Experimental Evaluation of Jamming Threat in LoRaWAN

Chin-Ya Huang *, Ching-Wei Lin *, Ray-Guang Cheng *, Shanchieh Jay Yang †, Shiann-Tsong Sheu ‡
* Dept. of Electronic and Computer Engineering, National Taiwan University of Science and Technology, Taiwan
† Dept. of Computer Engineering, Rochester Institute of Technology, USA.
‡ Dept. of Communication Engineering, National Central University, Taiwan
Email: chinya@gapps.ntust.edu.tw, B10002013@gmail.com, crg@mail.ntust.edu.tw, jay.yang@rit.edu, stsheu@ce.ncu.edu.tw

***Abstract*—LoRaWAN is a promising solution of Low-power wide area network (LPWAN) operating in unlicensed spectrum to support long range wireless services for Internet of Things (IoTs). However, with the growth of IoT devices deployed in a fixed geographic area, the immunity to interference on the communication increases significantly. Attackers may utilize such situation to jam packet transmission by emitting RF interference signal at the same time when a LoRa end node is sending data to the LoRa gateway. As a consequence, the transmission of the LoRa end node would fail due to collision which would in turn reduce the network performance. In this paper, we implement a LoRa jammer on commercial LoRa devices by modifying the open source and figure out the proper setting of the jammer through three scenarios aiming to evaluate the influence of LoRa transmission configuration on jamming performance. Specifically, the impact of non-orthogonality of LoRa transmission on jamming effect is investigated. Possible countermeasures for LoRaWAN are then presented to alleviate the jamming attacks.**

***Index Terms*—Jamming Threat, LoRaWAN, LPWAN, Channel Active Detection (CAD), Testbed.**

I. Introduction

Internet of Things (IoTs) has drawn attentions in providing new services such as status monitoring, estate tracking, and new modes of interaction by pervasively deploying smart devices. A group of various low-power wide area network technologies called low power wide area network (LPWAN) is proposed to support the long range wireless transmission for IoTs. Specifically, LoRaWAN [1], consisting of end nodes, gateways, network server(s), and applications, is one of the popular LPWAN solutions. However, the limitations on LoRaWAN have been discussed in literature from the viewpoint of security [2–6].

The signal interference caused by non-orthogonality of LoRa transmission would result in transmission failure. LoRa features six orthogonal spreading factors (SFs) [7] to improve channel capacity and spectrum efficiency. The orthogonality allows communications with different SFs on the same channel. The selection of the SF depends on communication range and message duration. The collision behavior of LoRaWAN has been discussed in [4]. Collision happens if the SFs and timing of any two LoRa end nodes are overlapping and the differences of their carrier frequency (CF) and transmission power (TP) are lower than certain thresholds. Furthermore, in [3], the authors find that the concurrent transmissions cannot be successfully decoded by a gateway if both transmissions have an offset of three or more symbol periods. Simulations and empirical experiments from the aspect of LoRa internetwork interference are studied in [8] and [9], respectively. They conclude that the interference degrades the LoRa network performance [8], but the packet could probably be received if the interference signal operates on different data rates and is 6 dB less than the target signal [9].

The immunity to interference and/or attack on the communication is crucial since radio frequency is essentially open medium in LoRaWAN [10]. An attacker may perform jamming attack by continuously sending random unauthenticated packets to the network using a commercially available LoRa device and free software downloaded from the Internet. As a result, the transmitted packets of the authorized LoRa device are jammed and the service to the LoRa device would be denied. In LoRaWAN, the orthogonality could directly affect the jamming performance. Different data rates are claimed to be orthogonal to each other due to the characteristic of SF. The collision would happen when the SFs of two packets transmitted at the same time are overlapping on the channel. According to [11], the orthogonality is not always held under different SFs, and the non-orthogonality occurs when two signals are transmitted with the same chirp rate, which is related to SF and bandwidth (BW).

The characteristic of LoRaWAN in data transmission makes signal easily jammed by attackers during the transmission, and thus the network performance degrades. This paper studies the jamming threat in LoRaWAN, considering the orthogonality and non-orthogonality of LoRa transmission. We implement the reactive jammer in commercial LoRa devices to characterize the jamming threat in LoRaWAN, and our experimental results show that the jammer with specific SF and BW combinations can corrupt packet even with low power. Note that we apply channel active detection (CAD) to realize the reactive jamming, but the open source of LoRa end node does not enable the CAD functionality completely. We modify and complete the implementation by ourselves to realize the jamming procedure. Our characterization offers insight for possible countermeasures for the jamming threat.

The rest of the paper is organized as follows. Section II describes the system model and highlights the jamming threat of LoRaWAN. The ideas realizing the jamming attack on a commercial LoRa transceiver and three experimental

978-1-7281-1217-6/19/$31.00 ©2019 IEEE

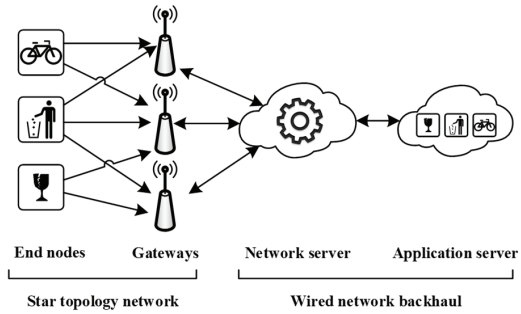


Fig. 1. LoRaWAN system architecture.

results are illustrated in Section III and Section IV. Finally, we propose the possible countermeasures of the described jamming threats in Section V and conclude our finding in Section VI.

II. Jamming Threat in LoRaWAN

A. System Description

LoRaWAN is a specification developed by LoRa Alliance™ aiming to provide seamless interoperability among end nodes. The wireless LoRa technology supports LoRa and frequency shift keying (FSK) modulation and can provide data rates ranging from 0.3 to 50 Kbps. Specifically, end nodes, gateways, network server(s), and application server(s) compose a LoRaWAN as illustrated in Figure 1. The end node transmits packets on designated uplink channel(s) and a number of gateways listen for packet reception. Each gateway forwards the received packets at hand to the designated network server, therefore the network server may have one or more copies of a single packet. The network server then forwards the received packets to the corresponding application server. For each received packet, the network server only forwards it once, and discards the duplicated ones if multiple copies are received. The network server is also responsible for selecting a proper gateway for the successive downlink transmission if it has pending packet(s) to be sent to the end node.

The LoRaWAN specifications define three different types of end nodes. Class A end node is the baseline feature and is designed for IoT applications. The end node uses pure ALOHA protocol to transmit data through the uplink channel. The end node may receive downlink data during two short downlink receive windows after the uplink data transmission. Class B end node is designed to support scheduled downlink transmissions. The end node should synchronize with the gateway by monitoring beacon signals periodically broadcasted by the gateway. Class C end node always stays awake for data reception and transmission.

The LoRa transceiver provides configurable parameters for developers to customize their application requirements. To simplify the parameter design, Semtech provides a LoRa calculator [12] to evaluate timing, RF and power consumption performance quickly. Three sets of LoRa parameter settings named RF setting, LoRa modem setting and packet setting are included in the calculator. The RF setting includes settings of the CF and TP of the transceiver. LoRaWAN specifies

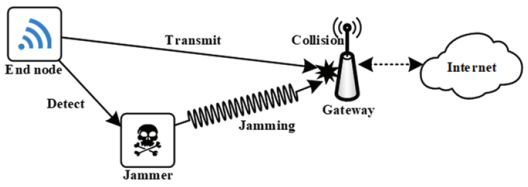


Fig. 2. LoRaWAN system under jamming attack.

the CF in the industrial, scientific, and medical (ISM) radio bands depending on regional regularity. In each band, up to sixty-four channels can be accessed. The LoRa modem setting includes the settings of parameters of SF, BW and coding rate (CR). They are used to determine the equivalent bitrate and time period on the air. The data rate of LoRaWAN can be derived from parameters of SF and BW. The coding rate is the parameter for forward error correction. A lower coding rate provides better protection of packets.

Additionally, LoRa transceiver supports three BWs, 125, 250, and 500 kHz. Depending on the usage of SF, data rate ranges from 0.3 to 27 Kbps for 125 kHz BW. To maximize both battery life of end nodes and overall network capacity, the network infrastructure manages the data rate and RF output power for each end node individually by means of an adaptive data rate (ADR) scheme. Then, the end node can transmit data on available channel at any time instance by using suitable data rate under the restrictions of applying pseudo-random channel hopping for each transmission and complying with the maximal duty-cycle.

B. Jamming Threat

According to the existing studies in [3–6], packet loss can still occur even LoRa transmission does not have high level of interference immunity as expected because of unavoidable collisions. Although jamming threat in LoRaWAN could be relieved by applying the restriction on duty cycle, it is still a challenge because attackers disregard the constraint. Moreover, features of LoRaWAN operating on unlicensed ISM band and employing pure ALOHA access scheme make the jamming attack more easily to be achieved.

Considering a LoRaWAN system suffered from jamming attack as shown in Figure 2, the system consists of a Class A end node, a gateway, and a reactive jammer. The end node and the gateway are standard LoRaWAN products. The end node transmits fixed-length packets to the gateway with fixed data rate. The transceiver of the gateway is capable of receiving all the data rates on the channel. It performs reception procedure as soon as it detects the preamble prior to the data packet. The reactive jammer is deployed between the end node and the gateway. The reactive jammer implements the function of a detector and a jammer operating under the same SF and BW on the fixed-channel.

Furthermore, the LoRa transceiver provides six orthogonal SFs, which can accommodate the channel capacity over various channel conditions. The orthogonality allows communications with different SFs on the same channel simultaneously. The selection of the SF depends on communication range and message duration. In LoRaWAN, the orthogonality could

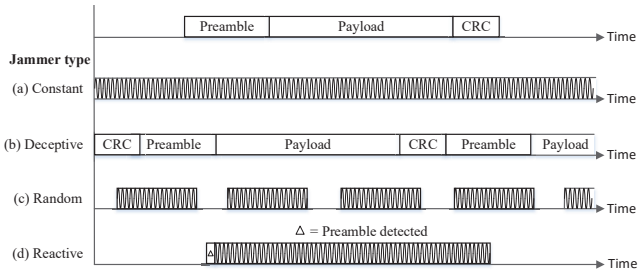


Fig. 3. Four jamming methods.

directly affect the jamming performance. Different data rates are claimed to be orthogonal to each other due to the characteristic of SF. Theoretically, when the packets with SF are overlapping on the channel, collision occurs. Specifically, the non-orthogonality happens when the chirp rates of two signals are the same [11]. In the presence of non-orthogonal pairs, the signals will interfere each other on the air. Therefore, the LoRa transmissions are destructible.

III. Design and Implementation of Jamming Attack

In this paper, a customized board is applied as the end node and reactive jammer. The board is comprised by STM32L152 series microcontroller and SX1272 transceiver provided by Semtech [13, 14]. The gateway is built up by Raspberry Pi 2 connected with iC880A-SPI provided by IMST. The experiment is considered as a line of sight system. We monitor the activities of the customized board and modify the parameters through the UART interface. Furthermore, we control Raspberry Pi 2 to lunch the gateway program through a router by Secure Shell (SSH). All the source codes of each end node refer to the open source code project for LoRaWAN development released by Semtech. However, the CAD functionality is not completely enabled. Under this condition, we modify the reference code by ourselves to realize the jamming flowchart on the LoRa end node.

A. Classification of Jamming

The concepts of jamming wireless communication are discussed in [7, 15, 16]. Four jamming methods can be deployed to affect the target network in different levels, constant, deceptive, random and reactive jammer as illustrated in Figure 3. The constant and deceptive jammer are categorized as the proactive jammer. The proactive jammer emits interference signal on the frequency channel without considering the channel status. The only difference between constant and deceptive jammer is the jamming contents. The constant jammer uses irregular signals but deceptive jammer uses legitimate packets. By pretending a legitimate end node, the deceptive jammer makes the network consider the crowded situation without concerning under jamming attack. Furthermore, the random jammer includes the idea of energy conservation. The jamming and sleep duration are selectable for the attacker. This enables the attacker to decide the tradeoff between the levels of jamming effect and power saving. Last, the reactive jammer only jams the frequency channel upon detecting channel activities which enhances power saving and the stealthiness comparing to other methods.

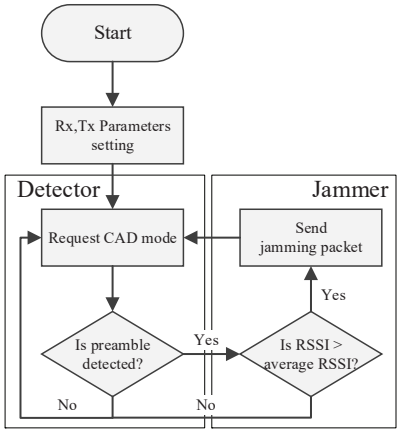


Fig. 4. Flowchart of reactive jamming.

B. Jamming Realization

The possible design of a reactive jamming uses the channel active detection (CAD) mode provided by the LoRa RF transceiver SX1271. Since LoRa provides transmission below the noise floor, the classic clear channel assessment (CCA) may not be efficient for LoRa communication. Hence, LoRa provides CAD for preamble detection. CAD firstly detects preamble, and then requests reception procedure upon detecting the preamble [13]. Although the miss detection would occur in low probability, the problem can be fixed by regarding with the received signal strength indicator (RSSI) during the CAD [14]. The attacker in this experiment will utilize CAD to trigger the jamming procedure aiming to interfere the data transmission in LoRaWAN.

To create reactive jamming, two components, detector and jammer are characterized for the reactive jammer. Figure 4 shows the flowchart of reactive jamming. Note that the open source of LoRa end node does not enable the CAD functionality completely, and then, we modify and complete the reference code by ourselves to realize the jamming flowchart. The initiative starts with the configuration of transceiver parameters including CF, SF, BW, TP and packet length. Next, the reactive jammer enters the detector part by operating CAD mode and continuously sensing preamble on the channel. Upon detecting preamble, the reactive jammer enters the jammer part and firstly fetches RSSI to prevent miss detection. The result is further applied to determine whether to attack the packet or not. After jamming, the reactive jammer returns back to the detector part and start next reactive jamming loop. Note that the reactive jammer keeps returning to CAD mode until preamble is detected, because the jammer does not know the timing of packet arrival.

Moreover, we rearrange the LoRa parameters as required on the reactive jammer. CF is fixed on single channel due to the transceiver limitation. TP is set as the maximum transmission power, 20 dBm. CR is set as the lowest protection level, $4/5$, because the jamming signal does not need protection. The packet length is set as 20 bytes according to the average sensor data length in LoRaWAN.

TABLE I
COMBINATIONS OF LORA CHARACTERIZED BY SF AND BW IN KHZ, THE MARK 'X' REPRESENTS NON-ORTHOGONAL COMBINATION [17]

SF		7	8	9	10	11	12
	BW	125					
7	125	x					
8			x				
9				x			
10					x		
11						x	
12							x
7	250						
8							
9		x					
10			x				
11				x			
12					x		
7	500						
8							
9							
10							
11		x					
12			x				

IV. EXPERIMENTAL RESULTS

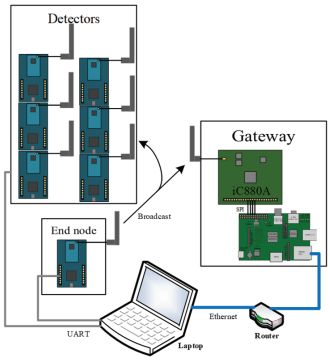
Three experiments are designed to evaluate the performance of reactive jamming attack on LoRaWAN. In the experiments, we choose the packet delivery rate (PDR), the ratio between correct packets received at the gateway and the total transmitted packets [15], as performance index of the reactive jammer. The reactive jammer is composed of the detector and the jammer. Firstly, we will investigate the susceptibility of the detector and the effectiveness of the jammer. We consider the orthogonality and non-orthogonality of LoRa transmission, and apply CAD to evaluate the fast detection of LoRa preamble. As illustrated in (1), two signals are non-orthogonal if their chirp rates are the same [11]. For each CAD, the transceiver receives signal on a specified frequency channel for one symbol duration and spends additional time analyzing received signal to determine detection result. Based on the formulation of T_{CAD}, the CAD mode can repeat at least six times within the preamble duration. Due to the fact, the detector of the reactive jammer could detect the preamble and perform the jamming on payload transmission in time. We further exploit the impact of non-orthogonality signal on interfering LoRa transmission to achieve jamming attack. Finally, we implement reactive jammer via open source to measure the PDRs under different conditions.

Moreover, two parameters, SF and BW, are set according to the goals of the experiments. LoRa provides six SFs and three BWs for different data rates, and thus there are eighteen combinations in total. Table I lists all of the combinations with respect to LoRaWAN data rates and the 'X' markers represent the non-orthogonal pairs [17].

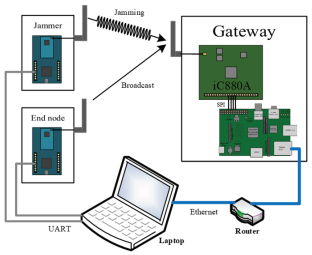
A. Experimental Scenarios

1) Experiment A: Clarification of the CAD performance under different combinations of SFs and BW

The setup of experiment A is shown in Figure 5(a), in which there are six detectors, one end node, and one gateway. For each test, the end node follows the assigned SF to transmit 2000 packets periodically on the fixed channel of 125 kHz BW. Six detectors are used to cover six SFs (from SF7 to SF12), respectively, and they continuously lunch CAD mode to detect the preamble on the fixed channel. The gateway is used to confirm the correctness of packets transmitted from end node in each test. Six test cases are considered in experiment A because packets can be transmitted by the end node with six different SFs. Each test case is executed twice for evaluating the detection capabilities when detectors use the same BW (125 kHz) or different BW (250 kHz) to detect preambles on the 125 kHz channel.



(a) Experiment A setup.



(b) Experiment B setup.

Fig. 5. Experimental setup.

TABLE II
EXPERIMENT B PARAMETERS SETTING

End node 125 kHz BW	Jammer 125 kHz BW	Jammer 250 kHz BW
SF7	SF7	SF7
SF8	SF8	SF8
SF9	SF9	SF9
SF10	SF10	SF10
SF11	SF11	SF11
SF12	SF12	SF12

2) Experiment B: Verification of the jamming effect with respect to BW and TP

Figure 5(b) shows the setup of experiment B, in which there are one end node, one jammer, and one gateway. The end node transmits 1000 packets periodically on a fixed channel with appropriate LoRaWAN data rate setting. For simplicity, on the end node side, CCA is disabled, and thus the end node will not check RSSI before transmission. On the jammer side, we select the constant jammer. According to the non-orthogonal pairs in Table I, the selections of SF with respect to BW are listed in Table II. The gateway lunches the packet logger program to record all received packets in each test. The experiments are tested under different settings of TP. We denote the difference of TP between the end node and jammer as ΔTP, and the ΔTP varies from -6 dB to +6 dB in a step of 3 dB. Further, PDR is applied to evaluate the jamming effect.

3) Experiment C: Evaluation of the jamming effect of the reactive jammer in LoRaWAN

In experiment A and B, we individually investigate the impact of parameters of the detector and the jammer on data transmission performance. Following the flowchart of the reactive jammer, we replace the constant jammer in experiment B with reactive jammer and make required changes for the reactive jammer realization. In this experiment, the BW is set as 125 kHz because the results of experiment B indicate that when bandwidth is 125 kHz, the jamming effect is better comparing to 250 kHz.

B. Experimental Results

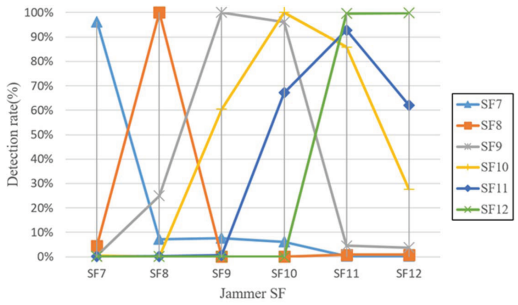
1) Experiment A: Clarification of the CAD performance under different combinations of SFs and BW

In the results of experiment A, we verify the performance of CAD under two BWs, 125 and 250 kHz. Intuitively, the selection of SF in both the jammer and end node under different BWs affects the probability in preamble detection. Figure 6 depicts the detection probability as a function of the SF used by the jammer (i.e., the detector) under different SFs used by the end node. As illustrated in Figure 6(a), more than 90% detection rate can be obtained when both the jammer and end node use the same SF and the same BW. For example, when the end node transmits preambles with SF9, the jammer with SF9 can detect all the preambles sent from end node. It is worthy to notice that when the SF of end node is greater than 8, the CAD could also detect the preambles transmitted with adjacent SF. For example, when the jammer applies SF10 to detect preambles, the ratios of detecting preambles transmitted by SF9 and SF11 are 96% and 67% respectively. As can be seen in Figure 6(b), the jammer with 250 kHz BW could obtain 100% detection rate when the applied SF is 2 less than that of end node. For example, the detection probability is 100% when the SFs of the end node and jammer are 11 and 9, respectively. Moreover, due to the same chirp rate, the CAD under 250 kHz BW would react to that under 125 kHz BW. Consequently, the reactive jammer could select appropriate SF and BW setup to achieve jamming attack.

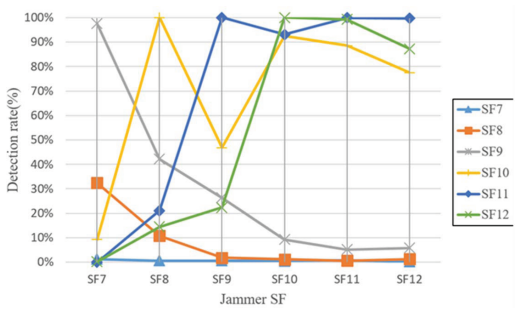
2) Experiment B: Verification of the jamming effect with respect to BW and TP

Figure 7 shows the PDR in accordance with SF and ΔTP under different BWs when the constant jammer is applied. Figure 7(a) illustrates the obtained PDRs as a function of SFs under different ΔTPs when BW is 125 kHz. We can find that, when $\Delta TP < +6$ dB, the PDR drops to around 0%, which indicates that all packets are totally jammed. Figure 7(b) shows the obtained PDRs as a function of SF under different ΔTPs when BW is 250 kHz. The PDR becomes 100% when ΔTP is +6 dB regardless the changes of SF. It is because none of the non-orthogonal pairs in 250 kHz BW can jam the packets. Furthermore, when the SF is below 11 and $\Delta TP < +6$ dB, the PDR drops sharply. Specifically, when the SF is between 7 and 9 and ΔTP is between -3 and -6 dB, the PDR drops to 0%. Hence, to better evaluate jamming effects, we would suggest to set BW as 125 kHz.

3) Experiment C: Evaluation of the jamming effect of the reactive jammer in LoRaWAN

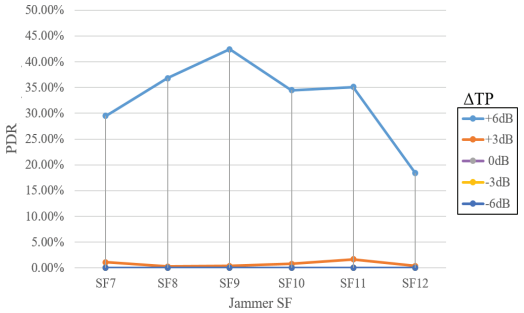


(a) Detection probability under 125 kHz BW.

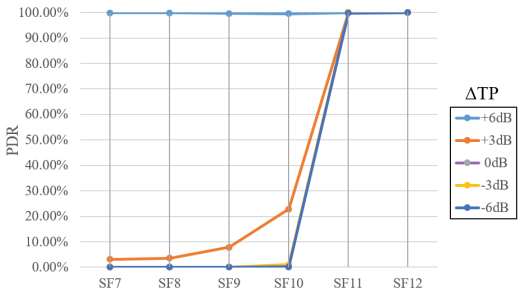


(b) Detection probability under 250 kHz BW.

Fig. 6. Performance of CAD under different combinations of SF and BW.



(a) PDRs under 125 kHz BW.



(b) PDRs under 250 kHz BW.

Fig. 7. Constantly jamming effects in accordance with SF and ΔTPs under different BWs.

According to the result obtained from the experiment B, we choose 125 kHz as channel bandwidth of the jammer for evaluating the performance of reactive jamming. As shown in Figure 8, the reactive jammer also has the ability to jam packets. When $\Delta TP < +3$ dB, the reactive jammer could effectively jam packets as the obtained PDRs are less than 10%. When ΔTP is +3 dB, the PDR increases with the increasing of the SF. It implies that the jammer applies a higher SF will result in less jamming effect, which is quite

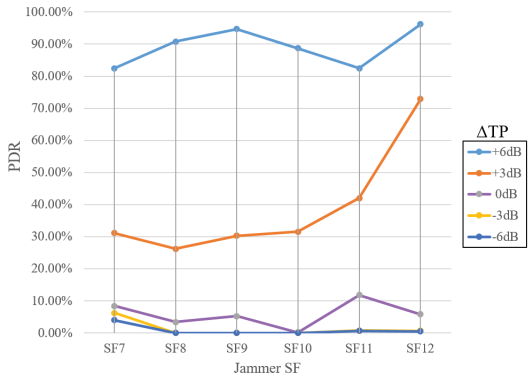


Fig. 8. Jamming effects of reactive jammer when BW is 125 kHz.

different from that of constant jammer. Additionally, when ΔTP is +6 dB, more than 80% packets are successfully received by the gateway. Under this condition, the obtained PDR is not as good as the constant jammer addressed in experiment B. However, the advantages of deploying reactive jammer are 1) the power efficiency of the reactive jammer is better than constant jammer, and 2) the LoRaWAN operator is difficult to detect the existence of the reactive jammer.

V. Effect and Countermeasures for Jamming Attack

LoRaWAN networks are typically organized in a star-of-stars topology in which gateways relay messages between the end node and the centralized network server in the core network. Gateways are usually connected to the network server via wired links while end nodes use single-hop LoRa communication to connect to one or more gateways in order to access the network server. The data transmission from an end node to the network server is treated as success if any of these gateways can successfully decode the received packet. In other words, the LoRaWAN data would be secured if the jammer fails to cover all serving gateways of an end node.

From the experimental results, we found that the non-orthogonality of LoRa transmission could be potential jamming threat for the data transmission in LoRaWAN. Specifically, when the end node and the jammer transmit signals at the same time, the signals with the same chirp rate will collide with each other which in turn causes failed reception at the gateway. Additionally, when the jammer enables the CAD mode for preamble detection, the LoRa transceiver still has the ability to block transmissions. The transmissions will be blocked if the SINR perceived at the gateway is below certain threshold. It indicates that deploying a reactive jammer nearing the gateways is a reasonable strategy to accomplish the jamming attack meanwhile avoiding the risk of being detected by the LoRaWAN operator.

However, the jamming may not be effective when the jammer is far from the gateway. Even though all gateways are within the coverage area of the jammer, the SINRs perceived at gateways should be different due to the geolocations of gateways, end node and jammer. Assuming the jammer and the end node are not collocated together, the diverse geolocations of multiple gateways are helpful to decode the data packets transmitted from the end node. Moreover, the conservative-based algorithm of determining the SF is an alternative approach against the malicious interference because the selection of SF is a trade-off between bit error rate and data rate. A lower value of SF is adopted, a lower bit error rate and a higher data rate would be derived.

VI. Conclusion

Attackers can utilize the weakness of physical layer to jam the data transmission of LoRaWAN. For example, the non-orthogonality of LoRa transmission could be potential jamming threat for data transmission. A jammer is developed in this paper with public LoRa transceiver with necessary change by us to enable CAD functionality. Evaluation results show that the jamming effect indeed is a security concern for LoRaWAN deployment. To overcome the jamming threat, we suggest the distributed deployments of the gateways in LoRaWAN.

References

[1] N. Sornin, M. Luis, T. Eirich, T.Kramp, and O.Hersent, "LoRaWAN Specification," *LoRa Alliance Inc., San Ramon, CA, Ver. 1.0.2*, Jul. 2016.

[2] U. Raza, P. Kulkarni, M. Sooriyabandara, "Low power wide area networks: An overview," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 855–873, Jan. 2017.

[3] M. Bor, J. Vidler, and U. Roedig, "LoRa for the Internet of Things," in *Proceedings of the 2016 International Conference on Embedded Wireless Systems and Networks, EWSN '16*, 2016, pp. 361–366.

[4] M. Bor and U. Roedig, "Do LoRa low-power wide-area networks scale?" in *Proceedings of the 19th ACM Int. Conf. Modeling, Analysis Simulation Wireless Mob. Syst.*, 2016, pp. 59–67.

[5] K. Mikhaylov, Juha Petaejaejaervi, and T. Haenninen, "Analysis of capacity and scalability of the LoRa low power wide area network technology," in *European Wireless 2016; 22nd European Wireless Conference, Oulu, Finland*, 2016, pp. 1–6.

[6] O. Georgiou and U. Raza, "Low power wide area network analysis: Can LoRa scale?" *IEEE Wireless Communications Letters*, vol. 6, no. 2, pp. 162–165, Apr. 2017.

[7] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 4, pp. 42–56, Fourth Quarter 2009.

[8] T. Voigt et al., "Mitigating inter-network interference in LoRa networks," *[Online]. Available: https://arxiv.org/abs/1611.00688*.

[9] K. Mikhaylov et al., "On LoRaWAN scalability: Empirical evaluation of susceptibility to inter-network interference, ," *in press*.

[10] K. Zhao and L. Ge, "A survey on the Internet of Things security," in *2013 Ninth International Conference on Computational Intelligence and Security, Leshan*, 2013, pp. 663–667.

[11] LoRa: Orthogonality, *[Online]. Available:http://sakshamaghoslya.blog-spot.tw/p/lora_6.html*.

[12] Semtech Corporation. (2013, July), "AN1200.13 SX1272/3/6/7/8 LoRa modem design guide," *(Revision 1) [Online]. Available: https://www.semtech.com/images/datasheet/LoraDesignGuide_STD.pdf*.

[13] ——, "AN1200.13 SX1272/3/6/7/8 LoRa modem design guide," *(Revision 1) [Online]. Available:https://www.semtech.com/images/datasheet/LoraDesignGuide_STD.pdf*.

[14] Semtech Corporation. (2014, Oct), "AN1200.21 reading channel RSSI during CAD," *(Revision 1.0) [Online]. Available:http://www.sem-tech.com/images/datasheet/an1200.21_std.pdf*.

[15] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, 2005, pp. 46–57.

[16] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of service attacks in wireless networks: The case of jammers," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 2, pp. 245–257, Second Quarter 2011.

[17] N. Sornin and L. Champion, "U.S. Patent No 14/755,602," Jan. 2016.