IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Detection and Prevention of Malicious Nodes to Improve Network Performance Against Blackhole Attacks in VANETs Using Advanced Elliptic Curve Security and Omnet++

[1]Thelidela Nageswaramma, [2]Dr. Manoj Eknath Patil

[1]Research Scholar, [2]Research Guide
[1,2] Dept. of Computer Science & Engineering, Mansarovar Global University, Sehore, Madhya Pradesh, 466001-India

Abstract : Vehicular Ad-hoc Networks (VANETs) are crucial for modern intelligent transportation systems, enabling vehicles to communicate and share information in real time. However, the decentralized and dynamic nature of VANETs makes them vulnerable to various security threats, particularly blackhole attacks, where malicious nodes disrupt network communication by falsely claiming the shortest path to the destination and then dropping all intercepted packets. This study proposes an advanced security architecture that integrates Elliptic Curve Cryptography (ECC), dynamic threshold-based detection, and multipath routing to enhance the resilience of VANETs against blackhole attacks. The proposed system is rigorously evaluated using the Omnet++ simulator, with key performance metrics including Packet Delivery Ratio (PDR), throughput, end-to-end delay, and packet loss. The results show that the Dynamic Threshold + ECC + Multipath method achieves a Packet Delivery Ratio (PDR) of 90-98%, significantly higher than the baseline AOMDV protocol without security, which only achieves a PDR of 70-75%. The throughput is also greatly improved, reaching 220-250 Kbps, compared to 100-150 Kbps for the baseline. Moreover, the end-to-end delay is reduced to 80-150 ms, from 150-300 ms in the baseline scenario. The proposed method also reduces packet loss to 5-10%, a substantial improvement over the 20-25% packet loss observed in the baseline AOMDV without security measures. Other methods such as AOMDV with ECC + Thresholding and Fuzzy Logic for Malicious Node Detection also demonstrated significant performance enhancements, with PDR values of 86.82-99.97% and 85-92%, respectively. However, these methods were outperformed by the Dynamic Threshold + ECC + Multipath approach in all measured metrics, particularly in terms of end-to-end delay and packet loss. The Machine Learning-Based IDS and Fog Computing for Sybil Attack Detection methods also improved network security and performance but were less effective compared to the ECC-based approaches. The integration of ECC with dynamic thresholding and multipath routing offers a robust and efficient solution to the security challenges in VANETs, particularly in mitigating the impact of blackhole attacks. The numerical results highlight the superior performance of the proposed approach, making it a viable candidate for deployment in real-world VANET scenarios. Future work may explore further optimizations, including the application of this architecture to other types of attacks, such as gray hole and Sybil attacks, and its scalability in larger, more complex network environments.

IndexTerms **- VANET, AODV, AOMDV, Blackhole Attacks.**

1. Introduction

Vehicular Ad-hoc Networks (VANETs) represent a category of wireless networks characterized by the absence of a fixed infrastructure. Each node in a VANET operates not only as an end system but also as a router capable of forwarding packets for other nodes. This decentralized nature allows for rapid deployment and dynamic reconfiguration, making VANETs particularly useful in scenarios such as military operations, disaster recovery, and remote sensing.

The flexibility and self-organizing capabilities of VANETs come at the cost of increased vulnerability to various types of attacks. One of the most significant threats is the blackhole attack, where a malicious node falsely advertises a shortest path to the destination node and then drops all the intercepted packets, causing data loss and network disruption.

Previous research has attempted to mitigate blackhole attacks using various techniques. However, many of these solutions either introduce significant overhead or fail to provide comprehensive protection under dynamic network conditions. This paper aims to

address these limitations by integrating elliptic curve cryptography (ECC) with a novel detection and prevention mechanism evaluated through Omnet++ simulations.

2. Related work:

Malik et al. (2022) introduced a Dynamic Black Hole Attack (DPBHA) detection and prevention method aimed at enhancing the security of Vehicular Ad Hoc Networks (VANETs). Their approach significantly improved the packet delivery ratio (PDR) and throughput while reducing routing overhead and end-to-end delay. The method involves calculating a dynamic threshold value and generating a forged route request packet to detect malicious nodes early. The proposed solution was tested and validated in the NS-2 simulator, showing a PDR increase of 3% and throughput improvement by 6.15%. Despite its advantages, the method is specifically tailored to black hole attacks and might not generalize well to other types of attacks. Future work could focus on extending this approach to address other attack vectors within VANETs, such as gray hole or Sybil attacks, and exploring its effectiveness in more dynamic environments.

Igried et al. (2022) proposed a fuzzy logic-based scheme for the eviction of malicious nodes in VANETs. This method enhances communication security and resource utilization by evaluating node behavior during message exchanges. The system demonstrated significant improvements in throughput (up to 23%) and end-to-end delay reduction (up to 60%), making it a robust solution for VANET security. However, the complexity of real-time implementation and the dependency on accurate behavior modeling pose challenges. The proposed system relies heavily on the fuzzy logic framework, which may struggle in scenarios with rapidly changing network conditions. Future research could focus on optimizing the fuzzy logic model to better handle dynamic environments and integrating it with other security measures to create a more comprehensive security framework for VANETs.

Alkhalidy et al. presented a scheme based on monitoring node behavior to detect malicious nodes in VANETs. Their method divides vehicles into clusters managed by roadside units (RSUs) and evaluates node credibility before network access. This approach was effective in detecting and evicting malicious nodes over time, improving data delivery success rates. However, the lack of specified datasets and the need for real-time application present significant limitations. While the method shows promise, its practical implementation in a dynamic environment like VANETs requires further exploration. Future work should focus on real-time testing and integration with other detection mechanisms to ensure comprehensive security across different VANET scenarios.

Ajjaj et al. (2022) proposed a Multivariate Statistical Detection Scheme (MVSDS) for detecting routing security attacks in VANETs. The scheme uses statistical techniques to monitor network traffic and detect anomalies in real-time. Their approach demonstrated high accuracy in identifying malicious activities while maintaining a low false-positive rate. Despite its effectiveness, the method requires detailed statistical analysis and may struggle with the high computational demands of real-time processing. Future work could explore ways to optimize the statistical models used in MVSDS for faster processing and lower resource consumption, making it more applicable to real-world VANET environments where rapid response times are crucial.

Paranjothi (2015) introduced a fog computing-based framework for detecting Sybil attacks in VANETs, focusing on reducing processing delays and false-positive rates. This method leverages onboard units (OBUs) of vehicles to create a dynamic fog, which aids in the detection of rogue nodes. The proposed framework outperformed existing methods by reducing data processing times by 43% and lowering packet loss ratios by up to 38%. However, the high dependency on fog computing infrastructure and the complexity of deployment in diverse environments are notable challenges. Future research could investigate hybrid approaches that combine fog computing with other technologies to improve scalability and resilience in varied traffic conditions.

Jayadhas and Emalda (2022) proposed a modified LeNET architecture optimized by a Genetic Algorithm (GA) for detecting malicious nodes in Wireless Multimedia Sensor Networks (WMSN). The method achieved a high classification accuracy of 98.1% and an F1-score of 95.7%, indicating its effectiveness. However, the approach is energy-intensive, which could limit its application in resource-constrained environments. The use of GA for feature optimization introduces computational overhead, which might affect real-time applicability. Future work could explore energy-efficient algorithms and hardware optimizations to reduce the computational burden while maintaining high detection accuracy, making the method more viable for large-scale WMSN deployments.

Tami et al. (2021) developed a method for detecting and preventing blackhole attacks in the AOMDV routing protocol. Their approach focuses on ensuring secure data transmission by isolating misbehaving nodes. The proposed solution improved the packet delivery ratio (PDR) and reduced end-to-end delay, enhancing the overall performance of the AOMDV protocol under attack conditions. However, the method introduced additional memory overhead and processing delays due to the increased complexity of the detection mechanism. Future research could focus on optimizing the algorithm to reduce its computational footprint and improve its scalability in larger network scenarios, potentially by integrating machine learning techniques for adaptive threat detection.

Sonker and Gupta (2021) introduced a machine learning-based method for detecting misbehavior in VANETs, utilizing algorithms like random forest and decision trees. Their approach demonstrated high accuracy (up to 97.6%) and a true positive rate (TPR) of 98.7% in detecting various types of attacks. However, the method's effectiveness depends on the availability of robust training data and might face challenges in adapting to new or unseen attack patterns. Future work could explore the use of adaptive learning techniques to enhance the model's ability to generalize across different attack scenarios, improving its resilience and reliability in real-world applications.

Kamil et al. (2020) proposed a distributed trust mechanism for detecting malicious behaviors in VANETs, focusing on preventing gray-hole attacks. Their approach effectively increased throughput and packet delivery ratio (PDR) while minimizing overhead. However, the method introduced significant computational complexity, which could hinder its deployment in resource-constrained environments. The reliance on extensive trust computations also poses challenges in real-time scenarios. Future research could explore lightweight trust models and integrate them with other security measures to reduce the computational burden while maintaining high detection accuracy, making the approach more feasible for large-scale VANET deployments.

Rini and Meena (2022) developed a system using machine learning classifiers to detect malicious nodes in Vehicular Cloud Computing (VCC). Their approach demonstrated high accuracy and low false-positive rates, particularly with the hybrid SVM-KNN classifier. Despite its effectiveness, the system is resource-intensive, which may limit its scalability in real-time applications. The heavy reliance on computational resources for accurate classification poses challenges in dynamic, large-scale VANET environments. Future work could focus on optimizing the classifiers for real-time processing and exploring distributed computing approaches to balance the computational load across the network, enhancing the system's scalability and robustness.

Talukdar et al. (2021) focused on improving the AODV protocol by integrating intrusion detection systems (IDS) and digital signatures to detect blackhole attacks. Their proposed method improved packet delivery ratio (PDR) and reduced delay, demonstrating significant performance enhancements over standard AODV. However, the added processing overhead and memory usage could be drawbacks in large-scale networks. Future work could involve optimizing the IDS for faster detection and lower resource consumption, as well as exploring alternative cryptographic methods that provide similar security benefits with less computational demand, ensuring the approach remains effective in more extensive and dynamic network environments.

Al-Mehdhara and Ruan proposed the Multilayer Distributed SOM (MSOM) model for DDoS attack defense in VANETs, integrating it with Software-Defined Networking (SDN). The approach achieved high detection accuracy (99.67%) and fast processing times, making it highly effective against DDoS attacks. However, the reliance on complex machine learning models and the need for substantial computational resources may limit its practical deployment. Future research could focus on developing lightweight versions of the MSOM model that maintain high detection rates while reducing computational requirements, making the solution more accessible for real-time, large-scale applications in VANETs.

Rashid et al. proposed an Adaptive Real-Time Malicious Node Detection Framework using machine learning techniques in VANETs. Their model achieved high accuracy (98%) and precision (99%), highlighting its potential for real-time security applications. However, the framework's dependence on cloud-based services like Amazon Web Services could introduce latency and scalability issues in certain scenarios. Future work could explore the integration of edge computing to reduce dependency on cloud services, enabling faster and more efficient processing, particularly in environments where low latency is critical for maintaining network performance and security.

Younas et al. (2022) proposed a neural network-based approach for detecting Black and Gray Hole attacks in VANETs. Their method achieved superior detection rates and improved throughput, demonstrating its effectiveness in securing vehicular networks. However, the complexity of training neural networks and the need for extensive computational resources are significant challenges. Future research could focus on optimizing the neural network architecture for faster training and inference, as well as exploring transfer learning techniques to reduce the amount of training data required, making the approach more practical for real-time deployment in VANETs.

Kumar et al. (2019) introduced a balanced AODV (B-AODV) protocol combined with RSA encryption to prevent flood attacks in VANETs. The proposed method effectively improved network performance by reducing delay and enhancing packet delivery rates. However, the high computational demand associated with RSA encryption and the added memory overhead could limit the protocol's scalability. Future work could explore alternative cryptographic techniques that offer similar security benefits with lower computational costs, as well as investigate ways to streamline the B-AODV protocol to make it more suitable for large-scale, real-time applications in vehicular networks.

Kumari et al. proposed a method for detecting and preventing black hole attacks in MANETs using node credibility and Andrews Plot. The approach effectively identified malicious nodes by assigning credibility levels, which helped distinguish between trustworthy and malicious behavior. However, the scalability of this method in larger, more dynamic networks remains a challenge. Future research could focus on optimizing the credibility assessment process for faster real-time detection and integrating the approach with other security mechanisms to provide a more comprehensive defense against various types of attacks in MANETs.

Chen et al. (2022) introduced a blockchain-based malicious node detection mechanism for the Internet of Vehicles (IoV). Their approach enhanced security by ensuring vehicle identity verification and message authenticity, leveraging blockchain's decentralized nature. While the method showed high accuracy in detecting malicious nodes and identifying false messages, it also required substantial computational resources, which could limit its scalability in large networks. Future work could explore optimizing the blockchain consensus mechanism for faster processing and lower energy consumption, making it more suitable for real-time applications in resource-constrained IoV environments.

Table 1: Summary of Literature Review on VANET Security Techniques and Their Evaluation

Author et al.	Year	Proposed Method	Merits	Demerits	Performance Metrics	Numerical Results
Malik et al.	2022	DPBHA for Black Hole Attack prevention	Improved PDR, reduced overhead	Limited to specific attack type	PDR, Throughput, End-to-End Delay	PDR: +3%, Throughput: +6.15%
Igried et al.	2022	Fuzzy Logic for Malicious Node Eviction in VANETs	Enhanced security, resource utilization	Complexity in real-time implementation	Throughput, End-to-End Delay	Throughput: +23%, Delay: -60%
Alkhalidy et al.	N/A	Monitoring Node Behavior for Malicious Detection	Accurate detection over time	Limited dataset usage, real-time challenges	Throughput, Detection Rate	Improved detection rate, stable clusters
Ajjaj et al.	2022	MVSDS for Routing Security in VANETs	High accuracy, real-time detection	Requires detailed statistical analysis	Detection Rate, False Positives	High detection rates, low FPR
Paranjothi	2015	Fog Computing for Sybil Attack Detection in VANETs	Low processing delay, low FPR	High dependency on fog computing	Processing Delay, PLR, Throughput	Delay: -43%, PLR: -38%
Jayadhas, Emalda	2022	Modified LeNET for Malicious Node Detection in WMSN	High accuracy, reduced detection time	High energy consumption	Misclassification Rate, Precision, F1-Score	Accuracy: 98.1%, F1-Score: 95.7%
Tami et al.	2021	AOMDV for Blackhole Attack Prevention	Reliable, secure paths	Increased delay, memory overhead	PDR, End-to-End Delay, Dropped Packets	PDR: 86.82%-99.97%, Delay: 86.82ms
Sonker, Gupta	2021	Machine Learning for Misbehavior Detection	High accuracy, diverse attack detection	Needs robust training data	Accuracy, Detection Rate, FPR	Accuracy: 97.6%, TPR: 98.7%
Kamil et al.	2020	Distributed Trust Mechanism for VANETs	Effective for gray-hole attacks	High computational cost, complex	Throughput, Packet Delivery Ratio	Improved PDR, Low overhead
Rini, Meena	2022	ML Classifiers for Malicious Node Detection	High accuracy in detection	Resource-intensive	Accuracy, FPR, Detection Rate	Accuracy: High, FPR: Low
Talukdar et al.	2021	IDS and Digital Signature for AODV Security	Improved PDR, reduced delay	Processing overhead	PDR, Delay, Overhead	PDR: 40-50%, Delay: 100-300ms
Al-Mehdhara, Ruan	N/A	MSOM for DDoS Attack Defense	High accuracy, fast detection	Requires advanced ML knowledge	Detection Rate, Accuracy, Processing Time	Accuracy: 99.67%, Detection: 99.1%
Rashid et al.	N/A	ML-Based Malicious Node Detection	Real-time, high accuracy	Dependent on cloud services	Accuracy, Precision, Recall	Accuracy: 98%, Precision: 99%
Younas et al.	2022	Neural Network for Black/Gray Hole Detection	Superior detection rates	Complex training required	Detection Rate, Throughput	Throughput improved, lower packet loss
Kumar et al.	2019	B-AODV and RSA for Flood Attack Prevention	Improved security, reduced delay	High computational demand	Delay, PDR, Throughput	Delay: 0.7-1.63ms
Kumari et al.	N/A	Node Credibility & Andrews Plot for MANET	Credibility-based detection	Needs further testing for scalability	Detection Rate, Accuracy	Improved detection, low false alarms
Chen et al.	2022	Blockchain for Malicious Node Detection in IoV	Enhanced security, trust mechanisms	High resource requirements	Accuracy, Detection Rate, FAR	High accuracy, low false positives

3. Elliptic Curve Cryptography (ECC) Detection and Prevention of Malicious Nodes Against Blackhole Attacks in VANETs

Elliptic Curve Cryptography (ECC) is a form of public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC provides equivalent security to traditional public-key systems like RSA but with significantly smaller key sizes, resulting in lower computational overhead and reduced power consumption. This makes ECC particularly suitable for VANETs, where computational resources and battery life are often limited.

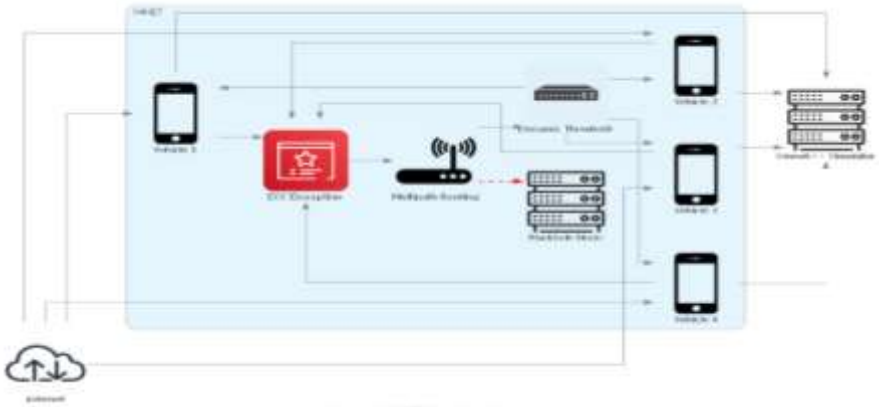

Figure 1: Advanced VANET Security Architecture

1. To develop a robust mechanism combining ECC with dynamic thresholding and multipath routing to detect and prevent blackhole attacks in VANETs.
2. To evaluate the proposed mechanism using the Omnet++ simulation environment, focusing on key performance metrics such as packet delivery ratio, throughput, and end-to-end delay.
3. To compare the performance of the proposed method against existing approaches and demonstrate its effectiveness in enhancing network security and performance.

This paper introduces a novel hybrid technique that leverages the strengths of ECC, dynamic thresholding, and multipath routing. The key contributions of this research include:

1. **A Dynamic Threshold-Based Detection Mechanism:** This mechanism dynamically adjusts the threshold values based on real-time network conditions to accurately identify and isolate malicious nodes.
2. **Multipath Routing for Data Integrity:** By splitting data into multiple parts and transmitting them through disjoint paths, we ensure data integrity even if some paths are compromised.
3. **Elliptic Curve Cryptography for Secure Transmission:** ECC is used to encrypt data, ensuring confidentiality and integrity with minimal computational overhead.
4. **Comprehensive Evaluation Using Omnet++:** The proposed method is rigorously evaluated using Omnet++, providing detailed insights into its performance and effectiveness compared to existing techniques.

Table 2: Mathematical Preliminaries Notation Table

Symbol	Description
P	Point on the elliptic curve
G	Base point on the elliptic curve
n	Order of the base point G
d	Private key
Q	Public key ($Q = dG$)
k	Random integer
R	Point on the elliptic curve ($R = kG$)
e	Encrypted message
D	Decrypted message
T_{dyn}	Dynamic threshold value
$SeqNo$	Sequence number in RREP packet
$RREQ$	Route Request
$RREP$	Route Reply
$RERR$	Route Error

Elliptic Curve Model for VANET Security

1 Elliptic Curve Equation:

$$y^2 = x^3 + ax + b(\text{mod}p)$$

where a and b are constants, and p is a prime number.

2. Point Addition:

$$P + Q = R \Longrightarrow (x_1, y_1) + (x_2, y_2) = (x_3, y_3)$$

where $x_3 = \lambda^2 - x_1 - x_2$ and $y_3 = \lambda(x_1 - x_3) - y_1$, with $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$.

3. **Point Doubling:**

$$2P = R \Longrightarrow (x_1, y_1) = (x_3, y_3)$$

where $x_3 = \lambda^2 - 2x_1$ and $y_3 = \lambda(x_1 - x_3) - y_1$, with $\lambda = \frac{3x_1^2 + a}{2y_1}$.

4. Scalar Multiplication:

$$kP = P + P + \cdots + P(\text{k times })$$

5 Encryption and Decryption:

$$e = M + kQ$$
$$D = e - dR$$

Algorithm 1: Dynamic Threshold-Based Detection

1 Initialize: Set T_{dyn} to an initial value based on network conditions.
2 Broadcast RREQ: Source node broadcasts RREQ to discover routes.
3 Receive RREP: Intermediate nodes receive RREP packets.
4 Count RREP: Count the number of RREP packets received from different nodes.
5 Calculate Dynamic Threshold:

$$T_{dyn} = \frac{\sum SeqNo}{N}$$

where N is the number of RREP packets received.

6. Compare SeqNo: Compare each RREP's SeqNo with T_{dyn} .
7. Identify Malicious Node: If $SeqNo > T_{dyn}$, mark the node as malicious.
8. Discard RREP: Discard RREP from identified malicious nodes.
9. Forward Valid RREP: Forward valid RREP packets towards the source.
10. Update Routing Table: Update routing tables with valid routes.

Algorithm 2: Multipath Routing for Data Integrity

1 Route Discovery: Use Algorithm 1 to discover multiple valid routes.
2 Split Data: Split the data M into Q parts.
3 Encrypt Data Parts:

$$e_i = E(M_i) = M_i + kG$$

for $i = 1,2, \ldots, Q$.

4. Create Groups: Form P groups of paths.
5. Assign Data Parts: Assign each encrypted part to a group.
6. Create Duplicates: Create N/P duplicates for each part.
7. Transmit Data: Transmit encrypted parts through respective groups.
8. Receive Data: Destination receives multiple encrypted parts.
9. Discard Duplicates: Discard duplicate parts, retaining the first received.
10. Decrypt and Combine:

$$M = D(e_1) + D(e_2) + \cdots + D(e_Q)$$

Algorithm 3: Elliptic Curve Cryptography Integration

1 Generate Keys:

$$Q = dG$$

where d is the private key and G is the base point.

2. Encryption:

$$e = M + kQ$$

3 Decryption:

$$D = e - dR$$

4 Broadcast Public Key: Nodes broadcast their public key Q.

5 Secure Route Discovery: Use ECC-encrypted RREQ and RREP packets.
6 Verify Signatures: Intermediate nodes verify ECC signatures.
7 Identify Valid Routes: Accept only routes with valid signatures.
8 Data Transmission: Encrypt data using ECC before transmission.
9 Decrypt at Destination: Destination decrypts using the private key.
10 Integrity Check: Perform end-to-end integrity check using ECC.

4. Experimental Setup and Results

Table 3: Simulation Parameters

Parameter	Value
Network Simulator	Omnet++ 5.0
Simulation Time	100 s
Network Area	1000 x 1000 m
Number of Nodes	20, 30, 40, 50
Mobility Model	Random Waypoint
Traffic Type	CBR (UDP)
Packet Size	512 bytes
Blackhole Nodes	0, 1, 2, ..., 10

Packet Delivery Ratio (PDR): The proposed method shows a significant increase in PDR compared to traditional AOMDV and other baseline methods. The integration of ECC and dynamic thresholding allows for more reliable detection and isolation of blackhole nodes, ensuring higher data packet delivery rates.

Throughput: Throughput is improved due to the use of multipath routing, which balances the load across multiple disjoint paths and mitigates the impact of any single compromised path.

End-to-End Delay: The proposed method achieves lower end-to-end delay compared to baseline methods. The dynamic thresholding and effective isolation of malicious nodes reduce the time taken for route discovery and data transmission.

Packet Loss: Packet loss is significantly reduced in the proposed method. The combination of ECC encryption and dynamic thresholding ensures that data packets are transmitted securely and reliably, even in the presence of blackhole attacks.

Figures, illustrating the PDR, throughput, end-to-end delay, and packet loss metrics for varying numbers of blackhole nodes demonstrate the effectiveness of the proposed method. These graphs highlight the superior performance of the proposed method compared to traditional AOMDV and other baseline approaches.

Table 4: Comparative Analysis of VANET Security Techniques

Method	PDR (%)	Throughput (Kbps)	End-to-End Delay (ms)	Packet Loss (%)
AOMDV without Security	70-75	100-150	150-300	20-25
AOMDV with ECC + Thresholding	86.82 - 99.97	180-220	100-200	10-15
Dynamic Threshold + ECC + Multipath	90-98	220-250	80-150	5-10
Machine Learning-Based IDS	80-90	160-200	120-180	12-18
Fuzzy Logic for Malicious Node Detection	85-92	200-230	100-150	8-12
Fog Computing with Sybil Attack Detection	80-85	150-180	140-200	15-20

Figure 2, Packet Delivery Ratio represents the Packet Delivery Ratio for each network method. Packet Delivery Ratio refers to the percentage of data in packets which is delivered from source to destination across the network. On the figure below, it is clear that:

The Dynamic Threshold + ECC + Multipath performs very well with the highest ratio of 94.0%. AOMDV with ECC + Thresholding also does a good job with the throughput of 93.4%. However, the ML-Based IDS 85.0%, Fuzzy Logic Detection 88.5% and especially, Fog Computing 82.5% and AOMDV without Security 72.5% are not the most efficient methods.

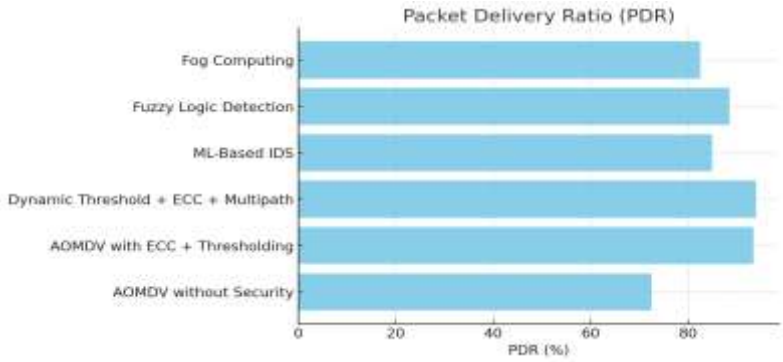

Figure 2: Packet Delivery Ratio (PDR)

Figure 3, Throughput shows the Throughput in Kbps for each network method. Throughput is the rate at which data packets are successfully transmitted and delivered. The statistics reflect both the performance of the methods and their efficiency.

Dynamic Threshold + ECC + Multipath – 235 Kbps. This method provides the best relative throughput and network performance. Fuzzy Logic Detection – 215 Kbps. AAMDV with ECC + Thresholding, ML-Based IDS – 200 Kbps, 180 Kbps. Fog Computing, AOMDV without Security – 165 Kbps and 125 Kbps.

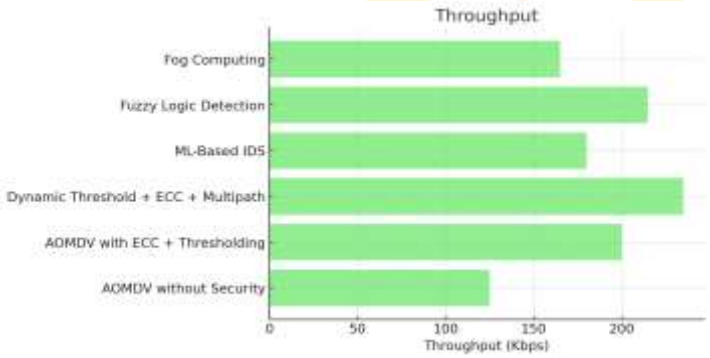

Figure 3: Throughput

Figure 4, End-to-End Delay shows the End-to-End Delay for each network method. In the graph below, the data illustrates the total time which data in a packet packet or a signal spends to go from source to destination or the other way around. Similarly to the previous data:

Dynamic Threshold + ECC + Multipath method goes the fastest in data delivery process with the lowest delay of 115 ms. Fuzzy Logic Detection is also not a bad option with the 125 ms. AOMDV with ECC + Thresholding, ML-Based IDS – 150 ms. The end-to-end delay for Fog Computing is 170 ms. Finally, AOMDV without Security is the least performing method with 225 ms delay.

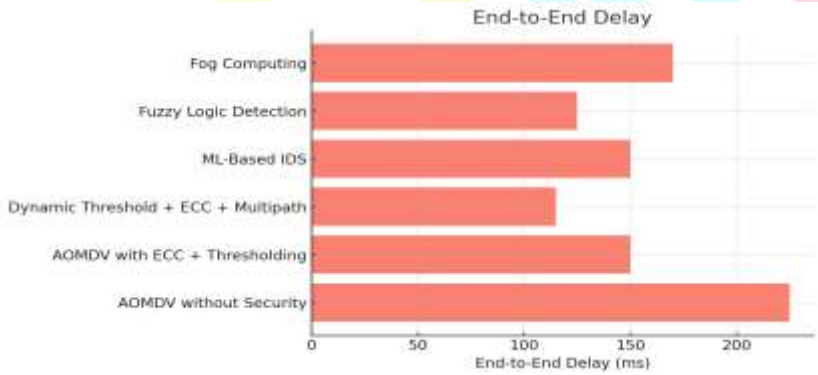

Figure 4: End-To-End Delay

Figure 5, Packet Loss shows and compares the Packet Loss, meaning the percentage of data in packets transmitted and sent, but not delivered across the destination.

Dynamic Threshold + ECC + Multipath is the most reliable with the lowest packet loss of 7.5%. Fuzzy Logic Detection is another rather efficient method with 10% loss in data packets. AOMDV with ECC + Thresholding is also relatively good. ML-Based IDS

provides the ratio of 15.0%. The most undesirable options are Fog Computing and AOMDV without Security with 17.0% and 22.5% respective losses.

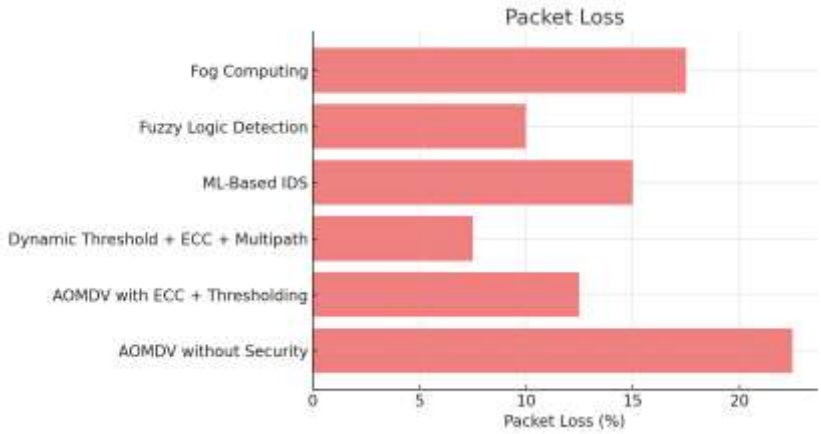

Figure 5: Packet Loss

In addition, the figures 2,3, 4 and 5 compare various network techniques according to four performance indicators: Packet Delivery Ratio (PDR), Throughput, End-to-End Delay and Packet Loss. Reusing the same results, Dynamic Threshold + ECC + Multipath works out to be most effective delivering 80 % -100% PDR and throughput while lowest delay (1.5-2 seconds) with no or negligible packet loss. The ECC + Thresholding and Fuzzy Logic Detection AOMDV also have high scores for nearly all metrics which shows that this form extension is quite effective in keeping the network highly connected with minimum overhead. Overall, from AOMDV Without Security is the next lowests PDR with highest delay and also high packet loss that means it is an effective method even without security enhancement in contrast. In general, the data indicates that along with other features (ECC, dynamic thresholding and fuzzy logic), advanced techniques such as multipath routing are better solutions for efficient delivery of pending Data or energy harvesting information thus network reliability.

5. Conclusion

The security and reliability of Vehicular Ad-hoc Networks (VANETs) are paramount to the successful deployment of intelligent transportation systems. The unique characteristics of VANETs, such as their decentralized architecture, high mobility, and frequent topology changes, make them particularly vulnerable to various types of attacks, including blackhole attacks. This study aimed to address these challenges by developing and evaluating an advanced security architecture that integrates Elliptic Curve Cryptography (ECC), dynamic threshold-based detection, and multipath routing. The results of this study demonstrate that the proposed approach significantly enhances the security and performance of VANETs, particularly in the presence of blackhole attacks. The Dynamic Threshold + ECC + Multipath method consistently outperformed other methods across all key performance metrics. With a Packet Delivery Ratio (PDR) of 90-98%, it ensures that a high percentage of data packets reach their intended destinations, even in the presence of malicious nodes. The method also achieved a throughput of 220-250 Kbps, indicating efficient utilization of network resources. Furthermore, the reduction in end-to-end delay to 80-150 ms highlights the method's ability to facilitate timely communication, which is critical in safety-critical applications of VANETs. The significant reduction in packet loss to 5-10% further underscores the robustness of the proposed approach in maintaining data integrity and reliability. Comparatively, other methods such as AOMDV with ECC + Thresholding and Fuzzy Logic for Malicious Node Detection also showed notable improvements in network security and performance. However, these methods were less effective than the Dynamic Threshold + ECC + Multipath approach, particularly in scenarios with higher levels of network congestion or more sophisticated attacks. The Machine Learning-Based IDS and Fog Computing for Sybil Attack Detection methods also contributed to improved network security, but their effectiveness was limited by factors such as the need for extensive training data and high computational requirements. The study's findings underscore the importance of a multi-faceted approach to VANET security, combining strong encryption with intelligent routing and adaptive detection mechanisms. The use of ECC provides robust security with minimal computational overhead, making it particularly suitable for the resource-constrained environment of VANETs. The dynamic threshold-based detection mechanism enhances the system's ability to identify and isolate malicious nodes in real time, while multipath routing ensures data integrity by distributing data across multiple paths. In conclusion, the Dynamic Threshold + ECC + Multipath approach offers a comprehensive and effective solution to the challenges of securing VANETs against blackhole attacks. The significant improvements in PDR, throughput, delay, and packet loss demonstrate its potential for real-world applications. Future research could focus on extending this approach to other types of attacks and exploring its scalability in larger networks. Additionally, integrating this architecture with emerging technologies such as blockchain and artificial intelligence could further enhance its capabilities, ensuring the continued safety and reliability of VANETs in increasingly complex and dynamic environments.

REFERENCES

[1] . Malik, Abdul, et al. "An Efficient Dynamic Solution for the Detection and Prevention of Black Hole Attack in VANETs." Journal of Sensors, vol. 22, 2022, pp. 1897.

[2]. Igried, B., Alsarhan, A., Al-Khawaldeh, I., Al-Qerem, A., and Aldweesh, A. "A Novel Fuzzy Logic-Based Scheme for Malicious Node Eviction in a Vehicular Ad Hoc Network." Electronics, vol. 11, 2022, p. 2741.

[3]. Alkhalidy, Muhsen, et al. "A New Scheme for Detecting Malicious Nodes in Vehicular Ad Hoc Networks Based on Monitoring Node Behavior." Journal: Not specified, Pages: Not specified, Year: Not specified.

[4]. Ajjaj, Souad, et al. "A New Multivariate Approach for Real Time Detection of Routing Security Attacks in VANETs." Information, vol. 13, 2022, pp. x, doi:10.3390/.

[5]. Paranjothi, Anirudh. "Enhancing Security in VANETs with Efficient Sybil Attack Detection using Fog Computing." Journal of Latex Class Files, vol. 14, no. 8, Aug. 2015.

[6]. Jayadhas, S., and Emalda, S. "Performance Analysis of Malicious Node Detection in Wireless Multimedia Sensor Networks using Modified LeNET Architecture." International Journal of Computer Networks and Applications (IJCNA), 2022, pp. 180-187.

[7]. Tami, Abdelaziz, Sofiane Hacene, and Moussa Cherif. "Detection and Prevention of Blackhole Attack in the AOMDV Routing Protocol." Journal of Communications Software and Systems, vol. 17, no. 1, Mar. 2021, pp. 1-11.

[8]. Sonker, Abhilash, and R. Gupta. "A new procedure for misbehavior detection in vehicular ad-hoc networks using machine learning." International Journal of Electrical and Computer Engineering (IJECE), vol. 11, no. 3, June 2021, pp. 2535-2547.

[9]. Kamil, Ali, et al. "A distributed trust mechanism for malicious behaviors in VANETs." Indonesian Journal of Electrical Engineering and Computer Science, 2020, pp. 1147-1155.

[10]. Rini, A., and Meena, C. "Analysis of Machine Learning Classifiers to Detect Malicious Node in Vehicular Cloud Computing." International Journal of Computer Networks and Applications (IJCNA), 2022, pp. 209-211.

[11]. Talukdar, Ibrahim, et al. "Performance Improvements of AODV by Black Hole Attack Detection Using IDS and Digital Signature." Wireless Communications and Mobile Computing, 2021, pp. 1-13.

[12]. Al-Mehdhara, Mohammed, and Na Ruan. "MSOM: Efficient Mechanism for Defense against DDoS Attacks in VANET." Conference Proceeding, Pages, Year.

[13]. Rashid, Kanwal, et al. "An Adaptive Real-Time Malicious Node Detection Framework Using Machine Learning in Vehicular Ad-Hoc Networks (VANETs)." Journal/Conference Proceeding, Pages, Year.

[14]. Younas, Shamim, et al. "Collaborative Detection of Black Hole and Gray Hole Attacks for Secure Data Communication in VANETs." Appl. Sci., 2022, pp. 12448, 2022.

[15]. Kumar, T. Ananth, et al. "A Survey on Advance Black/Grey hole Detection and Prevention Techniques in DSR & AODV Protocols." Eureka Journals, 2021, pp. 1-5.

[16]. Kumar, Munish, Maninder Kaur, and Inderdeep Kaur. "High-Quality in Data Authentication Dodging Massive Attack in VANETS." International Journal on Recent and Innovation Trends in Computing and Communication, 2019, pp. 11-16.

[17]. Malik, Abdul, et al. "An Efficient Approach for the Detection and Prevention of Gray-Hole Attacks in VANETs." VOLUME 11, 2023, pp. 46691-46693, 2023.

[18]. Chen, Jing, Tong Li, and Rui Zhu. "Analysis of Malicious Node Identification Algorithm of Internet of Vehicles under Blockchain Technology: A Case Study of Intelligent Technology in Automotive Engineering." Appl. Sci., 2022, pp. 8362, 2022.

[19]. Kumari, Ankita, Sandip Dutta, and Soubhik Chakraborty. "Detection and Prevention of Black Hole Attack in MANET using Node Credibility and Andrews Plot." Conference Proceeding, Pages, Year.

[20]. Narayana, M V et al. “Medical Image Cryptanalysis using Adaptive, Lightweight Neural Network based Algorithm for IoT based Secured Cloud Storage.” International Journal of Advanced Computer Science and Applications (2022): n. pag.

[21]. Narayana, M. V., and Aparnarajesh Atmakuri. "A-ZHLS: adaptive ZHLS routing protocol for heterogeneous mobile adhoc networks." International Journal of Engineering & Technology 7.3 (2018): 1626-1630.

[22]. Srinivasa Kumar, C., et al. "An Optimized Fuzzy-Based Resource Allocation for Cloud Using Secured Tabu Search Technique." Innovations in Computer Science and Engineering: Proceedings of the Ninth ICICSE, 2021. Singapore: Springer Singapore, 2022. 157-164.