A simulation tool to interpret error rates in LoRa systems under frequency-sweeping jamming

Artur Nogueira de Sao Jose, Virginie Deniau, Alexandre Boé, Eric Pierre Simon

URSI GASS 2023, Sapporo, Japan, 19 – 26 August 2023

A simulation tool to interpret error rates in LoRa systems under frequency-sweeping jamming

Artur N. de São José[(1)], Virginie Deniau*[(1)], Alexandre Boé[(2)(3)], and Eric Pierre Simon[(2)(3)]
(1) COSYS-LEOST, Université Gustave Eiffel, IFSTTAR, Université de Lille, F-59650 Villeneuve d'Ascq, France;
e-mail: artur.nogsj@gmail.com; virginie.deniau@univ-eiffel.fr
(2) Univ. Lille, CNRS, USR 3380—IRCICA—Institut de Recherche sur les Composants Logiciels et Matériels pour l'Information et la Communication Avancée, F-59000 Lille, France; e-mail: eric.simon@univ-lille.fr
(3) Univ. Lille, CNRS, Centrale Lille, Univ. Polytechnique Hauts-de-France, UMR 8520 - IEMN - Institut d'Electronique de Microélectronique et de Nanotechnologie, F-59000 Lille, France

Abstract

In a recent experimental study, we submitted a LoRa system to jamming attacks, consisting of frequency-sweeping intentional electromagnetic interference. In the present contribution, we reproduce this scenario in a computational environment aiming to explain the previously observed phenomena based on the LoRa symbol extraction process. Simulation results confirm that the susceptibility of LoRa systems is influenced by the interference sweep time. A good agreement between simulation and experiments was observed for sweep times between 5 and 20 µs.

1 Introduction

The railway industry is nowadays facing a digital revolution based on the introduction of new wireless communication systems [1, 2]. In this context, long-range wide area network (LoRaWAN) has been showing to be an efficient remote maintenance solution [3]. However, to operate in harsh electromagnetic (EM) environments such as railways, it is necessary to ensure the robustness of LoRaWANs face to intentional electromagnetic interference (IEMI) [4]. Indeed, IEMI is increasingly widespread nowadays due to the low prices and the easy manipulation of jammers. The first indication of a jamming attack is given by the LoRaWAN physical layer (PHY) signal integrity. It is therefore necessary to analyze the EM susceptibility of LoRa communications face to IEMI. However, it can be time consuming to run LoRa experiments with a statistically significant amount of results [3]. Therefore, it can be of particular interest to have a computational tool allowing one to quickly make predictions about the robustness of a LoRa communication link. In this work, we propose a simulation tool to accomplish such task.

2 Characterizing the signals

In this section, we detail the main characteristics of the LoRa and jamming signals. We also show how these two signals could possibly interact at the input of a LoRa receiver, resulting in symbol and bit errors. Figure 1 is a time-frequency plot of these two signals. As we can see, both can be described as sequences of chirps which sweep a certain frequency band during a fixed interval of time. This interval of time is the *symbol time* in the case of LoRa signals, while such repetition interval is known as *sweep time* (ST) in the case of jamming signals. The LoRa symbol time ranges from 1.025 ms to 32.8 ms, for spreading factors (SFs) of 7 and 12, respectively. On the other hand, jamming STs can change from one device to another. Commercial values typically vary from 1 µs to 50 µs [4]. In this work, we consider a LoRa symbol time of 1.025 ms (SF = 7), while the impacts of several jamming STs are evaluated. In terms of operating frequency bands, jamming signals are usually broadband devices once the goal is typically to jam several devices and communication services at the same time. In our study, we consider a jamming frequency band that ranges from 840 MHz to 980 MHz and a LoRa bandwidth of 125 kHz. Among the many characteristics of these signals, there is one which is of particular importance when it comes to the study of error rates caused by IEMI. It is the time instant where the LoRa instantaneous frequency abruptly changes from its maximum to its minimum value. Let us call this transition time instant T_{tr} ($T_{tr} = 200\,\mu s$ in the example given in Fig. 1). It is unique for each transmitted symbol. Therefore, if the IEMI corrupts this particular part of the LoRa waveform, the symbol information is compromised. As we can observe in Fig. 1, the jamming signal is not always within the LoRa channel boundaries. For the symbol corruption to happen, it is necessary that the IEMI is within these boundaries precisely at T_{tr}. The probability of such an event to occur depends on the jamming ST, the LoRa channel location and on the time shift between the IEMI and LoRa waveforms. In this work, we focus on the ST effects, so the phase shift is random, as described in the next section.

3 Proposed simulation tool

We developed a simulation tool[1] to understand better how the presence of frequency-sweeping IEMI can affect the demodulation process described in the previous section. In-

[1] Available at: `https://github.com/ansj1988/ursi2023`

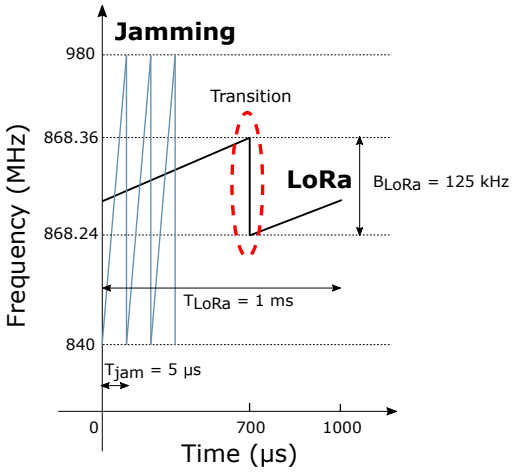

Figure 1. Time-frequency plot showing the main characteristics of LoRa signals and frequency-sweeping IEMI.

deed, the IEMI signal observed by a LoRa receiver is not necessarily identical to the one emitted by the jammer. This is due to the IEMI waveform modifications caused by specific electronic components of the LoRa receiver such as analog and digital filters and analog-to-digital converters (ADC), as well as the mixer and the down-chirp at the demodulation stage. In a worst-case scenario, the jamming signal spectrum at the last stage has one or more components with more energy than the received LoRa symbol, leading to the selection of a spurious symbol. To explain the whole simulation chain, we use the block diagram illustrated in Fig. 2. It can be divided into two big blocks, to be detailed in the next sub-sections: the first one comprises the processes that occur before the summation block (combining the signals) and the second one comprises the processes that occur after the summation block (processing the resulting signal). All our simulations are based on baseband versions of the LoRa signal and IEMI.

3.1 Combining the LoRa and jamming signals

The three input blocks in Fig. 2 represent the signals observed by the LoRa receiver: the useful LoRa signal, the IEMI and the background noise. Before combining these signals, however, we must ensure that they were sampled at the same rate during the same interval of time. Given that the LoRa receiver is not designed to receive and reconstruct spurious signals such as the frequency-sweeping IEMI, we need to consider the aliasing phenomenon suffered by the jamming signal due to the LoRa low sampling rate. Furthermore, we must take into account the modifications suffered by the jamming signal due to the analog filters typically present in radiofrequency frontends such as the SX1257 [5], whose bandwidth is very narrow compared to that of the IEMI. To simulate the distortions suffered by the jamming signal, we first generate a frequency-sweeping IEMI waveform based on a sufficiently high sampling rate of $250\,\mathrm{MS\,s^{-1}}$. We then apply a random time delay to avoid a bias caused by a fixed time shift between the LoRa signal and the IEMI, as previously discussed in Section 2. Then, we apply a frequency shift to the IEMI signal. We do that to take into account the fact that the IEMI frequency components seen by a LoRa receiver are equally spaced by $1/\mathrm{ST}$ Hz and they will only "invade" LoRa channels whose central frequencies are multiples of this value. For more details, please refer to [4]. Finally, we use a down-sampler with a factor of 1000 to convert the original IEMI sampling frequency of $250\,\mathrm{MS\,s^{-1}}$ into $250\,\mathrm{kS\,s^{-1}}$, which is the sampling rate used to generate the LoRa signal and the noise. The signals length is 1.025 ms, which is the $\mathrm{SF} = 7$ LoRa symbol time.

3.2 Processing the resulting signal

Once the three signals are sampled with the same rate during the same time interval, they are added to form a resulting signal. This signal is sent to a group of blocks inspired on LoRa baseband processors such as the SX1303 [6]. The signals pass through a LoRa filter with a bandwidth of 125 kHz. In the sequence, they are down-sampled to $125\,\mathrm{kS\,s^{-1}}$, which is the actual sampling rate adopted by commercial LoRa receivers with $\mathrm{SF} = 7$. The last stage is the conventional LoRa symbol extraction process. It consists on the generation of a raw down-chirp, which is a signal whose instantaneous frequency linearly reduces with time. The input signal is then multiplied by the raw down-chirp. In the absence of interference and with a relatively high level of signal-to-noise ratio (SNR), the result of this multiplication is a sine wave whose frequency uniquely represents one LoRa symbol. Therefore, the spectrum is simply an impulse in the frequency domain and the detection can be easily performed with an argmax function. In such situation, the output of the argmax function is an integer number from the set $\{0,1,2,...,2^{SF-1}\}$, each of them representing a frequency sample and, therefore, one LoRa symbol. However, as we will see in the following section, the presence of IEMI can affect this process and generate symbol detection errors.

4 Results

The simulation results are presented here together with the experimental results from [4]. These experiments were run in conducted mode, meaning the connection between the LoRa devices is established with cables instead of antennas. In both simulations and experiments, the EM susceptibility of a LoRa communication system with a transmitting frequency of 868.0 MHz was evaluated based on a frequency-sweeping IEMI with the following different sweep times: $\{1,2,5,10,20\}$ µs and with a jamming bandwidth of 140 MHz. All these parameters values are based on signals emitted by commercial jammers. The comparison between simulations and experiments will allow us to evaluate the capability of the proposed tool to make predictions, as well as its limitations. Figure 3a summarizes the simulation results in terms of symbol error rates (SER),

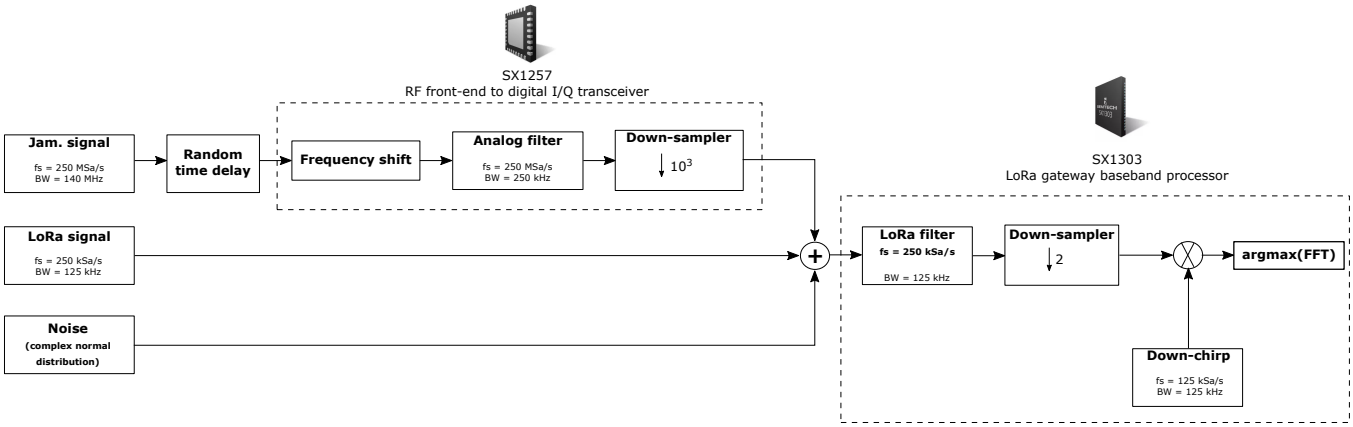

Figure 2. Summary of the proposed simulation tool with references to the corresponding physical components.

while the experimental results are shown in Fig. 3b in terms of byte error. In both cases, the error rates are evaluated within a range of signal-to-interference ratios (SIR). The SIR calculation follows the methodology described in [4]. All simulations were run with a fixed SNR of 20 dB.

4.1 Interpreting the results

Comparing the simulation and experimental results, we distinguish two groups of results. Group 1 which contains the values $\{5, 10, 20\}$ µs presents a good agreement between simulation and measurement results, while Group 2 which contains the values $\{1, 2\}$ µs reveals significant differences.

4.1.1 Group 1: $5-20$ µs sweeping times

In Figures 3a and 3b, the communication starts to be affected when the SIR is approximately -30 dB. Simulation indicates that the communication is completely degraded when the SIR reaches approximately -50 dB. However, experimental error rate curves are sharper, with a smaller SIR dynamic range. This difference can be due to the ideal propagation conditions in the simulation. Let us proceed with the analysis of the Group 1 curves. In Figs. 3a and 3b, the yellow, purple and green traces appear in the same order. The fact that, among these three traces, the yellow one is closer to 0 dB means that the LoRa communication is more sensitive to IEMI with a 5 µs sweep time. Analogously, the fact that the green trace contains smaller levels of SIR means that the LoRa communication is more robust to IEMI with a sweep time of 20 µs. Another way of understanding the behavior of the Group 1 interferences is through the LoRa symbol extraction process. Figure 4a represents the results of the last block (argmax[FFT]) of the diagram illustrated in Fig. 2, where a single peak (blue curve), corresponding to the transmitted symbol, in the frequency domain is normally expected. However, as we can see, the presence of IEMI produces several spurious peaks, which can potentially be detected as symbol instead of the initial transmitted symbol. The presence of the jamming signal can then disturb the LoRa symbol extraction process and introduces symbol errors at the reception.

4.1.2 Group 2: $1-2$ µs sweeping times

These curves present a different behavior compared to those of Group 1. In Fig. 3a, the SER stagnates around 55% when the SIR is reduced up to approximately -50 dB. Such behavior can be explained by the IEMI characteristics observed by the LoRa receiver during the symbol extraction process, as illustrated in Fig. 4b. This figure shows that, contrary to the IEMI sweep times greater than 5 µs which produce spurious peaks in the frequency domain, the IEMI with sweep times inferior to 5 µs have nearly flat spectra. A flat IEMI spectrum affects less the SER than a multi-peak IEMI spectrum because it does not create the risk to detect wrong symbols during the LoRa symbol extraction process. So, the simulation curves can be explained but do not correspond the experimental results in which a continuous increase of the SER levels is obtained. This shows that the simulation tool do not include all the factors impacting the SER, in case of 1 and 2 µs sweeping times.

5 Conclusions

In this work, we proposed a simulation tool that can enrich the EM susceptibility analysis of LoRa systems submitted to frequency-sweeping IEMI. Simulations results present a good agreement with experiments for sweep times between 5 and 20 µs, which correspond to the typical values of commercial jammers. Future works include the addition of a standard LoRa PHY frame structure to the simulator (in the current version, only random payload symbols are sent) and the definition of analytical expressions for the SER of LoRa systems under frequency-sweeping IEMI.

Acknowledgements

This work was performed in the framework of the LoRa-R project, which is co-financed by the European Union with

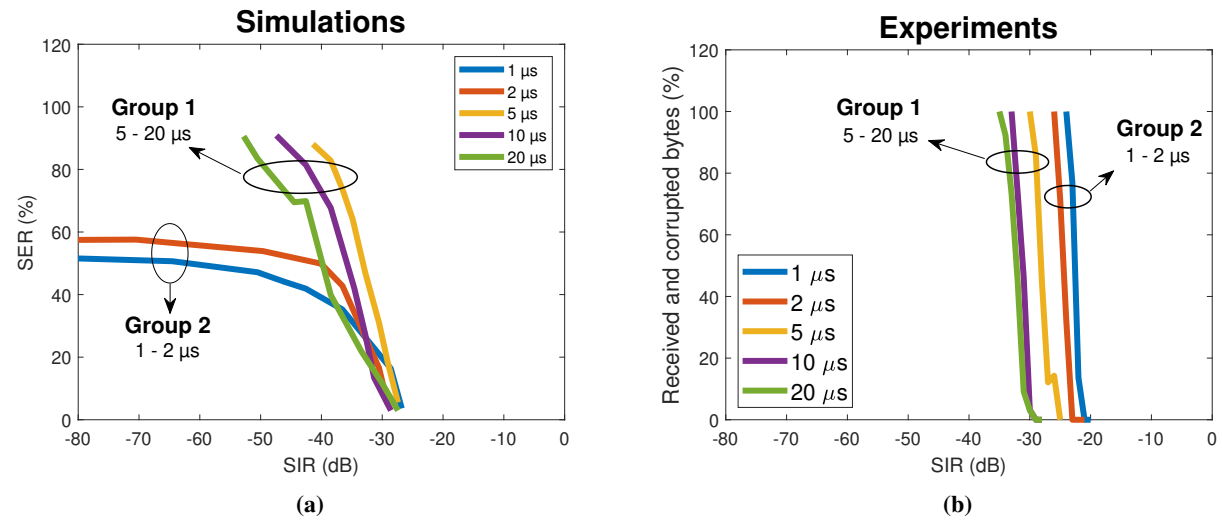

Figure 3. LoRa error rates obtained with a transmitting frequency of 868.0 MHz. (a) Simulations. (b) Experiments [4].

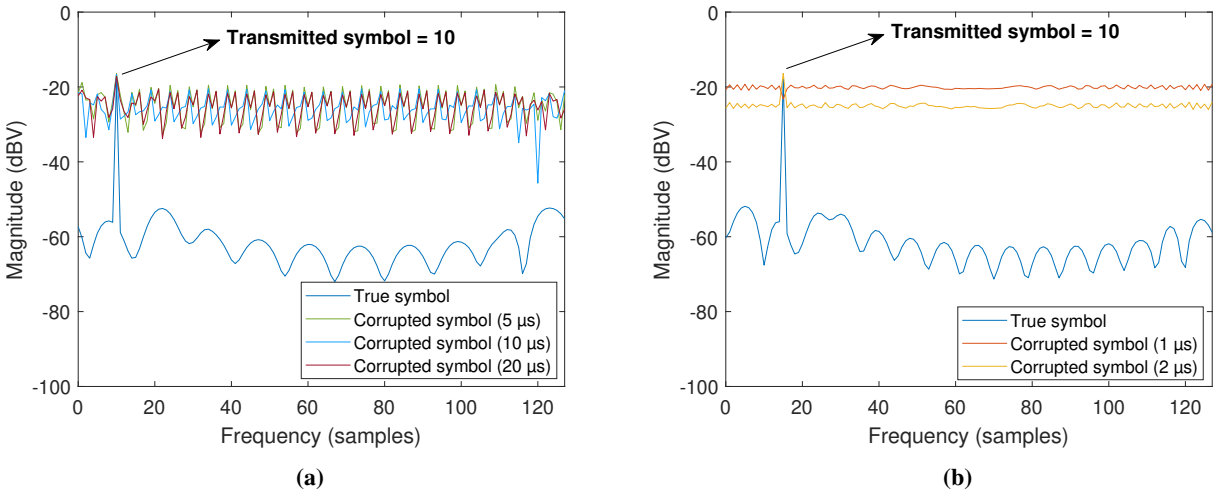

Figure 4. 868.0 MHz LoRa symbol extraction in the presence of IEMI with different sweep periods. (a) Group 1: $5-20$ µs. (b) Group 2: $1-2$ µs.

the European Regional Development Fund, the Hauts de France Region Council, and the SNCF railway company.

References

[1] R. He, B. Ai, G. Wang, K. Guan, Z. Zhong, A. F. Molisch, C. Briso-Rodriguez, and C. P. Oestges, "High-speed railway communications: From gsm-r to lte-r," *IEEE Vehicular Technology Magazine*, vol. 11, no. 3, pp. 49–58, 2016.

[2] Y. Alsaba, M. Berbineau, I. Dayoub, E. Masson, G. M. Adell, and E. Robert, "5g for remote driving of trains," in *Communication Technologies for Vehicles*, F. Krief, H. Aniss, L. Mendiboure, S. Chaumette, and M. Berbineau, Eds. Cham: Springer International Publishing, 2020, pp. 137–147.

[3] A. N. de São José, N. Chopinet, E. P. Simon, A. Boé, T. Vantroys, C. Gransart, and V. Deniau, "A comparative analysis of lora and lorawan in the presence of jammers and transient interference," in *2022 International Symposium on Electromagnetic Compatibility – EMC Europe*, 2022, pp. 586–591.

[4] A. N. De São José, V. Deniau, C. Gransart, T. Vantroys, A. Boé, and E. P. Simon, "Susceptibility of lora communications to intentional electromagnetic interference with different sweep periods," *Sensors*, vol. 22, no. 13, 2022.

[5] *SX1257 - Low Power Digital I and Q RF Multi-PHY Mode Transceiver*, Semtech, 3 2018, rev. 1.2.

[6] *SX1303 - LoRa Gateway Baseband Processor*, Semtech, 10 2020, rev. 1.2.