



Detection and Mitigation of DDoS Attacks in 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. Summary of the Research Papers
- 2. Critical Analysis
- 3. Connections between the papers
- 4. Conflicts Between the Findings
- 5. Synthesis Matrix for Literature Review
- 6. References

1. Summary of the Research Papers

Paper 1:

Machine Learning Approach of Hybrid KSVN

This paper proposes a hybrid machine learning approach based on KNN and SVM to detect DDoS attacks in VANET. The dataset was collected from Kaggle and divided into training and testing sets. The experimental results show that the hybrid KSVN achieved higher accuracy compared to single algorithms like SVM and KNN. However, the study was based only on simulation and did not test the model in real vehicular environments.

Paper 2:

Improved Detection and Mitigation of DDoS Attack using Greedy Approach

This research proposes a greedy-based mechanism to detect and mitigate DDoS attacks in VANET. The system monitors bandwidth usage and isolates malicious nodes when threshold limits are exceeded. Simulation was performed using NS-2. The results show improved throughput and reduced packet loss. However, the method was tested in a limited environment and may not handle large-scale attacks.

Paper 3:

DDoS Detection Mechanism Using Trust-Based Evaluation System in VANET

This paper introduces a trust-based evaluation system to detect DDoS attacks. It calculates trust values using factors like frequency statistics, residual energy, and data factor. The system achieved high detection rate and low energy consumption. The limitation of this work is the complexity of trust calculations and dependency on clustering.

Paper 4:

A Distributed Network Intrusion Detection System for Distributed Denial of Service Attacks in Vehicular Ad Hoc Network

This study proposes a distributed intrusion detection system using Apache Spark and Random Forest. The system was tested on NSL-KDD and UNSW-NB15 datasets. The results showed high accuracy (around 99%). The main advantage is scalability using big data tools. However, it was not tested in a real VANET environment.

Paper 5:**MSOM: Efficient Mechanism for Defense against DDoS Attacks in VANET**

This research integrates SDN architecture with a multilayer distributed SOM (MSOM) to detect DDoS attacks. The results show high detection accuracy (99.67%) and improved throughput. The distributed architecture reduces controller overload. However, the system design is complex and requires advanced SDN infrastructure.

Paper 6:**Hybrid Algorithm to Detect DDoS Attacks in VANETs**

This paper proposes a hybrid SVM-based algorithm combining AnovaDot and RBFDot kernels. The model was evaluated using simulated VANET data. Performance metrics such as accuracy, Gini, and KS showed improvement over single SVM kernels. The limitation is that the dataset was simulation-based and not real-world traffic.

2. Critical Analysis

Most of the selected papers focus on detecting DDoS attacks using machine learning techniques. Hybrid models generally perform better than single algorithms. Trust-based and SDN-based approaches provide better control and network management. However, many studies rely only on simulation or benchmark datasets instead of real VANET environments. Another limitation is the high computational overhead in complex models like MSOM and big data frameworks.

Machine learning approaches such as Random Forest and SVM show high accuracy, but they require proper feature selection. Trust-based systems improve reliability but may increase complexity. SDN-based solutions offer centralized management but can create single-point-of-failure risks if not distributed properly.

3. Connections Between the Papers

- All papers focus on DDoS detection in VANET.
- Most studies use machine learning techniques.
- Simulation-based evaluation is common in all works.
- Improving detection accuracy and reducing false alarms is a shared goal.
- Many approaches aim to reduce network delay and packet loss.

4. Conflicts Between the Findings

- Some papers use centralized SDN control, while others use distributed detection.
- Machine learning models focus on data classification, while trust-based models focus on behavior evaluation.
- Big data approaches emphasize scalability, while hybrid SVM focuses on classification accuracy.
- Some studies prioritize detection accuracy, while others focus on network performance metrics.

5. Synthesis Matrix for Literature Review

Study	Authors	Year	Methodology	Key Findings/Results	Limitations
Machine Learning Approach of Hybrid KSVN	Ms.Nivedita Kadam, Dr. Krovi Raja Sekhar	2021	KNN and SVM	Higher accuracy than single ML models	Simulation-based only
Improved Detection and Mitigation of DDoS	Charu Guleria, Harsh Kumar Verma	2018	Bandwidth Threshold Monitoring	Improved throughput and reduced packet loss	Limited network size
DDoS Detection Mechanism Using Trust-Based Evaluation System in VANET	M. POONGODI , MOUNIR HAMDI , ASHUTOSH SHARMA 2, AND PRADEEP KUMAR SINGH	2019	Trust Evaluation and Clustering	High detection rate and low energy consumption	Complex trust computation
A Distributed Network Intrusion Detection System for Distributed Denial of Service Attacks in Vehicular Ad Hoc Network	YING GAO , HONGRUI WU , BINJIE SONG, YAQIA JIN, XIONGWEN LUO, AND XING ZENG	2019	Spark and Random Forest	High accuracy ($\approx 99\%$)	Not tested in real VANET
MSOM: Efficient Mechanism for Defense against DDoS Attacks in VANET	Mohammed Al-Mehdhara and Na Ruan	2021	SDN and Multilayer SOM	99.67% detection accuracy	Complex architecture
Hybrid Algorithm to Detect DDoS Attacks in VANETs	Kaushik Adhikary ¹ · Shashi Bhushan ² · Sunil Kumar ³ · Kamlesh Dutta	2020	AnovaDot and RBFDot	Better than single SVM kernels	Simulation dataset

6. 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)