

Efficient Mechanism for Defense against DDoS Attacks in VANET Using MSOM

Problem Statement

Vehicular Ad Hoc Networks (VANETs) are a core component of Intelligent Transportation Systems (ITS), designed to enhance road safety, traffic management, and communication between vehicles and roadside infrastructure. However, the **wireless and decentralized nature of VANETs** exposes them to various cybersecurity threats, most notably, **Distributed Denial of Service (DDoS) attacks**, which can cripple network availability, delay data transmission, and compromise vehicular safety.

Traditional DDoS defense mechanisms in VANETs and Software-Defined Networking (SDN) architecture often suffer from **centralized bottlenecks**, high latency, and limited scalability. Furthermore, most existing Self-Organizing Map (SOM)-based detection models rely on a **single-layer structure**, which reduces their ability to handle large-scale dynamic traffic in real time.

To address these challenges, this research proposes an **efficient Multilayer Self-Organizing Map (MSOM)** integrated with a **Software-Defined VANET architecture**. This design aims to improve real-time DDoS detection, enhance classification accuracy, and ensure distributed control without compromising performance or scalability.

Research Objectives

- 1. To analyze DDoS vulnerabilities in VANET-based SDN environments**
 - Identify critical weaknesses in centralized DDoS defense models.
 - Examine latency, overhead, and scalability issues associated with conventional detection mechanisms.
- 2. To design and develop the MSOM-based defense architecture**
 - Combine distributed SDN controllers with multilayer SOM learning.
 - Enable both supervised and unsupervised learning for real-time traffic classification.
- 3. To evaluate the proposed MSOM approach**
 - Measure performance in terms of detection rate, accuracy, delay, and throughput.

- Compare MSOM results with Single SOM and Distributed SOM (DSOM) mechanisms.

4. To propose implementation guidelines for secure VANET systems

- Develop strategies for deploying MSOM in real-world vehicular networks.
- Provide recommendations for policymakers and system developers.

Literature Review

1. DDoS Threats in VANETs

VANETs are highly dynamic wireless networks where vehicles communicate through Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) channels. While these networks enable efficient data exchange, they are **vulnerable to DDoS flooding attacks** that exhaust bandwidth and computational resources, leading to severe communication delays or system crashes. Studies such as [3] highlight the **fatal consequences** of DDoS attacks on time-sensitive vehicular applications.

2. Software-Defined Networking (SDN) in VANETs

SDN introduces a **centralized control plane** and **programmable network management**, offering flexibility and dynamic security policy enforcement. However, traditional SDN architecture faces **single points of failure** and **latency issues** under heavy attack loads. Recent works [12][16] emphasize the need for **distributed and intelligent SDN controllers** to handle DDoS threats more effectively.

3. Self-Organizing Maps (SOMs) for Attack Detection

SOMs are **neural network models** used for clustering and anomaly detection. Prior research [9][14] demonstrates their capability to detect malicious traffic patterns in network systems. However, standard **SOM** suffers from limited scalability and potential performance degradation when trained on heterogeneous vehicular data. Therefore, improving SOM efficiency and distribution is critical for VANET-based DDoS defense.

4. The Multilayer Distributed SOM (MSOM) Approach

The MSOM model enhances conventional SOM by introducing:

- **Two-layer clustering and classification** (DSOM + CSOM).
- **Distributed learning** across multiple SDN controllers.

- **Pearson-based correlation distance metrics** for improved accuracy.

This hybrid design allows **real-time attack detection and mitigation** while maintaining low computational overhead. Experimental results indicate that MSOM achieves **99.67% accuracy** and faster recovery compared to baseline SOM models.

Proposed Framework

The proposed architecture integrates **MSOM modules within SDN controllers** in a distributed VANET environment. It consists of:

1. **Evolved Node Base Controllers (ENBC)** global control units managing policy enforcement and MSOM synchronization.
2. **Roadside Controllers (RSC)** local nodes responsible for real-time DDoS detection using DSOM and CSOM modules.
3. **Vehicle Agents** — local OpenFlow switches that apply flow rules and perform lightweight monitoring.

The system operates in six main phases:

1. DSOM Training
2. CSOM Classification
3. Feedback and Refinement
4. MSOM Merging
5. Distributed Updating
6. Attack Classification and Mitigation

This multi-phase approach enables **low-latency DDoS detection, adaptive learning, and cooperative mitigation** among controllers.

Experimental Evaluation

Simulation results using **CAIDA, NSL-KDD, and DARPA datasets** show:

- **Detection Rate:** 99.10%
- **Accuracy:** 99.67%
- **End-to-End Delay:** 15–20 ms
- **Improved Throughput:** +12% over standard SOM
- **Reduced CPU Load:** by 30–40% compared to centralized SDN models

The MSOM model demonstrated superior performance in handling both **TCP and ICMP flooding attacks**, maintaining stable **Packet Delivery Ratios (PDR)** and **low packet drop rates** under heavy load conditions.

Conclusion

This study presents an efficient **MSOM-based defense mechanism** for DDoS attacks in VANET environments. By leveraging the **programmability of SDN** and the **adaptive learning capabilities of neural networks**, the proposed system achieves high detection accuracy, distributed scalability, and minimal latency.

The findings confirm that **MSOM significantly enhances network resilience** against DDoS attacks while ensuring continuous vehicular communication and safety. Future research may extend this framework to address **privacy preservation, energy efficiency, and edge-computing integration** in next-generation intelligent transport systems.

References

1. Al-Mehdhara, M., & Ruan, N. (2021). *MSOM: Efficient Mechanism for Defense against DDoS Attacks in VANET*. *Wireless Communications and Mobile Computing*, 2021, Article ID 8891758. <https://doi.org/10.1155/2021/8891758>
2. Floodlight SDN Controller Documentation (2020).
3. CAIDA Dataset (2015). *Center for Applied Internet Data Analysis*.
4. DARPA Intrusion Detection Dataset (2009).
5. NSL-KDD Dataset (2009). *Network-Based Intrusion Detection*.

6. Adhikary, A. (2018). *Self-Organizing Maps for Network Security*.