Proceedings of

International Conference on Visual Analytics and Data Visualization (ICVADV 2025)

Date: 4-6, March 2025

Organised by: Francis Xavier Engineering College, Tirunelveli, India

48	Enhancing E-commerce using Fashion Recommendation System Vinodh Kumar S, Kumar P, Saravanan S	300
49	Non- Intrusive Load Monitoring Techniques for Intelligent Energy Management: A Comparative Study of Fhmm and LSTM Approach N. Rajkumar, Anitha Govindaram, R. Geetha, Subhamathi A S F, Nithya S. , Jose Anand A. ,	306
50	A Comparative Analysis of IoT Platform Tools: Security and Scalability Preferences in Device Management using Ahp Maheswari S. , N. Rajkumar, R. Geetha, Kalakuntla Theja, M. Malleswari, Jose Anand A. ,	312
51	Continuous Sign Language Recognition and Translation using Deep Learning Approach Rakesh Kumar M, Kumar P, Vaseekaran R	318
52	AI based Efficient Analysis and Monitoring of Sugarcane Buds Detection and Leaf Disease Classification Ananthajothi K, Kumar P, Koteeswaran V	324
53	Integrated Deep Learning Framework for Automated Glaucoma Detection, Optic Disc/ Cup Segmentation, and Cdr Calculation Tina Brivitha K J, Sophia S,	330
54	Gesturelanguagerecognitionthroughdeep Learning D. Pradeep, Monisha S, Nandhini J, Poogesh R, Praneeshwar R	338
55	Drone Cyber Attack Detection through Machine Learning Sophia S, Getzi Jeba Leelipushpam paulraj, Devanshu Kumar	346
56	Lightweight Contextual Llms for IoT Data Interpretation in Smart Cities Tamilarasan Kannadasan	354
57	Svd Processor to Minimize the Number of Rotations in Jacobi Algorithm Sudhakar K, Balaji N, Tharunkumar R B,	360
58	Automating Brain Hemorrhage Detection through Deep Learning Approaches Shakina Princess S, Vignesh. R,	367
59	Contextual Aligned Tamil Sign Language Retrieval System with Semantic Masked Transformer S Thillai Sivakavi, R I Minu	374
60	Visionaid: Enhancing Accessibility for the Visually Impaired with YOLO and Gtts Bhagya Lakshmi Raghupathy, Nithyashri J	380
61	Electric Vechicle Battery Parameters Monitoring System using IoT Aruna S, Dharaneesh V M, Hariprasath E, Somasundaram PL	387
62	Development of Solar Powered 21-level Transformer-less Multilevel Inverter B. SharmilaDevi, M. P. Prasanna Venkatesh, S. Sulochini, T. Sudhakaran, R. Srinithi	393
63	Intelligent Battery Management Strategy Kamalraj VR, Dharshine B, Archana J, Dhanush V, Indhumathi R	397
64	Exploring Depression and Co-dependency Among Spouses of Individuals with Alcohol Use Disorder Padmapriya D. , Mahalakshmi M. , Manisha V. , Manju S. , Suganya M. , Ajith M. ,	404
65	Enhanced Security Framework for Gray-hole Attack Prevention in Vehicular Networks S. Vimalnath, Midhun R, Kavinesh A S, Karvendan P, Kishore K	410
66	Enhancing Master Data Management Within Enterprise Resource Planning Systems using Artificial Intelligence for Optimized Business	416

Proceedings of the International Conference on Visual Analytics and Data Visualization (ICVADV-2025)
DVD Part Number: CFP25VQ6-DVD; ISBN: 979-8-3315-2138-7

Enhanced Security Framework for Gray-Hole Attack Prevention in Vehicular Networks

Dr. S. Vimalnath
Associate Professor
Electronics And Communication Engineering
M. Kumarasamy College Of Engineering
Karur, Tamil Nadu, India.
vimalnaths.ece@mkce.ac.in

Midhun R
Electronics And Communication Engineering
M. Kumarasamy College Of Engineering
Karur, Tamil Nadu, India.
rvmidhun5784@gmail.com

Kavinesh A S
Electronics And Communication Engineering
M. Kumarasamy College Of Engineering
Karur, Tamil Nadu, India.
Kavinesh565@gmail.com

Karvendan P
Electronics And Communication Engineering
M. Kumarasamy College Of Engineering
Karur, Tamil Nadu, India.
karvendanselva@gmail.com

Kishore K
Electronics And Communication Engineering
M. Kumarasamy College Of Engineering
Karur, Tamil Nadu, India.
kishoresuriya638@gmail.com

***Abstract* --The gray-hole attacks are certainly destructive to the integrity and reliability of vehicular ad-hoc networks where a malicious node will drop packets selectively while keeping the instance innocuous. Commercial and Safety Applications Vehicular Ad-Hoc Networks and IoT of Vehicles, ITS, and V2X VANETs nowadays are advancing fast in tune with the commercial and safety applications. Nonetheless, despite offering plenty of possible advantages, VANETs cowl an openly-distributed-dynamic nature that raises their exposure to different classes of attacks and threats, one of those being the gray-hole attack (GHA)_. The first version is known as Smart GHA that did not disclose its wrongdoing during routing discoveries, whereas in the second variant-a sequence-based GHA-it behaves wrongly at the route discovery stage but selectively drops packets-after the route was established-in this two-pronged form. The present work specifies the novel strategy in the field of security which is termed Detection and Prevention of GHA (DPGHA). In it, both forms of GHA have been detected and prevented in AODV-based VANETs. The dynamic threshold values defined in DPGHA are based on the anomalies in the packets that are received, forwarded, and generated with their sequence numbers. Dynamic threshold values and dynamic monitoring could increase computational complexity even more and increase the processing requirements imposed on a node with limited resources. The algorithm endorses cooperative detection of malicious behavior and vehicles' resilience. Simulation and evaluation of the ARBD algorithm indicate enhanced accuracy and efficiency in the identification of gray-hole attackers, thus securing and boosting VANET performance.**

Keywords:* *VANET, AODV, GHA, DPGHA.

I. INTRODUCTION

A. Vanet

Broadly defined, Vehicular A d-hoc Networks are a type of mobile wireless network where vehicles are the Considered nodes. The idea is that any vehicle might serve to relay messages. This creates mobile networks spread out quite large in dimension, as distances of about 100-300 meters between vehicles may be bridged. When a vehicle exits the transmission range, which signifies its network exit, a bunch of new vehicles may enter into the network, creating the chance of mobile networks out there. These networks facilitate real-time data exchange regarding safety, traffic management, and driver assistance.

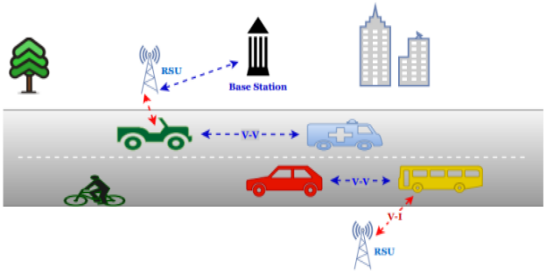

Fig 1: Vanet Design

For example, alerts concerning road conditions, accidents, and traffic congestion may be forwarded via VANET so as to raise efficiency and road safety. But associated with an increasing complexity and functionality of it is security problems. One of the huge devastating threats to VANET is the Gray-Hole Attack. A Gray-hole attack is fundamentally selective dropping of packets while forwarding others that makes detection even harder. A Black-Hole attack drops packets without executing any forwarding. Gray-Hole attacks cause hefty consequences, more so in safety-critical applications, such as collision avoidance and emergency messaging, where vehicular-to-vehicular and vehicular-to-infrastructure communications may be in jeopardy resulting from packet loss and/or delayed messaging, thus compromising safety.

B. Vanet Architecture And Functioning

A vehicular network consists of a number of vehicles known as vehicular nodes. As a prerequisite for the vehicular node system, the authority involved is the certification authority. Such vehicular nodes are designed to communicate each other by 5.9GHz radio frequency over a kilometer. This signal has a forged connection whereby it provides a good wireless access infrastructure to move around freely [1]. Every vehicle has this on-board unit, OBU. It communicates through radio signals between nodes or routers, thus making it easy for them to talk to one another. In the vehicular network, roadside units will act as routers and will usually mount physically near the roads while it connects the vehicles further on to other nodes as depicted in every individual on board. It also has a Tamper Proof here could be information such as driver identity, vehicle speed, trip information, route information, etc. Another such element is the Electronic License Plate (ELP), which is a special number for each vehicle and identification for vehicles. GPS is used for determining location nodes in vehicular networks. Each automobile utilizes GPS. The purpose of RSU is to stockpile all these vehicle-related data.

C. Gray-Hole Attack in VANETs

The Gray-Hole Attack utilizes the dynamic nature of VANETs, whereby nodes (vehicles) are highly mobile and topology changes in the network very fast. The fluid environment makes it even harder for traditional security mechanisms in the network because the node might take advantage and deliberately or selectively drop packets based on type, destination, and even time while pretending to be normal in other instances. Because the attacker is not interfering with all the incoming traffic, the malicious activities of the attacker go unnoticed very quickly by other nodes. The impact of this attack may be from causing slight delays in delivering any data to significantly affecting the reliability throughout the network. For example, critical information such as accident warnings, hazard notifications, or traffic signals may be selectively dropped, leading to communication failure and potential for accidents or the misdirection of traffic flow. The selective nature of the Gray-Hole Attack renders it especially pernicious since its greyness enables it to fly under the radar of most monitoring mechanisms, which would expect nodes to be either completely good or completely bad.

D. Need For Security In Vanets

Given the importance of VANETs for modern transportation systems, security and integrity of data become a prime concern. Attacks like Gray-Hole pose deep risks not only on the performance of the network but also to public safety. Therefore, solutions for securing VANETs have to detect malicious behavior robustly against various attacks, prevent such attacks, and ensure confidentiality and integrity of data without significant overhead and impact on performance. Given that designing adaptive, scalable, and efficient security mechanisms specifically tailored to the vulnerabilities of VANETs is challenging, a combined approach representing a detection, prevention, and secure communication mechanism that would prove appropriate in the highly dynamic environments of VANETs is necessary for successful protection against Gray-Hole attacks. This paper presents an Enhanced Security Framework for the prevention of Gray-Hole attacks in VANETs through combining several techniques for detection and prevention, with secure communication. It uses:

1) Reputation-Based Systems

Nodes are assigned reputation scores based on the behavior exhibited, like successful forwarding of packet. If a node continues dropping packets or acts abnormally, then its reputation score is reduced, and it becomes easier to discover Gray-Hole attackers.

2) Collaborative Detection

The nodes in this network collaborate with one another to verify the behavior of neighboring nodes. Using redundant paths and acknowledgments, they can detect whether a node is selectively dropping packets. Cross-verification techniques help to pinpoint malicious nodes by comparing received and forwarded data The framework uses secure versions of the routing protocols AODV (Ad hoc On-demand Distance Vector) and DSR (Dynamic Source Routing), along with enhanced security features. The protocols are then modified to monitor and validate node behaviors so as to identify the Gray-Hole attackers.

3) IDS

Intrusion Detection Systems (IDS) monitor the network for unusual behavior by identifying potential Gray-Hole attacks based upon traffic patterns and routing anomalies.

II. RELATED WORK

Gray hole attacks on VANETs are stealthy and targeted attacks, prompting significant research toward their detection and mitigation. The Gray-Hole attack consists of the situation where one in a series of routing or data packets is dropped in transit by an adversarial node; proper packet loss analyses render detection near impossible. A host of techniques ranging from intrusion detection systems (IDS) to secure routing protocols were touted over the years for their ability to thwart or even detect such attacks. Herein is discussed some of the key related work on the topic.

1. Intrusion Detection Systems (IDS) for Gray-Hole Attack Detection IDS generally intends to detect Gray-Hole attacks in VANET by monitoring the network traffic and its associated anomalies in nodes. IDS packets forward looking at their forwarding pattern also detect malicious behavior, such as selective packet dropping.

2.Hossain et al. (2016) proposed IDS-based solution to detect Gray Hole attacks with packet dropping ratio analysis. They monitor the nodes' packet forwarding behavior pattern and compare this with the patterns of expected ones. Nodes which have abnormally long packet dropping intervals are marked as potential Gray-Hole attackers. The main challenge for the method is scalability in large-scale networks with high vehicle mobility.

3.Tushar et al. (2018) proposed an IDS that applied machine learning in identifying anomalies in packet forwarding behavior. The model was designed with adaptation to various attack patterns for improving detection abilities. However, it suffers from resource consumption and complexity.

III. TECHNOLOGIES USED

A. Intrusion Detection Systems (IDS)

Intrusion Detection System (IDS) is perhaps the most critical in observing the behavior of network nodes in a vehicle ad hoc network. Detection of irregularities in basic functions is taken as having a suspicion of Gray-Hole attacks. IDSs typically engaged consist of: Traffic Monitoring. These tools monitor routing behavior and search for anomalies in network flows and packet movement patterns that may reveal a Gray-Hole attack, two examples being packet sniffers and network analyzers. Anomaly Detection Algorithms. Intrusion Detection Systems recognize abnormal packet dropping or packet forwarding behaviors by modelling normal behavior through machine learning or statistical techniques. Signature-Based IDS: This policy uses signatures of existing known attacks to detect known attack patterns. The IDS would discover Grey-Hole attacks by checking sensed traffic flows against known attack signatures for packet dropping or selective forwarding.

B. Trust and Reputation-Based Systems

A trust and reputation-based system, on the other hand, tries to evaluate the trustworthiness of nodes based on their past behavior, such as successful packet forwarding. Those malicious nodes, which perform selective packet dropping behaviors, would have low trust values, thus making it easier to detect them as Gray-Hole attackers. A trust-based method was put forward by Qin et al. (2013), wherein each node calculates its neighbor's trustworthiness based on the successful delivery rate of packets. Malicious nodes will come to be isolated and excluded from the network. Although trust-based systems have a great potential to mitigate Sybil attacks by the generation of multiple identities from an attacker to manipulate trust metrics, when two colluding nodes exchange dubious reputation information, Zhou et al. (2016) put forward an improved reputation system whereby nodes were allowed to exchange feedback about other nodes, depending on their interaction with them. Such a collaborative reputation model is indeed supposed to enhance detection accuracy further, but still, the malicious nodes would seek ways to manipulate reputation data.

C. Secure Routing Protocols

Secure routing protocols are designed to increase the efficacy of resilience against Gray-Hole attacks and facilitate the trustworthiness of the nodes that take part in the routing process for VANETs. Several protocols have been suggested for the protection of the two famous AODV and DSR routing protocols. Sharma et al., 2015 described a modification at AODV so as to ascertain Gray-Hole attacks against an improperly operating part of the protocol. Due to this alteration, a node is required to be put on careful observation for the censoring of packets while it is already informationally in possession of those packets for further forwarding, or terminate its routing. Such modification assists in identifying Gray Hole attackers before they perpetuate their harmful operations into the routing process. In 2014, Bhattacharyya et al. proposed a certain modification of the DSR protocol to counter Gray Hole attacks. Their proposition blocks non-trusted nodes during the route-finding operation; therefore, it diminishes the chances of making Gray-Hole attacks. This approach certainly tends to introduce another burden on communication as now-route validation is needed.

D. Multi-Path Routing

Multi-path routing, on the other hand, deals with forwarding data packets using several paths to enhance network resilience. This means that peering attacks of Gray- Holes could not stop the transmission toward the destination because the packets would be dropped along one path, and the other paths are likely to deliver the messages in the right direction. Santos et al. (2016) proposed a multi-path routing protocol that allows transmission over multiple disjoint paths. Along the entire route, a path is validated against a crosscheck of integrity as packets are forwarded along it. This way, the destructive nodes do not have any capability in jamming communication by dropping packets along only one path. The disadvantage of it is the additional overhead involved by the need to maintain and verify multiple paths concurrently in the network.

1) Collaborativedetection Mechanisms

Distributed Trust Models: In collaborative detection, there is mutual sharing of trust data, feedbacks, and behavior analysis of nodes with neighboring nodes for the collective detection of malicious behavior. Usually, distributed databases or peer-to-peer (P2P) networks are used for these sharing purposes. Data Aggregation: Nodes discuss information regarding the nature of behavior of other nodes and aggregate them in order to take decisions based on a good amount of data.

2) Machine Learning And Artificial Intelligence (Ai)

Anomaly Detection: ML algorithms are used in the form of SVM, decision trees, and neural networks. These algorithms learn normal and abnormal behavior patterns like selective packet dropping or malicious routing. This data is learned from network traffic over time with an improvement in the ability to identify Gray-Hole attacks. Reinforcement Learning: The essence of reinforcement learning in the case of adaptive security in VANETs is that it will learn to optimize the security parameters, such as attack thresholds and node behavior evaluation, relying on the ongoing observations and rewards from correct detection.

3) Cryptography

PKI is a special method of authentication offered in networking for confirming that nodes on the network are just the nodes that are supposed to be legitimate for participation in a routing process. Also, PKI prevents attacks on Gray-Hole since malicious nodes cannot masquerade as the legitimate ones in this case. Digital signatures are used primarily for integrity, to ensure that data has not been tampered with. A node forwarding a packet may sign it to authenticate itself and to ensure that attackers cannot modify it in mid-transmission. Cryptographic hash functions are being used in many secure routing protocols for detection of any changes in data and for ensuring data forwarded by nodes has not been altered.

4) Vehicular communication Technologies

Dedicated Short Range Communication (DSRC): DSRC is a vehicular communication medium developed for such applications as rain sensing, electronic toll collection, etc. It allows ultra-low latency information exchange causing most vehicular-to-vehicular and vehicular-to-infrastructure models of communication for real-time awareness of anomalous behaviors like Gray-Hole attacks. 5G and C-V2X: With the evolution of 5G connectivity and C-V2X, the most attention is drawn toward increased bandwidth, lesser latency, and improved reliability of communication related to vehicles. These technologies support real-time data dissemination for collaborative detection and mitigation of Gray-Hole attacks. Wi-Fi and Bluetooth: Wi-Fi or Bluetooth technologies are used in a short-range communication scheme among an unfortunate few car.

IV. PROPOSED SYSTEM

An integrated system combining multiple technologies and strategies is proposed for enhancing the safety of VANETs against Gray-Hole attacks. We will combine IDS, Reputation Management, Secure Routing Protocols, and mechanisms for Collaborative detection into one unique framework, making it more resilient to attacks while optimizing the use of network resources. The proposed system is designed to identify Gray-Hole attackers-sending nodes that selectively drop packets-by real-time monitoring, trust-based evaluations, and enhancements for secure routing. The system also allows mechanisms to work properly in the dynamic and mobile environment of VANETs without encountering significant overhead or performance degradation. Key Features of the Proposed System Dynamic Trust and Reputation System Intrusion Detection System (IDS) with Anomaly Detection Enhanced Secure Routing Protocol (AODV/DSR) Collaborative Detection Mechanism Adaptive Detection with Machine Learning Low-Overhead Multi-Path Routing

A. Dynamic Trust and Reputation System

Trust and reputation models are at the heart of identifying malicious nodes, especially Gray-Hole attackers, in a VANET. This proposed system employs a dynamic trust assessment mechanism based on packet forwarding node behaviors.

Trust Metrics: Each node will compute a trust score for its neighbors based on their past behavior, focusing on packet forwarding success rates and responsiveness to routing requests. Nodes that consistently drop packets (selectively drop certain packets while forwarding others) will have a lower trust score.

Adaptive Thresholds: These trust thresholds will be adaptive-they will change upon changing network conditions like mobility and density. False positives will be avoided as network conditions may sometimes cause loss of packets.

Reputation Sharing: Trust scores will be shared by neighboring nodes. Nodes can update and propagate trust values within their communication range, enabling them to detect Gray-Hole attacks based on collective data.

Sybil Attack Mitigation The system employs public-key cryptography (PKI) to authenticate nodes and their reputation data. Each node's identity will be validated by certificates issued by a trusted authority, and the update to their reputation will be signed digitally.

B. Ids With Anomaly Detection

An IDS will complement this reputation system by monitoring network traffic and detecting anomaly indicators of a Gray-Hole attack.

Packet forwarding monitoring: IDS will monitor packet forwarding behavior on each node and track dropped packets if these are being dropped at higher rates than normal. This will include the comparison of observed packet dropping behavior to baseline metrics for the detection of nodes that behave with selective packet dropping.

Anomaly Detection: The IDS will utilize machine learning to apply algorithms for example Support Vector Machines SVM or K-means clustering that detects abnormal packets that do not forward according to normal patterns. These models will be trained to recognize attack signatures and automatically classify behavior as normal or anomalous.

Collaborative IDS: The nodes will collaborate with each other by exchanging detection alerts to verify and improve the accuracy of the detection of attacks. Nodes with higher trust scores relied upon to a greater extent in the detection process.

C. Advanced Secure Routing Protocol (AODV / DSR)

The routing schemes, AODV and DSR, are thus prone to the Gray-Hole attack, which, in turn, involves the selective discard of packets by the malicious nodes in the route discovery and maintenance phases. The proposed system develops the protocols with enhanced security measures-Packet Forwarding Verification: A node will not pass on a packet toward a neighbor if it refused to forward it-up and thus, will be suspected and rejected from further consideration as a route. Route Integrity Validation: It will also check for integrity according to this protocol, where all nodes in the path can have trust values sufficiently above a pre-defined

TABLE:I Vanets Simulation Parameter

Parameter	Values
Area size	1000*1000
Nodes	100
Communication range	250 m
Mobility Model	Srinagar Highway
Simulation Time	900 seconds
Packet Transmission Parameters	512 bytes
Type of Traffic	CBR

threshold, any node with a low trust value will be suspected of being a Gray-Hole attack node and thus filtered from the routing table.

Security-Enhanced AODV/DSR: The protocols of the secure versions of AODV and DSR will encompass digital signatures for route authentication; all nodes participating in the route are authenticated by means of digital signatures. In such a case, only those nodes having authentic signatures will be utilized in route formation and maintenance.

D. Collaborative detection mechanism

The proposed system has a collaborative detection mechanism to enhance the accuracy and robustness of detection against Gray-Hole attacks, where nodes cooperate with each other. Feedback Exchange: Nodes exchange feedback about their experience with interactions from their neighboring nodes. A node that discovers it is being targeted by a neighbor node which persistently drops packets will disseminate a warning regarding the malicious node.

Voting Mechanism: A voting mechanism would be used to confirm the suspicious nodes. If independent nodes flag a node as malicious multiple times, it will be marked as a Gray-Hole attacker. This minimizes the chances of false alarms and ensures cooperation in the detection of malicious behaviors by the network.

Collaborative IDS: The collaborative detection system will also be integrated with the IDS. Nodes will cross-check the anomalies detected with neighboring nodes, thus increasing the overall accuracy of attack detection.

E. Adaptive Detection with Machine Learning

The proposed system uses machine learning (ML) to adaptively detect and respond to changing network conditions and attack patterns.

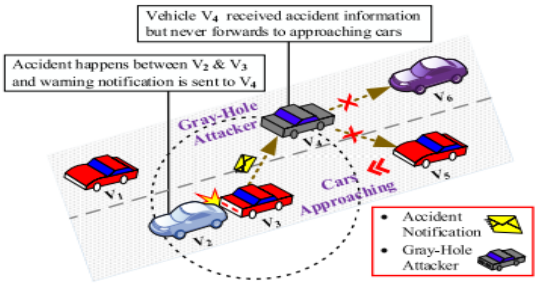

Fig:2 Architecture Diagram for Gray Hole Attack

Adaptive Detection Thresholds: It learns adaptively through reinforcement learning, adjusting the detection thresholds according to changes in the network conditions, such as mobility of nodes and network density. Under these varying conditions, this approach ensures that the system does not give too many false positives or negatives. Behavioral Prediction Machine learning models, especially in particular, supervised learning, predict future node behavior based on historical packet forwarding data. These would be trained to detect emergent Gray-Hole attack patterns for updating detection algorithms at run time.

F. Low Overhead Multi-Path Routing

To nullify the effects of Gray-Hole attacks, which rely on selective packet dropping, the proposed system incorporates multi-path routing to increase resilience. Multiple Routes: Unlike a single path, the system will send packets along multiple paths concurrently. If a Gray-Hole attacker disrupts one path by dropping packets, the other paths will ensure successful delivery. Route Selection: Multi-path routing algorithms will use trust-based metrics to select the most reliable paths for data transmission, minimizing the risk of relying on paths involving malicious nodes. Load Balancing: Multi-path routing also provides opportunities for load balancing across the network, reducing congestion and improving overall network performance.

V. SYSTEM ARCHITECTURE OVERVIEW

Node Communication: Each vehicle (node) communicates with other vehicles and infrastructure through DSRC or C-V2X communication technologies. Trust Management: The nodes dynamically compute and publish trust values based on the behavior of packet forwarding; neighbors are notified with trust information. IDS and Collaborative Detection: The IDS is monitoring the behavior of the packets forwarding to raise alerts. Nodes share feedbacks in peer-to-peer mode to collaborate to identify misbehavior. Secure Routing: The modified version of AODV/DSR is used so only trusted nodes are included within routing paths, and has cryptographic verification in addition to packet forwarding validation. Machine Learning and Adaptation: The system adapts the detection thresholds at runtime using real-time network conditions with the help of machine learning algorithms, continuously learning from data. Here is the detailed description of the simulation parameters for a DPGHA approach in

VANETs, using MATLAB and network simulators, or other custom MATLAB scripts. These parameters
will help you set up the simulation, evaluate performance, and compare those against any benchmark protocols**.**

VI. RESULT AND DISCUSSION

A simulation process on how to prevent a gray-hole attack (GHA) in vehicular ad-hoc networks using MATLAB will involve a step-by-step design of the simulation environment, attack implementation, and application of the dynamic prevention of gray-hole attack. Below is the broad outline of what one could do in MATLAB. Through MATLAB, one is further able to create and simulate VANETs and the possible network behaviors, which are

Let us discuss the simulation parameters for the approach of DPGHA against a gray-hole attack in VANETs with the help of MATLAB as well as network simulators like NS-2, SUMO, or custom MATLAB scripts. Such parameters will help you set up your simulation, evaluate performance, and compare the results against benchmark protocol

A. Performance Evaluation

The performance of the proposed DPGHA approach is assessed by comparing it to existing benchmark methods. To ensure a fair evaluation, the following performance metrics were considered: Routing Overhead. By focusing on this key metric, the study aims to quantify how efficiently the proposed approach manages the overhead associated with routing in the system. The comparison highlights the effectiveness of DPGHA in optimizing routing processes while minimizing additional communication costs, offering valuable insights into its practical applicability and advantages over traditional approaches. • Packet Delivery Ratio

- Throughput
- End-to-End Delay
- Packet Loss Ratio
- Detection Ratio

1) Routing Overhead

Routing overhead is defined as the number of Control packets (CPs) sent in comparison with the total number of Data packets (DPs) received at the destination end. The metric indicates the number of CPs required to send for a given the number of DPs. The major CPs of AODV routing protocol consist of RREQ, RREP, RERR (Route Error), and Hello messages.

$$ROH = \frac{\Sigma CP_{Transmitted}}{\Sigma DP_{Transmitted}} \quad \dots (1)$$

Increased overhead is measured. More number of RREPs will be desired routes to accommodate the increased number of malicious nodes in the network when routing overhead becomes very huge. More packets, due to a large number of malicious nodes, hence leads to loss more in conventional AODV. Hence average routing overhead of traditional AODV is about 5508.33.

2) Packet Delivery Ratio (PDR)

The PDR is referred to the ratio of the total number of Number of data packets sent by the source node to the total number of data packets received by the destination node. Calculated by

$$PDR = \left(\frac{\Sigma DP_{Received}}{\Sigma DP_{Sent}}\right) * 100 \quad \dots (2)$$

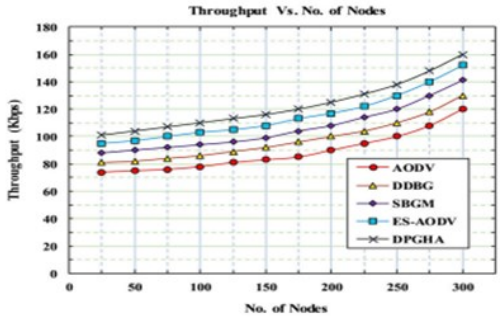

Fig 3: Comparison of throughput

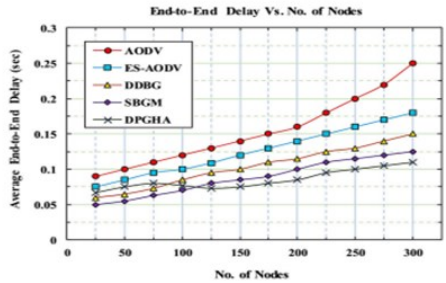

Fig 4: End To End Delay

VII. CONCLUSION

This proposed framework for Enhanced Security Framework for Gray-Hole Attack Prevention in VANETs provides a comprehensive and adaptive solution in the endeavor to tackle one of the most subtle and disruptive security threats in VANETs. The proposed framework is comprehensive, taking into account the various layers and security mechanisms: multiple layers of Intrusion Detection Systems (IDS), Trust and Reputation Management, Collaborative Detection, Secure Routing Protocols, and Machine Learning-based Adaptation, providing a strong defense against Gray-Hole attacks while maintaining efficiency and scalability in dynamic and high-mobility environments. Gray-Hole Intruders would be caught in the early stages through continuous monitoring and real-time analysis of packet forwarding behavior. IDS work effectively even in highly dynamic and large-scale VANETs. Prevention from Reputation-Based System: The framework reduces the dependency on any single node, and then by having a distributed trust and reputation management system, it makes the attack difficult and unnoticed to the attackers. Collaborative Defense: This framework improves detection since nodes can be in cooperation to exchange feedback for the identification of malicious behavior, thus ensuring higher accuracy and reliability in detecting Gray-Hole attacks. Adaptive Security: The system introduces machine learning to allow dynamic adjustments of detection thresholds by updating corresponding changes in attack patterns and network conditions to continuously improve protection against emerging and new threats. Efficient Routing: The advanced routing protocols with security mechanisms, such as AODV/DSR, will ensure that only trusted nodes take part in the forwarding of packets. This reduces the risks due to malicious nodes. Scalability and Flexibility: It is scalable to the VANETs growth and accordingly adaptable to diverse topologies and mobility patterns; thus, it is suitable for large and changing networks of vehicles constantly. Conclusion The Enhanced Security Framework has enhanced significantly the security posture of VANETs against Gray-Hole attacks. As a result of the integration of detection, prevention, and adaptive learning, vehicular communication systems will remain resolute, reliable, and secure in the real-world environment. More complex mechanisms can be further developed concerning the security requirements of VANETs, ensuring safe and efficient vehicular communications in the future.

VIII. FUTURE ENHANCEMENT

A. Integration with Blockchain for Trust Management

Others may evolve into integrated blockchain systems in the future for leveraging the Trust and Reputation Management system even better. A Decentralized Trust Ledger: Using a blockchain-based ledger for reputation scores of nodes tampered-proof and transparent can prevent manipulation of the trust system through an attacker to alter the reputation scores. Security with Smart Contracts: Security policies can be executed through blockchain-supported smart contracts. An example of this is the automatic exclusion of malicious nodes from the network or initiation of pre-programmed countermeasures when the occurrence of Gray-Hole attacks is detected. Benefits- Increased transparency and immutability in trust management. A better resisting-protection against Sybil and other trust-based attacks.

REFERENCES

[1] Rasheed Hussain, Fatima Hussain, Sherali Zeadally "*Integration of VANET and 5G Security: A review of design and implementation issues*" Elsevier Future Generation Computer Systems (Volume 101, December 2019).

[2] Xiaobo Wang; Yu Weng; Honghao Gao "*A Low-Latency and Energy-Efficient Multimeric Routing Protocol Based on Network Connectivity in VANET Communication*" IEEE Transactions on Green Communications and Networking (Volume: 5, Issue: 4, December 2021).

[3] Maryam Gillani, Hafiz Adnan Niaz, Muhammad Umar Farooq, Ata Ullah "*Data collection protocols for VANETs: a survey*" Springer Nature - Complex & Intelligent Systems (Volume 8, January 2022).

[4] S Vimalnath, G Ravi (2020) "*Optimized Geographic Routing in Mobile Ad Hoc Network using Bees Swarm Optimization*", Journal of Scientific & Industrial Research, Publishe: NISCAIR-CSI,Vol. 79, pp. 727-729.

[5] Abdul Malik, Muhammad Zahid Khan, Saeed Mian Qaisar, Mohammad Faisal, Gulzar Mehmood "*An Efficient Approach for the Detection and Prevention of Gray-Hole Attacks in VANETs*" IEEE Access (Volume: 11, 09 May 2023).

[6] Pooja Rani, Kavita, Sahil Verma, Gia Nhu Nguyen "*Mitigation of Black Hole and Gray Hole Attack Using Swarm Inspired Algorithm with Artificial Neural Network*" IEEE Access (Volume: 8, 25 June 2020).

[7] Vimalnath. S, Ravi. G., (2020). "*Optimized Geographic Routing in Mobile Ad Hoc Network Using Gray Wolf Optimization,*" EAI endorsed transaction. (Research Article-EAI.EU).

[8] Ansam Khraisat, Iqbal Gondal, Peter Vamplew, Joarder Kamruzzaman "*Survey of intrusion detection systems: techniques, datasets and challenges*" Springer Nature - Cybersecurity (Volume 2, article number 20, July 2019).

[9] Dr. T. Ananth Kumar1, A. Devi1, N. Padmapriya, S. Jayalakshmi1, P. Divya "*A Survey on Advance Black/Grey hole Detection and Prevention Techniques in DSR & AODV Protocols*" International Journal on Wireless, Networking & Mobile Communication Innovations (Volume 5, Issue 1 – 2021) ISSN: 2581-5113.

[10] Jeong-Kyu Bae, Myung-Chul Park, Eun-Ju Yang; Dae-Wha Seo "*Implementation and Performance Evaluation for DSRC-Based Vehicular Communication System*" IEEE Access (Volume: 9, 14 December 2020).

[11] Gurtej Kaur, Meenu Khurana, Amandeep Kaur "*VANET Cluster Based Gray Hole Attack Detection and Prevention*" Springer Nature – Computer Science (Volume 5, article number 186, January 2024).

[12] Vimalnath, M. S., Priyanka, S., & Sandhiya, M. (2020). "*Vehicle as vehicular networks for big data transfer between data centers in ICF".* (2020) International Research Journal of Engineering and Technology (IRJET), (e-ISSN: 2395-0056).

[13] Thabiso N. Khosa, Topside E. Mathonsi, and Deon P. Du Plessis "*A Model to Prevent Gray Hole Attack in Mobile Ad-Hoc Networks*" Journal of Advances in Information Technology, (Volume 14, No. 3, 2023).

[14] Kaoutar Ourouss, Najib Naja, Abdellah Jamali "*Defending Against Smart Gray hole Attack Within MANETs: A Reputation-Based Ant Colony Optimization Approach for Secure Route Discovery in DSR Protocol*" Springer Nature - Wireless Personal Communications (Volume 116, January 2020).

[15] Usama Arshad, Munam Ali Shah, Nadeem Javaid "*Futuristic blockchain based scalable and cost-effective 5G vehicular network architecture*" Science Direct - Vehicular Communications (Volume 31, October 2021).

[16] Sparsh Sharma, Ajay Kaul "*VANETs Cloud: Architecture, Applications, Challenges, and Issues*" Springer Nature - Archives of Computational Methods in Engineering (Volume 28, June 2021).

DVD ISBN: 979-8-3315-2138-7

https://icvadv.com/

Certificate of Presentation

Presented to

Dr. S Vimalnath

For presenting the research article titled

Enhanced Security Framework for Gray-Hole Attack Prevention in Vehicular Networks

In International Conference on Visual Analytics and Data Visualization (ICVADV-2025) on 04-06 March 2025, organized by Department of Electronics and Communication Engineering, Francis Xavier Engineering College Tirunelveli, Tamil Nadu, India in association with IEEE

Session Chair	Conference Chair	Principal
	Dr. G. Rajakumar	Dr. V. Velmurugan

FRANCIS XAVIER® ENGINEERING COLLEGE
AN AUTONOMOUS INSTITUTION
Vannarpettai, Tirunelveli - 627 003.

Certificate of Presentation

Presented to

Midhun R

For presenting the research article titled

Enhanced Security Framework for Gray-Hole Attack Prevention in Vehicular Networks

In International Conference on Visual Analytics and Data Visualization (ICVADV-2025) on 04-06 March 2025, organized by Department of Electronics and Communication Engineering, Francis Xavier Engineering College Tirunelveli, Tamil Nadu, India in association with IEEE

Session Chair	Conference Chair	Principal
	Dr. G. Rajakumar	Dr. V. Velmurugan

FRANCIS XAVIER® ENGINEERING COLLEGE
AN AUTONOMOUS INSTITUTION
Vannarpettai, Tirunelveli - 627 003.

Certificate of Presentation

Presented to

Kavinesh A S

For presenting the research article titled

Enhanced Security Framework for Gray-Hole Attack Prevention in Vehicular Networks

In International Conference on Visual Analytics and Data Visualization (ICVADV-2025) on 04-06 March 2025, organized by Department of Electronics and Communication Engineering, Francis Xavier Engineering College Tirunelveli, Tamil Nadu, India in association with IEEE

Session Chair	Conference Chair	Principal
	Dr. G. Rajakumar	Dr. V. Velmurugan

FRANCIS XAVIER® ENGINEERING COLLEGE
AN AUTONOMOUS INSTITUTION
Vannarpettai, Tirunelveli - 627 003.

Certificate of Presentation

Presented to

Karvendan P

For presenting the research article titled

Enhanced Security Framework for Gray-Hole Attack Prevention in Vehicular Networks

In International Conference on Visual Analytics and Data Visualization (ICVADV-2025) on 04-06 March 2025, organized by Department of Electronics and Communication Engineering, Francis Xavier Engineering College Tirunelveli, Tamil Nadu, India in association with IEEE

Session Chair	Conference Chair	Principal
	Dr. G. Rajakumar	Dr. V. Velmurugan

FRANCIS XAVIER® ENGINEERING COLLEGE
AN AUTONOMOUS INSTITUTION
Vannarpettai, Tirunelveli - 627 003.

Certificate of Presentation

Presented to

Kishore K

For presenting the research article titled

Enhanced Security Framework for Gray-Hole Attack Prevention in Vehicular Networks

In International Conference on Visual Analytics and Data Visualization (ICVADV-2025) on 04-06 March 2025, organized by Department of Electronics and Communication Engineering, Francis Xavier Engineering College Tirunelveli, Tamil Nadu, India in association with IEEE

Session Chair	Conference Chair	Principal
	Dr. G. Rajakumar	Dr. V. Velmurugan

FRANCIS XAVIER® ENGINEERING COLLEGE
AN AUTONOMOUS INSTITUTION
Vannarpettai, Tirunelveli - 627 003.