



ISSN: 2723-9535





Available online at www.HighTechJournal.org

HighTech and Innovation Journal

Vol. 4, No. 4, December, 2023



Simulation of Vehicular Bots-Based DDoS Attacks in Connected Vehicles Networks

Siti Fatimah Abdul Razak ^{1*}, Ku Yee Fang ¹, Noor Hisham Kamis ¹,
Anang Hudaya Muhammad Amin ², Sumendra Yogarayan ¹

¹ Faculty of Information Science and Technology, Multimedia University, Melaka 75450 Malaysia.

² Computer and Information Science Department, Higher Colleges of Technology, Dubai Men's College, United Arab Emirates.

Received 12 September 2023; Revised 11 November 2023; Accepted 23 November 2023; Published 01 December 2023

Abstract

Connected vehicles are more vulnerable to attacks than wired networks since they involve rapid mobility, continuous data flow across connected nodes, and dynamic network design in a distributed network environment. Distributed Denial of Service (DDoS) is one of the most common and dangerous security attacks on connected vehicle networks. Attackers can remotely control malicious nodes that are programmed to attack other nodes known. The compromised nodes are known as botnets, which will constantly flood the target nodes with User Datagram Protocol (UDP) packets, disrupting the target nodes data flow and operation. Hence, the goal of this research is to create and simulate a vehicular bot-based Distributed Denial of Service (DDoS) assault in connected vehicle networks. A simulation-based methodology is implemented to observe the impact of the number of bots, DDoS rate, and maximum bulk packet size on network performance. Using the NS-3 network simulator, 73 random mobile vehicle nodes with up to 100 vehicle bots were simulated, and the results are discussed. Regardless of the computational constraints, the findings from this study adds to understanding the risks and problems associated with data transmission by analyzing the impact of vehicular bot-based DDoS attacks on connected vehicle performance.

Keywords: Vehicular Bot Nodes; VANET; Distributed Denial of Services; NS3.

1. Introduction

Connected vehicle networks have developed as a breakthrough transportation technology, offering several gains in safety, efficiency, and convenience. These networks provide seamless communication and data sharing between vehicles, infrastructure, and other organizations, resulting in better traffic management, improved navigation systems, and real-time vehicle diagnostics [1, 2]. However, as connection and automation become more integrated in automobiles, new security issues emerge that must be addressed [3, 4].

Among the security risks that could significantly impair the operation and functions of connected vehicles are the Distributed Denial of Services (DDoS) attacks [5]. The attack is distributed, more powerful and severe compared to traditional Denial of Service (DoS) attacks and can occur at any layer of the network communication model [6]. Attackers send malicious messages from different locations and time slots towards the targeted node, causing the victim node to not be able to provide or receive services from genuine nodes [6, 7]. In a connected vehicle network, a DDoS attack may

* Corresponding author: fatimah.razak@mmu.edu.my

 <http://dx.doi.org/10.28991/HIJ-2023-04-04-014>

➤ This is an open access article under the CC-BY license (<https://creativecommons.org/licenses/by/4.0/>).

© Authors retain all copyrights.

cause the connected vehicle difficulties in transmitting or exchanging vehicle or traffic data with other connected vehicles, which could put the drivers and road users in danger when they are mobile on the road [8, 9]. In addition, the nodes will not be able to access centralized network services and important vehicle-to-vehicle (V2V) communication and vehicle-to-infrastructure (V2I) communication services [10].

Moreover, the attacker can access and alter network traffic signals and potentially harm the entire network via a wireless network [10–14]. An experimental study concluded that vehicle nodes will experience a drop in average throughput during a DDoS attack interval on the software-defined Internet of Vehicles. The authors used the Mininet-WiFi emulator and found that attack intensity mostly happens at the controller level [15]. In another study, authors utilized a simulation-based methodology using SUMO (Simulation of Urban Mobility), OMNET++, and Veins (vehicles in Network Simulation) to investigate DDoS attacks on vehicle nodes. A non-parametric statistical anomaly detection technique was proposed to detect and respond to attacks when they occur [15, 16]. Besides, an attack topology and network congestion involving several nodes were created in an open-source network simulator known as NS2 using a greedy technique to identify and mitigate DDoS attacks [17]. Since DDoS attacks can also occur in communications between vehicle nodes and the roadside unit (RSU), the authors proposed a new method called Multivariate Stream Analysis (MVSA) to identify the DDoS attack. The algorithm was applied and evaluated using NS2 as well [17, 18].

Multiple nodes maybe compromised and controlled remotely to launch attacks and overwhelm the targeted node [19]. A vehicular bot-based DDoS attack is a variation of DDoS attacks on vehicles. Vehicular bots that are compromised, hacked, or rogue nodes penetrate the network and perform DDoS attacks on the connected vehicles networks infrastructure. The bots overload the network resources and hinder connection with other legitimate nodes, thus disrupting the function and operation of connected vehicle applications [20]. The bots can also inject, alter, remove, or send fake messages to other nodes in the network, which may be hazardous to road users [21]. Therefore, understanding the behavior and consequences of vehicular bot-based DDoS attacks in connected vehicle networks is critical for building effective security procedures and responses. Moreover, real-world tests on operational connected vehicle networks are challenging, costly, and possibly disruptive. A study on DDoS attacks in vehicular communication environments is crucial, as no real-world dataset containing DDoS attacks on VANETs is publicly available [7]. As a result, simulation-based techniques provide a cost-effective and scalable means of studying the features and consequences of such attacks [19, 22–24].

Hence, the purpose of this study is to simulate and analyze vehicular bot-based DDoS attacks in connected vehicle networks. This research has analyzed the simulation results in terms of packet delivery, packet loss ratio, throughput, jitter, and end-to-end delay. The behavior and impact of these attacks were examined in controlled and configurable situations by employing simulation tools and models particularly developed for connected vehicle environments. The findings of this study can be used to inform the design and implementation of effective security solutions to reduce the danger of vehicular bot-based DDoS attacks.

The remainder of this paper is structured as follows: The simulation technique utilized in this work, including the tools, models, and measurements, is described in Section 2. Section 3 offers the simulation results and analyses, and Section 4 discusses the findings. Finally, Section 5 summarizes the important contributions of this research and discusses potential future directions. It is hoped that this study will help to improve knowledge of vehicular bot-based DDoS attacks in connected vehicle networks, as well as give insights into the creation of strong security methods to maintain the safe and dependable functioning of these networks in the face of new threats.

2. Simulation

The simulation-based technique creates a controlled and scalable connected vehicle environment for the purpose of this study. It is a prior step before proceeding to any real-world environment that reduces cost, avoids disruptions to operationally connected vehicles, and eliminates the risk of fatal outcomes when the network is attacked. The vehicular bot-based DDoS attacks are demonstrated and analyzed in this study based on the activities illustrated in Figure 1 [6, 23].

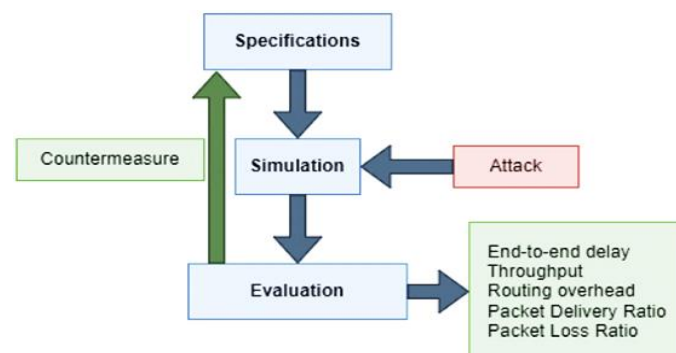


Figure 1. Simulation process

Initially, UBUNTU 18.0.0+, Eclipse SUMO, and NS-3, as well as the project dependencies, were installed before generating the connected vehicle environment and running the simulations. A minimum of 20 GB of storage is required for the installation and configuration of these tools. The NS-3 discrete-event network simulator [25] demonstrated how this attack affects communication among vehicular nodes. Simulation runs were performed systematically by changing the seeds for a random number of bots involved in different network loads and densities to evaluate the network performance when the network is experiencing DDoS attacks. This approach allowed us to observe the effects of the attacks under different conditions and obtain statistically significant results. The simulation environment was designed with the parameters in Table 1. For this study, 73 vehicle nodes were set to travel at a constant speed of 45 m/s and deployed using the 802.11p standard. Vehicle bots were randomly inserted during the simulation, where the value is set between 0 to 50. These bots will randomly generate packets of 5 MB to 25 MB to be sent to the target node. Furthermore, the Adhoc On-Demand Distance Vector (AODV) [26, 27] routing protocol was employed to facilitate traffic routing.

Table 1. Simulation parameters

Parameter	Value
Network simulator	NS-3.36.1
Routing protocol	AODV
Wireless communication	IEEE 802.11p
Selected network traffic area	Ayer Keroh, Melaka
Maximum simulation time	20s
Number of legitimate vehicles nodes	73
Number of bot nodes	0 – 300
Data rate of point-to-point channel	50Mbps
Delay in point-to-point channel	1ms
DDoS rate	20,480 – 102,400 kbps

In NS-3, a channel connects a node, and in this simulation, the channel selected is a point-to-point channel. Two PointToPointHelper objects, designated *pp1* and *pp2*, were created and set to 50 Mbps with a predefined delay of 1 ms. The vehicle nodes and vehicular bot nodes were generated and stored in separate containers, i.e., NetDeviceContainer[] and botDeviceContainer[], respectively. Moreover, the base address 10.0.0.0 was set with a subnet mask of 255.255.255.252 for vehicular bot nodes, while 10.1.1.0 and 10.1.2.0 with a subnet mask of 255.255.255.0 were dedicated to vehicular nodes. Compared to the vehicular nodes, new IP addresses were assigned to vehicular bots on a rotation basis. Moreover, the client node was configured to send large amounts of data using the TCP protocol.

2.1. DDoS Attack Setup

The client node is specified by the InetSocketAddress(). This information is required to deliver UDP packets. However, the OnOffHelper must be generated prior to the data transmission. At the same time, the client node is configured to send large amounts of data using the TCP protocol. In addition, two different types of packet sink applications were deployed for the server node. The first sink is a UDP sink and is set up to accept any UDP packets sent over a port specified in UDP_SINK_PORT. The second sink is set up to both receive and listen on the TCP_SINK_PORT port in the meantime. The MAX_SIMULATION_TIME seconds is the time limit after which both sinks are configured to stop. All incoming packets will be received and discarded by these sinks. Moreover, all vehicular bots are set to release packets constantly for 30 seconds.

The vehicular bot node positions were set in a grid layout. The grid is initially structured in rows, with a spacing of 5 units on the x-axis and 10 units on the y-axis. The grid's width is set to 5. Then, the mobility model for each node was set. A call back function, i.e., CourseChange(), is set up to log the course change events of mobility models in the simulation. The function was invoked whenever a course change occurred, and the log output was transmitted to the designated output stream.

In this study, the maximum number of packets per trace file is set to the maximum value of an unsigned 64-bit integer to be visualized in NetAnim. The x-coordinate is incremented by 1 for each iteration of the loop, while the y-coordinate is fixed at 30 to determine the placement of the bot nodes. The bot nodes will therefore be scattered horizontally as a result. The network traffic flow between client and server nodes was monitored using a flow monitor. The recorded data includes source and destination IP addresses, protocol, source and destination ports, number of bytes, packets sent, packet received, jitter, and end-to-end delay. The information allows estimation of bandwidth utilization and packet loss in the connected vehicle environment compromised by DDoS attacks from vehicular bot nodes.

Moreover, three assault scenarios were created to replicate various forms of vehicular bot-based DDoS attacks. Different scenarios of simulation were identified with manipulation of the number of vehicular bots involved, DDoS rate, and maximum bulk bytes. In Scenario 1, the number of bots was set as 10, 20, 30, 40, and 50. The simulation was run for 20s with a 1 ms channel delay, a 50 Mbps channel data rate, a 15 MB max bulk packet, and a DDoS rate of 40,960 kbps. In Scenario 2, the DDoS rate was set to 20480 kbps, 40960 kbps, 61440 kbps, 81920 kbps, and 102400 kbps. The simulation was also run for 20s with a 1 ms channel delay, 50 Mbps channel data rate, and a 15 MB max bulk packet. In this scenario, the impact of 20 vehicular bots in the connected vehicle network was investigated. Lastly, in Scenario 3, the simulation was run with 20 vehicular bots and a DDoS rate of 20480 kbps. The max bulk packets of 5 MB, 10 MB, 15 MB, 20 MB, and 25 MB were assessed for 20 s. The channel delay and channel data rate remain as in previous scenarios, i.e., 1 ms and 50 Mbs respectively. It is assumed that in critical vehicle safety applications, the Basic Safety Messages (BSM) packets are kept around 300–400 bytes for reliable and efficient data transmissions. Map and traffic data, vehicle telematics data, software updates or patches, etc. would require higher packet size. Hence, the packet size requirements will depend on the type of application.

2.2. Performance Metrics

The impact of vehicular bot-based DDoS attacks was measured based on the packet delivery ratio, packet loss ratio, throughput, jitter, and end-to-end delay by varying the number of bots, DDoS rate, and max bulk rate. By using NS-3, the mentioned variables can be used to analyze the efficiency and performance of the network [1, 28].

The packet delivery ratio indicates the proportion of successfully delivered packets out of all packets created. It gives information on the network’s capacity to manage legitimate communication amid malicious traffic [29]. The ratio of packets that are successfully communicated to those that are unsuccessfully communicated is known as the packet loss ratio. It displays the percentage of communication packets that were lost [19, 30, 31].

When a delay varies over time from end to end, it is referred to as jitter. Normal communication has very little jitter fluctuation. This variation is primarily caused by issues with traffic, congestion, etc. However, there are significant changes while under attack as a result of the violent vehicle's unusual actions [11].

End-to-end delay refers to the average amount of time it takes a packet to travel from the source of its origin to its destination. End-to-end delay aids in determining the impact of vehicular bot-based DDoS attacks on communication latency, which is critical for time-critical applications in connected vehicle networks. The performance of the network improves with decreasing delay [29].

Network throughput is a statistic that measures the quantity of authentic data successfully transmitted through a network in a particular time frame. It aids in determining the connected vehicle network's ability to manage regular traffic flow under assault scenarios. It is the statistic used to assess how well the network is performing [17, 18].

3. Results

In this study, NetAnim was employed to visualize the interaction between vehicle nodes and vehicular bot nodes when the simulation is run. Figure 2 shows the interaction between the client and server nodes in a connected vehicle network. The nodes are shown in a grid layout as specified in Section 2.2.

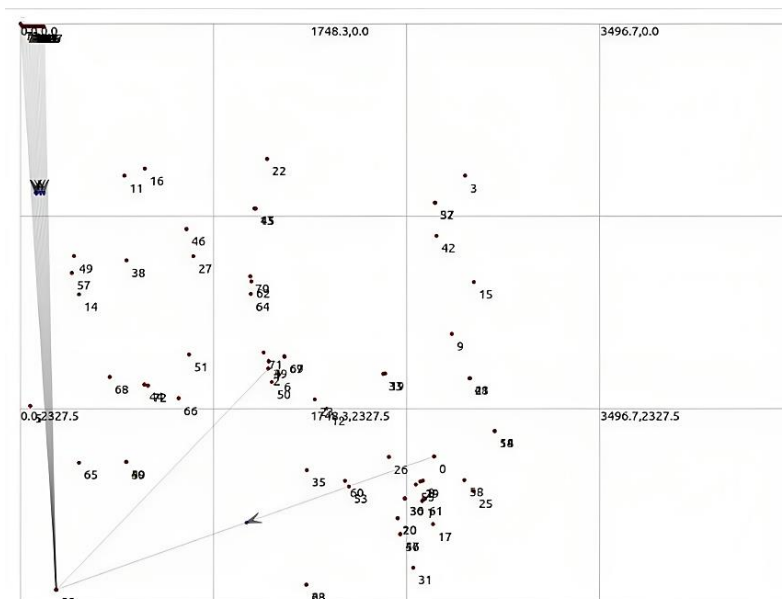


Figure 2. Vehicle nodes without DDoS attack

Assume that V_n represents vehicle nodes, where $n = \{1, 2, \dots, 73\}$. Based on Figure 2, the client node, which is V_0 , sends packets to V_2 , which is the server node, through the TCP communication protocol. At the same time, vehicular botnets launched an attack on V_2 by sending packets through the UDP communication protocol (grey shaded line in Figure 2). This has caused V_2 to be congested, and thus, packet flow from V_2 to V_{71} took more time than usual packet transmissions in the network, as shown in Figure 3.

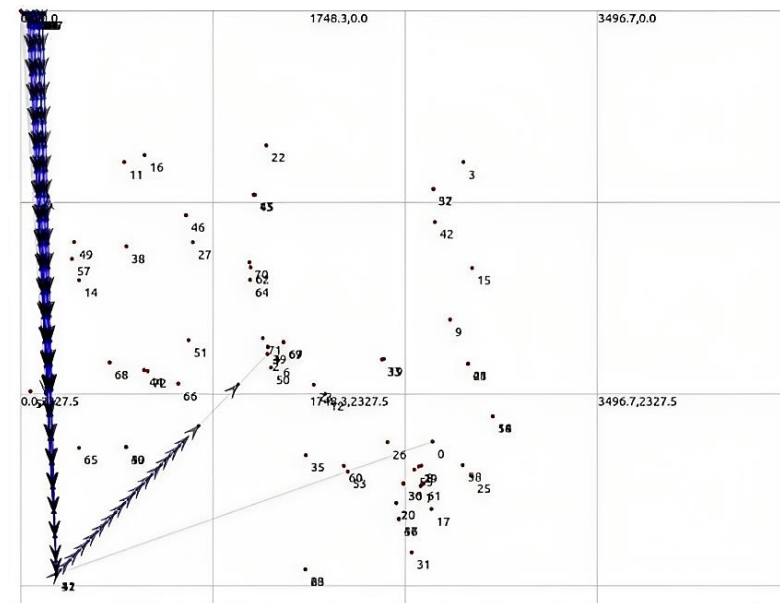


Figure 3. Vehicle node assaulted by vehicular bot nodes

3.1. Packet Delivery Ratio

The ratio of successfully delivered packets to the total number of packets sent is known as the packet delivery ratio. The packet delivery ratio may drop as the number of bots increases, as shown in Figure 4. The packet delivery ratio is high (99.9929%) in the absence of vehicular bots at the beginning of the simulation. When there are more than 20 bots, the decline becomes more noticeable. Increased network congestion and load can cause packet losses or drops, resulting in a decreased delivery ratio.

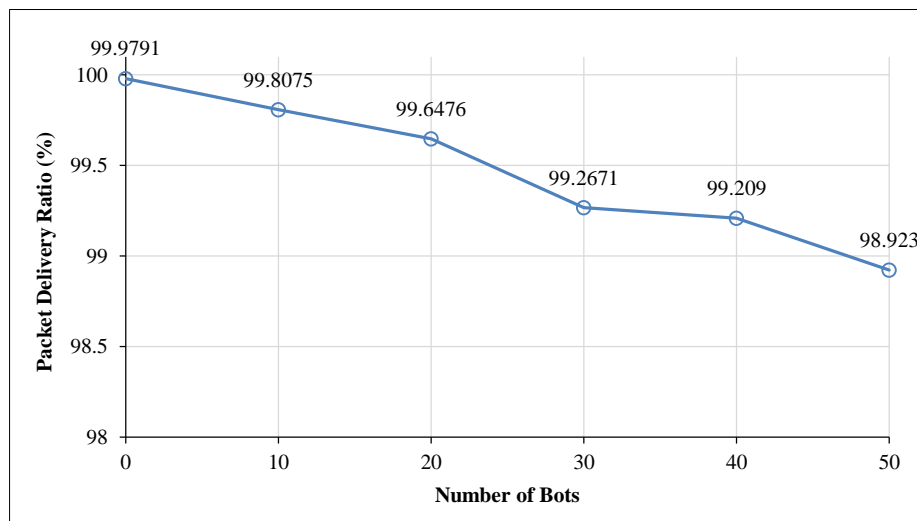


Figure 4. Packet delivery ratio vs. number of bots

Moreover, the packet delivery ratio may drop if the connected vehicle network gets overloaded and is unable to manage the inflow of attack packets transmitted by the vehicular bot nodes, simulating a greater DDoS attack rate. Since the simulation scale in this study is relatively small, it has been noted that despite varying DDoS rates, the packet delivery ratio constantly remains high (shown in Figure 5). The numbers, which range from 99.627% to 99.7541%, show that there is very minimal variance in the packet delivery. This appears to indicate the network's packet delivery performance is not significantly impacted by the DDoS rate. The high and steady values show that the connected vehicle network successfully maintains a high packet delivery rate, guaranteeing dependable packet transfer even under varied DDoS rates.

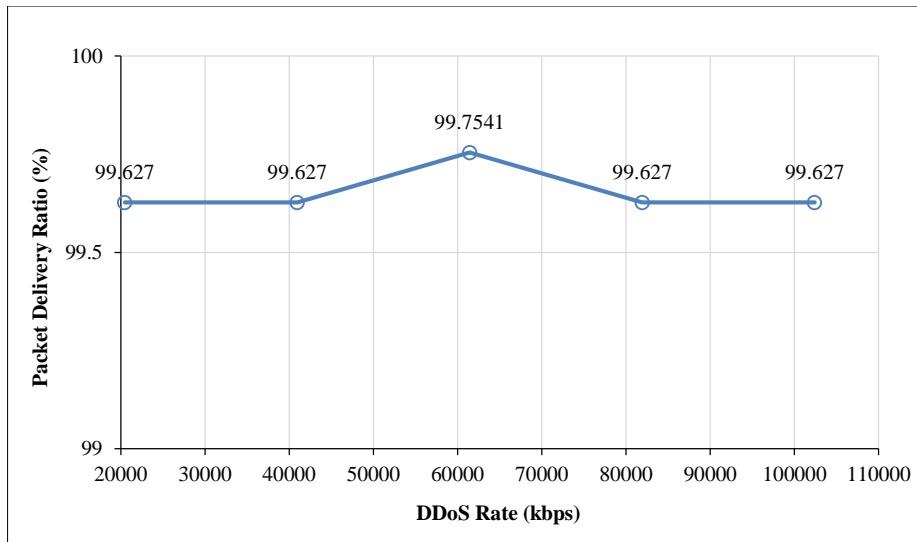


Figure 5. Packet delivery ratio vs. DDoS rate

Moreover, as the maximum bulk packet bytes increase from 5 MB to 10 MB, there is a slight improvement in the packet delivery ratio, indicating a higher percentage of successfully delivered packets, as shown in Figure 6. If the network resources are insufficient to handle huge packets, the maximum bulk bytes may have an impact on the packet delivery ratio, resulting in a lower delivery ratio. However, beyond 10 MB, the packet delivery ratio remains relatively stable at around 99.8% for maximum bulk packet bytes of 15 MB, 20 MB, and 25 MB.

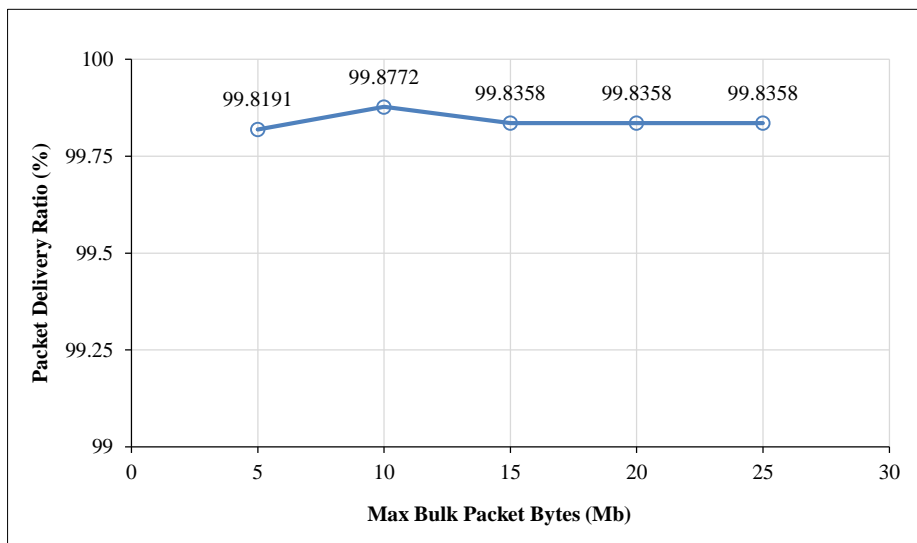


Figure 6. Packet delivery ratio vs. max bulk packet bytes

The consistent packet delivery ratio across higher maximum bulk packet byte values suggests that increasing the packet size does not significantly impact the successful delivery of packets. This indicates that the connected vehicle network is capable of handling larger packet sizes without significantly affecting packet delivery performance. Nevertheless

3.2. Packet Loss Ratio

The ratio of lost packets to the total number of packets sent is known as the packet loss ratio. Based on Figure 7, the packet loss ratio rises as the quantity of vehicular bot nodes rises. When there are no bots, the packet loss ratio is minimal at 0.0071%. However, when there are more bots, the packet loss ratio slowly increases. With a greater number of bots delivering DDoS attack traffic, the network may face significant packet loss owing to congestion, buffer overflow, or malicious packets being intentionally dropped. In our simulation, the increase becomes more noticeable when there are more than 30 vehicular bot nodes. Overall, the existence of bots in connected vehicle network environments may result in a larger packet loss ratio, which means a higher number of lost or undelivered packets during communication.

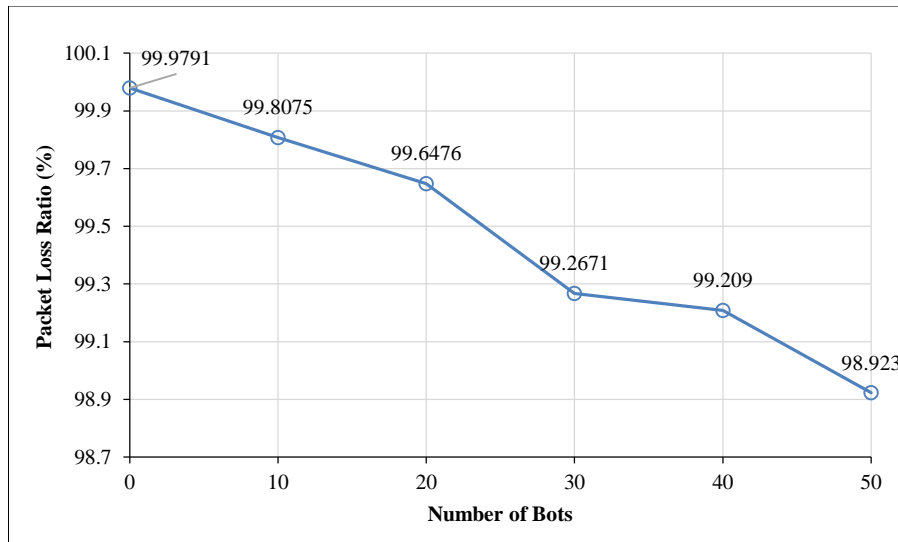


Figure 7. Packet loss ratio vs. number of bots

DDoS attacks launched by the vehicular bot nodes may cause extra data traffic that is not able to be managed by the connected vehicle network. Hence, the number of missed or lost packets will increase. In our simulation, the packet loss ratio stays rather low and stable at various DDoS rates, ranging from 0.2459% to 0.373%, as shown in Figure 8. This indicates that the network maintains a high level of packet delivery with a very low rate of packet loss. The network's resistance to DDoS attacks and capacity to lessen the impact on packet loss are both indicated by the low and steady packet loss ratio. It demonstrates how the network's congestion control and routing methods are adept at maintaining packet integrity even when DDoS rates change.

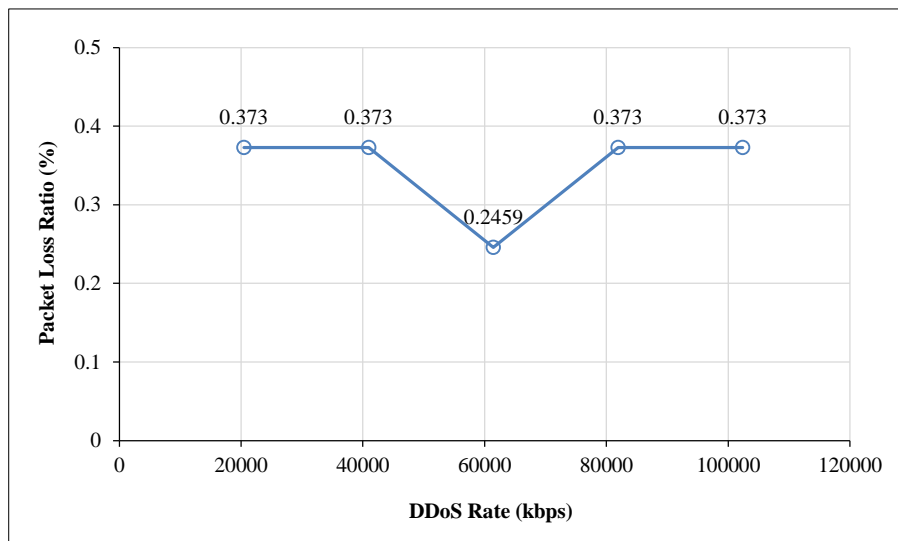


Figure 8. Packet loss ratio vs. DDoS rate

Figure 9 shows a decrease in the packet loss ratio, indicating a reduced number of lost packets when the maximum bulk packet bytes increase from 5 MB to 10 MB, as illustrated. For maximum bulk packet bytes of 15 Mb, 20 Mb, and 25 Mb, the packet loss percentage stays generally stable at roughly 0.16% after 10 Mb. In our simulations, increasing the packet size does not appear to have a major effect on packet loss, according to the consistent packet loss ratio throughout these larger maximum bulk packet byte values. This shows that higher packet sizes may be handled by the network infrastructure and protocols without noticeably raising the risk of packet loss.

Nevertheless, networks with limited capacity may incur higher packet loss ratios while transferring large packets due to congestion, buffer overflow, or the necessity for packet fragmentation.

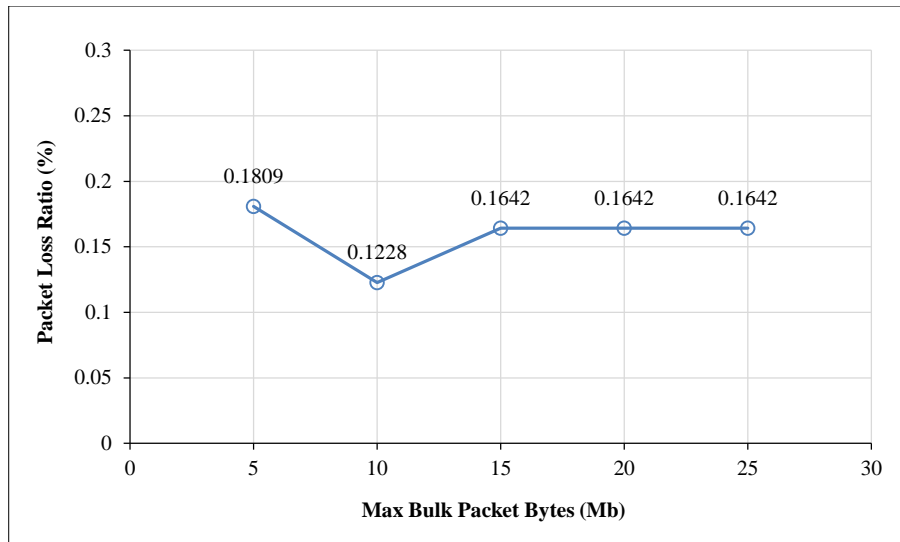


Figure 9. Packet loss ratio vs. max bulk packet bytes

3.3. Throughput

The volume of data delivered over a network in a specific amount of time is known as throughput. According to Figure 10, throughput tends to decline as the number of bots rises. The initial throughput is highest at 11.2916 kbps when there are no bots. However, the throughput drastically decreases as the number of bots rises. When there are more than 10 bots, the throughput decreases more noticeably. In general, as the number of vehicular bot nodes grows, the network's overall throughput may suffer owing to a lack of available capacity and an increase in collisions or packet failures.

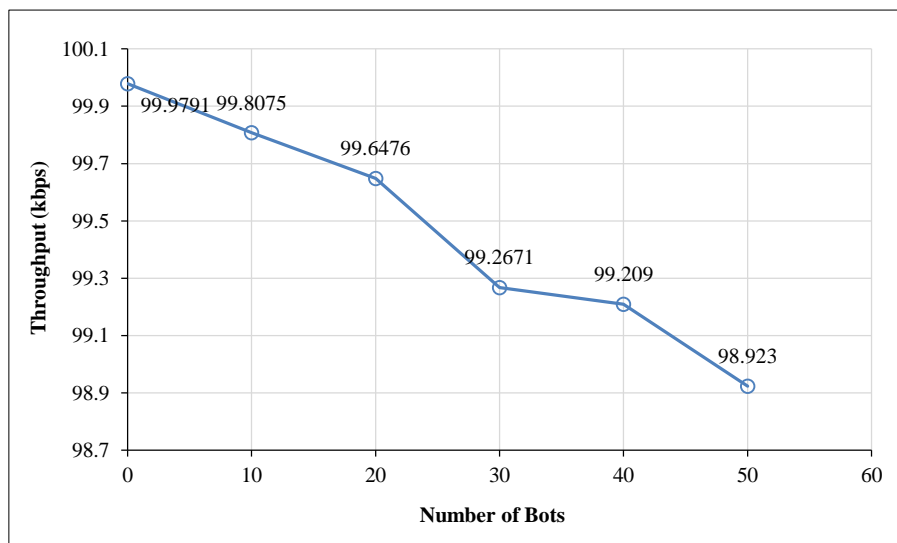


Figure 10. Throughput vs. number of bots

DDoS attack rates that are higher might overwhelm network bandwidth, lowering the available capacity for genuine traffic. As the network strains to accommodate the increasing attack volume, throughput may suffer. Based on Figure 11, it is seen that the throughput values remain largely consistent across varying DDoS rates. With a tiny variance of 0.0064 kbps, the throughput figures vary from 3.7328 kbps to 3.7392 kbps. This suggests that the DDoS rate has little effect on the throughput of the entire network. The throughput measures the volume of data transferred across the network in a given amount of time, and the steady numbers imply that the network keeps its data transmission rate constant despite fluctuations in DDoS rates.

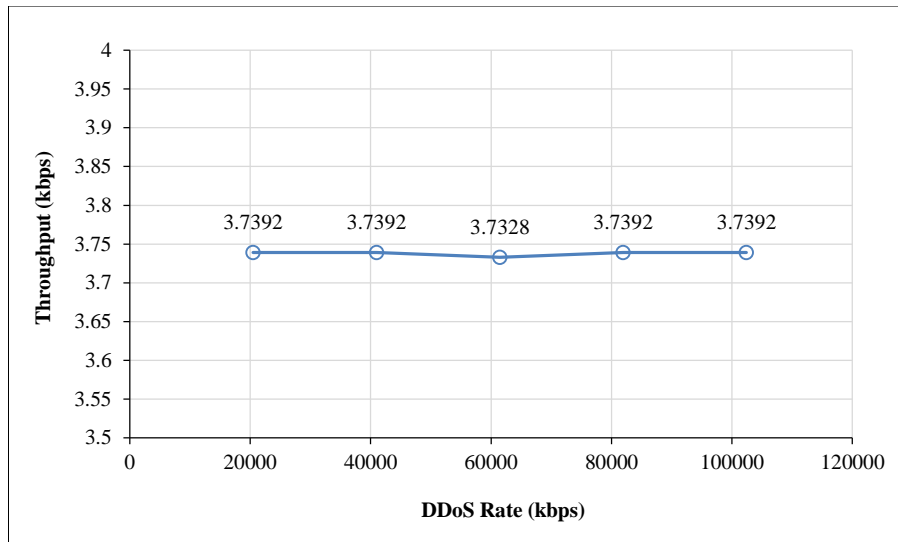


Figure 11. Throughput vs. DDoS rate

Larger maximum bulk bytes can have an effect on overall performance since they demand more bandwidth and resources to transmit. Throughput may be reduced if the network capacity is low. This is illustrated in Figure 12, where throughput also increases as the maximum bulk packet bytes rise from 5 MB to 10 MB and then to 15 MB. This suggests that larger packet sizes increase data transmission rates, which enhance network throughput.

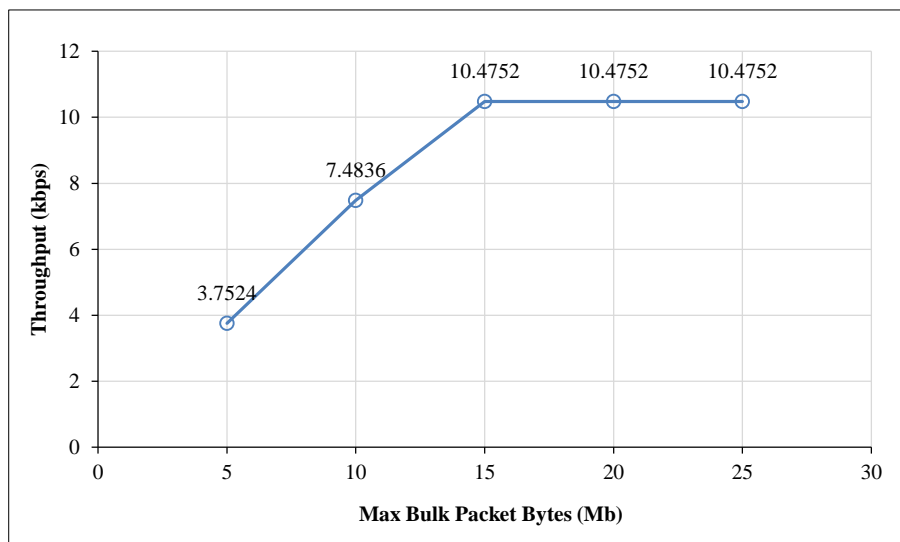


Figure 12. Throughput vs. max bulk packet bytes

It is important to keep in mind that after 15 MB, the throughput stays constant at 10.4572 kbps for any further increases in the maximum bulk packet bytes. The observed pattern indicates that there may be a network saturation point or limit that prohibits throughput from increasing past a particular packet size. Beyond 15 MB, increasing the maximum bulk packet bytes has little effect on the network’s ability to transmit data quickly. This saturation limit has been reached.

3.4. Jitter

The variance in packet delivery latency inside a network is referred to as jitter. Higher vehicular bot node density can cause more unpredictability in packet transmission timings, resulting in higher jitter. The bot’s uneven packet arrival might cause different inter-packet delays. Figure 13 illustrates that there is a slight rise in jitter when the number of bots rises from 0 to 10. However, when the number of bots is increased from 10 to 20, there is a noticeable increase in jitter. When there are more than 20 bots, the jitter varies in a similar range. This implies that the existence of bots causes jitter to increase noticeably, especially when the quantity exceeds a specific threshold.

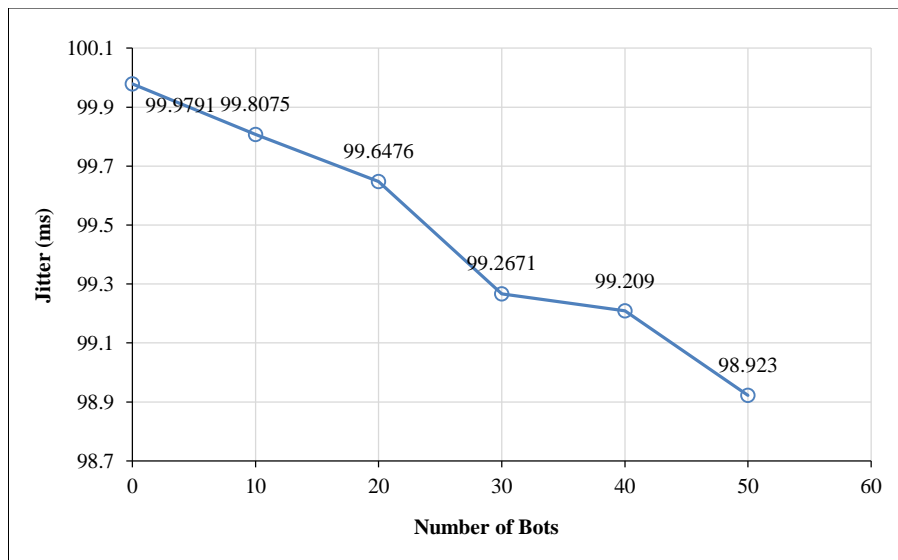


Figure 13. Jitter vs. number of bots

According to Figure 14, the jitter values are very consistent when the DDoS rate rises from 20,480 kbps to 102,400 kbps. There is only a 138 ms difference in the jitter values, which range from 17,334 to 17,472 ms. This suggests that the network jitter is not considerably impacted by the DDoS rate.

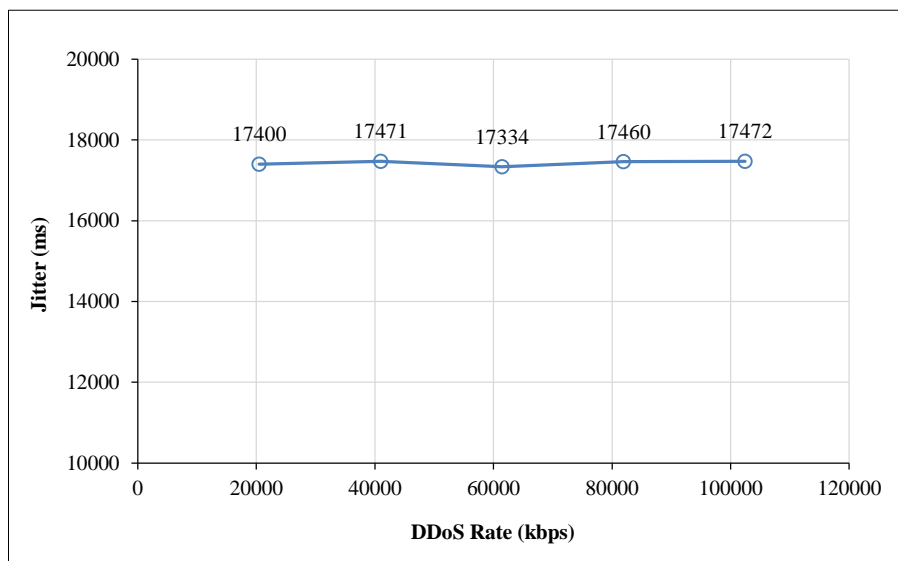


Figure 14. Jitter vs. DDoS rate

A stable jitter number indicates consistent packet timing, despite the higher DDoS rate. Jitter is the variation in packet arrival times. The network maintains a dependable and constant packet delivery mechanism even under high DDoS assault rates, as seen by the negligible variance in jitter. However, increased DDoS attack rates can normally cause greater abnormalities and affect packet transmission timings, leading to increased jitter.

Moreover, if the network has a mix of packet sizes, the presence of bigger bulk bytes might cause fluctuations in transmission delays and lead to higher jitter. Our simulation results in Figure 15 show that the jitter also increases as the maximum bulk packet bytes rise from 5 MB to 10 MB and then to 15 MB. This shows that greater packet size variations within the network are caused by larger packet sizes. However, it is noteworthy that for all consecutive increases in the maximum bulk packet bytes after 15 MB, the jitter remains constant at 24241 ms. The observed pattern points to the possibility of a network threshold or bottleneck that causes a constant degree of jitter above a particular packet size. Beyond 15 MB, subsequent increases in the maximum size of a bulk packet have little effect on the jitter that the packets encounter.

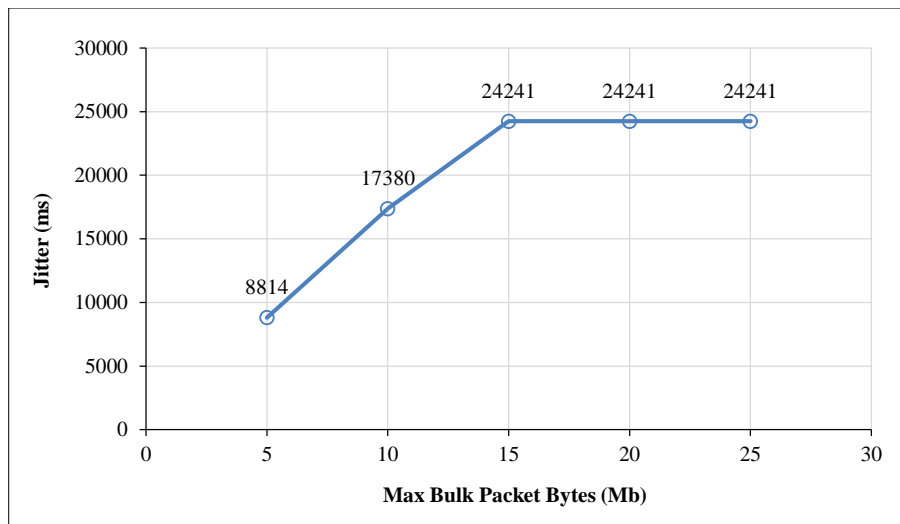


Figure 15. Jitter vs. max bulk packet bytes

3.5. End-to-end Delay

End-to-end delay, also referred to as response time, is the measure of the time it takes for a packet to be transmitted from the sender to the receiver, including all intermediate stations along the way. Factors such as processing, queuing, and transmission can affect the packet’s transmission and the total latency of the packets. Figure 16 shows that when the number of vehicular bot nodes increases, the delay decreases due to network saturation. As more vehicular bot nodes are added to the network, they consume more bandwidth and eventually reach a point where the total bandwidth consumed by all bots is greater than the total available bandwidth of the network. This creates a bottleneck that causes packets to queue up on network devices waiting to be transmitted, leading to an increase in dropped packets. Therefore, the delay decreases as the number of bots increases.

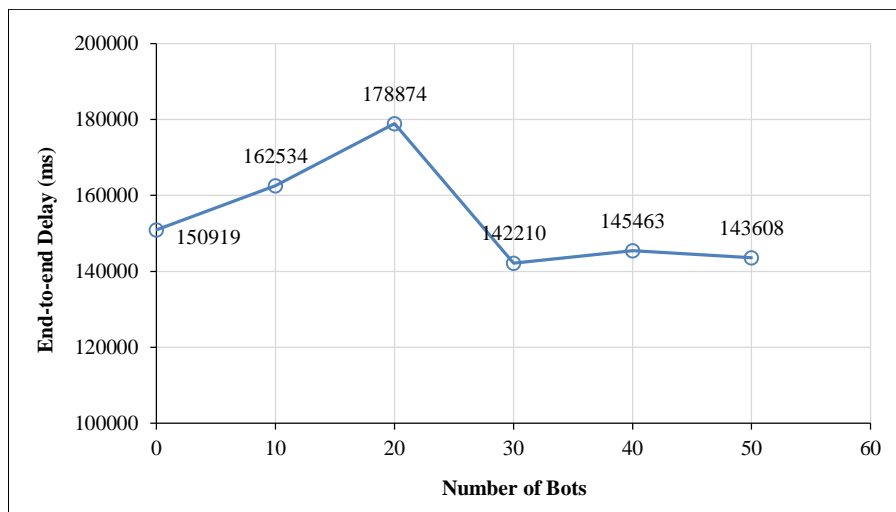


Figure 16. End-to-end delay vs. number of bots

In addition, higher DDoS attack rates can result in greater traffic load and network congestion, which can result in longer end-to-end delays as packets fight for limited resources. According to Figure 17, the end-to-end delay stays largely constant as the DDoS rate rises. Across various DDoS rates, the end-to-end delay values range from 181,064 ms to 188,307 ms. This suggests that in this case, the end-to-end delay is not much impacted by the DDoS rate. The network may be able to handle the increased DDoS rate without significantly delaying packet delivery, according to the rather consistent end-to-end delay.

Moreover, bigger maximum bulk bytes can result in longer packet transmission times, potentially increasing end-to-end latency since bigger packets take longer to transmit. Figure 18 shows that the end-to-end delay increases when the maximum bulk packet bytes rise from 5 MB to 10 MB and then to 15 MB. This implies that higher packet sizes cause greater transmission delays within the network. It is important to note that after 15 MB, the end-to-end latency stays the same at 366392 ms for any further increases in the maximum bulk packet bytes. The observed pattern points to the possibility of a network restriction or bottleneck that results in a delay saturation point. By increasing the maximum bulk packet bytes past this saturation point of 15 MB, the end-to-end delay is not greatly impacted.

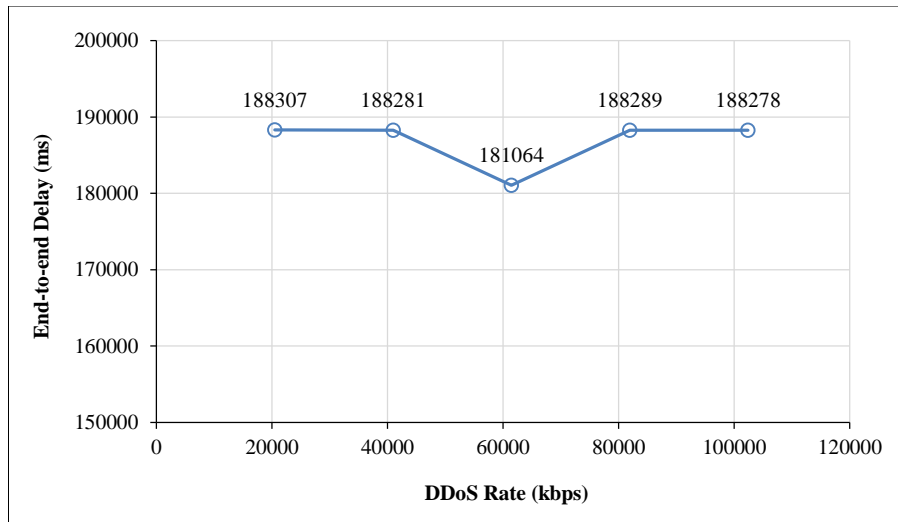


Figure 17. End-to-end delay vs. DDoS rate

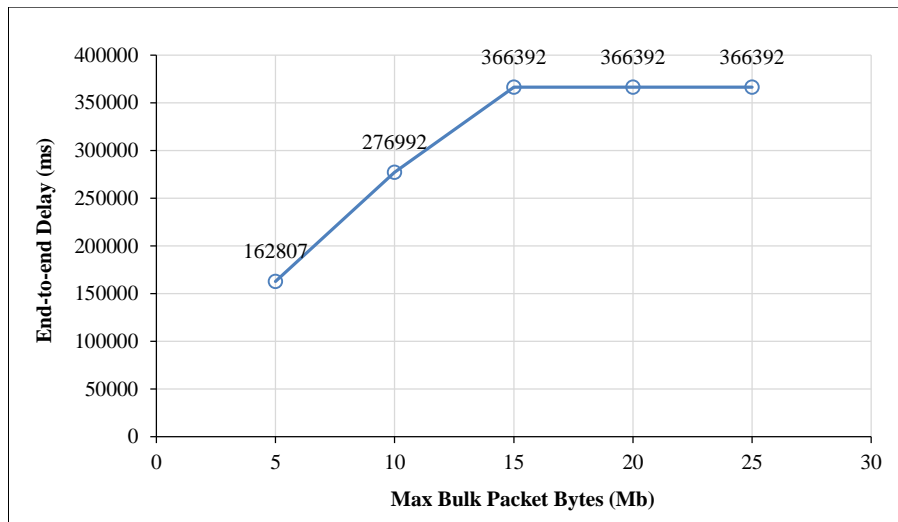


Figure 18. End-to-end delay vs. max bulk bytes

4. Discussions of Findings

In this study, the simulations demonstrate DDoS attacks performed by vehicular bots on legitimate nodes within the same network environment. Vehicular bots DDoS attack the simulation findings highlight the vital need for effective security methods to protect connected vehicle networks from DDoS attacks by vehicular bot nodes. The impact of these attacks on packet delivery, end-to-end delay, jitter, packet delivery ratio, packet loss ratio, and network throughput demonstrate the importance of proactive security measures. Afterwards, the intensity of the attack was further increased by increasing the number of bots from 0 to 100, 200, and 300. The results are shown in Table 2.

Table 2. Results with higher number of bots

Performance measures	0-bots	100-bots	200-bots	300-bots
End-to-end delay (ms)	389635	100814	94067	88789
Jitter (ms)	2937	23426	23054	22268
Throughput (kbps)	11.2916	0.8536	0.4484	0.3232
Packet delivery ratio (%)	99.993	97.711	95.894	94.063
Packet loss ratio (%)	0.0071	2.2894	4.1061	5.9371

The packet delivery ratio (PDR) statistic served as the metric to assess the network's capacity to handle legitimate communication in the midst of vehicular bot-based DDoS assaults. The results show a pronounced correlation between attack intensity and PDR decline. While mild attacks caused minimal PDR deviations, more severe assaults led to a significant drop in PDR, suggesting a substantial impairment in packet delivery.

The average time it took packets to travel from their origin to their destination was measured by the end-to-end delay metric. Our simulations demonstrated a strong link between higher attack intensity and increased end-to-end latency. As the attack intensity increased, the network became congested owing to the large volume of malicious data, resulting in longer packet delivery delays. Moreover, control signals in connected vehicles, such as those used for vehicle-to-infrastructure communication or cooperative driving systems, rely on consistent and timely packet transmission. Increased packet loss ratios can interrupt control signal transmission, causing delays or failures in the execution of essential orders and jeopardizing the overall performance and safety of the connected vehicle network. Time-sensitive applications, such as real-time navigation and the sharing of safety-related information, will also be impacted.

In addition, throughput quantifies the quantity of valid data transferred over the network in a particular time frame. In our findings, as the intensity of the attacks increased, there was a continual drop in network throughput. The existence of vehicular bot nodes that instigate DDoS attacks reduces network performance significantly, indicating a concentrated ability to manage regular traffic flow. The congestion induced by these attacks obstructs efficient data transfer and, consequently, overall network performance. Increased jitter, measured as fluctuations in packet arrival times, poses a risk to data integrity during network transmission. Inconsistent arrival intervals can compromise the meaning of data, potentially leading to misinterpretations or incomplete information. This could potentially influence data-driven applications such as driver assistance, vehicle diagnostics, and sensor data fusion.

Overall, the findings underline the need for adaptive detection systems capable of detecting and neutralizing threats with minimal false positives. The accuracy and efficiency of attack detection in real-time scenarios can be enhanced through the incorporation of fine-tuning detection algorithms and leveraging machine learning approaches. Furthermore, the research highlights the importance of dynamic network management systems that can adapt to changing attack conditions. Traffic re-routing and load balancing systems play a crucial role in mitigating the impact of these attacks by ensuring continuous and reliable connectivity for connected vehicles.

5. Conclusions

This study employed simulation experiments to investigate DDoS attacks launched by bots disguised as legitimate vehicles within connected vehicle networks. The differences in network performance under varying conditions, specifically by increasing the number of vehicular bot nodes, DDoS attack rate, and maximum bulk bytes within the simulation environment, are investigated.

Generally, the simulations demonstrated that vehicular bot nodes composed of coordinated DDoS attacks significantly impacted network performance. As the number of vehicular bots grows, the intensity and reach of the attack escalate. More bots imply more malicious traffic flooding the target node, consuming resources, and obstructing legitimate node traffic. As a result, the performance of connected vehicles will degrade as the number of bots increases. The Packet Delay Ratio experienced a steep decline, indicating an influence on packet delivery, especially under high attack intensity. With the network becoming congested due to the malicious data, the end-to-end delay increased, negatively impacting time-sensitive applications, and posing a threat to the overall functionality of connected vehicle networks. Furthermore, network throughput exhibited a decrease, revealing a reduced capacity for handling regular traffic flow.

In addition, tuning the DDoS rate, which controls how often and heavily bots attack the target, enables the impact of the attack on connected vehicle data transmissions to be further analyzed. Higher DDoS rates indicate more frequent and aggressive attacks, which overload the victim's resources and degrade network performance. This became increasingly evident as key metrics such as end-to-end delays, jitter, throughput, packet delivery, and loss ratios suffered noticeably under the escalating attack intensity.

The size of the malicious packets, determined by the maximum bulk bytes setting, also played a significant role in network performance. Larger packet sizes demand more network resources, increasing congestion and the possibility of packet losses. This congestion led to a domino effect: delays stretched, jitter increased, data slowed to an edge, and more packets went missing. Maximum bulk bytes have a direct proportionate influence on performance measures, as bigger packets require more processing and transmission time.

The simulation results gave useful insight into the patterns and impact of these attacks, demonstrating the risks and issues that connected vehicle networks encounter in ensuring secure and dependable communication. This study contributes to the advancement of knowledge in connected vehicle networks and DDoS attack mitigation strategies.

Nevertheless, like any simulation study, this study might not fully capture the complexity of real connected vehicle networks. Also, the way these bots act and what they can do constantly changes. Thus, this study might not capture every possible attack scenario. Lastly, the accuracy of the findings depends heavily on the network simulator parameters and environment settings. The development of strong security systems, proactive tactics, and policies may be derived to ensure the safe and dependable functioning of connected vehicle networks in the face of growing threats by analyzing the behavior and effect of vehicular bot-based DDoS attacks.

As connected vehicle networks grow, it is critical to address the security issues they pose. Future research should explore different scenarios and perform evaluations by leveraging simulation tools and methodologies. This may provide better insights to assist researchers, practitioners, and policymakers in developing effective solutions to mitigate the risks associated with vehicular bot-based DDoS attacks and ensure the secure and efficient operation of connected vehicle networks for the benefit of all stakeholders. More research is needed to improve the security and resilience of connected vehicle networks. Researchers could concentrate on improving and optimizing attack detection algorithms, studying mitigation measures, and establishing comprehensive security frameworks that take into account the dynamic nature of vehicular bot-based DDoS attacks.

6. Declarations

6.1. Author Contributions

Conceptualization, S.F.A.R. and S.Y.; methodology, K.Y.F. and N.H.K.; software, N.H.K.; writing—original draft preparation, S.F.A.R., K.Y.F., and A.H.M.A.; writing—review and editing, S.F.A.R. and N.H.K.; visualization, S.Y. All authors have read and agreed to the published version of the manuscript.

6.2. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

6.3. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

6.4. Acknowledgements

The authors would like to thank the Centre for Intelligent Cloud Computing for the encouragement and support for this study.

6.5. Institutional Review Board Statement

Not applicable.

6.6. Informed Consent Statement

Not applicable.

6.7. Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

7. References

- [1] Banafshehvaragh, S. T., & Rahmani, A. M. (2023). Intrusion, anomaly, and attack detection in smart vehicles. *Microprocessors and Microsystems*, 96. doi:10.1016/j.micpro.2022.104726.
- [2] Vamshi Krishna, K., & Ganesh Reddy, K. (2023). Classification of Distributed Denial of Service Attacks in VANET: A Survey. *Wireless Personal Communications*, 132(2), 933–964. doi:10.1007/s11277-023-10643-6.
- [3] Dibaei, M., Zheng, X., Jiang, K., Abbas, R., Liu, S., Zhang, Y., Xiang, Y., & Yu, S. (2020). Attacks and defences on intelligent connected vehicles: a survey. *Digital Communications and Networks*, 6(4), 399–421. doi:10.1016/j.dcan.2020.04.007.
- [4] Wei, T. Z., Razak, S. F. A., & Kamis, N. H. (2022). Secure Communication for Connected Vehicles Safety Applications. *IEEE 13th Control and System Graduate Research Colloquium, Conference Proceedings*, 71–76. doi:10.1109/ICSGRC55096.2022.9845160.
- [5] Zaidi, T., & Faisal, S. (2018). An overview: Various attacks in VANET. In *2018 4th International Conference on Computing Communication and Automation (ICCCA)*, 1–6. doi:10.1109/CCAA.2018.8777538
- [6] Baharlouei, H., Makanju, A., & Zincir-Heywood, N. (2022). Exploring Realistic VANET Simulations for Anomaly Detection of DDoS Attacks. *IEEE Vehicular Technology Conference, Helsinki, Finland*. doi:10.1109/VTC2022-Spring54318.2022.9860624.
- [7] Hezam Al Junaid, M. A., Syed, A. A., Mohd Warip, M. N., Fazira Ku Azir, K. N., & Romli, N. H. (2018). Classification of Security Attacks in VANET: A Review of Requirements and Perspectives. *MATEC Web of Conferences*, 150. doi:10.1051/mateconf/201815006038.
- [8] Gao, Y., Wu, H., Song, B., Jin, Y., Luo, X., & Zeng, X. (2019). A distributed network intrusion detection system for distributed denial of service attacks in vehicular ad hoc network. *IEEE Access*, 7, 154560–154571. doi:10.1109/ACCESS.2019.2948382.

- [9] Sharma, S., & Kaul, A. (2018). A survey on Intrusion Detection Systems and Honeypot based proactive security mechanisms in VANETs and VANET Cloud. *Vehicular Communications*, 12, 138–164. doi:10.1016/j.vehcom.2018.04.005.
- [10] Kadri, M. R., Abdelli, A., Ben Othman, J., & Mokdad, L. (2024). Survey and classification of Dos and DDoS attack detection and validation approaches for IoT environments. *Internet of Things (Netherlands)*, 25. doi:10.1016/j.iot.2023.101021.
- [11] Kolandaisamy, R., Md Noor, R., Ahmedy, I., Ahmad, I., Reza Z'Abu, M., Imran, M., & Alnuem, M. (2018). A Multivariate Stream Analysis Approach to Detect and Mitigate DDoS Attacks in Vehicular Ad Hoc Networks. *Wireless Communications and Mobile Computing*, 2874509. doi:10.1155/2018/2874509.
- [12] Adhikary, K., Bhushan, S., Kumar, S., & Dutta, K. (2020). Hybrid Algorithm to Detect DDoS Attacks in VANETs. *Wireless Personal Communications*, 114(4), 3613–3634. doi:10.1007/s11277-020-07549-y.
- [13] Gad, A. R., Nashat, A. A., & Barkat, T. M. (2021). Intrusion Detection System Using Machine Learning for Vehicular Ad Hoc Networks Based on ToN-IoT Dataset. *IEEE Access*, 9, 142206–142217. doi:10.1109/ACCESS.2021.3120626.
- [14] Nandy, T., Noor, R. M., Yamani Idna Bin Idris, M., & Bhattacharyya, S. (2020). T-BCIDS: Trust-Based Collaborative Intrusion Detection System for VANET. In *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications, NCETSTE A 2020. Trust-Based Collaborative Intrusion Detection System for VANET, Durgapur, India*. doi:10.1109/NCETSTE A48365.2020.9119934.
- [15] Shu, J., Zhou, L., Zhang, W., Du, X., & Guizani, M. (2021). Collaborative Intrusion Detection for VANETs: A Deep Learning-Based Distributed SDN Approach. *IEEE Transactions on Intelligent Transportation Systems*, 22(7), 4519–4530. doi:10.1109/TITS.2020.3027390.
- [16] Siddiqui, A. J., & Boukerche, A. (2018). On the Impact of DDoS Attacks on Software-Defined Internet-of-Vehicles Control Plane. *2018 14th International Wireless Communications and Mobile Computing Conference, IWCMC 2018*, 1284–1289. doi:10.1109/IWCMC.2018.8450433.
- [17] Haydari, A., & Yilmaz, Y. (2018). Real-Time Detection and Mitigation of DDoS Attacks in Intelligent Transportation Systems. *2018 IEEE Intelligent Transportation Systems Conference*, 1–7.
- [18] Kolandaisamy, R., Noor, R. M., Z'aba, M. R., Ahmedy, I., & Kolandaisamy, I. (2020). Adapted stream region for packet marking based on DDoS attack detection in vehicular ad hoc networks. *Journal of Supercomputing*, 76(8), 5948–5970. doi:10.1007/s11227-019-03088-x.
- [19] Guleria, C., & Verma, H. K. (2018). Improved detection and mitigation of DDOS attack in vehicular ad hoc network. *2018 4th International Conference on Computing Communication and Automation, ICCCA 2018*, 1–4. doi:10.1109/CCAA.2018.8777539.
- [20] Garip, M. T., Reiher, P., & Gerla, M. (2018). Botveillance: A vehicular botnet surveillance attack against pseudonymous systems in VANETs. *Proceedings of the 2018 11th IFIP Wireless and Mobile Networking Conference, WMNC 2018, Prague, Czech Republic*. doi:10.23919/WMNC.2018.8480909.
- [21] Chaouche, Y., Renault, E., & Boussaha, R. (2023). WEKA-based Real-Time Attack Detection for VANET Simulations. In *2023 31st International Conference on Software, Telecommunications and Computer Networks, SoftCOM 2023, Split, Croatia*. doi:10.23919/SoftCOM58365.2023.10271621.
- [22] Hameed Mir, Z., & Filali, F. (2017). Large-scale simulations and performance evaluation of connected cars - A V2V communication perspective. *Simulation Modelling Practice and Theory*, 73, 55–71. doi:10.1016/j.simpat.2017.01.004.
- [23] Abdul Razak, S. F., Yogarayan, S., Azman, A., Abdullah, M. F. A., Muhamad Amin, A. H., & Salleh, M. (2021). Simulation framework for connected vehicles: a scoping review. *F1000Research*, 10(10), 1265. doi:10.12688/f1000research.73398.1.
- [24] Boeglen, H., Hilt, B., & Drouhin, F. (2017). Emulating a Realistic VANET Channel in Ns-3. *Networking Simulation for Intelligent Transportation Systems: High Mobile Wireless Nodes*, 107-131. doi:10.1002/9781119407447.ch6.
- [25] Naveen, R., Chaitanya, N. S. V., Nikhil Srinivas, M., & Vineeth, N. (2020). Implementation of a Methodology for Detection and Prevention of Security Attacks in Vehicular Adhoc Networks. *2020 IEEE International Conference for Innovation in Technology, INOCON 2020*. doi:10.1109/INOCON50539.2020.9298365.
- [26] Fiade, A., Yudha Triadi, A., Sulhi, A., Ummi Masrurroh, S., Handayani, V., & Bayu Suseno, H. (2020). Performance Analysis of Black Hole Attack and Flooding Attack AODV Routing Protocol on VANET (Vehicular Ad-Hoc Network). *2020 8th International Conference on Cyber and IT Service Management, CITSM 2020*. doi:10.1109/CITSM50537.2020.9268789.
- [27] Shaban, A. M., Kurnaz, S., & Shantaf, A. M. (2020). Evaluation DSDV, AODV and OLSR routing protocols in real live by using SUMO with NS3 simulation in VANET. In *HORA 2020 - 2nd International Congress on Human-Computer Interaction, Optimization and Robotic Applications, Proceedings*, 1–5. doi:10.1109/HORA49412.2020.9152903.
- [28] Ahmad, S., Raza, I., Hasan Jamal, M., Djuraev, S., Hur, S., & Ashraf, I. (2023). Central Aggregator Intrusion Detection System for Denial of Service Attacks. *Computers, Materials and Continua*, 74(2), 2363–2377. doi:10.32604/cmc.2023.032694.

- [29] Baccari, S., Touati, H., Hadded, M., & Muhlethaler, P. (2020). Performance Impact Analysis of Security Attacks on Cross-Layer Routing Protocols in Vehicular Ad hoc Networks. 2020 28th International Conference on Software, Telecommunications and Computer Networks, SoftCOM 2020, 1–6. doi:10.23919/SoftCOM50211.2020.9238259.
- [30] Kamboj, S., & Mann, K. S. (2018). Detection of Multiple Malicious Nodes Using Entropy for Mitigating the Effect of Denial of Service Attack in VANETs. Proceedings - 4th International Conference on Computing Sciences, ICCS 2018, 72–79. doi:10.1109/ICCS.2018.00018.
- [31] Saggi, M. K., & Kaur, R. (2015). Isolation of Sybil attack in VANET using neighboring information. Souvenir of the 2015 IEEE International Advance Computing Conference, IACC 2015, 46–51. doi:10.1109/IADCC.2015.7154666.