

Course Title: Research Methodology in Computer Science

Course Code: AI800

Weighting: 20%

Lecturer: Dr. Mohammed Anbar

Hand-out Date: 28 June 2025

Hand-in Date: 12 July 2025

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

Assignment Report: literature Review Detect & Defense against DDoS Attacks in VANETs

Student ID: 251001992

Student Name: Meshal Alkhaldi

Table of contents:

- Summary research paper's
- Critical Analysis:
- Connections
- Conflicts between the findings
- Synthesis Matrix for Literature Review:
- References

Summary research paper's:

Paper1: Recognition of DDoS attacks on SD-VANET based on combination of hyperparameter optimization and feature selection

This paper focusing on recognizing DDoS attacks in Software-Defined Vehicular Ad Hoc Networks (SD-VANETs). The authors use machine learning to classify network traffic as either normal or a DDoS attack. They improve the accuracy of the machine learning models by selecting the most important features from a dataset and optimizing the models' parameters. Their approach achieves a high accuracy of 99.35% in detecting DDoS attacks. The authors emphasize the importance of feature selection and parameter optimization for improving the performance of machine learning models in detecting DDoS attacks in SD-VANETs. (Türkoğlu et al., 2022)

Paper2: Hybrid Algorithm to Detect DDoS Attacks in VANETs

Here we note that the authors propose a hybrid algorithm based on the SVM kernel methods of AnovaDot and RBFDot for detecting DDoS attacks in VANETs. The proposed hybrid algorithm is based on combining the two SVM kernels: AnovaDot and RBFDot. The algorithm developed is inspired from Chaining method. In this method output of the first model is given as an input to the second model. (Adhikary et al., 2020)

Paper3: DDoS Detection Mechanism Using Trust-Based Evaluation System in VANET

This paper proposes a trust-based framework for detecting DDoS attacks in VANETs. The framework uses a trust evaluation mechanism to identify malicious nodes and a clustering scheme for better intrusion prevention. The proposed system optimizes bandwidth utilization without compromising the security of the nodes in the network. (Poongodi et al., 2019)

Paper4: Machine Learning Approach of Hybrid KSVM Algorithm to Detect DDoS Attack in VANET

This paper proposes a hybrid KSVM scheme based on KNN and SVM algorithms to detect DDoS attacks in VANET. The proposed algorithm provides better results compared to other machine learning algorithms in terms of accuracy, sensitivity, precision, recall, and error percentage. (Kadam and Sekhar., 2021)

Paper5: Improved Detection and Mitigation of DDoS Attack in Vehicular ad hoc Network

This paper proposes a new mechanism for detecting and mitigating DDoS attacks in VANETs using a greedy approach. The proposed method is better than the existing method in terms of network throughput, network packet loss, and routing overhead. (Guleria & Verma., 2018)

Paper6: MSOM: Efficient Mechanism for Defense against DDoS Attacks in VANET

This paper proposes a secure VANET architecture using SDN and a Multilayer Distributed SOM (MSOM) model. The proposed MSOM system can effectively detect and mitigate DDoS attacks in VANETs, achieving a high accuracy rate (99.67%). (Al-Mehdhara & Ruan., 2021)

Critical Analysis:

The reviewed papers offer diverse approaches to DDoS attack detection and mitigation in VANETs, with varying strengths and weaknesses. Some studies propose hybrid algorithms combining different machine learning models or kernel functions for improved accuracy and efficiency. Others focus on hyperparameter optimization and feature selection to enhance detection accuracy and reduce computational overhead. Some studies leverage trust-based evaluation systems to isolate malicious nodes and maintain network connectivity. However, these approaches have limitations, such as scalability issues, reliance on centralized controllers, and the need for a priori knowledge of trust relationships.

Despite these limitations, the papers collectively contribute to the growing body of knowledge on DDoS attack detection and mitigation in VANETs. They highlight the potential of machine learning and other innovative techniques in detecting and mitigating DDoS attacks in VANETs, while also acknowledging the challenges and limitations that need to be addressed in future research.

Connections:

- 1- **Effectiveness of Machine Learning:** All the papers concur that machine learning techniques are highly effective in detecting and mitigating DDoS attacks in VANETs. They demonstrate the potential of machine learning to address the dynamic and complex nature of security threats in vehicular networks.
- 2- **Importance of Performance Metrics:** The papers consistently emphasize the importance of evaluating the performance of proposed methods using metrics such as accuracy, detection rate, throughput, packet loss, and delay. This shared focus on performance evaluation highlights the need for robust and reliable solutions to ensure the security and stability of VANETs.
- 3- **Simulation-Based Validation:** All the papers utilize simulation-based approaches to validate their proposed methods, employing tools like NS-2 and Mininet-WiFi to create controlled environments for experimentation. This shared research design allows for a systematic and rigorous evaluation of the effectiveness of different techniques in detecting and mitigating DDoS attacks.

Conflicts between the findings:

- 1- Methodology:** The papers present conflicting perspectives on the most effective methodology for detecting and mitigating DDoS attacks in VANETs. While some advocate for hybrid algorithms based on SVM kernels, others propose combining hyperparameter optimization with feature selection or utilizing trust-based evaluation systems.
- 2- Network Model:** The papers also disagree on the most suitable network model for implementing DDoS defense mechanisms. Some focus on traditional VANET models, while others advocate for Software-Defined VANETs (SD-VANETs) that leverage the centralized control and programmability of SDN.
- 3- Attack Types:** The papers further diverge in their focus on specific types of DDoS attacks. Some primarily address protocol-based attacks like UDP, TCP, and ICMP flooding, while others consider a broader range of attacks, including vehicle-to-vehicle and vehicle-to-infrastructure scenarios.

Synthesis Matrix for Literature Review:

Paper Name	Authors	Year	Research Design	Key Findings/Results	Methodology	Limitations
Recognition of DDoS attacks on SD-VANET based on combination of hyperparameter optimization and feature selection	Türkoğlu et al.	2022	Simulation-based	The proposed model can effectively detect DDoS attacks in SD-VANET with high accuracy.	Combination of hyperparameter optimization and feature selection	Relies on a centralized controller, which can be a single point of failure.
Hybrid Algorithm to Detect DDoS Attacks in VANETs	Adhikary et al.	2020	Simulation-based	The hybrid model outperforms single kernel models in terms of Accuracy, Gini, KS, MER, and H.	Hybrid algorithm based on SVM kernels (AnovaDot and RBFDot)	Limited scalability and adaptability to dynamic network conditions.
DDoS Detection Mechanism Using Trust-Based Evaluation	Poongodi et al.	2019	Simulation-based	The trust-based system can effectively isolate malicious nodes and	Trust-based evaluation system	Requires a priori knowledge of trust relationships between nodes.

System in VANET				maintain network connectivity.		
Machine Learning Approach of Hybrid KSVN Algorithm to Detect DDoS Attack in VANET	Kadam and Sekhar	2021	Simulation-based	The hybrid KSVM algorithm provides better results compared to other machine learning algorithms in terms of accuracy, sensitivity, precision, recall, and error percentage.	Hybrid KSVM scheme based on KNN and SVM algorithms	Limited information on dataset and evaluation metrics.
Improved Detection and Mitigation of DDoS Attack in Vehicular ad hoc Network	Guleria and Verma	2018	Simulation-based	The proposed method is better than the existing method in terms of network throughput, network packet loss, and routing overhead.	Greedy approach for detecting and mitigating DDoS attacks	Limited details on the proposed methodology and its complexity.
MSOM: Efficient Mechanism for Defense against DDoS Attacks in VANET	Al-Mehdhar a and Ruan	2021	Simulation-based	The proposed MSOM system can effectively detect and mitigate DDoS attacks in VANETs, achieving a high accuracy rate (99.67%).	Multilayer Distributed SOM (MSOM) model based on two levels of clustering and classification	The study focuses on a specific type of DDoS attack (flooding attack) and may not be generalizable to other types of DDoS attacks.

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.