Indian Journal of Computer Science and Technology
https://www.doi.org/10.59256/indjcst.20250401025
Volume 4, Issue1 (January-April 2025), PP: 166-170.
www.indjcst.com
ISSN No: 2583-5300

Secure Data Transmission Against Blackhole Attack in Manets

Kamaleshwaran M[1], Ramesh E R[2]
[1]M.sc, CFIS, Department of Computer Science Engineering, Dr. MGR University, Chennai, Tamilnadu, India.
[2]Assistant Professor, Center of Excellence in Digital Forensics, Chennai, Tamilnadu, India.

To Cite this Article: *Kamaleshwaran M[1], Ramesh E R[2], "Secure Data Transmission Against Blackhole Attack in Manets", Indian Journal of Computer Science and Technology, Volume 04, Issue 01 (January-April 2025), PP: 166-170.*

Abstract: *Blackhole attacks pose a significant threat to wireless networks by allowing a malicious node to falsely claim it has the most efficient route to the destination. Once data packets are routed through this node, it intercepts and discards them, resulting in data loss and network disruption. These attacks are particularly damaging in Mobile Ad Hoc Networks (MANETs), which are decentralized, self-configuring systems of mobile nodes that communicate wirelessly without fixed infrastructure. MANETs are widely used in applications requiring rapid and flexible deployment, such as military operations, disaster response, and remote communication. However, their open and dynamic nature makes them highly susceptible to security vulnerabilities. This research proposes a comprehensive system to ensure secure data transmission in MANETs by mitigating blackhole attacks. The solution includes detection techniques, which monitor packet forwarding behaviour and analyze route advertisements to identify malicious nodes, and prevention methods that incorporate trust-based routing and cryptographic mechanisms. The goal is to develop an efficient defense framework that enhances network reliability and security in dynamic, decentralized environments.*

Keywords: *MANETs (Mobile Ad Hoc Network), Blackhole Attack, AODV (Ad-hoc on-Demand Distance Vector), PDR (Packet Delivery Ratio), Discarding Data Packets, Secure Data Transmission.*

I.INTRODUCTION

Blackhole attacks represent a major security concern in wireless ad hoc networks. In such attacks, a compromised node falsely advertises itself as having the most efficient path to the destination, only to intercept and silently discard all received data packets. This not only leads to significant data loss but also disrupts the overall communication flow, causing a Denial of Service (DoS) within the network. These threats pose significant challenges in Mobile Ad Hoc Networks (MANETs), [1] which are decentralized and self-organizing networks composed of mobile devices that communicate through wireless connections. MANETs operate without any fixed infrastructure and are well-suited for applications requiring rapid and adaptable network deployment—such as military operations, disaster response, emergency communications, and scenarios in remote or hard-to-reach locations. However, their open and dynamic architecture makes them highly susceptible to various security vulnerabilities, including blackhole attacks.

This research aims to address these challenges by proposing a robust system for secure data transmission in MANETs. The proposed solution involves two major components: Detection Techniques: [3] Algorithms designed to detect malicious nodes by monitoring packet forwarding behaviour and identifying inconsistencies in route advertisements. Prevention Methods: [2] The development of secure routing protocols that incorporate trust-based mechanisms and cryptographic techniques to prevent untrusted nodes from participating in the routing process.

Additional measures include the use of multi-path routing 7to minimize data loss and ensure redundancy, as well as real-time anomaly detection to maintain secure communication even in highly dynamic environments. The scope of this research extends beyond simple detection, aiming to improve both network performance and security. Key research objectives include understanding the mechanisms of blackhole attacks, evaluating their impact on network behaviour, and designing efficient countermeasures. To support these goals, techniques such as the Watchdog Mechanism, [4] which observes neighbouring nodes for malicious behaviour, and Sequence Number Validation in protocols like SAODV [5] are integrated to strengthen the detection framework and enhance protocol resilience.

II.LITERATURE REVIEW

Y. Wang, J. Liu et al., [6] Hybrid Routing Protocols and Security Enhancements: Hybrid routing protocols that combine both proactive and reactive routing methods have been proposed to improve MANET security. These protocols allow dynamic route discovery while maintaining a balance between low overhead and high security. The addition of security enhancements, such as trust evaluation and multi-path routing, has shown to effectively prevent blackhole attacks by diversifying the paths used for data transmission.

Lidong Zhou; Z.J. Haas et al., [7] Cryptographic Approaches for Data Security: Cryptographic techniques, particularly symmetric encryption algorithms like AES (Advanced Encryption Standard), have been widely used to secure data transmission

in MANETs. These approaches ensure data confidentiality and integrity even in the presence of malicious nodes. Studies show that combining cryptographic methods with secure routing protocols can mitigate blackhole attacks while maintaining high data throughput and low delay.

Sayan Kumar Ray et al., [8] Trust-Based Secure Routing: Trust-based models have gained traction in MANET security research, focusing on evaluating nodes' trustworthiness based on their past behaviour. These models involve calculating trust scores based on packet forwarding success, route replies, and participation in the network. By ensuring that only trusted nodes participate in routing, these methods effectively prevent blackhole and other attacks. Researchers have demonstrated that trust-based routing significantly improves network reliability and security.

K. Sanzgiri; B. Dahill; B.N. Levine; C. Shields; E.M. Belding-Royer et al., [9] Blackhole Attack Detection Mechanisms: Blackhole attacks are a significant security threat in MANETs, where malicious nodes falsely advertise themselves as having the shortest path to the destination and drop all data packets. Various blackhole detection mechanisms have been proposed, such as monitoring the behaviour of nodes during route discovery and transmission phases. Algorithms based on anomaly detection and cross-checking packet delivery ratios have proven effective in identifying and isolating blackhole nodes.

Sergio Marti, T. J. Giuli, Kevin Lai, Mary Baker et al., [10] had proposed AODV-Based Secure Routing Protocols: Several studies have proposed modifications to the traditional AODV (Ad-hoc On-Demand Distance Vector) routing protocol to enhance security in MANETs. For instance, researchers have introduced trust-based approaches, where nodes monitor the behaviour of neighboring nodes and assign trust scores to ensure secure routing. These trust-based AODV variants have shown promise in detecting malicious nodes, including blackholes, by analyzing packet forwarding behaviour.[10]

Md Ibrahim Talukdar et al., [11] presented a denial-of service attacks like black hole attacks on general-purpose ad hoc on-demand distance vector protocol. It uses three approaches: normal AODV, black hole AODV, and detected black hole AODV, wherein we observe that black holes acutely degrade the performance of networks. We have detected the black hole attacks within the networks using two techniques: (1) intrusion detection system (IDS) and (2) encryption technique (digital signature) with the concept of prevention.

Muhammad Salman Pathan et al., [12] presented the AODV routing protocol is improved by incorporating an efficient and simple mechanism to mitigate black hole attacks. Mechanism to detect black hole attacks from MANET (MDBM) uses fake route request (RREQ) packets with an unreal destination address in order to detect black hole nodes prior to the actual routing process. Simulation experiment conducted has verified the performance of the proposed detection and prevention scheme.

III.PROPOSED METHODOLOGY

This research seeks to overcome the limitations of current solutions by offering a secure, scalable, and efficient framework. The proposed system incorporates sophisticated security mechanisms designed to detect, prevent, and mitigate blackhole attacks, thus ensuring secure and reliable data transmission in Mobile Ad Hoc Networks (MANETs). The design process of this solution involves addressing multiple aspects, each of which should align with the objectives the system aims to achieve. These aspects, such as compatibility, reliability, feasibility, user-friendliness, and security, must be met by every phase of the design. Constraints:

- Safeguarding sensitive data from malicious entities.
- Ensuring that users have confidence in the safety of their data.
- Detecting and preventing blackhole attacks in MANETs.
- The overall simulation is demonstrated using NS2.

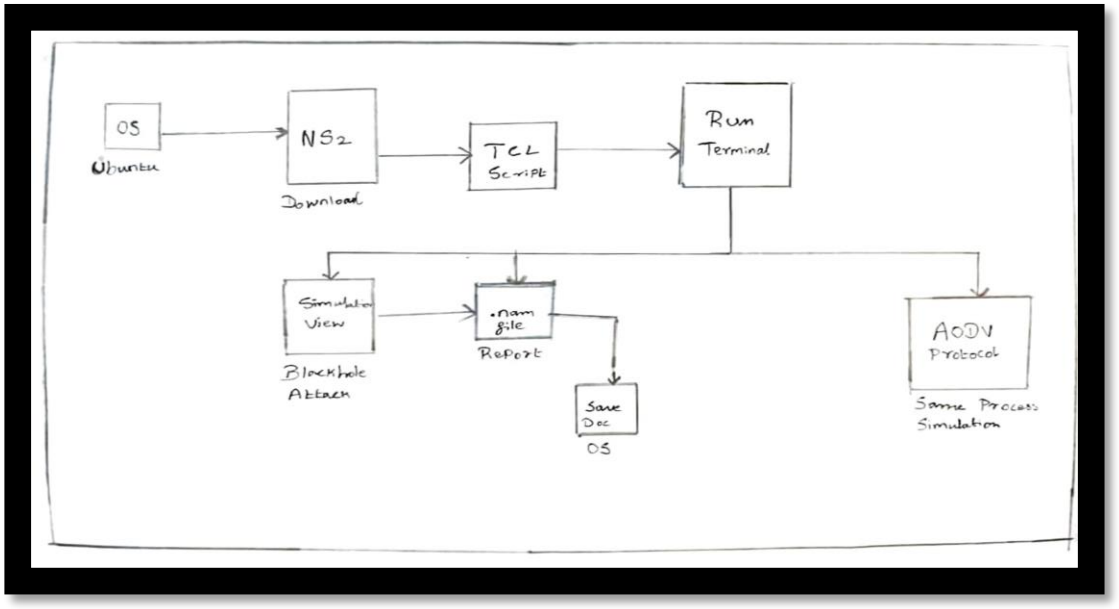

Fig 3.1: Architecture Diagram

This architecture diagram (Fig 3.1) illustrates the workflow of simulating a Blackhole attack. The process begins by opening the Ubuntu operating system, followed by installing Network Simulator version 2 (NS2). Next, a TCL script is written to simulate the Blackhole attack and the AODV protocol. Once the script is written, it is executed through the terminal, triggering the automatic launch of the network simulation animation. The simulation visualizes the Blackhole attack process and displays the results of the simulation. These results are automatically saved in the same directory where the TCL script is located. The same procedure is applied for simulating the AODV protocol.

Blackhole Attack

Network layer attacks generally serve two main purposes: either to prevent the forwarding of packets or to alter crucial data such as sequence numbers and hop counts [13]. In the case of a blackhole attack, a malicious node listens for the source or another node to broadcast a Route Request (RREQ) message into the network. Upon receiving this broadcast, the malicious node falsely claims to have a fresh route to the destination, typically by advertising the highest sequence number, and responds with a Route Reply (RREP) message. Once the source node receives the reply, it mistakenly assumes the reply came from a legitimate, trusted node, and begins forwarding packets toward the destination. Initially, the node may forward the packets correctly, but after some time, it begins to misbehave by dropping the packets consistently.

SAODV

In SAODV (Secure AODV), [15] the route discovery process is modified to support the finding of multiple secure routes to the destination instead of just one, with the RREQ messages allowing for multiple reverse routes to be created. The receive request method is adapted to accept RREQs with the same ID to establish multiple reverse paths, and the receive reply method is modified to accept multiple RREPs and create corresponding forward routes. These RREP packets are then forwarded to every reverse route to ensure reliable communication. The receive error method is updated to check if the node has an active alternate route, and if so, the RERR packet is not forwarded. The source node's route resolve method enables switching between active paths when one becomes insecure, and a route selector counter allows the source node to alternate between the best route and secondary routes for load balancing and redundancy. Security enhancements, such as digital signatures, hashes, and trust-based mechanisms, are incorporated to authenticate packets and prevent malicious activity like blackhole attacks, ensuring secure and reliable data transmission in MANETs

Network Simulator

Network Simulator (NS) [14] is an event-driven network simulation tool developed at the University of California, Berkeley. It incorporates a variety of network components, including protocols, applications, and traffic source behaviour. As shown in Figure 3.1: Network Simulator Architecture, NS-2 operates with a TCL script interpreter. To configure and run a simulation, the user writes a TCL script to trigger events; network objects and topology are set up using predefined functions in the NS library, which manages the start and stop of packet transmission through an event planner. The TCL script is interpreted by NS, which generates two primary analysis outputs: a Network Animator that visualizes the simulation process, and a trace file that records the behaviour of all simulated objects. These outputs are saved as files by NS, and the trace file data is processed using a GAWK script to calculate various performance metrics. The performance metrics help in analyzing and detecting the overall network behaviour during the simulation.

IV.FINDINGS

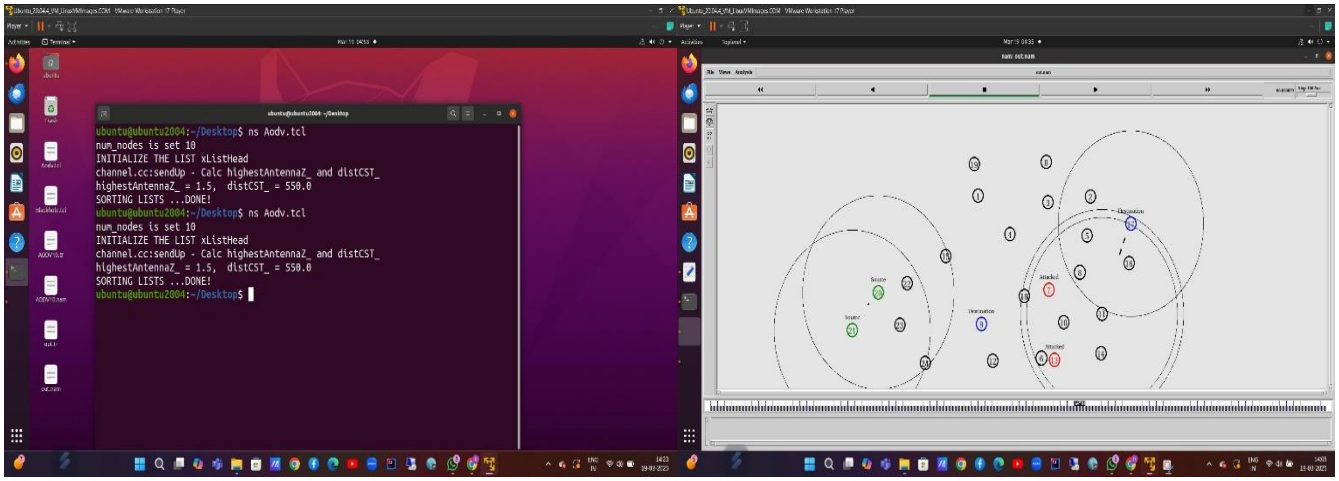

Fig 4.1: Run the TCL script *Fig 4.2: Blackhole Attack Simulation*

First I, Run the TCL Script of Blackhole attack visual with help of Network simulator version 2 in Ubuntu OS (fig 4.1), Then play the simulation of the blackhole attack in NS2 they will running in automatic (fig 4.2).

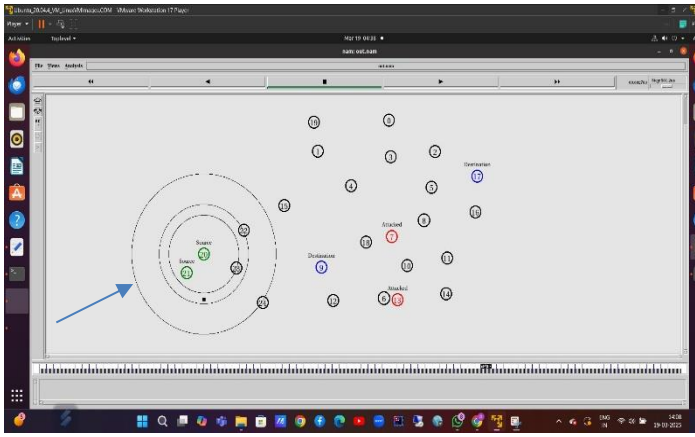

Fig 4.3: Packet dropping in simulation

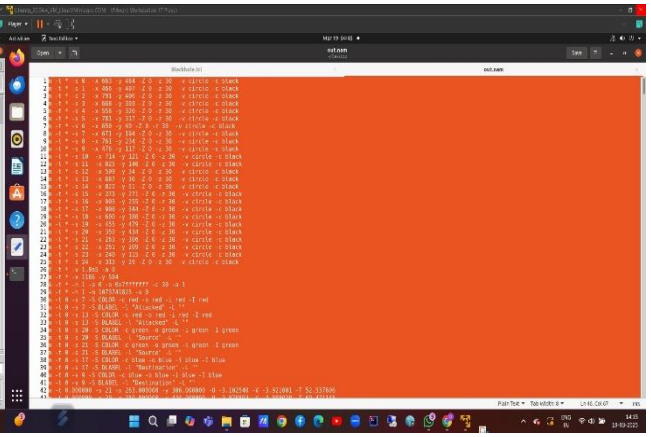

Fig 4.4: Result of Blackhole attack

The simulation during time attacker nodes are block the messages and dropping them in source node sides (fig 4.3), The simulation during they capture the time records and how many times packets are dropped in the simulation also show in the .nam file they are saved in same location of script file. (fig 4.4) This file saves the nodes travels speed and packet travels speed time also noted in the nam file.

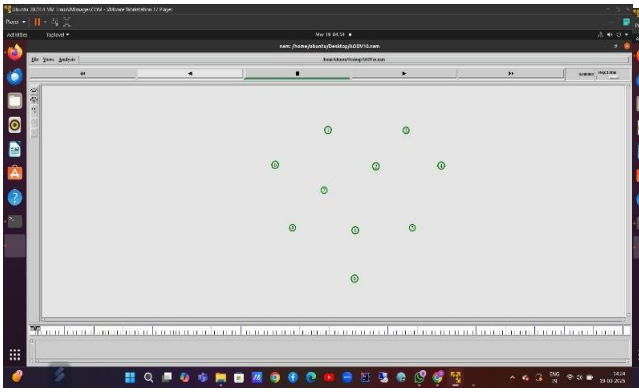

Fig 4.5: AODV network

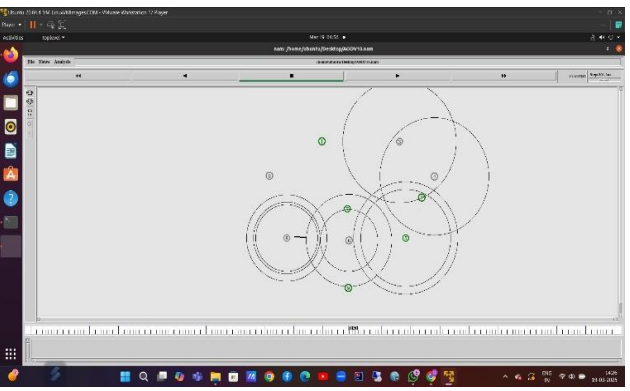

Fig 4.6: Result of AODV Routing

After seeing the Attack simulation, then we Run the prevention method of AODV protocol (fig 4.5), the simulation of AODV is "finding route to the destination" to "finding multiple routes" to the destination for send the data packets from source to destination in using RREQ and RREP for verify the nodes in the route path.

The Blackhole Attack are clearly proved in the Above Figures, Thats are clearly explain in the starting with script and run in the network simulations. The Above file of Nam file (fig 4.4) that's have Attack simulation running times and records of travels nodes. Then I run the AODV process in same of Network simulator that also same process of run the simulation that will show the how the packets are travels in the different routing paths. There are used for securely send the data packets in source node to destination node in MANETs network.

V.CONCLUSION

In conclusion, the proposed system for Secure Data Transmission in MANETs against Blackhole Attacks provides a highly effective solution for ensuring secure and reliable communication in decentralized, dynamic networks. By incorporating trust-based routing, encryption, and real-time anomaly detection, this system efficiently mitigates the impact of blackhole attacks, ensuring both data confidentiality and integrity. The mechanisms introduced, such as trust evaluation and blackhole detection, enhance the network's resilience by isolating malicious nodes and ensuring efficient data delivery. This approach not only strengthens the security of MANETs but also ensures that network performance remains optimal even in the face of adversarial attacks, making it a significant contribution to secure communication in mobile ad hoc networks.

Looking ahead, future work will focus on expanding the knowledge of MANETs and improving Routing Algorithms. This involves designing algorithms that use feedback from nodes about the behaviour of their neighbours, enabling dynamic route adjustments based on this information. Additionally, Periodic Network Monitoring will be implemented to regularly track network performance and node behaviour, allowing for the identification of anomalies that could signal a blackhole attack.

Reference

1. *Mobile Ad-Hoc Networks Applications and Its Challenges (2016), (Communications and Network) 08(03):131-136 Naeem Raza, Muhammad Umar Aftab, Muhammad Qasim Akbar, Omair Ashraf, doi:10.4236/cn.2016.83013*
2. *Blackhole Prevention Algorithms for AODV in Mobile Ad Hoc Network- A Review, Devottam Gaurav, Charu Wahi (2015) https://www.ijser.org/paper/Blackhole-Prevention-Algorithms-for-AODV-in-Mobile-Ad-Hoc-Network-A-Review.html*

3. *Khan, D., & Jamil, M. (2017). Study of detecting and overcoming black hole attacks in MANET: A review. 2017 International Symposium on Wireless Systems and Networks (ISWSN). doi:10.1109/iswsn.2017.8250039*
4. *IBFWA: Integrated Bloom Filter in Watchdog Algorithm for hybrid black hole attack detection in MANET, Vijaya Kumar Kollati & Somasundaram K, Pages 49-60, Published online: 17 Feb 2017 https://doi.org/10.1080/19393555.2016.1274805*
5. *SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack Publisher: IEEE, Songbai Lu, Longxuan Li, Kwok-Yan Lam, Lingyan Jia. 2009 International Conference on Computational Intelligence and Security, doi: 10.1109/CIS.2009.244*
6. *Secure Routing for Mobile Ad hoc Networks, Panagiotis Papadimitratos, Zygmunt J. Haas, Cryptography and Security (cs.CR), https://doi.org/10.48550/arXiv.2403.00404, Y. Wang, J. Liu, "Hybrid Secure Routing in Mobile Ad Hoc Networks," 2024.*
7. *"Securing ad hoc networks" Lidong Zhou; Z.J. Haas Published in: IEEE Network (Volume: 13, Issue: 6, Nov.-Dec. 1999) Page(s): 24 – 30, DOI: 10.1109/65.806983*
8. *GradeTrust: A secure trust based routing protocol for MANETs, Sayan Kumar Ray, doi:10.1109/ATNAC.2015.7366790, Conference: 25th International Telecommunication Networks and Applications Conference (ITNAC)*
9. *A secure routing protocol for ad hoc networks, Publisher: IEEE, K. Sanzgiri; B. Dahill; B.N. Levine; C. Shields; E.M. Belding-Royer, doi:10.1109/ICNP.2002.1181388*
10. *Mitigating routing misbehaviour in mobile ad hoc networks, Sergio Marti, T. J. Giuli, Kevin Lai, Mary Baker, https://doi.org/10.1145/345910.345955*
11. *Md Ibrahim Talukdar, Rosilah Hassan, Md Sharif Hossen, Khaleel Ahmad, Faizan Qamar, and Amjed Sid Ahmed "Performance Improvements of AODV by Black Hole Attack Detection Using IDS and Digital Signature" Hindawi Wireless Communications and Mobile Computing Volume 2021 Page: 1-13.*
12. *Muhammad Salman Pathan 1, Jingsha He 2, Nafei Zhu 3, Zulfiqar Ali Zardari 4, Muhammad Qasim Memon 5, Aneeka Azmat 6 "An Efficient Scheme for Detection and Prevention of Black Hole Attacks in AODV-Based MANETs" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 10, No. 1, 2019, Page: 243-251.*
13. *Analysis of Blackhole Attack in AODV and DSR Niranjan Panda, Binod Kumar Pattanayak, International Journal of Electrical and Computer Engineering (IJECE) Vol. 8, No. 5, October 2018, pp. 3093~3102 ISSN: 2088-8708, DOI: 10.11591/ijece.v8i5.pp.3093-3102*
14. *The Network Simulator NS 2, Home page. P_agina principal. http://www.isi.edu/nsnam/ns/*
15. *Xiaoxia Qi1, Qijin Wang and Fan Jiang "Multi-path Routing Improved Protocol in AODV Based on Nodes Energy" International Journal of Future Generation Communication and Networking Vol. 8, No. 1 (2015).*