

Research Title: Enhancing Trust and Security in Vehicular Ad-Hoc Networks Against DDoS Attacks

Student Name: Megern Qaisse

Student ID: 253001866

Course: Research Methodology in Computer Science (AI800)

Date: 19/12/2025

Research Title

A Hybrid Trust-and-Learning Framework for Real-Time DDoS Detection in Vehicular Ad-Hoc Networks (VANETs)

Abstract

Vehicular Ad-Hoc Networks (VANETs) enable vehicles and roadside units to exchange safety and traffic information such as accident warnings and congestion alerts. Because the network is decentralized and vehicles join and leave frequently, VANETs are vulnerable to distributed denial-of-service (DDoS) attacks. Attackers can flood the channel with spurious packets, crowding out legitimate safety messages and causing delays or packet loss. Existing countermeasures typically rely on either trust-based heuristics that are simple and fast but can be evaded, or machine-learning models that are accurate but computationally expensive for on-board units. This research proposes a hybrid framework that combines a lightweight trust-based edge filter with a small machine-learning module. The aim is to detect DDoS attacks quickly and accurately by using the trust filter as a first line of defence and forwarding suspicious flows to the learning module for deeper analysis. Simulations will compare the hybrid method with existing trust-only, threshold-only and deep-learning methods. The proposed approach is expected to lower false positives, reduce detection delay and maintain high packet delivery ratio under a variety of traffic conditions.

1 Introduction

Vehicular Ad-Hoc Networks (VANETs) form the communication layer of intelligent transportation systems. Vehicles and roadside units exchange short safety messages via vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. These messages warn drivers about collisions, roadworks, congestions and other hazards. Because VANETs are open networks and each vehicle acts as a node, malicious nodes can inject fake messages into the channel. Among the most serious threats are distributed

denial-of-service (DDoS) attacks, where attackers flood the network with unnecessary or malicious packets, preventing legitimate safety messages from being delivered on time. Such attacks may lead to missed warnings, increased accident risk and degraded public trust in VANET services. It is therefore crucial to design an intrusion-detection system that can detect and mitigate DDoS attacks while meeting VANET constraints such as limited on-board computation and real-time requirements.

2 Background

2.1 Trust-based approaches

Trust-based intrusion-detection systems assign a trust score to each vehicle based on behavioural metrics such as packet rate, inter-arrival time and message content consistency. Nodes with high trust are permitted to forward messages, whereas nodes with low trust may be ignored or blocked. Such systems are attractive because they require little computing power and can be executed on on-board units. However, thresholds are often static; an attacker sending malicious packets at a low rate may evade detection. Cluster-based trust schemes involve assigning a cluster head to monitor trust values within its group; while effective in reducing overhead, these schemes create single points of failure and may be vulnerable to collusion. Fuzzy logic can help adapt trust thresholds to changing conditions but still relies on careful tuning and may misclassify legitimate bursts of traffic.

2.2 Machine-learning approaches

Machine-learning models for VANET security use features extracted from network traffic (packet size, inter-arrival times, message entropy, etc.) to classify flows as benign or malicious. Supervised algorithms such as Random Forest, Support Vector Machines and k-Nearest Neighbors have been applied to intrusion detection. More recent work uses deep learning—e.g., stacked autoencoders—to learn latent representations of network flows and detect anomalies. These models achieve high detection accuracy in simulation but require substantial training data, computational resources and time to adapt to new attack strategies. Running such models directly on resource-constrained on-board units may not be feasible for real-time processing. Moreover, deep models may act as black boxes, making it difficult to interpret decisions.

2.3 Hybrid and adaptive approaches

Hybrid frameworks attempt to combine the speed of heuristic or trust-based methods with the accuracy of machine-learning models. A typical hybrid architecture employs a simple filter to quickly flag suspicious flows and forwards them to a learning module for deeper analysis. Some research uses feedback loops to tune thresholds based on the learning module's output. The challenge is to design a lightweight learning module that can operate on the edge or a nearby server while ensuring timely updates to the trust filter. There is limited work on real-time adaptation of thresholds to dynamic traffic conditions in VANETs.

3 Problem Statement

Domain: Real-time detection and mitigation of DDoS attacks in VANETs.

Problem: Existing detection schemes either rely on simple trust-based metrics that are fast but may be fooled by low-rate or coordinated attacks, or on machine-learning models that offer high accuracy but are computationally expensive for on-board units. There is currently no widely adopted solution that combines the advantages of both methods while meeting VANET constraints such as limited computing resources and real-time requirements.

Significance: Safety messages in VANETs must be delivered promptly to prevent accidents and maintain traffic flow. If DDoS attacks delay or drop these messages, the consequences can be fatal. Thus a solution that reduces false positives and ensures rapid detection can significantly enhance road safety and public trust.

Gap: Trust-based methods use fixed thresholds and cannot adapt to stealthy or colluding attackers; learning methods are effective but too slow for real-time detection on the edge. Hybrid methods exist but often lack adaptive feedback mechanisms and may not be tuned for dynamic traffic conditions.

Need: A balanced hybrid framework is needed where a lightweight trust-based filter quickly labels most traffic, and a small learning module handles only ambiguous cases. Continuous feedback should adjust thresholds based on current traffic patterns to maintain detection performance without overwhelming edge devices.

4 Research Objectives

1. **Design a trust-based edge filter:** Develop simple rules using metrics such as packet rate, inter-arrival time and duplicate ratio to label flows as normal, suspicious or malicious with minimal processing overhead.
2. **Develop a compact learning module:** Implement a Random Forest classifier and an autoencoder to detect anomalies among flows marked suspicious. Train and evaluate these models on realistic VANET traffic data.
3. **Integrate the trust filter and learning module:** Create a pipeline where suspicious flows are forwarded to the learning module for confirmation, and design a feedback mechanism to update trust thresholds based on learning outcomes.
4. **Evaluate against baselines:** Compare the hybrid system with a pure trust-based system, a simple threshold method and a pure learning-based system on metrics such as accuracy, false positive rate, detection delay, packet delivery ratio and resource usage.
5. **Test robustness under varying conditions:** Assess the hybrid system under diverse traffic densities (urban, suburban, highway), attack intensities (burst, trickle, on-off, collusion) and mobility patterns. Evaluate the effect of dynamic threshold adjustment on performance.

5 Research Scope

This study will evaluate intrusion-detection strategies using simulated VANET traffic. Real-world deployment and data collection are beyond the scope of this project, but we will employ mobility and propagation models representative of actual road networks. The research focuses on DDoS attacks; other attack types (e.g., Sybil, spoofing) or privacy-preserving mechanisms will not be addressed. Only anonymized network features will be used; no personal or vehicle identifiers will be collected.

6 Literature Review

(Extension from Assignment 1)

6.1 Leader-based trust systems

Kolandaisamy et al. proposed a leader-based intrusion-detection system for DDoS attacks in VANETs. Vehicles are grouped into clusters, and a cluster head monitors message rate and conflict signals within its cluster. Simulation results showed improved packet delivery ratio, but the method depends heavily on the accuracy and availability of the cluster head.

6.2 Fuzzy logic for trust evaluation

Guleria and Verma introduced a trust-based evaluation mechanism using fuzzy logic, where nodes are assigned trust scores based on their packet rate, timing and residual energy. The fuzzy controller adapts trust levels dynamically; however, the system requires careful parameter tuning and may misclassify legitimate bursts during high traffic.

6.3 Stacked autoencoders for DDoS detection

Polat et al. applied stacked sparse autoencoders (SSAE) to detect DDoS attacks in VANETs. The deep network learned latent features from network flows and achieved high detection accuracy in simulations. Nevertheless, SSAE models require substantial training data and computing power, making them challenging to deploy on edge devices.

6.4 Random Forest-based intrusion detection

Random Forest classifiers have been used widely in intrusion-detection tasks. Research shows that Random Forest can handle high-dimensional traffic features and provide robust performance with relatively low training cost. It is also interpretable and easier to implement on resource-constrained devices compared with deep models.

6.5 Blockchain-based trust management

Recent studies explore using blockchain to decentralize trust management in VANETs. Instead of relying on a central cluster head, trust scores and suspicious events are recorded on a distributed ledger. Vehicles reference the ledger to update their local trust scores. Blockchain improves resilience against single points of failure but introduces latency and storage overhead, and consensus mechanisms may be too heavy for real-time VANET applications.

6.6 Cooperative detection and voting schemes

Cooperative schemes rely on vehicles sharing observations about suspicious behavior and voting on trust scores. Such schemes can reduce misclassification but suffer from overhead and may be vulnerable to false reports if multiple compromised nodes collude.

6.7 Summary of literature

The literature reveals that trust-based methods are fast but can be bypassed by low-rate or coordinated attacks; machine-learning methods achieve high accuracy but may not be practical on on-board devices. Hybrid approaches show promise but need adaptive feedback to remain robust under dynamic traffic conditions. Research also highlights that decentralizing trust (e.g., via blockchain) may help but introduces additional overhead.

7 Research Methodology

This section outlines the proposed hybrid system design, algorithms and evaluation plan.

7.1 System design

1. **Edge trust filter:** Implemented on on-board units or roadside units, the trust filter continually monitors messages from each sender. For a fixed time window (e.g., one second), it computes metrics such as packet rate, inter-arrival time and duplicate ratio. Based on predetermined thresholds, it assigns a trust score and labels flows as normal, suspicious or malicious. To reduce false positives, the thresholds will be adapted based on traffic patterns.
2. **Learning module:** Running on an edge server (or more powerful road side unit), the learning module receives summary statistics of suspicious flows. It uses a Random Forest classifier trained on labeled data (normal and attack traffic) and an autoencoder to detect anomalies. The Random Forest outputs a probability that the flow is an attack; the autoencoder reconstruction error identifies unusual patterns. If both indicate an attack, the flow is flagged; otherwise the flow is re-evaluated by the trust filter.
3. **Feedback mechanism:** The learning module analyses the trust filter's performance over time. If the trust filter generates frequent false positives or misses attacks, the learning module suggests adjusting thresholds (e.g., increasing the acceptable packet rate during rush hours). These updates are sent back periodically.

7.2 Algorithm

1. **Data collection:** Simulate VANET traffic using an open-source network simulator (e.g., Veins or NS-3) with realistic mobility and propagation models.
2. **Feature extraction:** For each sender, record packet rate, inter-arrival time, duplicate ratio and other features (e.g., entropy of message content). Compute summary statistics for each time window.
3. **Trust filtering:** Assign trust scores based on thresholds. Label flows as safe (forward), suspicious (send to learning module) or malicious (drop).

4. **Learning stage:** Train a Random Forest classifier and autoencoder on a dataset of labeled normal and attack flows. For incoming suspicious flows, compute the probability of attack and reconstruction error. If both exceed predetermined thresholds, mark as malicious; if not, treat as normal or suspicious and adjust trust accordingly.
5. **Threshold update:** Periodically evaluate detection metrics (e.g., false positive rate). If performance degrades, update trust thresholds using feedback from the learning module.

7.3 Evaluation plan

1. **Scenarios:** Evaluate the system under different traffic conditions (urban, suburban, highway) and varying attack patterns (burst, slow trickle, on-off, colluding). Vary vehicle density to model rush hour and off-peak traffic.
2. **Baselines:** Compare the hybrid method with (i) trust-only detection, (ii) threshold-only detection using fixed limits, and (iii) learning-only detection where all traffic is processed by the Random Forest module.
3. **Metrics:** Measure precision, recall, F1 score, false positive rate, detection delay (time from attack start to detection), packet delivery ratio, CPU usage and memory consumption on the edge device, and communication overhead.
4. **Outcome analysis:** Analyze how the feedback mechanism adjusts thresholds under varying traffic. Evaluate trade-offs between detection accuracy and computational cost. Determine the conditions where the hybrid system outperforms baselines and where it may require further improvement.

8 Expected Outcomes

- **Improved detection speed:** The trust filter will allow rapid initial detection by labelling obvious malicious traffic, thereby reducing detection delay compared with pure learning methods.
- **Increased accuracy:** The learning module will reduce false positives by analyzing suspicious flows more carefully, improving precision and recall compared with pure trust-based systems.
- **Adaptability:** The feedback mechanism will adjust thresholds to match traffic patterns (e.g., raising packet rate thresholds during rush hours), ensuring stable performance under dynamic conditions.
- **Resource efficiency:** By forwarding only suspicious flows to the learning module, the hybrid system will use less CPU and memory on the edge and back-end than a learning-only system.
- **Practical deployment:** The simple architecture and lightweight components will make the system suitable for implementation on real VANET on-board units and roadside infrastructure.

9 Gantt Chart

The table below presents the proposed timeline (three months) for the research project. Each task spans an approximate duration in weeks.

Task	Month 1	Month 2	Month 3
Literature review & gap analysis	✓		
Define trust metrics & design edge filter	✓	✓	
Collect training data & feature extraction		✓	
Develop & train learning module		✓	
Integrate trust filter & learning module		✓	✓
Implement feedback mechanism			✓
Simulate scenarios (urban, suburban, highway)			✓
Evaluate metrics & adjust thresholds			✓
Prepare final report & presentation			✓

10 References

1. Kolandaisamy, et al., "A Distributed Network Intrusion Detection System for Distributed Denial-of-Service Attacks in Vehicular Ad Hoc Network," 2020.
2. Guleria, S., and Verma, P., "DDoS Detection Mechanism Using Trust-Based Evaluation System in VANET," 2018.
3. Polat, H., Dogan, M., et al., "Deep Network Approach with Stacked Sparse Autoencoders in Detection of DDoS Attacks on VANETs," *IET Communications*, 2021.
4. Research articles on Random Forest and blockchain trust management (see search results from trusted sources, e.g., MDPI and IEEE).
5. Additional studies on cooperative voting schemes and fuzzy logic for trust updates in VANET intrusion detection (various sources).

Note: This research proposal is a guidance document and should be customized with specific simulation data, detailed methodology steps and real citation information.