Mute the Immutable - Making WiFi-to-LoRa CTC Robust Against WiFi Selective Jamming

Sascha Rösler, Anatolij Zubow, and Falko Dressler
School of Electrical Engineering and Computer Science, TU Berlin, Germany
{roesler,zubow,dressler}@tkn.tu-berlin.de

***Abstract*—Cross-technology communication (CTC) is a key enabler for direct over-the-air communication between incompatible wireless technologies. By using signal emulation the CTC frame contains the waveform of both, underlying and the emulated technology, and is vulnerable to selective jamming attacks on both technologies, so-called technology-selective jamming (TSJ). In this paper, we target WiFi-to-LoRa CTC and present a low-cost hardware solution that allows to mute the signature from the underlying technology, making it robust against WiFi jamming. Its feasibility is demonstrated using a full prototype, where a selective WiFi jammer was unable to interrupt the emulated LoRa transmission.**

***Index Terms*—Cross-technology communication, CTC, jamming, WiFi, LoRa**

I. Introduction

The rise in the Internet of things increases the use of heterogeneous incompatible wireless technologies in the 2.4 GHz ISM band, such as WiFi, Bluetooth, ZigBee, and LoRa, requiring additional multi-technology gateways (MTG) for communication. Cross-technology communication (CTC) overcomes this limitation by allowing devices of different technologies to communicate with each other without the need for MTGs. Although the first CTC approaches used side channels, later approaches use signal emulation instead for higher data rates, as we do in the WiFi-to-LoRa CTC Wi-Lo [1]. For signal emulation the payload of a frame of one technology (the underlying technology) is chosen in a way that it forms in the air the waveform of the receiving technology (the emulated technology). This new signal contains the preambles of both technologies (Figure 1), which can both be attacked by technology-selective jamming (TSJ). Such a jammer first listens on a channel and, as soon as it detects a given preamble, it switches to jamming mode, only corrupting frames of this specific format [2]. This makes TSJ an energy efficient jamming method. Without this vulnerability CTC is a good candidate to increase resilience in a multi-link network, as we already analyzed [3]. In this paper, we present `hardenedWiLo` which solves the presented vulnerability by muting the immutable WiFi preamble of Wi-Lo with the help of a small hardware circuit. We show, that this approach successfully re-enables communication in a TSJ scenario.

II. Related Work

There are numerous works that handle jamming attacks. For example, Vanhoef and Piessens [2] studied how COTS WiFi hardware can be used to implement a WiFi TSJ to run a TKIP attack. Proano and Lazos [4] show that encryption prevents TSJ attacks, as randomization avoids recognizable patterns. In case of 5G, Skokowski et al. [5] renew the ideas of channel hopping, MIMO techniques and to adjust the transmission range. In ZigBee, introducing a random delay can avoid the jamming of fixed timing communication, as Achour et al. [6] discuss. Up to our knowledge, there is no work to strengthen CTC against TSJ.

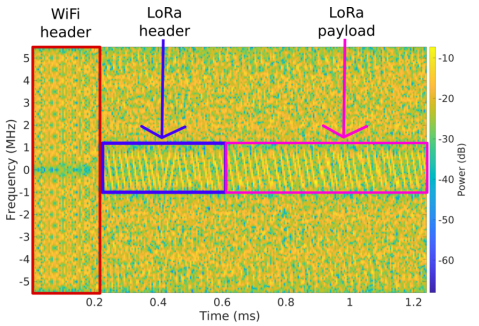


Figure 1. Spectrum of Wi-Lo signal with WiFi and emulated LoRa preamble

III. System Model & Problem Statement

We study how a co-located WiFi selective jammer effects a transmission from Wi-Lo to LoRa. Whenever the jammer detects a WiFi preamble, it starts its jamming actions. To make Wi-Lo robust against WiFi jamming we mute the WiFi preamble which is generated by the COTS WiFi card but not used for further transmission. However, the generation of the WiFi preamble is a core feature of the WiFi cards and can not be deactivated by software.

IV. Approach

To mute the immutable WiFi preamble, we developed a small hardware circuit to be placed between the WiFi card and its antenna (Figure 2). This circuit consists of (a) an ADL5910 board for packet detection, (b) a digital filter to prevent re-triggering of (c) the delay circuit. In case a packet is detected by (a), the WiFi preamble is muted by generating a pulse used as control input for the RF switch, such that antenna and WiFi card are disconnected during the duration of the WiFi preamble. Since Wi-Lo is based on IEEE 802.11b we adjust the pulse duration such that it has the length of the pure WiFi preamble (56 µs) or the length of a WiFi physical header (96 µs). For normal WiFi operation we propose adding an additional logic gate such that `hardenedWiLo` can be disabled via GPIO.

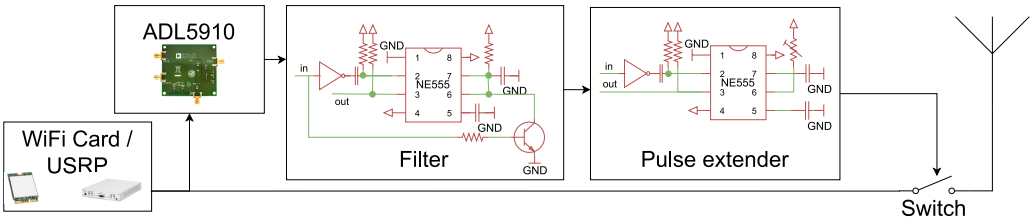


Figure 2. System model of `hardenedWiLo` including the ADL5910 for packet detection, a filter for retrigger prevention and NE555-based pulse extension

V. Performance Evaluation

For evaluation we are using the wired setup shown in Figures 3 and 4 consisting of an USRP-based transmitter, a COTS WiFi receiver, a LoRa receiver and a WiFi TSJ [2]. For comparison, we transmit packets of (a) WiFi 802.11b, (b) LoRa, (c) Wi-Lo under perfect channel conditions and jamming. For Wi-Lo we keep the switch closed while for `hardenedWiLo` we set t_m to 56 µs or 96 µs. We calculate the packet delivery ration (PDR) over 100 packets and repeat each experiment 10 times. Our results in Figure 5 reveal that while all three technologies reach a PDR of nearly 1.0 without jamming for a high transmission gain, nearly no WiFi and Wi-Lo packet is received in case the jammer is activated. With an activated muting of the WiFi preamble the Wi-Lo packets are received by the LoRa receiver, even thought the PDR is only 83% in case of $t_m = 96\,\mu s$. The lower PDR compared to $t_m = 56\,\mu s$ can be explained by the fact that an inaccurate packet detection can destroy parts of the LoRa packet.

VI. Conclusion

In this paper, we introduced a muting mechanism for signal emulation in CTC to strengthen CTC against technology specific jamming attack. For Wi-Lo, we show that a WiFi jammer can nearly completely prevent any communication. At the cost of a slightly reduced PDR, our approach successfully hides the Wi-Lo transmission from TSJ. For future work, we plan to use our approach for other CTCs.

Acknowledgements

This work was supported by the Federal Ministry of Education and Research (BMBF, Germany) within the 6G Research and Innovation Cluster 6G-RIC under Grant 16KISK020K as well as by the German Research Foundation (DFG) within the projects Resilient Worlds under grant DR 639/30-1 and ZU 235/4-1. We would like to thank Yeaeun Nam for helping with the implementation of the prototype and evaluation.

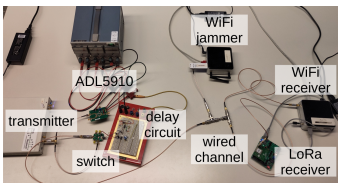


Figure 3. Wired setup in our lab

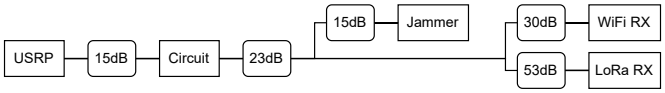
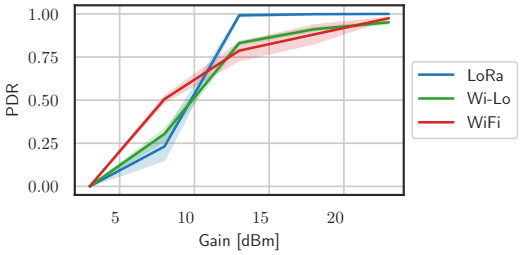
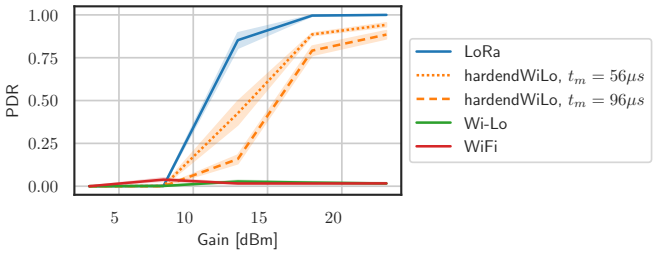


Figure 4. Schematic of wired experimental setup with attenuator



(a) no jamming



(b) under WiFi selective jamming

Figure 5. Selected results from experiments

References

[1] P. Gawłowicz, A. Zubow, and F. Dressler, "Wi-Lo: Emulation of LoRa using Commodity 802.11b WiFi Devices," in *IEEE International Conference on Communications (ICC 2022)*, Seoul, South Korea: IEEE, May 2022, pp. 4414–4419.

[2] M. Vanhoef and F. Piessens, "Advanced Wi-Fi Attacks Using Commodity Hardware," in *30th Annual Computer Security Applications Conference (ACSAC 2014)*, New Orleans, LA: ACM, Dec. 2014, pp. 256–265.

[3] A. Zubow, I. von Stebut, S. Rösler, and F. Dressler, "ResCTC: Resilience in Wireless Networks through Cross-Technology Communication," in *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2024)*, Valencia, Spain: IEEE, Sep. 2024.

[4] A. Proano and L. Lazos, "Packet-Hiding Methods for Preventing Selective Jamming Attacks," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, pp. 101–114, Jan. 2012.

[5] P. Skokowski, J. M. Kelner, K. Malon, K. Maślanka, A. Birutis, M. A. Vazquez, S. Saha, W. Low, A. Czapiewska, J. Magiera, P. Rajchowski, and S. Ambroziak, "Jamming and jamming mitigation for selected 5G military scenarios," *Procedia Computer Science*, vol. 205, pp. 258–267, 2022.

[6] M. Achour, M. Mana, and A. Rachedi, "On the issues of selective jamming in IEEE 802.15. 4-based wireless body area networks," *Peer-to-Peer Networking and Applications*, vol. 14, pp. 135–150, Jan. 2021.