DISSECTING DENIAL OF SERVICE (DoS) SYN FLOOD ATTACK DYNAMICS AND IMPACTS IN VEHICULAR COMMUNICATION SYSTEMS

Muhammad Arif Hakimi Zamrai[1*], *Kamaludin* Mohamad Yusof[1], *Afizi* Azizan[1]

[1]Faculty of Electrical Engineering, Universiti Teknologi Malaysia, Johor, Malaysia

Abstract. In the rapidly evolving landscape of vehicular networks, the resilience of vehicular communication systems against Denial of Service (DoS) attacks is critical. Existing research often overlooks the nuanced dynamics of such attacks, particularly in terms of packet size variability and vehicle mobility within Software-Define Internet of Vehicles (SD-IoV) systems. This study addresses this research gap by conducting a detailed analysis of SYN flood DoS attack patterns and their impact on SDN-controlled vehicular networks. This research examines the effects of different packet sizes in SYN packet—1 byte, 200 bytes, 360 bytes, and 1400 bytes—and explore how these packet size variations influence the efficacy of the attacks and the resultant downtime experienced by the victim car. This research findings reveal that SYN flood attacks employing minimal 1-byte packets can cause prolonged unresponsiveness in the victim vehicle, leading to a drastic drop in packet throughput. This research underscores the subtleties of DoS attack strategies and their significant implications on the functionality and safety of IoV environments. The alarming potential of such refined and coordinated DoS attack highlights an urgent need for the development of robust defense mechanisms that can adapt to the sophisticated landscape of vehicular cyber threats.

1 Introduction

As wireless communication technologies advance rapidly, they pave the way for the integration of the Internet of Vehicles (IoV) within intelligent, connected urban environments. Amidst this progress, the Software-Defined Networking (SDN) approach is emerging as a revolutionary framework that scholars and technologists are adopting to significantly enhance the management and adaptability of IoV systems. This initiative is steering the evolution of a novel concept known as the Software-Defined Internet of Vehicles (SD-IoV)[1]–[3].

The SD-IoV paradigm introduces new complexities, particularly in terms of network security. At the heart of the SD-IoV infrastructure resides the SDN controller, which is vulnerable to a critical point of failure, especially in the attack of Denial of Service (DoS) [4]. The incapacitation and single point of failure of the controller could spell a disaster for the entire network, with potentially catastrophic repercussions in smart urban locales.

* Corresponding author: mahakimi8@graduate.utm.my

Such a scenario could precipitate a cascade of adverse domino effects, including accidents, gridlocks, navigation errors, and interruptions to vital services and applications [5].

Despite the well-documented risks of DoS attacks, there are significant research gap in understanding the specific dynamics of these attacks within the SD-IoV context. Current literature lacks an in-depth exploration of how varying packet sizes and vehicle mobility affect the efficacy and impact of DoS attacks on SDN-IoV systems. This research seeks to address this gap by delving into the consequences of a particular type of DoS attack — SYN Flood — by varying its packet size and its impact to the victim car and its ability to respond during such attacks. This research study encompasses the dynamics of diverse SYN packet properties, with a special focus on different packet sizes and the implications of vehicular communication on the network's vulnerability.

1.1 Background

1.1.1 Software-Defined Internet of Vehicles (SD-IoV)

By harnessing the principles of SDN and leveraging advanced protocols, SD-IoV stands at the forefront of modernizing transportation infrastructures [6], [7]. The discussion unfolds as follows:

1. **SDN Principles and SD-IoV Architecture**: SDN is a foundation to SD-IoV, characterized by separating network management (control plane) from data traffic handling (data plane). This separation enhances centralized network governance and efficient data forwarding. The SD-IoV model extends this by integrating vehicles and infrastructure communication through Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) creating a dynamic network layer that supports various applications and services. This ecosystem allows multiple connection modes, leveraging both traditional wireless access points and innovative vehicular communication technologies. The vehicular communication would communicate through the standard of IEEE 802.11p which also known by names as Wireless Access for Vehicular Environment (WAVE) [8].

1.2 DoS Attack in IoV Contexts

DoS attack poses a significant threat to the IoV environment [9], [10]. These malicious endeavors aim to disrupt normal traffic, overwhelm network resources, and degrade essential service communication, to undermine the IoV's primary objective: seamless and efficient vehicular communication. In an IoV topology, a successful DoS attack can have dire consequences, ranging from minor disruptions in traffic communication to catastrophic failures in emergency response communications. The primary purpose of these communications is to enhance road safety, traffic efficiency, and to pave the way for seamless integration of autonomous vehicles in smart city [11].

1.2.1 Impact of DoS Attacks on Vehicular Communication:

DoS attacks aim to disrupt the regular functioning of a network by overwhelming it with traffic. In the context of vehicular communication:

Safety Implications: Safety messages in vehicular ad-hoc networks (VANETs) are time-sensitive and often prioritized based on their size and priority [15]. A successful DoS attack can impede the transmission of safety messages. If vehicles are unable to exchange safety messages, it can lead to a significant increase in the risk of collisions, especially in high-density traffic scenarios where communication between vehicles is vital for safe maneuvering. For autonomous vehicles, communication with surrounding vehicles and infrastructure is crucial for navigation and decision-making. A DoS attack can render an autonomous vehicle "blind" in terms of communication, severely affecting its capability to navigate safely [12].

Traffic Efficiency: One of the benefits of vehicular communication is the optimization of traffic flow. DoS attacks can hinder this, leading to traffic inefficiencies, longer commute times, and potential gridlocks.

1.3 Recent Works

There are many studies that relate with the DoS attack on the vehicular communication environment such as the one by al-Dhuraibi [13] which have examined the implications of DDoS attacks in VANETs. This study falls short on examining how this mobility interplays with specific attack vectors, such as SYN floods. In other study, Hosny [14] mentions that a DDoS attack can flood the IoV network with fake TCP or UDP messages, making the host unable to serve other nodes. This study focuses on the impact of UDP traffic during the DDoS attack, mentioning the use of UDP packets of 100 bytes sent. However, it does not mention conducting a similar in-depth analysis for SYN flood attacks, which are a subset of TCP-based attacks. The study by al-Rehan [15] provides a comprehensive approach to simulating UDP-based DDoS attacks in VANETs and generating a dataset that can be used for machine learning-based detection. However, it lacks exploration of SYN flood attacks in vehicular environment [15]. On the other research by Siddiqui, the study is not explicitly clear whether the DDoS attacks simulated in the study are based on TCP, UDP, or both. The attack that are being simulated is more about overwhelming the SDN controller with a large number of Packet-In messages [8]. The recent studies lack of understanding the impact of varying packet sizes in IoV—especially in understanding the nuanced effects of SYN flood attacks—which remains unaddressed. This research study aims to bridge this gap by focusing on the variabilities of data packet sizes and it impact to the vehicular communication against DoS threats.

1.4 Methodology

To create a realistic simulation of a DoS attack within SDN-IoV environment, multiple tools are integrated to handle both network and mobility aspects. The Simulation of Urban Mobility (SUMO) is employed to model traffic patterns and vehicle movement

within an urban setting. SUMO offers detailed customization of road networks, vehicle types, and routing, and it incorporates the Traffic Control Interface (TraCI) for real-time interaction between the traffic and network simulations. For network simulation, Mininet is utilized, a versatile network emulator that can create a realistic Software-Defined Networking (SDN) environment with a multiple of hosts, switches, and links. The Ryu-controller is used as a SDN controller to manage the network flow efficiently. To simulate the DoS attack, *hping3* is used to generate network traffic and alter the network TCP packet size. By integrating these tools, the methodology allows comprehensive simulation of DoS attacks in SDN-IoV. This provides a controlled environment to study the impacts of such attacks on traffic flow and impact on the network performance.

2 Results and Analysis

As vehicular communication technologies use DSRC [9], [16], [17], the evaluation of specific packet sizes becomes crucial. These 200 bytes, 360 bytes, and 1400 bytes packet size, represent various data transmission needs, from basic safety messages to extensive information sharing [16]. These sizes are repeatedly mentioned in various scenarios and environment in DSRC communication[17]. They represent standardized packet sizes used in empirical testing to assess the performance of these communication technologies. These sizes have been chosen to represent different levels of data requirements, from basic safety messages (BSMs) to more data-intensive transmissions.

- **200 bytes**: This packet size is often highlighted in discussions about the usage in vehicular communication, indicating that it is a standard measure for basic messages or signals. 200 bytes packet is frequently used in vehicular communications [16], [17].
- **360 bytes:** Specifically referenced in relation to a BSM with security certifications. 360 bytes packet size is typically used for safety messages that include security features and security information [16], [17].
- **1400 bytes**: This packet size is used for data-heavy requirements, possibly for scenarios that involve transmitting more extensive information beyond basic safety messages. The use of this larger packet size in testing may help in assessing the performance of DSRC and LTE-V2X in more data-demanding situations [16], [17].

2.1.1 TCP SYN with Various Data Packet Types DoS Threat Model

A SYN flood attack in an IoV context exploits the TCP handshake mechanism, inundating the controller with SYN requests without completing the connection establishment [18], [19]. This flood of unresolved sessions can exhaust the victim's resources, causing legitimate connection requests to be ignored. This study will use *hping3* to generate the malicious traffic and alter the packet size to 1 byte, 200 bytes, 360 bytes, and 1400 bytes. 1 byte is added to test out the maximum impact of SYN Flood during the attack interval. Car 1 will act as an attacker; Car 2 will be a victim; and Car 3 will be a benign user. Figure 1 below shows the topology of this research study, and the result is shown in Table 1 while car is stationary and Table 2 when car is moving.

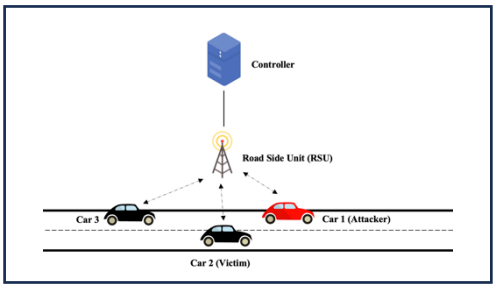

Fig. 1. The SDN-IoV topology for this research study.

When SYN data packet size is varied, the controller's task of distinguishing and handling each connection type becomes more complex [18]. This complexity can cause additional strain, increasing the likelihood of system hang-ups or crashes and potentially isolating segments of the vehicular network [19]. The attack result below is triggered during interval 30-60 seconds and the impact is illustrated in Figure 2.

Table 1. Packet throughput on different packet size when the car is stationary during the attack.

SYN Packet Size	Average Packets Throughput
1 byte	1.30 x 10^6 packets
200 bytes	4.67 x 10^6 packets
360 bytes	6.12 x 10^6 packets
1400 bytes	7.43 x 10^6 packets

Table 2. Packet throughput on different packet size when the car is moving during the attack.

SYN Packet Size	Average Packets Throughput
1 byte	3.07 x 10^6 packets
200 bytes	3.09 x 10^6 packets
360 bytes	3.48 x 10^6 packets
1400 bytes	4.23 x 10^6 packets

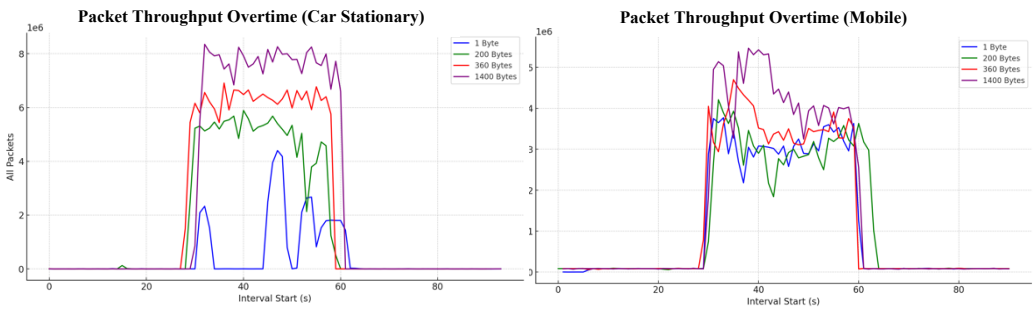

Fig. 2. The graph of the packet throughput to the car victim's interface.

1-byte packet:
Stationary – The graph shows a frequent spikes and dips to zero for period of 11 seconds, indicating the targeted system is completely unresponsive. This pattern indicates the victim being overwhelmed to the point it could not accept incoming traffic.
Mobile – The average packets throughput is 3.07 million during the attack interval. The movement introduces interference, causing the average packet is higher compared to stationary due to less effective attack.

200-byte packets:
Stationary – The total average packets throughput is 4.67 million packets, and it exhibits a significant drop between 52 and 53 second packets due to downtime, indicating a period of unresponsiveness. The recovery after the dip is also worth noting, as traffic volume surges and network attempting to catch up on delayed requests.
Mobile – The average packets received at the victim are significantly lower which is 3.09 million packets. Although there is a dip at 35 seconds due to downtime cause by the attack, it returns to the peak as it become more responsive.

360-byte packets:
Stationary - The traffic throughput is more intense and consistent compared to the smaller packet sizes. This consistency implies a continuous attack to the victim while maintaining the uptime. Unlike smaller packet size, the 360 bytes packet size observed no significant dip, showing while the network under stress, it is still responsive.
Mobile - The high peaks and deep valleys suggest a highly erratic pattern, a mark of communication experiencing interference, due to the attacker's movement, changing signal strengths, and environmental factors.

1400-byte packets:
Stationary – It shows minimal disruption in traffic due to the system's ability to buffer the traffic effectively, while operating under significant strain.
Mobile – The attack, while clearly persistent and the victim able to maintain the uptime under strain, it also shows signs of fragmentation with deep valley. This is due to the difficulties in maintaining a consistent attack on a moving target.

3 Conclusion

The conducted research on the impact of a DoS SYN flood attack to the vehicular networks shows inherent vulnerabilities that SD-IoV possess. Among all data packet sizes, 1-byte packets show the most disruptive to stationary and moving vehicular network. When the packets are sent in large numbers, these minuscule packets can cripple the target system's resource. The impact of such a high volume of small packets results in frequent and pronounced disruptions and poses severe risks, especially in real-world implementation of SD-IoV. Given the findings, it becomes unequivocally clear that vehicular networks, regardless of being stationary or moving, need to necessitate a comprehensive defensive mechanism. These defenses must be capable of countering the looming threats posed by SYN flood DoS threat.

References

[1] J. Joshi, K. Renuka, and P. Medikonda, "Secured and energy efficient data transmission in SDN-VANETs," *2018 22nd International Computer Science and Engineering Conference, ICSEC 2018*, 2018, doi: 10.1109/ICSEC.2018.8712714.

[2] J. Joshi, K. Renuka, and P. Medikonda, "Secured and energy efficient data transmission in SDN-VANETs," *2018 22nd International Computer Science and Engineering Conference, ICSEC 2018*, 2018, doi: 10.1109/ICSEC.2018.8712714.

[3] J. Joshi, K. Renuka, and P. Medikonda, "Secured and energy efficient data transmission in SDN-VANETs," *2018 22nd International Computer Science and Engineering Conference, ICSEC 2018*, 2018, doi: 10.1109/ICSEC.2018.8712714.

[4] L. Dridi and M. F. Zhani, "SDN-Guard: DoS Attacks Mitigation in SDN Networks," *Proceedings - 2016 5th IEEE International Conference on Cloud Networking, CloudNet 2016*, pp. 212–217, 2016, doi: 10.1109/CloudNet.2016.9.

[5] R. Sahbi, S. Ghanemi, and R. Djouani, "A Network Model for Internet of vehicles based on SDN and Cloud Computing," *Proceedings - 2018 International Conference on Wireless Networks and Mobile Communications, WINCOM 2018*, pp. 1–4, 2019, doi: 10.1109/WINCOM.2018.8629610.

[6] M. Arif, H. Zamrai, K. M. Yusof, and M. A. Azizan, "A Survey on Internet of Vehicle (IoV): Applications & Comparison of VANETs , IoV and SDN-IoV," no. December, 2021.

[7] M. T. Abbas, A. Muhammad, and W. C. Song, "SD-IoV: SDN enabled routing for internet of vehicles in road-aware approach," *J Ambient Intell Humaniz Comput*, vol. 11, no. 3, pp. 1265–1280, 2020, doi: 10.1007/s12652-019-01319-w.

[8] A. J. Siddiqui and A. Boukerche, "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*, pp. 1284–1289, 2018, doi: 10.1109/IWCMC.2018.8450433.

[9] H. Taslimasa, S. Dadkhah, E. C. P. Neto, P. Xiong, S. Ray, and A. A. Ghorbani, "Security issues in Internet of Vehicles (IoV): A comprehensive survey," *Internet of Things*, vol. 22, p. 100809, Jul. 2023, doi: 10.1016/J.IOT.2023.100809.

[10] Y. Otoum, Y. Wan, and A. Nayak, "Transfer Learning-Driven Intrusion Detection for Internet of Vehicles (IoV)," in *2022 International Wireless Communications and Mobile Computing (IWCMC)*, 2022, pp. 342–347. doi: 10.1109/IWCMC55113.2022.9825115.

[11] H. Taslimasa, S. Dadkhah, E. C. P. Neto, P. Xiong, S. Ray, and A. A. Ghorbani, "Security issues in Internet of Vehicles (IoV): A comprehensive survey," *Internet of Things*, vol. 22, p. 100809, 2023, doi: https://doi.org/10.1016/j.iot.2023.100809.

[12] D. M. M. Azzahar, M. Y. Darus, S. J. Elias, J. Jasmis, M. Z. Zakaria, and S. R. M. Dawam, "A Review: Standard Requirements for Internet of Vehicles (IoV) Safety Applications," *2020 5th IEEE International Conference on Recent Advances and Innovations in Engineering, ICRAIE 2020 - Proceeding*, vol. 2020, pp. 1–5, 2020, doi: 10.1109/ICRAIE51050.2020.9358383.

[13] W. A. Al-Dhuraibi and M. Elhadef, "Securing vehicular Ad-Hoc networks: A DDoS case study," in *Proceedings of 2nd International Conference on Computation, Automation and Knowledge Management, ICCAKM 2021*, Institute of Electrical and Electronics Engineers Inc., Jan. 2021, pp. 112–117. doi: 10.1109/ICCAKM50778.2021.9357733.

[14] H. M. Hosny, N. Sadek, and O. A. Abdel-Alim, "Security of 5G-IOV Networks:DDOS Case Study," in *International Telecommunications Conference,*

ITC-Egypt 2022 - Proceedings, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/ITC-Egypt55520.2022.9855708.

[15] F. A. Alhaidari and A. M. Alrehan, "A simulation work for generating a novel dataset to detect distributed denial of service attacks on Vehicular Ad hoc NETwork systems," *International Journal of Distributed Sensor Networks*, vol. 17, no. 3. SAGE Publications Ltd, 2021. doi: 10.1177/15501477211000287.

[16] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162–1182, 2011, doi: 10.1109/JPROC.2011.2132790.

[17] E. Moradi-Pari, D. Tian, M. Bahramgiri, S. Rajab, and S. Bai, "DSRC Versus LTE-V2X: Empirical Performance Analysis of Direct Vehicular Communication Technologies," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 5, pp. 4889–4903, May 2023, doi: 10.1109/TITS.2023.3247339.

[18] R. Swami, M. Dave, and V. Ranga, "Detection and Analysis of TCP-SYN DDoS Attack in Software-Defined Networking," *Wirel Pers Commun*, vol. 118, no. 4, pp. 2295–2317, 2021, doi: 10.1007/s11277-021-08127-6.

[19] J. L. Kuo, C. H. Shih, and Y. C. Chen, "Performance analysis of real-time streaming under TCP and UDP in VANET via OMNET," *2013 13th International Conference on ITS Telecommunications, ITST 2013*, no. October 2014, pp. 116–121, 2013, doi: 10.1109/ITST.2013.6685531.