Journal of Information Systems Engineering and Management
2025, 10(42s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A Framework for Malicious Node Detection in VANETs using Machine Learning Approaches

Nazish Siddiqui[1], Dr. Sheeba Praveen[2]
[1]*nazishcs016@gmail.com, Integral University, Department of Computer Science & Engineering, Lucknow, India*
[2]*sheeba@iul.ac.in, Integral University, Department of Computer Science & Engineering, Lucknow, India*

ARTICLE INFO

Received: 30 Dec 2024

Revised: 19 Feb 2025

Accepted: 27 Feb 2025

ABSTRACT

Vehicular Ad-hoc Networks (VANETs) are crucial for enhancing road safety, enabling autonomous driving, and supporting efficient traffic management. However, the open and highly dynamic nature of VANETs makes them vulnerable to various cyber threats posed by malicious nodes, including Sybil attacks, spoofing, and denial-of-service (DoS) attacks. This paper presents a novel hybrid detection framework that combines machine learning with a trust-based model to enhance malicious node detection in VANETs. The proposed system leverages machine learning for real-time anomaly detection by analyzing communication patterns, while the trust-based model evaluates each node's behavior and reputation to strengthen the accuracy of malicious activity detection. By integrating these approaches, the framework provides robust, adaptive, and precise detection capabilities, effectively minimizing false positives and improving resilience against emerging threats.

Our framework consists of a multi-layered architecture with data collection, feature extraction, machine learning-based anomaly detection, and a trust evaluation system that assigns trust scores based on historical and real-time interactions. The decision fusion module combines outputs from both machine learning and trust-based models to make informed decisions on potential threats. The proposed hybrid detection system significantly improves VANET security, offering an efficient and reliable solution for detecting and mitigating malicious nodes in complex vehicular networks.

Keywords: VANET, malicious node, machine learning, attacks.

INTRODUCTION

1.1 Background:

Vehicular Ad hoc Networks (VANETs) represent a pioneering advancement in the field of wireless communication, specifically tailored to support the unique needs of transportation systems. As part of the broader category of Mobile Ad hoc Networks (MANETs), VANETs enable vehicles to communicate with one another (Vehicle-to-Vehicle, or V2V) and with roadside infrastructure (Vehicle-to-Infrastructure, or V2I). This capability is essential for enhancing road safety, improving traffic efficiency, and fostering the development of intelligent transportation systems (ITS).

1.1.1.Overview of VANET Architecture

At the core of VANETs is a decentralized communication model that allows vehicles to act as mobile nodes within a network. Each vehicle is equipped with onboard units (OBUs) that facilitate communication through dedicated short-range communications (DSRC)[22][5] or cellular networks. These vehicles can exchange critical information such as location, speed, direction, and braking status in real-time. In addition, infrastructure components like traffic signals, road signs, and information kiosks are equipped with roadside units (RSUs) that communicate with vehicles to relay essential data regarding traffic conditions, accidents, and other hazards.

Journal of Information Systems Engineering and Management
2025, 10(42s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

1.1.2.Role in Modern Transportation Systems

- **Enhancing Road Safety**: One of the most significant benefits of VANETs is their potential to improve road safety. By enabling V2V communication, vehicles can share information about their environment, alerting drivers to imminent dangers such as collisions, road obstructions, or adverse weather conditions. This type of proactive communication can save lives by reducing the likelihood of accidents significantly.
- **Traffic Management and Efficiency**: VANETs also play a vital role in optimizing traffic flow. Through V2I communication, vehicles can receive real-time updates from traffic management systems, such as changes in signal patterns or congestion alerts. This information can guide drivers to alternative routes, helping to alleviate traffic jams and reduce travel time. Moreover, coordinated traffic signals can adapt to real-time conditions, further enhancing the overall efficiency of the transportation network.
- **Supporting Intelligent Transportation Systems (ITS)**: The integration of VANETs into ITS is a critical step toward achieving smart cities and sustainable transportation solutions. VANETs enable various applications, including automated toll collection, vehicle navigation systems, and parking management solutions. These applications rely on the continuous exchange of data between vehicles and infrastructure, fostering a more interconnected and efficient transportation ecosystem.
- **Facilitating Autonomous Vehicles**: As the development of autonomous vehicles accelerates, VANETs are essential for providing the communication backbone that supports vehicle autonomy. Autonomous vehicles require real-time data from their surroundings to make informed decisions. Through V2V and V2I communication, these vehicles can access a wealth of information that enhances their situational awareness and operational safety.

VANETs are transforming modern transportation systems by enabling seamless communication between vehicles and infrastructure. Their ability to enhance road safety, improve traffic management, support intelligent transportation applications, and facilitate the advancement of autonomous vehicles positions them as a cornerstone of future mobility solutions. As technology continues to evolve, the importance of VANETs will only increase, paving the way for smarter, safer, and more efficient transportation networks.

1.2 Security Challenges:

Vehicular Ad-hoc Networks (VANETs) are crucial for enabling vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, enhancing road safety, and improving traffic management. However, they are vulnerable to various threats, particularly from malicious nodes. Here are some of the key vulnerabilities and the threats posed by malicious nodes in VANETs:

1.2.1 Vulnerabilities & Threats:

- **Malicious Nodes:** Malicious nodes in VANETs can be vehicles or infrastructure units that have been compromised or intentionally misconfigured to disrupt normal operations. These nodes pose significant threats:
  - **Message Fabrication:** Malicious nodes may inject false messages into the network, which can mislead other vehicles. For instance, a compromised vehicle could falsely claim that there is an accident or road hazard ahead, causing unnecessary rerouting or panic among nearby drivers.
  - **Message Modification:** In some cases, an attacker might intercept and alter legitimate messages sent between vehicles. This can disrupt navigation systems, emergency alerts, or traffic coordination, potentially leading to accidents.
  - **Denial of Service (DoS) Attacks:** Malicious nodes can launch DoS attacks by flooding the network with excessive or malformed data. This can overwhelm the network, preventing important safety messages, like collision warnings, from reaching their intended recipients in time.
  - **Sybil Attacks:** In a Sybil attack, a malicious node creates multiple fake identities to manipulate network traffic or overwhelm network resources. By masquerading as several vehicles, an attacker could cause traffic jams, skew traffic data, or mislead traffic management systems.

Journal of Information Systems Engineering and Management
2025, 10(42s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- **Wormhole Attacks:** This involves two malicious nodes creating a tunnel between themselves to relay messages over an out-of-band connection. They can manipulate the time taken for messages to travel between nodes, leading to inaccurate positioning or timing data.
- **Blackhole and Grayhole Attacks:** In a blackhole attack, a malicious node drops all packets it receives, effectively cutting off communication to and from nearby vehicles. A grayhole attack is a subtler version where the node selectively drops packets, making it harder to detect.
- **Replay Attacks:** In replay attacks, a malicious node captures valid messages and replays them at a later time. This can cause vehicles to react to outdated or irrelevant information, such as responding to old traffic alerts that no longer apply.

- **Vulnerability to Privacy Breaches:** Malicious nodes can track vehicles' movement by intercepting and analyzing communication data. This exposes drivers to privacy risks, such as revealing their locations, routes, or personal information.
- **Routing Protocol Vulnerabilities:** VANETs typically rely on dynamic routing protocols, which are susceptible to attacks by malicious nodes. For example, a compromised node might advertise an incorrect routing path, disrupting message delivery across the network.

- **Eavesdropping:** Unauthorized nodes may intercept communications between vehicles, gaining access to sensitive data. This can be exploited to gather information on traffic patterns, vehicle identities, or even personal data linked to vehicle registration systems.

- **Position Falsification:** Malicious nodes may send false GPS information or vehicle positioning data, misleading nearby vehicles and causing them to make incorrect driving decisions. This can endanger safety by leading to collisions or congestion.

- **Flooding Attacks:** By broadcasting an excessive number of messages, a malicious node can cause a flooding attack that clogs the network. This can result in legitimate traffic, such as emergency vehicle warnings, being delayed or lost entirely.

- **Jamming Attacks:** Malicious nodes can perform jamming attacks by transmitting signals that interfere with the normal communication channels used in VANETs. This can degrade the quality of service or make communication impossible in certain areas.

1.2.2. Mitigating These Threats

To mitigate the vulnerabilities caused by malicious nodes in VANETs, several security mechanisms and protocols are being developed:

- **Cryptographic Measures:** Authentication, encryption, and digital signatures can ensure the integrity and authenticity of messages. Public Key Infrastructure (PKI) is often used for secure communication in VANETs.
- **Intrusion Detection Systems (IDS):** These systems monitor the network for abnormal behavior and can help detect malicious nodes or attacks.
- **Trust Management Systems:** Trust-based mechanisms can assess the behavior of nodes over time, identifying malicious actors based on suspicious activities.
- **Blockchain Technology:** Some researchers are exploring the use of blockchain to create secure, decentralized communication in VANETs, which can help mitigate issues like Sybil and blackhole attacks.
- **Position Verification Algorithms:** These are designed to ensure that the position information broadcasted by vehicles is accurate and trustworthy.

Journal of Information Systems Engineering and Management
2025, 10(42s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- **Anonymous Communication Protocols:** To preserve privacy, VANETs can employ techniques like pseudonymity or mix zones, where vehicles change their identifiers periodically to prevent tracking.

In summary, malicious nodes are a major threat to the safe and efficient operation of VANETs, as they can disrupt communication, degrade network performance, and endanger driver safety. Robust security measures, such as encryption, trust management, and intrusion detection, are essential to mitigate these vulnerabilities.

1.3 Objectives:

1.3.1. Aim:

The primary aim of the paper is to design and develop a robust detection framework that leverages machine learning techniques to accurately identify malicious nodes within a vehicular ad-hoc network (VANET) environment. This framework should enhance the security and reliability of VANETs by mitigating the impact of malicious actors that pose a threat to communication and safety.

1.3.2. Objectives:

- **To identify key characteristics of malicious nodes** in VANETs that differentiate them from legitimate nodes.
- **To develop a dataset or use existing datasets** that contain both normal and malicious node behaviors, ensuring a comprehensive representation of potential attack scenarios.
- **To explore various machine learning algorithms** (such as supervised, unsupervised, or semi-supervised learning) to detect malicious nodes based on the identified features.
- **To evaluate the performance of the proposed detection framework** using metrics such as accuracy, precision, recall, and false positive rate, ensuring that it effectively identifies malicious nodes while minimizing false alarms.
- **To compare the proposed framework with existing malicious node detection methods**, demonstrating its advantages in terms of detection accuracy, computational efficiency, and adaptability to different VANET scenarios.
- **To ensure the framework's robustness and scalability**, so that it can be applied to real-world VANET environments with varying traffic densities and communication patterns.

In essence, the paper aims to propose an intelligent and effective solution to the challenge of detecting malicious nodes in VANETs, ensuring secure and reliable communication for vehicular networks.

LITERATURE REVIEW

2.1 Overview of VANET Architecture:

Vehicular Ad-hoc Networks (VANETs) are a subset of Mobile Ad-hoc Networks (MANETs) specifically designed to support communication between vehicles on the road and between vehicles and infrastructure. They aim to improve road safety, reduce traffic congestion, and enable infotainment services. The architecture of VANETs comprises several components and communication types, namely **vehicle-to-vehicle (V2V)** and **vehicle-to-infrastructure (V2I)** communication, as well as some newer types of communication (e.g., V2X). Here's an in-depth overview of the architecture and key components of VANETs:

2.1.1. Components of VANET Architecture

A typical VANET architecture consists of the following three components:

- **On-Board Units (OBUs):** OBUs are communication devices installed in vehicles that facilitate V2V and V2I communication. They handle data processing, packet transmission, and routing, as well as running applications that enhance driving safety or provide infotainment services. OBUs rely on dedicated short-range communication (DSRC) or Cellular V2X (C-V2X) technologies.

Journal of Information Systems Engineering and Management
2025, 10(42s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- **Roadside Units (RSUs):** RSUs are stationary units placed at strategic points along roadways, such as intersections, traffic lights, or pedestrian crossings. These units communicate with OBUs to extend network coverage, relay data between vehicles, and connect vehicles to back-end servers or the internet. RSUs also play a critical role in facilitating V2I communication, especially for applications like traffic management, environmental monitoring, and emergency services.
- **Trust Authorities (TAs):** Also called Certification Authorities, TAs are centralized authorities responsible for managing security in VANETs. They issue cryptographic keys, manage identity verification, and revoke keys if a vehicle or RSU is compromised. TAs ensure data integrity and confidentiality, helping to prevent unauthorized access, data manipulation, and malicious activity within the network.

2.1.2. Types of Communication in VANETs

VANET communication is classified into several types based on the entities involved in the data exchange:

a. Vehicle-to-Vehicle (V2V) Communication

V2V communication enables direct data exchange between vehicles within a specific range. Vehicles communicate to share safety information such as position, speed, and braking status to prevent collisions and enhance situational awareness. Key applications of V2V communication include:

- **Collision avoidance:** Alerts drivers about potential collisions.
- **Platooning:** Allows vehicles to drive closely together in a coordinated manner, enhancing road capacity.
- **Emergency vehicle warnings:** Sends alerts to nearby vehicles when emergency vehicles are approaching.
- **Traffic and congestion updates:** Shares real-time traffic data to aid in rerouting or congestion avoidance.

b. Vehicle-to-Infrastructure (V2I) Communication

V2I communication enables data exchange between vehicles and RSUs (e.g., traffic lights or other fixed installations). V2I communication facilitates data sharing for applications that require information from a broader network beyond nearby vehicles. Examples of V2I applications include:

- **Traffic signal management:** Provides information to vehicles about traffic light changes or intersections, helping to manage traffic flow efficiently.
- **Parking assistance:** Offers real-time parking availability information.
- **Toll collection:** Facilitates automated toll payment as vehicles pass toll booths.
- **Environmental monitoring:** Collects data on road conditions, pollution levels, and weather information, relaying it back to vehicles or central systems.

c. Vehicle-to-Pedestrian (V2P) Communication

V2P communication is an emerging type that allows vehicles to communicate with pedestrians, especially those using mobile devices or wearable technology. This type of communication can help prevent accidents at pedestrian crossings or in areas with heavy foot traffic.

d. Vehicle-to-Network (V2N) Communication

V2N communication connects vehicles to backend servers or cloud platforms via cellular networks. This connection enables vehicles to receive information on traffic conditions, weather forecasts, map updates, or even content for infotainment.

e. Vehicle-to-Everything (V2X) Communication

Journal of Information Systems Engineering and Management
2025, 10(42s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

V2X communication is a broad term encompassing V2V, V2I, V2P, and V2N communication. V2X is the foundation of a connected vehicle ecosystem that enables real-time, comprehensive data sharing among vehicles, infrastructure, pedestrians, and networked systems, creating a fully connected transportation network.

2.1.3. Communication Technologies in VANETs

VANETs rely on specific communication technologies that support real-time, high-speed data transfer:

- **Dedicated Short-Range Communication (DSRC):** DSRC is a wireless communication standard specifically designed for V2V and V2I communication. It operates in the 5.9 GHz frequency band and supports low-latency data transmission over a range of 300-1000 meters, making it suitable for safety-critical applications.
- **Cellular V2X (C-V2X):** C-V2X is an advanced communication protocol that utilizes existing cellular infrastructure to support V2V, V2I, and V2N communications. It provides broader coverage than DSRC, enhanced data rates, and increased reliability, especially for applications involving data-intensive communication.
- **5G Technology:** With ultra-low latency, high data rates, and support for massive device connectivity, 5G is expected to play a significant role in VANETs. It enables advanced V2X applications such as autonomous driving, cooperative platooning, and remote vehicle control.

2.1.4. Key Functional Layers in VANET Architecture

The VANET architecture is typically structured into functional layers, similar to the OSI model:

- **Physical Layer:** This layer deals with data transmission over physical media, ensuring connectivity between nodes.
- **Data Link Layer:** Responsible for data frame delivery, MAC layer protocols in this layer handle collision avoidance and channel access in the shared communication environment.
- **Network Layer:** The network layer is responsible for routing and packet forwarding. VANETs use ad-hoc routing protocols, such as Ad-hoc On-Demand Distance Vector (AODV) and Geographic Routing Protocol (GRP), to handle the dynamic topology and mobility of nodes.
- **Transport Layer:** This layer manages end-to-end communication and provides reliable data transmission through protocols like Transmission Control Protocol (TCP) or User Datagram Protocol (UDP), depending on the application's requirements.
- **Application Layer:** The application layer hosts various VANET applications such as collision avoidance, traffic monitoring, emergency alerts, and infotainment services.

2.1.5. Security and Privacy Mechanisms in VANET Architecture

Since VANETs are vulnerable to threats such as eavesdropping, message tampering, and denial-of-service attacks, robust security mechanisms are integrated into the architecture:

- **Encryption and Authentication:** Encryption ensures data confidentiality, while authentication mechanisms verify the legitimacy of the data source, helping to prevent malicious attacks from unauthorized nodes.
- **Access Control:** Access control mechanisms regulate which nodes can communicate within the network, preventing unauthorized vehicles from accessing sensitive data.
- **Privacy Protection:** Privacy measures protect user identities and locations, using techniques such as pseudonymity or dynamic changing of identifiers.

2.1.6. Applications of VANETs

Journal of Information Systems Engineering and Management
2025, 10(42s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The VANET architecture supports a wide range of applications that benefit drivers, passengers, and traffic management authorities:

- **Safety Applications:** Accident prevention, lane-changing assistance, and warning notifications.
- **Traffic Management:** Real-time monitoring of traffic flow, congestion reduction, and optimized traffic light control.
- **Infotainment:** Internet access, media streaming, and social networking.
- **Environmental Monitoring:** Data collection on pollution and weather for use in vehicle or infrastructure decision-making.

VANET architecture is a comprehensive framework composed of mobile and stationary units, communication protocols, functional layers, and security mechanisms. Through V2V, V2I, V2P, and V2N communication, VANETs enable seamless data sharing across vehicles and infrastructure, improving safety, efficiency, and user experience on the road. The deployment of advanced technologies like DSRC, C-V2X, and 5G further enhances VANETs' capability to support critical applications and adapt to dynamic driving environments.

2.2 Existing Detection Techniques:

In Vehicular Ad-hoc Networks (VANETs), detecting malicious nodes is crucial for maintaining security, safety, and reliable communication. Various detection techniques are currently employed, ranging from traditional Intrusion Detection Systems (IDS) to advanced anomaly detection methods. Here's a review of some existing methods used for identifying malicious nodes in VANETs:

2.2.1. Signature-based Intrusion Detection Systems (IDS)

Signature-based IDS [17] techniques rely on the patterns and signatures of the already known attacks that are predefined. This method involves storing a database of attack patterns and comparing network traffic against this database to detect malicious nodes.

- **Advantages:** Signature-based IDS can quickly and accurately identify known attacks with minimal false positives.
- **Disadvantages:** These systems are limited in their ability to detect new or unknown attacks (zero-day attacks), as they lack the signatures to identify them. Additionally, the high mobility and dynamic topology in VANETs make it challenging to maintain and update the signature database.

Examples of Signature-based IDS in VANETs:

- Systems that identify packet flooding attacks by checking for unusually high packet transmission rates.
- IDS implementations for detecting Sybil attacks by comparing identity or position spoofing patterns.

2.2.2. Anomaly-based Intrusion Detection Systems (IDS)

Anomaly-based IDS [25] detect deviations from normal behavior in network traffic. This method typically establishes a baseline for normal network behavior, and any deviation from this baseline is flagged as potentially malicious.

- **Advantages:** Anomaly-based IDS can detect both known and unknown (new) attacks, making them useful for highly dynamic networks like VANETs.
- **Disadvantages:** Anomaly-based IDS are prone to high false-positive rates because network behavior can vary significantly based on external factors (e.g., traffic density, road conditions, and driver behavior). Setting an accurate baseline for normal behavior is challenging in VANETs due to constant changes in node location and communication patterns.

Examples of Anomaly-based IDS in VANETs:

Journal of Information Systems Engineering and Management
2025, 10(42s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- Systems that detect unusual speed or sudden braking patterns that deviate from expected driving behavior, which could indicate malicious node activity.
- IDS that flag communication patterns inconsistent with normal traffic, potentially identifying a DoS or Sybil attack.

2.2.3. Specification-based Detection

Specification-based detection contains the key characteristics of both the IDS, Signature-based and Anomaly-based. It involves defining a set of rules that describe acceptable network behaviour, and any deviation from these specifications is treated as suspicious.

- **Advantages:** This method has a lower false-positive rate than anomaly-based IDS, as it is tailored to specific VANET applications.
- **Disadvantages:** Creating accurate specifications for VANET applications can be complex, as they need to consider a wide range of acceptable behaviors to avoid generating false positives.

Examples of Specification-based Detection in VANETs:

- Systems that enforce predefined rules for how vehicles should respond to emergency signals or alerts.
- Applications where the system flags any unauthorized message exchange, such as messages coming from non-registered nodes, as potentially malicious.

2.2.4. Machine Learning-based Detection

Machine learning (ML) techniques [2][5] for IDS in VANETs involve training models on data from both benign and malicious activities to recognize patterns associated with malicious nodes. Common ML algorithms include decision trees, support vector machines (SVM), neural networks, and clustering methods.

- **Advantages:** ML-based detection can automatically adapt to changes in network traffic patterns and detect both known and unknown attacks, making them highly effective in the dynamic VANET environment.
- **Disadvantages:** Machine learning models can be computationally expensive and require large amounts of data for training. Additionally, their effectiveness depends on the quality of the training data and the ability to reduce false positives.

Examples of Machine Learning-based Detection in VANETs:

- Decision tree classifiers trained to detect misbehavior in communication patterns, identifying nodes that deviate from the norm.
- Clustering algorithms that analyze vehicle position and movement patterns to detect anomalies indicative of Sybil attacks or location spoofing.

2.2.5. Trust-based Detection Systems

Trust-based detection [20][21] systems evaluate the trustworthiness of nodes based on their behavior over time. In these systems, nodes accumulate trust scores based on interactions with other nodes, with nodes exhibiting suspicious behavior receiving lower trust scores.

- **Advantages:** Trust-based systems are resilient to certain types of attacks, like Sybil attacks, and they are more adaptable to dynamic environments where direct observation of malicious behavior may be challenging.
- **Disadvantages:** Trust-based systems can be vulnerable to “bad-mouthing” attacks, where malicious nodes collude to lower the trust scores of legitimate nodes, or “ballot-stuffing” attacks, where colluding nodes artificially inflate each other’s scores.

Examples of Trust-based Detection in VANETs:

Journal of Information Systems Engineering and Management
2025, 10(42s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- Reputation-based frameworks where each vehicle maintains trust scores for neighboring vehicles, decreasing trust for those behaving suspiciously (e.g., repeatedly sending conflicting location data).
- Collaborative trust models in which vehicles share reputation information to collectively assess the reliability of other nodes in the network.

2.2.6. Game Theory-based Detection

Game theory-based detection[27] employs mathematical models where vehicles and potential attackers are treated as players in a game. This approach models interactions between benign and malicious nodes as strategic games and uses optimal strategies to detect malicious activities.

- **Advantages:** Game theory-based approaches can help anticipate and mitigate attacks by analyzing the incentives and likely actions of attackers, making it an effective method for adaptive security in VANETs.
- **Disadvantages:** These methods can be computationally complex and require accurate modeling of attacker behavior, which may not be feasible in highly dynamic VANET environments.

Examples of Game Theory-based Detection in VANETs:

- Games where legitimate vehicles aim to minimize risks and attackers aim to maximize disruption, helping the system learn optimal responses to potential attacks.
- Detection systems where the trustworthiness of nodes is evaluated based on a cost-benefit model, rewarding cooperative nodes while penalizing malicious actions.

2.2.7. Hybrid Detection Systems

Hybrid detection systems combine multiple techniques, such as integrating anomaly-based and signature-based detection or combining machine learning with trust-based mechanisms, to leverage the strengths of each approach.

- **Advantages:** Hybrid systems improve detection accuracy by compensating for the weaknesses of individual methods, making them highly effective in complex and dynamic VANET environments.
- **Disadvantages:** They tend to be computationally intensive and may require complex configuration and management.

Examples of Hybrid Detection Systems in VANETs:

- Systems that use anomaly-based detection to identify potential threats and then verify these threats with signature-based detection for improved accuracy.
- Hybrid models that incorporate machine learning for anomaly detection and trust scores for context verification, reducing false positives.

Summary of Detection Techniques

Detection Technique	Pros	Cons
Signature-based IDS	High accuracy for known attacks	Limited against new attacks
Anomaly-based IDS	Detects unknown attacks	High false-positive rates
Specification-based	Low false positives	Challenging to define accurate specifications
Machine Learning-based	Adaptive, detects unknown attacks	Computationally intensive, data-dependent
Trust-based	Resilient, suitable for collaborative models	Vulnerable to collusion, requires trust modelling
Game Theory-based	Models attacker behavior, adaptive	High complexity, requires accurate behavior models

Journal of Information Systems Engineering and Management
2025, 10(42s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Detection Technique	Pros	Cons
Hybrid Systems	Combines strengths of multiple methods	High computational cost, complex configuration

2.3 Machine Learning Applications:

Machine learning (ML) is a powerful tool in the context of Vehicular Ad-hoc Networks (VANETs), as it enables vehicles and infrastructure components to analyze data, predict patterns, and improve safety and efficiency in real time. The dynamic nature of VANETs makes ML particularly useful for applications ranging from traffic management to intrusion detection. Here's an overview of some primary applications of machine learning in VANETs, followed by a summary of how ML is transforming network security, particularly through enhanced detection accuracy and adaptability.

2.3.1. Machine Learning Applications in VANETs

- **Traffic Flow Prediction and Congestion Management**
  - **Application:** ML algorithms can predict traffic patterns by analyzing vehicle speed, density, and historical data, which helps in preventing congestion and optimizing traffic flow.
  - **Example:** Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks are commonly used for time-series forecasting in traffic prediction, enabling real-time route optimization and congestion alerts.
  - **Impact:** Improves traffic flow, reduces travel times, and minimizes fuel consumption by providing drivers with optimal routes based on predicted traffic conditions.
- **Collision Avoidance and Safety Enhancements**
  - **Application:** Machine learning models analyze sensor data from surrounding vehicles and infrastructure to identify potential collision risks, alerting drivers or triggering automated braking systems.
  - **Example:** Deep learning models, such as Convolutional Neural Networks (CNNs), analyze visual data (e.g., camera feeds) and integrate with sensor data to identify obstacles or hazardous situations.
  - **Impact:** Enhances road safety by detecting and mitigating potential accidents, even in complex scenarios such as intersections or multi-lane highways.
- **Driver Behavior Analysis**
  - **Application:** Machine learning models evaluate driver behavior patterns (e.g., speed, lane changes, sudden braking) to detect risky or abnormal driving, such as distracted or aggressive driving.
  - **Example:** Support Vector Machines (SVM) and decision trees are often used to classify behaviors as safe or risky based on predefined features.
  - **Impact:** Enables early warning systems that can alert the driver or surrounding vehicles of potentially hazardous driving behaviors, improving overall road safety.
- **Location-based Services and Route Planning**
  - **Application:** ML models in VANETs enable personalized route recommendations by considering user preferences, traffic data, and road conditions.
  - **Example:** Reinforcement learning and collaborative filtering are used to provide tailored route suggestions based on a driver's historical route data and real-time traffic information.
  - **Impact:** Enhances user convenience by recommending faster or more fuel-efficient routes, potentially avoiding heavy traffic or high-risk areas.

Journal of Information Systems Engineering and Management
2025, 10(42s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- **Intrusion Detection and Security Monitoring**
    - **Application:** VANETs are vulnerable to security threats, such as Sybil attacks and false data injection. Machine learning models identify anomalies in communication patterns, helping to detect and prevent malicious activity.
    - **Example:** Anomaly detection algorithms, clustering techniques, and neural networks can analyze communication patterns to detect suspicious activities, alerting the network to potential threats.
    - **Impact:** Improves the overall security and reliability of the VANET by detecting intrusions early, mitigating risks to data integrity, and maintaining trust in the network.
- **Predictive Maintenance**
    - **Application:** Machine learning in VANETs can analyze sensor data from vehicles to predict when maintenance will be needed, reducing the likelihood of vehicle breakdowns on the road.
    - **Example:** Machine learning models, like decision trees and neural networks, analyze engine and performance data to predict failures before they occur.
    - **Impact:** Prevents vehicle downtime by allowing for timely repairs and maintenance, increasing vehicle longevity and enhancing the reliability of VANETs for all users.
- **Environmental and Emission Monitoring**
    - **Application:** ML algorithms help monitor vehicle emissions and suggest changes in driving behavior or alternative routes to reduce overall environmental impact.
    - **Example:** Regression models can predict emission levels based on driving speed, traffic patterns, and engine performance, helping cities develop eco-friendly traffic policies.
    - **Impact:** Supports sustainable urban mobility by identifying emission-heavy routes or behaviors and promoting more environmentally friendly driving habits.

2.3.2. Machine Learning in Network Security for VANETs

Machine learning plays a transformative role in network security within VANETs, where dynamic and frequent interactions between vehicles, infrastructure, and potentially malicious nodes present unique security challenges. Here's how machine learning enhances VANET security:

A. Enhanced Intrusion Detection and Prevention

- **Application:** Machine learning models, such as anomaly detection, are used to identify deviations in network traffic patterns that may indicate security breaches. These models classify network activities into normal and abnormal, allowing early detection of threats.
- **Impact:** Increases detection accuracy by learning from historical attack data and reducing false positives, crucial in VANETs where quick and accurate responses are necessary to prevent disruptions in communication and ensure vehicle safety.

B. Detection of Malicious Nodes and Message Integrity Attacks

- **Application:** Machine learning models analyze patterns in data transmission and behavior to detect malicious nodes that attempt to spread false information or launch Sybil attacks.
- **Example:** Supervised learning algorithms, like decision trees and SVMs, identify anomalies in data flows, signaling potential spoofing or message tampering.
- **Impact:** Prevents disruptions in communication by accurately identifying malicious nodes, thus ensuring reliable information flow within VANETs for safe decision-making.

Journal of Information Systems Engineering and Management
2025, 10(42s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

C. Phishing and Social Engineering Detection

- **Application:** Machine learning models identify and block social engineering and phishing attempts that target users in VANETs through deceptive messages or unsafe navigation prompts.
- **Example:** NLP and deep learning models are used to analyze message content for potential indicators of phishing, filtering out suspicious communication attempts.
- **Impact:** Reduces the success of phishing attacks within VANET environments by securing driver and vehicle communication channels, thus protecting personal and vehicular data.

D. Real-time Behavior Analysis for Intrusion Detection

- **Application:** Machine learning models in VANETs monitor real-time behavior of nodes, detecting anomalous activities that may signal a breach or malicious behavior.
- **Example:** Anomaly-based models establish a baseline of typical behavior and detect any deviations from this standard, identifying insider or outsider threats.
- **Impact:** Enables rapid detection of network anomalies, essential for preventing immediate threats and adapting to new, evolving attacks in the VANET environment.

E. Detection of Unauthorized Access and Secure Access Control

- **Application:** ML models enhance access control systems within VANETs by analyzing patterns in access requests and granting or denying access based on behavior analytics.
- **Example:** Techniques such as clustering and reinforcement learning models create dynamic access protocols based on usage history and access patterns.
- **Impact:** Improves security by dynamically adapting to new threats, preventing unauthorized access, and securing data exchange in VANETs.

2.3.3. Benefits of Machine Learning in VANET Network Security

- **Improved Detection Accuracy:** Machine learning's ability to analyze complex patterns enables precise detection of security threats. This minimizes false positives, making it easier to identify both known and unknown threats, enhancing the overall security of VANETs.
- **Adaptability to New Threats:** ML models continuously adapt to the evolving threats by learning from new data. This is especially important in VANETs, where attackers might use novel tactics that need real-time responses without pre-defined signatures.
- **Real-time Threat Detection and Response:** Machine learning models can process high volumes of data quickly, identifying threats in real time. This is critical in VANETs, where fast-moving vehicles rely on rapid, secure communication to ensure safety.
- **Scalability for Dynamic Networks:** VANETs involve a constantly changing network of vehicles, and machine learning models are scalable, capable of handling large, dynamic datasets. This makes ML suitable for VANETs, where manual security monitoring would be impractical.
- **Behavior-based Security for Advanced Threats:** ML models can detect subtle deviations in network behavior, making them particularly effective against advanced persistent threats (APTs) and insider attacks that might evade traditional signature-based methods.

Conclusion

Journal of Information Systems Engineering and Management
2025, 10(42s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Machine learning offers numerous applications in VANETs, ranging from traffic prediction and collision avoidance to intrusion detection and driver behavior analysis. In network security, ML enables accurate and adaptive detection of both known and unknown threats, helping VANETs maintain secure, reliable, and efficient communication in a dynamic environment. As machine learning techniques continue to advance, their applications in VANETs will expand, offering new levels of automation, adaptability, and security to support smart transportation systems.

PROPOSED FRAMEWORK

3.1 Framework Overview: To propose a hybrid detection system combining machine learning with a trust-based model in VANET, it's essential to outline an architecture that leverages both ML's data-driven detection capabilities and trust-based mechanisms' reliance on evaluating node behavior and reputation. This hybrid system aims to enhance security by improving detection accuracy, adaptability to new attacks, and resilience against malicious nodes. Here's a breakdown of how to structure this proposal:

3.1.1. Objectives of the Hybrid Detection System

- **Enhanced Detection Accuracy**: Combine ML's high detection accuracy with trust models to reduce false positives.
- **Real-time Detection**: Ensure that the system can detect malicious activities in real-time or near real-time to support dynamic, fast-moving VANET environments.
- **Adaptability to New Threats**: The ML component should continuously learn from emerging threats, while the trust model can evaluate new and existing nodes based on their behavior.
- **Resilience to Malicious Nodes**: The trust model helps the system identify untrustworthy nodes, while ML detects abnormal behaviors that might signify attacks.

3.1.2. Outline of the Hybrid System Architecture

A proposed hybrid system could include the following components:

- **Data Collection Module**: Collect data from vehicles, infrastructure, and roadside units (RSUs). Data sources include vehicle behavior, communication patterns, environmental factors, and historical reputation data of each node.
- **Feature Extraction and Preprocessing**: Extract features such as speed, distance, signal strength, message frequency, and trust metrics (reputation score, transaction history).
- **Machine Learning Module**: Use supervised or unsupervised ML algorithms to identify abnormal patterns. For example:
    - **Anomaly Detection Models**: Use clustering or autoencoders to flag suspicious behavior in the network.
    - **Classification Models**: Classify messages or nodes as "normal" or "malicious" based on patterns in the data.
- **Trust-Based Model**: Calculate a trust score for each node based on historical behavior, message validity, and interactions with other nodes. The trust score considers:
    - **Direct Trust**: A score based on the direct interaction history between two nodes.
    - **Indirect Trust**: A score calculated based on other nodes' feedback about a particular node.
    - **Dynamic Update Mechanism**: Trust scores are updated in real-time based on recent actions to account for changes in node behavior.

Journal of Information Systems Engineering and Management
2025, 10(42s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- **Decision Fusion Module**: Combines outputs from both the ML model and the trust-based model to make a final decision on whether to flag a node or communication as malicious. The fusion algorithm can use weight-based scoring, in which:
    - **Trust Model Confidence**: Prioritizes trust scores when detecting low-level threats or consistent behavior patterns.
    - **Machine Learning Confidence**: Prioritizes ML when detecting complex or emerging threats based on data patterns.

3.1.3. Proposed Work

The following steps outline the process involved in the proposed work:

- Each vehicle registers itself with the Certification Authority (CA).
- The CA provides the vehicle with credits and a certificate that grants access to the network.
- Upon verifying the vehicle's certificate, the Roadside Unit assigns it a pseudo ID.
- The sending vehicle (Vs) transmits the message "msg" along with a cost "C", formatted as: Data = msg + C;
- When the vehicle sends the message, the Trusted Platform Module (TPM) in the vehicle automatically deducts the cost "c" from its credits. The new credit score is updated as: $Cr_{new} = Cr_{old} - C$;
- Upon receiving the data, the receiving vehicle (Vr) checks the following parameters:
    - Density "D" of nodes in the network.
    - Number of nodes "N" from which the same message has been received.
    - The cost "C_k" associated with the transmission of the message from k numbers of vehicles.
- The authenticity of the message is verified using the proposed formula:
$$\mathbf{M_{auth} = \alpha D + \beta N + \gamma(\Sigma C_k) + \phi}$$
- The authenticity of the message, denoted as "M_{auth}", is assessed on the scale of 1-10 as follows:
    - If ($M_{auth} \geq 7$)
      Denotes **"High"** message authenticity;
      The message is accepted.
    - Else if ($4 \leq M_{auth} < 7$)
      Denotes **"Medium"** message authenticity;

      The message may either be accepted or rejected.
    - Else
      Denotes **"Low"** message authenticity;
      The message is rejected.
- If the receiving vehicle (Vr) determines the message to be valid, it sends an acknowledgment (ACK) to the sending node.
- The Trusted Platform Module (TPM) of the sending node will then increase its credits by "2C", and the updated credit score is calculated as:
$$Cr_{new} = Cr_{old} + 2C;$$
- If the message is rejected, no acknowledgment (ACK) is sent.

In our proposed approach, we focus on verifying the authenticity of the message to reduce the propagation of faulty data across the network. To achieve this, the following formula is used for message authentication:

$$M_{auth} = \alpha D + \beta N + \gamma(\Sigma C_k) + \phi$$

This formula includes several coefficients: the coefficient of density (α), the coefficient for the number of nodes sending the same message (β), the coefficient for the total sum of costs at which different vehicles transmit the message (γ), and the constant (ϕ).To derive and validate the values for the coefficients α, β, γ, and the constant ϕ used in this formula, we will undergo two key phases: the "Training Phase" and the "Testing Phase".

CONCLUSION

The detection techniques, when implemented in VANETs, aim to enhance network security by identifying malicious nodes, ensuring safer and more reliable communication for all vehicles in the network. Each technique offers unique strengths and limitations, and hybrid models often provide the best balance of detection accuracy and resource efficiency. By combining machine learning and trust-based approaches, this hybrid detection system is poised to provide a powerful defence mechanism in VANETs, capable of detecting a wide range of threats with high accuracy and adaptability. Using the Hybrid model will result in Reduced false positives, enhanced robustness, and improved scalability. The trust model complements the ML detection, making the system more resilient to single-event anomalies. By incorporating both ML and trust, the system is more adaptable to new and unknown threats. This approach scales effectively in large networks since trust scores help limit computational demands by focusing on high-risk nodes. However, privacy-preserving mechanisms must be considered, as sharing trust data could reveal sensitive information. Also, lightweight ML algorithms must be investigated to ensure efficient resource use.

REFRENCES

[1] Claudio Piccolo Fernandes, Carlos Montez, Daniel Domingos Adriano, Azzedine Boukerche, Michelle S. Wangham, “A blockchain-based reputation system for trusted VANET nodes“ Elsevier, Adhoc Networks, Vol. 140 (2023) Issue 103071, https://doi.org/10.1016/j.adhoc.2022.103071 pp. 1-18, December, 2022.

[2] Rashid, K.; Saeed, Y.; Ali, A.; Jamil, F.; Alkanhel, R.; Muthanna, A. “An Adaptive Real-Time Malicious Node Detection Framework Using Machine Learning in Vehicular Ad-Hoc Networks (VANETs)”, Sensors **2023**, MDPI, Volume. 23, Issue 2594. https://doi.org/10.3390/s23052594, pp. 1-34 February 2023.

[3] Hamayoun Shahwani, Syed Attique Shah, Muhammad Ashraf, Muhammad Akram, Jaehoon (Paul) Jeong, Jitae Shin, “A comprehensive survey on data dissemination in Vehicular Ad Hoc Networks”, Elsevier, Vehicular Communications, Vol. 34 (2022), Issue 100420, https://doi.org/10.1016/j.vehcom.2021.100420 pp. 1-17, October 2021.

[4] Abir Mcherguia, Tarek Moulahi, Sherali Zeadally, “ Survey on Artificial Intelligence (AI) techniques for Vehicular Ad-hoc Networks (VANETs)”, ”, Elsevier, Vehicular Communications, Vol. 34 (2022), Issue 100403, 10.1016/j.vehcom.2021.100403 pp. 1-16, April 2022.

[5] Anum Talpur, Mohan Gurusamy, “Machine Learning for Security in Vehicular Networks: A Comprehensive Survey”, IEEE, Vol.24, Issue 1, 10.1109/COMST.2021.3129079 pp.346-379, November 2021.

[6] Shafika Showkat Moni, D. Manivannan, ”A scalable and distributed architecture for secure and privacy-preserving authentication and message dissemination in VANETs”, Elsevier, Internet of Things, Vol. 13 (2021), Issue 100350, 10.1016/j.iot.2020.100350 pp. 1-21, December 2020.

[7] Xia Feng, Kaiping Cui, Haobin Jiang, Ze Li, ”EBAS: An Efficient Blockchain-Based Authentication Scheme for Secure Communication in Vehicular Ad Hoc Network”, MDPI, Symmetry, Vol. 14 (2022), Issue 1230, https://doi.org/10.3390/sym14061230 pp. 1-22, June 2022.

[8] Haobin Jiang et.al. “SAES: A self-checking authentication scheme with higher efficiency and security for VANET”, Peer-to-Peer Networking and Applications (2021), Volume 14, Springer Science+Business Media, LLC, part of Springer Nature, pp. 528-540, October 2020.

[9] Kang Tan et.al. “Machine learning in vehicular networking: An overview”, Elsevier, Digital Communications and Networks, Vol. 8, Issue 1, https://doi.org/10.1016/j.dcan.2021.10.007 pp. 18-24, February 2022.

[10] Sahil Khatri et.al. "Machine learning models and techniques for VANET based traffic management: Implementation issues and challenges", © Springer Science+Business Media, LLC, part of Springer Nature 2020, Peer-to-Peer Networking and Applications (2021), Vol 14, pp. 1778–1805, September 2020.
[11] Sami Abduljabbar Rashid et.al."Reliable and efficient data dissemination scheme in VANET: a review", International Journal of Electrical and Computer Engineering (IJECE) Volume 10, Issue 6, http://doi.org/10.11591/ijece.v10i6.pp6423-6434 pp. 6423-6434, December 2020
[12]Elmustafa Sayed Ali et.al. "Machine Learning Technologies for Secure Vehicular Communication in Internet of Vehicles: Recent Advances and Applications", Hindawi, Security and Communication Networks (2021), Vol. 1, 10.1155/2021/8868355 pp. 1-23, March 2021.
[13] Zehra Afzal et.al. "Security of Vehicular Ad-Hoc Networks (VANET): A survey", Third National Conference on Computational Intelligence (NCCI 2019), IOP Publishing, Journal of Physics, Volume-1427, 10.1088/1742-6596/1427/1/012015 pp. 1-9, 2020.
[14] Muhammad Sameer Sheikh et.al. "Security and Privacy in Vehicular Ad Hoc Network and Vehicle Cloud Computing: A Survey", Wiley, Hindawi, Wireless Communications and Mobile Computing Volume 2020, 10.1155/2020/5129620 pp. 1-25, January 2020.
[15] Krishna Verma et.al. "A STUDY ON VANET AND ITS SECURITY ISSUES", International Journal of Recent Scientific Research Vol. 10, Issue, 06(I), pp. 33298-33303, June 2019.
[16] R K Mahesh et. al. "SFTD: A SMART forwarding technique based reliable data dissemination scheme for VANETs ", Elsevier, Measurement: Sensors, Vol.24, Issue 100572, pp. 1-7, 10.1016/j.measen.2022.100572 November 2022.
[17] Maryam Rajabzadeh Asaar et.al. "A Secure and Efficient Authentication Technique for Vehicular Ad-Hoc Networks", IEEE Transactions on Vehicular Technology, Vol. 67, Issue. 6, pp. 5409-5423, 10.1109/TVT.2018.2822768 June 2018.
[18] Murtadha A. Alazzawi et. al. "Efficient Conditional Anonymity with Message Integrity and Authentication in a Vehicular Ad-Hoc Network", IEEE Access, Volume 7, pp. 71424-71435, June 2019.
[19] Archana K V et.al. "Incentive-based communication in van using blockchain technology", Journal of Emerging Technologies and Innovative Research (JETIR), Volume 6, Issue 5, pp. 334-337, May 2019.
[20] Nazish Siddiqui, Mohd Shahid Husain, "CTS: A Credit based Threshold System to Minimize the Dissemination of Faulty Data in Vehicular Adhoc Networks", in the proceedings of International Conference on Sustainable Computing Techniques in Engineering Science & Management, IJCTA, © International Science Press, Volume 9, Issue 17, pp. 8499-8508, 2016.
[21] N. Siddiqui, M.S.Husain, "An Approach to Minimize Faulty Data Propagation in Vehicular Adhoc Network", HCTL Open International Journal of Technology Innovations and Research (IJTIR) http://ijtir.hctl.org, Volume 21, Issue 1, e-ISSN: 2321-1814, ISBN (Print): 978-81- 932623-1-3, pp. 1-13, July 2016.
[22] Nazish Siddiqui, Mohd Shahid Husain, Mohammad Akbar, "Analysis of Security Challenges in Vehicular Adhoc Network", in the proceedings of the international conference on advancement in computer engineering & information technology, IJCSIT, pp. s87-s90, 2016.
[23] Muhammad Rizwan Ghori, Kamal Z. Zamli, Nik Quosthoni, Muhammad Hisyam, Mohamed Montaser, "Vehicular Ad-hoc Network (VANET): Review", in the proceedings of IEEE International Conference on Innovative Research and Development (ICIRD), pp. 1-6, 2018.
[24] Dajun Zhang, F. Richard Yu, Ruizhe Yang, and Li Zhu "Software-Defined Vehicular Networks With Trust Management: A Deep Reinforcement Learning Approach", IEEE Transactions On Intelligent Transportation Systems, Volume 23, Issue 2, https://doi.org/10.1109/TITS.2020.3025684 pp. 1400-1414, February 2022.
[25] Tejasvi Alladi ,Bhavya Gera, Ayush Agrawal, Vinay Chamola, and Fei Richard Yu " Deepadv: A Deep Neural Network Framework For Anomaly Detection In Vanets", IEEE Transactions On Vehicular Technology, Volume 70, Issue 11,10.1109/TVT.2021.3113807pp. 12013-12023, November 2021.
[26] Aekta Sharma and Arunita Jaekel, "Machine Learning Based Misbehaviour Detection in VANET Using Consecutive BSM Approach", IEEE Open Journal of Vehicular technology, Volume 3, pp. 1-14, 10.1109/OJVT.2021.3138354 December 2021.

Journal of Information Systems Engineering and Management
2025, 10(42s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

[27] Hadjer Messabih, Chaker Abdelaziz Kerrache, Youssra Cheriguene, Carlos T. Calafate, Fatima Zohra Bousbaa, "An Overview of Game Theory Approaches for Mobile Ad-Hoc Network's Security", IEEE Access, Volume 11, 10.1109/ACCESS.2023.3321082 pp. 1-25, October 2023.