

Course Title: Research Methodology in Computer Science **Course Code:** AI800

Weighting: 30 %

Lecturer: Dr. Mohammed Anbar

Hand-out Date: 6 July 2024

Hand-in Date: 4 Aug 2024

Hand-in Method: Online Submission via E-Learning.

RoadGuard: Robust Real-Time DDoS Defense for Next-Generation Vehicular Networks

Name: Mahmoud Salem

ID: 242001469

Table of content:

#	Item	Page
1	Problem Statement	3
2	Research Objectives:	4,5
3	References	7

Problem statement:

The domain of this research focuses on the critical domain of cybersecurity in Vehicular Ad Hoc Networks to detect and mitigate Distributed Denial of Service (DDoS) assaults in vehicular ad hoc networks (VANETs), which are dynamic and complicated networks. This research focuses on the crucial area of cybersecurity in VANETs.

VANETs are becoming more and more vulnerable to a range of cyberthreats, and DDoS attacks represent a serious and expanding danger to network performance and availability . Unique characteristics of VANETs, such as their mobile and dynamic nature and their high-speed, high-volume data streams, provide challenges for current detection methods. The crucial nature of VANET connections, where any disruption can have serious consequences for traffic control and road safety, makes this problem even more difficult.

Since VANETs are essential to the creation of intelligent transportation systems, effective DDoS detection is essential to guaranteeing their reliability and security. undetected denial-of-service (DDoS) attacks have the ability to interfere with vital vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications, which may cause traffic jams or even potentially fatal safety risks. Our transportation infrastructure is becoming more and more dependent on the security of VANETs as smart cities and autonomous cars proliferate.

Existing solutions provide advanced approaches utilizing deep learning and Software-Defined Networking (SDN) as well as more traditional methods for machine learning like Support Vector Machines (SVM) and K-Nearest Neighbors (KNN) (Galgotias University. School of Computing Science and Engineering et al., n.d.). Scalability, real-time performance, and adaptability to changing attack patterns are frequently limited with these methods (Al-Mehdhara & Ruan, 2021). Furthermore, they often fail to recognize the particular limitations of VANET contexts, namely low-latency detection requirements and the restricted computational capacity of vehicular nodes(Gao et al., 2019; Polat et al., 2020; Poongodi et al., 2019; Türkoğlu et al., 2022).

Although DDoS detection for traditional networks has advanced significantly, the unique characteristics of VANETs present new difficulties that remain to be completely addressed. Because VANETs have intermittent connections and quickly changing network topologies, it is challenging to implement traditional security solutions successfully due to their extremely dynamic nature. Furthermore, the development of comprehensive and effective solutions has been hampered by the strict real-time requirements and resource limits of vehicular nodes. In the context of VANETs, the quick development of DDoS attack tactics has likewise overtaken the creation of reliable detection mechanisms.

Although there has been development, there are still large gaps in DDoS detection for VANETs. Solutions that can efficiently expand to support large-scale VANET deployments are desperately needed. Operation with great accuracy and minimal false positive rates in real-time. Adapt to evolving attack patterns and new DDoS attack kinds targeted at VANETs. Take care of privacy issues without sacrificing security. Easily incorporate into the current VANET standards and protocols. Operate effectively on vehicular nodes with limited resources.

Research Objectives:

A high-tech, flexible, and private DDoS detection system for vehicular ad hoc networks (VANETs) is what we want to make. It should be able to work in real time, change to new attack patterns, and make good use of the limited computer power that is available.

To design a distributed detection system that works well with VANETs' changing topology and can handle large-scale operations, this will solve the problem of network scalability and flexibility to changing network structures.

To implement a real-time, low-latency detection system that meets the strict timing needs of vehicular communications while keeping high accuracy and low false positive rates. This will help meet the urgent need for quick and accurate threat identification in busy VANET settings.

To develop an adaptable framework that can change over time to find new and emerging DDoS attack patterns that are special to VANETs. This will help solve the problem of cyber threats in vehicular networks that are changing quickly.

To add privacy-protecting methods to the detection system, handling the important balance between privacy and security in VANET settings and resolving the conflict between strong security measures and protecting user privacy

To create a lightweight detection algorithm that can work with vehicle nodes that don't have a lot of resources. This will allow for efficient operation without sacrificing detection skills, which will solve the problem of limited computing power in vehicle systems.

To propose a way to easily and seamlessly connect the new system to existing VANET protocols and standards, making sure that they work together and can be used. This will help solve the problem of adding new security solutions to VANET platforms that are already in place.

To evaluate how well the suggested system works in terms of scalability, real-time operation, adaptability, privacy protection, and resource efficiency by running a lot of simulations and, if possible, using real-world VANET testbeds. This will meet the need for thorough and useful validation of the solution.

To compare how the suggested system stacks up against current DDoS detection methods for VANETs, showing how it can better handle the specific problems these networks face and giving a clear picture of how far it has come compared to the best methods used so far.

An advanced DDoS monitoring system made just for VANETs to deal with the particular challenges that these networks have. A distributed and flexible detection system that can handle large-scale VANET deployments and change with the topology of the network.

A real-time, low-latency detection system that works well in the fast-paced VANET setting and has a high level of accuracy and low false positive rates. A flexible system that may evolve over time to find new DDoS attack trends in VANETs.

An effective way to identify threats while protecting users' privacy, taking into account both security needs and privacy concerns. A simple detection method which performs best for vehicle nodes with limited resources. A method to make the new system work with VANET protocols and standards that are currently in place. Comprehensive performance test outcomes showing how well the system performs in terms of being able to scale, run in real time, adapt, protect data, and use resources efficiently. A comparison of the suggested system to other DDoS detection systems for VANETs that shows how it is better. Addition to what we know about VANET security, which might influence the direction of future research and how the industry works. Research results should be published in high-impact journals and presented at international conferences that are important. VANET operations in the real world might employ this technology, which would help make smart transportation systems safer.

References:

- Al-Mehdhara, M., & Ruan, N. (2021). MSOM: Efficient Mechanism for Defense against DDoS Attacks in VANET. *Wireless Communications and Mobile Computing*, 2021. <https://doi.org/10.1155/2021/8891758>
- Galgotias University. School of Computing Science and Engineering, Institute of Electrical and Electronics Engineers. Uttar Pradesh Section, & Institute of Electrical and Electronics Engineers. (n.d.). *2018 4th International Conference on Computing Communication and Automation (ICCCA)*.
- 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. <https://doi.org/10.1109/ACCESS.2019.2948382>
- Polat, H., Turkoglu, M., & Polat, O. (2020). Deep network approach with stacked sparse autoencoders in detection of DDoS attacks on SDN-based VANET. *IET Communications*, 14(22), 4089–4100. <https://doi.org/10.1049/iet-com.2020.0477>
- Poongodi, M., Hamdi, M., Sharma, A., Ma, M., & Singh, P. K. (2019). DDoS Detection Mechanism Using Trust-Based Evaluation System in VANET. *IEEE Access*, 7, 183532–183544. <https://doi.org/10.1109/ACCESS.2019.2960367>
- Türkoğlu, M., Polat, H., Koçak, C., & Polat, O. (2022). Recognition of DDoS attacks on SD-VANET based on combination of hyperparameter optimization and feature selection. *Expert Systems with Applications*, 203. <https://doi.org/10.1016/j.eswa.2022.117500>