Volume 10, Issue 9, September – 2025 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep900

Simulation of Gray Hole Attacks in MANETs Using NS2

Shalini Bhaskar Bajaj[1]

[1]Department of Computer Science and Engineering, Amity University Haryana, Gurugram, India

Publication Date: 2025/09/24

Abstract: The current era is defined by pervasive mobility, which significantly influences networking technologies. Evaluating new communication systems, particularly in terms of their reliability and adaptability within the Internet, has become a key focus for modern research. Thus, this area is focused on researchers to provide solutions for pressing challenges in Mobile Ad-Hoc Networks (MANETs). In this context, Mobile Ad Hoc Networks (MANETs) have emerged as a prominent area of study due to their decentralized structure and dynamic topology, making them suitable for environments lacking fixed infrastructure. However, these very characteristics also render MANETs highly vulnerable to security threats such as gray hole attacks. This paper investigates the impact of gray hole attacks on the Ad hoc On-Demand Distance Vector Routing (AODV) and Dynamic Source Routing (DSR) protocols. The results of these protocols were analyzed using the NS2.35 simulator on Ubuntu 22.04. A malicious node is introduced in the simulation, which initially behaves normally during route discovery but later drops data packets selectively. The study evaluates the effects of malicious node behavior on critical performance metrics such as packet delivery ratio, end-to-end delay and throughput. The findings underscore the susceptibility of DSR to such attacks and explore potential countermeasures to improve the security and robustness of routing in MANETs.

Keywords: *MANETs, AODV, DSR, Gray Hole Attack, NS2.*

How to Cite: Shalini Bhaskar Bajaj (2025) Simulation of Gray Hole Attacks in MANETs Using NS2. *International Journal of Innovative Science and Research Technology*, 10(9), 1392-1400. https://doi.org/10.38124/ijisrt/25sep900

I. INTRODUCTION

With the rapid evolution of wireless communication technologies, the concept of connecting devices without relying on fixed infrastructure has become increasingly practical. Mobile Ad Hoc Networks (MANETs) play a key role in realizing this vision, offering the flexibility to establish networks on-the-fly in remote, disaster-stricken, or military environments. MANETs consist of mobile nodes that communicate wirelessly in a self-organizing, infrastructure-less manner, making them ideal for scenarios where traditional networks are either unavailable or infeasible [1]. The dynamic and decentralized nature of MANETs, while advantageous, also exposes them to a wide range of security threats. One such threat is the gray hole attack, a type of insider attack where a compromised node initially behaves normally to gain trust but later begins to selectively drop data packets, disrupting communication in a stealthy manner. This unpredictability makes gray hole attacks difficult to detect and mitigate, posing a serious challenge to the reliability of routing protocols [2]. Routing in MANETs requires specialized protocols capable of handling frequent topology changes and intermittent connectivity. Among the reactive (on-demand) routing protocols, Dynamic Source Routing (DSR) is widely studied due to its ability to establish routes dynamically only when required, thereby reducing overhead. However, DSR's reliance on cooperative behavior among nodes makes it particularly vulnerable to attacks like gray hole, which exploit trust to degrade performance [3].

Detecting gray hole attacks in MANETs remains inherently complex due to their dual-phase behavior (legitimate participation followed by selective packet dropping) and dynamic network topologies. Unlike Blackhole attacks, which exhibit consistent malicious behavior, gray hole attackers strategically drop packets to evade detection while maintaining partial network functionality. Researchers have explored hybrid methodologies combining trust-based metrics (e.g., packet-forwarding ratios) and machine learning to distinguish erratic behavior from genuine node failures. Reputation-based systems, which track node collaboration and energy usage trends, help flag irregularities in cooperative conduct. However, the lack of centralized control infrastructure complicates continuous surveillance, requiring decentralized protocols that harmonize detection precision with resource efficiency [4].

Comparative studies between Blackhole and gray hole attacks reveal fundamental distinctions in operational impact and defensive approaches. While Blackhole assaults cause abrupt communication breakdowns by blocking all data, gray hole attacks erode network performance gradually, complicating their identification. Proposed DSR-specific countermeasures include enhanced route-discovery

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep900

protocols that authenticate paths via neighbor consensus or multipath verification, alongside cryptographic measures to block fake route replies [5]. Hybrid strategies, such as merging Ant Colony Optimization (ACO) with reputation tracking, show enhanced robustness by favoring routes with proven reliability. Nevertheless, achieving scalability and energy optimization persists as a hurdle in extensive or resource-limited network environments.

In this research, a gray hole attack is simulated in an AODV and DSR-based MANET using the NS-2.35 simulator on Ubuntu 22.04. A malicious node is introduced into the network, and its impact on critical performance metrics—packet delivery ratio, end-to-end delay, and throughput—is evaluated. The results offer insights into how gray hole attacks affect MANETs and highlight the need for robust security mechanisms. Furthermore, this study discusses potential countermeasures, such as Intrusion Detection Systems (IDS), to enhance routing protocol resilience.

By understanding the behavior and consequences of such internal threats, this work contributes toward the development of more secure and reliable communication in mobile ad-hoc environments.

➢ *Objectives*:

- To simulate a gray hole attack within a Mobile Ad Hoc Network (MANET) using NS-2.35 on Ubuntu 22.04 on AODV and DSR protocols.
- To assess the impact of the gray hole attack on crucial performance parameters including packet delivery ratio, end-to-end delay, and throughput.
- To investigate and suggest effective countermeasures that can enhance the security and resilience of the Dynamic Source Routing (DSR) protocol in the presence of such attacks.

➢ *The Subsequent Sections Follow this Structure:*

Section II reviews prior research on MANET vulnerabilities and gray hole attacks. Section III describes the simulation setup using NS-2.35 and the integration of a malicious node. Section IV presents results comparing normal and attack scenarios across key performance metrics. Section V concludes with findings, proposed countermeasures, and directions for future work.

II. RELATED WORK

Desanamukula et al. proposed a hybrid deep learning model integrating CNN, LSTM, and GRU architectures to enhance the detection of flooding attacks in MANETs, achieving high accuracy and improved network performance. The model leverages a novel DECEHGS optimization algorithm, combining Differential Evolution and Evolutionary Population Dynamics to enhance convergence and prevent local optima. Evaluated using MATLAB R2023a, the model demonstrates a 12% increase in packet delivery ratio and a 20% reduction in routing overhead. Despite its effectiveness, the approach faces challenges in computational complexity, real-world adaptability, and the need for continual retraining against evolving attack strategies [1].

Sharma proposed a survey emphasizing Gray-hole attacks as a significant security threat in MANETs, where selective packet dropping hampers data transmission. The study identifies vulnerabilities in widely used routing protocols like AODV and modified AODV due to their lack of built-in security mechanisms. To address this, an IDS-based technique is proposed, where each mobile node monitors network behavior by analyzing sequence numbers in RREQ and RREP packets. When a node's suspicious activity exceeds a defined threshold, it is isolated from the network to prevent further disruption [2].

Arega et al. conducted a performance analysis of MANET routing protocols AODV, DSR, and DSDV based on QoS metrics under varying network load and size. Their results indicated that DSR outperformed others in throughput, packet delivery ratio, and packet loss ratio under different node densities. DSDV performed better than AODV and DSR when considering large network sizes in terms of QoS delivery. The study suggested potential modifications to DSR and DSDV to enhance their efficiency in high-load and large-scale MANET scenarios [3].

Chowdari and Srinivas explored the challenges posed by Blackhole and gray hole attacks in Mobile Ad-hoc Networks (MANETs), noting that the lack of centralized control and constantly changing network topology make MANETs vulnerable to such denial-of-service threats. Their study highlights how these attacks severely degrade network performance by targeting the core aspects of security—integrity, confidentiality, and availability. They reviewed various existing methods aimed at detecting and minimizing the impact of malicious nodes, pointing out the strengths and limitations of each. The authors also emphasized the role of proactive and reactive routing strategies in enhancing route discovery and identifying abnormal node behavior, while encouraging further research to improve these mechanisms with fewer constraints [4].

Radha and Rao proposed the SDPEGH technique for detecting, preventing, and eliminating Gray Hole attacks in MANETs using the DSDV routing protocol, aiming to counter selective packet dropping. The method was implemented in NS-2 and evaluated through performance metrics such as Packet Delivery Ratio, throughput, security, and energy consumption. Their results demonstrated that SDPEGH outperforms existing techniques in terms of overall network performance and security. The study also suggested future work on evaluating gray hole impact across other routing protocols and additional performance metrics like delay and overhead [5].

Dipakkumar et al. conducted a simulation-based study analyzing the impact of gray hole attacks on AODV routing protocol in MANETs, where malicious nodes selectively drop data packets while falsely advertising optimal paths. They examined the nature of Gray Hole attacks, which are challenging to detect due to intermittent malicious behavior

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep900

and evaluated various detection techniques. Their results showed that such attacks significantly degrade network performance by reducing throughput and increasing end-to-end delays. The study also presented a comparative analysis of existing Gray Hole detection algorithms, highlighting their limitations like increased overhead and reduced speed [6].

The study by Behzad et al. emphasizes the severity of these attacks and proposes detection and defense mechanisms based on Round Trip Time (RTT) and Packet Forwarding Table (PFT) analysis. The proposed techniques evaluate the trustworthiness of nodes by monitoring packet delivery behavior and round-trip delays. These metrics help in identifying anomalies associated with packet dropping or route manipulation. Their simulations reveal that such strategies significantly improve network performance under attack, especially in terms of Packet Delivery Ratio (PDR) and throughput, while maintaining acceptable levels of end-to-end delay. The results also highlight that the defensive mechanisms become increasingly effective as the number of nodes grows and node mobility increases, showcasing their scalability and adaptability.

The integration of these defense techniques demonstrates that while standard protocols like AODV and DSR are vulnerable in their native form, their resilience can be substantially enhanced by embedding security-aware mechanisms. The proactive detection of malicious behavior through RTT and PFT not only mitigates the impact of Blackhole and gray hole attacks but also preserves critical performance metrics essential for the reliability of MANET applications. This underscores the need for incorporating lightweight, protocol-aware security extensions within the routing logic to ensure secure communication in decentralized and hostile network environments [7].

Weeks and Altun proposed an enhanced routing algorithm named Efficient Secure Dynamic Source Routing (ESDSR) to improve the performance of DSR in the presence of selfish or unreliable nodes in ad hoc wireless networks. Their approach modifies the traditional DSR protocol to detect nodes that deliberately drop packets to conserve their own resources and mitigate their impact on network performance. The ESDSR protocol incorporates mechanisms for identifying such selfish behavior and ensures more reliable routing paths by avoiding uncooperative nodes. Simulation results indicated a noticeable improvement in packet delivery ratios when using ESDSR compared to standard DSR. However, while the method strengthens packet transmission reliability, it focuses primarily on selfish behavior rather than targeted malicious attacks like gray hole or coordinated adversarial strategies, leaving scope for broader security enhancements and real-time adaptability in dynamic threat scenarios [8].

Raghu et al. proposed an Enhanced Dynamic Source Routing (DSR) protocol to analyze and mitigate black hole attacks in Mobile Ad Hoc Networks (MANETs) using NS2 by integrating a data control packet mechanism into the routing process. Their approach utilizes fake Route Request (RREQ) packets and monitors Route Reply (RREP) behaviors to detect malicious nodes that attempt to deceive other nodes by falsely advertising optimal paths and subsequently dropping or absorbing data packets. The proposed enhancement was evaluated based on key network performance metrics such as Packet Delivery Ratio, Throughput, End-to-End Delay, and Packet Drop Ratio, showing that the Enhanced DSR outperforms the traditional DSR in identifying and avoiding black hole nodes. The authors emphasized the importance of secure routing protocols in MANETs and introduced a node-based trust management scheme aimed at customizing trust metrics to improve routing decisions in dynamic and infrastructure-less network environments [9].

Verma and Barwar conducted a comparative performance analysis of the AODV and DSR routing protocols under blackhole and gray hole attacks in Mobile Ad Hoc Networks (MANETs) using NS2, focusing on critical metrics such as Packet Delivery Ratio, Average End-to-End Delay, and Average Throughput. Their study simulated Constant Bit Rate (CBR) traffic in various scenarios to evaluate how these protocols respond to security threats that involve malicious nodes dropping packets. The results revealed that AODV outperforms DSR in terms of packet delivery and throughput in both attack scenarios, while DSR exhibits higher end-to-end delay. However, both protocols showed slightly improved performance under grayhole attacks compared to blackhole attacks, highlighting the nuanced impact of different attack types on MANET routing efficiency [10].

Ourouss et al. proposed a Reputation-based Ant Colony Optimization Dynamic Source Routing (RACODSR) protocol to defend against smart gray hole attacks in Vehicular Ad Hoc Networks (VANETs), a subclass of MANETs, by enhancing secure route discovery within the DSR framework. Their approach incorporates realistic VANET mobility models, both with and without collision scenarios, generated using OpenStreetMap and SUMO, and simulated in NS2 to evaluate performance across metrics such as Drop Rate, Packet Delivery Ratio, Throughput, Jitter, End-to-End Delay, and Energy Consumption. The results demonstrated that RACODSR consistently outperforms the standard DSR protocol, even under challenging conditions involving smart gray hole attacks and vehicular collisions, by improving QoS metrics and reducing energy usage, thus highlighting its potential for enhancing road safety in intelligent transportation systems [11].

Khosa et al. proposed the GRAY-HP algorithm to effectively detect and prevent gray hole attacks in Mobile Ad Hoc Networks (MANETs) by integrating the Secure Detection Prevention and Elimination Gray Hole (SDPEGH) technique with a proactive scheme to improve node classification accuracy and maintain network performance. Recognizing the limitations of existing protocols in distinguishing between malicious and legitimate nodes, the authors designed GRAY-HP to eliminate gray hole threats while minimizing the false exclusion of innocent nodes. Simulated using NS2, the proposed algorithm demonstrated superior performance compared to Genetic Algorithm to Bacterial Foraging Optimization (GA-BFO) and Rough Set Theory (RSetTheory) in terms of throughput, packet delivery ratio, and routing overhead. The results showed that GRAY-HP increased

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep900

average throughput by approximately 90.9% and delivery ratio by about 89%, while reducing routing overhead by 5.7%, indicating its effectiveness in enhancing QoS and mitigating security threats in decentralized MANET environments [12].

Kumar et al. conducted a survey on advanced detection and prevention techniques for black hole and gray hole attacks in DSR and AODV routing protocols, focusing on their vulnerabilities in Delay Tolerant Networks (DTNs) due to limited connectivity and the risk of malicious nodes intercepting or dropping packets. The study reviewed existing methodologies aimed at ensuring secure data transmission by identifying and mitigating malicious behavior without compromising the routing path between source and destination nodes. Emphasizing the role of AODV in optimizing packet size and path selection, the survey compared various Wireless Sensor Network (WSN) approaches and concluded that the reliability of these protocols tends to improve as the number of participating nodes increases, highlighting the need for scalable and adaptive security mechanisms in MANET environments [13].

Mankotia et al. proposed a Dual Security Ad-hoc On-Demand Distance Vector (DS-AODV) protocol to combat both sequence number-based and smart gray-hole attacks in Mobile Ad Hoc Networks (MANETs) by incorporating two distinct security mechanisms during the route discovery and data transmission phases. The protocol addresses the limitations of single-layer defense strategies by integrating an intrusion detection system (IDS) that actively monitors neighboring nodes' behavior to detect malicious packet-dropping activities. Simulated in NS-2.35, the DS-AODV demonstrated enhanced performance compared to existing approaches, achieving a packet delivery rate of 98.20% and throughput of 19.73 kbps. The study highlighted that increasing IDS node coverage further improved network reliability and suggested future exploration of technologies like blockchain and deep reinforcement learning for more robust and intelligent MANET security solutions [14].

Hassan et al. conducted a comprehensive survey on enhancing intrusion detection in Mobile Ad Hoc Networks (MANETs) by leveraging advanced machine learning (ML) and optimization techniques. Their study emphasized the critical need for robust security mechanisms due to MANETs' vulnerability to attacks like blackhole and gray hole. They highlighted the effectiveness of Long Short-Term Memory (LSTM) networks and Federated Learning (FL) in improving detection accuracy and adaptability across distributed nodes. The authors also explored reinforcement learning and meta-heuristic algorithms for optimizing routing protocols and enhancing network resilience. Despite these advancements, challenges such as high computational costs, imbalanced datasets, and real-time detection difficulties persist. To address these issues, the study suggested implementing lightweight LSTM models, adaptive sampling, and cost-sensitive learning to enhance intrusion detection system performance in dynamic MANET environments [15].

Shafi et al. introduced the Machine Learning and Trust-Based AODV (ML-AODV) routing protocol to enhance security in Mobile Ad Hoc Networks (MANETs) against flooding and blackhole attacks. The protocol employs trust metrics—such as hop count, residual energy, and link expiration time—to assess node reliability, thereby preventing the propagation of unnecessary routing traffic caused by flooding attacks. To counter blackhole attacks, ML-AODV integrates an Artificial Neural Network (ANN) with a Support Vector Machine (SVM) classifier, facilitating the identification of malicious nodes and the selection of secure routing paths. Simulations conducted using the NS2 simulator demonstrated that ML-AODV outperforms both standard AODV and traditional trust-based AODV protocols, achieving higher throughput and reliability while reducing delay, routing overhead, and packet loss. This approach is particularly effective in semi-urban environments characterized by moderate node mobility and density [16].

Sarao evaluated the performance of the Ad hoc On-Demand Distance Vector (AODV) routing protocol in Mobile Ad Hoc Networks (MANETs) under various security attacks, specifically blackhole, gray hole, and rushing attacks. The research highlighted the inherent vulnerabilities of MANET routing protocols due to the lack of centralized control and infrastructure. Using the NS2 simulation tool, the study analyzed AODV's behavior across multiple network scenarios, varying parameters such as node density, mobility, and the number of malicious nodes. The findings indicated that blackhole and grayhole attacks significantly degrade AODV's performance, leading to reduced packet delivery ratio, lower throughput, and increased end-to-end delay. In contrast, AODV was found to be comparatively less affected by rushing attacks. These results underscore the necessity for enhanced security mechanisms in AODV-based MANETs to improve resilience against such attacks [17].

III. SIMULATION OF GRAYHOLE ATTACKS IN MANETS

Mobile Ad Hoc Networks (MANETs) are self-organizing, infrastructure-less networks that are increasingly deployed in critical real-world applications such as military surveillance and disaster management. However, their open and decentralized nature makes them highly susceptible to routing attacks. One such critical threat is the gray hole attack, in which a malicious node selectively drops packets after initially behaving correctly to gain trust. This disrupts communication reliability and severely impacts performance metrics such as packet delivery ratio and end-to-end delay. Two prominent routing protocols commonly used in MANETs are Ad hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR).

This research examines the impact of Grayhole attacks on MANETs by simulating the behavior of AODV and DSR routing protocols using NS2.35 on Ubuntu 22.04. The simulation environment was set up by writing custom TCL scripts to define network parameters such as node count, mobility, and traffic patterns. AWK scripts were also written to process the trace files and extract relevant performance metrics. A pre-existing C++ script within the NS2 framework was modified to enable accurate simulation and data extraction

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep900

relevant to the analysis of Grayhole behavior. For better visualization and analysis, Python was used to generate graphs depicting throughput and packet delivery ratio (PDR), allowing a clear comparison of the protocols under attack conditions.

➢ *Simulation using AODV Protocol*

AODV is a reactive routing protocol designed for MANETs that creates routes only when needed. It uses Route Request (RREQ) and Route Reply (RREP) messages for route discovery and maintains routes as long as they are required by the sources. When a source node needs to communicate with a destination, it broadcasts an RREQ. Intermediate nodes forward the request until it reaches the destination, which replies with an RREP. This protocol uses sequence numbers to ensure the freshness of routes and relies on hop-by-hop routing. AODV's on-demand nature makes it an appealing protocol in dynamic environments; however, its trust-based route discovery is vulnerable to malicious nodes. A Grayhole can exploit this by replying with fake RREP messages to insert itself into the path and then drop data packets. Studying AODV under attack helps analyze its limitations and resilience.

- *Protocol Modification***:** The AODV protocol source files, specifically aodv.cc and aodv.h, were modified to embed gray hole attack logic. The malicious behavior was implemented by altering the packet forwarding mechanism to selectively drop packets.
- *Simulation Environment Configuration***:** A simulation area of 800 m × 800 m was defined using **NS-2**. Nodes were deployed within this environment, and mobility was controlled using the Random Waypoint Model.
- *Attack Node Setup*: Node 1 was designated as the malicious gray hole node using Tcl scripting. This node responded to route request messages (RREQs) to get included in routes and then dropped data packets to simulate the attack.
- *Traffic Generation Constant Bit Rate (CBR):* Traffic was established between legitimate source and destination nodes to evaluate the impact of the attack on data transmission.
- *Performance Evaluation:* Performance metrics including Packet Delivery Ratio (PDR), Average Throughput, End-to-End Delay, and Routing Overhead were measured. These were computed using AWK scripts for post-simulation trace file analysis.

➢ *Simulation using DSR Protocol*

The Dynamic Source Routing (DSR) protocol is a reactive routing protocol tailored for Mobile Ad Hoc Networks (MANETs). DSR eliminates the need for periodic route advertisements by establishing paths only when required. Its operation revolves around two primary mechanisms: Route Discovery and Route Maintenance. When a source node intends to communicate with a destination and lacks a valid route, it initiates Route Discovery by broadcasting a Route Request (RREQ). Each intermediate node appends its address to the RREQ and forwards it until it reaches the intended destination. The destination responds with a Route Reply (RREP) that includes the entire path. Data packets are then transmitted with complete route information embedded in their headers, embodying a source routing approach.

While DSR's design is beneficial for highly dynamic networks, it is vulnerable to routing-based attacks such as the gray hole attack. In such an attack, a compromised node can deceive the route discovery process by falsely responding to RREQs, thus inserting itself into active routes. Once positioned, the attacker selectively drops data packets, disrupting communication without immediately revealing malicious behavior.

- *Protocol Modification:* To emulate the gray hole attack, the DSR implementation in NS-2 was altered by modifying the source files dsragent.cc and dsragent.h. The logic within the packet forwarding mechanism was adjusted to enable a designated node to intercept data packets and selectively drop them, thereby simulating the behavior of a gray hole attacker.
- *Simulation Setup:* The simulation was conducted within 800 m × 800 m area, using the NS-2 simulator. Nodes were distributed randomly within this area, and mobility patterns were introduced using the Random Waypoint Mobility Model, which allowed nodes to move independently, mimicking real-world conditions in a MANET.
- *Malicious Node Configuration:* Through Tcl script, Node 1 was configured as a malicious node. It was designed to send spoofed RREP messages in response to RREQs, misleading the source nodes into selecting routes that include the attacker. Once part of the routing path, the node dropped incoming data packets, thus executing the Grayhole attack.
- *Traffic Model (CBR):* The communication between non-malicious nodes was established using a Constant Bit Rate (CBR) traffic model to ensure consistent packet flow throughout the simulation. This helped in evaluating the network's performance both in normal and compromised conditions.
- *Evaluation Metrics:* Performance metrics including Packet Delivery Ratio (PDR), Average Throughput, End-to-End Delay, and Routing Overhead were measured. These were computed using AWK scripts for post-simulation trace file analysis.

These metrics enabled a comprehensive evaluation of the DSR protocol's behavior under adversarial conditions, offering insights into its robustness and vulnerability in the presence of malicious nodes

In summary, the gray hole attack was successfully simulated on both the AODV and DSR routing protocols using NS-2.35 by modifying their respective source files (aodv.cc, aodv.h, dsragent.cc, and dsragent.h). The simulation environment was configured with realistic mobility models and traffic patterns to closely reflect dynamic MANET conditions. A designated node was scripted to behave maliciously by exploiting the route discovery process and selectively dropping data packets. Through this setup, the

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep900

vulnerabilities of each protocol were exposed, enabling a detailed evaluation of their performance under attack. This simulation framework provides a solid foundation for analyzing and enhancing the security mechanisms of reactive routing protocols in MANETs.

IV. RESULTS

This research shows a comparative evaluation of the impact of the gray hole attack on two widely used reactive routing protocols—Ad hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR)—within a Mobile Ad Hoc Network (MANET). The simulations were conducted using NS-2.35 on Ubuntu 22.04, with six mobile nodes randomly deployed in an 800 × 800 m² area for 5, 10, 15, 20, 25 nodes network. In scenarios involving an attack, one node was configured to act as a malicious gray hole attacker, programmed to drop 50% of the data packets after route discovery to simulate selective forwarding behavior. To evaluate the effect of the attack, each protocol was tested under two conditions: a normal scenario without any attacker, and an attack scenario with the gray hole node active. All simulation parameters, including node movement patterns (based on the Random Waypoint model), mobility, and topology—were kept identical across both cases to ensure fair comparison. Constant Bit Rate (CBR) traffic was generated during the simulations. Key performance indicators such as the number of Packets Sent, Packets Received, Packets Dropped, Packet Delivery Ratio (PDR), Average End-to-End Delay, and Throughput were measured and extracted from the trace files using AWK scripts.

➢ *Performance of AODV*

- *Presence of Malicious Node as Attacker:* When subjected to the Grayhole attack, AODV's performance showed a consistent decline as network size increased. In the 5-node scenario, AODV managed to deliver 1,698 out of 2,103 packets, resulting in a PDR of 80.74% and a throughput of 260.11 Kbps. As the network expanded to 10 nodes, the impact of the malicious node was more pronounced, with a PDR dropping to 75.09% and throughput decreasing to 231.31 Kbps. In the 15-node network, the PDR further dropped to 69.08% and throughput to 223.231 Kbps. The 20-node setup experienced a more significant drop in performance, delivering only 1,372 out of 2,173 packets, resulting in a PDR of 63.14% and a throughput of 210.17 Kbps. Finally, the network configuration involving 25 nodes resulted in a PDR of 57.32% while a throughput of 191.6155 Kbps. These results reflect AODV's limited resilience to Grayhole attacks due to its dependency on single-route path selection, which becomes a point of failure when compromised.
- *Absence of Malicious Node:* Without the influence of any malicious activity, AODV displayed efficient and stable performance across various network scales. In the 5-node scenario, it successfully delivered all 2,507 packets with zero losses, achieving a perfect Packet Delivery Ratio (PDR) of 100% and a throughput of 384.038 Kbps. When scaled to 10 nodes, AODV continued to perform reliably, delivering 2,451 out of 2,528 packets, which resulted in a PDR of 96.95% and a throughput of 375.460 Kbps. In the 20-node configuration, a slight performance drop was observed with 432 packets lost out of 2,498 sent, leading to a PDR of 82.7% and a throughput of 316.482 Kbps. These outcomes highlight AODV's competence in maintaining reliable communication paths and handling increasing network sizes in secure environments.

➢ *Performance of DSR*

- *Presence of Malicious Node as Attacker:* DSR demonstrated comparatively better resilience than AODV under Grayhole attack conditions. In the 5-node scenario, 2,126 packets were transmitted with 1,746 successfully received, yielding a PDR of 82.13% and a throughput of 267.46 Kbps. In the 10-node network, performance remained stable with a PDR of 79.56% (1,662 out of 2,089 packets) and throughput of 254.60 Kbps. Expanding the network to 15 nodes led to a slight decrease in PDR to 79.58% and throughput to 255.996 Kbps. Even in the more extensive 20-node setup, DSR maintained a PDR of 78.94%, with 1,657 out of 2,099 packets delivered and a throughput of 253.83 Kbps. Continuing the trend, the 25-node network showed a PDR of 77.66% and a throughput of 248.096 Kbps. This consistent performance under attack highlights DSR's robustness, largely due to its source routing and route caching features that allow for dynamic path adjustments upon detecting route failure.
- *Absence of Malicious Node:* In the absence of a Grayhole attacker, DSR exhibited robust and consistent performance across all network sizes. In a 5-node configuration, the protocol delivered all 2,505 packets successfully with zero packet drops, resulting in a perfect Packet Delivery Ratio (PDR) of 100% and a throughput of 383.73 Kbps. In the 10-node setup, 2,468 out of 2,506 packets were received, leading to a high PDR of 98.48% and a throughput of 378.06 Kbps. The 20-node configuration achieved a PDR of 87.9% and a throughput of 337.162 Kbps, with 2,201 packets received out of 2,505 sent.

➢ *Performance Evaluation*

To evaluate the impact of Grayhole attacks, the AODV and DSR protocols were analyzed focusing specifically on two core performance indicators: the ratio of successfully delivered packets and the network's data transmission rate. The evaluation compares the behavior of both protocols in the presence and absence of malicious nodes. Below are the graphical representations of the performance of both protocols under varying network sizes and attack scenarios. Figure 1 presents the variation in packet delivery ratio with increasing number of nodes for both AODV and DSR protocols. It is observed that the PDR consistently declines as the number of nodes increases, with a sharper drop in scenarios involving malicious nodes. Notably, AODV demonstrates better resilience to Grayhole attacks compared to DSR, maintaining a relatively higher PDR even under attack conditions. The absence of malicious nodes results in significantly improved delivery ratios for both protocols, highlighting the impact of Grayhole attacks on network reliability.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep900

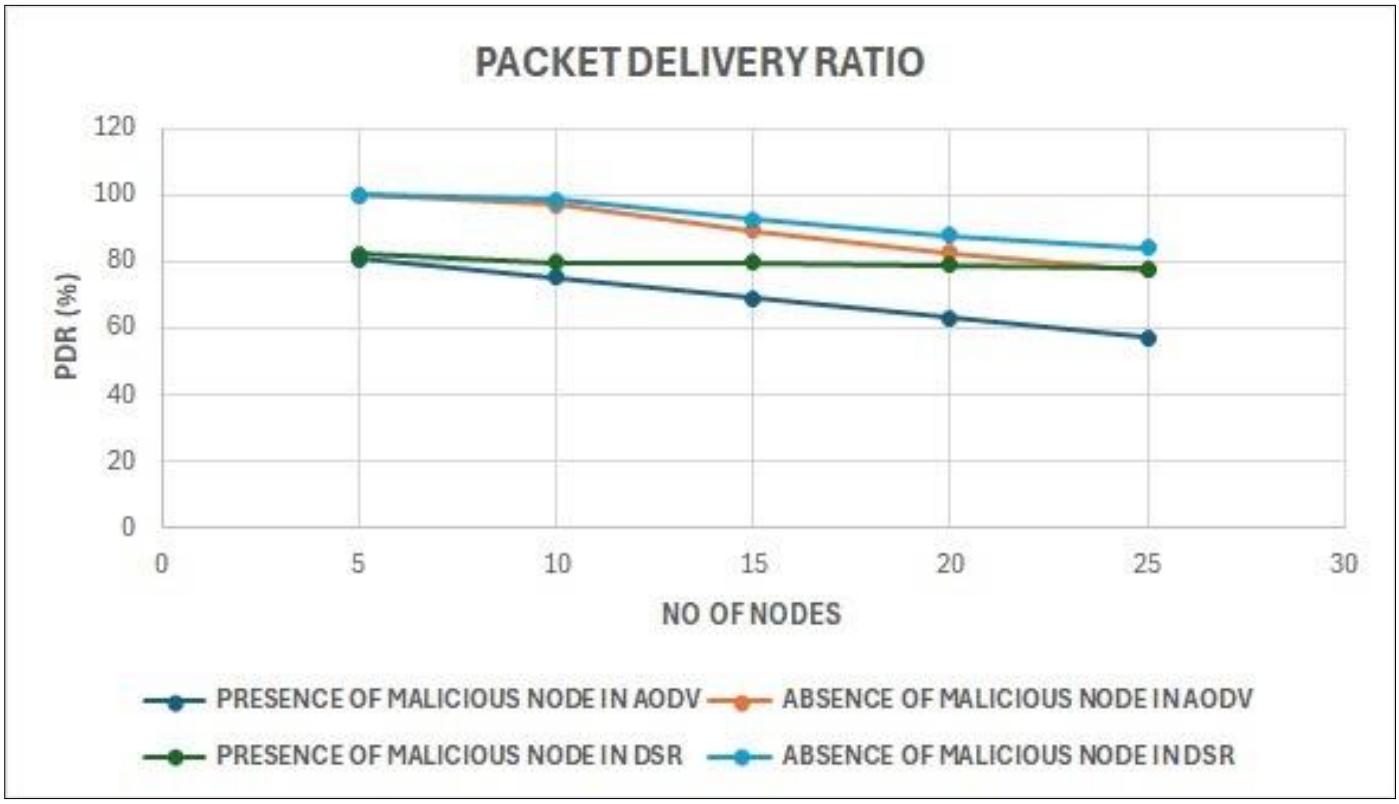

Fig 1 Packet Delivery Ratio Obtained in AODV and DSR Under Presence and Absence of Malicious Node

Figure 2 depicts the Throughput performance under the same conditions. The results reflect a pattern consistent with the PDR analysis, where throughput decreases with both the increase in node count and the introduction of malicious activity. AODV outperforms DSR in terms of throughput in both normal and attack scenarios. The reduction in throughput is particularly notable in DSR when exposed to Gray hole attacks, indicating a higher vulnerability to packet drops and route disruption.

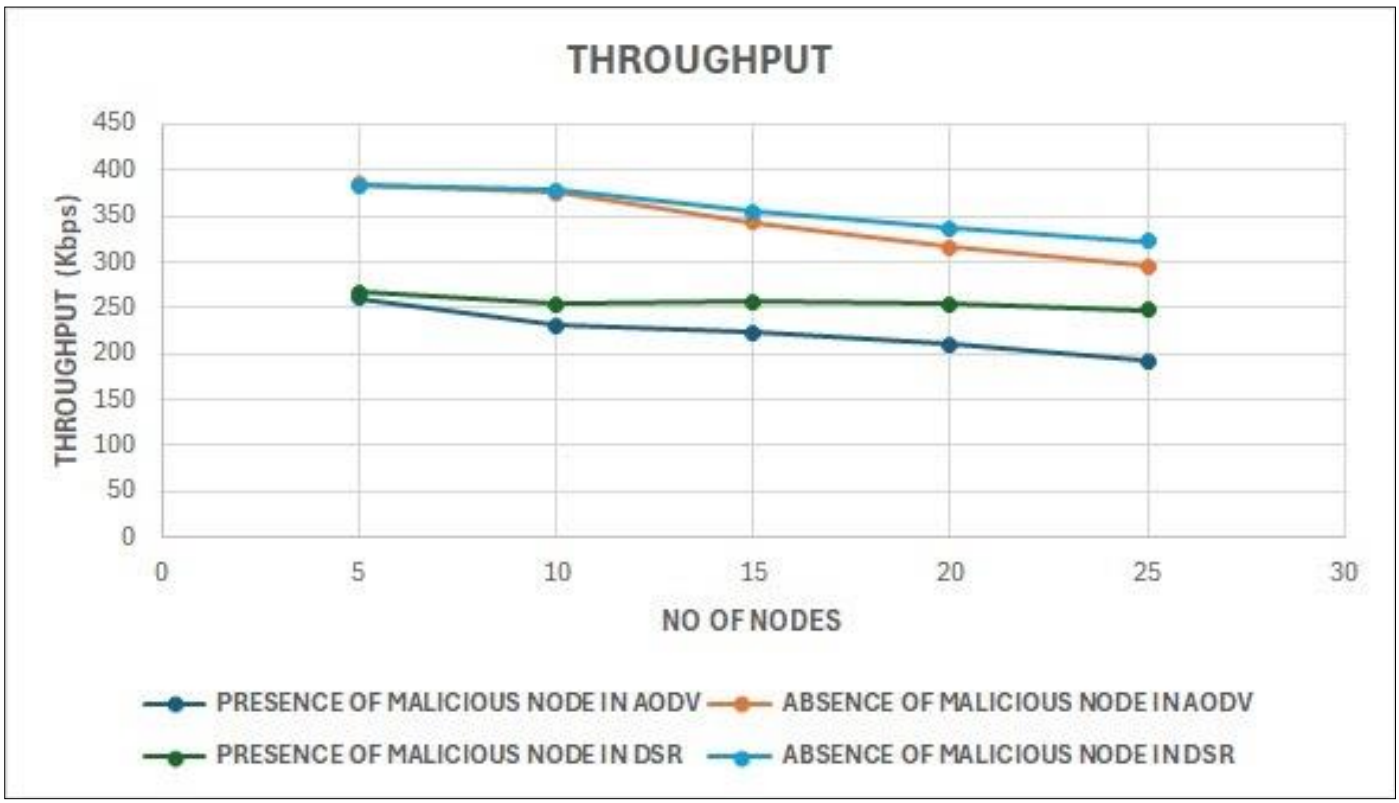

Fig 2 Packet Delivery Ratio Obtained in AODV and DSR Under Presence and Absence of Malicious Node

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep900

In conclusion, DSR consistently outperforms AODV under Grayhole attack scenarios due to its inherent design advantages. Unlike AODV, which relies on a single-route path that becomes vulnerable when compromised, DSR utilizes source routing and maintains multiple cached routes. This allows DSR to quickly adapt and reroute traffic when a malicious node is detected, minimizing packet loss and maintaining higher PDR and throughput. These dynamic routing capabilities enhance DSR's resilience against selective forwarding attacks like Grayhole, making it a more robust choice in hostile or compromised network environments.

➢ *Quantitative Summary*

To better understand the impact of gray hole attack on both the protocols, namely AODV and DSR, the PDR percentage and Throughput obtained is compared for different network configurations including 5, 10, 15, 20 and 25 nodes. The table below summarizes the data of packets sent, received and dropped for both the protocols in all the above-mentioned network configurations under the influence of a malicious node.

Table 1 Comparison of Performance of AODV and DSR Under Grayhole Attack

NO OF NODES	PROTOCOL	PACKETS SENT	PACKETS RECEIVED	PACKETS DROPPED	PACKET DELIVERY RATIO (%)	THROUGHPUT (KBPS)
5	AODV	2103	1698	405	80.74	260.11
	DSR	2126	1746	380	82.13	267.46
10	AODV	2011	1510	501	75.09	231.31
	DSR	2089	1662	427	79.56	254.6
15	AODV	2146	1482	664	69.08	223.231
	DSR	2107	1676	431	79.58	255.99
20	AODV	2173	1372	801	63.14	210
	DSR	2099	1657	442	78.94	253.83
25	AODV	2117	1213	904	57.32	191.6155
	DSR	2169	1684	485	77.665	248.096

The data in above Table indicates that DSR outperforms AODV across all parameters under the influence of a Gray hole attack. Although both protocols are adversely affected, DSR maintains better reliability, lower delay, and higher throughput. These findings highlight the advantage of source routing and cached route mechanisms in handling selective forwarding attacks in dynamic MANET environments

V. CONCLUSIONS AND FUTURE SCOPE

This research demonstrates the vulnerability of on-demand routing protocols like AODV and DSR to Gray hole attacks, wherein malicious nodes selectively drop packets to degrade network performance. By modifying the AODV and DSR protocol implementations in NS2, the study successfully simulated the erratic packet-dropping behaviors of gray hole nodes. The results, analyzed through trace files and visualized via NAM, revealed significant degradation in key performance metrics such as Packet Delivery Ratio (PDR) and throughput. The Packet Delivery Ratio was notably impacted due to the random dropping of packets by the malicious node, while the throughput and end-to-end delay statistics further confirmed the disruptive nature of the attack. This simulation reinforces the necessity of incorporating security-aware mechanisms within routing protocols, especially in dynamic and resource-constrained environments like mobile Ad-hoc networks (MANETs), where trust assumptions often fail.

Future research may focus on the integration of lightweight intrusion detection systems (IDS) with AODV and DSR to enhance their resilience against Grayhole and similar attacks. Investigating hybrid routing protocols that leverage the strengths of both AODV's efficiency and DSR's robustness could lead to more secure and adaptive solutions. Additionally, evaluating protocol performance under more complex and coordinated attacks—such as Blackhole, Wormhole, or Sybil attacks—and in dynamic network conditions involving mobility, energy constraints, and varying traffic loads would provide a more comprehensive understanding. The application of machine learning techniques for predictive and intelligent route selection also presents a promising avenue for improving secure communication in MANETs.

REFERENCES

[1]. D., P.K., Sandhya, E., Sk, K.S. et al. Enhancing security and efficiency in Mobile Ad Hoc Networks using a hybrid deep learning model for flooding attack detection. Sci Rep 15, 818 (2025). https://doi.org/10.1038/s41598-024-84421-0.

[2]. Sharma, R. (2016). Gray-hole Attack in Mobile Ad-hoc Networks: A Survey. International Journal of Computer Science and Information Technologies, 7(3), 1457-1460.

[3]. Arega, K. L., Raga, G., & Bareto, R. (2020). Survey on performance analysis of AODV, DSR and DSDV in MANET. Computer Engineering and Intelligent Systems, 11(3), 23-32.

[4]. Chowdari, R., & Srinivas, K. (2017). A survey on detection of Blackhole and Grayhole attacks in Mobile Ad-hoc Networks.

[5]. Radha, M., & Rao, M. N. (2019). Gray hole attack detection prevention and elimination using Sdpegh in Manet. International Journal of Engineering and Advanced Technology (IJEAT), 8(3).

[6]. Dipakkumar, J. S., Srivastava, A. K., & Vithlani, S. K. (2016, March). Simulation based study of gray hole

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep900

attack in MANET. In 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 3529-3534). IEEE.

[7]. Behzad, S., Fotohi, R., & Dadgar, F. (2015). Defense against the attacks of the black hole, gray hole and wormhole in MANETs based on RTT and PFT. *International Journal of Computer Science and Network Solutions (IJCSNS)*, *3*(3), 89-103.

[8]. Weeks, M., & Altun, G. (2006). Efficient, secure, dynamic source routing for ad-hoc networks. *Journal of Network and Systems Management*, *14*, 559-581.

[9]. Raghu, R., Nawaz, B., Sundar, S. S., Kumar, A. S., & Sivakumar, C. Enhanced DSR protocol to analyze black hole attack in MANETs using NS2. *academia. edu*.

[10]. Verma, M., & Barwar, N. C. (2014). A comparative analysis of DSR and AODV protocols under Blackhole and Grayhole attacks in MANET. International Journal of Computer Science and Information Technologies, 5(6), 7228-7231.Cormack, G. V., Lynam, T. R., & Riehle, D. M. (1998). Virtual reference collection: Model, recommendations, and implementation. Information Processing & Management, 34(3), 355-369.

[11]. Ourouss, K., Naja, N., & Jamali, A. (2021). Defending against smart grayhole attack within MANETs: A reputation-based ant colony optimization approach for secure route discovery in DSR protocol. Wireless Personal Communications, 116, 207-226.

[12]. Khosa, T. N., Mathonsi, T. E., & Du Plessis, D. P. (2023). A model to prevent gray hole attacks in mobile ad-hoc networks. Journal of Advances in Information Technology, 14(3), 532-542.

[13]. Kumar, T. A., Devi, A., Padmapriya, N., Jayalakshmi, S., & Divya, P. (2021). A Survey on Advance Black/Grey hole Detection and Prevention Techniques in DSR & AODV Protocols. International Journal on Wireless, Networking & Mobile Communication Innovations [ISSN: 2581-5113 (online)], 5(1).

[14]. MANKOTIA, V., Sunkaria, R. K., & Gurung, S. (2023). Dual Security Based Protocol Against Gray-Hole Attack in MANET. Adhoc & Sensor Wireless Networks, 56.

[15]. Hassan, S. M., Mohamad, M. M., & Muchtar, F. B. (2024). Advanced intrusion detection in MANETs: A survey of machine learning and optimization techniques for mitigating black/gray hole attacks. *IEEE Access*.

[16]. Shafi, S., Mounika, S., & Velliangiri, S. J. P. C. S. (2023). Machine learning and trust based AODV routing protocol to mitigate flooding and blackhole attacks in MANET. Procedia Computer Science, 218, 2309-2318.

[17]. Sarao, P. (2022). Performance Analysis of MANET under Security Attacks. *J. Commun.*, *17*(3), 194-202