

Detection and Mitigation of DDoS Attacks in VANET Using Multilayer Self-Organizing Map (MSOM)

Research Proposal

Student Name: Ghurmallah Salem Mohammed Alqarni

Course: AI800 – Research Methodology in Computer Science

Table of Contents

1. Abstract
2. Chapter 1 – Introduction
3. Chapter 2 – Literature Review
4. Chapter 3 – Research Methodology
5. Conclusion
6. References

Abstract

Vehicular Ad Hoc Networks (VANETs) play a major role in Intelligent Transportation Systems by enabling real-time communication between vehicles and roadside units. However, their wireless nature makes them vulnerable to Distributed Denial of Service (DDoS) attacks. Previous research proposed several detection models, including hybrid machine-learning methods (Adhikary et al., 2020), cluster-based routing analysis (Kolandaishamy et al., 2020), two-stage detection mechanisms (Guleria & Verma, 2018), trust-based systems (Poongodi et al., 2019), and distributed big-data intrusion detection models (Gao et al., 2019).

Most of these studies improved detection accuracy but relied heavily on simulation and faced scalability and latency issues.

This research aims to develop a Multilayer Self-Organizing Map (MSOM) integrated into distributed Software-Defined Networking (SDN) to enhance accuracy, reduce latency, and improve load distribution. Real datasets such as CAIDA (2015), DARPA (2009), and NSL-KDD (2009) are used for evaluation. Expected outcomes include achieving accuracy above 99%, reducing CPU load, and improving throughput.

Chapter 1 - Introduction

1.1 Introduction

Vehicular Ad Hoc Networks (VANETs) enable vehicles and roadside units to exchange information in real time, improving road safety and traffic efficiency. However, because VANETs operate in an open wireless environment, they are susceptible to Distributed Denial of Service (DDoS) attacks that disrupt communication and impact safety-critical applications (Guleria & Verma, 2018; Adhikary et al., 2020).

Multiple detection mechanisms have been proposed, including hybrid ML-based techniques (Adhikary et al., 2020), trust-based cluster models (Kolandaishamy et al., 2020), and SDN-enhanced detection frameworks (Al-Mehdhara & Ruan, 2021).

However, many still struggle with VANET mobility, scalability, and central controller overload (Al-Mehdhara & Ruan, 2021). This highlights the need for a distributed, scalable detection framework using intelligent learning.

1.2 Background

1.2.1 VANET Architecture

VANETs use V2V and V2I communication. These modes enhance safety but increase exposure to malicious traffic injection (Guleria & Verma, 2018).

1.2.2 DDoS Attacks in VANET

DDoS attacks flood the network with malicious packets, increasing delay and causing packet loss (Adhikary et al., 2020; Guleria & Verma, 2018).

1.2.3 SDN in VANET

Software-Defined Networking offers centralized management and programmable control but suffers from latency and controller bottlenecks under attack (Al-Mehdhara & Ruan, 2021; Floodlight, 2020).

1.2.4 SOM and MSOM

SOM is widely used for anomaly detection (Adhikary, 2018), but struggles with heterogeneous data. Multilayer SOM (MSOM) improves scalability and accuracy using distributed learning (Al-Mehdhara & Ruan, 2021).

1.3 Problem Statement

VANETs are highly vulnerable to DDoS attacks due to node mobility and wireless communication. While existing models such as SVM hybrids (Adhikary et al., 2020), SPPA trust models (Kolandaishamy et al., 2020), greedy mitigation

(Guleria & Verma, 2018), distributed ML models (Gao et al., 2019), and trust-matrix evaluation systems (Poongodi et al., 2019) have improved detection accuracy, they still suffer from overhead, high latency, and limited scalability.

SDN-based VANETs rely heavily on centralized controllers that risk failure under heavy attack traffic (Al-Mehdhara & Ruan, 2021).

Thus, a distributed, multilayer detection framework is required.

1.4 Research Objectives

1. Analyze DDoS vulnerabilities in SDN-based VANET systems (Guleria & Verma, 2018; Al-Mehdhara & Ruan, 2021).
2. Design a distributed MSOM model to improve detection accuracy and reduce latency (Al-Mehdhara & Ruan, 2021).
3. Evaluate using CAIDA (2015), DARPA (2009), and NSL-KDD (2009).
4. Provide recommendations for real-world adoption of MSOM.

1.5 Research Scope

This study focuses on detecting DDoS attacks using MSOM integrated within distributed SDN controllers.

Scope includes:

- TCP/ICMP flooding (Adhikary et al., 2020; Guleria & Verma, 2018; Al-Mehdhara & Ruan, 2021)
- Evaluation datasets: CAIDA (2015), DARPA (2009), NSL-KDD (2009)
- Performance metrics: accuracy, delay, throughput, CPU load

Excludes hardware deployment and non-DDoS attacks.

Chapter 2 - Literature Review

2.1 Summary of Previous Studies

2.1.1 Hybrid SVM Model

Achieved 96.5% accuracy using SVM kernels (Adhikary et al., 2020).

Limitation: simulation-only evaluation.

2.1.2 SPPA Model

Trust-based cluster routing with high detection accuracy (Kolandaismy et al., 2020).

Limitation: high computational cost.

2.1.3 Greedy Two-Stage Model

Simulates and mitigates DDoS using a greedy strategy (Guleria & Verma, 2018).

Limitation: applicable only to specific attack types.

2.1.4 MSOM Model

Achieved 99.67% detection accuracy using multilayer SOM and SDN (Al-Mehdhara & Ruan, 2021).

Limitation: SDN central controller risk.

2.1.5 Distributed NIDS

Uses Spark and Random Forest, achieving an accuracy of 99.95% (Gao et al., 2019).

Limitation: no real vehicular testing.

2.1.6 Trust-Matrix Model

Energy-efficient and accurate (Poongodi et al., 2019).

Limitation: requires tuning many parameters.

2.2 Comparative Analysis Table

Study	Approach	Strengths	Limitations
(1)	Hybrid SVM	High accuracy	Simulation-based evaluation only
(2)	Cluster-Based SPPA	Reduces false positives	High computational cost
(3)	Greedy Method	Low overhead	Limited to a single attack type
(4)	MSOM + SDN	99.67% accuracy	Risk of SDN central controller failure
(5)	Random Forest + Spark	High scalability	No real-world testing
(6)	Trust Matrix	Energy-efficient	Requires extensive parameter tuning

2.3 Discussion & Synthesis

2.3.1 Common Trends

- Heavy reliance on ML algorithms such as SVM, SOM, Random Forest (Adhikary et al., 2020; Al-Mehdhara & Ruan, 2021; Gao et al., 2019).
- Strong emphasis on accuracy, detection rate, and delay reduction.
- Most studies rely on simulators such as NS2 or Spark (Guleria & Verma, 2018; Gao et al., 2019).

2.3.2 Conflicts

- **Centralized vs. Distributed:** MSOM uses central SDN but distributed NIDS avoids controller bottlenecks (Al-Mehdhara & Ruan, 2021; Gao et al., 2019).
- **Machine Learning vs. Behavioral Evaluation:** Trust systems rely on node behavior, ML-based systems rely on training (Poongodi et al., 2019 vs. Adhikary et al., 2020).
- **Accuracy vs. Resource Cost:** SPPA achieves accuracy but with high computational load (Kolandaisamy et al., 2020).

2.3.2 Overall Conclusion

MSOM and distributed systems are promising for VANET security, but real-world testing remains limited.

Chapter 3 - Research Methodology

3.1 Overview

MSOM is integrated into distributed SDN architecture for improved scalability (Al-Mehdhara & Ruan, 2021).

3.2 Architecture

- **ENBC:** Main controller
- **RSC:** Local detection using DSOM/CSOM
- **Vehicle Agents:** OpenFlow-based nodes (Floodlight, 2020)

3.3 MSOM Workflow

Based on DSOM training, CSOM classification, refinement, merging, distributed updating, and attack mitigation (Al-Mehdhara & Ruan, 2021).

3.4 Datasets

CAIDA (2015), DARPA (2009), NSL-KDD (2009).

3.5 Evaluation Metrics

Accuracy, detection rate, end-to-end delay, CPU load, throughput (Al-Mehdhara & Ruan, 2021).

3.6 Expected Outcomes

- 99% accuracy.
- 15–20 ms latency.
- Lower CPU usage.
- 12% throughput improvement.

3.7 Gantt Chart

Research Tasks / Timeline (Weeks)	Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7	Week 8
Topic Selection & Proposal Writing								
Literature Review								
MSOM–SDN Model Design								
Dataset Collection & Preprocessing								
Implementation & Simulation								
Performance Evaluation								
Results Analysis								
Thesis Writing								
Final Review & Submission								

Conclusion

VANETs are critical for transportation safety but vulnerable to DDoS attacks. Prior studies demonstrate progress, yet limitations remain in scalability and real-world validation. The proposed MSOM-SDN framework offers a distributed and accurate solution, with significant improvements expected in detection rates, latency, and network stability.

References

Journal Articles & Conference Papers

Adhikary, K., Bhushan, S., Kumar, S., & Dutta, K. (2020). Hybrid algorithm to detect DDoS attacks in VANETs.

Wireless Personal Communications.

Kolandaisamy, R., Noor, R. M., Ahmedy, I., & Kiah, M. L. M. (2020). Stream Position Performance Analysis (SPPA) model for cluster-based routing in VANET. *Journal of Ambient Intelligence and Humanized Computing.*

Guleria, C., & Verma, H. (2018). Improved detection and mitigation of DDoS attack in vehicular ad hoc network (VANET). *2018 IEEE International Conference on Computing, Communication and Automation (ICCCA).*

Al-Mehdhara, M., & Ruan, N. (2021). MSOM: Efficient mechanism for defense against DDoS attacks in VANET.

Wireless Communications and Mobile Computing, 2021, Article 8891758.

Gao, Y., Wu, H., Song, B., et al. (2019). A distributed network intrusion detection system for DDoS attacks in VANET.

IEEE Access.

Poongodi, M., Hamdi, M., Sharma, A., Ma, M., & Singh, P. K. (2019). DDoS detection mechanism using trust-based evaluation system in VANET. *IEEE Access.*

Datasets (APA formatting)

CAIDA. (2015). *CAIDA DDoS attack dataset*. Center for Applied Internet Data Analysis.

DARPA. (2009). *DARPA intrusion detection evaluation dataset 2009*. Defense Advanced Research Projects Agency.

NSL-KDD. (2009). *NSL-KDD dataset for network intrusion detection*.

Books / Technical Documentation

Adhikary, A. (2018). *Self-organizing maps for network security*.

Project Floodlight. (2020). *Floodlight SDN controller documentation*.