Jamming Attack on DSRC Communication Caused by a C-V2X Sidelink Device

Breno Sousa
LASIGE
Faculdade de Ciencias
Universidade de Lisboa
Lisbon, Portugal
bfmelo@ciencias.ulisboa.pt

Naercio Magaia
Department of Informatics
University of Sussex
Brighton, United Kingdom
N.Magaia@sussex.ac.uk

Sara Silva
LASIGE
Faculdade de Ciencias
Universidade de Lisboa
Lisbon, Portugal
sgsilva@ciencias.ulisboa.pt

Hieu Nguyen and Yong Liang Guan
School of EEE
Nanyang Technological University
Singapore, Singapore
{nguyenth, eylguan}@ntu.edu.sg

***Abstract*—Academia and industry are constantly striving to improve the driving experience, where vehicles can now communicate, and different technologies can coexist and share the wireless medium to send and receive information. In terms of vehicle-to-vehicle (V2V) communication, vehicles can use Dedicated Short-Range Communication (DSRC) or Cellular Vehicle-to-Everything (C-V2X) sidelink technologies to communicate on the roads by sharing the 5.9 GHz band. However, coexistence between the two technologies remains challenging, as interference can occur when both technologies use co-channels to send vehicle messages in parallel, degrading the Packet Delivery Ratio (PDR) metric. In addition, malicious users can carry out various types of attacks to disrupt the vehicle connection, such as jamming attacks. In this paper, we transmitted packets using a constant bit rate (CBR). We considered Line-of-Sight (LOS) and Non-Line-of-Sight (NLOS) scenarios (i.e., in the DSRC communication) to understand how damaging the jamming attack can be. Based on our tests, the jamming attack caused by the C-V2X co-channel interference can cause an attenuation in the signal loss of up to 24 dB (i.e., using a packet size of 256 bytes) and up to 35 dB (i.e., using a packet size of 1,399 bytes), and signal-to-interference and noise ratio (SINR) by up to 26 dB (i.e., using a packet size of 256 bytes) and up to 40 dB (i.e., using a packet size of 1,399 bytes). Furthermore, we analyzed the interference effects in different data rates such as 3, 4.5, 6, 9, 12, 18, 24, and 27 Mbps.**

***Index Terms*—DSRC, C-V2X, jamming attack, interference, co-channel.**

I. Introduction

Intelligent Transportation Systems (ITS) applications were designed to make it more efficient in managing traffic problems by providing optimized solutions. The application of the Internet of Things (IoT) and edge computing concepts in a vehicular context gave rise to the Internet of Vehicles (IoV) [1]. IoV's architecture extends the Vehicular Adhoc NETworks (VANETs) to include a) Vehicle-to-Vehicle (V2V) communication, where vehicles share data with other surrounding vehicles in a broadcast manner; b) Vehicle-to-Roadside (V2R) communication, where vehicles share data with roadside units (RSU) to access additional systems/applications on the roads; c) Vehicle-to-Infrastructure (V2I) communication, where vehicles share information with various infrastructures such as road sensors, traffic lights, among others; d) Vehicle to Personal devices (V2P) communication, aiming to share information with personal devices such as smartphones; e) Vehicle-to-Sensor (V2S) communication, where internal vehicle's sensors process externally collected data, such as collision avoidance systems; and, f) Vehicle-to-everything (V2X) communication, to allow the vehicle to communicate with any compatible device [2].

Today, two vehicular communication technologies are available: Dedicated Short-Range Communication (DSRC) and Cellular Vehicle-to-Everything (C-V2X) sidelink. DSRC was first proposed to support safety applications in vehicular scenarios [3]. DSRC is based on the IEEE 802.11p standard for Wireless Access in Vehicular Environments (WAVE) [4]. C-V2X is based on the 3rd Generation Partnership Project (3GPP), which uses cellular technology such as Long Term Evolution (LTE) and New Radio 5G (Fifth-Generation) [5]. Since both technologies use the same 5.9 GHz band, some problems may occur.

Therefore, vehicular networks are prone to various types of attacks, such as denial-of-service (DoS) attacks, fabrication attacks, and jamming attacks. Dealing with the latter attacks is not trivial, as its conceptual meaning is related to channel interference [6]. In a nutshell, as the devices compete for the same medium access for sending and receiving information, in order to perform a jamming attack, a malicious user intentionally attempts to disrupt the reception of network packets by sending an interference signal on the same channel/frequency as legitimate devices to disrupt them.

In addition, Basic Safety Messages (BSMs) can be used for collision avoidance or to report adversarial road conditions. However, malicious users can interfere with the medium access by constantly sending malicious signals/packets, that is, using a C-V2X sidelink device to jam a DSRC communication or vice-versa. Please, note that, in contrast to DoS, the jammer attacker does not need to send network packets to a target device, since its target is the medium access.

In this work, we analyzed the effects of the jamming attack on DSRC communication in Line-of-Sight (LOS) and Non-Line-of-Sight (NLOS) scenarios. We used different packet sizes to study the channel degradation for each scenario. We tested our scenarios considering different modulations (i.e., BPSK, QPSK, 16QAM, and 64QAM) and coding schemes (i.e., 1/2 and 3/4) to understand how the data transmission

rate and packet size would influence the Packet Delivery Ratio (PDR).

The rest of the paper is organized as follows: Section II presents the related work. Section III describes the LOS and NLOS scenarios in the DSRC communication. Section IV presents each scenario's PDR and Packet Loss Ratio (PLR) considering different packet sizes. Section V presents a discussion of the proposed scenarios. Finally, Section VI presents conclusions.

II. Related Work

Using network simulators enables overcoming the lack of a real testbed. However, their use and the generated outputs may be biased since their results are based on the implemented scenario and do not consider the real performance of vehicular hardware. Physical devices behave according to their hardware specifications and the environment. Thus, building a scenario using physical devices and performing a jamming attack can give us a more realistic performance of a real scenario under this type of attack. Nonetheless, we searched for published papers that used physical devices in the vehicular context that performed jamming attacks. However, our search for these types of papers was not fruitful, as most papers use simulators. So we extend the study of jamming attacks in the vehicular networks with our study by using physical devices and reporting the performance of the proper vehicular hardware technology.

G. Nardini et al. [7] analyzed the coexistence of C-V2X and DSRC. They used the WiLabV2XSim simulator to perform their analysis, which was considered scenarios with up to 3,000 vehicles. Although their research is not about jamming attacks, their experiments considered co- and adjacent-channel interference. Furthermore, their experiments are related to understanding the channel busy and packet reception ratios in both technologies caused by interference.

As an example of how simulators may be biased and not capture the real effect of a jamming attack, authors in [8] reported a PLR of just 32.65%, while in our worst case we reported a PLR of 91.70%. In addition, it lacks testing their solution considering different modulations and coding scheme.

G. Twardokus and H. Rahbari [9] analyzed the effects of jamming attacks in the vehicular context. Their analysis considered the jamming problem in the C-V2X sidelink communication, where three physical devices were used. Similarly to our study, they also reported a PLR of around 90% and a degraded C-V2X channel throughput by 50%. Unlike our study, they do not consider the jamming attack in the communication of DSRC devices and co-channel interference.

A. S. Da Silva [10] et al. highlighted some driving use cases of jamming attacks on vehicular scenarios: first, the vehicular protocols need to share real-time data and can be affected directly by a jammer on the roads; second, jamming attack on do not pass warning, which a jammer compromises the function of sending warnings when an autonomous vehicle chooses to maneuver to overtake another vehicle, and this lack of communication can be aggravated in rainy and snowy scenarios; third, jamming attack on intersection movement assist, where a autonomous vehicle can be affected by not receiving assistance when it chooses to turn in selected directions, where there is no traffic information.

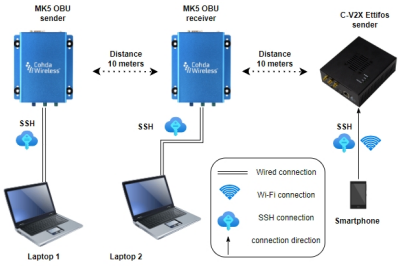


Fig. 1: Testbed overview.

M. Arif [11] et al. studied the jamming attack in Cellular-Assisted Vehicular Communications, where they performed simulations in MATLAB using the Monte Carlo algorithm. Their study considered the effects of clusters of jamming attackers. In [10], the authors discuss threats and countermeasures for radio jamming in Vehicle-to-Everything (V2X) communication, in which they use the Simu5G [7] simulator to analyze a proposed beamforming strategy and reduce the effects of jamming attack.

H. Nguyen and Y. L. Guan [12] analyzed the effects of C-V2X interference on DSRC communication using adjacent channels. Their experiment reported a PDR of 90% and 80% in the LOS and NLOS scenarios, respectively. However, as we can see in Section IV, the jamming attack caused by co-channel interference is more harmful.

III. Experiment Model

We aim to consider the effects of the jamming attack caused by co-channel interference from a C-V2X device (i.e., the jamming device) in LOS and NLOS scenarios. For this purpose, we built a testbed using DSRC and C-V2CX devices, see Fig. 1. In addition, our scenario aimed to emulate urban traffic where vehicles may be near, such as traffic jams, intersections, and traffic lights. We used three devices, namely two Cohda MK5 OBUs (i.e., one sender and one receiver device) and one Etiffos C-V2X sidelink, where each MK5 OBU has a wired connection to a laptop to enable us to start the data transmission. The receiver device is 10 meters far away from the sender device (please note that other works have also used this distance, such as [13] (e.g., busy highways scenario) and [14] (e.g., clustering)). To run the C-V2X application, we connected a smartphone to the C-V2X device. All devices are using channel 184. Please note that we use a Secure Shell (SSH) connection to access all devices and, concerning the C-V2X device, we are using the LTE-V2X sidelink version. Further, we chose the packet size based on the work [15].

The application used by the MK5 OBU sender was implemented in Python, and sockets are used to share data in broadcast mode. We used the following settings: 1) modulation

(a) LOS scenario

(b) NLOS scenario

Fig. 2: Test scenarios. (a) shows the LOS scenario considering the DSRC communication, where there is no obstruction between the sender and the receiver. (b) shows the NLOS scenario considering the DSRC communication, where we have a brick wall as an obstruction.

and coding schemes (MCS): BPSK with 1/2 (data rate: 3 Mbps), BPSK with 3/4 (data rate: 4.5 Mbps), QPSK with 1/2 (data rate: 6 Mbps), QPSK with 2/3 (data rate: 9 Mbps), 16QAM with 1/2 (data rate: 12 Mbps), 16QAM with 3/4 (data rate: 18 Mbps), 64QAM with 1/2 (data rate: 24 Mbps) and 64QAM with 3/4 (data rate: 27 Mbps); 2) bandwidth: 10 MHz; 3) packet rate: 50 Hz; 4) packet size: 256 and 1,399 bytes.

The application sent 20,000 packets, at a constant bit rate (CBR), in each scenario to understand the impact of the jamming attack and see how it affects the Packet Delivery Ratio (PDL) performance. Since we have eight MCS, as mentioned, we need to run four runs for each scenario, that is, four runs considering the LOS scenarios and another four runs for the NLOS scenarios. The PDR and PDL metrics are calculated using Equations 1 and 2.

$$PDR = (\text{Total Received Packets}/\text{Total Sent Packets}) \times 100 \quad (1)$$

$$PLR = 100\% - \text{PDR} \quad (2)$$

For the LOS scenario, we need to run the configuration considering: 1) 1 MK5 OBU as the sender (i.e., using packet size 256 bytes) and 1 MK5 OBU as the receiver, but without the C-V2X device; 2) 1 MK5 OBU as the sender (i.e., using packet size 256 bytes) and 1 MK5 OBU as the receiver, and 1 C-V2X device to interfere in the MK5 OBU communication; 3) 1 MK5 OBU as the sender (i.e., using packet size 1,399 bytes) and 1 MK5 OBU as the receiver, but without the C-V2X device; 4) 1 MK5 OBU as the sender (i.e., using packet size 1,399 bytes) and 1 MK5 OBU as the receiver, and 1 C-V2X device to interfere in the MK5 OBU communication. NLOS follows the same configurations. Fig. 2a shows the used devices in the LOS scenario, while Fig. 2b shows the used devices in the NLOS scenario.

We set the MK5 OBU and C-V2X sidelink to transmit at +23 dBm. We also set the jamming device to send one packet every 20 milliseconds, i.e., 50 packets per second with a packet size of 5,000 bytes. Therefore, our choice of 5,000 bytes was the maximum packet size that the jamming device could send, and smaller packet sizes would not have the same reported effect. In our experiments, we have seen that the PDR decreases as the packet size increases. Further, we used a spectrum analyzer to see how busy the channel is for our scenarios. Fig. 3 shows how crowded the channel is in our experiments, where the blue line represents the average channel usage, and the yellow line represents the instantaneous channel usage.

IV. Experiment Results and Analysis

To assess link quality between the MK5 OBU sender and receiver, we analyzed signal-to-noise ratio (SNR) and signal-to-interference and noise ratio (SINR) under LOS and NLOS conditions, with and without jamming. In Equation 3,

$$SNR = \frac{P_{\text{signal}}(mW)}{P_{\text{noise}}(mW)} \quad (3)$$

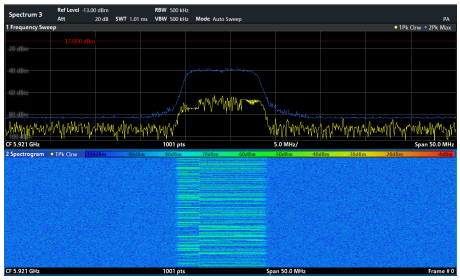
where $P_{\text{signal}}(mW)$ is the average power and $P_{\text{noise}}(mW)$ is the average noise. However, since we have dBm values in Table I, we need to convert them to milliwatts (mW). By the definition of Equation 4 [16], which converts mW to dBm, we can use Equation 5 to convert from dBm to mW.

$$P\ (\text{dBm}) = 10 \log_{10} \left(\frac{P_{\text{signal}}(\text{mW})}{1\ \text{mW}} \right) \quad (4)$$

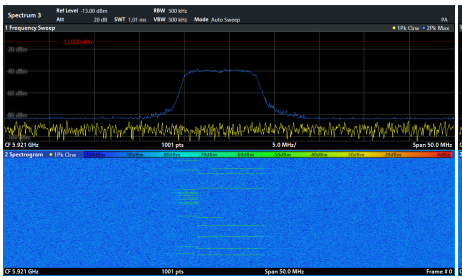
$$P(mW) = 1mW \times 10^{\frac{P(dBm)}{10}} \quad (5)$$

$$\text{SINR} = 10 \log_{10} \left(\frac{P_{\text{Rx}}}{P_{\text{noise}} + P_{\text{interference\_Rx}}} \right) \quad (6)$$

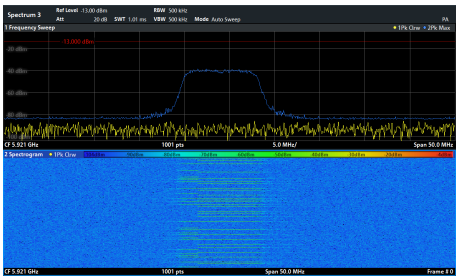
where $P_{\text{interference}}(mW)$ is the interference caused by the jamming device. By converting our *Prx* (i.e., received power) and *Noise* reported in Table I to mW and using Equations 3, 4, and 5, we get the SNR for the scenarios without jamming traffic. In addition, we can also get the SINR for the scenarios with jamming traffic using Equation 6: 1) LOS scenario without jamming traffic and packet size of 256 bytes: SNR = 43 dB; 2) LOS scenario with jamming traffic and packet size of 256 bytes: SINR = 26 dB; 3) NLOS scenario without jamming traffic and packet size of 256 bytes: SNR = 21 dB;



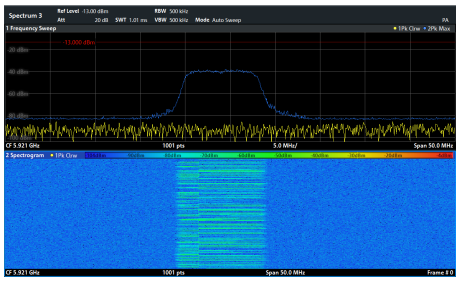
(a) Only jamming traffic (packet size: 5,000 bytes)



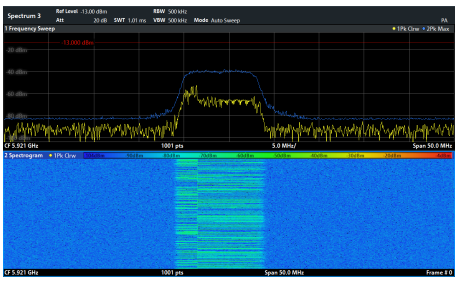
(b) MK5 OBU (packet size: 256 bytes) without jamming traffic



(c) MK5 OBU (packet size: 1,399 bytes) without jamming traffic



(d) MK5 OBU (packet size: 256 bytes) and jamming traffic (packet size: 5,000 bytes)



(e) MK5 OBU (packet size: 1,399 bytes) and jamming traffic (packet size: 5,000 bytes)

Fig. 3: Channel occupancy seen by the spectrum analyzer as the spectrogram (Blue line is the average spectrum and yellow line is the instantaneous spectrum).

TABLE I: Achieved SNR and SINR Values

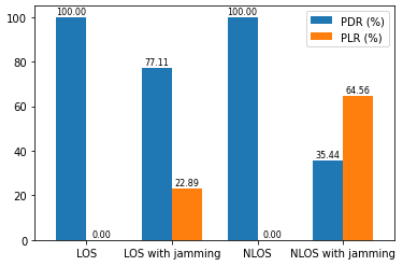
Scenario	Packet Size	*Prx* (dBm)	Noise (dBm)	Noise + Interference (dBm)	SNR (dB)	SINR (dB)
LOS w/o jamming	256 bytes	-61	-104	-	43	-
LOS w/ jamming	256 bytes	-57	-	-83	-	26
NLOS w/o jamming	256 bytes	-80	-101	-	21	-
NLOS w/ jamming	256 bytes	-81	-	-81	-	0
LOS w/o jamming	1,399 bytes	-66	-102	-	36	-
LOS w/ jamming	1,399 bytes	-55	-	-83	-	28
NLOS w/o jamming	1,399 bytes	-77	-102	-	25	-
NLOS w/ jamming	1,399 bytes	-90	-	-78	-	-12

4) NLOS scenario with jamming traffic and packet size of 256 bytes: SINR = 0 dB; 5) LOS scenario without jamming traffic and packet size of 1,399 bytes: SNR = 36 dB; 6) LOS scenario with jamming traffic and packet size of 1,399 bytes: SINR = 28 dB; 7) NLOS scenario without jamming traffic and packet size of 1,399 bytes: SNR = 25 dB; 8) NLOS scenario with jamming traffic and packet size of 1,399 bytes: SINR = -12 dB. In addition, Figures 4, 5, 6, 7, 8, 9, 10, and 11 shows the number of packets received and lost for all MCS tested. The results show that, without interference, DSRC maintains a low PLR due to the SNR and SINR values in Table I, regardless of modulation or packet size. However, with a C-V2X jammer, DSRC performance degrades significantly.

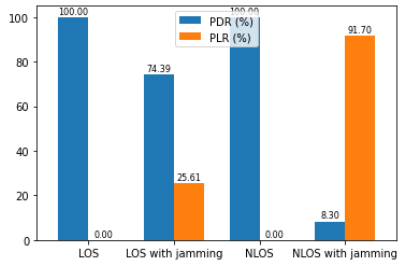
V. Discussion

Considering our demonstrated PDR and PLR due to jamming interference, there is a serious concern about the joint use of C-V2X and DSRC using the same channel in platooning scenarios, where the PDR must be at least 90% to meet the quality of service (QoS) [17]. When we used a data rate of 18 Mbps (i.e., 16QAM modulation and coding rate of 3/4) in the NLOS scenario with jamming traffic, we showed a PLR of 39.47%. Please note that a more harmful degradation could be observed in the network if the mobility and high speed of the vehicles were considered [15]. Taking into account the signal loss and the reported SINR, we can highlight:

- **Signal quality (SNR - 256 bytes)**: When we analyze the SNR in both scenarios, transmitting packets with 256 bytes and without the jamming attack, we can see a signal loss of 22 dB caused by just a brick wall. However, on congested roads, the number of vehicles or big vehicles [18] can further attenuate the signal quality, indicating a serious concern that may be addressed in future research.
- **Signal quality (SNR - 1,399 bytes)**: When transmitting

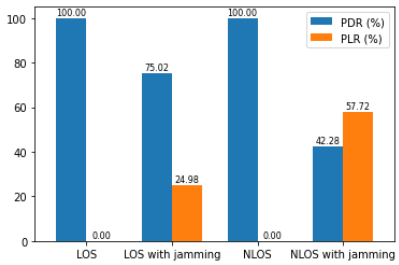


(a) 256 bytes

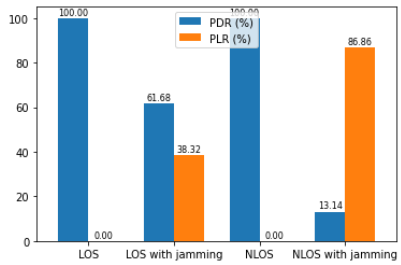


(b) 1,399 bytes

Fig. 4: PDR *versus* PLR for BPSK 1/2 modulation.

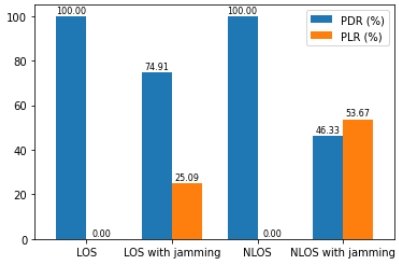


(a) 256 bytes

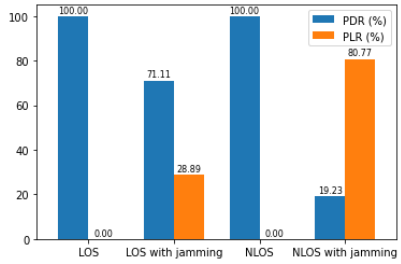


(b) 1,399 bytes

Fig. 5: PDR *versus* PLR for BPSK 3/4 modulation.

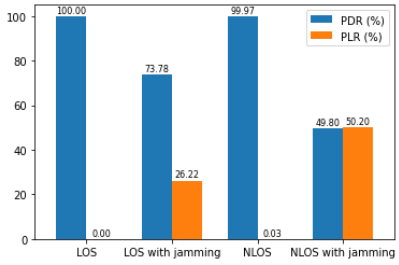


(a) 256 bytes

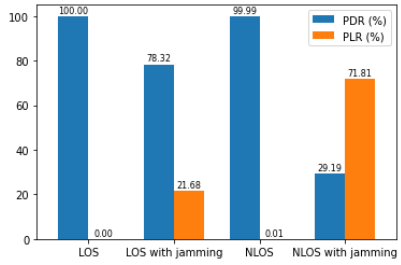


(b) 1,399 bytes

Fig. 6: PDR *versus* PLR for QPSK 1/2 modulation.



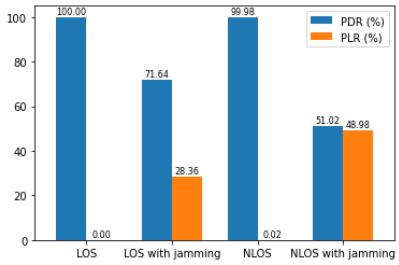
(a) 256 bytes



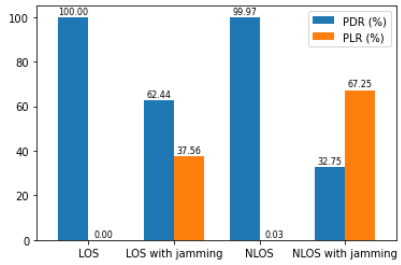
(b) 1,399 bytes

Fig. 7: PDR *versus* PLR for QPSK 3/4 modulation.

packets of 1,399 bytes, the achieved SNR indicates a signal loss of 11 dB. Despite this, our experiments in LOS and NLOS scenarios show a PDR above 99% for most modulation and coding rates. Notably, packet losses occurred even without a jamming attacker. In NLOS, using 64QAM with a coding rate of 1/2 and packet size

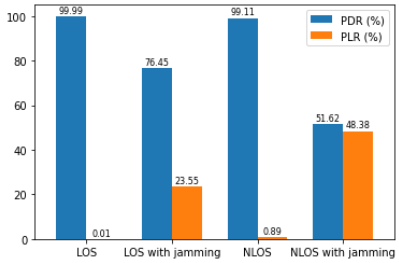


(a) 256 bytes

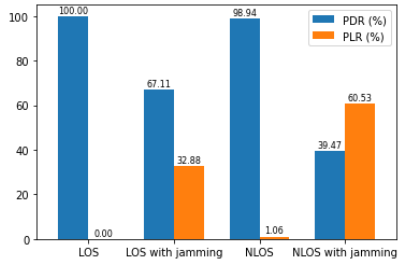


(b) 1,399 bytes

Fig. 8: PDR *versus* PLR for 16QAM 1/2 modulation.

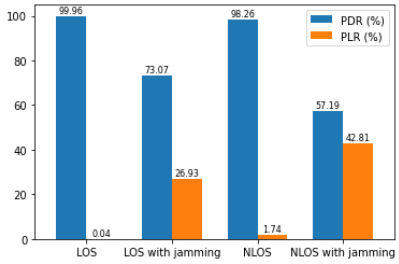


(a) 256 bytes

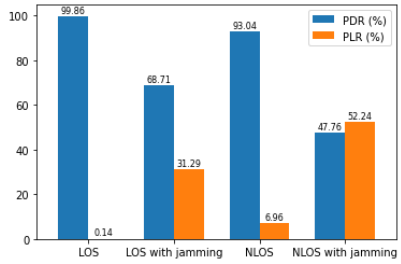


(b) 1,399 bytes

Fig. 9: PDR *versus* PLR for 16QAM 3/4 modulation.

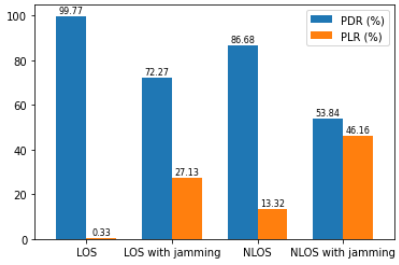


(a) 256 bytes

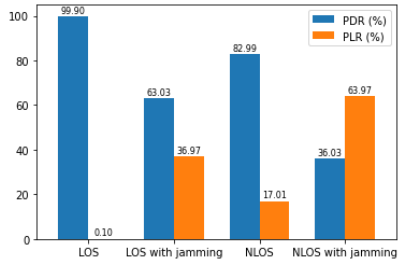


(b) 1,399 bytes

Fig. 10: PDR *versus* PLR for 64QAM 1/2 modulation.



(a) 256 bytes



(b) 1,399 bytes

Fig. 11: PDR *versus* PLR for 64QAM 3/4 modulation.

of 1,399 bytes, 6.96% of packets were lost. With a coding rate of 3/4, losses reached 13.32% for a packet size of 256 bytes and 17.01% for a packet size of 1,399 bytes.

- **Signal quality (SINR - 256 bytes)**: In this case, the jamming attack resulted in an average PLR of 29% in LOS scenarios. Furthermore, when the sender device

TABLE II: PDR Degradation (%) Due to Jamming Attack (Compared to No Jamming)

Scenario	BPSK 1/2	BPSK 3/4	QPSK 1/2	QPSK 2/3	16QAM 1/2	16QAM 3/4	64QAM 1/2	64QAM 3/4
LOS, 256 bytes	22.89	24.98	25.09	26.22	28.36	23.54	26.89	27.5
LOS, 1,399 bytes	25.61	38.32	28.89	21.68	37.56	32.89	31.15	36.87
NLOS, 256 bytes	64.56	57.72	54.67	50.17	48.96	47.49	41.07	32.84
NLOS, 1,399 bytes	91.7	86.86	80.77	70.80	67.12	51.47	45.28	46.96

transmitted packets of 256 bytes, the SINR dropped from 26 dB (as observed in the LOS scenario) to 0 dB, indicating a severe deterioration in signal quality.

- **Signal quality (SINR - 1,399 bytes)**: the NLOS with the jamming traffic and a packet of 1,399 bytes has a more harmful scenario. The SINR decreased from 28 dB (e.g., LOS scenario) to -12 dB, i.e., a very poor signal quality.

Furthermore, when comparing the best and worst-case scenarios (e.g., the LOS scenario with jamming traffic and a packet size of 1,399 bytes, and the NLOS scenario with jamming attack and a packet size of 1,399 bytes, respectively), there is a degradation in SINR of 40 dB, which can justify the PLR of 91.7% in the NLOS scenario with jamming traffic and a packet size of 1,399 bytes under BPSK modulation and a coding rate of 1/2. Table II shows the PDR degradation due to the jamming attack for each MCS used. The mean degradation for LOS with 256 and 1,399 bytes is 25.68% and 31.62%, respectively. For NLOS with 256 and 1,399 bytes, it is 49.69% and 67.62%, respectively. This emphasizes the severity of the jamming attack in the NLOS scenario.

VI. Conclusion

In this paper, to analyze the impacts of different data transmission rates in LOS and NLOS scenarios, we used different modulations such as BPSK, QPSK, 16QAM, and 64QAM combined with packet transmission rate and different packet sizes (e.g., 256 and 1,399 bytes). The most harmful scenarios (i.e., high packet loss problem) we reported are the NLOS scenarios with jamming traffic and a packet size of 1,399 bytes. For example, when we transmitted at 3 Mbps and a packet size of 1,399 bytes, we got a PLR of 91.70%. In addition, when we transmitted at the same data rate but using a packet size of 256 bytes, the PLR decreased to 64.56%.

Acknowledgment

This work was supported by H2020-MSCA-RISE under grant No. 101006411; and by Fundação para a Ciência e a Tecnologia (FCT), Portugal, through doctoral grant SFRH/BD/151413/2021 (https://doi.org/10.54499/SFRH/BD/151413/2021) under the MIT Portugal Program, and through funding of the LASIGE Research Unit, ref. UID/00408/2025 (https://doi.org/10.54499/UID/00408/2025).

References

[1] N. Magaia, P. Gomes, L. Silva, B. Sousa, C. X. Mavromoustakis, and G. Mastorakis, "Development of mobile iot solutions: approaches, architectures, and methodologies," *IEEE Internet of Things Journal*, vol. 8, no. 22, pp. 16 452–16 472, 2020.

[2] R. Gasmi and M. Aliouat, "Vehicular ad hoc networks versus internet of vehicles-a comparative view," in *2019 international conference on networking and advanced systems (ICNAS)*. IEEE, 2019, pp. 1–6.

[3] X. Wu, S. Subramanian, R. Guha, R. G. White, J. Li, K. W. Lu, A. Bucceri, and T. Zhang, "Vehicular communications using dsrc: Challenges, enhancements, and evolution," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 399–408, 2013.

[4] L. Silva, N. Magaia, B. Sousa, A. Kobusińska, A. Casimiro, C. X. Mavromoustakis, G. Mastorakis, and V. H. C. De Albuquerque, "Computing paradigms in emerging vehicular environments: A review," *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 3, pp. 491–511, 2021.

[5] Z. Ali, S. Lagén, L. Giupponi, and R. Rouil, "3gpp nr v2x mode 2: Overview, models and system-level evaluation," *IEEE Access*, vol. 9, pp. 89 554–89 579, 2021.

[6] 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, 2009.

[7] G. Nardini, D. Sabella, G. Stea, P. Thakkar, and A. Virdis, "Simu5g–an omnet++ library for end-to-end performance evaluation of 5g networks," *IEEE Access*, vol. 8, pp. 181 176–181 191, 2020.

[8] M. Talukder and J. Xie, "Symjam: Symbiotic jamming attacks on nr-v2x," in *GLOBECOM 2024-2024 IEEE Global Communications Conference*. IEEE, 2024, pp. 523–528.

[9] G. Twardokus and H. Rahbari, "Vehicle-to-nothing? securing c-v2x against protocol-aware dos attacks," in *IEEE INFOCOM 2022-IEEE Conference on Computer Communications*. IEEE, 2022, pp. 1629–1638.

[10] A. S. Da Silva, J. P. J. Da Costa, G. A. Santos, Z. Miri, M. I. Fauzi, A. Vinel, E. P. de Freitas, and K. Kastell, "Radio jamming in vehicle-to-everything communication systems: Threats and countermeasures," in *2023 23rd International Conference on Transparent Optical Networks (ICTON)*. IEEE, 2023, pp. 1–4.

[11] M. Arif, W. Kim, and S. Qureshi, "Interference characterization in cellular-assisted vehicular communications with jamming," *IEEE Access*, vol. 10, pp. 42 469–42 480, 2022.

[12] H. Nguyen and Y. L. Guan, "Dsrc performance under the adjacent channel interference of cellular-based v2x at 5.9ghz band," in *Vehicular Technology Conference. IEEE 99th Vehicular Technology Conference. VTC Spring 2024 (in press)*. IEEE, 2024.

[13] J. Speiranr, E. Shakshukir, A. Yasar, and H. Malik, "Results of eebl simulation for the smartphone vanet," *Procedia Computer Science*, vol. 231, pp. 86–95, 2024.

[14] H. Wang, R. P. Liu, W. Ni, W. Chen, and I. B. Collings, "Vanet modeling and clustering design under practical traffic, channel and mobility conditions," *IEEE Transactions on Communications*, vol. 63, no. 3, pp. 870–881, 2015.

[15] S. Gao, A. Lim, and D. Bevly, "An empirical study of dsrc v2v performance in truck platooning scenarios," *Digital Communications and Networks*, vol. 2, no. 4, pp. 233–244, 2016.

[16] B. Razavi and R. Behzad, *RF microelectronics*. Prentice hall New York, 2012, vol. 2.

[17] E. Moradi-Pari, D. Tian, M. Bahramgiri, S. Rajab, and S. Bai, "Dsrc versus lte-v2x: Empirical performance analysis of direct vehicular communication technologies," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 5, pp. 4889–4903, 2023.

[18] H. Nguyen, X. Xiaoli, M. Noor-A-Rahim, Y. L. Guan, D. Pesch, H. Li, and A. Filippi, "Impact of big vehicle shadowing on vehicle-to-vehicle communications," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 7, pp. 6902–6915, 2020.