Modeling and Mitigating Physical-Layer Jamming in Connected Vehicular Networks

1st Kumoulica Allu
Dept. Information Science Technology
Univ. of Houston
Houston, TX
Email: Kallu@cougarnet.uh.edu

2nd Yunpeng Zhang
Dept. Information Science Technology
Univ. of Houston
Houston, TX
Email: yzhan226@Central.uh.edu

3rd Changqing Luo
Dept. Information Science Technology
Univ. of Houston
Houston, TX
Email: cluo3@central.uh.edu

4th Renjie Hu
Dept. Information Science Technology
Univ. of Houston
Houston, TX
Email: rhu7@central.uh.edu

***Abstract*—Connected vehicles rely on vehicle-to-everything (V2X) communication to support safety-critical and cooperative driving applications. The open nature of wireless channels makes these systems vulnerable to physical-layer jamming attacks, which can disrupt message exchange and potentially compromise traffic safety. In this paper, we present an integrated cyber–physical simulation framework that models jamming attacks in connected vehicular networks using OMNeT++, SUMO, and Veins. We emulate realistic barrage-style jamming through protocol-compliant interference at the IEEE 802.11p physical layer and evaluate its impact on key communication metrics, including packet delivery ratio, latency, and channel utilization. We further implement frequency hopping as a mitigation strategy and assess its effectiveness under sustained interference. Our results show that jamming significantly degrades communication reliability and that mitigation mechanisms can partially restore network performance. These findings highlight the importance of resilient communication design in future intelligent transportation systems.**

***Index Terms*—Vehicular Communication, Jamming Attack, Sumo, Veins, OMNET++.**

I. Introduction

The emergence of Connected and Automated Vehicles (CAVs) has paved the way for intelligent transportation systems (ITS) that promise enhanced safety, mobility, and environmental sustainability. Through Vehicle-to-Everything (V2X) communication—comprising – which includes vehicle-to-vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Vehicle-to-Network (V2N) links—vehicles can exchange critical safety information such as position, velocity, and intent. Technologies such as Dedicated Short Range Communication (DSRC) and Cellular V2X (C-V2X) form the backbone of this connectivity. However, the reliance on open and shared wireless channels makes vehicular networks inherently vulnerable to jamming attacks, a form of Denial-of-Service (DoS) at the physical layer that can severely degrade communication reliability and, consequently, road safety.

A jamming attack occurs when an adversary intentionally emits interfering signals to disrupt legitimate communications. Even short bursts of interference can lead to packet loss, increased latency, and communication blackouts, which, in turn, destabilize cooperative driving functions such as platooning, adaptive cruise control, and intersection coordination. Recent studies have shown that the effects of jamming can propagate from the communication layer to the transportation layer, resulting in traffic congestion, emergency braking, and multi-vehicle collisions. The highly dynamic nature of vehicular environments—characterized by rapid topological changes, mobility, and variable propagation conditions—further complicates the detection and mitigation of such attacks.

To ensure safe and dependable operation, resilience against jamming must be a core design principle in connected vehicle systems. Resilient communication involves the ability to withstand and recover from intentional interference while maintaining essential message exchanges. Approaches such as frequency hopping, beamforming, redundant message dissemination, and machine learning–based anomaly detection have been explored to enhance robustness. However, evaluating their real-world performance requires comprehensive simulation frameworks that can model both the vehicular dynamics and the wireless communication impairments introduced by attackers.

This paper presents a simulation framework for analyzing resilient vehicular communication under jamming attacks. Using co-simulation tools such as OMNeT++, SUMO, and Veins, the framework enables the study of how different jamming strategies—barrage, reactive, deceptive—impact network performance and traffic flow. It also supports the evaluation of mitigation techniques, allowing researchers to test resilience strategies before real-world deployment.The goal of this study is to understand how communication attacks affect real-world traffic safety and to use this understanding to build more secure connected vehicle systems.

II. Related Work

Connected and automated vehicles (CAVs) heavily rely on wireless communication to support safety–critical applications, making them vulnerable to cyberattacks such as Distributed Denial of Service (DDoS), jamming, and message falsification. Accordingly, significant research has examined how cyber threats degrade communication reliability, traffic stability, and vehicular control.

Early studies on DDoS attacks in vehicular networks primarily focused on Internet-type traffic, such as UDP flooding, without considering safety-critical V2X messages. For example, Wehby et al. evaluated DDoS attacks using Cooperative Awareness Messages (CAMs) and demonstrated that high-rate CAM flooding can silently degrade cooperative services, increase channel load, and cause significant message denial even when vehicles remain operational[7]. Their work highlighted that DDoS attacks targeting CAMs—core safety messages—pose substantially higher risks than those using infotainment-based traffic.

In the domain of jamming attacks, Silva et al. examined radio-frequency interference in DSRC-based V2X systems and presented driving scenarios where jamming disrupts Basic Safety Messages (BSMs), leading to critical hazards at intersections and during overtaking maneuvers[2]. They further evaluated countermeasures using antenna-array beamforming, showing that techniques such as Capon beamforming significantly improve Signal-to-Interference-plus-Noise Ratio (SINR) under jamming. Similarly, Mokdad et al. proposed DJAVAN, a jamming-attack detection mechanism for VANETs that leverages Packet Delivery Ratio (PDR) thresholds to differentiate between natural packet loss and malicious interference[3].

Beyond communication-layer attacks, several works explored cyber-physical impacts on vehicle dynamics and traffic flow. Silwal et al. analyzed cyberattacks such as false information injection, acceleration manipulation, and platoon-leader identity attacks using a connected car-following model. Their results showed that compromised communication can trigger traffic instability, collisions, and reduced road capacity[4]. Khattak, Masoud, and others (as summarized therein) similarly demonstrated that disturbances propagate rapidly through CAV platoons, degrading stability in multi-vehicle formations.

To enhance resilience against DoS conditions, Biron et al. developed a control-oriented mitigation strategy for Cooperative Adaptive Cruise Control (CACC), modeling DoS as stochastic communication delay. Their method integrated Luenberger observers and delay estimators to maintain platoon spacing even during heavy packet losses or delayed inter-vehicle updates[5].

In-vehicle networks (IVNs) represent another vulnerable subsystem. A comprehensive survey by Rathore et al. detailed a wide range of cyberattack vectors, including infotainment interfaces, telematics units, sensors, USB ports, and especially the Controller Area Network (CAN), which lacks authentication and encryption by design. The study reviewed machine-learning-based intrusion detection systems (IDS), cryptographic solutions, and multi-layer defense architectures for securing internal automotive networks[6].

Overall, existing studies consistently highlight that wireless communication forms the primary attack surface for connected vehicles, and that both DDoS and jamming attacks can severely impair safety-critical operations. However, most prior efforts either focus on communication-level metrics (e.g., packet loss, latency) or examine internal IVN vulnerabilities separately. There remains a need for integrated frameworks that jointly evaluate communication-layer disruptions, vehicular control responses, and real-time traffic impacts—an area to which the present work contributes.

Existing DoS and jamming studies mostly stop at packet loss analysis, whereas our work connects realistic jamming behavior to its cyber–physical impact using an integrated traffic and communication simulation.

III. System Architecture

Our framework brings together vehicle mobility, wireless message exchange, and simulated attack mechanisms into a single co-simulation platform to study their combined effects.

A. SUMO Mobility and Traffic Control Layer

The mobility environment is constructed in SUMO using a grid-like road network consisting of four interconnected road segments and two signalized intersections. Each road segment supports bi-directional traffic, while traffic lights manage vehicle movement through the junctions. SUMO provides microscopic control of vehicle dynamics, including car-following, lane-changing, acceleration, and braking. The helloworld.sumocfg configuration manages vehicle routes, traffic light logic, and simulation parameters. Vehicles enter the network from different directions, traverse the intersections, and interact with signal phases in real time. Through TraCI, SUMO continuously streams vehicle positions, speeds, and traffic light states to the communication stack.

B. OMNeT++ Communication Layer

OMNeT++ serves as the discrete-event simulator where network behavior is modeled. Each SUMO vehicle is represented as a wireless node (e.g., node[0]...node[n]), equipped with modules for IEEE 802.11p/WAVE communication. OMNeT++ handles packet transmission, medium access, and PHY/MAC interactions. Key communication parameters—such as frequency, transmission power, interference, and data rate—are fully configurable, enabling accurate modeling of jamming conditions. Traffic light controllers are also instantiated within OMNeT++ to mirror SUMO's signal logic, ensuring synchronized behavior across simulators.

C. Veins Co-Simulation Integration

The Veins framework provides real-time synchronization between SUMO and OMNeT++ using the TraCI protocol. The manager module in OMNeT++ initializes TraCI and coordinates bidirectional data exchange. Vehicle mobility

events—such as speed updates, stopping at red signals, or passing through intersections—are transmitted to OMNeT++ each simulation step. Conversely, communication outcomes, including packet loss or interference caused by jamming, immediately influence the behavior of connected vehicles. This tight coupling ensures that mobility reacts to communication impairments without delay, allowing realistic experimentation with jamming attacks.

D. Attack Modeling Layer

A custom jammer module is integrated into the OMNeT++ physical layer to manipulate key IEEE 802.11p parameters during simulation. By altering noise levels, received signal power, or interference values, the system can emulate barrage jamming, deceptive jamming, and signal attenuation at the PHY layer. These attacks directly degrade V2V/V2I message reception, affecting cooperative behavior at intersections—especially during signal changes or congestion. The architecture supports configurable attack start times, durations, and target vehicles, allowing controlled and repeatable experiments.

E. Jamming Attack Modeling

A custom jammer module modifies IEEE 802.11p PHY-layer parameters to emulate realistic adversarial interference. Barrage jamming is configured by injecting continuous high-power noise into the channel, raising the noise floor and reducing the signal-to-noise ratio (SNR). Destructive interference is simulated by applying a destructiveness factor D $\in$ [0,1], which attenuates the received signal power of legitimate frames. These manipulations directly influence packet decoding performance, leading to corrupted safety messages, increased latency, and reduced packet delivery ratio (PDR). The framework supports configurable attack start times, durations, jammer mobility, and target vehicles.

F. Frequency Hopping Scheme

To enhance resilience against physical-layer interference, we implement a mitigation strategy: Frequency Hopping Spread Spectrum (FHSS). FHSS dynamically shifts vehicle communication among multiple frequency channels using a pseudo-random hopping sequence. Each vehicle switches channels every 200 ms across a pool of three IEEE 802.11p frequency bands. By distributing transmissions across multiple channels, the likelihood of sustained jammer overlap is significantly reduced. While minor synchronization overhead is introduced, FHSS effectively disrupts continuous and pulsed interference patterns.

IV. Methodology

The simulation methodology encompasses the configuration of mobility, communication, jamming, and mitigation modules within the co-simulation environment.

A. Simulation Environment Setup

The experiments utilize OMNeT++ 6.2.0, SUMO 1.19.0, and Veins 5.3.1 running under Python 3.11. Compatibility constraints between Veins 5.3.1 and newer SUMO releases (e.g., 1.24.0) were identified, caused by changes to the TraCI message format, which resulted in connection mismatches during initialization. These factors motivated the use of SUMO 1.19.0 to maintain stable TraCI coupling.

B. Baseline Scenario Configuration

A single-intersection road network is created in SUMO with 15 vehicles following predefined trajectories. Traffic light logic, acceleration behavior, and car-following models are included to ensure realistic mobility dynamics. OMNeT++ nodes corresponding to each vehicle transmit Cooperative Awareness Messages (CAMs)/Basic Safety Messages (BSMs) at fixed intervals using IEEE 802.11p.

C. Attack Scenario Configuration

To evaluate the resilience of vehicular communication, we implement physical-layer jamming strategie: barrage jamming. The attack is modeled using protocol-compliant IEEE 802.11p transmissions within OMNeT++ to ensure realistic medium access behavior. The barrage jammer is implemented as a stationary roadside unit (RSU) positioned near the signalized intersection where communication density is highest. The attacker continuously transmits wireless frames at an aggressive rate and elevated transmission power, thereby saturating the shared wireless medium. The jammer transmits 300-byte frames every 1 ms, resulting in approximately 1000 packets per second. Transmission power is configured at 23 dBm, exceeding typical vehicle transmission levels to maximize interference coverage. The attack is activated at simulation time 20 s and remains active until 300 s. This configuration creates persistent channel congestion, leading to frequent collisions, extended backoff durations, and decoding failures at the physical layer. The barrage jammer represents a worst-case denial-of-service scenario commonly studied in wireless interference attacks.

D. Mitigation Scenario Implementation

To enhance resilience against sustained physical-layer interference, we implement a Frequency Hopping Spread Spectrum (FHSS) mitigation strategy in the IEEE 802.11p communication layer. In this approach, each vehicle dynamically switches its transmission and reception frequency among a predefined set of channels using a shared pseudo-random hopping sequence. The hopping pool consists of three channels (one control channel and two service channels), which reflects practical constraints in DSRC/WAVE systems where only a limited number of channels are available for safety-critical communication. Vehicles switch channels every 200 ms, selected as a balanced trade-off between hopping agility and synchronization stability: shorter intervals can reduce jammer overlap but increase switching overhead and misalignment

risk, while longer intervals may allow the jammer to disrupt communication for extended periods. Synchronization between communicating vehicles is maintained through periodic beacon alignment, where nodes follow the same hopping schedule based on a common simulation time reference and message periodicity. This design allows legitimate nodes to remain coordinated while reducing the probability that the jammer continuously overlaps with the active channel, thereby improving packet delivery and bounding latency under barrage-style interference.

V. Result and Analysis

VI. Conclusion and Future Work

Acknowledgment

This work is funded by the US Department of Transportation (USDOT) Tier-1 University Transportation Center (UTC) Transportation Cybersecurity Center for Advanced Research and Education (CYBER-CARE). (Grant No. 69A3552348332), and Theorizing Connected Vehicle (CV) Based Advanced Traffic Management System (ATMS) Vulnerability Analysis and Strategizing for Cyber Security (Grant No. I0509667)

References

[1] Sommer, C., Eckhoff, D., Brummer, A., Buse, D. S., Hagenauer, F., Joerer, S., & Segata, M. (2019). Veins: The open source vehicular network simulation framework. In Recent advances in network simulation: the OMNeT++ environment and its ecosystem (pp. 215-252). Cham: Springer International Publishing.

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

[3] Mokdad, L., Ben-Othman, J., & Nguyen, A. T. (2015). DJAVAN: Detecting jamming attacks in Vehicle Ad hoc Networks. Performance Evaluation, 87, 47-59.

[4] Silwal, S., Gao, L., Zhang, Y., Senouci, A., & Mo, Y. L. (2024). Assessing cybersecurity risks and traffic impact in connected autonomous vehicles. In International Conference on Transportation and Development 2024 (pp. 652-662).

[5] Biron, Z. A., Dey, S., & Pisu, P. (2017, May). Resilient control strategy under denial of service in connected vehicles. In 2017 American Control Conference (ACC) (pp. 4971-4976). IEEE.

[6] Rathore, R. S., Hewage, C., Kaiwartya, O., & Lloret, J. (2022). In-vehicle communication cyber security: challenges and solutions. Sensors, 22(17), 6679.

[7] Wehby, A., Zeadally, S., Khatoun, R., Bouchouia, M. L., & Fadlallah, A. (2024, July). How does distributed denial of service affect the connected cars environment?. In 2024 10th International Conference on Control, Decision and Information Technologies (CoDIT) (pp. 164-170). IEEE.

[8] Amoozadeh, M., Raghuramu, A., Chuah, C. N., Ghosal, D., Zhang, H. M., Rowe, J., & Levitt, K. (2015). Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. IEEE Communications Magazine, 53(6), 126-132.

[9] Stepanyants, V. G., & Romanov, A. Y. (2023). A survey of integrated simulation environments for connected automated vehicles: Requirements, tools, and architecture. IEEE Intelligent Transportation Systems Magazine, 16(2), 6-22.

[10] Arellano, W., & Mahgoub, I. (2013, December). TrafficModeler extensions: A case for rapid VANET simulation using, OMNET++, SUMO, and VEINS. In 2013 High Capacity Optical Networks and Emerging/Enabling Technologies (pp. 109-115). IEEE.

[11]