On the Performance Evaluation of LoRaWAN with Re-transmissions under Jamming

Ivan Martinez*, Fabienne Nouvel*, Samer Lahoud†, Philippe Tanguy‡, Melhem El Helou†
*IETR, UMR 6164 CNRS — Institut National des Sciences Appliquées de Rennes, Rennes, France.
†CIMTI, ESIB — Université Saint-Joseph de Beyrouth, Mar Roukoz, Lebanon.
‡Lab-STICC, UMR 6285 CNRS — Université Bretagne Sud, Lorient, France.

{ivamarti,nouvel}@insa-rennes.fr*, {samer.lahoud,melhem.helou}@usj.edu.lb†, philippe.tanguy@univ-ubs.fr‡

***Abstract*—This paper explores the possibility of having confirmed traffic in LoRaWAN networks under channel-oblivious jamming. Our results show that a LoRaWAN cell can handle up to 500 end-devices with a relatively good message success probability (~ 0.8) if the network is strongly jammed (60% of the time) by using a maximum of 16 re-transmissions. We have also proved that, using a channel for downlink transmissions operating in the lowest SF is a major weakness in the LoRaWAN specification. Indeed, our results suggest that for a LoRaWAN cell with 600 end-devices the network goodput can be decreased by $\sim 53.06\%$ when ACK transmissions on the second receive window are allowed. This was done by using an open-source network simulator that allows to evaluate many scenarios that can help LoRaWAN operators to better scale their networks in order to be more resilient against jamming attacks before actual deployments.**

***Index Terms*—LoRaWAN, IoT, Jamming, NS3, LPWAN networks, ACK.**

I. Introduction

IoT technologies are key enablers of a huge number of application domains in our current society. Indeed, if we look at the most recent predictions of the number of objects connected to internet it can be seen that according to Cisco's expectations 500 billions of devices will be connected by 2030 [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 [2]. These outstanding figures have been reached largely thanks to the different wireless technologies present in the market.

Currently there are several wireless technologies that can be used for any IoT use-case. Low Power Wide Area Networks (LPWAN), such as LoRaWAN, SigFox, and NB-IoT are new wireless protocols. They 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) in terms of memory and processing capabilities. Consequently, the security is a challenge for this type of network.

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. Hence, if implemented well, LPWAN networks can reasonably be secured against attacks at upper levels such as replay attacks or DoS. Nevertheless, this does not shield them against attacks at a lower level such as jammer-type attacks.

A jamming attack takes place at the PHY layer. It could be an external node that broadcasts random unauthenticated packets in the network with the aim of disrupting communications by decreasing the signal-to-noise-plus-interference ratio (SNIR) or by generating collisions. Jamming attacks can be classified into two, namely, Channel-aware and Channel-oblivious. The former being aware of the channel activity in order to trigger the attack and the latter sending unauthenticated packets randomly.

A performance evaluation of the LoRaWAN protocol under these two jamming attacks using a ns3-simulation approach was already presented by the authors in [3][1]. This paper is an extension in which we explore confirmed traffic to improve the network resilience. For that, we first present an Aloha-type LoRaWAN simulation model with authenticated traffic, then we evaluate the network performance in the presence of channel-oblivious jammers. Finally we evaluate the cost of having a re-transmission mechanism[2].

The remainder of this paper is structured as follows: Section II gives an overview of the LoRaWAN protocol. In section III, we present previous works done on Jamming countermeasures for LoRaWAN. Section IV presents our LoRaWAN network model. Section V gives a description of the threat model. In section VII, we present the simulation scenarios and corresponding results. Finally, section VIII provides a conclusion and future directions of our work.

II. LoRaWAN Overview

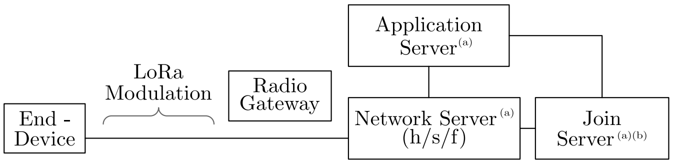
LoRaWAN networks are defined in the LoRaWAN specification (v1.0 and v1.1) [4]–[6]. It is designed for allowing

[1] ns-3 lorawan simulator for LoRaWAN under jamming available at https://sourcesup.renater.fr/lorawan-jamming/

[2] This work has been partially funded by the Conseil Régional de Bretagne and the Université Bretagne Loire.

978-1-7281-8086-1/20/$31.00 ©2020 IEEE

wireless connectivity for battery-based end-devices that can be mobile or fixed. It operates in the Sub 1 GHz band and is typically deployed in a star-of-stars topology. The modulation scheme (LoRa) used is a proprietary spread spectrum modulation, which is a variant of Chirp Spread Spectrum modulation (CSS). A LoRaWAN network is composed of End-Devices (ED), Concentrators/Gateways (GW), a network Server (NS), an Application Server (AS) and (for LoRaWAN 1.1) a Join Server (JS). A top level diagram is depicted in Fig. 1.



(a) Depending on the deployment these three servers can be merged into one
(b) The Join Server was formally introduced in LoRaWAN Backend interfaces v 1.0
(c) h - home, s - serving, f - forwarding

Fig. 1: Top level LoRaWAN Architecture

All the exchanges made between ED and GWs are spread out on different frequency channels and data rates (ranging from 0.3 to 50 kb/s). The selection of the data rate is a trade-off between communication range and message transmission duration. EDs may transmit on any channel available at any time, using any available data rate. Channel selection is done by following a pseudo-random approach. However, the transmission is restricted to a maximum duty-cycle and time duration is predefined for each sub-band according to local regulations. At the MAC Layer, the protocol used is an Aloha-type protocol.

III. Previous Works

Research on security issues in LPWAN networks focus at different layers. In [7], different LPWAN vulnerabilities are studied, combined with several Proof-of-Concept (PoC) attacks toward LoRaWAN (packet forging), Sigfox (replay with DoS) and NB-IoT (attack using malicious UE). It proves the existence of the vulnerabilities in both the specification and off-the-shelf hardware and services. Regarding security issues in LoRaWAN networks, several works have been done for attacks at the MAC and upper layers [8]–[10]. Regarding jamming attacks in LoRaWAN, in [11] a selective jamming attack on a LoRaWAN network was implemented by using commodity hardware, showing success rates close to 100%. In [12], a jammer has been implanted in a LoRa small board by modifying the open source code (Semtech) and the impacts through three scenarios are studied aiming at evaluating the influence of LoRa transmission configuration on jamming performance. Regarding these studies and to the best of our knowledge, most of the previous works focus on experiment but not on event-based simulation associated with a re-transmissions scheme for LoRaWAN. A network simulator as the one presented in this work allows to evaluate many scenarios that can help operators to better scale their networks in order to be more resilient against attacks before actual deployments.

IV. Network model

In the following we present the network model used to simulate LoRaWAN with re-transmissions. We first present the wireless channel model used, then the channel access, and finally the re-transmissions scheme considered.

A. Wireless Channel

In regards to the shared wireless channel connecting EDs and GWs, at the physical level the LoRa Modulation is used. Under this modulation, the transmitter generates chirp signals by varying their frequency over the time, which enhances the signal robustness. Hence, it employs orthogonal Spreading Factors (SF) (7 to 12) that provide a trade-off between data rate and coverage range [3,13]. EDs are configured to use the best SF possible, so that the received power at the GW is above the GW sensitivity according to Table I. Hence, SF are configured prior data exchanges and it remains immutable during the session.

TABLE I: LoRaWAN devices Sensitivities for 125 Khz

Device	SF7 [dBm]	SF8 [dBm]	SF9 [dBm]	SF10 [dBm]	SF11 [dBm]	SF12 [dBm]	Ref.
GW	-130.0	-132.5	-135.0	-137.5	-140.0	-142.5	[14]
ED	-124	-127	-130	-133	-135	-137	[13]

Transmission parameters of EDs and GW are modeled as the SEMTECH SX1272 and the SX1301 respectively. Hence, for uplink and first ACK transmissions, the network operates in the 868 MHz band. We consider three channels: 868.1, 868.3 and 868.5 MHz. As for second ACK transmissions, we consider that the network operates in the 869.525 MHz band. For the propagation model, we consider a radio propagation model based on the well-known log-distance path loss model, which is presented in [15] and can be described as:

$$L = L_0 + 10 \cdot n \cdot \frac{d}{d_0} \tag{1}$$

where: n is the path loss distance exponent, d_0 is reference distance [m], L_0 is the path loss at reference distance [dB], d is distance [m] and L is the path loss [dB].

We also considered the *capture effect*. A packet collision occurs when two or more radio signals are overlapped in time at the receiver. In an Pure Aloha system, this collision results in all packets being destroyed. However, in case of capture effect a collision might not result in packet loss. The capture effect occurs when the receiver stays synchronised to the strongest signal even though a collision has occurred. Thus, we consider that a particular signal X can be successfully decoded if:

$$SINR_x = \frac{P_x}{\sum P_I + \sigma^2} > T_h \tag{2}$$

where $SINR_x$ is the signal-to-interference-plus-noise ratio of the signal X, P_x is the power of the signal X, $\sum P_I$ is the aggregated interference power from other active users in the network, σ^2 is the white channel power, T_h is the minimum SINR threshold required to successfully decode the signal X. The selection of Th is based on real measurements from previous investigations as presented in [16,17].

B. LoRaWAN Channel Access

As presented in Fig. 2, the LoRaWAN transmission process is divided into two phases, referred to as *uplink* and *downlink*, respectively. To transmit a packet, the ED select one of the main uplink channels. Once the packet is received, the NS replies with two ACKs. The first one is sent on the same channel used for the uplink transmission. The second ACK is sent a dedicated downlink channel after a given timeout. The first ACK is sent using the same SF, while the second ACK is sent at a pre-defined SF, which is by default the lowest one.

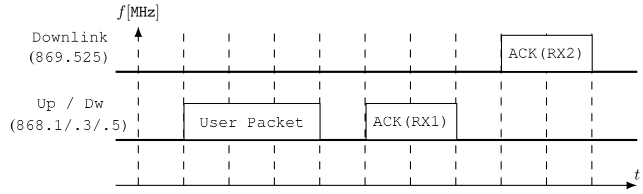


Fig. 2: LoRaWAN Transmission Schedule

In this paper we consider the case where one GW serves a large number of LoRaWAN compliant EDs. Hence, we consider that uplink transmissions attempts are done according to a Poisson point process with parameter (λ_u) which is defined as the user packet generation rate. We also assume that all user packets have the same length l_u. The packet transmission time T_u depends on the SF as defined in [3,18]. Then, given a duty-cycle limitation d_u the packet generation rate for each ED verifies $\lambda_u \cdot T_u \leq d_u$.

C. Re-transmissions scheme

We consider the re-transmission scheme depicted in Fig. 3. This scheme aims at mitigating information lost due to packet collisions. The scheme works as follows: the ED sends a message (a packet identified with a unique ID), then if the message reaches the gateway, it sends back an ACK with length l_a and transmission time T_a. If the ACK does not reach the ED before a time-out T_o, it makes a re-transmission[3]. The timeout countdown is reset after each packet transmission. It is set as the time required by the GW to detect a user packet plus the time required by the ED to detect an ACK preamble. The user packet is re-transmitted a maximum r times. Under this scheme, three cases may arise:

- the user and ACK packets are well received,
- a user packet is lost due to collisions with another user/jamming packet. Then, the packet is resent,
- a user packet is well received but ACK is lost due to jamming collision. Hence, it is re-transmitted.

It should be noted that a message can lead to multiple packets depending on network congestion. Additionally, since we only considered one GW, there is no possibility of collisions between ACK packets.

V. Threat model

For our threat model, we consider a network architecture as the one presented in Fig. 4. As we can see, the network is composed of: multiple EDs, which are considered to be legitimate nodes since they meet the LoRaWAN specification and band restrictions, a legitimate Gateway that handles the radio channel with end-devices, a network server that is in charge of handling the joint procedure and an Application Server.

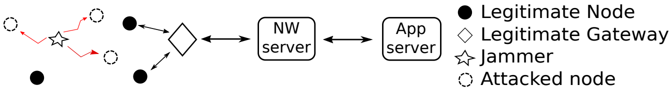


Fig. 4: Threat Model

We assume that the attack takes place at the access network. We consider that jammers do not a belong to the network, and that from the hardware point of view they have the same characteristics as regular EDs. Jammers do not listen to the channel, and they transmit randomly on the same bands, channels and SFs as legitimate nodes.

Similarly to EDs, we assume that the jammer's arrival packet times, follows a Poisson distribution with a given parameter λ_j, all packets sent by jammers have the same packet length l_j, and that contrary to legitimate nodes, they are allowed to select an arbitrary duty-cycle d_j.

Jammers can either transmit on the 868 MHz band or on the 869.25 band, and in both cases the transmission power is set to 14 dBm. Jammers are characterised by the normalised jammig traffic load (G_j), which is defined as the aggregate traffic injected by all jammers as a proportion of the maximum band capacity. That is to say that for a $G_j = 1$, all SF and channels of the band are occupied by at least one jammer.

VI. Simulation Scenarios

In this section we present the simulation scenarios used. We first introduce the performance metric considered, then a network baseline, and then three different simulation scenarios that allows to assess the performance impact of jamming on LoRaWAN with re-transmissions.

A. Performance metrics

We considered three performance metrics: (i) the Network Goodput (NG), defined as the average number of messages per second $[msg/s]$ well received by the GW, (ii) the Message Success Probability (MSP), defined as the probability of having a message well received after, at most, r re-transmissions, and (iii) the average number of re-transmissions per message.

[3] Transmission times of message re-transmissions are set according to the same Poisson point process as messages. Hence, the parameter (λ_u) and duty-cycle (d_u) restriction are respected and no exponential back-off mechanism is implemented.

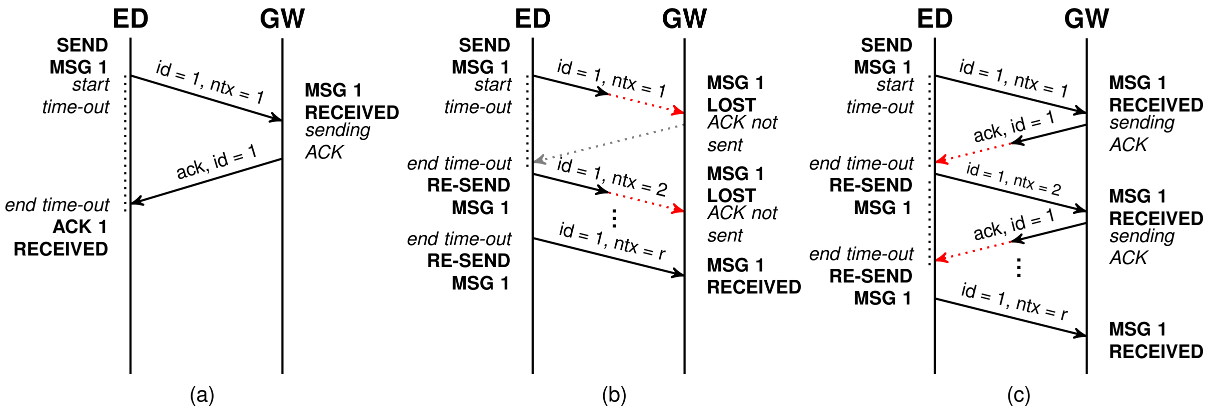


Fig. 3: Acknowledgment Scheme: (a) data and ACK packets are well received, (b) data packet is lost, (c) data packet is well received but ACK is lost.

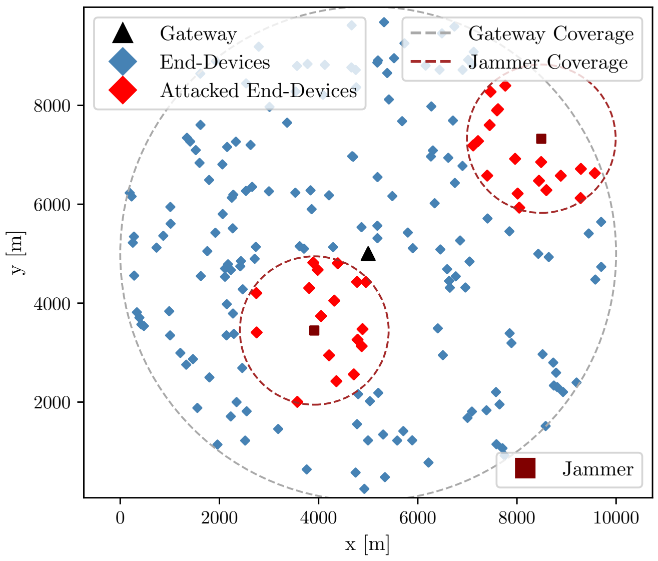


Fig. 5: Simulation Scenario

B. LoRaWAN network baseline

We consider a LoRaWAN cell consisting of several EDs and one GW under jamming as presented in Fig. 5. EDs are uniformly distributed around the GW within a radius of 5 km. EDs are static and configured to use the best SF possible as a function of their position and the GW's sensitivity. Hence, according to the Path-loss model considered and the uniform distribution of nodes, SF are distributed as follows: $\{SF_7 = 0.33,\ SF_8 = 0.22,\ SF_9 = 0.1,\ SF_{10} = 0.09,\ SF_{11} = 0.19,\ SF_{12} = 0.07\}$.

As regards the ED's application profile, we considered a packet length l_u of 50 bytes, and that all EDs, are configured to use a duty-cycle d_u of 0.01. Thus, depending on the SF, T_u varies from 82.17 ms to 1.81 s.

For uplink and first ACK transmissions, the cell operates in the 868 MHz band, three sub-bands are considered: 868.1, 868.3 and 868.5 MHz, each one with a bandwidth of 125 kHz, all EDs belong to Class A with confirmed traffic. For the second ACK, a separate channel operating in the 869.525 MHz band is used, an SF of 12 is considered. The ACK packet length (l_a) is set to 25 bytes, and the ACK transmission time T_a varies from $46, 33$ ms to 1.15 s as a function of the SF.

TABLE II: Simulation Parameters

	Parameter	Scenario (a)	Scenarios (b), and (c)
Network	N_u	$1, 100, \dots, 2000$	$100, 500$
	l_u	50 bytes	50 bytes
	l_a	25 bytes	25 bytes
	d_u	0.01	0.01
	SF	7 - 12	7 - 12
	T_u	82.17 ms - 1.81 s	82.17 ms - 1.81 s
	T_a	$46, 33$ ms - 1.15 s	$46, 33$ ms - 1.15 s
	r	0 - 64	0 - 64
	radius	5 km	5 km
Jammers	l_j	-	50 bytes
	T_j	-	82.17 ms - 1.81 s
	G_j	-	$0.1 - 1$
	N_j	-	25
Path-loss	d_0	40 m	40 m
	n	2.08	2.08
	L_0	107.41 dB	107.41 dB
	Th	6 dB	6 dB
	σ^2	-123 dBm	-123 dBm
Band	Up / Dw	868.1/.3/.5 MHz	868.1/.3/.5 MHz
	Downlink	869.525 MHz	869.525 MHz
Simulation time		10 h	10 h

C. Simulation Scenarios

We define three scenarios considering the LoRaWAN cell described before with parameters reported in Table II.

Scenario (a): In this scenario we evaluated the performance of the LoRaWAN baseline network. We simulated a cell with N_u varying from 1 to 2000 and r varying from 0 to 64.

Scenario (b): In this scenario, we simulated a LoRaWAN cell under the attack of jammers transmitting either on the

868 MHz band only or on the 869.525 MHz. The number of EDs is set to 100. The network is under the attack of 25 jammers whose aggregate traffic load (G_j) varies from 0 to 2. The jammer's packet length l_j is set to 50 bytes with a transmission time T_j varying from 82.17 ms to 1.81 s (as a function of the SF).

Scenario (c): In this scenario, we evaluate performance of a LoRaWAN cell with $N_u = 500$ Simulation parameters are set identically to scenario (b).

VII. Results and discussion

This section presents the results obtained for the different simulation scenarios.

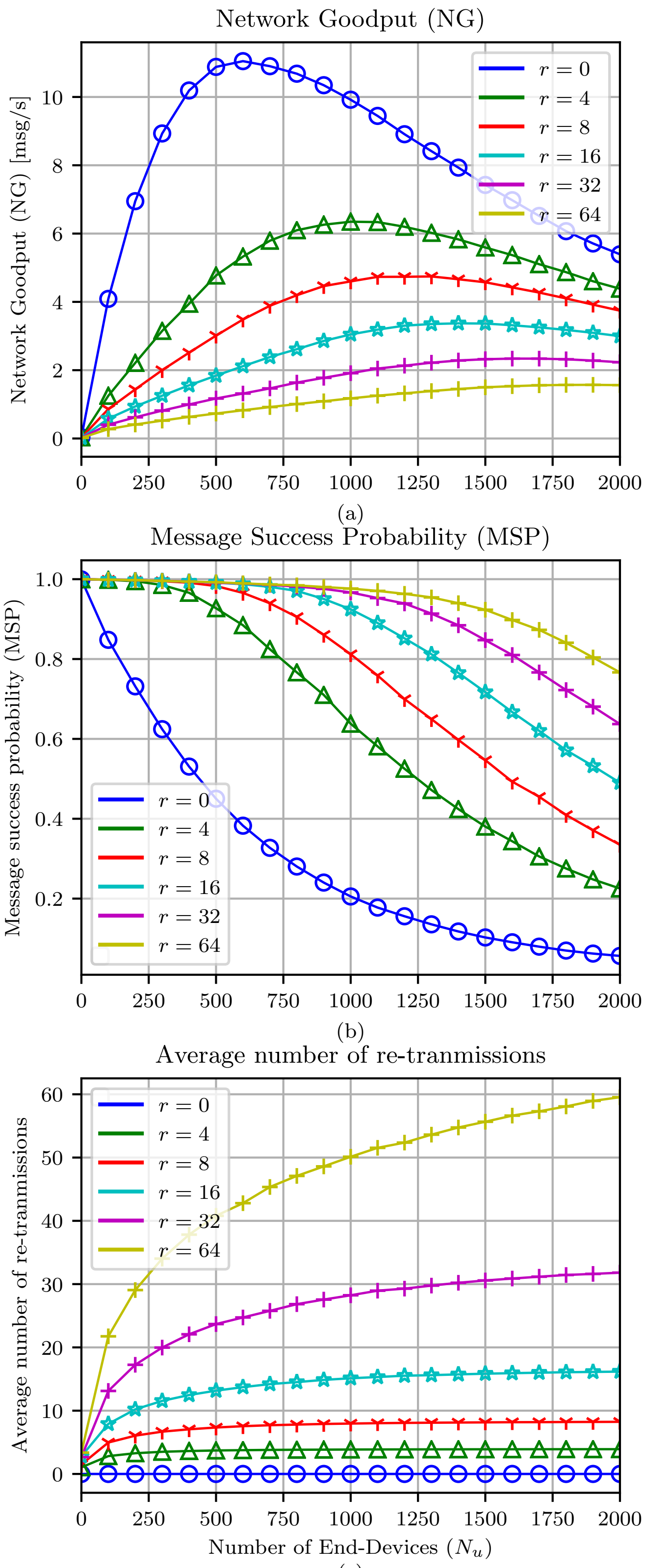
Scenario (a): Fig. 6 presents performance evaluation of a LoRaWAN cell with packet re-transmissions. Different network configurations varying N_u and r were considered. Fig. 6 (a), presents the NG. For $r = 0$, all packets are sent only once, this means that the number of packets and messages is the same[4]. Hence, a classic behavior of an Aloha-type network can be observed, reaching the maximum goodput at [11 msg/s] for $N_u = 600$.

On the contrary, for $r > 0$ we note that, as r increases the goodput obtained decreases. This decrease is caused by two reasons: (i) ACKs sent in the same band and SF as user data packets cause collisions with user packets, and (ii) ACKs sent in the 869.525 MHz band are sent with $SF = 12$. Hence, the GW is locked a considerable amount of time sending a single ACK packet (1.15 s). Consequently, as the number of ED increases, its responsiveness decreases as it becomes saturated. Then, EDs begin to make unnecessary re-transmissions even when the original packet arrived well.

From Fig. 6 (b), we can see that the MSP degrades rapidly by increasing the number of EDs for $r = 0$. For example, the MSP falls to 0.37 when $N_u = 600$. This reduction becomes even more important for networks with $N_u \geq 1500$ where this number falls to only 0.1 or less.

On the other hand, for $r > 0$, it can be seen that the higher r is, the higher the probability of success on the messages will be, thus increasing the network reliability. Indeed, the selection of r should consider the number of EDs an operator is willing to serve. For example, there is no point in selecting $r = 8$ for $N_u \geq 1400$ since the MSP will decay to 0.6 or less.

Fig. 6 (c), present the average number of re-transmissions per message as a function of r and N_u. We can see that this number increases in proportion to the number of EDs served in the network. Hence, there is a compromise between the NG and the average number of re-transmissions. As a result, if an operator is willing to have an adequate NG, it needs to carefully decide the number of re-transmission the application needs to support.



(a)

(b)

(c)

Fig. 6: Network Performance of a LoRaWAN cell considering re-transmissions: (a) Network Goodput, (b) Message Success Probability and (c) Average Number of Re-transmissions.

[4] It should be noted that, as packet transmissions and re-transmissions are the result of the same Poisson point process with parameter (λ_u) and duty-cycle restriction (d_u), the user traffic load is the same regardless r. For this simulation scenario and SF distribution, the average traffic load per user is 2.83 [packets/min].

Scenario (b): Fig. 7 presents the performance evaluation of a LoRaWAN cell with $N_u = 100$ under jamming as a function of the jammer's traffic load (G_j). Clearly, when jammers transmit on the 868 MHz Band, the greater G_j is, the lower the goodput is, and the higher the average number of re-transmissions is. Indeed, for all cases, the NG droops to nearly zero when $G_j = 2.0$. However, the network can alleviate the problem of jammers when they jam moderately by allowing re-transmissions. For instance, for a G_j of 0.2, the MSP goes from 0.44 for $r = 0$ to 0.91 for $r = 4$. This figure can be even better for $r = 32$, where a MSP close to 1 is achieved.

On the contrary, for jammers transmitting on the 868.525 MHz band, the impact on the NG is much less important. Indeed, for $r = 4$ the NG downs from 1.19 to 1.01 [msg/s] in the worst case. As for the MSP, we can see that it stay constant regardless the value of G_j. Besides, the average number of re-transmissions increases although the performance of the network does not improve.

Scenario (c): In contrast with scenario (b), from Fig. 8 we note that for $N_u = 500$ the impact that jammers transmitting on the 868 MHz band have on the MSP is much more important. This is due to the fact that the channel quality even without jammers is already very degraded. Indeed, the MSP reached without re-transmissions is only 0.44. Consequently, to obtain an MSP close to 1, a higher r is necessary. For example to deal with a G_j of 0.2, an r of 8 is needed in order to get a MSP of 0.98. As for the average number of re-transmissions, a behaviour similar to that with $N_u = 100$ is obtained. It increases as G_j increases.

As for jammers transmitting on the downlink band, a similar behaviour as in scenario (b) is obtained. Hence, the impact on the NG is much less important and the MSP stays constant regardless the G_j.

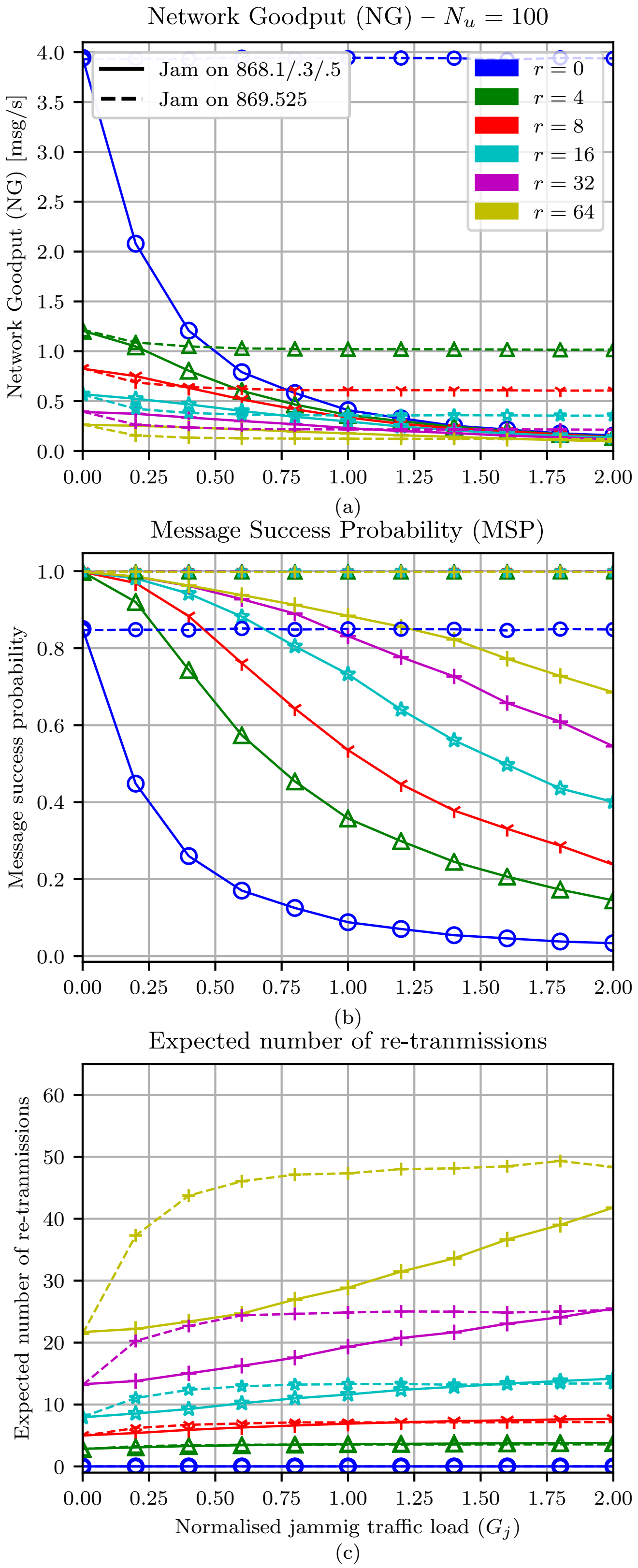
VIII. Conclusion and Future Work

The investigations in this paper have led to an evaluation of a simple and low-cost re-transmission mechanism that allows to improve the reliability of a LoRaWAN network under the attack of Channel-Oblivious Jammers.

We have shown the interest of implementing this type of mechanism even when the network is not being attacked. Our results suggest that a LoRaWAN cell, can handle up to 1000 end-devices with a good MSP (~ 0.8) and a relatively good user goodput ($\sim$ 16 msg/h) by allowing the transmission of a given message a maximum of 8 times.

We have also shown, that if the network is put under attack of several jammers on the uplink channel, the network can still manage to have an acceptable message success probability. Indeed, our results demonstrate that a LoRaWAN cell can handle up to 500 nodes when being jammed 60% of the time and still obtain a good MSP (~ 0.8) if the maximum number of re-transmissions is set to 16.

We have also proved that, using a dedicated channel for downlink transmissions operating in the lowest SF is a major weakness in the LoRaWAN specification. Indeed, we have



(a)

(b)

(c)

Fig. 7: Network Performance of a LoRaWAN cell under jamming with $N_u = 100$: (a) Network Goodput, (b) Message Success Probability and (c) Average Number of Retransmissions.

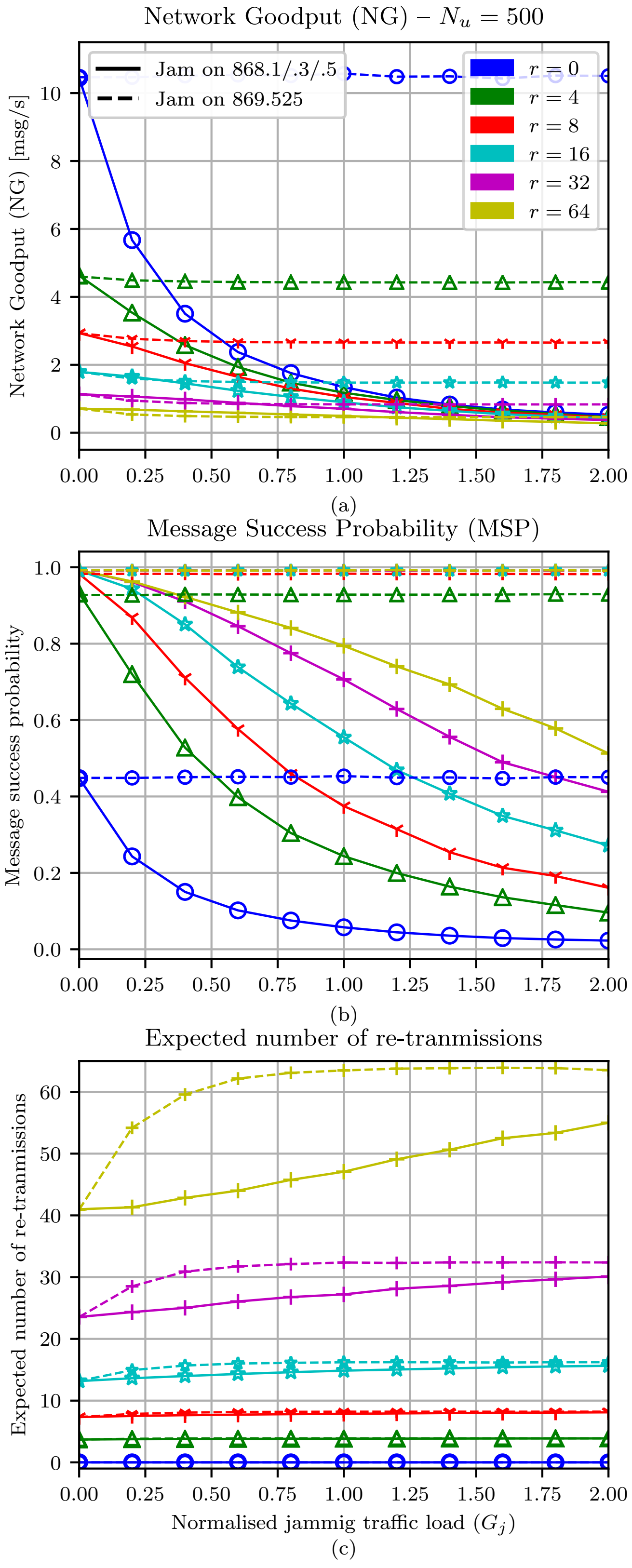


Fig. 8: Network Performance of a LoRaWAN cell under jamming with $N_u = 500$: (a) Network Goodput, (b) Message Success Probability and (c) Average Number of Re-transmissions.

proven that the NG can be decreased by $\sim 53.06\%$ (considering 600 ED) when re-transmissions are allowed. This is due to the fact that, as the GW expends a lot of time transmitting ACKs, it gets rapidly saturated as the number of EDs increases. A further analysis should be done in order to evaluate the possibility of acknowledging only a portion of the traffic instead of doing it for the totality of the traffic.

Finally, we have shown that there is a compromise between the NG achieved and the average number of re-transmissions per message. A further analysis should be done on how this can affect the power consumption of the EDs, and consequently the battery replacement rate.

References

[1] Cisco, "Internet of Things - Connected Means Informed," 2016.

[2] M. . Company. (2017) Security in the internet of things.

[3] I. Martinez, P. Tanguy, and F. Nouvel, "On the performance evaluation of LoRaWAN under jamming," in *2019 12th IFIP Wireless and Mobile Networking Conference (WMNC)*. IEEE, Sep. 2019. [Online]. Available: https://doi.org/10.23919/wmnc.2019.8881830

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

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

[6] ——, "LoRaWAN Backend Interfaces 1.0 Specification," Tech. Rep., 2017.

[7] F. L. Coman, K. M. Malarski, M. N. Petersen, and S. Ruepp, "Security issues in internet of things: Vulnerability analysis of lorawan, sigfox and nb-iot," in *2019 Global IoT Summit (GIoTS)*, June 2019, pp. 1–6.

[8] I. Butun, N. Pereira, and M. Gidlund, "Security risk analysis of LoRaWAN and future directions," *Future Internet*, vol. 11, no. 1, p. 3, Dec. 2018. [Online]. Available: https://doi.org/10.3390/fi11010003

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

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

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

[12] C.-Y. Huang, C.-W. Lin, R.-G. Cheng, S. J. Yang, and S.-T. Sheu, "Experimental evaluation of jamming threat in LoRaWAN," in *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*. IEEE, Apr. 2019. [Online]. Available: https://doi.org/10.1109/vtcspring.2019.8746374

[13] SEMTECH, "SX1272/3/6/7/8 LoRa Modem Designer's Guide," Tech. Rep., 2013.

[14] ——, "SX1301 LoRaWAN Gateway - Datasheet," Tech. Rep., 2017.

[15] D.-T. Ta, K. Khawam, S. Lahoud, C. Adjih, and S. Martin, "LoRa-MAB: A flexible simulator for decentralized learning resource allocation in IoT networks," in *2019 12th IFIP Wireless and Mobile Networking Conference (WMNC)*. IEEE, Sep. 2019. [Online]. Available: https://doi.org/10.23919/wmnc.2019.8881393

[16] M. C. Bor, U. Roedig, T. Voigt, and J. M. Alonso, "Do LoRa low-power wide-area networks scale?" in *Proceedings of the 19th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems - MSWiM '16*. ACM Press, 2016. [Online]. Available: https://doi.org/10.1145/2988287.2989163

[17] 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.

[18] SEMTECH, "An1200.22 - LoRa Modulation Basics," Tech. Rep., 2015.