



A Hybrid and Scalable Framework for Detection and Mitigation of DDoS Attacks in Vehicular Ad Hoc Networks (VANETs)

Course Code: AI800

Course Title: Research Methodology in Computer Science

Lecturer: Dr. Mohammed Anbar

Student ID: 261001995

Student Name: Amro Ismail Mohamed

Table of Contents

- 1. Problem Statement
- 2. Research Objectives
- 3. Reference

1. Problem Statement

Vehicular Ad Hoc Networks (VANETs) represent a critical component of Intelligent Transportation Systems (ITS), enabling real-time communication among vehicles and roadside units. However, due to their distributed and highly dynamic nature, VANETs are particularly vulnerable to Distributed Denial of Service (DDoS) attacks. These attacks can disrupt communication channels, degrade network performance, and compromise road safety.

Several existing studies have attempted to detect and mitigate DDoS attacks in VANET environments using different approaches. Machine learning-based models such as hybrid KNN-SVM (Kadam & Sekhar, 2021) and hybrid SVM kernels (Adhikary et al., 2020) have demonstrated improved detection accuracy compared to single classifiers. Similarly, distributed intrusion detection systems using Random Forest and big data frameworks such as Apache Spark achieved high detection rates (Gao et al., 2019). Trust-based evaluation systems have also been proposed to enhance detection reliability and reduce energy consumption (Poongodi et al., 2019). Moreover, SDN-based mechanisms combined with multilayer SOM architectures showed promising detection accuracy and improved throughput (Al-Mehdhara & Ruan, 2021), while bandwidth-threshold greedy approaches aimed at reducing packet loss and improving mitigation efficiency (Guleria & Verma, 2018).

Despite these advancements, significant challenges remain. Most of the existing solutions rely heavily on simulation environments or benchmark datasets rather than real-world VANET traffic (Kadam & Sekhar, 2021; Adhikary et al., 2020; Gao et al., 2019). Additionally, complex models such as trust-based systems and SDN-SOM architectures introduce high computational overhead and architectural complexity, which may not be suitable for highly dynamic vehicular environments (Poongodi et al., 2019; Al-Mehdhara & Ruan, 2021). Furthermore, there is a trade-off between detection accuracy, scalability, computational efficiency, and real-time performance that has not been comprehensively addressed across existing studies.

The significance of this problem lies in the safety-critical nature of VANET applications. Failure to detect or mitigate DDoS attacks in real time can result in delayed safety messages, increased packet loss, and potentially hazardous traffic conditions. Therefore, there is a need for a scalable, lightweight, and accurate detection and mitigation framework that integrates the strengths of existing machine learning, trust-based, and distributed approaches while addressing their limitations.

This research aims to develop a comprehensive and scalable hybrid framework capable of achieving high detection accuracy, low false alarm rate, reduced computational overhead, and improved real-time mitigation performance in VANET environments.

2. Research Objectives

To design and develop a scalable and efficient hybrid framework for detecting and mitigating DDoS attacks in VANETs that balances detection accuracy, computational efficiency, and real-time performance.

- **To analyze** the limitations and challenges of existing DDoS detection and mitigation techniques in VANETs, including machine learning, trust-based, SDN-based, and distributed approaches.
- **To evaluate** the performance trade-offs among detection accuracy, scalability, computational overhead, and real-time responsiveness in current solutions.

- **To design** a hybrid detection model that integrates machine learning techniques with lightweight trust or traffic-monitoring mechanisms to improve robustness.
- **To develop** an efficient mitigation mechanism that reduces packet loss and maintains network throughput during DDoS attacks.
- **To implement and test** the proposed framework using realistic VANET simulation environments and benchmark datasets.
- **To compare** the proposed framework with existing approaches in terms of detection rate, false positive rate, scalability, energy consumption, and network performance metrics.

3. References

- ✚ Ms.Nivedita Kadam, Dr. Krovi Raja Sekhar (2021). Machine Learning Approach of Hybrid KSVN Algorithm to Detect DDoS Attack in VANET.
- ✚ Charu Guleria, Harsh Kumar Verma (2018). Improved Detection and Mitigation of DDoS Attack in Vehicular ad hoc Network.
- ✚ M. POONGODI , MOUNIR HAMDI , ASHUTOSH SHARMA 2, AND PRADEEP KUMAR SINGH (2019). DDoS Detection Mechanism Using Trust-Based Evaluation System in VANET.
- ✚ YING GAO , HONGRUI WU , BINJIE SONG, YAQIA JIN, XIONGWEN LUO, AND XING ZENG (2019). A Distributed Network Intrusion Detection System for Distributed Denial of Service Attacks in Vehicular Ad Hoc Network.
- ✚ Mohammed Al-Mehdhara and Na Ruan (2021). MSOM: Efficient Mechanism for Defense against DDoS Attacks in VANET.
- ✚ Kaushik Adhikary¹ · Shashi Bhushan² · Sunil Kumar³ · Kamlesh Dutta (2020). Hybrid Algorithm to Detect DDoS Attacks in VANETs.

<https://www.dropbox.com/scl/fo/jstgybsb9hbqrong6djvg/h?rlkey=8fbl0f7z6o9aqdb1i6wp6uo4e&dl=0>

(Detecting DDOS in VANET)