A Comparative Analysis of LoRa and LoRaWAN in the Presence of Jammers and Transient Interference

Artur N. de São José
COSYS-LEOST, Univ Gustave Eiffel, IFSTTAR, Univ Lille
Villeneuve d'Ascq, France
artur.nogsj@gmail.com

Nathan Chopinet
COSYS-LEOST, Univ Gustave Eiffel, IFSTTAR, Univ Lille
Villeneuve d'Ascq, France
nathan.chopinet@univ-eiffel.fr

Eric Pierre Simon
Univ. Lille, CNRS, USR 3380 - IRCICA
Villeneuve d'Ascq, France
eric.simon@univ-lille.fr

Alexandre Boé
Univ. Lille, CNRS, USR 3380 - IRCICA
Villeneuve d'Ascq, France
alexandre.boe@univ-lille.fr

Thomas Vantroys
Univ. Lille, CNRS, USR 3380 - IRCICA
Villeneuve d'Ascq, France
thomas.vantroys@univ-lille.fr

Chrisophe Gransart
COSYS-LEOST, Univ Gustave Eiffel, IFSTTAR, Univ Lille
Villeneuve d'Ascq, France
christophe.gransart@univ-eiffel.fr

Virginie Deniau
COSYS-LEOST, Univ Gustave Eiffel, IFSTTAR, Univ Lille
Villeneuve d'Ascq, France
virginie.deniau@univ-eiffel.fr

***Abstract*—There is a lack of studies about the susceptibility of LoRa networks to specific interference sources such as broadband jammers and the train catenary, which produces transient interference in a railway environment. In this paper, we investigate this topic by separately analyzing the proprietary LoRa physical layer and the open medium access control layer. Such an approach allows us to decompose the interference effects into two elements: the signal integrity effects at the physical layer and the counter measures of the LoRaWAN protocol.**

***Index Terms*—LoRa, railway communication, jamming, electromagnetic transients**

I. Introduction

Long range (LoRa) communications are one of the main technologies used nowadays for the deployment of internet-of-things (IoT)-based networks. Such a technology is defined by a proprietary physical layer (PHY) and by an open medium access control (MAC) layer, also known as LoRa wide area network (LoRaWAN). LoRaWAN is an open communication protocol standardized by the LoRa Alliance [1].

Some PHY layer parameters can be chosen and even dynamically changed in order to provide a good trade-off between throughput and range in a LoRa-based wireless network. This is possible thanks to a set of different data rates (DR), each of them consisting of a combination of spreading factor (SF) and bandwidth (B). The SF is an integer number ranging from 7 to 12, being inversely proportional to the throughput, and directly proportional to the range [1]. More details about the LoRa PHY layer parameters are given in Section II-A.

However, this trade-off can be compromised if the electromagnetic (EM) environment is polluted. In this context, one of the main EM interference (EMI) sources are the legal or illegal IoT devices that operate simultaneously with a given LoRa transmitter. In [2], authors use software-defined radio (SDR) and capture effect indicators to analyze multiuser interference. Authors in [3] simulate both channel-aware and channel-oblivious jamming effects. In [4], an Arduino-based jammer is programmed in order to disturb a gateway.

Despite the growing number of publications about the coexistence of IoT devices in LoRa networks and the introduction of malicious LoRa nodes to disturb the communications, there is a lack of studies focused on the railway EM environment. Indeed, LoRa and LoRaWAN are being studied for use in trains. In a railway environment, the two main EMI sources are the catenary contact (metal contact that connects the internal electric system of the train to the external supply lines, eventually producing electric arcs), and certain illegal jamming devices [5], which can be designed to simultaneously disturb different communication systems and users. In this paper, we describe an experimental study about the EM susceptibility of LoRa/LoRaWAN networks facing these two EMI sources.

Our second contribution is a comparative analysis between the performances of LoRa communication systems either based only on the PHY layer or on the open LoRaWAN protocol. In the past few years, several reverse engineering studies applied to the LoRa PHY layer have been published, giving some interesting information about its properties [6]. In this sense, the comparison we bring here will help to elucidate certain behaviors of LoRa/LoRaWAN networks in

This work was performed in the framework of the LoRa-R project, which is co-financed by the European Union with the European Regional Development Fund, the Hauts de France Region Council, and the SNCF railway company.

978-1-7281-5579-1/20/$31.00 ©2022 IEEE

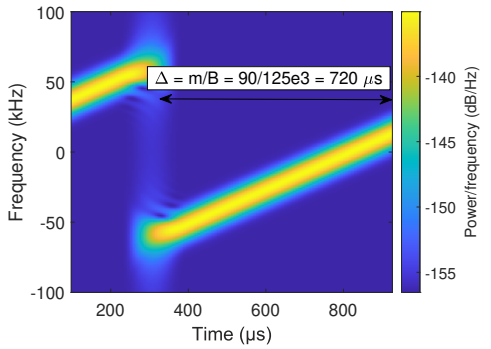


Fig. 1: LoRa symbol with index 90 (SF = 7, B = 125 kHz, SF = 7 and T_{sym} = 1 ms).

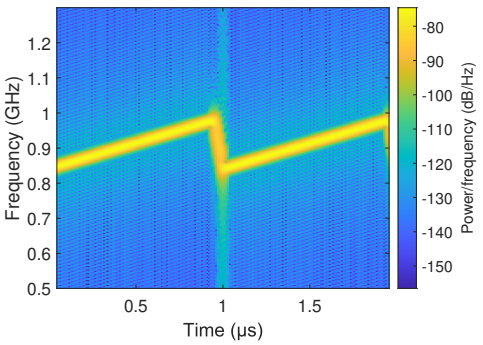


Fig. 2: Two cycles of a jamming signal (frequency versus time) with a T_{jam} = 1 μs covering the 840-980 MHz frequency band.

the presence of EMI. Throughout this paper, the terms LoRa and LoRaWAN are used to denote the PHY layer and the full protocol, respectively.

II. Description of the Signals

A. LoRa

In a LoRa communication system, symbols are transmitted through a chirp spreading spectrum (CSS)-modulated waveform. The symbols to be transmitted are represented by integer numbers in the range $0, 1, ..., 2^{SF}$, where SF is the spreading factor, ranging from 7 to 12. All these symbols can be encoded by circularly shifting an up-chirp waveform, whose duration is $T_{sym} = 2^{SF}/B$. The magnitude of the circular shift is m/B, where m is the symbol index and B is the bandwidth (125 kHz, 250 kHz or 500 kHz), meaning that each symbol is uniquely represented by a specific shift. To illustrate that, Fig. 1 shows a LoRa signal, in the time-frequency domain, carrying the information of the symbol index 90.

In a transmission process, these symbols are organized in frames. A typical PHY frame includes a preamble, an optional header, the payload and a cyclic redundancy check (CRC) field. The complete structure of a LoRa frame at the PHY, MAC and application layers can be found in [7]. In this work, we initially focus on the PHY layer only, and then we consider all the layers of the LoRaWAN protocol. The adopted frequency band is the EU863-870 (centered on the 868 MHz ISM band) and, in particular, one of the mandatory frequency equal to 868.3 MHz.

Reliability of the received data can be increased at the cost of throughput reduction by adding parity bits to the LoRa frames. The ratio of information bits per byte (excluding the parity bits) is the coding rate (CR). In this work, we adopt CR = 4/8.

B. Jamming signal

Different types of jammers are available in the black market. The most common ones emit EM waves, with the typical behavior illustrated in Fig. 2. Similarly to the LoRa signals illustrated in Fig. 1, these interfering signals are also frequency modulated. This means that, during a time interval called *sweep time* (T_{jam}), a sinusoidal carrier has its instantaneous frequency changed from a minimum to a maximum value. Such a change can be smooth or abrupt, depending on the ratio between the jamming sweep time and bandwidth. This process repeats until the jammer is turned off. The jamming signal exemplified in Fig. 2 has a T_{jam} = 1 μs and its frequency band is 840-980 MHz.

In this work, we evaluate the impact of jamming signals with different T_{jam} values over the LoRa/LoRaWAN communications. This is motivated by the existence of commercial jammers with different sweep times. Furthermore, the 840-980 MHz frequency band is also attributed to commercial jammers. Such devices can simultaneously disturb LoRa and other services, such as global system for mobile communications (GSM). Narrow band jammers targeting specific communication services can also be found on the market, but are less common up to know, due to its limited application. For this reason, we will only consider the broadband jamming signals covering the 840-980 MHz band.

Despite the similarities between the LoRa and jamming waveforms, there are important differences between these two signals. The first difference is that jamming up-chirps are not shifted because there is no information to be transmitted. The second difference refers to the bandwidth: while the LoRa signals are narrow band, the jamming signals described here are broadband, covering the 840-980 MHz band, to cover different uses and protocols. Finally, the duration of the chirps is very different: while the order of magnitude of a LoRa chirp is in the range of millisecond, a typical jamming sweep time can last a few microseconds

C. Transient interference

The transient interference we investigated results from an electric arc formed during the contact between the train catenary with the supply line located above. The catenary is a sliding metallic bar that connects the electrical system of a train to the external supply lines. From time to time along a certain route, there can be a loss of contact between the catenary and the supply lines, producing arcs. Consequently, a sequence of transient over-voltages is generated, and propagated through the internal cabling of the train.

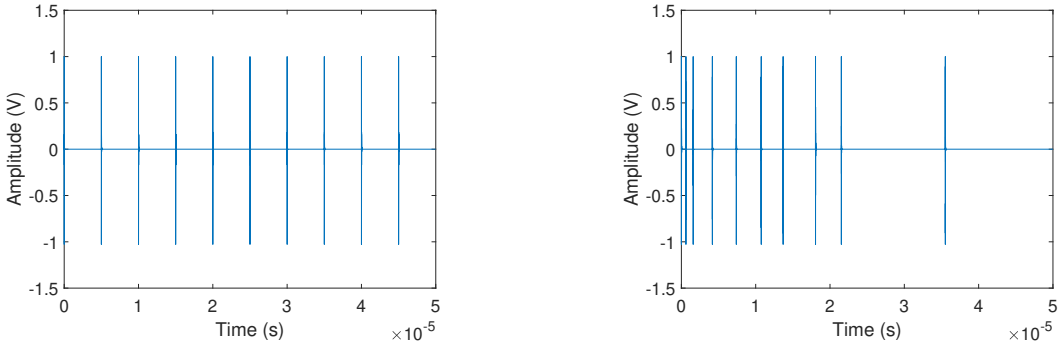


Fig. 3: Sequences of transient pulses separated by (a) a fixed time interval of 5 μs, and (b) an average time interval of 5 μs.

In most EM susceptibility test standards such as the EN 61000-4-4, this phenomenon is usually modeled as a sequence of regularly spaced pulses, as shown in Fig. 3a. However, the electric arcs in a railway do not necessarily occur on a regular basis. For this reason, we consider in our study not only the classical waveform, but also a more realistic one, composed of irregularly spaced transients, as illustrated in Fig. 3b. For a fair comparison between these two waveforms, the same number of transients within a given time interval is generated. This will result in an identical average time between transients. For example, in Figs. 3a and 3b, 10 transients are generated during 50 μs, resulting in a 5 μs time interval between transients.

III. Test bench

To evaluate the behavior of LoRa networks facing the interfering signals described in the previous section, experiments were conducted at the Electromagnetic Compatibility Laboratory of the Gustave Eiffel University, Villeneuve d'Ascq, France, as illustrated in Fig. 4. The test methodology can be described as follows.

For first experiments, LoRa and jamming signals at a fixed power are generated, keeping a very high signal-to-interference ratio (SIR). The LoRa signals are generated using transceivers, while the jamming signals are synthesized in MATLAB, and loaded in an arbitrary signal generator. Then, with the use of a dedicated computer connected to the LoRa devices, we verify that this condition leads to a null data loss.

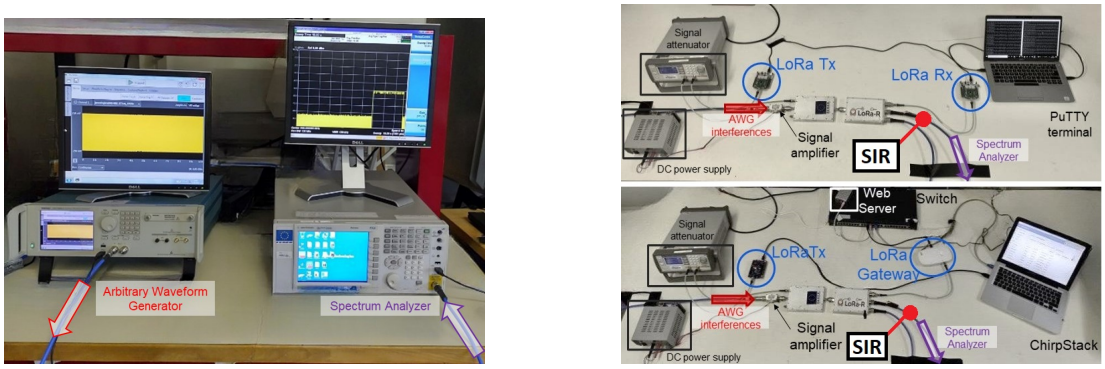
Once the stable condition described above is obtained, the SIR is gradually decreased, thanks to a variable attenuator connected to the LoRa transmitter output. The SIR is measured with the help of a spectrum analyzer configured with a central frequency of 868.3 MHz and a resolution bandwidth (RBW) of either 130 kHz (transient EMI) or 10 MHz (jamming EMI). A larger RBW was defined for the broadband jamming signal because it provides power levels which are closer to those emitted by the jammer. For each attenuation level, the reliability of the LoRa uplink (UL) communication is monitored. The criteria used to check this aspect is described in Section IV. The attenuation levels are chosen in such a way to cover the operating range of the communication system. The minimum and maximum attenuation levels correspond to the best and worst interference scenarios, *i.e.* maximum and minimum SIR, respectively.

We are mainly interested in distinguishing the behaviors of fully- and partially-implemented LoRa networks, in the presence of EMI. So, we used two different test benches, while keeping the same test methodology. In the first instance, only the physical layer (PHY) of the LoRaWAN protocol was implemented. This is illustrated in Fig. 4 (right side, up). Then, a full version of the protocol was implemented using a LoRa transceiver, an industrial gateway and servers. The test bench can be seen in Fig. 4 (right side, down). Finally, an Agilent PXA N9030A signal analyzer was used to observe the signals behaviors, in time and frequency domains.

A pair of SX1272 transceivers was used to implement a simple LoRa network. Two configurations were tested: SF = 7, CR = 4/8 and SF = 12, CR = 4/8. During the execution of the tests, information about the transmitted and received data was obtained by connecting a laptop to the LoRa devices and by running Putty (https://www.putty.org/). On the other hand, SX1276 transceivers, a Kerlink FemtoCell gateway, a Raspberry web server and the open-source network server ChirpStack (https://www.chirpstack.io/) were used to implement a complete version of LoRaWAN. The connection between the laptop where ChirpStack is running and the gateways is done through the web server and a switch. ChirpStack provided access to both the UL and downlink (DL) data flow during the tests. During the LoRaWAN tests, adaptive data rate (ADR) was not activated. The ADR is a mechanism that changes the SF and transmitting power in order to establish a trade-off between the reliability of the communication link and energy efficiency of the LoRa device.

IV. Error indicators

In order to quantify the reliability of LoRa communications in the presence of EMI, we set up error indicators. They are obtained thanks to a laptop equipped with Putty and with access to ChirpStack as well as a spectrum analyzer (see Fig. 4). In the following sub-sections, we define the error indicators of the LoRa and LoRaWAN test setups.



(a) (b)

Fig. 4: Experimental setup. (a) Signal generator and spectrum analyzer, used in all tests. (b) Up, the LoRa test setup, and down, the LoRaWAN test setup. A variable attenuator is used to control the SIR, and a dedicated laptop is used to monitor the communications. The SIR measuring points are highlighted with red bullets.

A. LoRa error indicators

During the execution of the tests, two reports on the communications are analyzed. One of them contains the exact moment where each LoRa frame is sent by the transmitter, as well as the payload content. Nevertheless, it is unpractical to analyze the entire payload content in real-time. So, we focus our attention on a specific part of the payload that contains a counter incremented each time a packet is sent. At the receiver side, we can access the exact time instant the frames arrive and their content. By comparing the transmitted and received counter, it is possible to infer about the received signal integrity.

A frequent problem in this context is the inability of the receiver to track LoRa frames, *i.e.* to identify the beginning of a specific frame. This happens when the EMI affects the synchronization field of a LoRa frame. The result is data loss, since the frame is discarded by the receiver.

During our investigation, we progressively reduce the SIR and we stop the test when the first communication problem happens (due to a corrupted counter value, a non-synchronized LoRa frame, or any other issue). The corresponding SIR is considered as the critical level. All results shown in Section V are expressed in terms of these critical SIR levels.

B. LoRaWAN error indicators

To evaluate the quality of the LoRaWAN UL during the tests, we simultaneously performed spectral analysis and verified the LoRa packets that arrive at the gateway. It allows to see if any counter measure is being taken by the LoRaWAN system against the EMI. One of the countermeasure observed during the tests consists in a DL channel change.

Our methodology considers that, if the DL signal (also known as acknowledgement, ACK) starts to be transmitted in a different channel, we must continue to reduce the SIR (indeed, frequency hopping is present in the LoRaWAN specification [7]). In other words, we do not consider this as a communication integrity problem. However, if the ACK signal disappears, we consider that the corresponding SIR level as critical.

In order to complement the graphical analyses, we, again, run Putty. It can be particularly useful when the visual inspection of the spectrum analyzer becomes difficult to be done. In this case, the test is interrupted every time we observe a warning message and the corresponding SIR level is registered.

V. Results

All results presented here are expressed in terms of critical SIR, *i.e.* SIR levels that are sufficient to cause data loss between the LoRa/LoRaWAN transmitter and the receiver. These results are shown in Figs. 5 and 6. They correspond to the EM susceptibility of the LoRa/LoRaWAN systems, facing transients and jamming EMI, respectively. More specifically, Figs. 5a, 5c, 6a and 6c refer to the LoRa system, while Figs. 5b, 5d, 6b and 6d refer to the LoRaWAN system. For each experimental configuration, 5 measurements were taken.

Results shown in Figs. 5a and 5c suggest that the LoRa system might be insensitive to the repetition rate of transient EMI. A comparison between these two graphs also reveals that higher SF lead to more negative SIR levels, meaning a higher degree of robustness, as expected. In Fig. 5a (SF = 7), the critical SIR is approximately -25 dB while in Fig. 5c (SF = 12), it is approximately -50 dB.

Experimental results related to the susceptibility of LoRa systems facing jamming interference are shown in Figs. 6a and 6c. They suggest a higher susceptibility to slower jammers, with a sweep time equal to or higher than 10 μs. Indeed, if we compare the critical SIR levels related to the sweep times within the interval 1-5 μs with those related to the 10-50 μs interval, we can observe an increase approximately equal to 50 dB. These results are particularly useful in a scenario where jammers with different sweep times are available in the black market. Our analyses indicate that certain jammers could be a threat to LoRa systems while others, not.

The results discussed here so far, which are related to the LoRa system, present a very low dispersion level, meaning that they are repeteable. This allows to more precisely describe the communication system behavior in the presence of

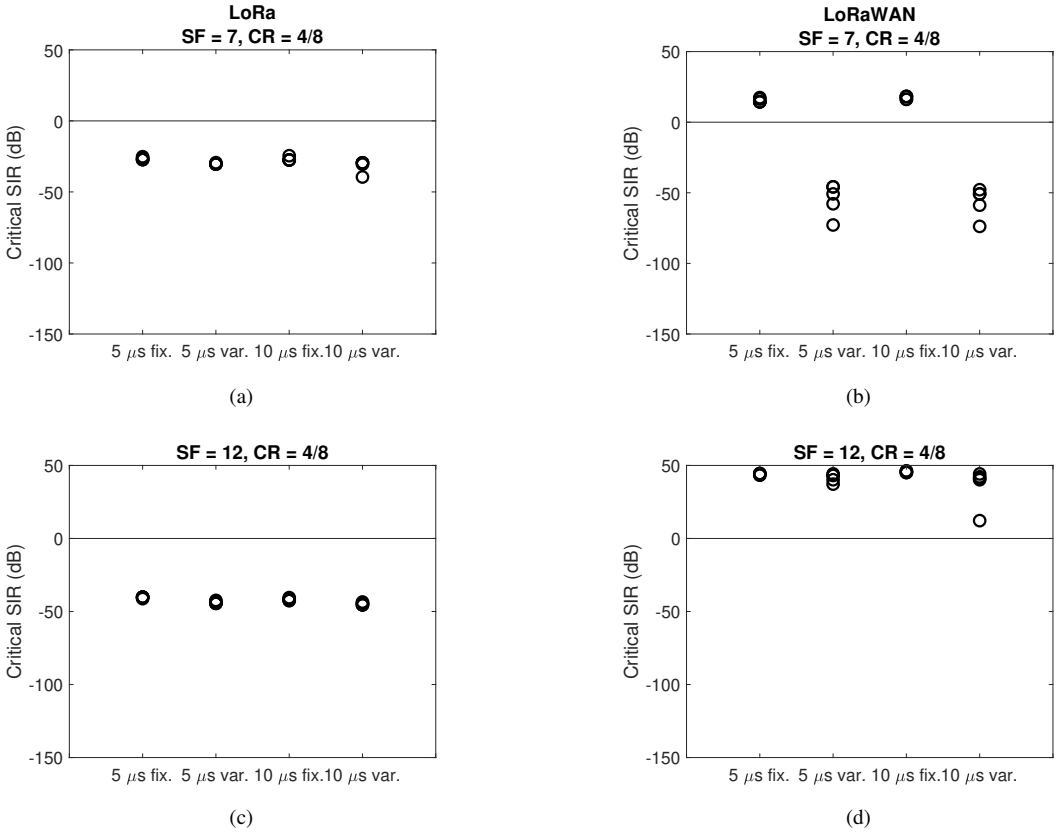


Fig. 5: Susceptibility of LoRa (left) and LoRaWAN (right) facing transient EMI with fixed and variable repetition rates.

interference. On the other hand, the LoRaWAN test results do not present clear patterns while presenting higher dispersion levels, which makes the interpretation more difficult.

Comparisons between the critical SIR levels of LoRa and LoRaWAN systems configured with the same parameters and facing the same EMI reveal different behaviors. In general, we observe that the critical SIR levels of the LoRaWAN system are equal to or higher than those measured with the LoRa test setup. The only exception is the case where T_{jam} = 30 μs (compare Figs. 6a and 6b). Furthermore, contrary to our expectations, the SF=12 LoRaWAN configuration seems to be less robust than the SF=7 one for certain types of EMI (*e.g.* compare Figs. 5b and 5d).

On the other hand, if we compare Figs. 5a and 5b, we see that the critical SIR levels are not so different when the interval between transients is variable. However, the critical SIR levels are 50 dB higher for LoRaWAN when these intervals are fixed. The dispersion levels inherent to the LoRaWAN results can be as high as 100 dB, as highlighted in Fig. 6d.

We attribute the higher dispersion levels of the LoRaWAN tests to the possible countermeasures taken by the LoRa devices. We believe that, once the receiver identifies that the UL signal is degraded, it changes the DL channel. This procedure can work well for static EMI, *i.e.* for those interfering signals that always occupy the same frequency band. However, the jamming signals under investigation are sometimes inside the channel and sometimes outside. Therefore, frequency hopping will sometimes be efficient as a countermeasure and sometimes, not. This can be easily identified when the jamming signal is fast (see Fig. 6d). As a last remark, it is important to remind that all the LoRaWAN tests were made with ADR off. We believe that the corresponding susceptibility levels could be different (maybe lower critical SIR) if the ADR was on.

VI. Conclusions

Experimental results on the EM susceptibility of LoRa/LoRaWAN systems are presented. The work is focused on two typical EMI sources found in the railway environment: the transients coming from electric arcs produced by the catenary contact, and the jamming signals coming from malicious radiofrequency devices.

Two experimental test setups were proposed. One of these test benches is designed to isolate the PHY layer of the LoRaWAN protocol, while in the second approach we implement all the network layers. Without this separation, we could not distinguish between the signal integrity problems caused by the EMI and the counter measures of the LoRaWAN protocol. Our results show that these two scenarios can lead to significantly different results. Therefore, both the physical and management layers must be considered for a complete LoRa/LoRaWAN susceptibility analysis. To the best of our knowledge, this type of analysis was never done before.

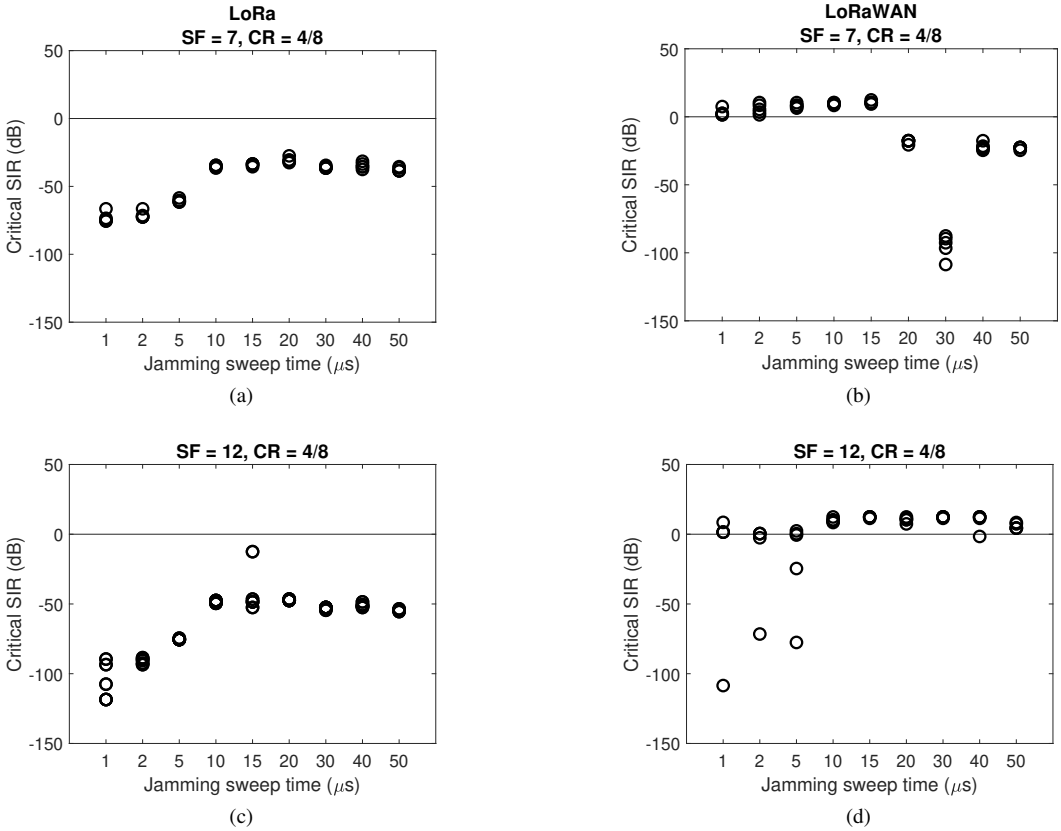


Fig. 6: Susceptibility of LoRa (left) and LoRaWAN (right) facing jamming signals with different sweep times.

Results based on critical SIR levels suggest that LoRa systems might be insensitive to the repetition rate of transient EMI, but sensitive to the jamming sweep time. In this context, the inclusion of the MAC layer changes the communication system behavior. The critical SIR levels of LoRaWAN showed to be equal to or greater than those obtained with LoRa, with the only exception being the jammer with T_{jam} = 30 μs. Nevertheless, more studies must be done in order to fully explain the behavior of LoRaWAN networks facing transient and jamming EMI.

We expect that this paper will promote discussions about the susceptibility of LoRa/LoRaWAN systems, going beyond the classical multiuser scenario, where the interference is another LoRa signal. Future studies can include, for example, narrow band or even continuous wave (CW) jammers. Besides, we intend to investigate the higher data dispersion of certain LoRaWAN test results and why LoRa and LoRaWAN behaviors diverge.

REFERENCES

[1] Semtech, *What are LoRa® and LoRaWAN®?*. Accessed on: February 10, 2022. [Online]. Available: https://lora-developers.semtech.com/documentation/tech-papers-and-guides/lora-and-lorawan/

[2] T. Elshabrawy, P. Edward, M. Ashour and J. Robert, "Practical Evaluation of LoRa under Co-Technology Interference," 2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall), 2020, pp. 1-5, doi: 10.1109/VTC2020-Fall49728.2020.9348620.

[3] I. Martinez, P. Tanguy and F. Nouvel, "On the performance evaluation of LoRaWAN under Jamming," 2019 12th IFIP Wireless and Mobile Networking Conference (WMNC), 2019, pp. 141-145, doi: 10.23919/WMNC.2019.8881830.

[4] T. Perković and D. Siriščević, "Low-Cost LoRaWAN Jammer," 2020 5th International Conference on Smart and Sustainable Technologies (SpliTech), 2020, pp. 1-6, doi: 10.23919/SpliTech49282.2020.9243739.

[5] Z. Ma, X. Chen, M. Xiao, G. K. Karagiannidis and P. Fan, "Interference Control for Railway Wireless Communication Systems: Techniques, Challenges, and Trends," in IEEE Vehicular Technology Magazine, vol. 15, no. 3, pp. 51-58, Sept. 2020, doi: 10.1109/MVT.2020.2970160.

[6] J. Tapparel, "Complete reverse engineering of LoRa PHY," 2019. [Online]. Available: https://www.epfl.ch/labs/tcl/wp-content/uploads/2020/02/Reverse_Eng_Report.pdf

[7] LoRa Alliance, *LoRaWAN™ 1.1 Specification*. Accessed on: February 15, 2022. [Online]. Available: https://lora-alliance.org/wp-content/uploads/2020/11/lorawantm_specification_-v1.1.pdf