International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 08 Aug. 2024, pp: 386-395 www.ijaem.net ISSN: 2395-5252

An Optimized Mechanism to Detect Black hole Attack in Manet (OMDBM)

[1]Babangida Abubakar Albaba, [2]Umar Barau Sani
[1][2] Department of Computer Science, Umaru Musa Yaradua University Katsina

Date of Submission: 15-08-2024 Date of Acceptance: 25-08-2024

ABSTRACT: Mobile Ad-hoc Networks (MANETs) is one of the applications of wireless technology. The mobile ad-hoc network has emerged as a critical communication technology in fields such as military defence networks, rescue operations command centres, automotive networks, and so on. This research studies a Mechanism to Detect Black Hole Attacks from MANET (MDBM) to optimize the security function for multiple attacks simultaneously. The proposed Optimized Mechanism to Detect Black Hole Attacks in Manet (OMDBM) improves Packet Delivery Ratio (PDR), End-to-End Delay (ED), and Network Throughput (NT) against black hole, gray hole, and wormhole attacks in MANETs by combining two methods for malicious node detection in the network, which are packet drop threshold and RTT calculations. In addition, the OMDBM also provides efficient communication between source and destination in which the packet loss decreases as the network size increases. In the proposed scheme, packet drop ratio, ED, and Network throughput metrics were utilized to measure the performance of the proposed system. The results show that the proposed method consistently demonstrates higher throughput compared to the existing system, highlighting its efficiency and robustness in handling increased network traffic while maintaining security against various attacks.

KEYWORDS: Mobile ad hoc network; black hole,gray hole, wormhole, andAD-hoc on-demand distance vector

I. INTRODUCTION

Wireless technology is an alternative to traditional wired technology which is often used for connecting devices wirelessly. Wireless transmission is the exchange of data over a distance without a physical channel, It also provides a solution to the long-range transmission that is expensive to implement using a wired connection, It also offers connections to the Internet and Intranet using the least radio waves [1]. Wireless is the collection of nodes with radio devices that can send and receive data packets in multi-hop and route data packets through its closest nodes in which data is transmitted between sender and receiver [2]). The Mobile Ad-hoc Network (MANET) is one of the applications of wireless technology. It is an un-centralize network where nodes can communicate with each other wirelessly [3], These networks act in the absence of any exterior router for managing connection, the node serves as the router for packet forwarding or routing [4]. It is a self-organized and un-static network with many transferable materials [5]. It also has an autonomous structure where every node is moving freely in any direction in the network [6]

The structure of this network makes security an area of focus for researchers, security is one of the most vital and considerable issues in any communication, Mobile ad-hoc Network (MANET) inclusive. Nowadays, most of our communication is done wirelessly, which makes security extremely important to prevent and protect our packets from various types of attacks such as black hole attacks, wormhole attacks, jellyfish attacks, gray hole attacks, etc.

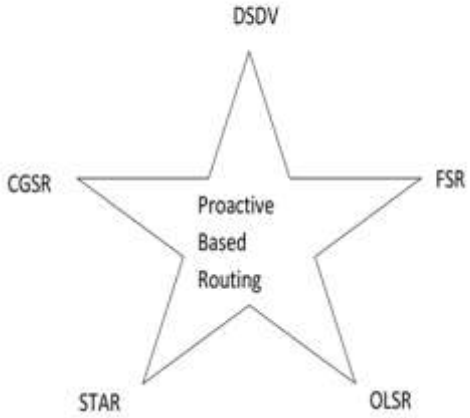
II. INTRODUCTION

Routing protocols used to handle the communication of nodes in an Ad-hoc network by helping the nodes to find routes required to get to their destinations which are:

1) Proactive Routing Protocol: Every node in the routing table data structure is maintained the table is updated with the latest information and every node has route information to every other node.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 08 Aug. 2024, pp: 386-395 www.ijaem.net ISSN: 2395-5252

TYPESOF PROACTIVE ROUTING PROTOCOL [10]



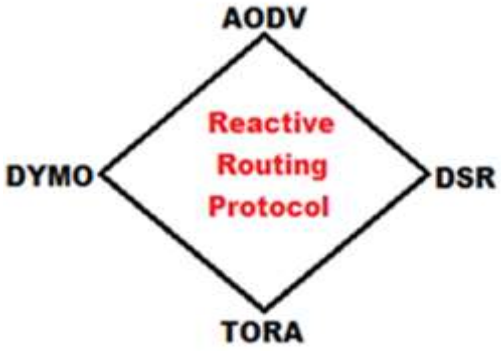
a. Optimized Link State Routing Protocol (OLSR): This is based on two topology management mechanisms: neighbourhood detection and neighbourhood sensing. HELLO, TC, MID, and HNA are four types of control messages used by the OLSR protocol to utilize both of these processes. HELLO packets are also used by the OLSR protocol for neighbourhood sensing. To scatter the TC packets, optimum dissemination or MPRs are used to communicate the topological data. The TC messages are a set of connections that are used to manage the OLSR protocol's packets in the vicinity of network nodes.
b. Dynamic Sequence Distance Vector (DSDV): This is a proactive protocol that assures loop-free routes and is based on the Bellman-Ford algorithm. The distance vector shortest path routing algorithm is used to pick a single path to a destination. Each node exchanges its neighbour (routing) table with its neighbours regularly. Two types of update packets are utilized to limit the amount of overhead transferred across the network. Full dumps and incremental packets are the terms for them.

2) Reactive Routing Protocol: In this protocol, paths are set up from source to destination if they are needed and are maintained until data is transmitted. There are various types of reactive routing protocols and the most common ones are Adhoc On-demand Distance Vector (AODV) which is our main concern.
a. Ad-hoc On-demand Distance Vector (AODV): Is a routing protocol that provides a route between both source and destination for intended devices as needed by a broadcasting route request message (RREQ) and route replay message (RREP) for both source and destination respectively.

b. Dynamic Source Routing Protocol (DSR): This is a MANET-optimized reactive routing mechanism. Route Discovery and Maintenance are the two aspects of DSR. Because the process of determining a path is only performed when a node requests it, the protocol is also known as On-Demand Routing. The routing information is sent from the source nodes to each node's cache route in DSR. While sending data, the source node checks the route cache for a valid destination route, and if none is found, it begins the route discovery process by broadcasting route request (RREQ) packets; if the node finds a valid route to its destination and receives these RREQ packets, a route from the source to its destination is established.

3) Hybrid Routing Protocol: It is a mix of proactive and reactive protocol techniques in which the best features of both earlier protocols are combined to create an immediate reactive neighbourhood with proactive connections up to a certain distance. A reactive evaluation is carried out if an application wishes to send packets to a node outside of this zone. This makes all paths inside a node's coverage region available right away. Routing tables in conjunction with root nodes are used to develop proactive routing protocols at first. If a node discovers that it doesn't know how to go to the source nodes' destinations, it will use the reactive routing strategy to find out.

TYPES REACTIVE ROUTING PROTOCOL [10].



III. RELATED WORK

Goswami and Wadhwa (2019) Proposed an improved AODV Protocol for Congestion Control in MANET Using Cryptography Technique, it's an improvement of AODV Protocol for congestion control. it also provides a solution against active attacks by checking the route with the least possibility of error or congestion during transmission within the community. It also used the

techniques of the multi-path protocol by declaring multiple routes from source to destination and sending a DESK-encrypted message to the next node and direct destination path established, then followed by RREQ and waiting for the RREP message before continuing with forwarding packets. The network performance improved in terms of throughput and packet delivery ratio [3].

Shashwat et al., (2017) Proposed a Modified AODV Protocol for preventing black hole attacks in MANET. The enhancement in AOVD is done by providing significant security against black hole attacks, in which the network performance increases on throughput and packet loss. Where IDS is used to prevent genuine nodes and also Manage the RQ Table and SN Table. [4].

Jatothu and Singh (2017) An Efficient routing and High-Security transmission Using AODV and Distributed Protocol key generation with dual RSA. The proposed AODV- DRSA-QC provides high security against the black hole attack which will announce the appearance of an attack on the other node in the network, the security solution is done with the aid of quantum cryptography and dual RSA. hence the AODV-DRSA-QC techniques came up with greater performance compared to AODV-QC in the network in terms of energy consumption, dead node, and alive node [5].

Goswami et al., (2020) based on Blackhole Attack Detection in MANETs Using Trust-Based Technique. As the researcher stated the Proposed method brings better results than traditional AODV and B-AODV by Securing the network from black hole attacks and also gives the other nodes the ability to rectify the malicious node themselves. The S_AODV improves the network performance in terms of throughput, packet delivery ratio, and End-to-End delay. [11].

Varshney and Sagar (2018) is an Improved AODV Protocol to Detect Malicious Node in Ad-hoc Networks. The researchers stated that the Security mechanism of AODV has been improved in the network by providing a solution against black hole and gray hole attacks using the RSA key exchange algorithm to share a private key between both the source node and the destination node that will be encrypted or decrypt by each. In which the network performance increased in terms of packet delivery ratio and throughput. [12]

Gnanaselvi et al., (2019) Proposed Secured Packet Transfer Using HASME for AODV Protocol to Detect Black Hole Attack and Gray Hole Attack. The proposed HASME (Hybrid Algorithm for Secure MANET Environment) could be able to detect black hole and gray hole attacks in the network by integrating the Two Fish Algorithm with the SHA-512 Algorithm. also, the proposed method has secured encryption methods that are commonly used to detect various black hole and gray hole attacks in the network. the network performance increased on throughput, packet loss, packet delivery ratio, and end-to-end delay, hence the packets are transmitted securely using a non-malicious node. [13]

Harikrishnan, et al., (2019) Proposed Gray Hole Attack Minimization for Ad-hoc Network Using Contradiction. The proposed method provides a security solution to the network like MANET, loT, and VANET for detecting gray hole attacks using BFST (Breadth-First Search Tree) and MST (Minimum Spanning Tree) in which the attacker will be detected also the algorithm can find the shortest path in the network by dropping the path to the attacker if detected [14].

Yaday and Upadhyay (2016) Proposed A Common Architecture for the Detection and Prevention of Black Hole Attack and Worm Hole Attack in MANET. The proposed algorithm provides a solution to the network by detection and prevention of both black hole attack wormhole attacks at a time by combining two methods for malicious node detection in the network, which are packet drop threshold and RTT calculations. It also provides efficient communication between source to destination in which the proposed architecture improved an End-to-end delay, Packet delivery ratio, and Throughput compared to traditional AODV [15]

Muhammad et al., (2019) proposed a Mechanism to Detect Black hole attacks in MANET MDBM, the authors introduced a simple and innovative mechanism for detecting the black holenodes in AODV-based MANETs by using fake RREQ packet to bait the black hole nodes during early stages. This scheme was verified and implemented on the AODV protocol. As the proposed scheme doesn't generate any extra control packets or any mathematical calculations during routing, the results of the simulations reveal that the performance of the proposed scheme is very similar to the native AODV in terms of delay [7].

Security is the most critical issue to address to have more efficient and reliable data exchange over the network due to the nature of the Mobile Ad-hoc Network (MANET). When communication happens between two nodes, the malicious node provides false identification; therefore, security is the trustworthy data transfer over the network. The attackers are concentrating their efforts on routing protocols. There are other routing protocols, but the most prevalent is the Ad-hoc On-Demand Distance Vector (AODV)

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 08 Aug. 2024, pp: 386-395 www.ijaem.net ISSN: 2395-5252

protocol, which is the focus of our investigation. In terms of Ad-hoc On-Demand Distance Vector (AODV) security, the bulk of the algorithms most critical issue to address to have more efficient and examined are incapable of addressing three attacks at once, and only a few are capable of addressing two attacks at once. The primary goal of this research is to create hybrid algorithms that will address three attacks at the same time.

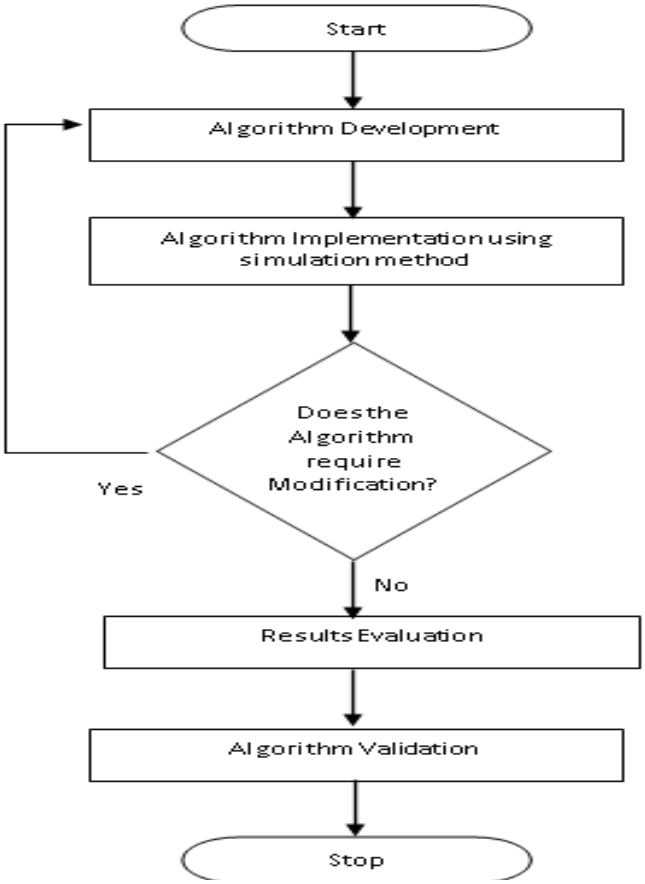
IV. PROBLEM FORMULATION

Despite researchers' efforts to identify and address security gaps in Mobile Ad-hoc Networks (MANETs), many challenges remain, particularly concerning gray hole, black hole, and wormhole attacks. Most studies focus on mitigating one or, at most, two types of attacks simultaneously. With the increasing demand for high-speed networks, secure data transmission, and the proliferation of communication devices, the security of data exchange between heterogeneous devices becomes a critical issue in MANETs. Therefore, our primary objective is to enhanced the security of MANETs by optimizing the Mechanism to Detect Black hole attacks in Manet (MDBM) based on the Ad-hocOn-demand Distance Vector (AODV) protocol. This optimization aimed to address multiple attacks simultaneously, thereby improving overall network security.

V. RESEARCH FRAMEWORK

The framework of the enhanced algorithm is presented in this section as a form of chart in Fig. 3. the optimization starts by developing the MDBM algorithm, then the algorithm is simulated, and after that, the algorithm is implemented, after the implementation a decision is made either evaluating the results or modifying the existing algorithm, and then evaluating the results of the algorithm. Finally, validating the algorithm. phases of the optimized algorithm required to perform the simulation experiment.

FRAME WORK OF THE OPTIMIZED MODEL



VI. DETAILED STAGES OF THE PROPOSED MECHANISM

A. Detection Phase

1) Initialization: The algorithm starts by assigning an initial trust score (like 0.5) to all

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 08 Aug. 2024, pp: 386-395 www.ijaem.net ISSN: 2395-5252

nodes in the network. This establishes a baseline forreputation.

2) Periodic Baiting: The algorithm broadcasts a specially crafted route request (RREQ) packet at a pre-defined interval (BaitTime). This RREQ has a unique identifier and a non-existent destination address.
3) Identifying Malicious Responses: If a node receives this fake RREQ and responds with a route reply (RREP), it's considered suspicious. The algorithm analyses the RREP for signs of blackhole, wormhole, or grayholebehaviour .
4) Tracing and Reputation Update: Based on the RREP analysis, the suspicious node is identified using its address and the path information. The reputation score of this node is then decreased based on the severity of the suspected attack. This update is broadcast to neighbouring nodes.
5) ReputationConsensus: neighbouring nodes share their reputation updates for the suspicious node. A distributed consensus algorithm is used to ensure all nodes agree on a final reputation score for the suspected node. This final score is then used to update the local reputation score of that node on each participating device.
6) Blacklisting: If the final reputation score falls below a certain threshold (<0.5), the node is added to a "MaliciousList". This list includes information about the suspected attack type and the aggregated reputation score.

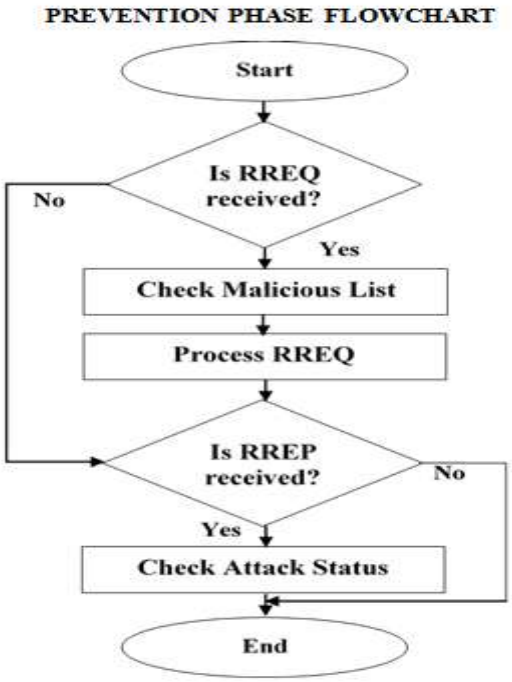
B. Prevention Phase

1) Checking for Blacklisted Nodes: Whenever a regular RREQ packet is received, the algorithm checks the MaliciousList. If the source or any node along the reported route is on the blacklist (considering both attack type and reputation score), the RREQ is discarded, and the route is not considered.
2) Secure Routing: Only RREQ packets free from blacklisted nodes are processed further for route discovery, ensuring data doesn't flow through potentially malicious nodes.

This two-phase approach helps secure OMDBM routing by proactively identifying and preventing malicious nodes from disrupting data flow in the network.

Algorithm 1. Detection Phase

```
InitializeNodeTrust():
   trust[node] = 0.5  for each node
if CurrentTime == BaitTime:
unique_id = generateUniqueIdentifier()
destination_address = generateNonExistentAddress()
   TTL = initialTTLValue()
Broadcast(fakeRREQ(unique_id, destination_address, TTL))
UpdateBaitTime()
```



International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 08 Aug. 2024, pp: 386-395 www.ijaem.net ISSN: 2395-5252

For each received RREP for fakeRREQ:
suspicious_node = analyzeRREP()
TraceAndAdjustReputation(suspicious_node)
BroadcastReputationUpdate(suspicious_node)
AggregateReputationScores():
UseConsensus() →UpdateLocalReputation()
ConstructMaliciousList():
AddToMaliciousList(suspicious_node) for each suspicious node
AppendMaliciousListToRREQ():
IncludeMaliciousInfo()
BroadcastRREQ():
BroadcastRREQPacket()

Algorithm 2. Prevention Phase
Start
if RREQ_received:
CheckMaliciousList()
ProcessRREQ
if RREP_received:
CheckAttackStatus()

PREVENTION PHASE FLOWCHART

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 08 Aug. 2024, pp: 386-395 www.ijaem.net ISSN: 2395-5252

VII. RESULTS

Simulation modelling is used in this research, among the various methods of performance analysis, simulation modeling is the simplest and most convenient to use. NS-2 (ver. 2.35) simulator was used to examine the effectiveness of OMDBM under the black hole, gray hole, and wormhole assault. Simulations were run altering the number of nodes and the number of malicious nodes. Packet drop ratio (PDR), average end-to-end delay (ED), and Network throughput (NP) metrics were utilized to measure the performance of the proposed scheme. The simulations were done out in a 1000x1000 m2 area by applying the IEEE 802.11 MAC protocol. During the simulations, both source and destination nodes were deployed at the opposite ends of the network initially. The benign nodes were scattered randomly around the area, equipped to execute the MDBM and OMDBM. Table 3.1 provides the simulation parameters.

In this stage, simulations were performed by varying the number of nodes from 20 to 80 nodes. Also, the number of malicious nodes is 5 nodes in the network and varying the number of normal nodes from 15 to 75. The number of malicious nodes of black hole, warm hole and gray hole in the network was 5.

SIMULATION PARAMETERS

Parameters	**Values**
Coverage area	$1000\times1000m^2$
MAC layer protocol	IEEE 802.11
Communication range of the node	250m
Type of traffic	CBR-UDP
Mobility model	Random
Nodes total number	100
Mobility	15 m/sec
Number of malicious nodes (varying)	20-80
Participating Protocols	MDBM, OMDBM

A. Packet Delivery Ratio

As shown in Fig. 6, as the percentage of malicious nodes increases, there is a significant drop in packet delivery ratio. The graph shows that the proposed system consistently achieves a higher Packet Delivery Ratio (PDR) compared to the existing system across various numbers of nodes, ranging from 20 to 80. This improvement suggests that the proposed system is more efficient and reliable in delivering data packets. The existing system primarily addresses black hole attacks, which are a specific type of network attack where malicious nodes drop packets instead of forwarding them. In contrast, the proposed system not only mitigates black hole attacks but also addresses gray hole and wormhole attacks. Gray hole attacks involve nodes selectively dropping packets, while wormhole attacks involve tunnelling packets between two locations in the network, potentially disrupting communication.

B. End-to-end Delay

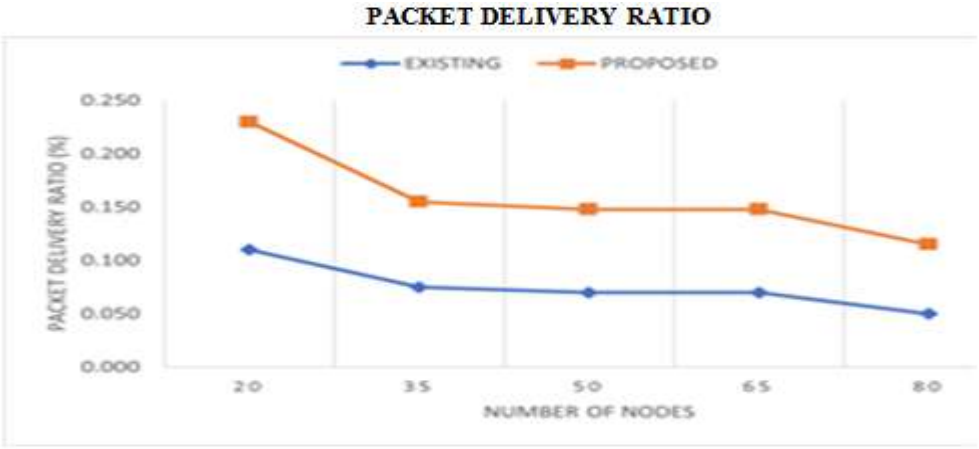
As shown in Fig. 7, with the increase in the number of malicious nodes, the End-to-end delay in the network is increasing. The graph provides a comparison of the end-to-end delay, measured in milliseconds (ms), for both existing and proposed systems across various numbers of nodes ranging from 20 to 80. The proposed system consistently exhibits a higher end-to-end delay compared to the existing system across all tested numbers of nodes. This increased delay can be attributed to the additional security measures implemented in the proposed system, which go beyond addressing black hole attacks to include protections against gray hole and wormhole attacks. These measures likely involve more complex processing, such as additional verification steps or more sophisticated routing protocols, which contribute to the observed delay.

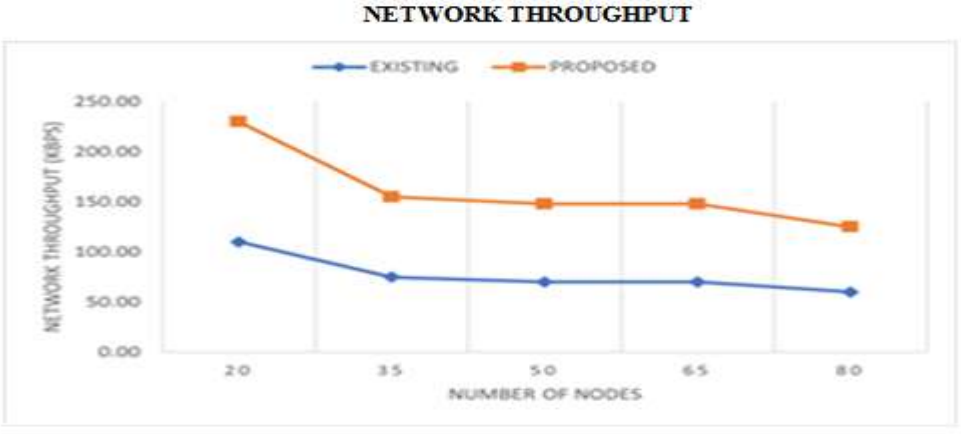
C. Network Throughput

As shown in Fig. 8, The graph illustrates the network throughput, measured in kilobits per second (kbps), for existing and proposed systems across different numbers of nodes, from 20 to 80. The proposed system consistently demonstrates higher throughput compared to the existing system,

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 08 Aug. 2024, pp: 386-395 www.ijaem.net ISSN: 2395-5252

indicating superior data transmission efficiency. For 20 nodes, the proposed system achieves higher throughput, suggesting efficient data handling even in smaller networks. As the node count increases to 35 and 50, the proposed system maintains its performance lead, likely due to optimized routing protocols and effective congestion control. This trend continues at 65 and 80 nodes, where the proposed system consistently outperforms the existing system. This suggests that the proposed system's advanced security features and data handling mechanisms, such as improved routing and error correction, do not compromise throughput





VIII. CONCLUSION

The proposed Optimized Mechanism to Detect Black Hole Attacks in Mobile Ad-Hoc Networks (OMDBM) is a better algorithm than the current Mechanism to Detect Black Hole Attacks in MANETs (MDBM) algorithm. It makes mobile ad-hoc networks (MANETs) much safer and faster. The OMDBM employs a comprehensive two-phase approach to address not just black hole attacks, but also gray hole and wormhole attacks. The detection phase baits and traces malicious nodes, while the prevention phase avoids routing data through these compromised nodes. This multi-pronged security strategy results in consistently higher packet delivery ratios, lower end-to-end delays, and improved network throughput across various node densities. By tackling a broader range of security threats, the OMDBM demonstrates superior efficiency and robustness in handling increased network traffic while maintaining secure communication. As a result, the proposed system is a more effective solution for networks that require high data rates and secure data exchange.

For future work, the algorithm can be extended to handle additional types of attacks beyond black holes, gray holes, and wormholes to provide even more comprehensive security for MANETs. Integrating the OMDBM security mechanisms with other routing protocols beyond just AODV will expand its applicability across different MANET environments. By addressing these potential areas for future work, the OMDBM algorithm can be further refined and optimized to deliver even more secure and efficient data communication in mobile ad-hoc network environments.

REFERENCES

[1] M. Krishnamurthy and H. M. Rajashekara, " Current Trends in Wireless Technologies in Academic Libraries," DESIDOC Journal of Library & Information Technology, vol. 31, no. 1, pp. 41– 48, Jan. 2011, doi: 10.14429/djlit.31.1.763.

[2] M. D. Nikose, " CPAODV. A Cross Layer Path Metric Algorithm for TCP improvement in Wireless Networks." [Online]. Available: https://sites.google.com/site/ijcsis/

[3] B. Goswami Parth Wadhwa and A. Prajapati, " Design and Improve AODV Protocol for Congestion Control in MANET using Cryptography Technique," IJIRST-International Journal for Innovative Research in Science & Technology|, vol. 5, 2019, [Online]. Available: www.ijirst.org

[4] Y. Shashwat, P. Pandey, K. V. Arya, and S. Kumar, " A modified AODV protocol for preventing blackhole attack in MANETs," Information Security Journal, vol. 26, no. 5, pp. 240– 248, Sep. 2017, doi: 10.1080/19393555.2017.1358780.

[5] R. Jatothu and R. P. Singh, " Efficient routing and High security transmission using AODV and Distributed protocol key generation with Dual RSA," 2017. [Online]. Available: http://www.ripublication.com

[6] S. Sugumaran and P. Venkatesan, " Optimized trust path for control the packet dropping and collusion attack using ant colony in MANET," Int J Eng Adv Technol, vol. 8, no. 6, pp. 4833– 4841, Aug. 2019, doi: 10.35940/ijeat.F9117.088619.

[7] M. S. Pathan, J. He, N. Zhu, Z. A. Zardari, and M. Q. Memon, " An Efficient Scheme for Detection and Prevention of Black Hole Attacks in AODV-Based MANETs," 2019. [Online]. Available: www.ijacsa.thesai.org

[8] R. Sharma, " COGNITIVE RADIO FOR MOBILE AD-HOC NETWORKS (MANETs) AND WIRELESS SENSOR NETWORKS (WSNs): APPLICATIONS, OPEN RESEARCH ISSUES AND RESEARCH DIRECTIONS."

[9] M. S. Sabri, "MOBILE AD-HOC NETWORKS : APPLICATIONS AND," no. May, 2021.

[10] R. Kaur and M. Khurana, "Vehicular Ad-hoc Network-A Literature Review on Simulation Tools." [Online]. Available: https://www.researchgate.net/publication/274964023

[11] M. Goswami*, Dr. P. Sharma, and A. Bhargava, " Black Hole Attack Detection in MANETs using Trust Based Technique," International Journal of Innovative Technology and Exploring Engineering, vol. 9, no. 4, pp. 1446– 1451, Feb. 2020, doi: 10.35940/ijitee.D1497.029420.

[12] 2018 International Conference on Advances in Computing, Communication Control and Networking : 12-13 October 2018, Greater Noida (UP), India. Institute of Electrical and Electronics Engineers, 2018.

[13] "Gnanaselvi, Vanatthan, Eswaran - 2019 - Secured Packet Transfer using HASME for AODV Protocol to Detect Black hole and Gray hole Attack" .

[14] " Gray-Hole Attack Minimization for Ad-Hoc Networks Using Contradiction," International Journal of Information Systems and Computer Sciences, vol. 8, no. 2, pp. 81– 83, Apr. 2019, doi:

10.30534/ijiscs/2019/19822019.

[15] N. Yadav, A. Upadhyay, R. Gandhi, and P. Vishwavidyalay, " A Common Architecture for Detection and Prevention of Black Hole and Warm Hole Attack in MANET." [Online]. Available: http://www.ijert.org

[16] N. Akhtar, M. A. Khan, A. Ullah, and M. Y. Javed, " Congestion avoidance for smart devices by caching information in MANETS and IoT," IEEE Access, vol. 7, pp. 71459– 71471, 2019, doi: 10.1109/ACCESS.2019.2918990.