Real-World Evaluation of Protocol-Compliant Denial-of-Service Attacks on C-V2X-based Forward Collision Warning Systems

Jean Michel Tine*
Ph.D. Student
Glenn Department of Civil Engineering
Clemson University, Clemson, SC 29634, USA
Email: jtine@clemson.edu

Mohammed Aldeen
Ph.D. Student
School of Computing
Clemson University, Clemson, SC 29634, USA
Email: mshujaa@clemson.edu

Abyad Enan
Ph.D. Student
Glenn Department of Civil Engineering
Clemson University, Clemson, SC 29634, USA
Email: aenan@clemson.edu

M Sabbir Salek, Ph.D.
Senior Engineer
USDOT National Center for Transportation Cybersecurity and Resiliency (TraCR)
414A One Research Dr, Greenville, SC 29607, USA
Email: msalek@clemson.edu

Long Cheng, Ph.D.
Associate Professor
School of Computing
Clemson University, Clemson, SC 29634, USA
Email: lcheng2@clemson.edu

Mashrur Chowdhury, Ph.D., P.E.
Eugene Douglas Mays Chair of Transportation
Glenn Department of Civil Engineering
Clemson University, Clemson, South Carolina, 29634
Email: mac@clemson.edu

Word Count: 7250 words + 1 table (250 words per table) = 7500words

*Corresponding author

Tine, Aldeen, Enan, Salek, Cheng, Chowdhury.

ABSTRACT

Cellular Vehicle-to-Everything (C-V2X) technology enables low-latency, reliable communications essential for safety applications such as a Forward Collision Warning (FCW) system. C-V2X deployments operate under strict protocol compliance with the 3rd Generation Partnership Project (3GPP) and the Society of Automotive Engineers Standard (SAE) J2735 specifications to ensure interoperability. This paper presents a real-world testbed evaluation of protocol-compliant Denial-of-Service (DoS) attacks using User Datagram Protocol (UDP) flooding and oversized Basic Safety Message (BSM) attacks that exploit transport- and application-layer vulnerabilities in C-V2X. The attacks presented in this study transmit valid messages over standard PC5 sidelinks, fully adhering to 3GPP and SAE J2735 specifications, but at abnormally high rates and with oversized payloads that overload the receiver resources without breaching any protocol rules such as IEEE 1609. Using a real-world connected vehicle testbed with commercially available On-Board Units (OBUs), we demonstrate that high-rate UDP flooding and oversized payload of BSM flooding can severely degrade FCW performance. Results show that UDP flooding alone reduces packet delivery ratio by up to 87% and increases latency to over 400ms, while oversized BSM floods overload receiver processing resources, delaying or completely suppressing FCW alerts. When UDP and BSM attacks are executed simultaneously, they cause near-total communication failure, preventing FCW warnings entirely. These findings reveal that protocol-compliant communications do not necessarily guarantee safe or reliable operation of C-V2X-based safety applications. These findings highlight a critical security gap in current C-V2X implementations and underscore the need for future research into robust defense mechanisms to safeguard safety applications against stealthy, standards-compliant flooding attacks.

Keywords: C-V2X, Forward Collision Warning, Denial-of-Service, Transport Layer Flooding, Application Layer Flooding, Protocol Compliance.

INTRODUCTION

Modern transportation systems are undergoing a significant shift as vehicles evolve from isolated actors into interconnected agents capable of communicating with other vehicles, road infrastructure and vulnerable road users. This connectivity is realized through Cellular Vehicle-to-Everything (C-V2X), a transformative wireless technology that supports Vehicle-to-Vehicle (V2V), vehicle to Infrastructure (V2I), Vehicle to Pedestrian (V2P) and Vehicle to Network (V2N) communications (*1*). The specifications for the C-V2X communications begin with the release 14 of the 3rd Generation Partnership Project (3GPP) (*2*). This release comprises two new modes of Long-Term Evolution (LTE) operation (i.e., Mode 3 and Mode 4) which differ from their resource allocation. As shown in **Figure 1**, Mode 3 relies on the cellular base-station to perform resource allocation. On the other hand, Mode 4 enables vehicles to allocate resources on their own, using the PC5 sidelink interface, which is a cellular technology defined in 3GPP standards that enables direct communication with other nodes (e.g., connected vehicles, Roadside Unit (RSU)). Through this PC5 sidelink, connected vehicles broadcast Basic Safety Message (BSMs), typically at 10Hz, containing critical real time data, such as position, speed, heading, and brake status. These messages are designed in agreement with the Society of Automotive Engineers (SAE) J2735 standard (*3*), hence forming the foundation for real-time safety applications, like Forward Collision Warning (FCW), Emergency Electronic Brake Light (EEBL) alerts, and intersection movement assist.
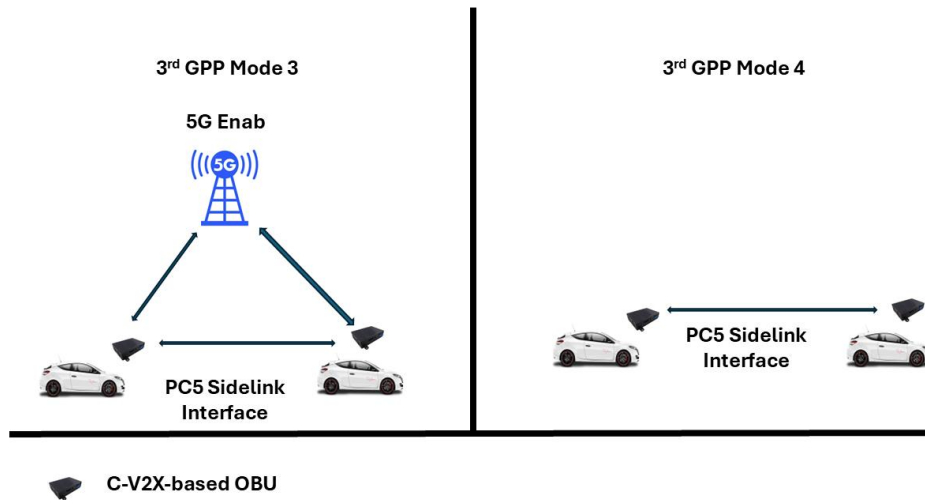

Figure 1 Modes 3 and 4 of C-V2X Communication

The design goal of C-V2X focuses on low latency (under 50 ms) and high packet delivery ratio (PDR) of at least 90% to meet the timing requirements of connected vehicle safety applications (*4*, *5*). These features make it a more capable successor to the Dedicated Short Range Communication (DSRC) technology, following IEEE 802.11p, by offering greater range and improved reliability under different channel conditions (*4*) (*6*). However, as opposed to Mode 3, where a central base station arbitrates resource allocation, C-V2X heavily relies on contention-based scheduling due to its autonomous resource selection in Mode 4. This decentralized approach eliminates central arbitration (i.e., flow control) and introduces vulnerability under congested conditions (*7*). In Mode 4, vehicles select communication resources based on local sensing of channel availability, a method known as sensing-based semi-persistent scheduling (SB-SPS) (*6*). While this method allows vehicles to operate independently of cellular infrastructure, it also increases the likelihood of resource collisions, especially when many connected vehicles attempt to transmit BSMs simultaneously in dense traffic scenarios. Without a mechanism to dynamically coordinate or control message rates, excessive legitimate traffic can saturate the channel, leading to increased latency, packet loss, and degraded reliability. This challenges the

fundamental performance goals of C-V2X technology, particularly for connected vehicle safety applications that require timely and reliable message delivery (*8*).

To regulate message traffic and mitigate congestion, 3GPP defines Decentralized Congestion Control (DCC) mechanisms based on two channel-level metrics; these metrics are the Channel Busy Ratio (CBR) and the Channel Occupancy Ratio (COR) (*9*, *10*). CBR estimates the proportion of busy channels, while COR reflects a transmitter's own usage of a channel. When COR exceeds the predefined threshold relative to the measured CBR, connected vehicles must adjust their message rates and resource usage by dropping or delaying application-layer packets (*8*). However, these congestion controls prioritize radio stability over application responsiveness and may hinder the timely delivery of crucial safety messages (*11*).

Although these mechanisms aim to stabilize Mode 4's decentralized operation, they can be exploited within the bounds of protocol compliance. Rather than relying on spoofing or jamming, protocol-compliant misuse could leverage valid yet abnormal transmissions (e.g., high-rate or oversized payload BSMs) to degrade C-V2X communication performance. These behaviors evade traditional security filters, hence, can overwhelm C-V2X receivers, elevate latency, and suppress safety alerts.

As demonstrated by Trkulja *et al.* (*12*), adversarial selection of resource blocks, while fully compliant with SB-SPS standards, can introduce systematic collisions that significantly reduce packet reception. Moreover, Twardokus and Rahnari (*13*) showed that authentic BSMs transmitted at excessive rates deplete receiver resources, induce delays, and suppress application-layer alerts. Even proposed mitigations like interleaved one-shot SPS in (*14*) still observe meaningful degradation in PDR, inter-packet gap, and age of information. While these studies have shown how standards-compliant message behaviors can cause performance degradation, most have relied on simulation environments or focused on either the transport or the application layer. Moreover, few have evaluated how combined protocol-compliant attacks, involving multiple layers, impact actual C-V2X-based safety applications in real-world conditions.

Connected vehicles' communications are also managed by the IEEE 1609 family, which define the Wireless Access in Vehicular Environments (WAVE) protocol stack (15). Positioned above the User Datagram Protocol (UDP) layer, WAVE provides essential services that enable secure, low-latency vehicular communications. A critical component of this family is IEEE 1609.3, which defines networking and transport services for WAVE, including the WAVE Short Message Protocol (WSMP) for low-latency safety messages and full IPv6 support for non-safety applications. (16). While the IEEE 1609 security framework establishes a robust foundation for trusted communications, it does not fully address the threat of protocol-compliant attacks. Such attacks exploit standard-compliant behaviors, thus evading detection while still degrading the performance of safety-critical applications. These gaps are particularly concerning for C-V2X-based connected vehicle applications.

This paper addresses these gaps by presenting a real-world case study of protocol-compliant Denial-of-Service (DoS) attacks on a C-V2X-based FCW system. We investigate flooding scenarios at both the transport layer (via high-frequency UDP packets) and the application layer (via oversized BSMs), and demonstrate their combined effect on message delivery, latency, and FCW alert suppression. Using a connected vehicle testbed with commercial On-Board Units (OBUs), we conduct empirical evaluations, revealing how standards-compliant, yet excessive traffic can severely degrade safety-critical communications without violating any protocol specifications. This paper makes three key contributions:

- We design and implement a UDP flooding DoS attack on a real-world C-V2X testbed using commercial OBUs to study its impact on communication reliability and FCW functionality.
- We develop an oversized-BSM (i.e., high payload) flooding DoS attack that stresses C-V2X receiver-side processing resources and analyzes how such protocol-compliant behavior affects message handling and safety alert generation.
- We evaluate the combined effect of simultaneous UDP and oversized-BSM floods on C-V2X communications, providing an empirical understanding of cross-layer protocol-compliant DoS attacks.

The remainder of this paper is organized as follows: first, we provide background on the C-V2X communication stack and related studies on performance degradation in connected vehicle systems. Second, we present our attack model and describe the real-world experimental testbed setup using commercial OBUs to evaluate protocol-compliant flooding attacks. Third, we detail our attack implementation, including both transport-layer UDP flooding and application-layer BSM flooding scenarios and their combined effects. Next, we present empirical results quantifying the impact on message delivery, latency, and FCW alert responsiveness and discuss the broader implications for C-V2X safety and resilience. Finally, the paper presents a few potential mitigation approaches, discusses study limitations, and outlines future research directions, along with the conclusions.

BACKGROUND AND RELATED WORK

This section explains the C-V2X communication stack, IEEE 1609 security framework, and DCC mechanisms relevant to DoS resilience. It also reviews prior research on congestion and protocol-compliant vulnerabilities to present how this study addresses the gap within relevant literature.

Background

To fully understand how protocol-compliant DoS attacks can impact C-V2X-based safety systems, it is important to first clarify the underlying technical architecture. C-V2X communication technology is organized in a hierarchical stack similar to the Open Systems Interconnection (OSI) model, consisting of four primary layers as illustrated in **Figure 2**; the physical layer, the Medium Access Control (MAC) layer, the network and transport layers, and the application layer (*17*) (*18*). Each of these layers performs a specific role, collectively enabling low-latency and reliable communication required by real-time connected vehicle safety applications.
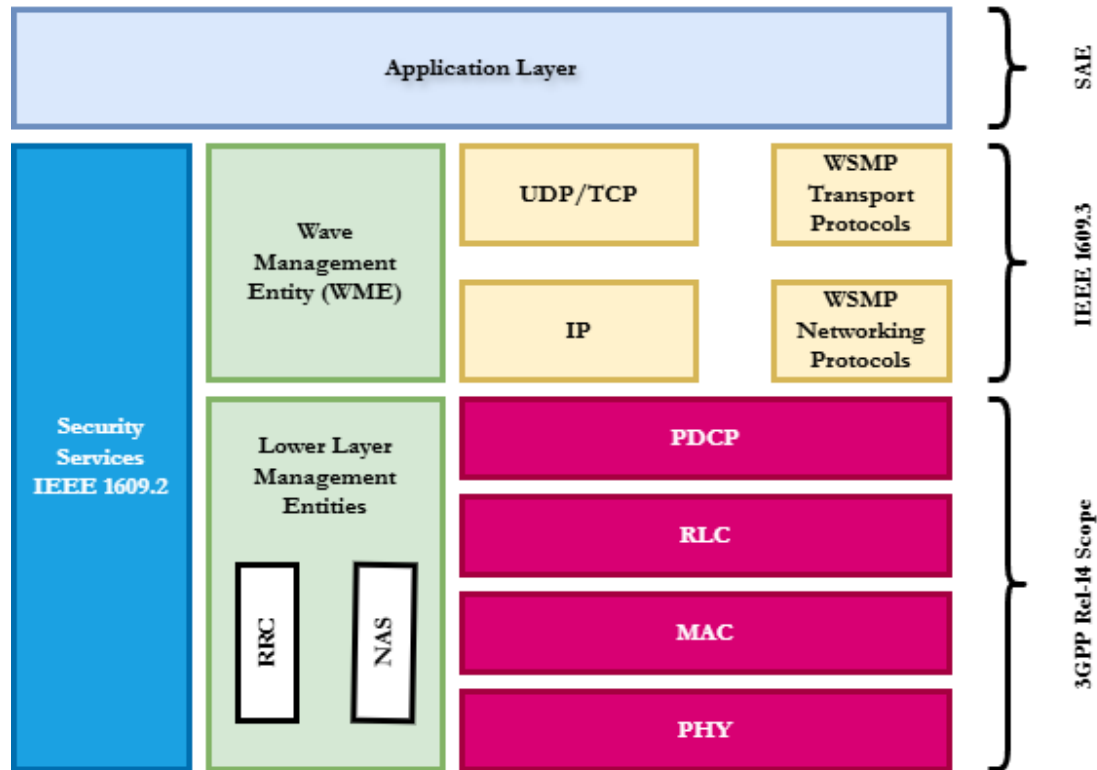

Figure 2 C-V2X communication stack

Physical Layer
At the physical layer (denoted as PHY in **Figure 2**), C-V2X functions primarily within the dedicated 5.9 GHz Intelligent Transportation Systems (ITS) band, which has been reserved solely for supporting reliable, short-range vehicular communication for road safety purposes (*19*, *20*). Communication in this ITS band leverages Orthogonal Frequency-Division Multiplexing (OFDM), a digital modulation technique that divides the available frequency band into multiple orthogonal sub-channels. Across these sub-channels, the OFDM simultaneously transmits signals to effectively mitigate the effect of multipath fading (*21*). Furthermore, OFDM's inherent resilience to interference and its ability to support high data rates and low latency transmission make it particularly suitable for the rapidly changing conditions encountered by vehicles moving at high speeds (*22*).

In the context of our study, the physical layer's design for robust and rapid transmission is critical because it serves as the foundational layer that carries higher-layer messages, such as BSMs, over the air. Although this layer is optimized for reliability and performance, its effectiveness inherently depends on efficient and coordinated use of the wireless channel at the layers above it. Excessive or poorly managed transmissions originating from upper layers (such as the transport and application layers targeted by our DoS scenarios) can severely degrade the physical layer performance. This shows increased interference, reduced signal quality, and diminished reliability of safety-critical communication, ultimately hindering the timely delivery of safety alerts (*8*, *23*, *24*). Thus, understanding the operational mechanisms and limitations of the physical layer is crucial when evaluating the impact of protocol-compliant DoS attacks on overall C-V2X system performance.

MAC Layer
Directly above the physical layer is the MAC layer, which manages how vehicles access the wireless channel. In C-V2X Mode 4, the MAC uses SB-SPS, allowing vehicles to autonomously select time-frequency slots based on sensed local channel activity. As mentioned in the introduction, this decentralized method enables communication without cellular infrastructure but also increases the risk that multiple vehicles choose the same slot simultaneously, especially in densely populated road environments resulting in packet collisions, interference, and message loss (*1*).

Though SB-SPS typically delivers low latency under normal load, this advantage collapses under congested or adversarial traffic. Multiple vehicles selecting identical resources or receiving excessive, protocol-compliant transmissions can saturate MAC resources, cause scheduling collisions, and impair the timely delivery of BSMs (*25*). In our study, we focus on how upper-layer floods, i.e., deliberate but syntactically valid traffic originating from the application or transport layers, exacerbate vulnerabilities in SB-SPS and compromise real-time safety functions such as FCW.

Network and Transport Layer
Above the MAC layer lies the network and transport layers, responsible for ensuring efficient data exchange between vehicles. In C-V2X, the UDP is used on the transport layer due to its minimal overhead and rapid transmission capability. UDP operates on a connectionless basis, meaning it sends packets without requiring acknowledgments or retransmissions, significantly reducing latency (*13*). While ideal for safety-critical messaging, this design inherently lacks congestion control or flow regulation. Consequently, an excessive rate of UDP packets, such as empty packets sent at high frequency, can easily saturate receiver-side buffers, leading to increased packet drop rates, prolonged processing delays, and reduced reliability in message delivery.

This vulnerability directly motivates our research, as we investigate how even protocol-compliant yet high-frequency UDP packet flooding from legitimate nodes can overwhelm receivers and negatively impact the safety applications' function, including collision warning alerts.

Application Layer
At the top of the communication stack, the application layer is responsible for formulating and parsing messages that carry critical safety information. In C-V2X deployments, vehicles regularly broadcast BSMs in compliance with the SAE J2735 standard (*26*). These BSMs serve as input for safety applications, such as FCW, EEBL, and intersection movement assist. While BSMs follow standardized formats, optional data fields allow flexibility in message size, potentially creating opportunities for oversized yet valid messages. Transmitting these larger messages at unusually high frequencies can exhaust receiver-side processing resources, delay the parsing and processing of legitimate safety alerts, and ultimately disrupt timely safety responses. This scenario, which we refer to as application-layer flooding, is what our study explores through empirical evaluations, demonstrating how legitimate yet excessive messaging at the application layer can silently degrade critical C-V2X safety operations.

IEEE 1609 Family and Security Integration
IEEE 1609 family of standards form the foundation of secure communications in connected vehicle networks, defining the WAVE protocol stack that enables interoperability among On-Board Units (OBUs) and RSUs (*15*). Within this group, IEEE 1609.2 defines the security layer responsible primarily for message authentication, digital signatures, and certificate management, while optional encryption is also supported (*16*). These mechanisms ensure that safety-critical messages such as BSMs are trustworthy and protected against spoofing, tampering, or unauthorized access. To Complement these services, IEEE 1609.3 defines networking and transport layer services that operate above UDP/TCP (*15*). It introduces the WAVE Short Message Protocol (WSMP), which enables low-latency dissemination of safety messages by minimizing protocol overhead. In addition, IEEE 1609.3 supports IPv6-based communication for broader IP applications, allowing simultaneous delivery of safety and non-safety messages (*27*). Together, IEEE 1609.2 and 1609.3 provide structured message handling, prioritization, and secure delivery mechanisms critical to vehicular safety systems.

 Despite these protections, prior research has identified that the IEEE 1609 family does not inherently address protocol-compliant DoS attacks. Adversaries can exploit legitimate use of UDP, as supported in IEEE 1609.3, to send high volumes of valid messages without violating protocol specifications (*28*). This excessive yet standards-compliant traffic can overwhelm lower-layer resources, disrupt medium access scheduling (*12*), and degrade the performance of safety applications such as FCW. Studies have shown that authenticated and encrypted messages, even when fully compliant with IEEE 1609.2 security requirements, can lead to significant congestion and delayed safety alerts if transmitted in high frequency (*29*).

 Our work builds upon this standards-based foundation by empirically demonstrating how protocol-compliant message floods can impair safety-critical C-V2X applications. Using commercial OBUs, we evaluate real-world flooding scenarios involving high-frequency UDP packets and oversized BSMs. These attacks leverage mechanisms defined in IEEE 1609.3 and remain fully standards-compliant under IEEE 1609.2 security policies. By analyzing their impact on message delivery, latency, and FCW alert generation, our study highlights an unmitigated vulnerability within the existing WAVE security framework that warrants further attention from the cybersecurity community.

Related Work
Previous research on C-V2X communication has primarily focused on the reliability and efficiency of safety-critical messaging under normal and congested network conditions. Studies have extensively explored the resilience of C-V2X against common cyber threats, including spoofing attacks, jamming, and packet manipulation (*22, 30*). However, relatively few studies have investigated how strictly protocol-compliant behavior could become a source of vulnerability.

 Early research by Boban *et al.* (2018) and Garcia *et al.* (2021) provided a foundational understanding of the capabilities and limitations of C-V2X, specifically analyzing communication performance metrics, such as latency, PDR, and interference resilience (*31*). These studies revealed the robust nature of C-V2X compared to traditional technologies like DSRC, but primarily addressed ideal or

moderately congested scenarios, leaving extreme conditions unexplored. Recent contributions by Twardokus and Rahbari (2022) highlighted potential vulnerabilities coming from legitimate, yet excessive, BSM transmission rates (*13*). Their simulation-based analysis indicated significant receiver-side congestion and processing delays when faced with abnormally high message rates. Although insightful, these simulations lacked validation through real-world deployments and only considered single-layer threats, i.e., either at the transport or the application layer, independently. Fouda *et al.* (2023) expanded on these findings by examining the impact of Hybrid Automatic Repeat Request (HARQ) retransmissions and the resulting delays in safety-critical messages under congested conditions (*32*). Their work suggested that although retransmissions improve reliability, they simultaneously introduced substantial latency, potentially jeopardizing timely safety warnings. Yet, their analysis remained predominantly theoretical and did not examine combined-layer threats. McCarthy *et al.* (2021) developed OpenCV2X, i.e., an open-source simulation environment, specifically modeling the impact of oversized or irregular traffic patterns on sidelink scheduling performance (*33*). Their work demonstrated that irregular application-layer traffic could severely degrade performance metrics. Despite this progress, their simulations did not explore the combined effect of simultaneous transport-layer flooding, nor were the findings validated through field testing.

Consequently, there remains limited empirical evidence regarding how a combined protocol-compliant flooding simultaneously at the transport and the application layers could affect real-world safety-critical applications such as an FCW system. Our study addresses this gap by conducting a real-world testbed-based experimental evaluation of such multi-layer DoS scenarios. We measure real-time impacts on latency, message delivery, and FCW application performance, offering practical insights and present corresponding mitigation recommendations that do not require changes to existing C-V2X standards or protocols.

METHODS

The methods section describes the experimental approach used to evaluate DoS threats. It explains the attack model, experimental testbed, and metrics used to assess performance degradation under flooding attacks.

Experimental Method

To assess the resilience of C-V2X FCW systems under realistic adversarial conditions, we devised an experimental method, as shown in **Figure 3**. For these experiments, we first define a realistic attack model in which an adversary uses a fully compliant C-V2X device to generate excess traffic at both the transport and the application layers. Next, we establish baseline performance by driving two vehicles equipped with commercial Cohda MK6C OBUs under normal conditions, measuring PDR, end-to-end latency, and FCW trigger timing. Finally, we implement and execute protocol-compliant flooding attacks, transport-layer UDP flooding, and application-layer oversized BSM floods, both independently and in combination while continuously monitoring the same performance metrics. By comparing attack scenarios against our baseline, we quantify how each flooding strategy degrades communication reliability and delays or suppresses collision warnings, thus revealing the vulnerabilities of C-V2X FCW systems under stealthy, standards-compliant DoS conditions.
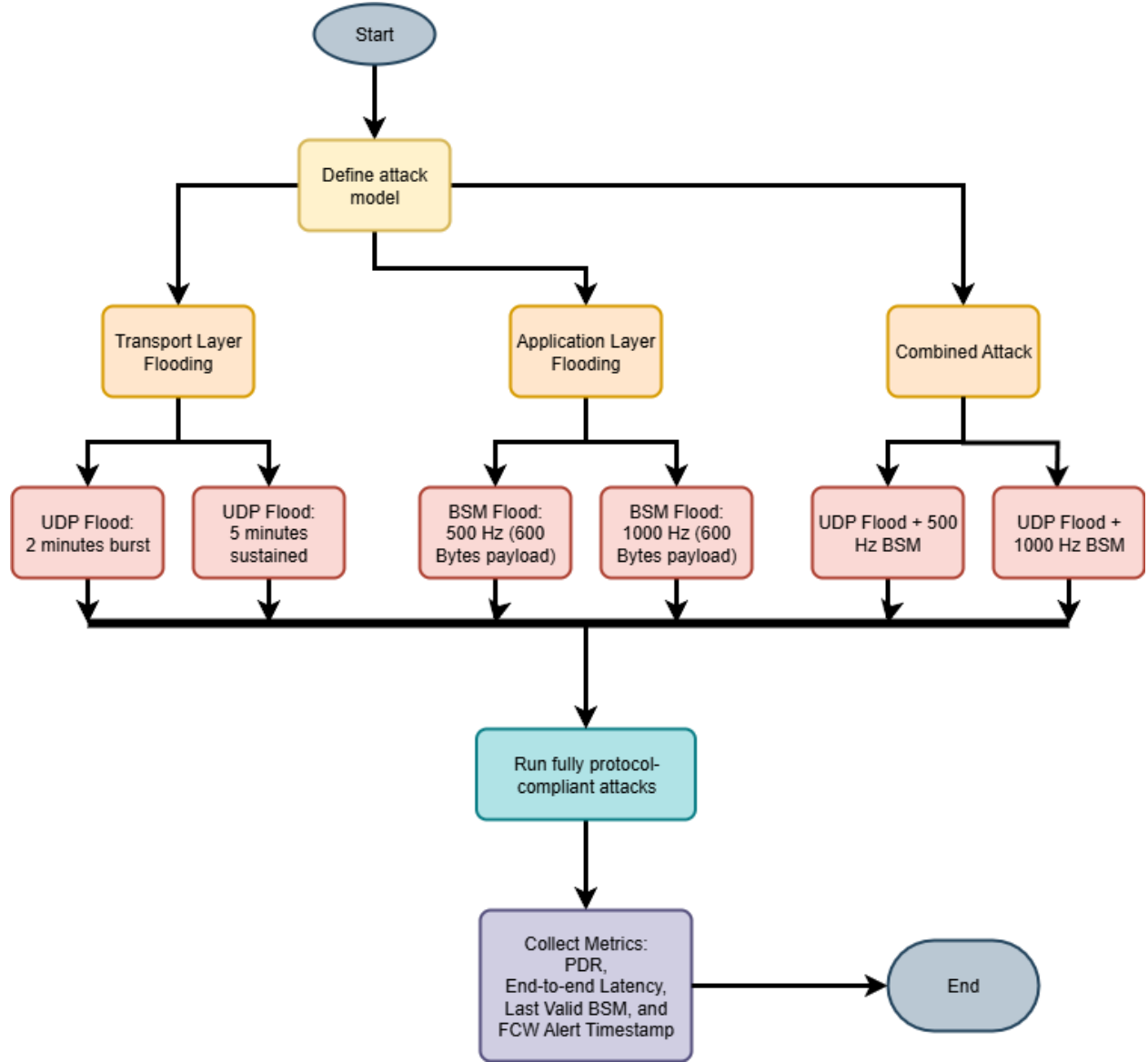
Figure 3 Experimental plan for three DoS attack scenarios

Attack Model

In our attack model, we consider an adversary with full access to a standards-compliant C-V2X device, including the capability of transmit BSMs and UDP packets over the PC5 sidelink. Importantly, the attacker does not spoof message content, manipulate identifiers, or violate protocol specifications. Instead, the adversary exploits a design-level weakness in C-V2X communications: the lack of built-in rate control and congestion management mechanisms.

By deliberately increasing the volume and frequency of otherwise valid transmissions, the attacker can saturate wireless channel resources, overload receiver-side message queues, and delay the timely processing of genuine safety-critical data. Because these transmissions fully comply with the 3GPP and SAE J2735 standards, they are difficult to distinguish from legitimate traffic. This makes the attack stealthy and challenging to detect using conventional intrusion prevention or anomaly-based filtering systems.

This model reflects a realistic and practical attack scenario, in which a malicious, or compromised, yet fully authorized vehicle or RSUgenerates excessive, protocol-compliant traffic. Such behavior could occur unintentionally due to faulty firmware or can be exercised maliciously due to adversarial reprogramming. In either case, the result is a DoS condition that silently degrades communication reliability and delays safety application responses without breaching security policies. As mentioned before, we target two layers in this attack model as follows:

- **Transport Layer**: Exploiting UDP's connectionless and unregulated transmission behavior to create floods that saturate receiver buffers.
- **Application Layer**: Transmitting oversized or abnormally frequent BSMs that adhere to protocol rules but induce excessive processing delays and resource contention.

The objective of the adversary is to degrade the performance of a C-V2X-based FCW system while remaining fully compliant with protocol specifications. Specifically, the attacker aims to reduce packet delivery and increase end-to-end latency to levels that compromise safety alert generation. We evaluate this degradation using the following performance metrics:

$$PDR = \frac{N_{recv}}{N_{sent}} \times 100\% \tag{1}$$

$$L_{avg} = \frac{1}{N_{recv}} \sum_{i=1}^{N_{recv}} (t_i^{rx} - t_i^{tx}) \tag{2}$$

where, N_{sent} and N_{recv} are the number of BSMs transmitted and successfully processed by the FCW logic, respectively, and t_i^{rx}, t_i^{tx} are the transmission and reception timestamps for message i.

Under normal conditions, these metrics satisfy application-layer requirements (i.e., $PDR \geq 90\%$ and $L_{avg} \leq 50\ ms$). However, when combining both legitimate and adversarial messages, the PC5 interface's service capacity λ_{PC5} is saturated, hence the receiver's message queue is overloaded. This leads to increased delays and packet loss, which is modeled by:

$$Q(t + \Delta t) = Q(t) + A(t) - D(t) \tag{3}$$

where, $Q(t)$ represents the instantaneous queue length (number of unprocessed messages) at time t, $A(t)$ the aggregate packet arrival rate (i.e., attack and non-attack traffic), and $D(t)$ denotes the packet dispatch rate, typically bounded λ_{PC5}. Under normal conditions, $A(t) = D(t)$ maintains a steady queue state and when $A(t) < D(t)$ the queue size decreases, meaning that the receiver is processing the messages faster than they arrive, gradually emptying the queue. However, when $A(t) > D(t)$, the queue grows unbounded, leading to buffer overflow, increased latency, and potential suppression of safety-critical alerts such as FCW. This highlights the necessity of keeping traffic rates within the receiver's processing capacity to uphold the reliability of C-V2X safety applications. In the application-layer flooding scenario, oversized yet standard-compliant BSMs are transmitted. Although these messages do not increase the physical channel occupancy beyond capacity, they introduce substantial computational overhead on the receiver. Specifically, the parsing and validation of larger payloads require more CPU cycles and memory operations per message, effectively lowering the number of messages that can be processed within a given time window. Even when the arrival rate $A(t)$ remains within normal channel capacity, the effective dispatch rate $D_{eff}(t)$ is reduced due to resources being overloaded, as shown in the following equation:

$$Q(t + \Delta t) = Q(t) + A(t) - D_{eff}(t), \qquad D_{eff}(t) < \lambda_{PC5} \tag{4}$$

$$D_{eff}(t) = \frac{1}{T_{processing}(S)} \tag{5}$$

where, $T_{processing}(S)$ is the processing time per message and increases with payload size S. Even if it is below the physical channel limit $A(t) < \lambda_{PC5}$, $D_{eff}(t)$ drops because $T_{processing}(S)$ is longer.

CASE STUDY: PROTOCOL-COMPLIANT DOS ATTACKS IN CONNECTED VEHICLES
This section details the real-world implementation of the attack model using two connected vehicles and commercial OBUs. It establishes baseline FCW performance, describes the staged DoS attack executions, and explains how each scenario stresses system resources.

Experimental Setup and Baseline Operating Condition
We evaluate the safety application, FCW, under our attacks in a real-world testbed, as shown in **Figure 4**. Using two vehicles, each equipped with a Cohda MK6C Evaluation Kit (EVK) OBU running 3GPP Release 14 firmware and a rooftop omnidirectional antenna for robust sidelink communication. **Figure** 4 illustrates the experimental setup, where vehicle A moves towards vehicle B under normal driving conditions.
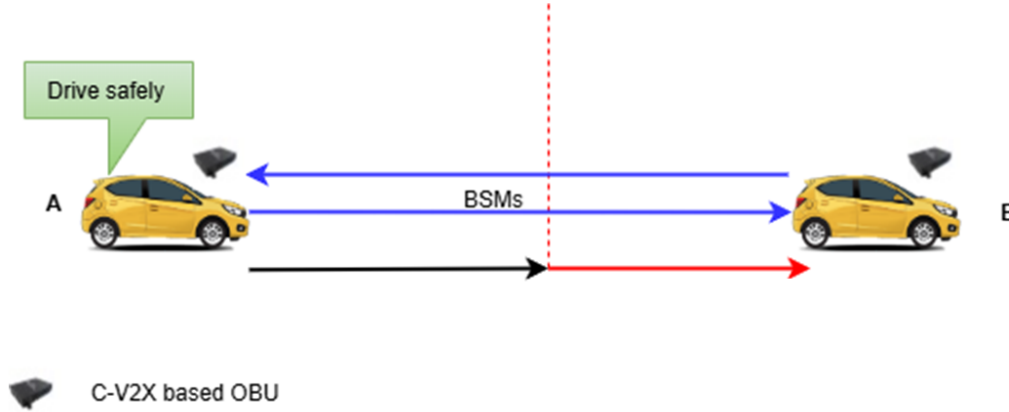

Figure 4 Experimental setup

Each OBU broadcasts and receives BSMs at a frequency of 10 Hz. In this study, we used the BSM fields speed, longitude, latitude, and braking status, as these are essential inputs for the FCW algorithm to evaluate collision risk and trigger timely alerts. The FCW application continuously computes the Time-to-Collision (TTC) between two vehicles using their relative positions and speeds:

$$TTC\,(t) = \frac{d(t)}{v_A(t) - v_B(t)} \tag{6}$$

where, $d(t)$ is the gap between vehicles A and B, and $v_B(t)$, $v_A(t)$ are the speeds of vehicles A and B, respectively.

In our case vehicle B is stationary (i.e., $v_B(t) = 0$) and the follower vehicle A is moving, therefore the TTC simplifies to $TTC\,(t) = \frac{d(t)}{v_A(t)}$ and a safety alert is issued when the TTC falls below a threshold of 3 seconds, minimum to balance timely warning and false-alarm rate in FCW systems (*34*).
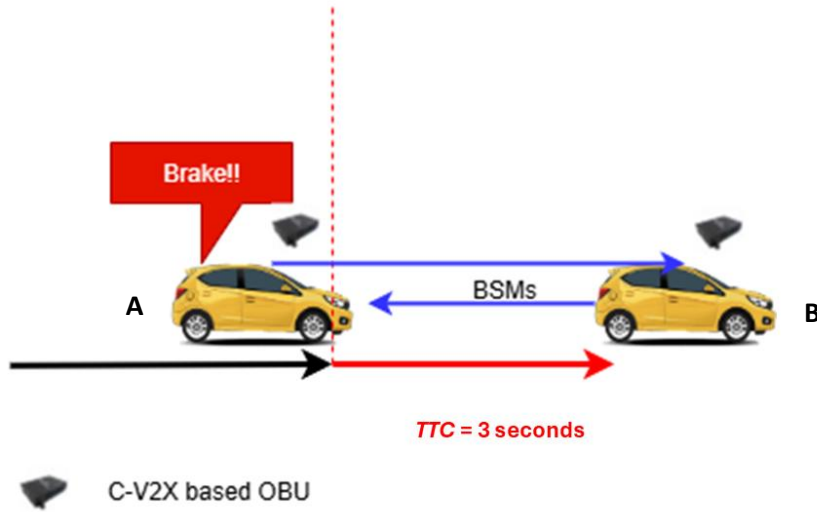
Figure 5 FCW alert when TTC falls below the threshold chosen for this study

Before introducing the DoS attacks, we established a baseline to define the normal performance of our connected vehicle FCW application. At normal conditions, the system operates at a 10Hz BSM transmission rate, and the C-V2X PC5 sidelink maintains high reliability and low latency, ensuring the timely delivery of BSMs for the FCW application.

Figure 6(a) shows the BSM latency distribution over time during our baseline operation. The latency value remained consistently below the threshold of 50 milliseconds, averaging 35 milliseconds. These characteristics align with the C-V2X design target for safety applications and enable the FCW algorithm to continuously compute TTC without delay, triggering alerts promptly when the oncoming vehicle A is within 30 meters of vehicle B, the critical zone. Meanwhile, **Figure 6(b)** shows the BSM packet rate measured during our baseline operation. The transmission frequency remained stable at 10 packets per second, with minimal fluctuation. This stability contributed to a PDR exceeding 99%, confirming that the communication stack functioned optimally under normal conditions. These baseline performances from our testbed serve as a reference point for the following experiments involving transport and application-layer flooding attacks.
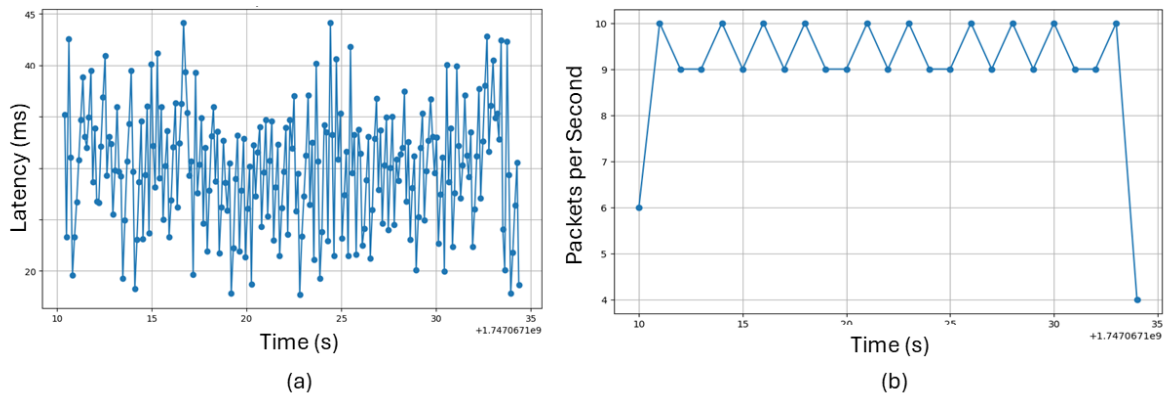

(a)　　　　　　　　　　　(b)

Figure 6 C-V2X communication performance for baseline (i.e., non-attack) operating condition

Attack Execution

Tine, Aldeen, Enan, Salek, Cheng, Chowdhury.

Building on the experimental setup described above, we designed and executed a series of DoS attacks to evaluate the impact of protocol-compliant flooding on the FCW application. The same two-vehicle testbed equipped with Cohda MK6C OBUs was used; however, as shown in Figure 6, we introduced an additional attack control system acting as an adversarial node. This system consists of a high-performance laptop directly interfaced with one of the OBUs, allowing us to generate synthetic yet standards-compliant traffic. This approach effectively transforms the OBU into a malicious connected vehicle node without requiring hardware modifications or protocol violations.
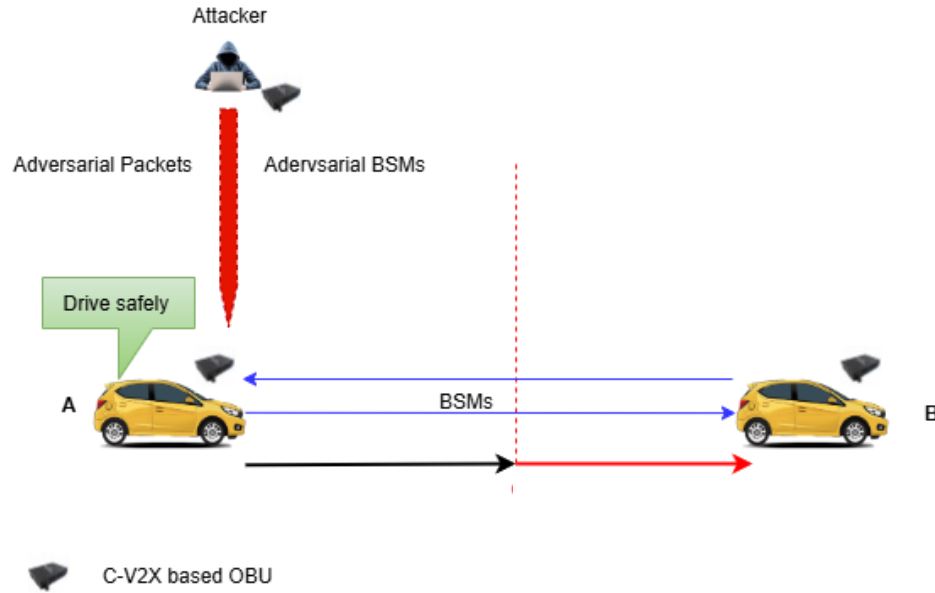

Figure 7 Attack setup

The first wave of attacks targeted the transport layer. Consider a scenario where an otherwise normal device suddenly starts sending an overwhelming number of empty UDP packets. The messages themselves are valid and comply with communication protocols, but the sheer volume quickly overwhelms the receiver's buffer. We tested this behavior in two ways. In the first case, the attacker unleashed a short yet intense burst lasting two minutes, similar to a quick, disruptive wave. In the second case, the flood was kept for five minutes, persistently filling message queues and forcing the system to struggle with processing delays. Both attacks were fully standards-compliant, which made them appear legitimate, yet they were specifically designed to exhaust resources and slow down the flow of safety-critical information to the FCW system.

After observing how the transport layer responded, we crafted attacks aimed at the application layer. Normally, vehicles exchange BSMs at 10Hz, which is a balanced rate designed for reliable and timely communication. For this application-layer attack, the attacker drastically increased this rate to 500 BSMs per second, overloading the channel with a flood of messages. While every message still followed protocol rules and appeared legitimate, the excessive volume congested the communication pathway. Processing legitimate safety messages became a challenge. To push the system further, we doubled the rate to 1,000 messages per second, overwhelming both the channel and the receiver's ability to handle incoming data and extending processing resources to their limits.

Finally, to replicate more real-world attacks, we combined these flooding techniques. In one scenario, the system faced a UDP flood and a simultaneous 500 Hz BSM with a payload of 600 bytes, creating two layers of stress: transport-layer congestion and application-layer message overload. The ultimate test came when we paired a sustained UDP flood with a 1,000 Hz BSM, a worst-case attack that

saturated communication buffers and message handling capabilities, leaving the system on the edge of a complete communication breakdown.

These attacks were carefully crafted to look normal while behaving stealthily enough to bypass conventional detection. By gradually escalating the attack duration, message frequency, and layering techniques, we crafted realistic adversarial conditions that exposed how protocol-compliant message floods could silently disrupt communication and delay safety-critical alerts of an FCW application.

RESULTS

In this section, we present the impact of protocol-compliant flooding attacks on C-V2X-based OBU communications and their direct effect on FCW. **Figure 8** and **Table 1** present detailed performance metrics for each tested scenario, including PDR, average end-to-end latency, and the resulting impact on FCW alert generation.

Under baseline conditions (10 Hz BSM), the system maintained a high PDR of 99.2% with an average latency of only 35 ms. Consequently, the FCW system reliably triggered timely safety alerts, with the last valid BSM received at 17.00 s and the alert triggered shortly after at 17.42 s. These metrics, i.e., last valid BSM's timestamp and FCW trigger timestamp, are critical for evaluating system responsiveness. The last valid BSM's timestamp represents the final successfully processed safety message before a potential collision, whereas the FCW trigger timestamp indicates when the collision warning is activated based on these messages. These metrics directly reflect the system's ability to issue alerts within the safety-critical TTC threshold of 3 seconds.

When we executed a transport-layer UDP flood attack for 2 minutes, the latency increased to 156 ms and PDR dropped to 89% as shown in **Figure 8**, causing a delayed FCW alert. The last valid BSM in this scenario was received at 17.21 s, with the alert triggered at 18.30 s. Extending the flood duration to 5 minutes severely impacted system performance, reducing PDR to 12.4% and elevating latency to 400 ms. As a result, the FCW system failed to issue an alert, as the last valid message was received at 5.37 s.

In application-layer flooding scenarios, transmitting valid but oversized BSMs at 500 Hz moderately degraded performance, lowering PDR to 67.3% and raising latency to 105 ms. The FCW alert was triggered at 19.50 s, nearly 2 seconds after the last valid BSM was received at 17.50 s. Increasing the frequency to 1000 Hz intensified these effects, further reducing PDR to 41.5% and increasing latency to 180 ms, resulting in a missed FCW alert.

The most severe impacts occurred under combined flooding attacks. With simultaneous UDP flood and a 500 Hz BSM flood, PDR dropped sharply to 28.7% with latency reaching 250 ms. The last valid BSM was received at 45.12s, meaning the system lost communication significantly earlier than in other "missed alert" cases, leading to a severe impact despite similar alert outcomes. Combining a UDP flood with a 1000 Hz BSM flood caused the most extreme degradation, with PDR falling to 10.2% and latency exceeding 420 ms. The last valid message arrived at 4.83 s, completely disabling the FCW system well before reaching the 3-second TTC threshold, leaving no opportunity for late FCW alert generation.

Collectively, these empirical results show that layered, protocol-compliant flooding attacks substantially compromise both communication reliability and application-layer responsiveness. Earlier breakdowns indicate heavier attack impact, as they eliminate even the possibility of a delayed FCW
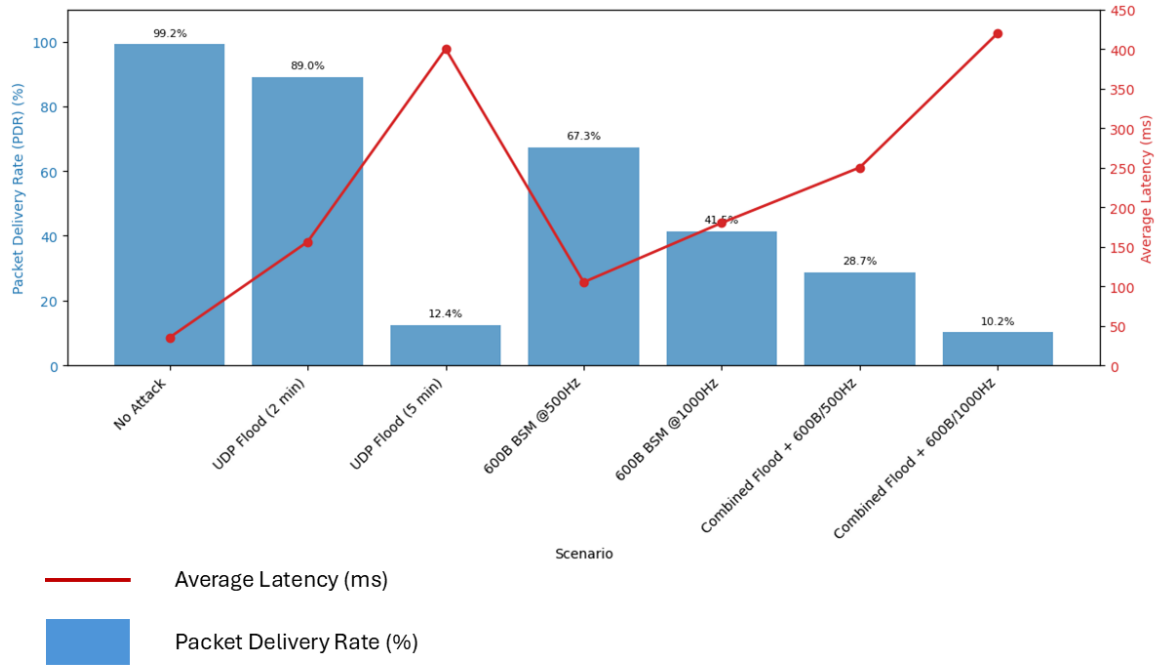
response.

Figure 8 Impact of transport and application-layer attacks on C-V2X communication performance

TABLE 1 Impact of Protocol-Compliant Attacks on Valid BSM Reception and FCW Functionality

Scenario	Average Latency (Maximum Threshold: 50 ms)	PDR (Minimum Threshold: 90%)	Last Valid BSM's Timestamp	FCW Trigger Timestamp	FCW Alert	Attack Success
Baseline	35 ms	99.2 %	17.00 s	17.42 s	Timely alert	No attack
UDP Flood (2 minutes)	156 ms	89.0 %	17.21 s	18.30 s	Delayed alert	Successful
UDP Flood (5 minutes)	400 ms	12.4 %	5.37 s	No trigger	Missed alert	Successful
500Hz Valid BSM Flood	105 ms	67.3 %	17.50 s	19.50 s	Delayed alert	Successful
1000Hz Valid BSM Flood	180 ms	41.5 %	4.83s	No trigger	Missed alert	Successful
Flood + 500Hz BSM (600 Bytes)	250 ms	28.7 %	5.12 s	No trigger	Missed alert	Successful

Flood + 1000Hz BSM (600 Bytes)	420 ms	10.2 %	4.83 s	No trigger	Missed alert	Successful

DISCUSSION

Our experimental findings reveal a critical vulnerability in current C-V2X safety systems. The ability to severely degrade FCW performance through protocol-compliant attacks demonstrates that adherence to communication standards alone is insufficient to guarantee safe operation of connected vehicle systems. Also, the current design of DCC, while effective at protecting radio interface stability, creates vulnerabilities at higher protocol layers, leaving FCW and similar safety systems exposed to stealthy, standards-compliant DoS conditions.

While this study focused on FCW, the protocol-compliant flooding techniques demonstrated here could be extended to evaluate other critical C-V2X safety applications. EEBL systems, which rely on rapid BSM processing to detect emergency braking events from surrounding vehicles, would likely exhibit similar vulnerabilities to oversized BSM floods that delay message parsing. Also, multi-vehicle attack scenarios could represent a particularly concerning extension of this work. If multiple compromised vehicles in a traffic area simultaneously execute coordinated UDP and BSM floods, the resulting network congestion could effectively disable C-V2X safety communications across an entire road segment.

The experimental evaluation was conducted under controlled conditions that may not fully capture the complexities of real-world vehicular environments, such as varying traffic densities, high-speed mobility, and unpredictable wireless interference. Furthermore, this work intentionally focuses on protocol-compliant flooding attacks, as opposed to other forms of cyberattacks, such as spoofing and jamming, which have already been extensively investigated in prior research. By narrowing the scope, this study isolates and highlights the often-overlooked threat of compliant flooding attacks. However, future research could combine these well-studied attacks with protocol-compliant threats to provide a more holistic understanding of security challenges in C-V2X networks. Additionally, the hardware and software platform used in these experiments may not fully represent the behavior of other commercial OBUs or safety application architectures, potentially influencing latency and packet delivery outcomes. Finally, the analysis centered on FCW alone, while other safety-critical applications that rely on timely message delivery, such as cooperative braking or intersection collision avoidance, were not inspected.

CONCLUSIONS AND FUTURE WORK

This study demonstrates that protocol-compliant flooding attacks pose a serious threat to C-V2X safety applications. Through real-world testing, we show that high-rate UDP floods and oversized BSM floods individually and in combination can push system metrics well beyond safe operating thresholds, leading to delayed or entirely suppressed collision warnings. Securing C-V2X thus requires extending beyond traditional radio frequency (RF) protections to include the application and transport layer resilience against overwhelming but valid traffic patterns.

The results indicate that current security mechanisms, including those defined in the IEEE 1609 family security protocols), primarily address authentication, integrity, and RF-layer protections. They do not mitigate resource exhaustion caused by valid but overwhelming traffic(*35*) This exposes a gap in protocol and system-level defenses where authenticated, standards-compliant messages can still disrupt time-critical safety functions. Addressing this issue will require resilience improvements at the transport and the application layers, complementing existing IEEE 1609 protections.

Future work should explore multi-vector attacks that combine spoofing, jamming, and protocol-compliant flooding to provide a broader security assessment. Developing intrusion detection and prevention mechanisms that extend the IEEE 1609 security framework to handle resource exhaustion will

be key. Large-scale field trials under varied traffic conditions and across different OBU platforms, as well as studies on other safety applications, such as cooperative braking and intersection collision avoidance, are necessary next steps. Ultimately, protocol enhancements and updated standardization efforts will be essential to ensure connected vehicle safety application remain reliable under stealthy flooding attacks in real-world deployments.

AUTHOR CONTRIBUTIONS

The authors confirm their contribution to the paper: J. Tine, M. Aldeen, A. Enan, M.S. Salek, L. Cheng, M. Chowdhury. All authors reviewed the results and approved the final version of the manuscript.

REFERENCES

1. Ficzere, D., P. Varga, A. Wippelhauser, H. Hejazi, O. Csernyava, A. Kovács, and C. Hegedűs. Large-Scale Cellular Vehicle-to-Everything Deployments Based on 5G—Critical Challenges, Solutions, and Vision towards 6G: A Survey. *Sensors*, Vol. 23, No. 16, 2023, p. 7031. https://doi.org/10.3390/s23167031.

2. Mansouri, A., V. Martinez, and J. Harri. A First Investigation of Congestion Control for LTE-V2X Mode 4. Presented at the 2019 15th Annual Conference on Wireless On-demand Network Systems and Services (WONS), Wengen, Switzerland, 2019.

3. Enan, A., A. A. Mamun, J. M. Tine, J. Mwakalonge, D. A. Indah, G. Comert, and M. Chowdhury. Basic Safety Message Generation through a Video-Based Analytics for Potential Safety Applications. *ACM Journal on Autonomous Transportation Systems*, Vol. 1, No. 4, 2024, pp. 1–26. https://doi.org/10.1145/3643823.

4. Zadobrischi, E., and M. Dimian. Vehicular Communications Utility in Road Safety Applications: A Step toward Self-Aware Intelligent Traffic Systems. *Symmetry*, Vol. 13, No. 3, 2021, p. 438. https://doi.org/10.3390/sym13030438.

5. Kutila, M., K. Kauvo, P. Pyykonen, X. Zhang, V. G. Martinez, Y. Zheng, and S. Xu. A C-V2X/5G Field Study for Supporting Automated Driving. Presented at the 2021 IEEE Intelligent Vehicles Symposium (IV), Nagoya, Japan, 2021.

6. Gonzalez-Martin, M., M. Sepulcre, R. Molina-Masegosa, and J. Gozalvez. Analytical Models of the Performance of C-V2X Mode 4 Vehicular Communications. *IEEE Transactions on Vehicular Technology*, Vol. 68, No. 2, 2019, pp. 1155–1166. https://doi.org/10.1109/TVT.2018.2888704.

7. Gonzalez-Martin, M., M. Sepulcre, R. Molina-Masegosa, and J. Gozalvez. Analytical Models of the Performance of C-V2X Mode 4 Vehicular Communications. *IEEE Transactions on Vehicular Technology*, Vol. 68, No. 2, 2019, pp. 1155–1166. https://doi.org/10.1109/TVT.2018.2888704.

8. McCarthy, B., and A. O'Driscoll. Congestion Control in the Cellular-V2X Sidelink. https://arxiv.org/abs/2106.04871. Accessed July 28, 2025.

9. Chihi, H., and R. Boualegue. Congestion Control Investigation into 5G V2V. https://www.researchsquare.com/article/rs-312939/v1. Accessed July 31, 2025.

10. Balador, A., E. Cinque, M. Pratesi, F. Valentini, C. Bai, A. A. Gómez, and M. Mohammadi. Survey on Decentralized Congestion Control Methods for Vehicular Communication. *Vehicular Communications*, Vol. 33, 2022, p. 100394. https://doi.org/10.1016/j.vehcom.2021.100394.

11. Sepulcre, M., J. Mira, G. Thandavarayan, and J. Gozalvez. Is Packet Dropping a Suitable Congestion Control Mechanism for Vehicular Networks? Presented at the 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), Antwerp, Belgium, 2020.

12. Trkulja, N., D. Starobinski, and R. A. Berry. Denial-of-Service Attacks on C-V2X Networks. http://arxiv.org/abs/2010.13725. Accessed July 28, 2025.

13. Twardokus, G., and H. Rahbari. Vehicle-to-Nothing? Securing C-V2X Against Protocol-Aware DoS Attacks. Presented at the IEEE INFOCOM 2022 - IEEE Conference on Computer Communications, London, United Kingdom, 2022.

14. Fouda, A., R. Berry, and I. Vukovic. Interleaved One-Shot Semi-Persistent Scheduling for BSM Transmissions in C-V2X Networks. http://arxiv.org/abs/2110.00056. Accessed July 28, 2025.

15. 1609.3-*2020 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE)--Networking - Redline*. IEEE, S.l., 2021.

16. 1609.2-*2016 - IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages*. IEEE, S.l., 2016.

17. Silva, T. R., T. D. S. Correia, J. F. M. Sarubbi, and F. V. C. Martins. Roadside Units Deployment in Hybrid VANETs with Synchronous Communication. Presented at the 2018 IEEE 87th Vehicular Technology Conference (VTC Spring), Porto, 2018.

18. Wang, J., I. Topilin, A. Feofilova, M. Shao, and Y. Wang. Cooperative Intelligent Transport Systems: The Impact of C-V2X Communication Technologies on Road Safety and Traffic Efficiency. *Sensors*, Vol. 25, No. 7, 2025, p. 2132. https://doi.org/10.3390/s25072132.

19. Dapa, K. B. S. A., G. Point, S. Bensator, and F. E. Boukour. Vehicular Communications Over OFDM Radar Sensing in the 77 GHz mmWave Band. *IEEE Access*, Vol. 11, 2023, pp. 4821–4829. https://doi.org/10.1109/ACCESS.2023.3235199.

20. Shtaiwi, E., Abdelhadi, H. Li, Z. Han, and H. V. Poor. Orthogonal Time Frequency Space for Integrated Sensing and Communication: A Survey. http://arxiv.org/abs/2402.09637. Accessed July 28, 2025.

21. Prokes, A., J. Blumenstein, J. Vychodil, T. Mikulasek, R. Marsalek, E. Zochmann, H. Groll, C. F. Mecklenbrauker, T. Zemen, A. Chandra, H. Hammoud, and A. F. Molisch. Multipath Propagation Analysis for Vehicle-to-Infrastructure Communication at 60 GHz. Presented at the 2019 IEEE Vehicular Networking Conference (VNC), Los Angeles, CA, USA, 2019.

22. Shah, G., M. Zaman, M. Saifuddin, B. Toghi, and Y. Fallah. Scalable Cellular V2X Solutions: Large-Scale Deployment Challenges of Connected Vehicle Safety Networks. *Automotive Innovation*, Vol. 7, No. 3, 2024, pp. 373–382. https://doi.org/10.1007/s42154-023-00277-6.

23. Paranjothi, A., M. S. Khan, and S. Zeadally. A Survey on Congestion Detection and Control in Connected Vehicles. *Ad Hoc Networks*, Vol. 108, 2020, p. 102277. https://doi.org/10.1016/j.adhoc.2020.102277.

24. Toghi, B., M. Saifuddin, H. N. Mahjoub, M. O. Mughal, Y. P. Fallah, J. Rao, and S. Das. Multiple Access in Cellular V2X: Performance Analysis in Highly Congested Vehicular Networks. Presented at the 2018 IEEE Vehicular Networking Conference (VNC), Taipei, Taiwan, 2018.

25. Tabassum, M., and A. Oliveira. Collision Probabilities Between User Equipment Using 5G NR Sidelink Time-Domain-Based Resource Allocation in C-V2X. *Electronics*, Vol. 14, No. 4, 2025, p. 751. https://doi.org/10.3390/electronics14040751.

26. Fouda, A., R. Berry, and I. Vukovic. Study of BSM Inter-Packet Gap Tails in C-V2X Networks. http://arxiv.org/abs/2311.16904. Accessed July 28, 2025.

27. Kenney, J. B. Dedicated Short-Range Communications (DSRC) Standards in the United States. *Proceedings of the IEEE*, Vol. 99, No. 7, 2011, pp. 1162–1182. https://doi.org/10.1109/JPROC.2011.2132790.

28. Petit, J., and S. E. Shladover. Potential Cyberattacks on Automated Vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 2014, pp. 1–11. https://doi.org/10.1109/TITS.2014.2342271.

29. Abdollahi Biron, Z., S. Dey, and P. Pisu. Real-Time Detection and Estimation of Denial of Service Attack in Connected Vehicle Systems. *IEEE Transactions on Intelligent Transportation Systems*, Vol. 19, No. 12, 2018, pp. 3893–3902. https://doi.org/10.1109/TITS.2018.2791484.

30. Boban, M., A. Kousaridas, K. Manolakis, J. Eichinger, and W. Xu. Connected Roads of the Future: Use Cases, Requirements, and Design Considerations for Vehicle-to-Everything Communications. *IEEE Vehicular Technology Magazine*, Vol. 13, No. 3, 2018, pp. 110–123. https://doi.org/10.1109/MVT.2017.2777259.

31. Garcia, M. H. C., A. Molina-Galan, M. Boban, J. Gozalvez, B. Coll-Perales, T. Şahin, and A. Kousaridas. A Tutorial on 5G NR V2X Communications. *IEEE Communications Surveys & Tutorials*, Vol. 23, No. 3, 2021, pp. 1972–2026. https://doi.org/10.1109/COMST.2021.3057017.

32. Fouda, A., R. Berry, and I. Vukovic. HARQ Retransmissions in C-V2X: A BSM Latency Analysis. https://arxiv.org/abs/2311.16983. Accessed July 28, 2025.

33. McCarthy, B., A. Burbano-Abril, V. R. Licea, and A. O'Driscoll. OpenCV2X: Modelling of the V2X Cellular Sidelink and Performance Evaluation for Aperiodic Traffic. https://arxiv.org/abs/2103.13212. Accessed July 28, 2025.

34. Ma, J., J. Li, Z. Gong, and H. Huang. An Adaptive Multi-Staged Forward Collision Warning System Using a Light Gradient Boosting Machine. *Information*, Vol. 13, No. 10, 2022, p. 483. https://doi.org/10.3390/info13100483.

35. Bitsikas, E., and A. Ranganathan. Security Analysis of 5G NR Device-to-Device Sidelink Communications. http://arxiv.org/abs/2502.16650. Accessed Aug. 2, 2025.