

Enhancing Detect & Defense against DDoS Attacks in VANETs

Course Title: Research Methodology in Computer Science

Course Code: AI800

Weighting: 30%

Lecturer: Dr. Mohammed Anbar

Hand-out Date: 22 February 2025

Hand-in Date: 15 March 2025

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

Student ID: 251001992

Student Name: Meshal Alkhaldi

Problem Statement: In the domain of **Vehicular Ad Hoc Networks (VANETs)**, a critical challenge lies in **detecting and mitigating Distributed Denial-of-Service (DDoS) attacks**, which threaten network availability, safety-critical communications, and data integrity. Despite advancements in machine learning (ML) and hybrid algorithms, existing solutions face some limitations such as **scalability in dynamic environments**, **reliance on centralized controllers** (which is known a single point of failure), and **dependence on pre-established trust relationships** (Türkoğlu et al., 2022; Poongodi et al., 2019). For instance, while hybrid SVM models achieve high accuracy (Adhikary et al., 2020), they struggle with real-time adaptability in large-scale VANETs. Similarly, trust-based systems (Poongodi et al., 2019) need prior trust knowledge, which is impractical in open vehicular environments. These limitations hinder the deployment of robust defenses, leading to **delayed incident response, compromised vehicle safety, and degraded network performance** (Al-Mehdhara & Ruan, 2021).

Current approaches, such as **hyperparameter-optimized ML models** (Türkoğlu et al., 2022) and **Software-Defined Networking (SDN)-based architectures** (Al-Mehdhara & Ruan, 2021), prioritize detection accuracy but overlook computational efficiency and decentralization. This **gap highlights** the need for research that **integrates lightweight ML techniques with decentralized trust mechanisms** to balance accuracy, scalability, and resilience in VANETs.

Research Objectives:

The primary goal of this research is to **analyze the existing challenge, and design a decentralized and adaptive framework for DDoS attack detection and mitigation in VANETs**.

To achieve this, the following objectives are proposed:

1. **To Identify** the limitations of the existing centralized and trust-dependent DDoS detection methods in VANETs, focusing on scalability and adaptability (e.g., Türkoğlu et al., 2022; Poongodi et al., 2019).
2. **To design** a hybrid detection model combining **lightweight ML algorithms** (e.g., optimized decision trees) with **distributed trust evaluation** to reduce reliance on centralized controllers.
3. **To implement** a decentralized mitigation mechanism using SDN principles to isolate malicious nodes dynamically, ensuring minimal disruption to legitimate traffic.
4. **To evaluate** the framework's performance against metrics such as detection accuracy, latency, and computational overhead, benchmarking it against state-of-the-art solutions (e.g., MSOM by Al-Mehdhara & Ruan, 2021).

Literature Review: Detect & Defense Against DDoS Attacks in VANETs

Vehicular Ad Hoc Networks (VANETs) are essential for enabling communication among vehicles and between vehicles and infrastructure. These networks are critical for applications such as traffic management, safety alerts, and autonomous driving. However, VANETs are highly vulnerable to Distributed Denial of Service (DDoS) attacks, which can severely disrupt their functionality. Over the years, researchers have proposed various methods to detect and mitigate DDoS attacks in VANETs, employing techniques like machine learning, hybrid algorithms, and trust-based systems. This review examines these approaches, analyzing their strengths, weaknesses, and potential for improving DDoS defense in VANETs.

Recognition of DDoS Attacks on SD-VANETs Based on Combination of Hyperparameter Optimization and Feature Selection

This paper proposes a machine learning-based approach for recognizing DDoS attacks in **Software-Defined VANETs (SD-VANETs)**. The authors combine **hyperparameter optimization** and **feature selection** to enhance the accuracy of their detection models, achieving a high accuracy rate of **99.35%**. Their method focuses on optimizing the parameters of the machine learning models and selecting the most important features from the dataset to improve performance. However, a key limitation of this approach is the reliance on a **centralized controller**, which could become a **single point of failure** in the network (Türkoğlu et al., 2022).

Hybrid Algorithm to Detect DDoS Attacks in VANETs

This paper introduces a **hybrid algorithm** that uses **SVM kernel methods** (AnovaDot and RBFDot) to detect DDoS attacks in VANETs. The hybrid approach combines the outputs of two different models, utilizing a **chaining method**, where the output of one model serves as the input for another. The proposed system shows improved performance over single kernel models, achieving better accuracy in detection. However, the algorithm struggles with **scalability** and its ability to adapt to dynamic network conditions, making it less effective in large-scale VANETs (Adhikary et al., 2020).

DDoS Detection Mechanism Using Trust-Based Evaluation System in VANET

A **trust-based framework** is proposed for detecting DDoS attacks in VANETs. The system evaluates the trustworthiness of nodes and uses a **clustering scheme** to identify and isolate malicious nodes. This method optimizes **bandwidth utilization** and ensures network security. The key advantage of this approach is its ability to prevent attack propagation within the network. However, it requires **a priori knowledge of trust relationships** between nodes, which can be a significant limitation in dynamic environments where trust levels are constantly changing (Poongodi et al., 2019).

Machine Learning Approach of Hybrid KSVM Algorithm to Detect DDoS Attack in VANET

This paper introduces a **hybrid KSVM (Kernel Support Vector Machine)** scheme, combining **KNN (K-Nearest Neighbors)** and **SVM** algorithms to detect DDoS attacks in VANETs. The results indicate that the hybrid KSVM model outperforms other machine learning algorithms in terms of **accuracy, sensitivity, precision, and recall**. The approach provides robust detection performance across different attack scenarios. However, limited information is provided regarding the **dataset** used and the **evaluation metrics**, which could hinder its practical application in real-world systems (**Kadam and Sekhar, 2021**).

Improved Detection and Mitigation of DDoS Attack in Vehicular Ad Hoc Networks

This paper presents a **greedy approach** for detecting and mitigating DDoS attacks in VANETs. The proposed method demonstrates improvements in **network throughput, packet loss, and routing overhead** compared to existing methods. The greedy approach is simple to implement and effectively reduces the impact of DDoS attacks on network performance. However, the **complexity** of the proposed methodology and its ability to handle diverse attack types are not thoroughly discussed, limiting its scalability (**Guleria & Verma, 2018**).

MSOM: Efficient Mechanism for Defense Against DDoS Attacks in VANET

This paper proposes a **Multilayer Distributed SOM (MSOM)** model for detecting and mitigating DDoS attacks in VANETs. The MSOM system achieves an impressive **99.67% accuracy** in detecting DDoS attacks. This approach leverages **SDN (Software-Defined Networking)** to control and manage the network's security efficiently. The MSOM model provides excellent performance for certain types of DDoS attacks, especially **flooding attacks**.

However, the model is specialized for specific attack types, limiting its generalizability to other forms of DDoS attacks (**Al-Mehdhara & Ruan, 2021**).

Implications for Future Research:

The literature review addresses all the limitations identified in the research and indicates the need for further research. The researchers can contribute to the development of more resilient, scalable, and adaptive systems that significantly improve the security of VANETs against DDoS attacks and other emerging threats.

References:

- Adhikary, K., Bhushan, S., Kumar, S., & Dutta, K. (2020). Hybrid Algorithm to Detect DDoS Attacks in VANETs. *Wireless Personal Communications*, 114(4), 3613-3634.
- Al-Mehdhara, M., & Ruan, N. (2021). MSOM: Efficient Mechanism for Defense against DDoS Attacks in VANET. *Wireless Communications and Mobile Computing*, 2021, 8891758.
- Guleria, C., & Verma, H. K. (2018, December). Improved Detection and Mitigation of DDoS Attack in Vehicular ad hoc Network. In 2018 4th International Conference on Computing Communication and Automation (ICCCA) (pp. 1-4). IEEE.
- Kadam, N., & Sekhar, K. R. (2021). Machine Learning Approach of Hybrid KSVN Algorithm to Detect DDoS Attack in VANET. *International Journal of Advanced Computer Science and Applications*, 12(7), 718-722.
- Poongodi, M., Hamdi, M., Sharma, A., Ma, M., & Singh, P. K. (2019, December). DDoS Detection Mechanism Using Trust-Based Evaluation System in VANET. In *IEEE Access* (Vol. 7, pp. 183532-183544).
- 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, 117500.