On the performance evaluation of LoRaWAN under Jamming

Ivan Marino Martinez Bolivar, Fabienne Nouvel, Tanguy Philippe

On the performance evaluation of LoRaWAN under Jamming

Ivan Martinez*, Philippe Tanguy†, Fabienne Nouvel*
*IETR, UMR 6164 CNRS — Institut National des Sciences Appliquées de Rennes, Rennes, France.
†Lab-STICC, UMR 6285 CNRS — Université Bretagne Sud, Lorient, France.

{ivamarti,nouvel}@insa-rennes.fr*, philippe.tanguy@univ-ubs.fr†

***Abstract*—In this paper we evaluate the performance of the LoRaWAN protocol under channel-aware and channel-oblivious jamming. We obtained three key results, namely: (i) LoRaWAN networks are particularly vulnerable to jamming attacks, we have shown that the network throughput of the simulation scenarios chosen can be decreased by $\sim 56\%$ when 25 jammers send unauthenticated packets permanently in the network, (ii) the gateway's performance is dramatically affected as a consequence of jammers. Our results suggest that the resources used to process packets coming from jammers could be 100 times higher than that of regular end-devices, and (iii) the network performance impact of jammers is highly correlated with the jammer class. We have shown that channel-oblivious jammers impacts the network performance widely, while channel-aware jammers impact the network locally. For this, we propose an ns-3 LoRaWAN module extension incorporating jamming attacks.**

***Index Terms*—LoRaWAN, IoT, Jamming, NS3, Network performance, LPWAN Networks, ALOHA**

I. Introduction

IoT technologies are key enablers of a huge number of application domains in our current society. Indeed, according to Cisco's expectations 50 billions of devices will be connected by 2020 [1], and according to the McKinsey Global Institute the IoT sector could have an annual economic impact of €3.15 trillion to €11.1 trillion by 2025. Low Power Wide Area Networks (LPWAN), such as LoRaWAN, SigFox and NB-IoT are new wireless protocols that have emerged to fill the gap left by classical wireless networks. Their main characteristic is to provide modest data-rates and wide coverage while at the same time offering very low power consumption.

Providing this trade-off between low power consumption and wide coverage cannot be reached without using very constrained end-devices (EDs). As a consequence, security is a challenge in LPWAN. Security in LPWAN technologies is currently provided by symmetric-key algorithms such as AES 128 at upper levels. In the case of LoRaWAN it offers application level payload encryption and network level integrity. This means that, if implemented well, LPWAN networks can reasonably be secured against MAC or upper level attacks such as replay and DoS. But nevertheless, this does not shield them against jammer-type attacks. A jamming attack takes place at the PHY layer, it could be an external node that sends random unauthenticated packets with the aim of disrupting communications by decreasing the SINR.

In this paper, we evaluate the performance of the LoRaWAN protocol under jamming attacks by following a simulation approach. To do that we perform multiple simulations where LoRaWAN networks are put under attack by jammers. We evaluated both channel-aware and channel-oblivious jammers. The former being able to sense the network and react based on its measurements, while the latter sending unauthenticated packets in a regular basis with the aim of disturbing the communication between EDs and Gateways (GWs).

ISBN 978-3-903176-18-8 ©2019 IFIP

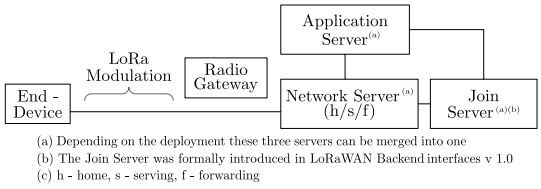

Fig. 1. Top level LoRaWAN Architecture

The remainder of this paper is structured as follows. Section II gives an overview of the LoRaWAN protocol. In section III previous works done on jamming and LoRaWAN modeling is presented. Section IV gives an overview of the ns3-module extension we developed. Section V describes the simulation scenarios and corresponding results. Finally, Section VI provides a conclusion and future directions of our work.

II. LoRaWAN

LoRaWAN networks are defined in the LoRaWAN standard (v1.0 and v1.1) [2,3]. They are designed for allowing wireless connectivity for battery-based EDs that can be mobile or fixed. They modulate the signals in the Sub 1 GHz ISM band using a proprietary spread spectrum modulation, which is a variant of a Chirp Spread Spectrum modulation (CSS). LoraWAN networks are typically deployed in a star topology.

As shown in Fig. 1, a LoRaWAN network is composed by EDs, Gateways (GWs), a Network Server (NS), an Application Server (AS) and a Join Server (JS).

At the PHY layer, the band used in Europe is the g1 band $(868 - 868.6MHz)$ with a maximum transmission power of $14\ dBm$ and a bandwidth of $125\ kHz$. EDs and GWs must respect a duty-cycle (DC) according to the operational band. At the MAC layer, it uses an ALOHA-type protocol. Security in LoRaWAN is offered by means of application payload encryption and network level authentication (AES-CMAC).

A. LoRa Time on Air

As described before, LoRaWAN Networks are subject to DC restrictions. To manage that, it is necessary to be able to

calculate the time on air of a given modem configuration [4]. The symbol duration is given by:

$$T_{sym} = 2^{SF}/BW \tag{1}$$

The necessary time to send a packet is given by the sum of the preamble and payload duration:

$$T_{packet} = T_{pre} + T_{pay} \tag{2}$$

where T_{pre} and T_{pay}, are given by Eq.s (3) and (4):

$$T_{pre} = T_{sym} \cdot (n_{bytes} + 4.25) \tag{3}$$

$$\begin{aligned} T_{pay} &= T_{sym} \cdot (8 + \max(ceil(Sym_{Nb}) \cdot (CR+4), 0)) \\ Sym_{Nb} &= \frac{8 \cdot PL - 4 \cdot SF + 28 + 16 \cdot CRC - 20 \cdot H}{4 \cdot (SF - 2 \cdot DE)} \end{aligned} \tag{4}$$

where PL is the number of payload bytes, $H = 1$ when the header is enabled, $DE = 1$ when the low data rate optimization is enabled, $CRC = 1$ when CRC is enabled and CR the coding rate *(1 to 4)*. The time for the received windows is also modeled for the case where there is no confirmed traffic. The time required to detect a preamble is given by Eq. (5) and it is used to compute the first receive window.

$$T_{dpre} = T_{rx1} = N_{dsym} \cdot T_{sym} \tag{5}$$

where $N_{dsym} = 8$ for SFs 11 and 12, and $N_{dsym} = 12$ for the others [5]. For the second receive window, we model it as the T_{CAD} (Channel Activity Detection) [4] given by Eq. (6).

$$T_{rx2} = T_{CAD} = (2^{SF} + 32)/BW \tag{6}$$

III. Previous Works

Most of the research done on LoRaWAN simulation/modeling have been focused on characteristics such as coverage, scalability, delay, throughput, collisions and energy consumption [6]–[9]. However, the simulation/modeling of all these features in LoRaWAN networks under jamming attacks have received very limited attention.

In [8,9] a LoRaWAN ns-3 module was presented. They modeled a LoRa-based IoT network for a typical urban scenario showing that LoRa networks scale well achieving packet success rates above 95% in presence of a number of EDs in the order of 10^4. Then, they extended their work to networks with confirmed traffic. We extended this ns3 module for LoRaWAN networks in the presence of jamming nodes.

Regarding security issues in LoRaWAN Networks, several works have been done for attacks at the MAC and upper layers [10]–[12], showing that there are vulnerabilities in LoraWAN (v1.0 and v1.1) that can be exploited. They also proposed some countermeasures that mostly rely on the implementation of cryptographic algorithms.

As regards jamming attacks in LoRaWAN. In [13] a selective jamming attack on a LoRaWAN Network was implemented by using commodity hardware, showing success rates close to 100%.

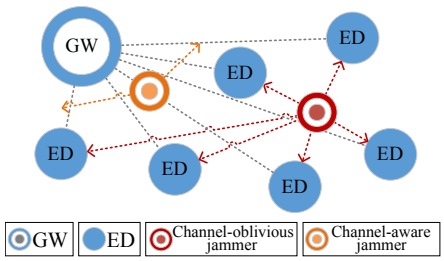

Fig. 2. Jamming Categories

With regards to collision modeling in LoRaWAN Networks, three approaches are proposed in the literature. The first one was proposed in [14], it considers that collisions in LoRaWAN networks mostly occur when two or more transmissions happen at the same time with the same SF. Thus, the interference is modeled based on co-channel rejection measurements for all couples of SF. The second one considers that even if there are two or more events at the same SF, a packet can be successfully demodulated at the GW due to the capture effect [7,15]. There are some works suggesting that the frequency offset due to hardware limitations should be considered as a parameter when it comes to define if a collision occurred or not [7]. For our simulations we keep the first approach proposed in [14].

In [6] the impact of interference on LoRaWAN scalability is studied. The authors developed a simulator based on real transmission measurements showing that a packet is completely lost when the preamble is affected by the interfering packet.

Based on this literature review, we conclude that, to the best of our knowledge, this paper is the first one that provides a detailed event-based simulator that allows to simulate LoRaWAN Networks in the presence of jamming nodes. We consider both channel-oblivious and channel-aware jammers.

IV. NS3-Based module for LoRaWAN Jamming attacks

A. Threat model

As a threat model, we consider that the jammer is not a part of the network and that all the nodes in the network meet the LoRaWAN standard and band restrictions. In contrast, jammers, that from the hardware point of view have the same characteristics as regular EDs, are capable of not following the standard. Furthermore, as presented in Table I, we consider both $14dBm$ and $20dBm$ as transmission power, the former selected so that it is the same as regular nodes and the latter allowing jammers to transmit strong enough to take advantage of the capture-effect and to have higher jamming success rates.

As shown in Fig. 2 we classify jammers into two categories according to their capability of sensing the medium: *channel-aware* and *channel-oblivious*.

a) ***Channel-aware jammer****:* It listens to one of the g1 sub-bands and once it detects any activity on the channel, it sends back a packet on the same channel and SF. The attack timing, as shown in Fig. 3, is defined in Eq. (7):

$$T_{jam} = T_{dpre} + T_{sw} + T_{tx} \tag{7}$$

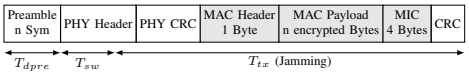

Fig. 3. Channel-Aware jammer timing

TABLE I
THREAT MODEL - JAMMER TRANSMISSION PARAMETERS

Parameter	Channel-aware	Channel-oblivious
DC	1	0.2 to 1
SF	7 to 12	7 to 12
Packet Size	50 $bytes$	10000 $bytes$
Tx Power (P_{TXj})	20 dBm	14 dBm and 20 dBm
Packet time on air	*See Eq. 2*	
Sensitivity	*SX1272 [4]* (same as ED)	
Bands	868.1, 868.3 and 868.5 MHz	

where T_{dpre} is the time necessary to detect a frame, T_{sw} the switching time, which is the time required to switch from reception to transmission state, and T_{tx} the duration of jamming. The response time of the attack is the sum of the two duration T_{dpre} and T_{sw}. T_{dpre} is modeled by using Eq. (5) and T_{sw} is set as $0s$, which is the ideal case.

*b) **Channel-oblivious jammer**:* This jammer does not listen the channel, it transmits periodically on all the three channels *(one at a time)* with a given DC, and it selects a random SF each time a packet is sent.

B. Jammer modeling in NS3

To model the LoRaWAN Network and the attacker classes described before, we take as a base the ns3 module for LoRaWAN developed in [8] and extended in [9].We extended this module in order to add support for jammer nodes that do not meet the LoRaWAN standard. [16]. Jammers are capable of:

- Not follow the regulated parameters of the corresponding sub-band (DC, packet length and Tx power)
- Sense the medium in order to detect packets coming from other EDs and GWs.
- Send back unauthenticated packets if a regular packet is detected.
- Deterministically select the sub-band to transmit.

Thus, we added three classes to the ns3 module in order to model the behaviour of a jammer:

1) Application jammer and its helper : it defines three parameters: application period, packet length and initial transmission delay.
2) JammerLoraMac : this class defines the MAC layer of the jammer. In this class, jammers have the same functions of a normal EDs but DC limitation was removed, we also add the possibility of deterministically selecting the sub-band for each transmission, so that it can be predefined.
3) JammerLoraPhy : This class defines the PHY layer of the jammer. In this class we implement the T_{jam}, which is time necessary to detect and send back a packet as described previously in Eq. (7).

We also added several functions to already existing classes:

1) LoRa Phy : In this class we add three functions that implement the timing necessary to model the behaviour jammers, as defined in Eq.s (5), (6) and (7).
2) Lora Interference Helper: In this class we extend the model to add support to the capture-effect. We consider that there are two situations in which two packets are overlapped: In the first case, the strong packet arrives first and the radio transceiver synchronizes to it. As long as the stronger packet's signal-to-interference power ratio exceed a threshold of 6 dB, it is received normally. In the second case, the stronger packet arrives latter, the radio transceiver synchronizes to the weak packet resulting in both packets being lost. The selection of this threshold and the general scheme is based on actual measurements and from previous investigations as presented in [7,14].

As for the detection of packet losses, a packet lost is interpreted as a consequence of three causes: **(i) Packet under sensitivity**: the reception power was under the sensitivity of the GW [17], **(ii) Packet rejection:** the packet was dropped at the GW because all the 8 reception paths were occupied [8,17] and **(iii) Packet collision:** we consider the model proposed Goursaud in [14], and we also incorporated the capture-effect as described before.

V. RESULTS AND DISCUSSION

A. Simulation Scenarios

We considered a LoRaWAN cell consisting of several EDs and one GW under jamming attacks. EDs are uniformly distributed around the GW within a radius of 7500 m, which is the maximal distance a GW can receive a packet on a SF 12. EDs and GWs follow the requirements defined in the SEMTECH SX1272 and the SX1301 [4,17].

The static EDs belong to Class A and there is no support for confirmed traffic. They are configured to use the best SF possible, so that the received power at the GW is above the GW sensitivity. As regards the ED's application profile, we considered a payload length of 50 $bytes$, and an application period of 30 min. The network operates in the g1 band with a bandwidth of 125 kHz.

In regards to the jammer's threat model, we simulate two jammers: channel-aware and channel-oblivious as described in Section IV and Table I.

We have considered different combinations of the number of EDs and jammers in the LoRaWAN cell described before. We define three different scenarios as described below with parameters reported in Table II.

Scenario a): In this simulation scenario we evaluated the network performance impact of channel-oblivious jammers. We simulate a LoRaWAN network with 100 EDs and 1 GW, the number of jammers vary from 0 to 25, and the jammer's DC vary from 0.2 to 1.

Scenario b): With this scenario we evaluate the impact of channel-oblivious jammers sending packets permanently on the GW performance. We simulate a LoRaWAN cell with 1 GW and we vary the number of EDs from 100 to 300, the number of permanent jammers vary from 0 to 40.

TABLE II
SIMULATION SCENARIOS

Parameter	Scenario a)	Scenario b)	Scenario c)
Number of GWs	1	1	1
GW reception Paths	8	8	8
GW sensitivity	*SX1301 [17]*	*SX1301 [17]*	*SX1301 [17]*
Number of ED	100	$100 - 300$	1000
ED's payload length	50 *bytes*	50 *bytes*	50 *bytes*
ED's packet time on air	*See Eq. 2*	*See Eq. 2*	*See Eq. 2*
ED's transmission Power	14 dBm	14 dBm	14 dBm
ED's sensitivity	*SX1272 [4]*	*SX1272 [4]*	*SX1272 [4]*
ED's deployment	$U(0, 7500m)$	$U(0, 7500m)$	$U(0, 7500m)$
ED's application period	30 min	30 min	30 min
ED's duty-cycle	0.01	0.01	0.01
Band	g1 (125 kHz)	g1 (125 kHz)	g1 (125 kHz)
LoRaWAN class	A (no ACK)	A (no ACK)	A (no ACK)
Jammer TX parameters	*See Table I*	*See Table I*	*See Table I*
Channel-oblivious jammer	$0 - 25$	$0 - 40$	10, $DC = 0.5$
Channel-aware jammer	0	0	10
Initial transmission delay	$U(0, 1h)$	$U(0, 1h)$	$U(0, 1h)$
Simulation time	1000 h	1000 h	1000 h
T_{sw}	—	—	$0s$

Scenario c): We simulate a LoRaWAN cell with 1 GW and 1000 EDs. This cell was put under attack by 10 channel-oblivious ($DC = 0.5$) and 10 channel-aware jammers.

B. Results

Scenario a) Fig. 4 presents the network performance of a LoRaWAN network under channel-oblivious jamming when varying the number of jammers, the jammers' DC, and the jammers' Tx power. We considered four different performance metrics: packet loss probability, collision probability, packet rejection probability and network throughput.

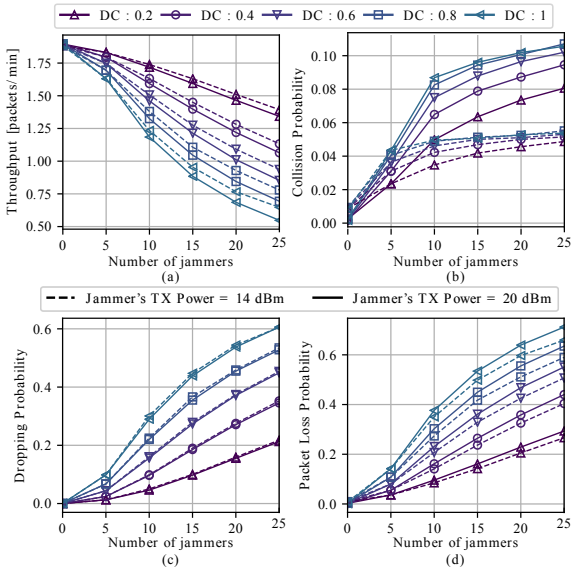

Fig. 4. Network performance of LoRaWAN Networks under channel-oblivious jammers — (a) Network throughput, (b) Collision probability, (c) Dropping probability and (d) Packet loss probability

From Fig. 4 (a) we can observe that the performance degrades rapidly by increasing the number of jammers and its corresponding DC. For example, in a cell configuration with 100 EDs without jammers, the network achieves a throughput of 1.9 $packets/min$. Adding 10 jammers with a $DC = 0.6$ causes this number to fall to 1.45 $packets/min$ and 1.50 $packets/min$ respectively. For the worst case (*25 channel-oblivious jammers with* $DC = 1$), this number fall to only 0.55 $packets/min$ and 0.64 $packets/min$ respectively.

From Fig. 4 (b) and Fig. 4 (c), we note that the vast majority of losses are due to packet dropping at the GW. Indeed, for the worst case considered *(25 channel-oblivious, DC=1,* $P_{TXj} = 20\ dBm$*)*, the proportion of packet losses due to packet collision is only 0.10, while packet dropping is 0.60.

It should also be noted that the collision probability is highly correlated with the jammers' transmission power. For example, in the case where the network is put under attack of 25 jammers the packet loss probability is 2.1 times bigger when the $P_{TXj} = 20\ dBm$. This is due to the fact that, the signal-to-interference ratio is lower when jammers transmit with higher transmission power.

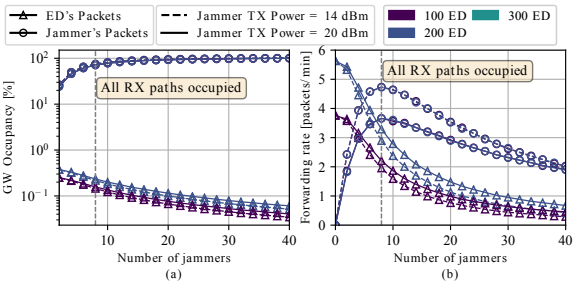

Fig. 5. GW performance impact of Channel-oblivious jammers (DC=1) — (a) GW occupancy and (b) packet forwarding rate.

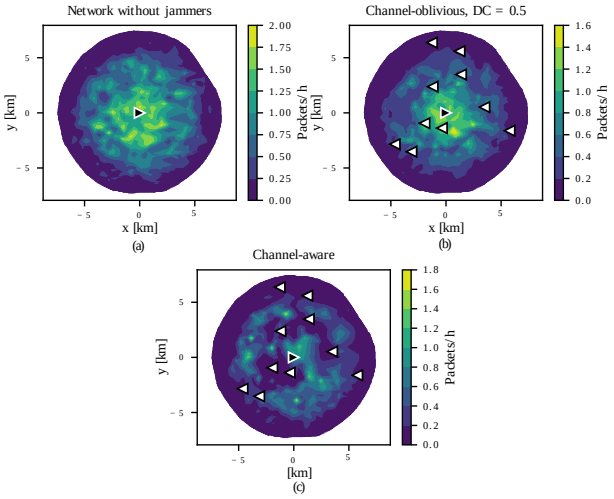

Fig. 6. ED's throughput ($packets/h$) of a LoRaWAN network under jamming attacks, ▶ represents the GW and ◁ represents a jammer.

Scenario b) Fig. 5 presents the GW performance when the network is under channel-oblivious jammerg with a $DC = 1$. We considered two metrics: the *GW occupancy*, defined as the percentage of time the GW is busy processing packets, and the *packet forwarding rate*, defined as the number of packets per minute the GW can process. We compute both metrics for packets coming from EDs and jammers.

From Fig. 5 (a), we can see that the time expend by the GW

to process packets coming from EDs decreases as the number of jammers increases. If we consider the case where there is only one jammer, the difference of time can be of the order of 10^2. In fact, as defined by the standard, GWs act as simple relays that do not perform any data-frame filtering in order to discard external packets.

From Fig. 5 (b), we note that by increasing the number of jammers, the number of EDs' packets processed by the gateway decreases. In fact, for a baseline cell with no jammer and 100 EDs, the gateway is able to process $1.9\ packets/min$, while for the case where there are 40 channel-oblivious jammers with $DC = 1$, this number fall to only 0.13 and $0.21\ packets/min$ respectively. This holds true for scenarios with 200 and 300 EDs.

As regards the jammer's transmission power, it can be seen that for the case where 8 jammers are present in the network, the GW is able to process $3.6\ packets/min$ when $P_{TXj} = 20\ dBm$, while for the case where $P_{TXj} = 14\ dBm$ this number grows to 4.73.

Scenario c) Fig. 6 depicts a linear interpolation of the throughput (in $packets/h$) achieved by each EDs in a LoRaWAN cell from a geographical point of view. We present this metric for the case with no jammer and for the cases in which the cell is under attack.

Fig.6 (a), shows the baseline cell with no jammer. As expected, EDs close to the GW achieve the highest throughput. Inversely, EDs deployed in the periphery presents lower performance. This is due to the fact that EDs are deployed so that the best possible SF is selected based on the reception sensitivity of the GW.

As for the channel-oblivious, depicted in Fig.6 (b) the network performance decreases widely. The throughput achieved by all EDs is decreased by 16.6% when adding 10 jammers with a $DC = 0.5$.

Finally, for the channel-aware, the performance impact is highly correlated with the jammers' geographical position. Indeed, EDs close enough to jammers experienced a throughput reduction of 99.8%, which is consistent with experimental implementations as presented in [13].

VI. Conclusion and future work

In this paper, we have proposed an open source [16] extension of the ns-3 module for LoRaWAN presented in [8] that allows to model both, channel-aware and channel-oblivious jammers in LoRaWAN networks. We have evaluated the network performance impact of each type of jammer by computing both ED and GW side metrics. In the former we considered four metrics: packet loss probability, collision probability, dropping probability and normalized network throughput while in the latter we have considered two: GW occupancy and GW forwarding rate. The results have shown that LoRaWAN networks are particularly vulnerable to these types of attacks. Indeed, we have shown that for the simulation scenarios chosen, the average throughput reached by ED can be decreased by $\sim 56\%$ in the worst cases when the network is put under attack by 25 channel-aware jammers with $DC = 0.5$.

The impact of the jammers' transmission power on the effectiveness of the attack is also studied. We model the interference as the result of two phenomena: the co-channel rejection matrix and the capture-effect. We have shown that the probability of a packet loss caused by a collision is bigger when jammers transmit at least 6dB higher than regular ED.

We have shown that GWs acting as pure relays is an important vulnerability in LoRaWAN. Our results suggest that, in the case where the network is under the attack by only one channel-oblivious jammer, the gateway spends 100 times more time processing packets coming from jammers than that of legetimate EDs.

Finally, we evaluated the network performance impact from a spatial perspective. We showed that the impact attack area is highly correlated with the jammer-type. The results showed that channel-oblivious jammers impact the network widely, while reactive jammers impact the network locally.

As for the future work, we will focus on the conception and implementation of counter-measures against jamming. For that, we will explore solutions at the gateway level such as authenticated preambles and also the implementation of intrusion detection systems (IDS), using approaches such as statistical analysis and machine-learning.

References

[1] D. Evans, "The Internet of Things How the Next Evolution of the Internet Is Changing Everything," 2011.

[2] L. Alliance, "LoRa Specification 1.0.1," Tech. Rep., 2015.

[3] ——, "LoRaWAN 1.1 and Backend Interfaces 1.0," Tech. Rep., 2017.

[4] SEMTECH, "SX1272 LoRa Designer's Guide," Tech. Rep., 2013.

[5] L. Casals, B. Mir, R. Vidal, and C. Gomez, "Modeling the energy performance of LoRaWAN," *Sensors*, vol. 17, no. 10, p. 2364, oct 2017.

[6] J. Haxhibeqiri, F. Van den Abeele, I. Moerman, and J. Hoebeke, "Lora scalability: A simulation model based on interference measurements," *Sensors*, vol. 17, no. 6, 2017.

[7] M. C. Bor, U. Roedig, T. Voigt, and J. M. Alonso, "Do LoRa low-power wide-area networks scale?" in *19th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems - MSWiM '16*. ACM Press, 2016.

[8] D. Magrin, M. Centenaro, and L. Vangelista, "Performance evaluation of LoRa networks in a smart city scenario," in *2017 IEEE International Conference on Communications (ICC)*. IEEE, may 2017.

[9] M. Capuzzo, D. Magrin, and A. Zanella, "Confirmed traffic in LoRaWAN: Pitfalls and countermeasures," in *2018 17th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net)*. IEEE, jun 2018.

[10] I. Butun, N. Pereira, and M. Gidlund, "Security risk analysis of LoRaWAN and future directions," *Future Internet*, vol. 11, no. 1, dec 2018.

[11] S. Tomasin, S. Zulian, and L. Vangelista, "Security analysis of LoRaWAN join procedure for internet of things networks," in *Wireless Communications and Networking Conference*. IEEE, mar 2017.

[12] X. Yang, E. Karampatzakis, C. Doerr, and F. Kuipers, "Security vulnerabilities in LoRaWAN," in *Third International Conference on Internet-of-Things Design and Implementation (IoTDI)*. IEEE, apr 2018.

[13] E. Aras, N. Small, G. S. Ramachandran, S. Delbruel, W. Joosen, and D. Hughes, "Selective jamming of LoRaWAN using commodity hardware," in *14th EAI International Conference on Mobile and Ubiquitous Systems Computing Networking and Services*. ACM Press, 2017.

[14] C. Goursaud and J. M. Gorce, "Dedicated networks for IoT: PHY / MAC state of the art and challenges," *EAI Endorsed Transactions on Internet of Things*, vol. 1, no. 1, p. 150597, oct 2015.

[15] A. Rahmadhani and F. Kuipers, "When LoRaWAN frames collide," in *12th International Workshop on Wireless Network Testbeds, Experimental Evaluation & Characterization - WiNTECH '18*. ACM Press, 2018.

[16] (2019) ns-3 lorawan-jamming, v0.1. [Online]. Available: https://sourcesup.renater.fr/lorawan-jamming/

[17] SEMTECH, "SX1301 Datasheet," Tech. Rep., 2017.