Kashifa Khan, 2026, 14:4
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

# Machine Learning based Blackhole Attacker Detection and Prevention Approach in VANET

**Kashifa Khan, Devdas Saraswat Associate Professor**
Computer Science & Engineering, LNCT University
Bhopal (M.P.)

**Abstract- Vehicular Ad hoc Network (VANETs) face numerous issues due to the free movement of vehicles within the network. These problems include high bandwidth consumption, as vehicles often wait for responses and properly received traffic information from one another. The innovative RSML system enhances communication speed but requires additional security features to identify and shield the VANET from blackhole attacks. RSML incorporates machine learning techniques within roadside units (RSUs) to safeguard the transportation network. In the context of routing, blackhole attackers seek to disrupt normal routing functions. These attackers consistently generate high sequence numbers to participate in the routing process. The RSML method utilizes machine learning to effectively detect and mitigate black hole threats in vehicular ad hoc networks. By employing advanced algorithms, the RSML method can adapt to changing attack patterns, ensuring strong protection for vehicle communications. Establishing a route in vehicular communication is challenging because a malicious vehicle can exploit this process for its advantage. The RSML approach maintains the record of attacker malicious functioning and match the malicious functions. Therefore, it is essential to select a routing technique that guarantees secure communication. The performance of RSML is compared with existing balckhole attack, T-AODV and ANN-AODV. The performance of novel RSML scheme is better.**

**Keywords— VANET, Routing, Security, Attacker, Vehicles.**

## I. INTRODUCTION

A vehicle-to-vehicle or vehicle-to-RSU message exchange network is called a vehicular ad hoc network. Vehicular ad hoc networks are intricate wireless communication networks that include both centralized and decentralized control mechanisms to enable smooth data transfer between cars [1][12]. This intricate communication system exchanges data between devices using a specific architecture that is semi-ad hoc (some devices are fixed; some are moveable). A blackhole-like routing assault that disrupts the route connectivity from source to destination vehicles, unwanted bandwidth uses by malevolent vehicles, and network disruption are some of the issues that arise in the dynamic vehicular network scenario [3]. The main goal of this research is to use the machine learning approach of decision trees and clustering techniques to provide secure and dependable packet delivery within vehicle networks. Predictive VANET Routing Using Machine Learning In the context of VANETs, the application of machine learning techniques to route prediction has emerged as an important area of research. One such technique is the use of supervised learning model decision trees. By identifying the ideal hyperplane that divides various classes, decision trees are excellent at classifying and predicting data, which makes them ideal for identifying complex patterns in vehicle movement [4][5]. They are very useful tools for figuring out the optimal paths within VANETs because of their ability to handle large datasets and adapt to continuously changing network conditions [5]. By spotting patterns in real-time traffic data and accounting for factors like traffic, road conditions, and vehicle movement, these models offer advantages over traditional routing algorithms. Additionally, they generate more adaptable and efficient routing options.

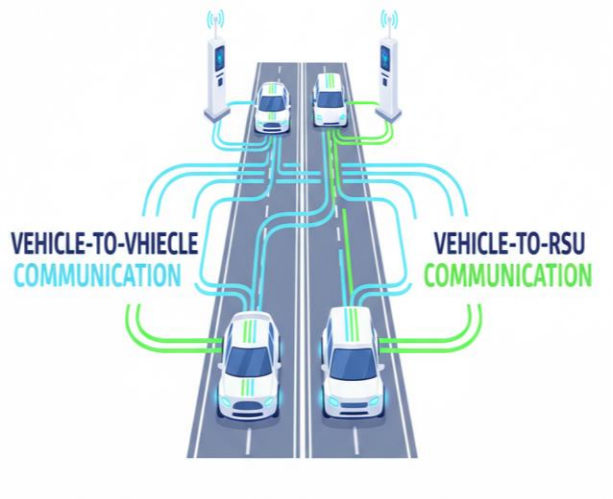


Fig.1 Example of VANET with RSUs

Moreover, using a single model is not the only advantage of machine learning-based routing prediction. The machine learning models used to predict VANET routing are shown in Figure 1. By leveraging the benefits of several models, ensemble techniques have demonstrated impressive performance in increasing prediction accuracy and generalization [6]. Hybrid models, which combine the best aspects of both methods, offer a comprehensive solution that benefits from both the flexibility of machine learning and the stability of conventional routing. Models must be able to adapt to changing conditions because vehicle environments are dynamic. In the end, safer and more efficient transportation systems will result from intelligent, context-aware decision-making made possible by machine learning techniques in VANET routing prediction.

## II. SECURITY REQUIREMENT IN VANET

In Vehicular Ad Hoc Networks (VANETs), security requirements are crucial to ensure the safe and reliable exchange of information between vehicles and infrastructure. Key requirements include authentication (verifying the identity of participating entities), confidentiality (protecting data from unauthorized access), integrity (ensuring messages are not tampered with), availability (guaranteeing timely access to network services), and non-repudiation (preventing denial of message transmission or receipt) [7][8]. Meeting these requirements helps prevent malicious attacks, ensures trust among users, and maintains the overall safety of vehicular communication systems.

**1. Authentication**

ensures that only legitimate vehicles and infrastructure components can participate in the network. When a vehicle sends a safety alert (e.g., about a road hazard), authentication verifies that the alert really came from a trusted vehicle and not from a malicious attacker pretending to be one.

**2. Confidentiality**

Confidentiality protects sensitive information from being accessed by unauthorized parties. If a vehicle's location and route information are sent to a traffic management center, confidentiality ensures only the intended receiver can read this data, preventing eavesdroppers from tracking the vehicle's movements.

**3. Integrity**

Integrity guarantees that the data exchanged is not altered or tampered with during transmission. If a vehicle broadcasts a message about a traffic jam, integrity mechanisms (like digital signatures) ensure the message isn't changed by an attacker to create false information or confusion.

**4. Availability**

Availability ensures that VANET services for traffic security and communication channels are accessible when needed, without undue delay or interruption. During an accident, vehicles must promptly send emergency messages to nearby cars. Availability ensures the network isn't disrupted by denial-of-service attacks or technical failures.

**5. Non-Repudiation**

Non-repudiation ensures that a sender cannot deny sending a message, and a receiver cannot deny receiving it.

If a vehicle reports a violation or accident, non-repudiation mechanisms (such as digitally signed records) prevent the sender from later claiming, "I never sent that message," and provide evidence if needed for legal or insurance purposes.

## III. LITERATURE SURVEY

In this section mentioned the literature survey part of research and in this section mentioned the drawbacks of each research.

Mahmood ul Hassan et al. [9], poposed an ANN-Based Intelligent Secure Routing Protocol in Vehicular Ad Hoc Networks. Concerns regarding hostile nodes, which usually result in packet loss as a result of their security operations, were addressed by employing a technique that was based on artificial neural networks (ANN). One component of this solution was the utilization of a modified AODV routing protocol for the purpose of forecasting and selecting optimal paths. They implemented an intelligent cluster-based routing strategy in order to enhance the effectiveness of the network routing process.

Mohamed Elhoseny and K. Shankar [10], proposed a Energy Efficient Optimal Routing for Communication in VANETs via Clustering Model. The purpose of clustering the vehicle nodes, this study makes use of the K-Medoid Clustering model. In order to guarantee convincing communication, the subsequent step involves locating nodes that are efficient with energy. For the purpose of achieving energy-efficient communication, we employ a metaheuristic algorithm such as the Enhanced Dragonfly Algorithm (EDA) to determine which nodes within each cluster are efficient.

Youcef Azzoug et al. [11] proposed an Improved junction-based routing for VANETs using a Bio-inspired route stability approach. In this approach, they offer warm-inspired optimization, which is a one-of-a-kind method for reducing the number of lost data packets based on a new route stability concept. An algorithm known as Intelligent Water Drops (IWD), which is a bio-inspired meta-heuristic technique, is utilized by them in order to monitor the consistency of road segment routing in both a reactive and proactive manner. Through the collection of trustworthy and up-to-date connection information for inaccessible road lengths, the objective of IWD is to gradually evaluate the level of stability that these road stretches possess. In the latter case, the calculation is carried out by making use of specified routing factors, which include the history of route traffic, data forwarding, and vehicle speed.

Hamideh Fatemidokht et al. [12] proposed an efficient clustering algorithm based on quality of service and monitoring of malicious vehicles in vehicular ad hoc networks. Through the use of this protocol, a dependable and stable cluster is specified, which in turn increases both stability and connectivity during communications. The three components that make up this protocol are as follows: (1) computing the quality of service (QoS) of vehicles and selecting a more reliable vehicle to serve as the cluster head; (2) selecting a set of appropriate neighboring nodes to serve as gateways for retransmitting packets; and (3) utilizing the gateway recovery algorithm to select an alternative gateway in the event that the link fails.

Gurjot Kaur et al. [13] proposed an article titled "Hybrid optimization enabled trust-based secure routing with deep learning-based attack detection in VANET" was written by Within the scope of this research, they present a hybrid optimization-based Deep Maxout Network (DMN) for the purpose of attack categorization within VANET. To select and route Cluster Heads (CHs), a hybrid optimization strategy is utilized as the method of choice. The method of feature selection is of utmost significance for the successful completion of the classification process. Additionally, DMN is utilized for the purpose of classifying attacks, which are taught using a training approach for optimization.

Thanh Nguyen Canh et al. [14] proposed a Machine Learning-Based Malicious Vehicle Detection for Security Threats and Attacks in Vehicle Ad-hoc Network. A thorough investigation into the application of machine learning to the detection of black holes in VANET is presented in this research. The discriminating features that were proposed (source address, destination address, source port, and destination port) were successful in detecting blackhole assaults at an early stage. The research analyzed and compared a number of different machine learning algorithms, including gradient

boosting, random forest, support vector machines, k-nearest neighbors, Gaussian Naive Bayes, and logistic regression, with the goal of identifying both appropriate and inappropriate nodes.

Fuad A. Ghaleb et al. [15] proposed an ensemble-Based Hybrid Context-Aware Misbehavior Detection Model for Vehicular Ad Hoc Network. Specifically, they present an ensemble hybrid context-aware misbehavior detection model in this paper. By combining a large number of random and uncorrelated classifiers inside a population with a number of independent classifiers, EHCA-MDS is able to harness the power of variety and the wisdom of the crowd. In order to recognize the numerous sorts of misbehaving automobiles that communicate erroneous mobility information, these classifiers collaborate with one another. In order to generate the classifier crowds, they utilized both supervised and unsupervised instructional methods. The robust statistical outlier classifiers were given live updates in order to identify any new dangers that may have emerged. A large number of intelligent classifiers were trained using the random forest method in order to make predictions about the automobiles' class based on the pattern that was seen. In conjunction with one another, the hybrid and multidimensional statistical classifiers provided by the model have the potential to identify complicated assaults that the single-classifier technique is unable to correctly recognize.

G. Soni et al [16], proposed a novel privacy-preserving under denser traffic management (PPDM) routing strategy for the 6G-VANET to protect it against malicious black hole attacks in VANET. All key information from traffic status packets supplied by leading cars to the following vehicles is discarded by black hole vehicles. A security system detects and prevents packet drops on a connection through a node. The blachhole attacker presence interrupt the normal routing performance but with the help of 6G network the fast communication is possible that improves routing performance.

Srihari Kannan et al. [17] Ubiquitous Vehicular Ad-Hoc Network Computing Using Deep Neural Network with Internet of Things-Based Bat Agents for Traffic Management. Through the utilization of deep neural networks (DNN) and bat algorithms (BA), this paper presents a dynamic method of traffic control that can be implemented in vehicular ad hoc networks (VANETs). via the utilization of the former, they are able to maximize efficiency by directing cars via congested routes, which ultimately results in a decreased average latency. They integrate the Internet of Things (IoT) with the latter, moving it across VANETs in order to evaluate the current state of traffic congestion between network nodes.

Abdul Karim Kazi et al. [18] proposed an Effective Routing Protocol for VANET in Urban Scenarios. In this work, they describe a novel routing protocol called Dynamic Trilateral Enrollment (DyTE) with the goal of increasing throughput and achieving a higher Packet Delivery Ratio (PDR). A dynamic trilateral zone is chosen by this protocol in order to locate the vehicle that is the destination. This is accomplished by allowing only relevant nodes to take part in the communication process. The location coordinates of the source and destination nodes are used to make this determination.

## IV. PROPOSED MACHINE LEARNING BASED APPROACH

In Vehicular Ad Hoc Networks (VANETs), blackhole attackers pose a significant threat by maliciously dropping packets and disrupting network communication. Leveraging machine learning techniques provides a proactive approach to enhance security against such attacks. By analyzing network behavior and extracting key features—such as abnormal packet dropping patterns and irregular route reply messages—machine learning models can accurately distinguish between normal and malicious activities. These models can be trained on a variety of simulated or real-world data to detect blackhole attacks in real time, enabling swift countermeasures like isolating compromised nodes. As a result, incorporating machine learning into VANET security frameworks greatly improves the network's resilience, reliability, and overall safety for intelligent transportation systems.

**1. Data Collection**
Gather network traffic data from VANET simulations or real-world deployments.
Ensure the dataset contains both normal and attack scenarios (including blackhole attacks).

**2. Data Preprocessing**
Cleanse the data (handle missing values, remove noise).

Extract relevant features (e.g., packet drop rate, sequence number changes, routing behaviour).

- Packet forwarding ratio (forwarded/received packets)
- Number of dropped packets by each node
- Abnormal route replies (e.g., nodes claiming shortest routes too frequently)
- Sequence number gaps
- Response time to route requests

**Feature Selection/Engineering**

- Select the most indicative features for blackhole attacks.
- Apply dimensionality reduction techniques based on the simulation information stored in trace file.

**3. Labeling**
Manually or automatically label data as 'normal' or 'blackhole attack'.

**Model Selection**
Choose suitable machine learning algorithms with is based on the attacker symptoms detection like packets dropping.

**Model Training**
Split data into training and testing sets. And Train the model using the simulation data.

**Model Evaluation**
Evaluate performance using metrics like throughput, data receiving and overhead

**Detection/Deployment**

- Implement the security for black hole attacker in the VANET environment.
- Monitor simulation network traffic and classify it as normal or under attack.

**Continuous Update**

- Periodically retrain the model with new data to adapt to evolving attack strategies.

**4. Common Features Used for attacker detection are:**

- Packet forwarding ratio
- Route request/response patterns
- Number of dropped packets
- Node sequence number changes
- Response time to route requests

## V. RESULT ANALYSIS

In this section mentioned the performance analysis of previous T-AODV, presence of blackhole attack, ANN-AODV and novel RSML. The performance of proposed scheme is better as compare to other.

**1. Data Receiving Percentage Performance Analysis**
The table presents a Min–Max–Range analysis of data receiving percentage for different routing protocols under varying network sizes. The minimum and maximum values indicate the lowest and highest data reception achieved, while the range reflects the variation in performance.

Among the protocols, RSML demonstrates the most stable and reliable performance, as it has the highest minimum value and the smallest range (3.71), indicating consistent data delivery across all scenarios. ANN-AODV also shows strong performance with relatively high values and moderate variation. In contrast, T-AODV exhibits a larger range (16.12), suggesting greater fluctuation in performance. The Blackhole protocol records the lowest minimum value and significant variation, highlighting its vulnerability and poor performance under attack conditions. Overall, protocols with smaller ranges and higher minimum values are more efficient and consistent in data transmission.

Table 1. Data Receiving Percentage Analysis

| Protocol Type | Receive Performance | | |
|---|---|---|---|
| | Min | Max | Range |
| Vampire | 39.99 | 50.94 | 10.95 |
| TAODV | 44.29 | 60.41 | 16.12 |
| SAODV | 64.16 | 77.71 | 13.55 |
| HAPV | 79.14 | 82.85 | 3.71 |

**2. Throughput Performance Analysis**

The table 2 presents a throughput performance analysis of four routing protocols—Vampire, TAODV, SAODV, and HAPV—using minimum, maximum, and range values. Among the protocols, HAPV achieves the highest throughput values (min = 10.15, max = 11.66), indicating superior data transmission efficiency, while maintaining a relatively small range (1.51), which reflects stable performance. SAODV also demonstrates strong and consistent performance with a low range of 1.24. In contrast, TAODV shows a larger range (3.04), indicating greater variability and less consistency in throughput. The Vampire protocol records the lowest throughput values overall, highlighting its poor performance. Overall, protocols with higher minimum values and smaller ranges, such as HAPV and SAODV, provide better and more reliable throughput performance.

Table 2. Throughput Performance Analysis

| Protocol Type | Throughput Performance | | |
|---|---|---|---|
| | Min | Max | Range |
| Vampire | 3 | 4.78 | 1.78 |
| TAODV | 3.85 | 6.89 | 3.04 |
| SAODV | 8.5 | 9.74 | 1.24 |
| HAPV | 10.15 | 11.66 | 1.51 |

**3. Data forwarding Analysis**

The table 3 presents a Min–Max–Range analysis of the forwarding ratio for different routing protocols. RSML achieves the highest forwarding ratio, with values ranging from 0.81 to 0.91, indicating superior packet delivery efficiency, while maintaining a moderate range (0.10) that reflects consistent performance. ANN-AODV also performs well, with values between 0.61 and 0.71 and a similar range (0.10), showing stable behaviour. T-AODV demonstrates moderate performance but with a higher range (0.12), indicating greater variability in packet forwarding. In contrast, the Blackhole protocol has the lowest forwarding ratio, ranging from 0.25 to 0.30, which highlights its poor performance under attack conditions despite having the smallest range (0.05). Overall, protocols with higher minimum values and controlled ranges, such as RSML and ANN-AODV, provide more reliable and efficient forwarding performance.

Table 3 Forwarding Ratio Analysis

| Protocol Type | Forwarding Performance | | |
|---|---|---|---|
| | Min | Max | Range |
| Vampire | 0.25 | 0.3 | 0.05 |
| TAODV | 0.51 | 0.63 | 0.12 |
| SAODV | 0.61 | 0.71 | 0.1 |
| HAPV | 0.81 | 0.91 | 0.1 |

## VII. CONCLUSION

In a Vehicular Ad Hoc Network (VANET), vehicles exchange traffic status information with one another to help prevent congestion. The process of forming routes in vehicular communication is essential, as a malicious node can divert the path or disrupt the network for personal gain during this stage. Therefore, it is crucial to select an appropriate routing method that ensures secure communication. This research introduces an RSML approach designed to secure traffic information that may be compromised due to blackhole attacks in VANET. While this proposed method facilitates the fastest communication route, it requires enhancements through a security mechanism capable of detecting and preventing blackhole attacks within the VANET. A vehicle obtains the communication channel from the roadside unit (RSU) when it tries to communicate with another vehicle. Machine learning (ML) is an algorithmic framework employed to analyse large volumes of traffic data to identify patterns and support decision-making or forecasting. This proactive strategy not only enhances security but also improves overall network efficiency, leading to

safer and more reliable vehicular interactions. The novel methods provide more secure communication between nodes while ensuring effective communication with minimal overhead. These strategies enhance resource allocation and offer a more dependable and resilient network infrastructure. Ultimately, the implementation of these sophisticated routing algorithms facilitates scalable and sustainable network solutions across many applications. The network simulator-2 simulates our proposed methodology and examines the network's performance during communication.

## REFERENCES


1. Arun Singh Kaurav and Sushama Rani, “Detection and prevention from different attacks in VANET: A Survey,” Journal of Physics: Conference Series, International Conference on Physics and Energy 2021 (ICPAE 2021), Vol. 40. March 2021.
2. G. Soni, K. Chandravanshi, N. Kunhare, M. Bhargava, “Data Receiving Analysis for Secure Routing from Blackhole Attack in a Spontaneous Network Using Blockchain Method, Proceedings of International Conference on Network Security and Blockchain Technology. ICNSBT 2023, Lecture Notes in Networks and Systems, vol 738, pp. 513-524, 2024.
3. G. Soni, K. Chandravanshi, M.K. Jhariya, R. Rajput, “An IPS Approach to Secure V-RSU Communication from Blackhole and Wormhole Attacks in VANET”, Contemporary Issues in Communication, Cloud and Big Data Analytics. Lecture Notes in Networks and Systems, vol 281, pp. 67-65, 2022.
4. T. N. Canh and X. HoangVan, "Machine Learning-Based Malicious Vehicle Detection for Security Threats and Attacks in Vehicle Ad-Hoc Network (VANET) Communications," 2023 RIVF International Conference on Computing and Communication Technologies (RIVF), pp. 206-211, 2023.
5. J. N and R. Patil, "Enhanced Machine Learning Based Techniques for Security in Vehicular Ad-Hoc Networks," 2023 International Conference on Advancement in Computation & Computer Technologies (InCACCT), pp. 386-393, 2023.
6. K. Chandravanshi, G. Soni, J. Ahmed, C. Gautam and K. Khan, "Machine Learning Technique for Mobility and Signal Strength-Based Route Selection in MANET," First International Conference on Software, Systems and Information Technology (SSITCON), Tumkur, India, pp. 1-7, 2024.
7. Mamata Rath, Bibudhendu Pati, Binod Kumar Pattanayak, “An Overview on Social Networking: Design, Issues, Emerging Trends, and Security,” Social Network Analytics Computational Research Methods and Techniques, pp. 21-47, 2019.
8. Thanmayee Karimireddy, Ahmad Ghulam A Bakshi, "A Hybrid Security Framework for the Vehicular Communications in VANET", IEEE WiSPNET Conference, 2016.
9. M. ul Hassan, A. A. Al-Awady, A. Ali, M. Sifat Ullah Akram, M, M.M. Iqbal, J. Khan, Y.N. Abdelrahman Ali. “ANN-Based Intelligent Secure Routing Protocol in Vehicular Ad Hoc Networks (VANETs) Using Enhanced AODV. Sensors, Vol. 24, 2024.
10. Elhoseny, Mohamed & Shankar, Kripa, “Energy Efficient Optimal Routing for Communication in VANETs via Clustering Model,” 2020.
11. Youcef Azzoug, Abdelmadjid Boukra, Improved junction-based routing for VANETs using a Bio-inspired route stability approach,Ad Hoc Networks, Vol. 53,2024.
12. Hamideh Fatemidokht, Marjan Kuchaki Rafsanjani, QMM-VANET: An efficient clustering algorithm based on QoS and monitoring of malicious vehicles in vehicular ad hoc networks, Journal of Systems and Software, Vol.165, 2020.
13. Gurjot Kaur, Deepti Kakkar, Hybrid optimization enabled trust-based secure routing with deep learning-based attack detection in VANET, Ad Hoc Networks, Volume 136, 2022.
14. Thanh Nguyen Canh, Xiem HoangVan “Machine Learning-Based Malicious Vehicle Detection for Security Threats and Attacks in Vehicle Ad-hoc Network (VANET) Communications”, RIVF International Conference on Computing and Communication Technologies, Hanoi, Vietnam, 2023,
15. F.A. Ghaleb, M.A. Maarof, A. Zainal, B.A.S Al-rimy, A. Alsaeedi, W. Boulila, “Ensemble-Based Hybrid

Context-Aware Misbehavior Detection Model for Vehicular Ad Hoc Network," Remote Sensing, Vol.11. 2019.

16. G. Soni, K. Chandravanshi, "A Novel Privacy-Preserving and Denser Traffic Management System in 6G-VANET Routing Against Black Hole Attack." Sustainable Communication Networks and Application. Lecture Notes on Data Engineering and Communications Technologies, vol 93, pp. 649-663, 2022.
17. K. Srihari, G. Dhiman, Y. Natarajan, A. Sharma, Ashutosh S. Mohanty, M. Soni, U. Easwaran, H. Ghorbani, A. Asheralieva, M. Gheisari, "Ubiquitous Vehicular Ad-Hoc Network Computing Using Deep Neural Network with IoT-Based Bat Agents for Traffic Management. Electronics", Vol. 10(7), 2021.
18. A. K. Kazi and S. M. Khan, "DyTE: An Effective Routing Protocol for VANET in Urban Scenarios", Eng. Technol. Appl. Sci. Res., vol. 11, no. 2, pp. 6979–6985, Apr. 2021.
19. Sindhwani, M.; Sachdeva, S.; Gupta, A.; Tanwar, S.; Alqahtani, F.; Tolba, A.; Raboaca, M.S. A Novel Context-Aware Reliable Routing Protocol and SVM Implementation in Vehicular Area Networks. Mathematics ,Vol. 11. 2023, 11,