IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 28, Issue 5, Ser. II (Sep. – Oct. 2026), PP 20-30
www.iosrjournals.org

Hash-Based Node Behavior Analysis for Grayhole Attack Detection in MANETs for Enhanced Reliability

Jatin verma[1], Anshu Bhasin[2] , Sandeep Singh[3]
[1]*Department of CSE, IKG Punjab Technical University* [2]*Department of CSE, IKG Punjab Technical University*
[2]*Department of CSE, Lyallpur Khalsa College, Jalandhar*

Abstract:
A mobile ad-hoc network (MANET) refers to a dynamically formed and distributed wireless network that is susceptible to several routing attacks. Such attacks adversely affect network performance by causing packet loss, routing disruptions, and a decline in packet delivery efficiency. This paper proposes a hybrid Grayhole attack detection framework that combines feature weighting, hashing mechanisms, linear regression, and dynamic thresholding techniques to identify malicious nodes and enhance network security. The proposed model analyzes node behavior using network parameters including packets sent, packets received, delay, latency, and jitter. A Hybrid Feature Value (HFV) is generated through feature normalization and standard deviation-based weighting, while hashing and regression techniques are employed to evaluate node behavior and prediction errors. The calculated Hybrid Detection Score (HDS) is used in a two-stage verification process to accurately distinguish malicious nodes from legitimate nodes while reducing false detections. Simulation results demonstrate that the proposed model achieves an average Packet Delivery Ratio (PDR) of 97.57%, a Packet Loss Rate (PLR) of 2.43%, a detection accuracy of 97.64%, and a routing overhead of 2.18%. The results demonstrate that the proposed approach effectively detects malicious nodes, reduces packet loss, improves packet delivery, and enhances communication reliability in dynamic MANET environments.
Key Word*: Grayhole Attack, MANETs, Hashing, Linear Regression, Dynamic Threshold, IDS*

Date of Submission: 14-09-2026 Date of Acceptance: 25-09-2026

I. Introduction

Wireless communication technologies have been rapidly growing and greatly impacting modern networking systems due to their wide applications in military communication, civilian services, disaster recovery, environmental monitoring and commercial sectors [1][2]. Among these technologies, mobile ad hoc networks (MANETs) have attracted a great deal of research attention because of their self-configuring and infrastructure-less properties. In MANETs, mobile nodes communicate directly, without a centralized administration or a fixed infrastructure [3][4].

The mobility of nodes results in dynamic and unpredictable change of network topology, which makes routing and network management difficult [5][6]. In MANET, unlike traditional networks, every node performs both communication and routing functions. Nodes need to cooperate all the time to maintain efficient network connectivity [7][8]. However, the decentralized and open nature of MANETs makes it very vulnerable to security threats. In the real world, some nodes may behave maliciously and launch attacks such as packet dropping, routing disruption, dissemination of false routing information, etc. which can severely affect the network performance and reliability [9][10].

Security remains one of the most critical and extensively investigated issues in ad hoc networks, as malicious intruders can easily. interfere with and disrupt the routing process [11]. Among various security threats, packet drop attacks are considered highly dangerous because they directly degrade network performance and communication reliability. In such attacks, malicious nodes intentionally discard packets that are forwarded through them according to the attack strategy employed. Furthermore, smart packet drop attacks use varying and adaptive mechanisms to target the network, making their detection and prevention more difficult, and therefore they continue to remain a significant unresolved challenge in MANET environments.

Gray Hole attack is one of the major security threats in Mobile Ad Hoc Networks (MANETs) because of its selective packet dropping behavior. In this attack, a malicious node acts as a legitimate node and sends forged Route Reply (RREP) messages during the route discovery process to attract network traffic. After the malicious node gets into the communication path, it drops packets selectively rather than forwarding them to the destination node.

recognized Unlike the Black Hole attack, a Gray Hole node does not drop all packets continuously but forwards some packets while dropping others under certain conditions like time, packet type or node identity. This

behavior is selective and unpredictable, which makes it difficult to detect the attack. In Fig 1. Node 5 is acting as a Gray Hole node in the MANET environment. The source Node 1 broadcasts a Route Request (RREQ) message to discover a route toward the destination Node 9. The malicious node responds with a forged Route Reply (RREP) message claiming a fresh and shorter route to the destination. The source node chooses Node 5 as an intermediate forwarding node for data transmission because of the fake RREP.

Node 5 starts dropping packets selectively after becoming part of the active route. In a Black Hole attack all the packets are dropped, whereas the Gray Hole node forwards some packets normally and drops others selectively. Due to the intermittent nature of the malicious behavior, the attack is hard to be detected by conventional security mechanisms.

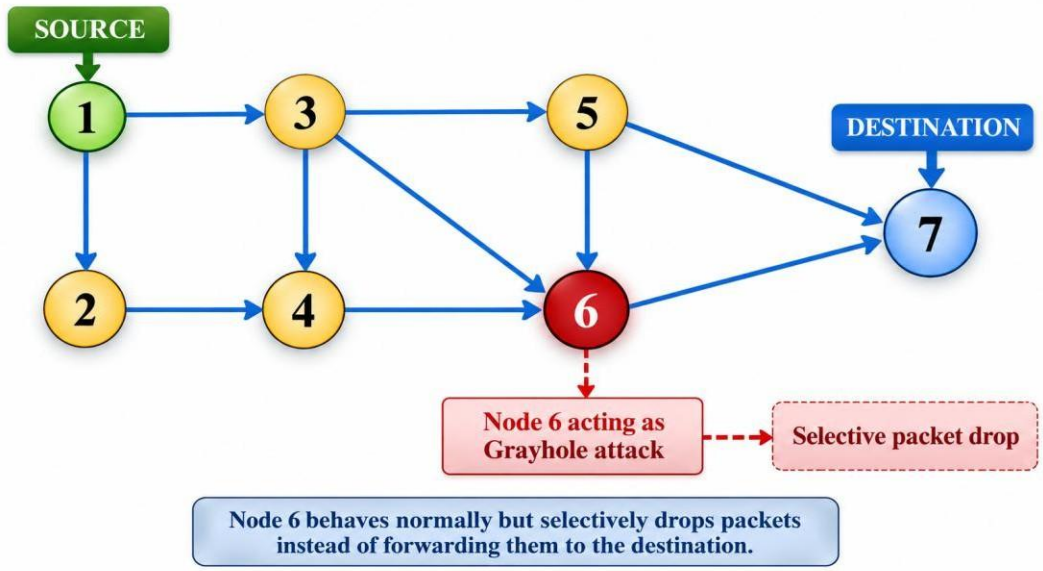

Fig 1. Illustration of Gray Hole Attack

One of the major challenges in MANETs is the identification of reliable and malicious nodes and the isolation of misbehaving nodes from the network. Therefore, an efficient and comprehensive mechanism is required to defend against different types of packet drop attacks. For precise identification of malicious nodes, the proposed framework aims to minimize false positives while keeping communication costs and routing overhead at acceptable levels.

To address this issue threshold based malicious node detection model is proposed for MANETs to effectively identify and isolate Gray Hole nodes. The model continuously monitors network behavioral parameters, including inbound packets, outbound packets, latency, jitter, and delay, to analyze node activities during communication. Packet forwarding behavior is evaluated through the drop ratio, while feature normalization and standard deviation weighting are applied to generate a Hybrid Feature Value (HFV) that represents the overall behavior of each node. SHA-256 hashing is then employed to derive an additional behavioral feature, and a linear regression model is used to estimate expected node behavior. The resulting prediction error, together with the normalized drop ratio and HFV, is utilized to compute the Hybrid Detection Score (HDS). A dynamic threshold generated from statistical characteristics of the HDS values is used to identify abnormal behavior.

In the proposed system, nodes whose Hybrid Detection Score exceeds a dynamic threshold are identified as suspicious and subjected to rehashing and dynamic re-evaluation for further verification. Nodes that consistently exhibit abnormal behavior are confirmed as malicious and isolated from the routing path to prevent packet-dropping attacks. The proposed mechanism aims to improve packet delivery ratio, reduce packet loss and false detections, and enhance network security, reliability, and routing stability while maintaining low routing overhead in the MANET environment.

II. Releated Work

Gurung and Mankotia et al. [12] proposed the ABGF-AODV protocol to detect black-hole, gray-hole, and flooding attacks using IDS monitoring and dynamic thresholds. Malicious nodes are isolated through ALERT and blacklist mechanisms, improving packet delivery and network security. However, the method increases routing overhead and energy consumption. Mohammad and Stefano et al. [13] proposed a hybrid

Watchdog-DSR approach to detect black-hole and gray-hole attacks. By monitoring packet forwarding behavior, the method improves packet delivery ratio, reduces latency, and lowers false positives. However, continuous monitoring increases computational overhead. Khattak et al. [14] proposed a hash-based malicious node detection scheme that selects an alternative route and verifies packet integrity using SHA-128. Hash mismatches indicate malicious activity, improving attack detection at the cost of additional processing overhead. Wadhwani et al. [15] proposed a trust-based system in which each node calculates the trust of neighbouring nodes by counting RREQ and RREP packets. Josephine et al. [16] presented a mechanism which evaluates the node features based on three factors and classifies these nodes into trusted or malicious. Initially, the support vector regression method is used to create a weak learner, after that ensemble classifier is used to create strong classification. Khanna et al. [17] introduced a lightweight trust-based mechanism by modifying AODV protocol to detect Blackhole attack and its variants in an efficient and effective manner. Authors used window and historical trust to find final trust. The window trust is calculated on three important parameters which includes energy consumption, packet forwarding ratio and link stability.

Kollati et al. [18] mechanism supports high mobility and increases the network performance. In this scheme Certificate Authority, uses a hash table and validates all nodes through the process of key generation. If any node is detected as malicious then it is added to the Blackhole list. It also checks the transmission failure and provides high fault tolerance. Moradipour et al. [19] proposed the AGHA (Anti-Gray Hole Attack) mechanism for MANETs using AODV. The scheme employs IDS nodes and a DTI table to identify malicious nodes based on abnormal RREP packets and packet-forwarding behavior. Malicious nodes are isolated through ALERT packets, improving packet delivery and reducing packet loss. However, continuous monitoring and multiple control packets increase routing overhead, memory usage, and energy consumption. Ullah et al. [20] calculated the trust using a hyperbolic tangent function. The optimal route is chosen based on trust and threshold value.

III. Proposed Algorithm

While extensive research has focused on the detection of Black Hole attacks, Gray Hole attacks remain more difficult to identify due to their selective and intermittent packet-dropping behavior. To address this challenge, an adaptive threshold-based Hybrid Anomaly Detection Model is proposed for the accurate detection and isolation of Gray Hole nodes in MANETs.

The proposed model integrates statistical feature analysis, hashing, and dynamic thresholding to identify malicious node behavior with low computational overhead. Initially, network behavioral parameters, including inbound packets, outbound packets, latency, jitter, and delay, are collected for each node during communication. The packet forwarding behavior is quantified using the packet drop ratio, while the remaining features are normalized and weighted using the standard deviation weighting method. The weighted features are then aggregated to compute a Hybrid Feature Value (HFV), representing the overall behavioral characteristics of a node.

To derive an additional behavioral indicator, the SHA-256 hashing algorithm is applied to the HFV. The generated hash values are converted into numerical form and normalized to obtain the Normalized Hash Value (NHV). Subsequently, a linear regression model is employed to establish the relationship between the NHV and the normalized drop ratio, enabling the prediction of expected node behavior. The deviation between the observed and predicted behavior is measured through the prediction error, which is further normalized. The normalized error, normalized drop ratio, and HFV are then combined to calculate the Hybrid Detection Score (HDS).

A dynamic threshold is generated from the statistical characteristics of the HDS values to distinguish normal and abnormal node behavior under varying network conditions. Nodes whose HDS exceeds the threshold are classified as suspicious and subjected to a second-stage verification process. During this stage, suspicious nodes undergo rehashing, parameter recomputation, and threshold recalculation. Nodes that continue to exceed the updated threshold are confirmed as malicious and isolated from the routing path, whereas the remaining nodes are classified as legitimate nodes. The proposed two-stage detection framework improves Gray Hole node detection accuracy, reduces false positives, minimizes packet loss, and enhances packet delivery performance, network reliability, and routing stability in MANETs. The overall workflow of the proposed system is illustrated in Fig. 2.

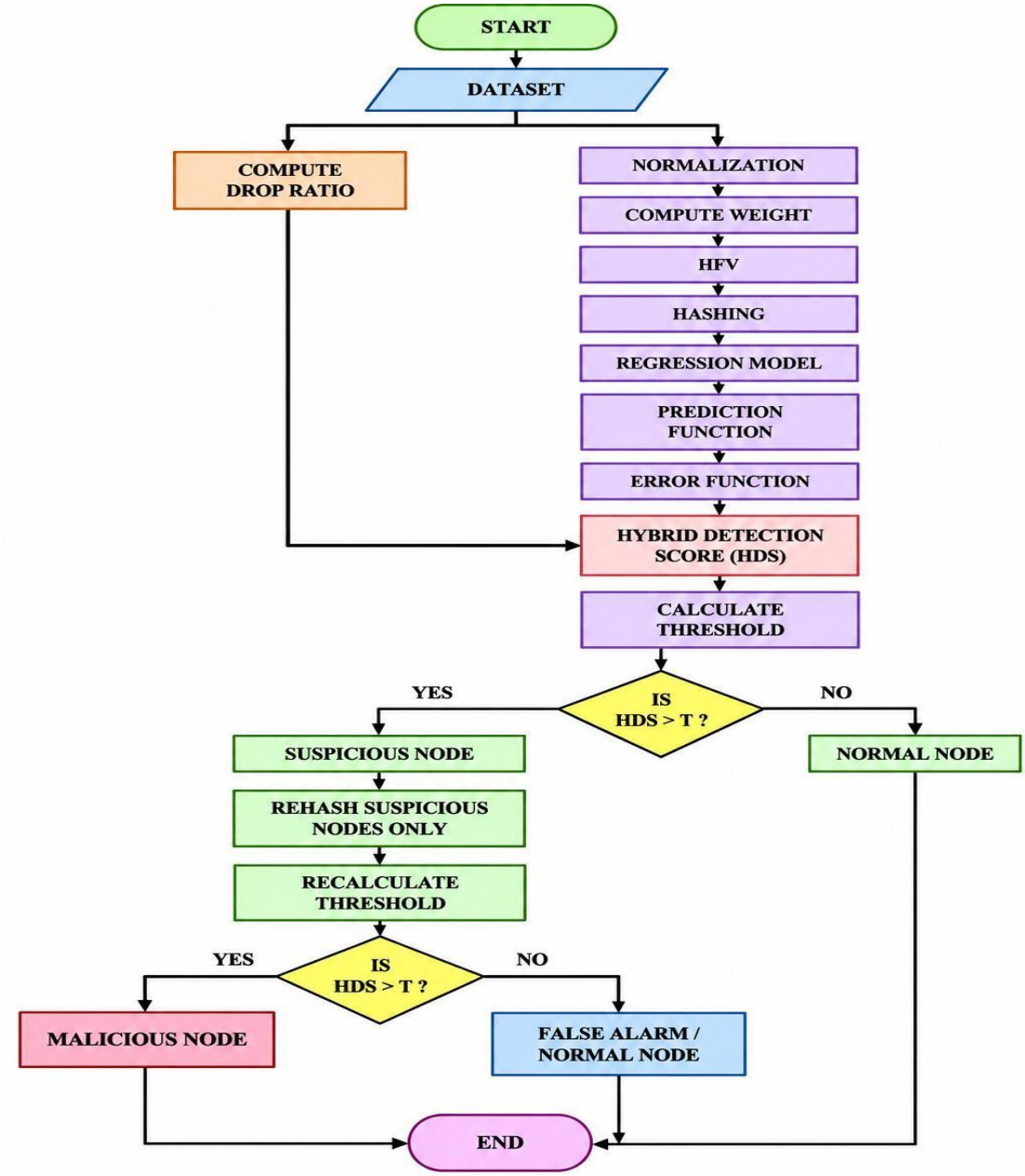

Fig (2) Flow Chart for the Proposed System

In the initial phase, the network is monitored to collect behavioral parameters for each node, including inbound packets, outbound packets, latency, jitter, and delay. These parameters provide valuable information regarding packet forwarding behavior and network performance. The packet forwarding behavior of a node is quantified using the Drop Ratio (DR), which represents the proportion of packets dropped by a node during communication. The Drop Ratio for node *i* is calculated using Equation 1.

$$DR_i = \frac{Inbound_i - Outbound_i}{Inbound_i} \quad (1)$$

Where Inbound and Outbound are the number of packets received and forwarded by node *i* respectively. To eliminate the effect of varying feature scales and ensure uniformity among the collected parameters, Min-Max normalization is applied. The normalized value of each feature is computed using Equation (2), where X_{min} and X_{max} denote the minimum and maximum values of the corresponding feature in the dataset.

$$X'_i = \frac{X_i - X_{min}}{X_{max} - X_{min}} \quad (2)$$

Since different network parameters contribute unequally to malicious node detection, feature importance is determined using the Standard Deviation Weighting Method. The mean and standard deviation of each normalized feature are computed, and the corresponding feature weights are calculated using Equation 3. Features exhibiting greater variation are assigned higher weights because they provide more discriminative information for anomaly detection.

$$W_K = \frac{\sigma_K}{\Sigma\sigma_j} \quad (3)$$

Where W_K is the weight of feature k and σk is the standard deviation of feature k and $\Sigma\sigma j$ represent the sum of standard deviation of all features.

The calculated weights are then utilized to generate the Hybrid Feature Value (HFV). The HFV combines multiple normalized network parameters into a single behavioral metric that comprehensively represents node activity. By integrating traffic characteristics and network performance indicators, the HFV captures both communication behavior and packet forwarding performance. The HFV of node *i* is obtained by aggregating these heterogeneous features into a single metric using equation 4.

$$HFV_i = w_{1NFeature_i} + w_{2NFeature_i} + w_{3NFeature_i} + w_{4NFeature_i} + w_{5NFeature_i} \quad (4)$$

To derive an additional behavioral indicator, the SHA-256 hashing algorithm is applied to the generated HFV. The hashing process transforms the combined feature information into a unique hash value, as shown in Equation 5. Since the generated hash values cannot be directly used in mathematical computations, they are converted into numerical form and normalized using Min - Max normalization to produce the Normalized Hash Value (NHV), as defined in Equation 6.

$$Hash_i = SHA256(HFV_i) \quad (5)$$

$$NHV_i = \frac{H_i - H_{min}}{H_{max} - H_{min}} \quad (6)$$

Where $Hash_i$ represent the generated hash value from the Hybrid Feature Value of node *i* and NHV_i is the normalized Hash Value.

The linear regression model is employed to capture the relationship between the Normalized Hash Value (NHV) and the normalized drop ratio. The obtained regression function is then used to predict the expected node behavior, and the prediction error is calculated and normalized. The resulting normalized error is subsequently utilized in the computation of the Hybrid Detection Score (HDS). The Hybrid Detection Score is computed using equation 7.

$$HDS_i = w_{1E_i} + w_{2NDR_i} + w_{3NHV_i} \quad (7)$$

Fixed thresholds are often ineffective in MANET environments because network conditions continuously change due to node mobility and dynamic topology variations. Therefore, the proposed model employs an adaptive thresholding mechanism based on the Median Absolute Deviation. Initially, a base threshold is computed using Equation 8.

$$T_{\{base\}} = Median(HDS) + K \times MAD \quad (8)$$

To further customize the threshold for individual nodes, the mean and standard deviation of the Hybrid Feature Values are calculated. A Deviation Index (DI) is then determined for each node using Equation 9, representing the degree of deviation from average network behavior.

$$DI_i = \frac{\{|HFV_i - \mu_{\{HFV\}}|\}}{\{\sigma_{\{HFV\}}\}} \quad (9)$$

The final node specific threshold is than calculated using equation 10 where λ denotes the sensitivity parameters.

$$T_i = T_{base}(1 + \lambda DI_i) \quad (10)$$

During the first detection stage if node satisfying $HDSi > Ti$ are classified as suspicious and forwarded to the second verification stage. The values of the suspicious nodes are rehashed, and the HFV and HDS are then recomputed for these nodes, where λ is replaced with λ′ such that λ′ > λ. The nodes are subsequently evaluated using a refined threshold, as defined in Equations (11) and (12).

$$Tbase2 = Median(HDS) \quad (11)$$

$$T^2_i = T_{base2}(1 + \lambda' DI_i) \quad (12)$$

Nodes that continue to satisfy the condition $HDS^2 > T^2$ after the second evaluation are confirmed as malicious. These nodes are immediately isolated from the routing path to prevent packet-dropping attacks and routing disruptions. The remaining suspicious nodes are reclassified as legitimate nodes, thereby reducing false positive detections.

IV. Simulation Parameters

The simulation of the proposed mechanism is performed using Python. Through simulation, validation of effectiveness and efficiency of the proposed mechanism on the basis of different parameters is performed against the published mechanisms. Table 1 includes various network parameters along with their respective values which are fixed during the simulation: -

Parameters	Values
Network Type Simulation Area	MANET
Simulation Time Number of Nodes	1000 * 1000 m^2
Normal Nodes Malicious Nodes	100 sec
Routing Protocols	150
	25-145
Traffic type MAC Protocol	5-15
Transmission Range	AODV,AGHA, PROPOSED UDP/CBR IEEE 802.11 250m
Mobility Speed Packet Size	10-50 m/s
Performance Metrics	512 Bytes
	Accuracy, TP, TN, FP, FN

Table1: Simulation Parameters

V. Result and Discussion

V.I. Result

The proposed Hybrid Anomaly Detection Model was evaluated under different MANET configurations to assess its effectiveness in detecting Gray Hole nodes. The performance was analyzed using detection metrics, including True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN), as well as network performance metrics such as Packet Delivery Ratio (PDR), Packet Loss Rate (PLR), Detection Accuracy, and Routing Overhead.

V.I. Scenario with 50 nodes

The proposed model was evaluated in a 50-node MANET with different numbers of malicious nodes. As shown in Table 2, the model achieved perfect detection for 5 and 15 malicious nodes, with no false positives or false negatives. For 10 malicious nodes, only one FP and one FN were observed, demonstrating the model's high detection capability and robustness.

S. No	Malicious Nodes	TP	TN	FP	FN
I.	5	5	45	0	0
II.	10	9	39	1	1

III.	15	15	35	0	0

Table 2: Classification Results for a 50-Node MANET

V.I.II Scenario with 100 nodes

The proposed model was evaluated in a 100-node MANET to assess its scalability. As shown in Table 3, the model achieved near-perfect classification, with only one false positive when 5 malicious nodes were present. For 10 and 15 malicious nodes, no false positives or false negatives were observed, demonstrating the model's consistent detection performance.

S.No	Malicious Nodes	TP	TN	FP	FN
I.	5	4	95	1	0
II.	10	10	90	0	0
III.	15	15	85	0	0

Table 3: Classification Results for a 100-Node MANET

V.I.III Scenario with 150 nodes

The proposed model was evaluated in a 150-node MANET to assess its performance under increased network complexity. As shown in Table 4, the model achieved high detection performance, with no false positives in any scenario. Only one false negative was observed when 15 malicious nodes were present, demonstrating the model's reliability and scalability.

S.No	Malicious Nodes	TP	TN	FP	FN
I.	5	5	45	0	0
II.	10	10	140	0	0
III.	15	14	135	0	1

Table 4: Classification Results for a 150-Node MANET

V.II DISCUSSION

V.II.I. Packet Delivery Rate

In order to calculate the packet delivery ratio (PDR), the total number of packets successfully received by the destination nodes np^i is divided by the total number of packets transmitted from the source nodes np^i . The Packet Delivery Rate is calculated using the equation 13.

$$PDR = \frac{\Sigma_{i=1}^{n} np_D^i}{\Sigma_{i=1}^{n} np_S^i} * 100 \qquad (13)$$

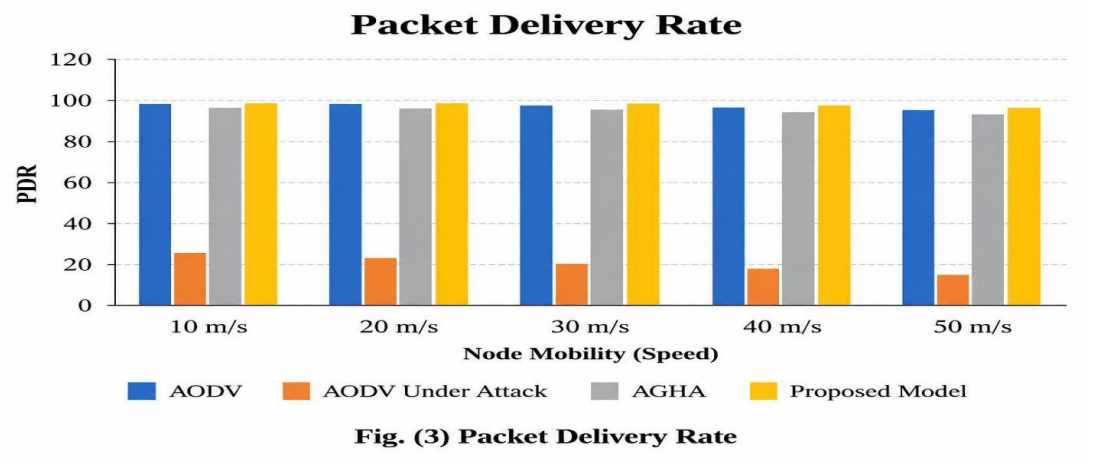

Fig. (3) Packet Delivery Rate

The results presented in Fig. 3 show that the average PDR of the standard AODV protocol is

approximately 97.51% across all mobility speeds. However, when Gray Hole attacks are introduced, the average PDR drops significantly to 22.34%, indicating severe degradation in network performance. The AGHA model achieves an average PDR of 96.21%, while the proposed model attains the highest average PDR of 97.57%.

Furthermore, the packet delivery ratio decreases gradually as the node mobility speed increases from 10 m/s to 50 m/s due to frequent route failures and rapid topology changes in MANET environments. At 10 m/s, the PDR values of AODV, AODV under attack, AGHA, and the proposed model are 98.8%, 25.8%, 98.1%, and 98.4%, respectively. At 50 m/s, these values decrease to 96.15%, 18.6%, 94.02%, and 96.7%, respectively. The results demonstrate that the proposed model effectively mitigates the impact of Gray Hole attacks and maintains reliable packet delivery even under high mobility conditions.

V.II. II Packet Loss Rate

Packet Loss Rate (PLR) represents the percentage of packets that fail to reach their intended destination. It is calculated by determining the difference between the total packets transmitted by the source node and the packets successfully received at the destination node, as given in Equations 14 and 15.

$$PLR = \frac{\sum_{i=1}^{n} (np_S^i - np_D^i)}{\sum_{i=1}^{n} np_S^i} * 100 \quad (14)$$

$$PLR = 100 - PDR \quad (15)$$

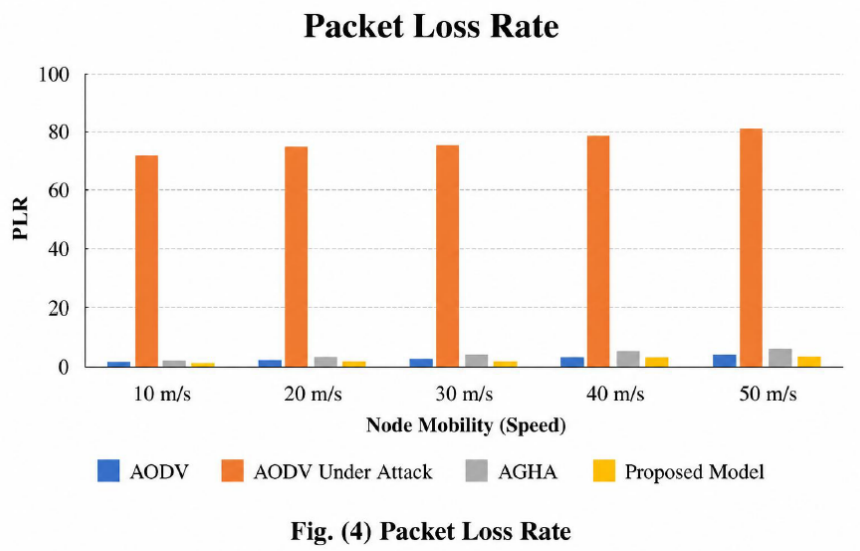

Fig. (4) Packet Loss Rate

The results shown in Fig. 4 indicate that the average PLR of the AGHA model is approximately 3.79%, whereas the proposed model achieves a lower average PLR of 2.43%. As node mobility increases from 10 m/s to 50 m/s, the packet loss rate increases because of frequent route breakages and dynamic topology changes. Nevertheless, the proposed model consistently outperforms AGHA by maintaining a lower packet loss rate at all mobility levels.

Specifically, at 10 m/s, the PLR is reduced from 1.90% in AGHA to 1.60% in the proposed model. Similarly, at 50 m/s, the PLR decreases from 5.98% to 3.30%. These findings indicate that the proposed detection framework successfully minimizes packet losses caused by malicious node activities and enhances overall network reliability.

V.II.III. Detection Accuracy

Detection Accuracy is used to evaluate the effectiveness of the anomaly detection mechanism in identifying both normal and malicious nodes. It is calculated as the ratio of correctly classified nodes (True Positives and True Negatives) to the total number of nodes in the network, as defined in Equation 16.

$$Detection\ Accuracy = \frac{(TP+TN)}{(TP+TN+FN)} * 100 \quad (16)$$

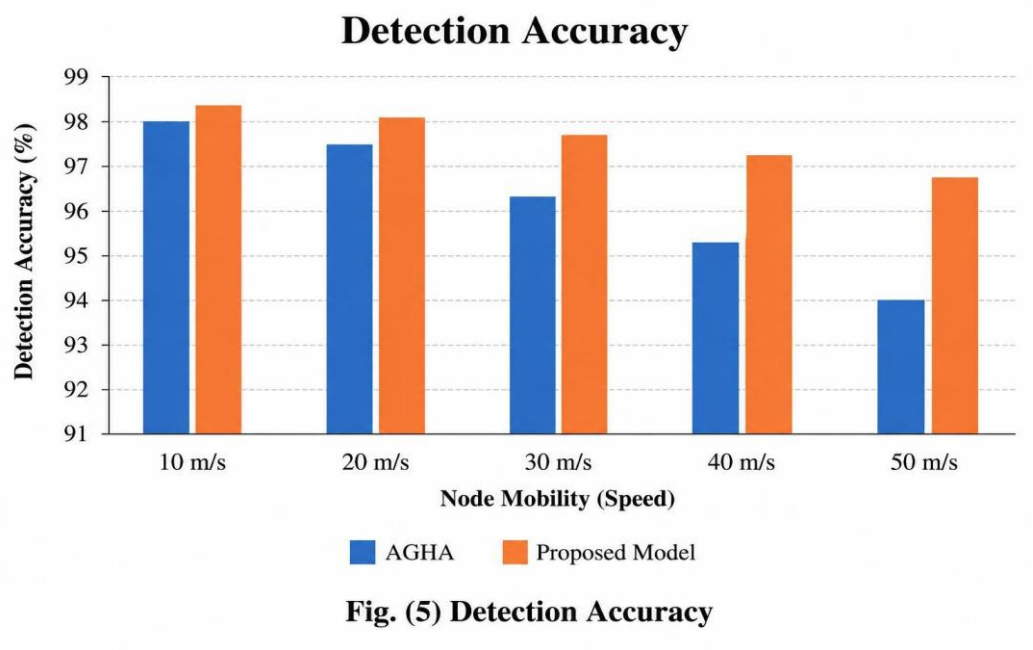

Fig. (5) Detection Accuracy

As illustrated in Fig. 5, the AGHA model achieves an average detection accuracy of approximately 96.28% across all mobility speeds. In comparison, the proposed model provides a higher average detection accuracy of 97.64%. Although the detection accuracy gradually decreases with increasing node mobility due to rapid topology variations and unstable routing paths, the proposed model consistently maintains superior performance.

At a mobility speed of 10 m/s, the detection accuracies of AGHA and the proposed model are 98.10% and 98.40%, respectively. When the mobility speed increases to 50 m/s, the detection accuracy decreases to 94.10% for AGHA and 96.80% for the proposed model. These results confirm the effectiveness of the proposed anomaly detection framework in accurately identifying Gray Hole nodes under varying network conditions.

V.II.IV Routing Overhead

Routing Overhead is defined as the ratio of the total number of routing control packets transmitted within the network to the total number of data packets successfully received at the destination nodes. It is calculated using Equation 17.

$$Routing\ Overhead = \frac{\sum_{i=1}^{n} CP_i}{\sum_{i=1}^{n} DP_i} \quad (17)$$

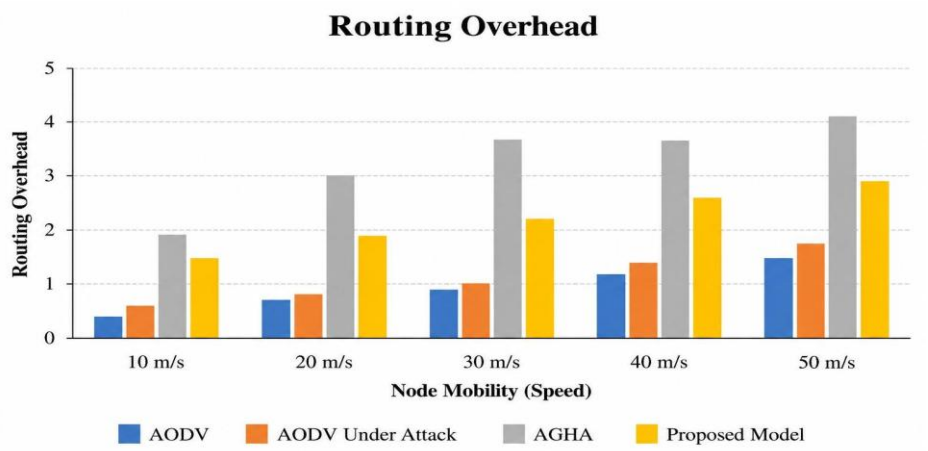

Fig. (6) Routing Overhead

The results presented in Fig. 6 show that the average routing overhead of the standard AODV protocol is approximately 0.89% for all mobility speeds. Under attack conditions, the routing overhead increases to about 1.08%. The AGHA model incurs a relatively higher average routing overhead of 3.25%, whereas the proposed model reduces the routing overhead to 2.18%.

Additionally, routing overhead increases as the node mobility speed rises from 10 m/s to 50 m/s due to frequent route discoveries, topology changes, and the transmission of additional control packets. At 10 m/s, the routing overhead values of AODV, AODV under attack, AGHA, and the proposed model are 0.35%, 0.52%, 1.85%, and 1.40%, respectively. At 50 m/s, these values increase to 1.40%, 1.72%, 4.10%, and 2.90%, respectively.

VI. Conclusion

This paper addresses the challenge of Grayhole attacks in Mobile Ad Hoc Networks and evaluates the capability of the proposed hybrid framework to detect and mitigate selective packet-dropping behavior. The simulation results confirm that the proposed approach can accurately identify malicious nodes while maintaining reliable and efficient network communication. The achieved Packet Delivery Ratio of 97.57%, detection accuracy of 97.64%, Packet Loss Rate of 2.43%, and routing overhead of 2.18% demonstrate a favorable balance between security performance and communication efficiency.

An important contribution of the proposed framework is its ability to improve the reliability of attack detection through multi-stage verification, thereby reducing false detections and strengthening confidence in malicious node identification. The findings show that combining complementary analytical techniques provides a robust mechanism for distinguishing malicious packet-dropping behavior from normal network variations in dynamic MANET environments.

Overall, the proposed work contributes to the development of more secure and reliable routing mechanisms for MANETs. The framework provides an effective foundation for future research on adaptive security solutions, particularly under larger network sizes, increased mobility, and more complex or multiple attack scenarios.

References

[1]. A. Moussaoui, F. Semchedine, and A. Boukerram. (2014). "A link-state QoS routing protocol based on link stability for mobile ad hoc networks", Journal of Network and Computer Applications. 39: 117–125.
[2]. Z. Ma, D. Zhang, J. Chen, and Y. Hou. (2017). "Shadow detection of moving objects based on multisource information in Internet of Things", Journal of Experimental & Theoretical Artificial Intelligence. 29(3): 649–661.
[3]. S. S. Tan, X. P. Li, and Q. K. Dong. (2015). "Trust-based routing mechanism for securing OLSR-based MANET", Ad Hoc Networks. 30: 84–98.
[4]. Z. Wei, H. Tang, F. R. Yu, M. Wang, and P. Mason. (2014). "Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning", IEEE Transactions on Vehicular Technology. 63(9): 4647–4658.
[5]. R. Lacuesta, J. Lloret, S. Sendra, and L. Peñalver. (2014). "Spontaneous ad hoc mobile cloud computing network", Scientific World Journal. 2014: 1–11.
[6]. S. Badiwal, A. Kulshrestha, and N. Garg. (2017). "Analysis of blackhole attack in MANET using AODV routing protocol", International Journal of Computer Applications. 168(8): 27–33.
[7]. A. Bhasin, S. Singh, and A. Kalia. (2020). "Energy conscious packet transmission in wireless networks using trust based

mechanism: A cognitive approach", in Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's. Cham, Switzerland: Springer. pp. 218–238.

[8]. F. H. Tsung, H. P. Chiang, and H. Chiehchao. (2018). "Blackhole along with other attacks in MANET: A survey", Journal of Information Processing Systems. 14(1): 56–78.

[9]. S. Singh, A. Bhasin, and A. Kalia. (2021). "Capitulation of mitigation techniques of packet drop attacks in MANET to foreground nuances and ascertain trends", International Journal of Communication Systems. 34(10): e4822.

[10]. S. Balaji and M. Rajaram. (2016). "SIPTAN: Securing inimitable and plundering track for ad hoc network", Wireless Personal Communications. 90: 679–699.

[11]. B. K. Tripathy, S. K. Jena, V. Reddy, S. Das, and S. Panda. (2020). "A novel communication framework between MANET and WSN in IoT-based smart environment", International Journal of Information Technology. 12(3): 809–818.

[12]. S. Gurung and V. Mankotia. (2024). "ABGF-AODV Protocol to Prevent Black Hole, Gray-Hole and Flooding Attacks in MANET", Telecommunication Systems. 86: 811–827.

[13]. T. N. Khosa, T. E. Mathonsi, and D. P. Du Plessis. (2023). "A model to prevent gray hole attack in mobile ad-hoc networks", Journal of Advances in Information Technology. 14(3): 535–541.

[14]. H. Khattak, F. Khurshid, and N. ul Amin. (2013). "Preventing black and gray hole attacks in AODV using optimal path routing and hash", in Proceedings of the 10th IEEE International Conference on Networking, Sensing and Control (ICNSC). pp. 645–648.

[15]. G. K. Wadhwani, S. K. Khatri, and S. K. Mutto. (2020). "Trust framework for attack resilience in MANET using AODV", Journal of Discrete Mathematical Sciences and Cryptography. 23(1): 209–220.

[16]. J. A. Josephine and S. Senthilkumar. (2020). "Tanimoto Support Vector Regressive Linear Program Boost Based Node Trust Evaluation for Secure Communication in MANET", Wireless Personal Communications.

[17]. N. Khanna and M. Sachdeva. (2020). "BEST: Battery, Efficiency and Stability based trust mechanism using enhanced AODV for mitigation of Blackhole attack and its variants in MANETs", Ad Hoc & Sensor Wireless Networks. 46(3/4): 215–264.

[18]. V. K. Kollati and K. Somasundaram. (2017). "IBFWA: Integrated bloom filter in watchdog algorithm for hybrid Blackhole attack detection in MANET", Information Security Journal: A Global Perspective. 26(1): 49–60.

[19]. O. Moradipour and M. Fathi. (2020). "An Anti-Gray Hole Attack Scheme in Mobile Ad Hoc Network", International Journal of Wireless Information Networks. 27(4): 558–567.

[20]. K. Ullah and P. Das. (2018). "Trust-based routing for mitigating Grayhole attack in MANET", in Proceedings of the International Conference on Computing and Communication Systems. Lecture Notes in Networks and Systems. Singapore: Springer.