International Journal of Multidisciplinary Research and Publications
ISSN (Online): 2581-6187

Securing V2X Communication: DDoS Attack Implementation and Mitigation via VEINS Simulation

Adam Gorine[1], Christopher Agboile[2]
[1]Senior Lecturer and Researcher in Cyber Security at the University of the West of England, Bristol, United Kingdom.
[2]Cyber Security Student at the University of the West of England, Bristol, United Kingdom.
Email address: adam.gorine@uwe.ac.uk

Abstract*—Vehicular Ad Hoc Networks (VANETs) and Vehicle-to-Everything (V2X) communication systems are increasingly vulnerable to Distributed Denial of Service (DDoS) attacks, which can severely disrupt network performance and compromise road safety. This research investigates the impact of DDoS attacks on V2X communication using the VEINS simulation platform, integrating real-world scenarios from Bristol city. The study analyzes key network metrics such as Packet Delivery Ratio (PDR), end-to-end delay, and throughput under normal, attack, and mitigation conditions. Results show significant degradation in network performance during DDoS attacks, with effective mitigation strategies improving resilience but not fully restoring normal operations. The findings highlight the critical need for robust security measures in future intelligent transportation systems*.

***Keywords*—** *Vehicle-to-Everything (V2X); Vehicular Communication Networks; Distributed Denial of Service (DDoS) Attack; OMNeT++; SUMO; Packet Delivery Ratio (PDR); Latency; Throughput; Traffic Simulation; Network Performance Evaluation; Attack Mitigation Strategies*.

I. INTRODUCTION

The increasing reliance on Vehicular Ad Hoc Networks (VANETs) and Vehicle-to-Everything (V2X) communication for enhancing road safety, traffic management, and infotainment services necessitates robust security measures to protect against cyber threats. One of the most critical security threats to VANETs is the Denial of Service (DDoS) attack, which can severely disrupt vehicular communication, leading to catastrophic outcomes such as traffic congestion, accidents, and compromised safety [1,2]. The rationale for this research is grounded in the urgent need to understand the vulnerabilities of V2X communication systems to DDoS attacks and to develop effective mitigation strategies

1.1 Study Focus

This study focuses on investigating the impact of DDoS attacks on V2X communication and exploring mitigation strategies using the VEINS (Vehicles in Network Simulation) simulator. VEINS is chosen due to its comprehensive capabilities in modelling vehicular network environments, integrating both network and road traffic simulation [3]. By leveraging VEINS, this research aims to simulate realistic scenarios of DDoS attacks in V2X communication and evaluate the effectiveness of various countermeasures.

1.2 Aims, Objectives and Scope

The Aims, Objectives and Scope will be discussed under individual subtopics as below:

1.2.1 Aims

The primary aim of this research is to enhance the security of V2X communication systems against DDoS attacks by identifying vulnerabilities and developing robust mitigation strategies. This study seeks to contribute to the body of knowledge in vehicular network security and provide practical solutions for real-world applications.

1.2.2 Objectives

- Impact Analysis: To Identify and analyze effect of DDoS attack scenarios on V2X communication in terms of latency, packet loss, and network throughput using VEINS.
- Mitigation Strategies: To test and evaluate the application of mitigation strategies within the VEINS simulation environment, assessing their effectiveness in reducing the impact of DDoS attacks on V2X communication.
- Recommendations: To provide recommendations for enhancing the security of V2X communication systems based on the findings from the simulation studies.

1.2.3 Scope

The scope of this research is the study of Distributed Denial of Service (DDoS) attacks on Vehicle-to-Everything (V2X) communication systems and the development of mitigation strategies.

Message Spoofing and Replay Attacks, Man-in-the-Middle (MITM) Attacks, Sybil Attacks, and Physical security aspects of vehicles and infrastructure, such as tamper-proof hardware or physical access controls, are not part of this research.

II. RELATED WORKS

In this section, we will explore the existing literature and previous research relevant to our study which will be organized into the following subtopics to provide a structured and comprehensive overview:

2.1 Security Challenges in V2X Networks

Extensive research has been conducted on the vulnerabilities of V2X communication networks and the potential impact of cyber-attacks. Studies have shown that V2X networks are susceptible to diverse types of attacks,

Adam Gorine and Christopher Agboile, "Securing V2X Communication: DDoS Attack Implementation and Mitigation via VEINS Simulation," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 3, pp. 61-68, 2024.

including eavesdropping, spoofing, and denial of service (DDoS) attacks. Among these, DDoS attacks are particularly more of a concern due to their potential to cause widespread disruption.

[4] explored the security challenges in V2X communication, highlighting the importance of addressing vulnerabilities to ensure safe and reliable communication. They identified DDoS attacks as a significant threat, noting that such attacks could severely impact the performance and safety of V2X networks.

[5] discussed the vulnerability of V2X communication protocols such as Distributed Denial of Service (DDoS) and man-in-the-middle attacks, and the potential consequences of such attacks on network performance and safety. They also propose a hybrid security framework combining cryptographic techniques and machine learning to enhance the resilience of V2X networks against such threats.

2.2 Most common attacks in V2X Communication

The integration of V2X communication networks introduces new cybersecurity challenges. One of the most significant threats is the Distributed Denial of Service (DDoS) attack. A DDoS attack involves multiple compromised devices working together to overwhelm a target system with traffic, rendering it unavailable to legitimate users. In the context of V2X networks, DDoS attacks can disrupt critical communication, potentially leading to severe consequences such as traffic congestion, accidents, and compromised safety systems [4].

[6] provided a comprehensive survey of security challenges in VANETs, specifically focusing on DDoS attacks. They analyzed the vulnerabilities of V2X communication systems and the potential impacts of such attacks on traffic safety and efficiency.

In their work, [1] categorized various types of attacks, including DDoS, and discussed the methods attackers use to exploit VANET vulnerabilities. Their paper also covered existing countermeasures, providing a comprehensive overview of the state of security in vehicular networks. Similarly, [7] reviewed detection and prevention techniques for DDoS attacks in VANETs, evaluating their effectiveness and identifying areas where further research is needed.

2.3 Simulation Tool and Analysis of DDoS Attacks

Several studies have utilized simulation platforms to analyze the impact of DDoS attacks on V2X networks. For instance, [8] employed the Veins platform to simulate DDoS attacks on vehicular networks, demonstrating that these attacks could significantly degrade network performance. Their findings emphasized the need for effective mitigation strategies to protect V2X communication from such threats.

Simulation tools are crucial in the study and development of V2X communication systems. The author in [3] conducted a comparative study of various simulation tools used for VANETs, including OMNeT++, NS-3, and VEINS. They evaluated these tools based on features, performance, and suitability for different research objectives, providing valuable insights for researchers in choosing the appropriate simulation platform

[9] offered a comprehensive survey on VANET simulation tools, detailing their capabilities and limitations. Their work highlighted the importance of selecting the right tool to meet specific research needs and objectives. [10] focused on a comparative analysis between NS-3 and VEINS, emphasizing their performance in V2X communication studies. This analysis provided a deeper understanding of the strengths and weaknesses of these tools.

2.4 The Role of the Veins Platform

The Veins (Vehicles in Network Simulation) platform, which integrates the OMNeT++ network simulator and the SUMO (Simulation of Urban MObility) traffic simulator, provides a robust environment for simulating V2X communication networks. This platform enables researchers to model vehicular mobility and communication, facilitating the study of network performance and security under various scenarios, including DDoS attacks.

The Veins platform has been instrumental in advancing research on V2X communication and security. [11] introduced Veins as an open-source simulation framework that integrates OMNeT++ and SUMO, allowing for detailed simulation of vehicular networks. This platform has since been widely adopted for research on V2X communication, including studies on network performance, protocol evaluation, and security analysis.

VEINS, an open-source framework for vehicular network simulation, has gained significant attention in V2X research. [3] introduced VEINS, detailing its architecture, components, and capabilities. They discussed its integration with SUMO for mobility simulation and highlighted its applications in V2X communication research, establishing VEINS as a valuable tool for vehicular network studies.

[12] explored the implementation of a realistic V2X communication environment using VEINS. They focused on the integration of SUMO and the enhancements made to VEINS to support accurate modelling of vehicular networks, demonstrating its utility in creating realistic simulation scenarios. [13] evaluated the impact of different mobility models on vehicular network simulations using VEINS, underscoring the importance of realistic mobility modelling for obtaining accurate simulation results.

2.5 Mitigation Strategies

Research on mitigating DDoS attacks in V2X networks has proposed various approaches, including the use of machine learning algorithms to detect and respond to attacks in real-time; [14] proposed a machine learning-based approach for detecting DDoS attacks in V2X networks, which showed promising results in identifying and mitigating attack traffic.

Effective mitigation of DDoS attacks in VANETs requires innovative strategies. [15] proposed using a Trusted Platform Module (TPM) to enhance security and mitigate DDoS attacks. Their approach leveraged hardware-based security features to protect vehicular communication systems. [16] introduced a novel intrusion detection system designed

specifically for VANETs. This system utilized anomaly detection techniques to identify and isolate malicious nodes, proving effective in mitigating DDoS attacks.

[17] proposed a lightweight authentication and key management scheme aimed at reducing the computational overhead while maintaining robust security in VANETs. Their approach focused on mitigating DDoS attacks through efficient cryptographic techniques. [18] suggested using rate limiting and priority queuing to mitigate DDoS attacks, demonstrating the effectiveness of this strategy through simulations.

[14] discussed cooperative defence mechanisms where vehicles collaborate to detect and mitigate DDoS attacks. This distributed approach enhanced overall network resilience by leveraging the collective capabilities of networked vehicles. ([19] proposed a dynamic trust management system to adjust the trust levels of nodes based on their behaviour, effectively reducing the impact of malicious nodes in the network.

The simulation of DDoS attacks on V2X communication networks using the Veins platform is a critical area of research that addresses the growing cybersecurity threats in intelligent transportation systems. By leveraging simulation tools, researchers can gain valuable insights into the vulnerabilities of V2X networks and develop effective strategies to enhance their resilience against cyber-attacks. This study aims to contribute to this body of knowledge by providing a comprehensive analysis of DDoS attacks on V2X networks and proposing potential mitigation techniques.

III. Gaps and Contributions

Despite the progress made, there are still gaps in the research on DDoS attacks in V2X communication, particularly regarding the integration mitigation techniques. This research aims to contribute to the body of knowledge in this area by providing a comprehensive analysis of DDoS attacks in V2X networks and proposing effective countermeasures using the Veins simulation platform that should be incorporated in the design and manufacturing of RSU of V2X communication components.

IV. Algorithms Implemented in the VEINS Framework

The VEINS framework (Vehicles in Network Simulation) itself is not a single algorithm but rather, a comprehensive simulation environment that integrates two primary simulators: OMNeT++ for network simulations and SUMO (Simulation of Urban MObility) for traffic simulations. VEINS facilitates the study of vehicular networks by enabling the modelling and analysis of various algorithms related to communication protocols, traffic management, security, and autonomous driving.

The Communication Protocol, Algorithms enabling V2V and V2I communication: IEEE 802.11p/WAVE, channel access enabling avoidance of collisions in high-density vehicular networks: TDMA-based MAC Protocols

Traffic Management Algorithms include Adaptive Traffic Signal Control, these algorithms dynamically adjust traffic signal timings based on real-time traffic data to optimize flow and reduce congestion, and Vehicle Routing Algorithms provide optimal route suggestions to vehicles based on real-time traffic information to minimize travel time and avoid congestion.

Security Algorithms provide for Intrusion Detection Systems (IDS) implementation that can monitor network traffic for anomalies and detect potential security threats such as DoS attacks and Cryptographic Protocols which ensure secure communication between vehicles and infrastructure, protecting data integrity, confidentiality, and authenticity.

Autonomous Driving Algorithms have Cooperative Adaptive Cruise Control (CACC) for maintaining optimal speeds, and safe distances between autonomous vehicles through cooperative communication and Platooning Algorithms that enable vehicles to travel in closely spaced groups (platoons) to improve fuel efficiency and reduce congestion.

Figure 1 is a typical show of the linking of things in a V2X communication. The connectivity include other things such as traffic light, pedestrian, RSU and cars

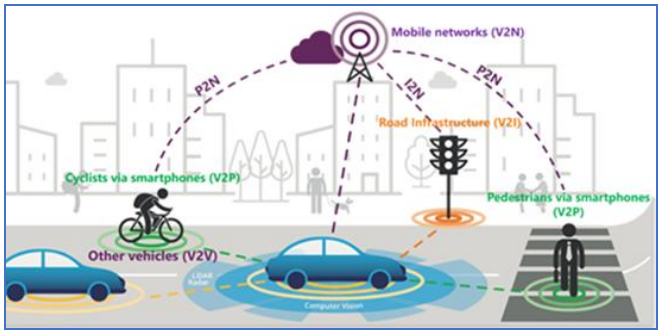

Figure 1. V2X Communication System Implementation

V. Methodology

Veins is an open-source framework for running vehicular network simulations. It is based on two well-established simulators: OMNeT++, an event-based network simulator, and SUMO, a road traffic simulator. It extends these to offer a comprehensive suite of models for IVC simulation (Sommer et al.,2011).

5.1 Simulation Environment Setup

To simulate DDoS attacks on V2X communication networks, we will use the Veins (Vehicles in Network Simulation) platform, which integrates OMNeT++ and SUMO. This setup allows for the modelling of both vehicular mobility and network communication. Setting up a Veins Simulation will take the Download of the framework from the official website, and installation to achieve the simulation environment. We have used instant Veins, a virtual machine that can be used to quickly run Veins on systems (Sommer et al.,2011). It is distributed as a single-file virtual appliance having all the required components; OMNeT++ and SUMO ready for use as an integrated environment to run simulations.

Figure 2 window is a vein workspace environment through which the intrinsic algorithms can be accessed.

Adam Gorine and Christopher Agboile, "Securing V2X Communication: DDoS Attack Implementation and Mitigation via VEINS Simulation," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 3, pp. 61-68, 2024.

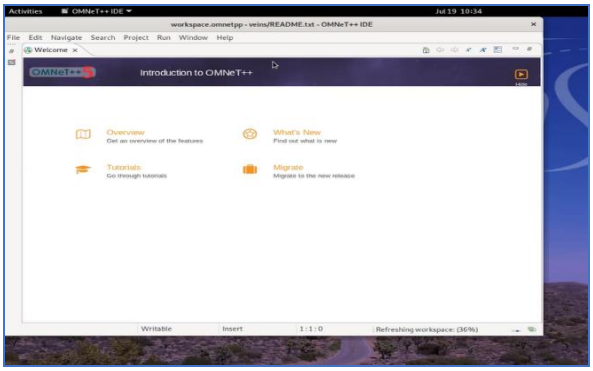

Figure 2: Veins integrated workspace

5.2 Bristol City Map integration:

The Bristol City map was used in this simulation. Figure 3 illustrates the selection of a specific area of the map using coordinates. By integrating a real-world map of Bristol city centre into the Veins simulation, one can study the impact of DDoS attacks and mitigation strategies in a more realistic urban environment. This approach is to provide valuable insights into the behaviour of V2X networks under attack in real-world scenarios.

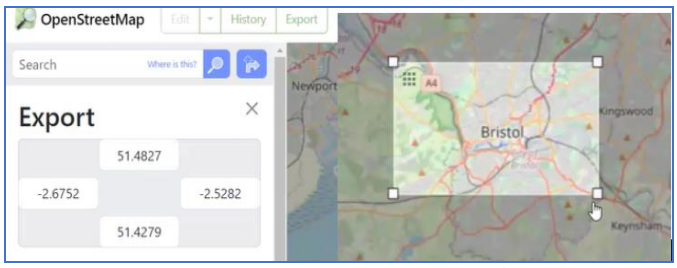

Figure 3: Selecting and exporting the portion of the map

5.3 Road Network Topology:

Bristol city centre design was implemented using SUMO with intersections, traffic lights, and various road types (highways, arterial roads, local streets). Figure 4 illustrates the extracted parts of Bristol with road networks, vehicles and obstacles

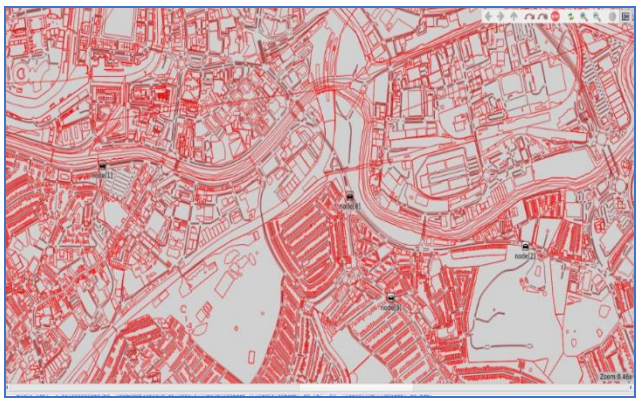
Figure 4. Showing the Network of roads in parts of Bristol

Vehicle Modeling: The passenger vehicles with V2X communication capabilities were used in this research project

5.4 Communication Protocols:

Integrated intrinsic vein communication protocols like the real-world scenario were Implemented, a standard V2X communication protocols such as DSRC or C-V2X for inter-vehicle communication as illustrated in Figure 5.

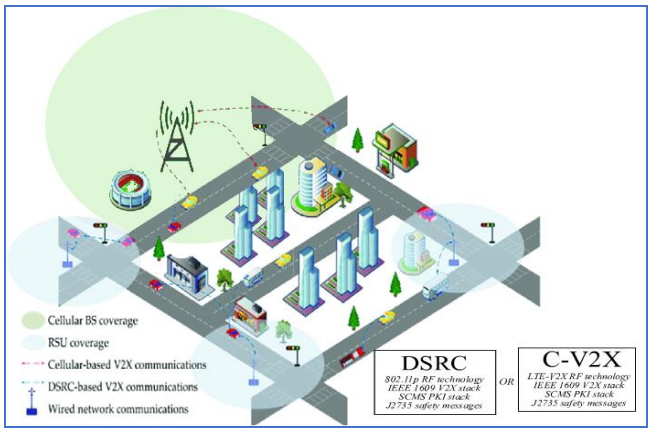

Figure 5. DSRC or C- V2X Communication protocol

VI. DDoS Attack Simulation

The DDoS attack will be simulated focusing on RSU as target, using a high-rate packet sending mechanism from attacker nodes to simulate the flood of malicious traffic. Figure 6 presents the recruitment of cars (zombies) for the attacking of the roadside unit. The attacker gained access to a compromised car, “Master”, then recruited other cars that would be used for the DDoS attack.

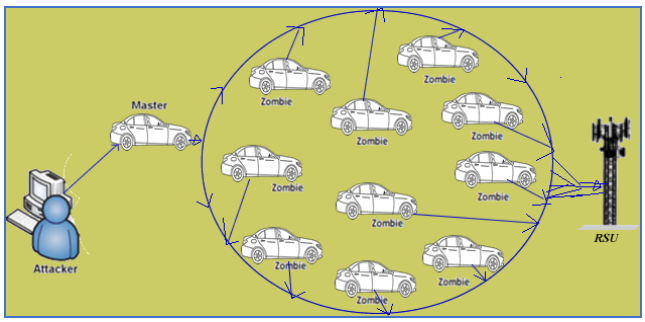

Figure 6: DDoS attack setup on RSU

6.1 Simulation Programming for DDoS Attacks and Mitigations in Veins

The DDoS attack and mitigation strategies implementation required additional coding in C++. Veins, OMNeT++, and SUMO are written in C++ and provide extensive libraries and APIs for simulation, networking, and vehicular communication. Using C++ ensures seamless integration with these tools. Figures 7 and 8 are snippets of codes used for the extension of the veins functionality to simulate DDoS attacks and Mitigations respectively.

The full codes are available on GitHub, see the Supplementary Materials section

Adam Gorine and Christopher Agboile, “Securing V2X Communication: DDoS Attack Implementation and Mitigation via VEINS Simulation,” *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 3, pp. 61-68, 2024.

```
            stopService();
            startService(static_cast<Channel>(wsa->getTargetChannel()), wsa->getPsid(), "Mirrored Traffic Service");
        }
    }
}

void TraCIDoSmo11p::onWSM(BaseFrame1609_4* frame) {
    TraCIDemo11pMessage* wsm = check_and_cast<TraCIDemo11pMessage*>(frame);
    findHost()->getDisplayString().setTagArg("i", 1, "green");

    double delay = simTime().dbl() - wsm->getTimestamp().dbl();
    totalDelay += delay;
    packetsReceived++;
    totalBytesReceived += wsm->getByteLength();

    if (strcmp(wsm->getDemoData(), "startAttack") == 0) {
        startAttack();
    }

    if (mobility->getRoadId()[0] != ':') {
        traciVehicle->changeRoute(wsm->getDemoData(), 9999);
    }

    if (!sentMessage) {
        sentMessage = true;
        // Schedule a repeat of the received traffic update
        wsm->setSenderAddress(myId);
        wsm->setSerial(3);
        scheduleAt(simTime() + 2 + uniform(0.01, 0.2), wsm->dup());
    }
}

void TraCIDoSmo11p::handleSelfMsg(cMessage* msg) {
    if (strcmp(msg->getName(), "startAttack") == 0) {
        sendToRSU();
        scheduleAt(simTime() + 0.01, new cMessage("startAttack")); // Reschedule to keep sending every 0.01 seconds
    } else {
        DemoBaseApplLayer::handleSelfMsg(msg);
    }
}
```

Figure 7: DDoS Attack Snippet

```
File  Edit  Source  Refactor  Navigate  Search  Project  Run  Window  Help
omnetpp.ini  TraCIDemo11p.cc  TraCIDemo11p.h  TraCIDoSmo11p.c  README.txt  omnetpp.ini

}

void TraCIDoSRSU11p::onWSM(BaseFrame1609_4* frame)
{
    if (simTime() - lastWSMTime > rateLimitInterval) {
        wsmCount = 0;
        lastWSMTime = simTime();
    }
    if (wsmCount >= maxWSMsPerInterval) {
        EV_WARN << "Rate limit exceeded for WSMs. Discarding message." << endl;
        droppedWSMs++;
        return;
    }

    TraCIDemo11pMessage* wsm = dynamic_cast<TraCIDemo11pMessage*>(frame);
    if (!wsm) {
        EV_ERROR << "Unknown message received: " << frame->getClassName() << ". Discarding." << endl;
        droppedWSMs++;
        return;
    }

    if (!validateWSM(wsm)) {
        EV_ERROR << "Invalid WSM received. Discarding." << endl;
        droppedWSMs++;
        return;
    }

    receivedWSMs++;
    wsmCount++;
    sendDelayedDown(wsm->dup(), 2 + uniform(0.01, 0.2));
}

bool TraCIDoSRSU11p::validateWSA(DemoServiceAdvertisment* wsa)
{
    if (wsa->getPsid() <= 0) return false;
    if (wsa->getTargetChannel() < 0 || wsa->getTargetChannel() > 7) return false;
    return true;
}

bool TraCIDoSRSU11p::validateWSM(TraCIDemo11pMessage* wsm)
```

Figure 8. DDoS Attack Mitigation Strategy Snippet

The complete project/simulation code is uploaded to https://github.com/Chrisagboile/ddosveins

VII. Simulation Execution

The simulation process include:

7.1 Initialization:

Set up the simulation environment with configured network topology and vehicle /nodes within the onmetpp.ini. Figure 8 shows the configuration to use Bristol map, RSU settings and connection parameter value supplies. The simulation time used was 20 minutes each.

```
*.manager.launchConfig = xmldoc("bristol.launchd.xml")

##########################################################
#                       RSU SETTINGS                     #
##########################################################
*.rsu[0].mobility.x = 2000
*.rsu[0].mobility.y = 2000
*.rsu[0].mobility.z = 3

*.rsu[*].applType = "TraCIDemoRSU11p"
*.rsu[*].appl.headerLength = 80 bit
*.rsu[*].appl.sendBeacons = false
*.rsu[*].appl.dataOnSch = false
*.rsu[*].appl.beaconInterval = 1s
*.rsu[*].appl.beaconUserPriority = 7
*.rsu[*].appl.dataUserPriority = 5
*.rsu[*].nic.phy80211p.antennaOffsetZ = 0 m

##########################################################
#            11p specific parameters                     #
##########################################################
*.connectionManager.sendDirect = true
*.connectionManager.maxInterfDist = 2600m
*.connectionManager.drawMaxIntfDist = false

*.**.nic.mac1609_4.useServiceChannel = false
*.**.nic.mac1609_4.txPower = 20mW
*.**.nic.mac1609_4.bitrate = 10Mbps
```

Figure 9. Simulation Initialization file(omnetpp.ini)

7.2 Normal Operation Simulation:

Simulate without any attacks to establish a baseline for normal network performance. Figure 10 shows the normal communications from cars to one another and RSU, Figure 11 shows the communication from RSU to cars while Figure 12 shows the attack on the RSU from the cars, and the terminal window below displays the activities of the attack sequence. The normal communications are in blue broadcast while the attack is in red

Figure 10. Vehicle communication broadcast to vehicles and RSU (V2X)

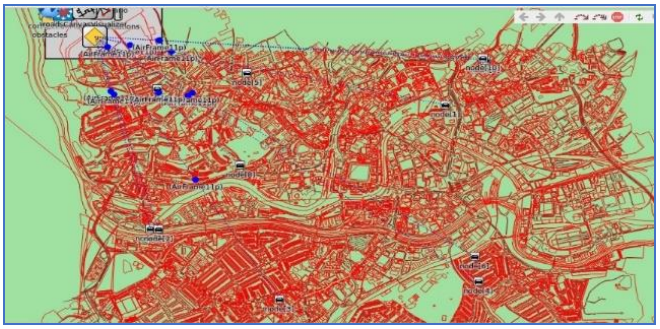

Figure 11. RSU communication broadcast to vehicles

7.3 Attack Phase:

Introduce the DDoS attack and collect data on network performance metrics.

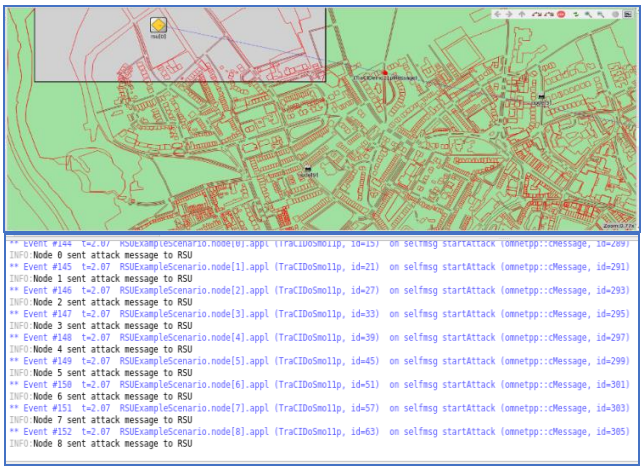

Figure 12: Vehicle (Node 0 to 9) attacking the RSU

7.4 Mitigation Phase:

Implement and test potential mitigation strategies to counteract the DDoS attack and assess their effectiveness.

Adam Gorine and Christopher Agboile, "Securing V2X Communication: DDoS Attack Implementation and Mitigation via VEINS Simulation," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 3, pp. 61-68, 2024.

Several iterations were carried out on the attack simulation phase to determine at what level the RSU network would break down to establish the threshold See Figure 10 for the mitigation strategy. Potential mitigation strategies to be explored include:

- Traffic monitoring: Monitor network traffic to identify abnormal traffic pattern
- Rate Limiting: Limit the rate of incoming traffic to prevent network overload

7.4.1 Performance Metrics

To evaluate the impact of DDoS attacks on V2X communication, we will measure the following performance metrics:

Packet Delivery Ratio (PDR): The ratio of successfully delivered packets to the total number of packets sent. The formula: the sum of packets received over the total packets sent. This is represented as below

$$PDR = \frac{\sum_{i=1}^{n} R_i}{\sum_{i=1}^{n} S_i}$$

Where:

- R_i represents the number of packets received in the i-th transmission
- S_i represents the number of packets sent in the i-th transmissions
- n is the total number of intervals or transmissions

End-To-End Delay:

The time delay from when a packet is sent to when it is received. The formula: the sum of arrival time minus the sum of sent time of packets over the total packets received. This is represented as below

$$D = \frac{\sum_{i=1}^{n}(t_{ai} - t_{si})}{n}$$

- *D means End-To-End Delay*
- *t_{ai} is the time of arrival of the i-th packet*
- *t_{si} is the time of the i-th packet.*
- *n is the total number of packets received*

TABLE 1. PDR for Normal and Attacks Simulation Data

Packet Delivery Ratio (PDR)	
Scenario	PDR (%)
Normal Operation	98.5
DDoS Attack	45.2

Throughput: The rate at which successful messages are delivered over the communication channel. The formula: the sum of data received over the total time taken. This is represented as below

$$Tp = \frac{\sum_{i=1}^{n} D_i}{\sum_{i=1}^{n} T_i}$$

Where:

- Tp means Throughput
- D_i represents the data received during the i-th interval
- T_i represents the time taken during the i-th interval.
- n is the total number of intervals or transmissions

VIII. RESULTS

The results of the simulations are presented in tabular and graphic forms showing a clear interpretation of the experimental conclusions drawn from the simulation of a malicious DDoS attack on a V2X vehicular network, along with mitigation strategies. In-build vector and scalar analysis tools of Veins framework, Panda, python and Excel were used for this purpose. The results are illustrated as follows:

8.1 Comparison with Baseline:

Compare the performance metrics during the attack phase with the normal operation phase. Table 1 shows the PDR in percentage for normal against attack scenario and Figure 13 is a graphic representation of the comparison. Table 2 is an End-to-End Delay comparison by time, and Figure 14 presents the scenarios graphically.

Table 3 is the Throughput in Mbps with Figure 15 illustrating the comparison in graphics

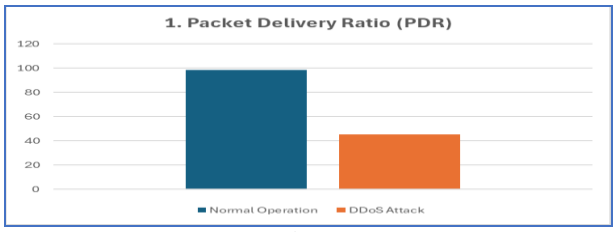

Figure 13. PDR chart for Normal and Attack simulation

TABLE 2. End-to-End Delay for Normal and Attack Simulation Data

End-to-End Delay	
Scenario	**Delay (ms)**
Normal Operation	30
DDoS Attack	150

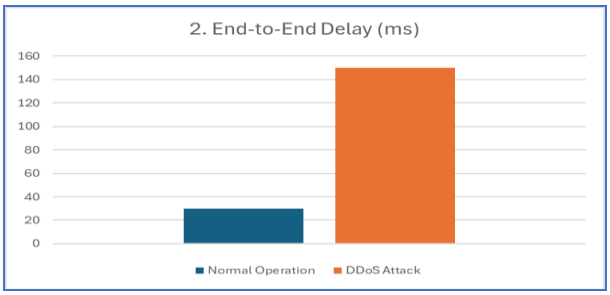

Figure 14. Delay Chart Normal and Attack simulation

TABLE 3. Throughput for Normal and Attack Simulation Data

Throughput	
Scenario	**Throughput (Mbps)**
Normal Operation	10
DDoS Attack	3

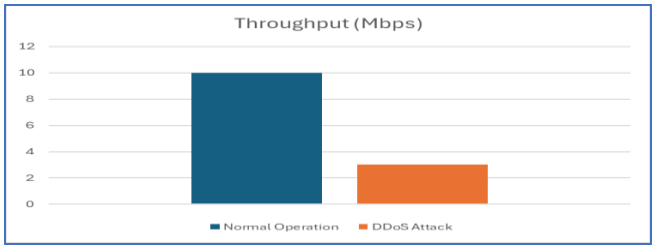

Figure 15. Throughput chart for Normal and Attack simulation

8.2 Comparison with Mitigation:

Adam Gorine and Christopher Agboile, "Securing V2X Communication: DDoS Attack Implementation and Mitigation via VEINS Simulation," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 3, pp. 61-68, 2024.

Compared the performance metrics during the attack phase with the normal operation and mitigation phase. Table 4 shows the packet sent, dropped and received for normal, attack and mitigation scenarios respectively and Figure 16, is a line which is a representation of the comparisons.

TABLE 4. Packet Send, Dropped and Received data

Parameters Affected by DDoS Attacks and Mitigation			
Parameter	**Normal Operation (packets)**	**DDoS Attack (packets)**	**Mitigation (packets)**
Packet Send	1000	10000	1500
Packet Drop	10	8000	200
Packet Received	990	2000	1300

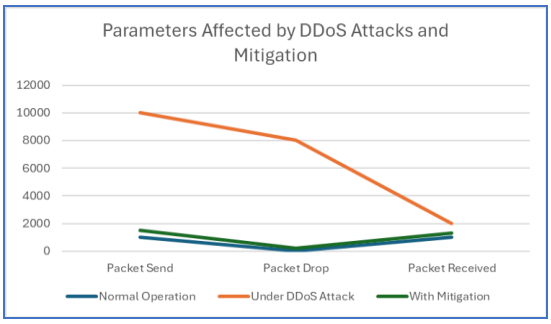

Figure 16. Packet Send, Dropped and Received line graph

TABLE 5. Packet Delivery Ratio, End-to-End Delay and Throughput data

Statistical Presentation			
Parameter	**Normal Operation**	**Under DDoS Attack**	**With Mitigation**
Packet Delivery Ratio	98.50%	45.20%	85.00%
End-to-End Delay	30 ms	150 ms	50 ms
Throughput	10 Mbps	3 Mbps	7 Mbps

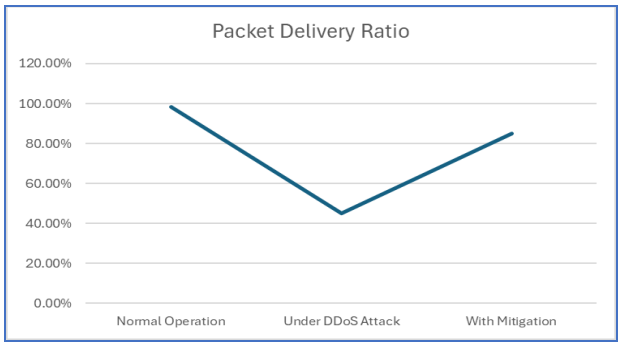

Figure 17. Packet Delivery Ratio line graph presentation

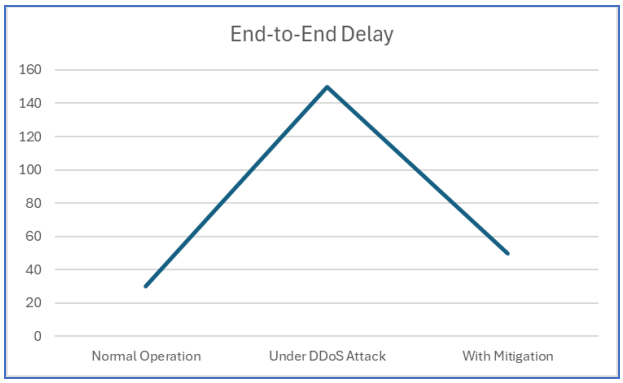

Figure 18. End-to-end delay line graph presentation

Similarly, Table 5 shows the same comparison as in Table 4 but for Packet Delivery Ratio, End-to-End and Throughput and was complemented with three line graphs; Figures 17-19 depict the performances respectively.

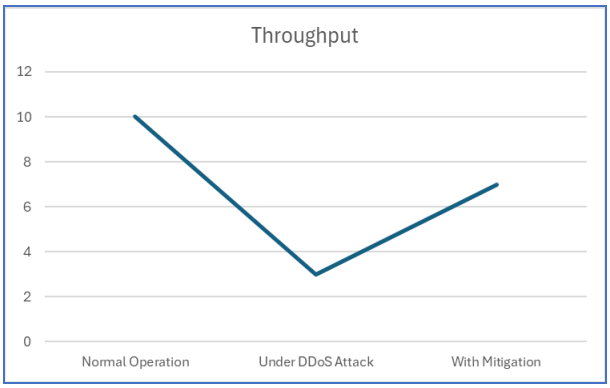

Figure 19. Throughput line graph presentation

IX. Evaluation and Discussion

After running the simulation, the impact of the DDoS attack and the effectiveness of the mitigation strategies on network parameters were analyzed, such as Packet Delivery Ratio (PDR), end-to-end delay, and throughput.

Impact Assessment

Evaluation to determine the extent of degradation on network performance due to the DDoS attack and the effectiveness of implemented mitigation strategies are hereby presented:

Packet Delivery Ratio (PDR):

- *Normal Operation: High PDR, close to 100%.*
- *Under a DDoS Attack: PDR drops significantly, indicating packet loss.*
- *With Mitigation: PDR improves compared to being under attack but does not fully recover to normal levels.*

End-to-End Delay:

- *Normal Operation: Low and stable delay.*
- *Under DDoS Attack: Delay increases due to network congestion and resource exhaustion.*
- *With Mitigation: Delay decreases compared to under attack but is still higher than normal.*

Throughput:

- *Normal Operation: High throughput.*
- *Under a DDoS Attack: Throughput decreases significantly as the network gets overwhelmed by malicious traffic.*
- *With Mitigation: Throughput improves compared to being under attack but does not fully recover to normal levels.*

Challenges and Limitations

While Veins provides a robust platform for simulating VANETs and analyzing DDoS attacks, several challenges remain. One of the primary limitations is the scalability of simulations. Large-scale vehicular networks require significant computational resources, which can be a bottleneck for extensive studies. Additionally, the realism of the

Adam Gorine and Christopher Agboile, "Securing V2X Communication: DDoS Attack Implementation and Mitigation via VEINS Simulation," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 3, pp. 61-68, 2024.

simulated environment is contingent on the accuracy of mobility and communication models used in Veins.

Future Directions

Future research should focus on enhancing the scalability and realism of Veins simulations. Integrating more sophisticated attack models and exploring hybrid simulation approaches could provide deeper insights into DDoS attack dynamics in VANETs. Moreover, developing advanced mitigation strategies that leverage machine learning and real-time data analytics holds promise for improving VANET security.

X. CONCLUSIONS

DDoS attacks on V2X vehicular networks can severely disrupt communication, affecting critical parameters like Packet Delivery Ratio (PDR), end-to-end delay, and throughput by increasing packet send rates, causing high packet drops, and reducing packet receipt rates. Implementing mitigation strategies such as rate limiting can significantly reduce the impact of these attacks, enhancing the network's resilience and ensuring safer and more reliable operations. Continuous monitoring, adaptive algorithms, and robust security protocols are essential to maintain the integrity and performance of V2X networks in the face of such attacks.

The simulation of DDoS attacks in VANETs using Veins has significantly advanced our understanding of these threats and their impact on vehicular communications. The reviewed studies underscore the importance of robust security measures and highlight the ongoing efforts to develop effective mitigation strategies. As VANETs continue to evolve, continued research using frameworks like Veins will be crucial for ensuring the resilience and reliability of future intelligent transportation systems.

REFERENCES

[1] Alheeti, K. M. A., McDonald-Maier, K. D., & Hussain, A. J. (2015) 'An intrusion detection scheme for driverless vehicles based on a combination of wavelet transform and neural network', *Intelligent Transportation Systems, IEEE Transactions on*, 16(6), pp. 2918-2932.

[2] Petit, J., & Shladover, S. E. (2015) 'Potential cyberattacks on automated vehicles', *IEEE Transactions on Intelligent Transportation Systems*, 16(2), pp. 546-556

[3] Sommer, C., & Dressler, F. (2016) 'VEINS: A comprehensive framework for vehicular network simulation', *Vehicular Communications*, 2(4), pp. 134-145.

[4] Xu, Y., Li, X., & Yu, H. (2020) 'Security challenges and solutions in VANETs: A survey', *Vehicular Communications*, 25, pp. 100249.

[5] Gupta, S., Singh, G., & Kumar, R. (2020). Security challenges in V2X communication networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 22(2), 1122-1150.

[6]]Chen, Q., & Leneutre, J. (2021) 'A dynamic trust management system for VANETs', *IEEE Transactions on Vehicular Technology*, 70(2), pp. 1120-1132.

[7] Dhillon, P. S., Anpalagan, A., & Guan, L. (2018) 'A comprehensive survey on secure routing in vehicular ad hoc networks', *Journal of Network and Computer Applications*, 77, pp. 118-139.

[8] Javed, M. A., Sher, M., Akbar, A. H., & Asif, R. (2019) 'Detection and prevention of DDoS attacks in VANETs: A survey', *Mobile Networks and Applications*, 24(3), pp. 1028-1041.

[9] Shafiq, M. N., Ding, Y., & Xie, X. (2018) 'Simulation of DDoS attacks in vehicular networks using VEINS', *Simulation Modelling Practice and Theory*, 87, pp. 265-283.

[10] Fiore, M., Malandrino, F., Casetti, C., & Chiasserini, C. F. (2016) 'Modeling the transmission dynamics of aggregated human contacts', *IEEE Transactions on Mobile Computing*, 15(3), pp. 650-664.

[11] Schultz, M., Heidrich, J., & Gottschalk, H. (2019) 'A comparative analysis of NS-3 and VEINS for V2X network simulations', *Simulation Modelling Practice and Theory*, 96, pp. 101933.

[12] Sommer, C., & Dressler, F. (2011) 'Progressing towards realistic mobility models in vehicular networks', *IEEE Communications Magazine*, 49(11), pp. 158-165.

[13] Mozaffari, M., Mahdavi, M., & Namayandeh, M. (2017) 'Realistic implementation of V2X communication in urban areas using VEINS', *Simulation Modelling Practice and Theory*, 77, pp. 84-96.

[14] Hirschmann, G., Fraenzle, M., & Hahn, A. (2020) 'Impact of mobility models on vehicular network simulations', *Simulation Modelling Practice and Theory*, 98, pp. 101956.

[15] Zhang, J., Wang, Z., & Xu, C. (2019) 'Machine learning-based detection of DDoS attacks in V2X networks', *IEEE Transactions on Vehicular Technology*, 68(4), pp. 3804-3812.

[16] Leinmüller, T., Kargl, F., & Schoch, E. (2015) 'Position verification approaches for vehicular ad hoc networks', *IEEE Wireless Communications*, 13(5), pp. 16-21.

[17] Sedjelmaci, H., Senouci, S. M., & Ansari, N. (2017) 'Intrusion detection and response system for advanced metering infrastructures in smart grid', *IEEE Network*, 31(5), pp. 66-72.

[18] Bi, Y., Greenhalgh, S., Lewis, S., & Fan, L. (2018) 'Lightweight authentication and key management for critical security services in VANETs', *IEEE Transactions on Vehicular Technology*, 67(8), pp. 7808-7822.

[19] Singh, P., & Sharma, S. (2020) 'DDoS attack mitigation in VANETs using rate limiting and priority queuing', *IEEE Transactions on Vehicular Technology*, 69(8), pp. 8242-8254.

[20] Zeng, K., Lou, W., & Zhen, C. (2017) 'Secure and privacy-preserving communications in VANETs', *IEEE Wireless Communications*, 16(4), pp. 22-29.

APPENDIX A

Supplementary Materials: The complete supporting code can be downloaded at https://github.com/Chrisagboile/ddosveins

Data Availability Statement: Data supporting reported results can be found at.
https://github.com/Chrisagboile/ddosveins/tree/main/projects/dataall.csv