouraging detection accuracy reported in laboratory conditions (i.e. static RF channel with stationary devices), the performance of meta-data differencing might be degraded in some real-world LoRaWAN wireless scenarios. For instance, antenna detuning, path-loss and fading might cause large deviations in e.g. RSSI values which could increase the number of false positives. Such channel conditions can be found e.g. in transportation/logistics where the sensors are mobile. In such a case, it would be beneficial to apply other meta-data source such as Fcnt, which shall not be affected by varying RF channel conditions. Furthermore, we have considered a jammer attacker model where the jammer transmits a jamming waveform immediately after detecting a victim device address. While this strategy leads to efficient DoS condition, the jammer can be detected e.g. via Fcnt value inspection. A more stealthy jamming strategy would target the encrypted payload instead, which leaves the MAC layer meta-data unaffected. Nevertheless, the SNR and the RSSI based detectors could be applied as a countermeasure in such a case.

The foremost application of the reactive jammer detector is to achieve a timely intrusion detection against DoS attacks in LoRaWAN networks. As it turns out, since the wormhole attacks [7] utilize reactive jamming, our method could be extended to detect such attacks as well. Due to light-weight

Table 2: State-of-the-art jamming detection techniques

Reference	Technology	Jamming type	Accuracy
This work	LoRaWAN	Reactive	99%
[11]	LoRaWAN	Wideband	-
[10]	LoRaWAN	Triggered	98%
[16]	Zigbee	Reactive	100%

design of our algorithm, the jamming detection can be easily embedded to LoRaWAN edge devices. Hence, although the detection was implemented at a listener gateway in our current test-bed, it is possible to mount the detection logic also on a ultra-light weight LoRa microcontroller unit, which would decrease the deployment costs as well as increase the energy efficiency.

6 CONCLUSIONS

In this paper we presented a novel reactive jamming detector for LoRaWAN networks. Our work excels the state-of-the-art by considering several meta-data sources of a LoRaWAN packet, which become affected by reactive jamming attacks. According to our evaluations RSSI, SNR and Fcnt values as input data for the detection algorithm deliver the best detection performance. With the meta-data differencing, i.e. absolute difference between meta-data of a normally received LoRaWAN packet and a jammed packet, a detection accuracy of up to 99% can be achieved. Such per packet based detection is well suited for application with event based signaling such as gas/flood or water-leak monitoring. In the future works, we aim to further validate the proposed method in a real world LoRaWAN use-case and implement a real-time version of the detection algorithm.

REFERENCES

[1] Absar-Ul-Haque Ahmar, Emekcan Aras, Thien Duc Nguyen, Sam Michiels, Wouter Joosen, and Danny Hughes. 2020. CRAM: Robust Medium Access Control for LPWAN using Cryptographic Frequency Hopping. In *2020 16th International Conference on Distributed Computing in Sensor Systems (DCOSS)*. 95–102. https://doi.org/10.1109/DCOSS49796.2020.00026

[2] Muhammad Asad Ullah, Konstantin Mikhaylov, and Hirley Alves. 2021. Massive Machine-Type Communication and Satellite Integration for Remote Areas. *IEEE Wireless Communications* 28, 4 (2021), 74–80. https://doi.org/10.1109/MWC.100.2000477

[3] Orne Brocaar. 2022. *Chirpstack Open-Source LoRaWAN Network Server.* Retrieved May 10, 2022 from https://github.com/brocaar/chirpstack-network-server

[4] Clément Demeslay, Roland Gautier, Anthony Fiche, and Gilles Burel. 2021. Band & Tone Jamming Analysis and Detection on LoRa signals. arXiv:2107.07782 [eess.SP]

[5] Petr Gotthard. 2022. *Compact server for private LoRaWAN networks Github Repository.* Retrieved May 10, 2022 from https://github.com/gotthardp/lorawan-server

[6] Frank Hessel. 2020. *Chirpotle Github Repository.* Retrieved May 10, 2022 from https://github.com/seemoo-lab/chirpotle

[7] Frank Hessel, Lars Almon, and Flor Álvarez. 2020. ChirpOTLE: A Framework for Practical LoRaWAN Security Evaluation. In *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks* (Linz, Austria) *(WiSec '20)*. Association for Computing Machinery, New York, NY, USA, 306–316. https://doi.org/10.1145/3395351.3399423

[8] LoRa Alliance 2017. *LoRaWAN Specification 1.1.* LoRa Alliance.

[9] Ivan Martinez, Fabienne Nouvel, Samer Lahoud, Philippe Tanguy, and Melhem El Helou. 2020. On the performance evaluation of LoRaWAN with re-transmissions under jamming. In *Proc. IEEE Symposium on Computers and Communications (ISCC)*. 1–7.

[10] Ivan Marino Martinez Bolivar. 2021. *Jamming on LoRaWAN Networks : from modelling to detection.* Doctoral Thesis. Institut National des Sciences Appliquées de Rennes. https://tel.archives-ouvertes.fr/tel-03196484

[11] Mohammad Mezanur Rahman Monjur, Joseph Heacock, Rui Sun, and Qiaoyan Yu. 2021. An Attack Analysis Framework for LoRaWAN applied Advanced Manufacturing. In *2021 IEEE International Symposium on Technologies for Homeland Security (HST)*. 1–7. https://doi.org/10.1109/HST53381.2021.9619847

[12] Sarra Naoui, Mohamed Elhoucine Elhdhili, and Leila Azouz Saidane. 2016. Enhancing the security of the IoT LoraWAN architecture. In *2016 International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks (PEMWN)*. 1–7. https://doi.org/10.1109/PEMWN.2016.7842904

[13] Henri Ruotsalainen, Guanxiong Shen, Junqing Zhang, and Radek Fujdiak. 2022. LoRaWAN Physical Layer-Based Attacks and Countermeasures, A Review. *Sensors* 22, 9 (2022). https://doi.org/10.3390/s22093127

[14] Henri Ruotsalainen, Junqing Zhang, and Stepan Grebeniuk. 2020. Experimental Investigation on Wireless Key Generation for Low-Power Wide-Area Networks. *IEEE Internet of Things Journal* 7, 3 (2020), 1745–1755. https://doi.org/10.1109/JIOT.2019.2946919

[15] Semtech. 2020. *LoRaWAN packet forwarder tool for PG1301 Github Repository.* Retrieved May 10, 2022 from https://github.com/fhessel/dragino_pi_gateway_fwd

[16] Mario Strasser, Boris Danev, and Srdjan Čapkun. 2010. Detection of Reactive Jamming in Sensor Networks. *ACM Trans. Sen. Netw.* 7, 2, Article 16 (sep 2010), 29 pages. https://doi.org/10.1145/1824766.1824772