Technical Report on Driving Use Cases for Highly Automated Driving and Key Performance Indicators

Christian Müller[1], João P. J. da Costa[2], Giovanni A. dos Santos[2], Yorman Munoz[1], Farzad Nozarian[1], Igor Vozniak[1], Antonio S. da Silva[2] and Axel Heßler[3]

Abstract—**The white paper focuses on enhancing autonomous driving safety by mitigating Vehicle-to-everything (V2X) communication vulnerabilities to cyberattacks such as spoofing and jamming. It addresses the protection of Vulnerable Road Users (VRUs) by improving detection and situational awareness through V2X technology. Emphasis is placed on domain adaptation for the Beyond 5G Virtual Environment for Cybersecurity Testing of V2X Systems (B5GCyberTestV2X) simulation platform to withstand real-world conditions. Antenna array-based systems are proposed to alleviate the negative impact of jamming and spoofing attacks, specifically in urban scenarios such as intersections. These systems can attenuate jammer signals, amplify legitimate ones, and in the case of spoofing attacks, they enable parameter extraction for spoofer identification. Moreover, semi-supervised and unsupervised learning approaches are discussed for their potential to boost performance and robustness in complex environments. The paper refers to relevant scenarios from the German In-Depth Accident Database (GIDAS), including intersections, lane changes, merging, and pedestrian or cyclist scenarios. The white paper is structured in seven sections: introduction, project and V2X system descriptions, challenges and countermeasures, Driving Use Cases (DUC) based on GIDAS and 3GPP, AI-based mitigation strategies and simulation research, and proposed Key Performance Indicators (KPIs) following the 3GPP report. It contributes to the comprehensive B5GCyberTestV2X project.**

Index Terms—**Vehicle-to-everything (V2X) communication, cooperative perception, spoofing attacks, jamming attacks, driving use cases (DUC), key performance indicators (KPIs)**

I. Preliminaries

B5GCyberTestV2X[4] targets the cybersecurity gap in Beyond 5G (B5G) V2X communication, proposing a virtual, open-source cybersecurity environment for testing and validating V2X algorithms and use cases for autonomous vehicles. It seeks to extend the autonomous vehicles' perception through sensor systems and V2X connectivity, a task unfulfilled by existing solutions such as VEINS [1] and Simu5G [2] due to their inattention to cybersecurity.

Our project's goal is to create the world's first B5G virtual V2X environment prioritizing cybersecurity, laying the foundation for a novel B5G V2X architecture considering communication, processing, and information security. It concentrates on testing cybersecurity solutions at the physical layer, specifically against jamming and spoofing attacks involving intentional electromagnetic interference (IEMI). The creation of B5GCyberTestV2X involves extending the 5G virtual environment, developing a 6G virtual and cybersecurity environment, and proposing mechanisms to counter jamming [3] and spoofing for V2X systems. The project aims to enhance the economic viability of the proposed technical solution, solidify the German automotive industry, and establish a strong market position for the project partners in cybersecurity research related to Trustworthy Artificial Intelligence (AI).

V2X communication is vital for autonomous driving, enhancing safety, efficiency, and the driving experience by enabling vehicles to share information. Autonomous vehicles, that rely on sensor systems, can experience limitations in field-of-view and performance under challenging conditions, potentially causing accidents. To mitigate these issues, V2X connectivity allows vehicles to share sensor data, thus enhancing environmental perception and collective decision-making. B5GCyberTestV2X seeks to fulfill the need for a comprehensive V2X simulation tool, focusing on B5G V2X communication cybersecurity, which is crucial for ensuring the safety and reliability of autonomous driving systems. The subsequent two subsections delve into the German In-Depth Accident Study (GIDAS) scenarios I-A as a reference for the driving use cases selection, and an overview of V2X systems I-B including different network layers' protocols and technical parameters.

A. GIDAS Scenarios

This subsection discusses the development of scenarios based on the GIDAS database to shape the driving use cases for B5GCyberTestV2X. The scenarios, informed by techniques such as domain adaptation, human behavior modeling, and semi-supervised and unsupervised learning aim to address the challenges of V2X communication in autonomous driving.

The GIDAS database provides rich information on real-world accidents and yields valuable insights for practical use cases. Examining these scenarios reveals patterns, interactions, and risk factors, enhancing the relevance and accuracy of the use cases.

The scenarios can be categorized as follows:

1) Intersection Scenarios: Accidents at intersections due to failure to yield, misjudging gaps, or turning across traffic.
2) Lane Change and Merging Scenarios: Accidents from improper lane changes or merging maneuvers.

[1] German Research Center for Artificial Intelligence (DFKI) 67663 Kaiserslautern, Germany

[2] Hamm-Lippstadt University of Applied Sciences (HSHL), 59063 Hamm, Germany

[3] TITUS Research GmbH, 15745 Wildau, Germany

[4]http://b5gcybertestv2x.hshl.de

3) Pedestrian and Cyclist Scenarios: Accidents involving pedestrians or cyclists and motor vehicles, usually caused by inadequate visibility, failure to yield, or misjudging speed and distance.

Given B5GCyberTestV2X's focus on Vulnerable Road Users (VRUs), we emphasize intersection and pedestrian/cyclist scenarios. Intersection scenarios involving VRUs are crucial due to the complex interactions between different road users. Analyzing these scenarios uncovers factors contributing to accidents, such as visibility issues, infrastructure inadequacy, and communication failures.

Pedestrian and cyclist scenarios hold significance as these VRUs are particularly vulnerable. Studying these scenarios helps identify common causes of collisions and explore potential mitigation strategies, including effective V2X communication strategies.

DFKI has successfully developed implementations of relevant GIDAS scenarios in the OpenDS [4] and CARLA [5] simulators, creating thousands of variations to represent real-world situations. These form the basis for further development and testing of the V2X communication system. To maximize the potential of B5GCyberTestV2X, it is imperative to extend these implementations to incorporate V2X communication capabilities, explore accident prevention, assess V2X system security and reliability, and identify potential vulnerabilities and mitigation strategies.

B. V2X Communication Systems

V2X technology is specified differently by various standard organizations, such as IEEE [6], 3GPP [7], and ITS [8]. Table I gives a synopsis of state-of-the-art V2X communication systems, their enabling technologies, corresponding protocols, standards, and dedicated bandwidths. Note that the V2X systems Intelligent Transport Systems (ITS) G5 – Safety EU, Dedicated short-range communication (DSRC) – Safety US and ITS-G5 Release 2 - Car 2 Car Communication Consortium (C2C-CC) do not consider 5G and B5G communication. However, 3GPP schemes do consider 4G Long Term Evolution (LTE) and 5G New Radio (NR). B5GCyberTestV2X's main goal is the further development of 5G NR. Below is a summary of each V2X system in Table I.

- ITS G5 – Safety EU: An EU initiative, demonstrating the effectiveness of ITS G5 in road safety improvement by deploying safety applications such as collision avoidance and VRU protection [9].
- DSRC – Safety US: A U.S. initiative, improving highway safety via DSRC, which enables safety-critical short-distance communication for applications like collision avoidance and emergency vehicle notification [10].
- ITS-G5 Release 2 - C2C-CC: The second ITS communication standard for DSRC technology. It aims to improve road safety and transportation system efficiency through cooperative ITS systems [11].
- LTE-PC5 - Mode 4 3GPP Release 16: A 3GPP-developed specification set enhancing mobile communication system capabilities for vehicular communication [7]. It offers a higher data rate and a more robust communication link than other V2X communication technologies.
- C-V2X LTE-Uu – Mode 3GPP Release 16: Uses existing LTE network infrastructure to offer V2X communication, providing better coverage, reliability, and latency. The 3GPP Release 16 specifications include enhancements for C-V2X LTE-Uu, such as improved security and privacy, and improved interference management [7].
- 5G NR - PC5 3GPP Release 16: Designed to offer faster data rates, lower latency, and greater capacity. It supports direct communication between vehicles and infrastructure without needing a cellular network [7].
- 5G NR C-V2X –Uu 3GPP Release 16: Enables direct communication over cellular networks between vehicles, pedestrians, and infrastructure, offering higher data rates, reliability, and lower latency [7].
- 5G NR C-V2X and Beyond –Uu 3GPP Release 17: An extension of C-V2X technology supporting advanced use cases beyond safety applications, such as ADAS and autonomous driving. This includes enhancements to the network-based communication mode for non-safety-critical applications such as traffic management and infotainment [7].

II. General Applicability

In an era where vehicles are rapidly integrating with V2X communication technologies, the imperative role of cybersecurity cannot be underestimated. Cybersecurity measures span the range of securing data transmission, preserving privacy, and protecting essential systems from malevolent attacks. By deploying solid cybersecurity tactics, potential risks and vulnerabilities can be effectively neutralized, facilitating the seamless adoption of V2X communication technologies in the autonomous driving landscape. This invariably fosters the development of future transport systems that are safe, efficient, and resilient.

This section comprises three subsections. Subsection II-A elaborates on V2X-Spoofing and V2X-Jamming attacks. Subsection II-B outlines countermeasures from the V2X perspective, while Subsection II-C discusses countermeasures from the autonomous driving perspective.

A. V2X-Spoofing and V2X-Jamming in Autonomous Driving

Spoofing and jamming represent significant cyber threats to the V2X channel, posing substantial risks to autonomous vehicles' safety by disrupting their perception systems. Spoofing involves broadcasting fabricated data to the V2X channel, masquerading as a legitimate source [12], while jamming involves deliberate interference with the V2X channel via radio signal transmission on the same frequency [13]. This can result in autonomous vehicles receiving misleading information or failing to receive critical data, potentially causing severe accidents.

B. Mitigation Measures on the V2X-Side

To safeguard against V2X spoofing and jamming attacks, a multi-layered mitigation approach within the Autonomous Driving (AD) architecture is necessary. This strategy includes:

TABLE I
V2X COMMUNICATION SCHEMES

V2X Communications Schemes	Physical Layer	Data Link Layer	Application Layer: Safety Messages	Bandwidth	Frequency Range (Europe)	Types of X2X communication
Intelligent Transport Systems (ITS) G5 – Safety EU	IEEE 802.11p • OFDM • Convolutional code • BPSK • QPSK • 16QAM • 64-QAM	CSMA/CA, MC/DCC, LCC	CAM, DENM	10 MHz or 20 MHz	5.85 GHz to 5.925 GHz	V2N, V2P, V2L, and V2V (short range)
Dedicated short-range communication (DSRC) – Safety US	IEEE 802.11p • OFDM	IEEE 1609.4 • CSMA/CA • MC/DCC • LCC	BSM	75 MHz	5.85 GHz to 5.925 GHz	V2N, V2P, V2L, and V2V (short range)
ITS-G5 Release 2 - Car 2 Car Communication Consortium (C2C-CC)	IEEE 802.11bd • BPSK-DCM • BPSK • QPSK • (16, 64 or 256)-QAM	MCO	CAM	Interoperable 10 MHz or 20 MHz	5.9 GHz and 60 GHz	V2V
LTE-PC5 - Mode 4 3GPP Release 16	• SC-FDMA • FDD • TDD • Convolutional code	PDCP, RLC, MAC, PHY	BSM, CAM, DENM	up to 20 MHz	up to 6 GHz	V2I, V2V, and V2P (PC5 interface)
Cellular vehicle-to-everything (C-V2X) LTE-Uu – Mode 3GPP Release 16	• SC-FDMA	PDCP, RLC, MAC, PHY	BSM, CAM, DENM	10 MHz or 20 MHz	5.85 GHz to 5.925 GHz	V2N, V2P, V2L, and V2V (short range)
5G New Radio (NR) - PC5 3GPP Release 16	• CP-OFDM • QPSK • (16 or 64)QAM	PDCP, RLC, MAC, PHY	BSM, CAM, DENM	10 MHz or 20 MHz	5.85 GHZ to 5.925 GHZ	V2N, V2P, V2L, and V2V (short range)
5G New Radio (NR) C-V2X –Uu 3GPP Release 16	• CP-OFDM • QPSK	PDCP, RLC, MAC, PHY	BSM, CAM, DENM	10 MHz or 20 MHz	5.85 GHZ to 5.925 GHZ	V2N, V2P, V2L, and V2V (short range)
5G New Radio (NR) C-V2X and Beyond –Uu 3GPP Release 17	• CP-OFDM	PDCP, RLC, MAC, PHY	BSM, CAM, DENM	10 MHz or 20 MHz	5.85 GHZ to 5.925 GHZ	V2N, V2P, V2L, and V2V (short range)

- Use of antenna array-based systems for beamforming.
- Dynamic parameter estimation via antenna array-based systems.
- Adaptive channel coding to compensate for jamming interference.
- Leveraging millimeter wave and Terahertz spectrum for communication in an interference environment.
- Use of secure communication protocols.
- Implementation of robust authentication mechanisms.
- Multi-factor authentication.
- Data integrity and validation mechanisms.
- Use of multiple communication channels.
- Spectrum sharing and frequency hopping.
- Machine learning and AI-based anomaly detection.

C. Mitigation Measures in the Autonomous Driving (AD)-Side

Mitigation strategies for autonomous driving systems focus on enhancing system reliability, security, and robustness. The strategies include:

- Data Augmentation, Diverse Training, and Generative Techniques.
- Multi-Sensor Fusion.
- Robustness against Adversarial Attacks.
- AI Model Validation and Verification.
- AI Explainability and Transparency.
- Human-in-the-Loop interaction.

To conclude, successfully implementing mitigation measures requires careful attention to information exchange via V2X communication and computational responsibilities' allocation. There are two potential scenarios: a centralized solution leveraging 6G networks for data transmission and processing, and a decentralized solution where each autonomous vehicle independently processes data and shares it via the V2X channel. Each approach presents unique opportunities and challenges related to network capacity, latency, security, resource optimization, system resilience, and cooperative decision-making.

III. V2X Application Scenarios Pertaining to Vulnerable Road Users

This research emphasizes securing vulnerable road users (VRUs), such as pedestrians, cyclists, and motorcyclists, who often bear high traffic risks. We explore specific use cases aimed at enhancing VRU safety through V2X communication, a pivotal element in autonomous driving for VRU safety.

V2X technology facilitates real-time information exchange between autonomous vehicles and surrounding infrastructure, other vehicles, and VRUs, consequently enhancing safety through improved situational awareness. V2X benefits concerning VRUs entail:

1) **Enhanced Detection:** V2X ensures the accurate and prompt detection of VRUs, outperforming traditional onboard sensors in conditions like blind corners, obstructed views, or poor lighting.
2) **Augmented Situational Awareness:** Information exchange with infrastructure, other vehicles, and VRUs (via smartphones or wearables), enables a holistic understanding of the environment, aiding effective hazard response.
3) **Proactive Safety Measures:** Advanced VRU warnings enable autonomous vehicles to adjust driving behavior and prevent accidents.
4) **Collaborative Collision Avoidance:** V2X facilitates cooperative collision prevention, where vehicles and VRUs share relevant information.

However, jamming and spoofing threats pose significant risks to VRU safety by compromising V2X communication integrity. Jamming disrupts communication, reducing autonomous vehicles' situational awareness, and increasing VRU collision risks. Spoofing introduces false information, leading to erroneous decisions and potentially aggressive vehicle maneuvers, thereby endangering VRUs.

Three use cases based on the 3GPP report [7] emphasize these risks and countermeasures:

A. Scenario 1: Do not pass warning

Adapted use case 1a (Figure 1) shows a collision due to jammer drone interference with vehicle communication. This underscores the need for a resilient communication framework and failsafe mechanisms against interference [7].

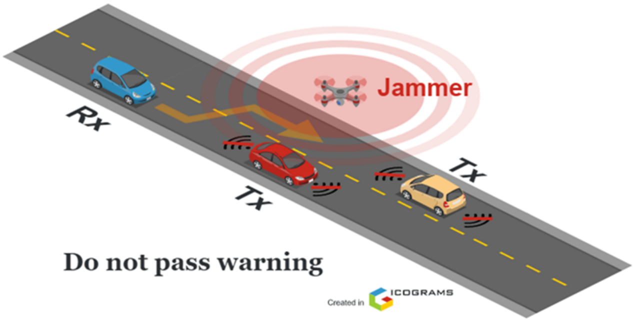

Fig. 1. Do not pass warning in the presence of a jammer.

Adapted use case 1b (Figure 2) depicts a collision resulting from a spoofer drone sending false information masquerading as a Road Side Unit (RSU). This highlights V2X communication systems' vulnerability to spoofing attacks and emphasizes a secure framework for preventing false information injection.

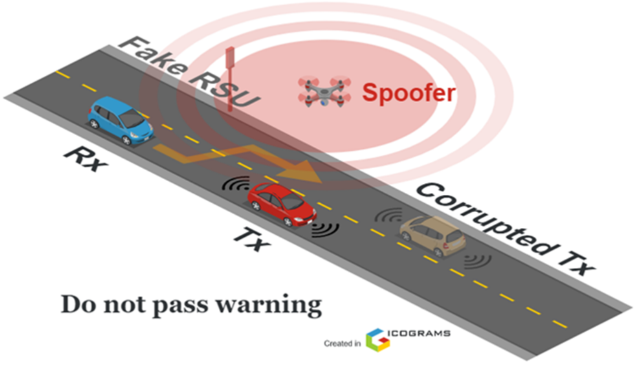

Fig. 2. Do not pass warning in the presence of a spoofer.

Adapted use case 1c (Figure 3) demonstrates beamforming technology's potential to prevent collisions under jammer drone interference. The beamforming technology filters out the drone's signal, focusing on line-of-sight (LOS) signals from transmitting (Tx) vehicles, improving the signal-to-noise ratio and reducing interference.

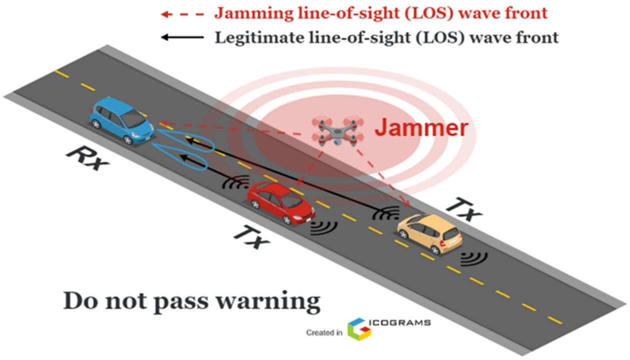
Jamming line-of-sight (LOS) wave front
Legitimate line-of-sight (LOS) wave front
Jammer
Rx
Tx
Tx
Do not pass warning
Created in ICOGRAMS

Fig. 3. Do not pass warning using beamforming to mitigate the jammer interference.

Adapted use case 1d (Figure 4) employs beamforming technology with a Reconfigurable Intelligent Surface (RIS) [14] to prevent a collision under jammer drone interference. The RIS, a smart surface controlled to dynamically adapt to different environmental conditions, helps improve signal quality and reduce interference by focusing the signal on receiving (Rx) vehicles.

Adapted use case 1e (Figure 5) uses Direction of Arrival (DoA) [15] estimation to prevent a collision when a spoofer drone sends false information. If the DoA estimation and the verification do not match with the information from the spoofer drone, the vehicle ignores the fake information and takes appropriate action to prevent a collision, thereby enhancing V2X communication's safety and effectiveness.

B. Scenario 2: Alert for Vulnerable Road Users at Blind Intersections

Figure 6 (Driving Use Case 2a) depicts a scenario where jammer drone interference compromises the communication

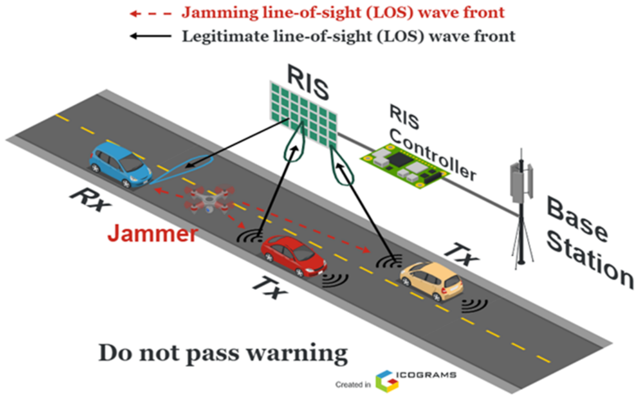
Jamming line-of-sight (LOS) wave front
Legitimate line-of-sight (LOS) wave front
RIS
RIS Controller
Base Station
Rx
Jammer
Tx
Tx
Do not pass warning
Created in ICOGRAMS

Fig. 4. Do not pass warning using beamforming relay with an RIS to mitigate the jammer interference.

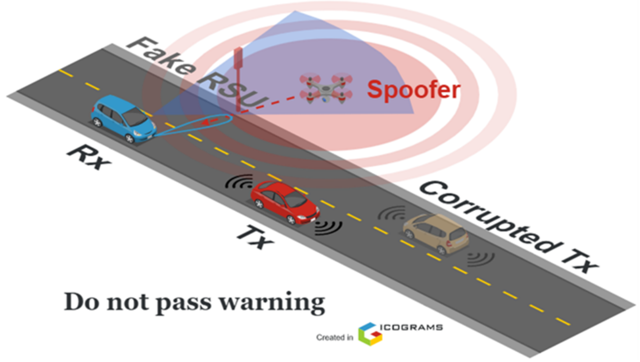

Fig. 5. Do not pass warning using the direction of arrival estimation via antenna arrays and drone detection via cameras to identify a spoofer.

between a vehicle, pedestrian, and cyclist at a blind intersection, causing a collision. Here, the vital safety information is lost due to drone jamming, leading to the vehicle-driver striking the pedestrian and cyclist. This scenario underscores the necessity of robust V2X communication for safeguarding vulnerable road users and its susceptibility to external interference.

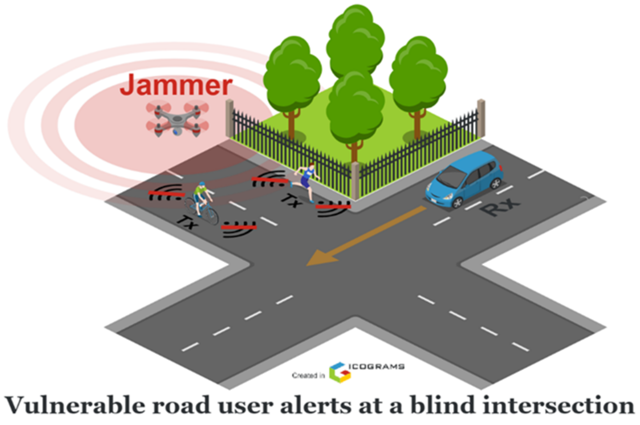

Fig. 6. Vulnerable Road Users Alert at Blind Intersection in the presence of a jammer.

Figure 7 (Driving Use Case 2b) presents a situation wherein a spoofer drone, masquerading as a faux Road Side Unit (RSU), manipulates the communication, leading to a collision. The erroneous information from the spoofer results in an inability of the vehicle to perceive the real situation, underscoring the vulnerability of V2X systems to spoofing attacks and the need for secure communication frameworks.

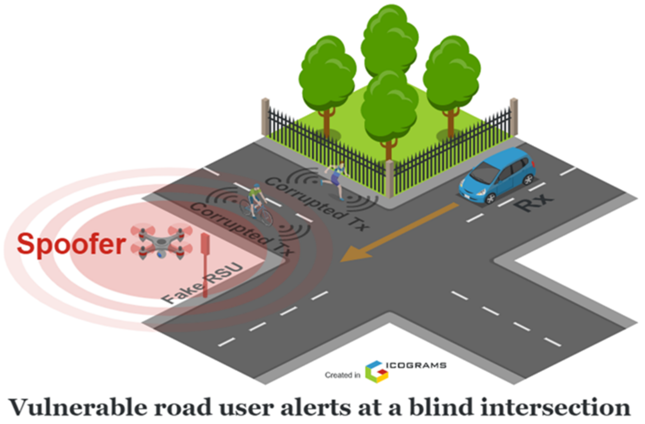

Fig. 7. Vulnerable Road Users Alert at Blind Intersection in the presence of a spoofer.

Figure 8 (Driving Use Case 2c) describes a jammer drone disrupting communication. However, beamforming technology in the Rx vehicle filters non-line-of-sight (NLOS) signals, facilitating the vehicle to avoid collisions and navigate safely, highlighting the potential of beamforming in enhancing V2X communication reliability [16].

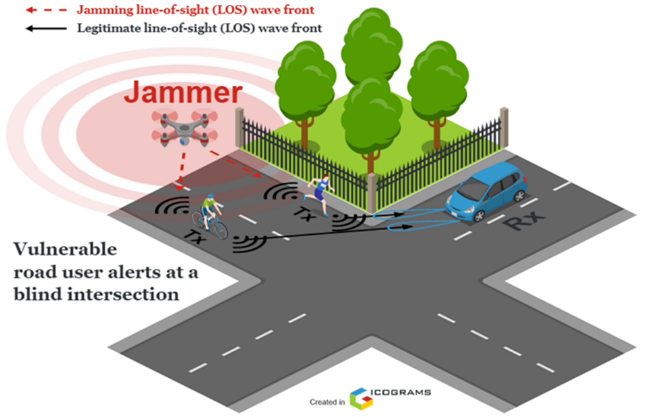
Jamming line-of-sight (LOS) wave front
Legitimate line-of-sight (LOS) wave front
Jammer
Tx
Tx
Rx
Vulnerable road user alerts at a blind intersection
Created in ICOGRAMS

Fig. 8. Vulnerable Road Users Alert at Blind Intersection using beamforming to mitigate the jammer interference.

Figure 9 (Driving Use Case 2d) presents a similar jammer drone scenario. However, the beamforming technology is ineffective due to the drone being on the line-of-sight (LOS) path. To circumvent this, a Reconfigurable Intelligent Surface (RIS) in the Rx vehicle, used as a relay with beamforming, redirects the signal path, ensuring the necessary information is received, demonstrating the utility of beamforming and RIS to improve V2X communication reliability.

Figure 10 (Driving Use Case 2e) depicts a spoofer drone posing as an infrastructure component. However, the Rx vehicle, equipped with an antenna array, estimates the Direction of Arrival (DoA) [15] from the drone and can thus ignore

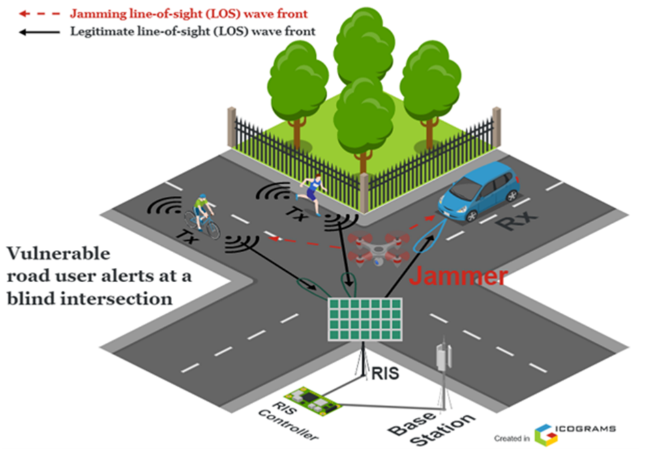
Jamming line-of-sight (LOS) wave front
Legitimate line-of-sight (LOS) wave front
Vulnerable road user alerts at a blind intersection
Tx
Tx
Rx
Jammer
RIS
RIS Controller
Base Station
Created in ICOGRAMS

Fig. 9. Vulnerable Road Users Alert at Blind Intersection using beamforming relay with a RIS to mitigate the jammer interference.

the misleading information, avoiding a collision. This scenario emphasizes the effectiveness of DoA estimation in combating spoofing attacks in V2X communication systems.

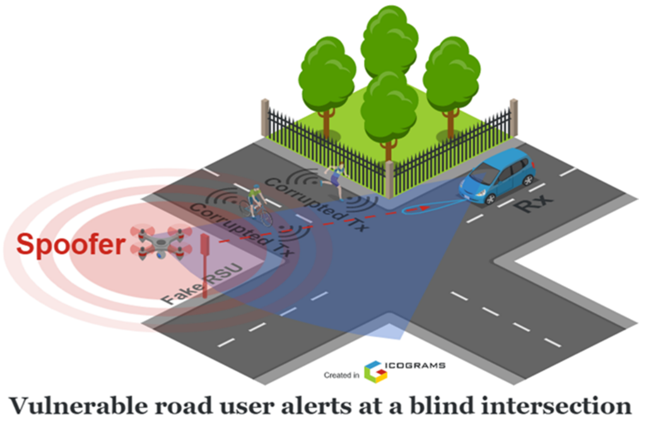

Fig. 10. Vulnerable Road Users Alert at Blind Intersection using direction of arrival estimation via antenna arrays and drone detection via cameras to identify a spoofer.

C. Scenario 3: Assisting Left Turns

Figure 11 (Driving Use Case 3a) showcases a jammer drone disrupting inter-vehicle communication during a left turn, resulting in a collision. This incident signifies the importance of resilient V2X communication in providing real-time, accurate vehicular information, especially during complex maneuvers such as left turns.

Figure 12 (Driving Use Case 3b) demonstrates a spoofer drone posing as an RSU and manipulating communication, leading to a collision at the crossover. The inability of the Rx vehicle to receive precise information accentuates the need for a secure communication framework that can safeguard against spoofing attacks in V2X systems.

Figure 13 (Driving Use Case 3c) involves a jammer drone interfering with inter-vehicle communication. However, the Rx vehicle, equipped with beamforming technology, successfully filters the LOS signals, avoiding a collision. This scenario underlines the potential of advanced signal processing techniques, such as beamforming, in enhancing the safety and efficacy of V2X communication in real-world scenarios.

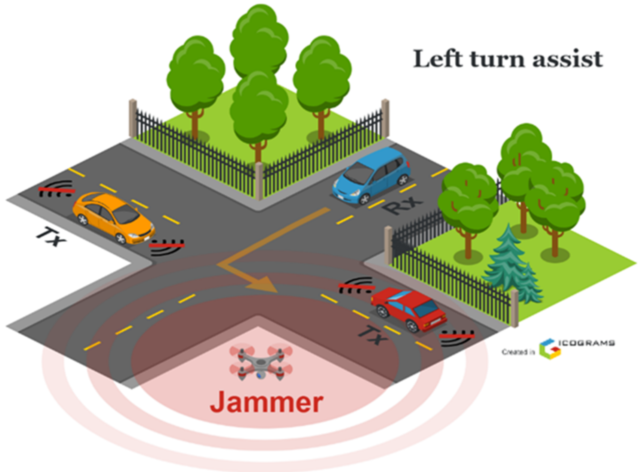

Fig. 11. Left Turn Assist in the presence of a jammer.

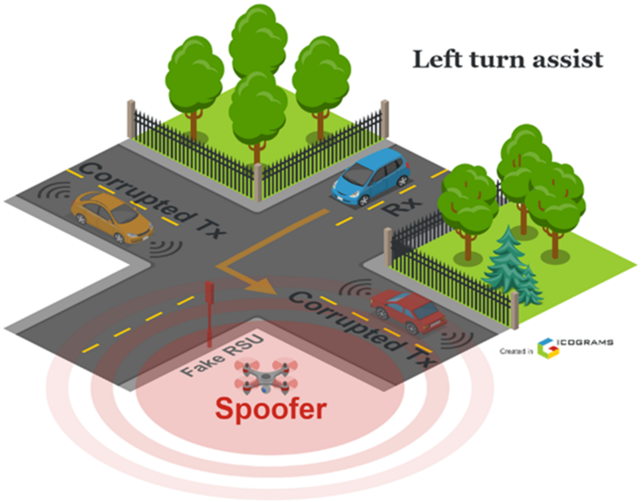

Fig. 12. Left Turn Assist in the presence of a spoofer.

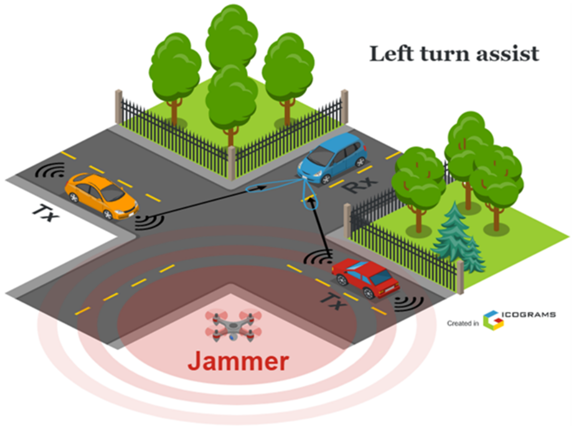

Fig. 13. Left Turn Assist using beamforming to mitigate the jammer interference.

IV. Additional Considerations and Implications

A. Use-Case Data Requirements and Network Limitations

Various V2X use cases, such as Coordinated Maneuver, Cooperative Perception, and Video Data Sharing for Assisted and Improved Automated Driving (VaD), necessitate high data transfer rates, low latency, and exceptional reliability. For instance, Coordinated Maneuver mandates a data rate per vehicle exceeding 15 Mbps, latency below 5-100 ms, and reliability exceeding 99.999% [7], [17], [18].

Similarly, Cooperative Perception involves sharing high-resolution perception data among vehicles, necessitating data rate per link exceeding 700 Mbps and latency less than 5 ms [19]. VaD, however, highlights the limitation of the existing LTE PC5 standard in supporting a stream of raw RGB video of 1280x720 resolution at 30 Hz, exceeding 700 Mbps [20], [21].

B. Transmission of Raw Data and Cybersecurity Implications

The emerging area of virtual sensors—converting existing sensor data into novel insights—promises potential cost and complexity reduction. However, transmitting raw data, particularly LIDAR point cloud data, poses significant cybersecurity challenges [22].

Spoofing and jamming attacks may compromise virtual sensor data integrity, causing inaccurate environmental perception and potentially hazardous situations. Furthermore, malicious actors could exploit the open architecture of virtual sensor systems to insert malicious code, compromising vehicle security and privacy.

Robust and reliable cybersecurity mechanisms are therefore crucial. Potential measures include secure and reliable transmission protocols, advanced algorithms for detecting and mitigating cyber threats, rigorous testing, and validation procedures.

Interestingly, LIDAR point cloud data, due to its natural coherence, provides a significant opportunity for AI-based mitigation measures, particularly in distribution-based detection of manipulation.

V. Enhanced AI-Based Mitigations and Bridging the Simulation Gap

A. Domain Adaptation and Its Implication on b5GCyberTestV2X

To tackle the simulation gap in our B5GCyberTestV2X project—disparity between virtual and real-world scenarios—we propose incorporating domain adaptation techniques. This approach will ensure models generalize well across diverse situations, creating a more accurate representation of real-world conditions, particularly in VRU use cases.

B. Simulated Data for VRU Use-Cases

We will leverage simulation data to better understand the behavior of VRUs in the context of spoofing and jamming research. A comprehensive understanding of human behavior is fundamental to ensuring the robustness and safety of V2X communication systems.

C. Learning Approaches for Robust Autonomous Systems

Addressing limited data availability in the target domain necessitates semi-supervised and unsupervised learning techniques. By exploiting weak or noisy labels and inherent data structure, these approaches can extract valuable insights and improve model performance. This strategy will enable efficient utilization of limited target domain data, enhancing the generalizability of developed models and further bridging the simulation gap. This holistic approach strives to provide a solid foundation for secure and reliable V2X communication systems within the autonomous driving landscape.

D. Domain Adaptation

The *B5GCyberTestV2X* simulation platform should exhibit robust adaptability, given the fast-paced advancements in connected and autonomous vehicles. Domain Adaptation aids in this by transferring knowledge from one data-rich domain to a limited-data domain, ensuring model performance across diverse environments, hence escalating the platform's resilience.

Several factors necessitate the incorporation of domain adaptation: Safety, to minimize risks for all road users; Robustness and generalization, ensuring the algorithms perform under diverse real-world conditions; and Sensor and perception discrepancies, to account for deviations in simulated and actual sensor outputs.

Domain Adaptation is also related to mitigating jamming and spoofing problems. It aids in the development of robust detection and mitigation techniques, realistic simulation of attacks, and adaptability to emerging threats.

E. Simulation Data for VRU Behavior, Spoofing and Jamming

Understanding pedestrian walking trajectories at urban intersections is crucial for VRU protection and mitigation of spoofing and jamming. Pedestrian trajectory data enhances safety, aids in developing robust algorithms, and contributes to the development of effective countermeasures against attacks.

F. Semi-supervised and Unsupervised Learning

Incorporating semi-supervised and unsupervised learning techniques can significantly improve autonomous driving systems' performance in complex urban environments and against jamming and spoofing attacks.

Semi-supervised learning, working with limited or noisy annotations, allows model adaptation to real-world conditions, including diverse VRU behaviors. It also aids in the development of algorithms to detect and mitigate the impacts of jamming and spoofing attacks, even in ambiguous information scenarios.

Unsupervised learning, training models without labeled data, allows for pattern and structure learning from the data itself, beneficial in domain adaptation and understanding pedestrian trajectories. Its applications include feature learning, to understand pedestrian behavior and movement patterns, and anomaly detection, to identify unusual patterns indicating potential jamming or spoofing attacks. This contributes to the system's resilience against such threats.

VI. Key Performance Indicators (KPIs)

This section outlines some critical performance metrics for this project. We will review KPIs from two 3GPP TR 22.886 [7] scenarios related to the selected driving use cases: Intersection safety information provisioning for urban driving and Collective perception of the environment.

A. Intersection Safety Information Provisioning for Urban Driving

According to the 3GPP TR 22.886, the Local Dynamic Map (LDM) messages contain HD map, traffic signal information, and moving status and location information for pedestrians and vehicles. LDM messages typically range from 400 to 500 bytes.

In a scenario with 200 vehicles and 50 LDM/s, each LDM with 500 bytes, the minimum data rate is 38 Mbps. Given a packet transmission efficiency from 60 % to 80 %, the 3GPP adopts a data rate of 50 Mbps.

In jamming driving use cases, packet loss is significant, leading to a packet transmission efficiency from 0 % to 20 %. Therefore, the first KPI is achieving a packet transmission efficiency above 60 %. Given 50 LDM per second, the beamforming tracking adjustment must occur within 20 ms.

For spoofing driving use cases, false scenario information is transmitted by the spoofer. Therefore, DOA estimation and object detection of the spoofer must be done within 20 ms to identify the spoofer without causing accidents.

B. Collective Perception of Environment (CPE)

In the CPE scenario, an overtaking maneuver is considered where vehicle C receives information from Truck B and issues a warning. As per 3GPP, the KPIs defined for this scenario are:

- 3 ms end-to-end latency and 99.999 % reliability within 200 m communication range
- 10 ms end-to-end latency and 99.99 % reliability within 500 m communication range
- 50 ms end-to-end latency and 99 % reliability within 1000 m communication range
- Peak data rate of 1 Gbps for a single UE for a short period in range of 50 m, in case of an imminent collision

In jamming driving use cases, the data rate and reliability are reduced, and latency increases. Strategies involving beamforming, RIS, mmWaves [22], adaptive coding, and communication must be adopted to guarantee a 99.999 % reliability with 3 ms end-to-end latency and data rate of 50 Mb/s for pre-processed data or 1 Gb/s for raw data.

For spoofing driving use cases, the spoofer can tamper with the raw data, removing or adding non-existent objects or obstacles. Thus, we need to develop algorithms to detect tampered information and AI strategies for consensus to verify shared information consistency. The processing time should ideally be 3 ms.

Acknowledgment

This study was financed by the Bundesamt für Sicherheit in der Informationstechnik (BSI) through the project Beyond 5G Virtuelle Umgebung für Cybersicherheitstests von V2X-Systemen (B5GCyberTestV2X).

References

[1] C. Sommer, R. German, and F. Dressler, “Bidirectionally coupled network and road traffic simulation for improved ivc analysis,” *IEEE Transactions on mobile computing*, vol. 10, no. 1, pp. 3–15, 2010.

[2] 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.

[3] A. S. da Silva, J. P. J. da Costa, G. A. Santos, Z. Miri, M. I. B. M. Fauzi, A. Vinel, E. P. de Freitas, and K. Kastell, “Radio jamming in vehicle-to-everything communication systems: Threats and countermeasures,” in *nternational Conference on Transparent Optical Networks (ICTON)*. Budapest University of Technology and Economics, 2023.

[4] R. Math, A. Mahr, M. M. Moniri, and C. Müller, “Opends: A new open-source driving simulator for research,” *GMM-Fachbericht-AmE 2013*, vol. 2, 2013.

[5] A. Dosovitskiy, G. Ros, F. Codevilla, A. Lopez, and V. Koltun, “CARLA: An open urban driving simulator,” in *Proceedings of the 1st Annual Conference on Robot Learning*, 2017, pp. 1–16.

[6] IEEE, “IEEE website,” https://www.ieee.org, accessed: January 01, 2023.

[7] 3rd Generation Partnership Project (3GPP), “3GPP,” https://www.3gpp.org, 2023, accessed: January 01, 2023.

[8] CEN/TC 278, “ITS standardization,” https://www.itsstandards.eu, 2023, accessed: May 10, 2023.

[9] A. Festag, “Cooperative intelligent transport systems standards in europe,” *IEEE communications magazine*, vol. 52, no. 12, pp. 166–172, 2014.

[10] J. B. Kenney, “Dedicated short-range communications (dsrc) standards in the united states,” *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162–1182, 2011.

[11] CAR 2 CAR Communication Consortium, “CAR 2 CAR Communication Consortium,” https://www.car-2-car.org, 2023, accessed: May 10, 2023.

[12] T. Limbasiya, K. Z. Teng, S. Chattopadhyay, and J. Zhou, “A systematic survey of attack detection and prevention in connected and autonomous vehicles,” *Vehicular Communications*, p. 100515, 2022.

[13] H. Pirayesh and H. Zeng, “Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey,” *IEEE communications surveys & tutorials*, vol. 24, no. 2, pp. 767–809, 2022.

[14] M. A. ElMossallamy, H. Zhang, L. Song, K. G. Seddik, Z. Han, and G. Y. Li, “Reconfigurable intelligent surfaces for wireless communications: Principles, challenges, and opportunities,” *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 3, pp. 990–1002, 2020.

[15] E. Holzman, “Introduction to direction-of-arrival estimation (chen, z.; 2010)[reviews and abstracts],” *IEEE Antennas and Propagation Magazine*, vol. 53, no. 1, pp. 110–111, 2011.

[16] W. Liu and S. Weiss, *Wideband beamforming: concepts and techniques*. John Wiley & Sons, 2010.

[17] A. Correa, R. Alms, J. Gozalvez, M. Sepulcre, M. Rondinone, R. Blokpoel, L. Lücken, and G. Thandavarayan, “Infrastructure support for cooperative maneuvers in connected and automated driving,” in *2019 IEEE Intelligent Vehicles Symposium (IV)*. IEEE, 2019, pp. 20–25.

[18] B. Lehmann, H.-J. Günther, and L. Wolf, “A generic approach towards maneuver coordination for automated vehicles,” in *2018 21st International Conference on Intelligent Transportation Systems (ITSC)*. IEEE, 2018, pp. 3333–3339.

[19] A. Caillot, S. Ouerghi, P. Vasseur, R. Boutteau, and Y. Dupuis, “Survey on cooperative perception in an automotive context,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 9, pp. 14 204–14 223, 2022.

[20] M. Mueck and I. Karls, *Networking vehicles to everything: Evolving automotive solutions*. Walter de Gruyter GmbH & Co KG, 2018.

[21] G. Kovács and L. Bokor, “Towards realistic simulation of mec-based collective perception: an initial edge service design for the artery/simu5g framework,” in *1st Workshop on Intelligent Infocommunication Networks, Systems and Services (WI2NS2)*. Budapest University of Technology and Economics, 2023, pp. 53–58.

[22] A. V. Lopez, A. Chervyakov, G. Chance, S. Verma, and Y. Tang, “Opportunities and challenges of mmwave nr,” *IEEE Wireless Communications*, vol. 26, no. 2, pp. 4–6, 2019.