DEMO: Illuminating the BlindSpot: Efficient Single-Node Selective Jamming for LoRaWAN

Vincenz Mechler
Secure Mobile Networking Lab
TU Darmstadt, Germany
vmechler@seemoo.tu-darmstadt.de

Frank Hessel
Secure Mobile Networking Lab
TU Darmstadt, Germany
fhessel@seemoo.tu-darmstadt.de

Matthias Hollick
Secure Mobile Networking Lab
TU Darmstadt, Germany
mhollick@seemoo.tu-darmstadt.de

Bastian Bloessl
Secure Mobile Networking Lab
TU Darmstadt, Germany
bbloessl@seemoo.tu-darmstadt.de

Abstract

LoRaWAN has become a widely adopted, cost-effective solution for Low-Power Wide-Area Networks (LPWANs), bridging the gap between short-range wireless protocols and high-power cellular networks. Its affordable hardware and robust physical layer make it a key enabler for Internet of Things (IoT) applications across sectors like agriculture, smart cities, and industrial automation—domains where security is of central importance. Investigating LoRaWAN's resilience against physical-layer attacks, we developed *BlindSpot*, a novel jamming attack targeting state-of-the-art LoRaWAN gateways. Unlike traditional jammers, BlindSpot does not rely on overpowering transmissions but prevents their reception by exhausting resources at the gateway. This is possible since commercial gateway processors have only a limited number of demodulators for parallel frame reception. In this demo, we show the effectiveness of the attack against a commercial LoRaWAN gateway, compare it to traditional jamming, and show how our Software-Defined Radio (SDR)-based receiver can overcome the attack.

ACM Reference Format:
Vincenz Mechler, Frank Hessel, Matthias Hollick, and Bastian Bloessl. 2025. DEMO: Illuminating the BlindSpot: Efficient Single-Node Selective Jamming for LoRaWAN. In *18th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec 2025), June 30-July 3, 2025, Arlington, VA, USA.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3734477.3736153

1 Introduction

With the growing demand for low-power, long-range connectivity across industries like smart cities, agriculture, healthcare, and industrial automation, LoRaWAN has become a major player in the Internet of Things (IoT) landscape [4]. With low cost of the hardware components and low power consumption, it is a popular choice for deployments where physical access for maintenance is challenging. As LoRaWAN is being integrated into more and more systems, among those critical infrastructure and production processes, confidentiality, integrity, and availability of the technology become ever more important. Yet, many vulnerabilities have been discovered over the course of its history, enabling, e.g., eavesdropping and replay attacks [2, 7]. Furthermore, like any wireless technology, LoRaWAN is susceptible to jamming, which can directly impact the availability of the network and also act as an enabler for attacks on higher layers.

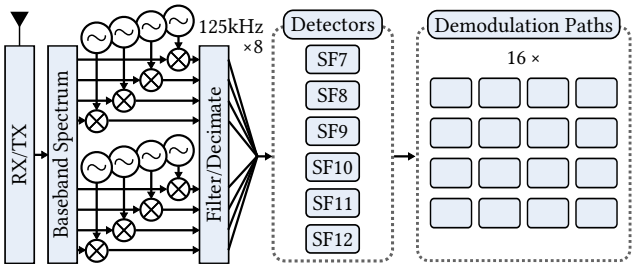

Figure 1: Simplified receiver structure of the SX1302 LoRa baseband processor, used in LoRaWAN gateways.

2 BlindSpot

Studying LoRaWAN's resilience to physical-layer attacks, we recently introduced *BlindSpot* [5], a novel attack that enables jamming and selective replay of arbitrary uplink frames. While traditional jamming relies on overpowering or corrupting legitimate transmissions and, therefore, requires the jammer to create a relatively high interference power level, our attack is based on precisely controlled resource exhaustion at the gateway.

This is possible since commercial gateways have only a limited number of demodulation paths available in their baseband signal processor. Depending on the chip, there are 8 to 16 demodulation paths, enabling the reception of at most 16 frames in parallel. Figure 1 shows the relevant parts of the SX1302 LoRa baseband processor, a state-of-the-art transceiver for LoRaWAN gateways that can detect frames with arbitrary Spreading Factors (SFs) on 8 frequency channels and dispatch them dynamically to one of the 16 available demodulation paths.

This is in contrast to the high number of available subchannels in typical LoRaWAN deployments, e.g., 8 frequency channels with 6 possible SFs, resulting in 48 logical channels in the EU 863–870 frequency plan. While a commercial gateway can listen on all 48

WiSec 2025, Arlington, VA, USA

ACM ISBN 979-8-4007-1530-3/2025/06
https://doi.org/10.1145/3734477.3736153

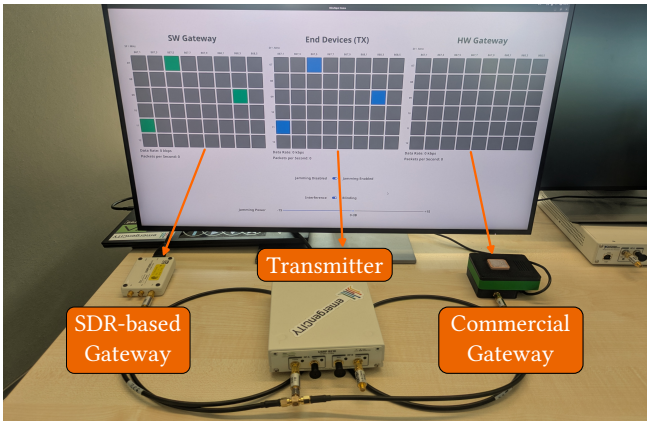

Figure 2: Photograph of our demonstrator setup. The uplink traffic and the jamming signals are generated by the SDR in the middle and fed to a commercial gateway and an SDR-based gateway.

logical channels at the same time, it can only decode as many frames in parallel as it has demodulation paths available. By occupying all available demodulation paths in the LoRa baseband processor with bogus frames, an attacker can effectively prevent the reception of legitimate uplink frames. This works as long as the blinding frames are received by the gateway, independent of the power level of the original transmission that should be jammed.

Using this new mechanism, BlindSpot comes with different trade-offs compared to traditional interference-based jamming attacks regarding range, energy consumption, and exposure of the attacker. Even though the LoRa physical layer is very robust, traditional jamming attacks can provide high success rates, given enough transmit power. However, the attack becomes ineffective as soon as the power level of the jamming signal fails to create the necessary interference at the gateway. Even with the most advanced strategies, the attacker has to push the Signal-to-Interference Ratio (SIR) down below 5 dB [1, 3].

BlindSpot, in turn, is effective at significantly lower power levels, as it only requires the reception of the blinding frames by the gateway. As a result, our attack can cover a larger area and is less sensitive to the placement of end devices, gateways, and the attacking node.

3 Demonstration

In our demonstration, we focus on visualizing the effectiveness of the blinding attack against a commercial LoRaWAN gateway and show how it can be countered with an SDR-based receiver implementation that is not limited in the number of available demodulation paths. To keep the demonstration setup compact, we use an SDR to generate both the original transmissions and the jamming signals. The combined signal is then fed into a commercial LoRaWAN gateway and our open source SDR-based LoRa gateway [6]. All signal processing is implemented using our FutureSDR framework,[1] enabling efficient and portable SDR applications.

[1] https://www.futuresdr.org

To comply with regulatory restrictions and to avoid interfering with other systems, we connect the devices via cable and attenuators. Since the attack is not targeted and affects all gateways in range, this also prevents adverse effects on existing LoRaWAN deployments. The resulting setup is shown in Figure 2.

Our graphical user interface visualizes the resource grid of the LoRaWAN EU 863–870 frequency plan (8 channels with 6 possible SFs). The three blocks show the three entities of the setup: The transmitter, generating both the uplink traffic and the jamming signals, in the middle; the commercial gateway to the right; and the SDR-based gateway on the left. Each cell shows the reception (passed and failed checksum in green and orange, respectively) and transmission (in blue) of frames on the corresponding subchannel in real-time, by changing its color for the duration of the frame.

The transmitting SDR generates uplink traffic, choosing random channels and SFs. In addition, the user can switch between interference-based jamming, BlindSpot, or disable jamming altogether. The jamming power can be adjusted on the fly, which allows exploring the performance of the strategies in different scenarios, e.g., when the attacker is significantly closer to or farther away from the gateway than the legitimate end devices. The transmitter and gateways further show approximate transmitted and received data rates, respectively. Therefore, the effect of the jamming attack can be observed live under varying parameters, and our blinding attack can be directly compared to traditional interference-based jamming. Finally, the direct comparison between a commercial LoRaWAN gateway and our SDR-based implementation illustrates the vulnerability and shows how a receiver that is not limited in the number of demodulation paths can counter the attack.

References

[1] D. Croce, M. Gucciardo, S. Mangione, G. Santaromita, and I. Tinnirello. 2018. Impact of LoRa Imperfect Orthogonality: Analysis of Link-Level Performance. 22, 4, (Apr. 2018). doi:10.1109/LCOMM.2018.2797057.

[2] F. Hessel, L. Almon, and M. Hollick. 2023. LoRaWAN Security: An Evolvable Survey on Vulnerabilities, Attacks and their Systematic Mitigation. *ACM Transactions on Sensor Networks*, 18, 4, (Mar. 2023). doi:10.1145/3561973.

[3] N. Hou, X. Xia, and Y. Zheng. 2023. Jamming of LoRa PHY and Countermeasure. *ACM Transactions on Sensor Networks*, 19, 4, (Nov. 2023). doi:10.1145/3583137.

[4] M. Jouhari, N. Saeed, M.-S. Alouini, and E. M. Amhoud. 2023. A Survey on Scalable LoRaWAN for Massive IoT: Recent Advances, Potentials, and Challenges. *IEEE Communications Surveys & Tutorials*, 25, 3, 1841–1876. doi:10.1109/COMST.2023.3274934.

[5] V. Mechler, F. Hessel, M. Hollick, and B. Bloessl. 2025. BlindSpot: Efficient Single-Node Selective Jamming for LoRaWAN. In *18th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. ACM, Arlington, VA. doi:10.1145/3734477.3734724.

[6] V. Mechler, M. Hollick, and B. Bloessl. 2024. Beyond Sensing: A High-Performance Software-Defined LoRa Gateway. In *30th Annual International Conference on Mobile Computing and Networking (MobiCom 2024), 18th ACM International Workshop on Wireless Network Testbeds, Experimental evaluation and Characterization (WiNTECH 2024)*. ACM, Washington, DC, (Nov. 2024). doi:10.1145/3636534.3697317.

[7] H. Noura, T. Hatoum, O. Salman, J.-P. Yaacoub, and A. Chehab. 2020. LoRaWAN Security Survey: Issues, Threats and Possible Mitigation Techniques. *Internet of Things*, 12. doi:10.1016/j.iot.2020.100303.

This work has been co-funded by the LOEWE initiative (Hesse, Germany) within the emergenCITY [LOEWE/1/12/519/03/05.001(0016)/72] center, as well as the German Research Foundation (DFG) in the Collaborative Research Center (SFB) 1053 MAKI (Project-ID 210487104). The authors acknowledge the financial support by the Federal Ministry of Education and Research of Germany in the project "Open6GHub" (grant number: 16KISK014).