

- **Course Title:** Research Methodology in Computer Science
- **Course Code:** AI800
- **Lecturer:** Dr. Mohammed Anbar
- **Student Name:** Ghurmallah Salem Mohammed Alqarni
- **Student ID:** [253000384](#)

Assignment Report: Detection and Mitigation of DDoS Attacks in Vehicular Ad Hoc Networks (VANETs).

1. Summary of Research Papers

Paper 1: *Hybrid Algorithm to Detect DDoS Attacks in VANETs* - Adhikary et al. (2020) (1) presents a hybrid detection model combining SVM kernels (AnovaDot and RBFDot) to identify DDoS attacks. The model uses features such as packet loss, jitter, and collision rates for both training and testing. Results show higher accuracy and reliability compared to single-kernel methods. However, the approach depends on simulated datasets and lacks evaluation in real vehicular scenarios.

Paper 2: *Stream Position Performance Analysis Model (SPPA)* - Kolandaisamy et al. (2020) (2) introduce a Stream Position Performance Analysis (SPPA) model for cluster-based routing environments. The system evaluates conflict data, attack signature rates, and trustworthiness of packets to detect malicious activities. This model enhances VANET performance by reducing false positives and improving decision-making at cluster heads. The limitation lies in the model's complexity and computational overhead under high mobility.

Paper 3: *Improved Detection and Mitigation of DDoS Attacks in VANET* - Guleria and Verma (2018) (3) propose a two-stage mechanism: (1) simulating DDoS attacks and network congestion, and (2) detecting and mitigating them using a greedy approach in NS-2 simulations. The proposed method outperforms existing algorithms in packet loss reduction, routing overhead, and throughput improvement. However, it focuses on a specific attack scenario and does not generalize to other forms of DDoS attacks.

Paper 4: *MSOM - Efficient Mechanism for Defense against DDoS Attacks in VANET* - Al-Mehdhara and Ruan (2021) (4) develop a Multilayer Self-Organizing Map (MSOM) within an SDN-based VANET architecture. This hybrid model uses clustering and classification layers for accurate attack detection. It achieves 99.67% accuracy and demonstrates resilience under dynamic traffic conditions. However, the SDN central controller introduces a potential single point of failure, which may limit scalability.

Paper 5: *Distributed Network Intrusion Detection System for DDoS Attacks in VANET* - Gao et al. (2019) (5) propose a distributed Network Intrusion Detection System (NIDS) using Apache Spark for real-time data processing and Random Forest classification. The system efficiently handles large-scale traffic and achieves 99.95% accuracy with minimal false alarms. The study emphasizes scalability and big data integration but lacks testing on live vehicular networks.

Paper 6: *DDoS Detection Mechanism Using Trust-Based Evaluation System in VANET* - Poongodi et al. (2019) (6) design a trust-based framework that evaluates node behavior using multiple parameters, including residual energy, trust policy, and frequency statistics. By forming a trust evaluation matrix, the system detects attackers while maintaining low bandwidth consumption. This hybrid trust-clustering approach achieves high packet delivery and energy efficiency, though it requires additional calibration for large-scale deployments.

2. Critical Analysis

The six selected studies (1–6) collectively demonstrate the growing emphasis on integrating machine learning and software-defined networking (SDN) to improve DDoS detection in VANETs. Hybrid models combining algorithms such as SVM, SOM, and Random Forest enhance detection adaptability and accuracy. However, a common limitation across all studies is the dependence on simulation environments rather than real vehicular implementations, which limits external validity. Trust-based and distributed systems (5, 6) offer scalability but also increase computational complexity, which may not be feasible in resource-constrained vehicles.

3. Connections

1. **Shared Objective:** All studies aim to detect and mitigate DDoS attacks in VANETs (1–6).
2. **Core Technologies:** Machine learning and SDN architectures are commonly used (1, 4, 5).
3. **Evaluation Metrics:** Accuracy, packet delivery ratio (PDR), latency, and false alarm rate are standard metrics.
4. **Testing Environments:** Most studies use simulation platforms such as NS-2, NS-3, or Apache Spark (3, 5).
5. **System Scalability:** Distributed and cluster-based designs improve performance under dynamic traffic conditions (2, 5).

4. Conflicts Between the Findings

1. **Centralized vs. Distributed Detection:** Centralized SDN systems like MSOM (4) offer high precision but risk single-point failures, whereas distributed approaches like NIDS (5) improve resilience but add complexity.
2. **Heuristic vs. Learning-Based Models:** Traditional rule-based models are simpler but less adaptive than ML-driven systems requiring extensive training data (1, 4, 5).
3. **Simulation vs. Real Implementation:** Simulated setups (1–3, 5) show ideal results not always reproducible in real-world VANETs.
4. **Performance Trade-offs:** High accuracy often comes with increased latency or computational costs (2, 4).

5. **Energy and Resource Constraints:** Trust-based frameworks (6) provide reliability but may overload vehicle nodes with extra processing.

5. Synthesis Matrix for Literature Review

Study	Authors	Year	Approach	Algorithm/Technique	Accuracy (%)	Strengths	Limitations
Hybrid Algorithm	Adhikary et al. (1)	2020	ML Hybrid	SVM (AnovaDot + RBFDot)	96.5	Improved accuracy	Simulation only
SPPA Model	Kolandaisamy et al. (2)	2020	Cluster-based	Stream Position Analysis	95.8	High trust accuracy	High computational cost
Improved Detection & Mitigation	Guleria & Verma (3)	2018	Greedy approach	Two-stage detection	93.4	Reduced overhead	Limited to specific attacks
MSOM	Al-Mehdhara & Ruan (4)	2021	SDN + Neural Network	Multilayer SOM	99.67	High precision	Central controller risk
Distributed NIDS	Gao et al. (5)	2019	Big Data + ML	Random Forest + Spark	99.95	Scalable, real-time	No live testing
Trust-Based Detection	Poongodi et al. (6)	2019	Trust & Cluster	Trust Matrix Evaluation	97.2	Energy-efficient	Complex parameter tuning

6. References

1. Adhikary, K., Bhushan, S., Kumar, S., & Dutta, K. (2020). *Hybrid Algorithm to Detect DDoS Attacks in VANETs*. Wireless Personal Communications.
2. Kolandaisamy, R., Noor, R., Ahmedy, I., & Kiah, M. (2020). *Stream Position Performance Analysis Model for Cluster-based Routing in VANET*. Journal of Ambient Intelligence and Humanized Computing.
3. Guleria, C., & Verma, H. (2018). *Improved Detection and Mitigation of DDoS Attack in Vehicular Ad Hoc Network*. IEEE ICCCA.
4. Al-Mehdhara, M., & Ruan, N. (2021). *MSOM: Efficient Mechanism for Defense against DDoS Attacks in VANET*. Wireless Communications and Mobile Computing.
5. Gao, Y., Wu, H., Song, B., et al. (2019). *A Distributed Network Intrusion Detection System for DDoS Attacks in VANET*. IEEE Access.
6. Poongodi, M., Hamdi, M., Sharma, A., Ma, M., & Singh, P. K. (2019). *DDoS Detection Mechanism Using Trust-Based Evaluation System in VANET*. IEEE Access.