



A Hybrid and Scalable Framework for Detection and Mitigation of Distributed Denial of Service (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. Abstract
- 2. Introduction
 - Background
 - Characteristics of VANET
 - DDoS Attacks in VANET
- 3. Problem Statement
- 4. Research Objectives
- 5. Research Scope
- 6. Literature Review
- 7. Research Methodology
 - Phase 1: Literature Review
 - Phase 2: Qualitative Analysis
 - Phase 3: Quantitative Simulation
 - Phase 4: Framework Development and Validation
- 8. Ethical Considerations
- 9. Limitations
- 10. Expected Outcomes
- 11. Gantt Chart
- 12. References

1. Summary of the Research Papers

Vehicular Ad Hoc Networks (VANETs) represent a fundamental component of Intelligent Transportation Systems (ITS), enabling real-time communication between vehicles and roadside units to enhance road safety and traffic efficiency.

However, the distributed and highly dynamic nature of VANET exposes them to significant cybersecurity threats, particularly Distributed Denial of Service (DDoS) attacks.

DDoS attacks aim to disrupt network availability by overwhelming communication channels with malicious traffic, leading to increased latency, packet loss, and degraded throughput.

Existing detection mechanisms, including machine learning classifiers, trust-based models, and SDN-based architectures, often suffer from scalability limitations, high computational overhead, or reliance on centralized infrastructures.

This research proposes a hybrid and scalable framework that integrates lightweight machine learning algorithms with distributed traffic monitoring mechanisms at the RSU level.

The framework aims to enhance detection accuracy while minimizing delay and resource consumption.

The proposed solution will be evaluated using realistic VANET simulation environments and benchmark datasets to measure detection rate, false positive rate, throughput, and latency performance.

2. Introduction

VANETs enable Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication, supporting safety-critical applications such as collision warnings, emergency notifications, and traffic management.

Due to their wireless and decentralized structure, VANETs face numerous security challenges that threaten communication reliability.

Background

VANETs consist of On-Board Units (OBUs) installed in vehicles and Roadside Units (RSUs) deployed along roads.

Communication occurs using DSRC or cellular technologies. The high mobility of nodes and constantly changing topology introduce unique security challenges compared to traditional networks.

Characteristics of VANET

- ✓ High node mobility
- ✓ Dynamic topology
- ✓ Low latency requirements
- ✓ Short-lived communication sessions
- ✓ Distributed architecture

DDoS Attacks in VANET

In a DDoS attack, multiple compromised vehicles flood the network with excessive traffic, preventing legitimate vehicles from exchanging safety messages.

These attacks may result in congestion, reduced packet delivery ratio, and delayed emergency alerts, potentially causing real-world accidents.

3. Problem Statement

Despite significant research efforts in detecting DDoS attacks in VANETs, existing solutions exhibit critical limitations.

Machine learning-based approaches often require extensive computational resources, while trust-based and SDN-based models introduce architectural complexity and scalability concerns.

Many studies focus on detection accuracy without adequately addressing network performance degradation during attacks.

There remains a need for a lightweight, scalable, and distributed framework that balances detection accuracy, computational efficiency, and real-time mitigation performance in dynamic VANET environments.

4. Research Objectives

- ✚ **To analyze** current DDoS detection mechanisms in VANET environments.
- ✚ **To identify** scalability and performance limitations in existing approaches.
- ✚ **To design** a hybrid detection framework integrating ML and distributed monitoring.
- ✚ **To implement** a mitigation strategy that minimizes network disruption.
- ✚ **To evaluate** system performance using simulation metrics.

5. Research Scope

This research focuses on flooding-based DDoS attacks in VANET environments.

The study emphasizes hybrid detection strategies and performance optimization using simulation tools such as NS-3. Cryptographic authentication enhancements are beyond the scope of this proposal.

6. Literature Review

Recent studies have proposed various DDoS detection mechanisms in VANETs. Hybrid KNN-SVM classifiers demonstrated improved classification accuracy compared to standalone models.

Random Forest-based distributed intrusion detection systems enhanced scalability but increased computational load.

Trust-based evaluation systems improved reliability by assigning trust scores to vehicles.

However, these methods introduced processing overhead.

SDN-based architectures enabled centralized monitoring but created single-point-of-failure risks.

Recent advancements (2022–2024) explore edge computing and federated learning approaches to distribute detection tasks and improve scalability.

However, comprehensive frameworks that integrate scalability, low latency, and high detection accuracy remain limited.

7. Research Methodology

Phase 1: Literature Review

A systematic literature review will be conducted using IEEE Xplore, SpringerLink, and ScienceDirect databases.

Phase 2: Qualitative Analysis

Comparative analysis of existing detection frameworks will be performed to identify performance gaps and scalability limitations.

Phase 3: Quantitative Simulation

The proposed framework will be implemented using NS-3 simulator to generate realistic VANET traffic scenarios under DDoS attack conditions.

Phase 4: Framework Development and Validation

A hybrid architecture integrating lightweight Random Forest classifier and distributed RSU monitoring will be developed and validated against benchmark models.

8. Ethical Considerations

- ✦ This research does not involve human participants or personal data.
- ✦ All datasets used will be publicly available and anonymized.
- ✦ The framework is designed strictly for defensive cybersecurity purposes.

9. Limitations

Simulation-based evaluation may not fully represent real-world deployment challenges.

Additionally, hardware constraints of actual vehicular systems may affect implementation feasibility.

10. Expected Outcomes

- ✦ Detection accuracy above 97–98%
- ✦ Reduced false positive rate
- ✦ Improved throughput under attack scenarios
- ✦ Lower end-to-end delay compared to existing models

11. Gantt Chart – Research Timeline

Task	Nov	Dec	Jan	Feb	Mar
Literature Review	■	■			
Qualitative Analysis		■			
Framework Design		■	■		
Simulation Implementation			■	■	
Performance Evaluation				■	
Final Report Writing				■	■

12. 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)