INTERNATIONAL JOURNAL OF SOFTWARE ENGINEERING & COMPUTER SYSTEMS (IJSECS)
ISSN: 2289-8522 e-ISSN: 2180-0650
VOL. 9, ISSUE 1, 68 – 75
DOI: https://doi.org/10.15282/ijsecs.9.1.2023.7.0111

ORIGINAL ARTICLE

Enhanced On-demand Distance Vector Routing Protocol to prevent Blackhole Attack in MANET

O. M. Olanrewaju[1], A. A. Abdulwasiu[1,*] and N. Abdulhafiz[1]

[1]Faculty of Computing and Artificial Intelligence, Federal University Dutsin-ma, Katsina, Nigeria.

ABSTRACT – Wireless networks are becoming increasingly popular. Mobile ad hoc networks are one category among the different types of wireless networks that transmit packets from the sender node to the receiver node without the use of a base station or infrastructure, as the nodes serve as both hosts and routers. These networks are referred to as mobile because they are movable. MANET is an ad-hoc network that can change positions at any time, and nodes can join or leave at any moment, making it vulnerable to attacks such as Blackhole. Existing solutions, in some ways, led to more memory space consumption, while others led to an overhead. This research proposes an Enhanced On-demand Distance Vector (AODV) routing protocol to prevent Blackhole attacks on MANETs using Diffie Hellman and Message Digest 5 (DHMD), implemented using Network Simulator 2 (NS2). The performance of the proposed protocol was evaluated using the following parameters: Packet Delivery Ratio, throughput, End to End (E2E) Delay, and routing overhead. It was concluded that DHMD has reduced network overhead as it resulted to 23% while AODV resulted at 38% and memory consumption for DHMD gave 0.52ms compared to AODV that gave 0.81ms due to Blackhole prevention. This research will help to mitigate the effect of blackhole attacks in a network and increase network performance by reducing overhead and memory consumption.

ARTICLE HISTORY
Received: 26 October 2022
Revised: 22 March 2023
Accepted: 2 May 2023
Published: 23 June 2023

KEYWORDS
Mobile Ad-hoc Network
Blackhole
AODV Routing Protocol
Network Simulator 2

INTRODUCTION

A network may be either wired or wireless, with the wireless category further divided into traditional wireless networks and wireless Ad-hoc networks. In traditional wireless networks, there are infrastructures such as base stations, high-speed backbones, and online servers, and network operators manage and maintain system policies. The second category is wireless Ad-hoc networks, which are infrastructureless and have no base stations, backbones, or dedicated servers. They are self-organized, self-configured, and self-healing networks that deal with multi-hop wireless communication. Ad-hoc networks are a type of multi-hop wireless network where nodes serve as both hosts and routers, and communication takes place between nodes without any central control. When the nodes are movable and can change the topology, it is called a Mobile Ad-hoc network (MANET).

Mobile Ad Hoc Network, shortened as MANET, was created in 1970 as the Packet Radio Network (PRNET) [1]. MANET has a dynamic topology, and therefore requires a specific routing protocol. So far, there is no fixed infrastructure available for MANET, and because nodes are mobile, routing becomes a special consideration. MANET protocols can be categorized into three different types: reactive routing protocols (also called On-Demand), proactive routing protocols (also called Table-Driven), and hybrid routing protocols [2].

Reactive routing protocols are also called On-demand routing protocols, where route information is not exchanged periodically. Therefore, route discovery is initiated whenever new data transmission occurs. If no route is available from the source to the destination, this reduces overhead and makes the protocols more scalable. However, the process of determining routes may result in higher latency values [3]. The routing protocol is assisted by three mechanisms: Route Discovery, Route Maintenance, and Route Failure Recovery. Examples of Reactive routing protocols are AODV, DSR, ABR, RODV, SSA, FORP, PLBR, etc. For this proposed research work, AODV will be considered.

The AODV (Ad hoc On-demand Distance Vector Routing) algorithm requires low memory and processing load for establishing routes from node to node. It uses sequence numbers (a measure of the freshness of a packet) and hop counts (the number of intermediate nodes a packet must visit before reaching the destination node from the sender node) for route discovery in MANET. Communication in AODV is through path discovery or path maintenance messages. A Route REQuest (RREQ) and Route REPly (RREP) message contains path discovery and Route ERRor (RERR), while Hello Messages contain path maintenance. When a source node broadcasts an RREQ for the destination node, intermediate nodes search for a matching reverse route in their routing table. If there is a matching reverse route in the intermediate node, and the sequence number is greater than the previous entry, the entry is updated with the one from the RREQ. The intermediate nodes broadcast the RREQ packet until it reaches the receiver node. When the destination node receives the RREQ packet, it sends back an RREP packet that travels through the same path traversed during the RREQ packet generation [4]. Figure 1 shows an AODV routing protocol with RREQ and RREP messages and hop counts.

*CORRESPONDING AUTHOR | A. A. Abdulwasiu | ✉ ibnwasar@gmail.com

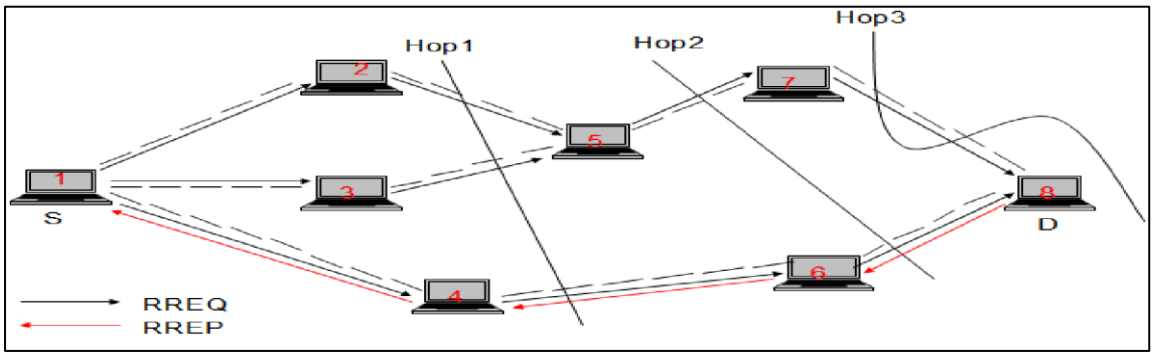

Figure 1. AODV Routing Protocol [5].

MANET has many challenges, such as limited range of wireless transmission, varying characteristics of wireless links, packet losses, battery restrictions, issues with routing, quality of service, and security. However, security is a significant challenge that needs to be addressed in MANET due to its wireless nature, which makes it vulnerable to various attacks [6].

The features of MANET negate the way in which the goals of security, including confidentiality, integrity, authentication, availability, access control, and non-repudiation, are typically achieved, thereby making it vulnerable to different types of attacks. Intruders may attack any of the seven layers described by ISO, which include the application layer, transport layer, multi-layer, network layer, physical layer, and data link layer. This research work will focus on the network layer attacks. In the network layer, attacks may either be passive or active, internal or external. Passive attacks do not destroy normal functionality, but active attacks involve interruption of information, fabrication or modification, thereby disrupting the normal functionality of a MANET. Examples of active attacks are Wormhole attack, Grey-hole attack, Blackhole attack, Byzantine, flooding, consumption of resources, and disclosure of location attacks [7].

The attack to be examined in the proposed research is the **Black hole attack**. This attack fakes the RREQ sent by the source node to the destination with RREP message of higher sequence number and shortest path to the destination, drops the packet without sending it to the destination when that packet is sent to it [8]. A Blackhole attack is a type of cyberattack that occurs in wireless ad hoc networks. In this attack, a malicious node uses its position in the network to attract and intercept all the data packets transmitted by other nodes. The data packets are then dropped, effectively creating a "black hole" in the network where all the data disappears.

The Blackhole attack is a serious threat to the security of wireless ad hoc networks, which are used in a variety of applications, including military and emergency response systems, sensor networks, and mobile ad hoc networks. The attack can cause a denial of service, disrupt communication, and compromise the confidentiality and integrity of the data transmitted. One of the most common techniques used in Blackhole attacks is the manipulation of the routing protocol. The attacker can modify the routing information to attract all the traffic to its node and then drop the packets or send fake data to the destination nodes [9].

The main problem with existing research is the consumption of much memory space by the security techniques developed, which causes end-to-end delay. Moreover, some techniques lead to overhead. This research intends to address these issues and ensure that the security is stronger, making it more difficult for the Blackhole to penetrate the network. With this, the research will contribute to the security aspect of the Mobile Ad-hoc Network, especially in the battlefield by the Military and in emergency situations.

RELATED WORK

This section discusses the existing work done on black hole detection and prevention in the AODV routing protocol of MANET. It covers the techniques used, how they work, the survey, advantages, and weaknesses of literature that exist.

Yugarshi et.al proposed an AODV protocol to block black hole attacks in MANET. Each node has a Data Routing Information (DRI) table. The sender node starts forwarding the Route Request (RREQ) packet, and when an intermediate node responds with a Route Reply (RREP) packet, the sender node confirms its DRI table to know if the intermediate node is a reliable node or not. If the intermediate node is reliable, then the sending of data packets will continue to the destination node through that intermediate node. If not, then it stops sending. However, each node having a DRI table takes a long time to process and requires large storage space to detect the attack [10].

According toAshish and Belmehdi in MANET, each node serves as both a host and a router. The intermediate node hides the packet or message without forwarding it to their neighbor node until an acknowledgment (ACK) mechanism is ascertained. In this ACK scheme, each node is required to send an acknowledgment packet to the route request packet sent by the source node, and then the source node will determine which node is reliable. The performance of AODV and OLSR protocols was evaluated in terms of Packet Delivery Ratio and throughput. This ACK approach produces better packet delivery ratios and the highest malicious node detection ratio. But in this technique, the acknowledgments are based on without authentication done on the acknowledgment packet. Therefore, authentication needs to be done on the acknowledgment. Additionally, the throughput obtained is low [11].

A study done by Ashwini et al. worked on the DSR protocol to curb black hole attacks. The technique used was an intruder detection system to identify the black hole, and when the suspected node is discovered, the Intruder Detection System node will exempt the node from the network. That is, the sender node makes the data packets in a different block, and data is sent one block at a time. The sender node also sends several data blocks to the recipient node. The packet drop ratio, end-to-end delay, and network overhead were the parameters considered, and it was recorded that the rate of packet loss reduces [12].

Another study proposed by Umar et al. named System for Detecting Intrusion (IDS) to detect black hole nodes. In this, the Sequence number of the receiving node, delay of packet processing, hop count, and queuing delay were all used and examined by the sender node while sending information. This technique was analyzed using 50 nodes in an area of 1500 m by 1500 m using the NetSim2 simulator, and parameters considered were Packet Delivery Rate, Throughput, and Detection Rate. From this existing study, the black hole attack can be detected by using some MANET features such as route reply, route request, location, hop count, time neighborhood, and data packets, which call for extra external hardware [3].

While a research studied by Kumar and Sumasudaram worked on a novel technique to fish out black hole attacks, which is based on an efficient crypto-key mechanism. A special group key technique called Diffie-Hellman was employed for key agreement, which is sent to only authenticate members that authenticate the nodes in the network before the transfer of data packets. This technique considered various parameters such as time used, Route Reply (RREP), hop count, and Delivery Ratio of Packet (PDR). Furthermore, the analysis was done using NS2 simulator. Nevertheless, this research uses many cryptography techniques that lead to an increase in overhead and processing time [13].

The proposed cross-layer framework Ibrahin et al. uses fuzzy-based trust evaluation to classify nodes as certain, untrusted, or distrusted regarding data forwarding and dropping. The source node transmits a Route Transmission Signal packet for channel reservation, and the intermediate node sends a CTS signal by piggybacking whenever it is ready. The simulation was conducted using MATLAB with 196 nodes and 20 attacker nodes, and different parameters were used to evaluate the network's performance. It was discovered that the protocol achieved an average of 83% packet delivery ratio. However, the system requires more space for the fuzzy dataset, and an increase in nodes leads to an increase in the dataset, resulting in space complexity [14].

Philomina et al. implemented a blackhole attack on the AODV protocol with three approaches: normal AODV, Blackhole AODV (BH_AODV), and Detected Blackhole AODV (D_BH_AODV). Blackhole was detected using two techniques: Intrusion Detection System (IDS) and Digital Signature Encryption Techniques. The results were investigated for Packet Delivery Rate, Delay, and overhead, but the throughput was not considered [9].

Kadry et al. modified the route discovery mechanism by adding two fields to RREQ. The first field uses the current coordinates (x, y) of the node for broadcasting, and the second field records the Route Request Factor (RQF). Only one field was added to RREP named Route Efficiency Factor (REF), and it was assumed that all nodes are homogeneous and equipped with GPS devices to obtain their (x, y) coordinates. The performance was evaluated using Packet Delivery Fraction, Energy Consumption, Network Lifetime, End-to-End Delay, and the throughput, although this was primarily for the DSR routing protocol, not the AODV routing protocol [15].

Abdulsalam et al. proposed an approach based on accumulative reputation values collected by watchdog from all neighbors for selecting the best path towards the destination. Each node has a reputation table with a count of sent packets. The research considers performance factors such as overhead, Packet Delivery Ratio, and Average End-to-End Delay, although the End-to-End Delay didn't change compared to the paper it intends to enhance [16]. From the literature reviewed, it has been discovered that researchers have provided different solutions to protect the AODV routing protocol from blackhole attacks. However, most of the research resulted in space consumption due to the algorithm used, resulting in end-to-end delay, overhead, and time complexity that need to be addressed. This is the focus of this research work.

METHODOLOGY

The aim of this research paper is to secure the AODV routing protocol from black hole attacks in Mobile Adhoc Networks while also considering memory space management to improve end-to-end delay and reduce network overhead. When the sender node broadcasts a Route Request to the neighboring nodes, it will be rebroadcasted to the next node until it reaches the receiving node. In this process, an attacker node known as a black hole is forced to send a Route Reply of the highest sequence number, proving that it has the shortest path to the receiving node.

Simulator Used

The Enhanced Ad-hoc On-demand Distance Vector using Deffie Hellman and Message Digest (DHMD) routing protocol is an improved version of the Ad-hoc On-demand Distance Vector (AODV) routing protocol. It is designed to mitigate the Blackhole attack in Mobile Ad-hoc Networks (MANETs).

The simulator used is Network Simulator version 2 (NS-2), it is a popular open-source network simulation tool that is widely used for simulating and analyzing network protocols. NS2 provides a wide range of tools and features for simulating different types of networks, including wired, wireless, and mobile networks. NS2 is written in C++ and supports both C++ and TCL scripting languages. To simulate the DHMD protocol and its performance against the effect of Blackhole attack, researchers typically use NS2. Which was implemented in C++ and then use TCL scripting to configure the simulation parameters, network topology, and other simulation settings that are included in Table 1. The hardware used for simulating the network protocol and the Blackhole attack in MANETs is typically a personal computer.

The choice of hardware depends on the complexity of the simulation and the size of the network being simulated. For this research an 8GB RAM, core i7, 1TB Hard disk space with an Ubuntu Operating system was used.

Simulation Approaches

Network Simulator 2 was adopted to simulate the behaviour of the reactive routing protocol called AODV protocol without blackhole attack and later blackhole attack was added by using the blackhole code. All the experiments were tested and evaluated using simulation and we considered AODV with blackhole and DHMD with blackhole. Simulation results are gotten from these two different mobile scenarios. The node-type scenario was designed randomly which means that the addresses of malicious node and the starting time of the malicious behaviour were completely random. For this experiment purpose, the starting time of the malicious node behaviour sets randomly between 0 seconds and 10 seconds and the starting time of data packet sending for a connection not regarding the node-type, sets randomly between 0 seconds and 30 seconds. While our simulation scenarios were examined for only CBR traffic on the node. And we examined the experiments for different numbers of nodes (5, 10, 15, 20, 25, 30, 35, 40, 45 and 50). Node mobility was modelled with the random waypoint method. We examined our experiments on the same simulation areas (1200m X 1000m area) to ensure the effect of number of nodes and pause time on the results are perfectly examined. Figure 2 depicts the steps that were applied within the network implementation.

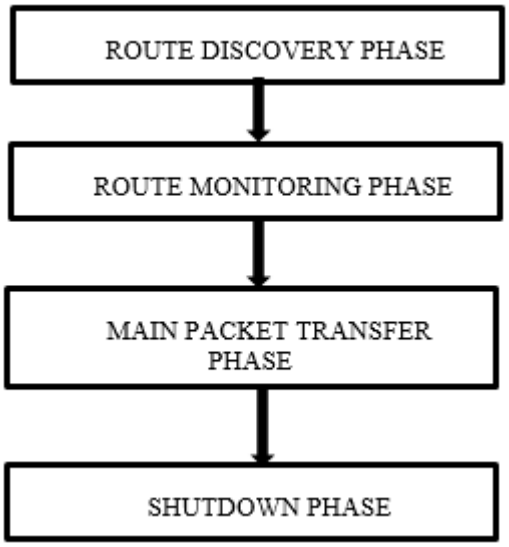

Figure 2. Steps in the network.

Route Discovery Phase: The sender node transmits a route request (RReq) message to the neighboring nodes to get a route to the receiving node. Every intermediate node continues to forward the RReq to their next neighbor until the receiving node receives the request.

The Route Monitoring Phase: Each node forwards data via the shortest path to the receiving node. The sender node creates an input message (M) and then computes its message digest (MD) using the MD5 message digest algorithm. The source node also uses its private key in Deffie Hellman Algorithms (DHA) to further encrypt the message digest to get (EMD). The encrypted message digest (EMD) is attached to the input message (M), and the whole message (M, EMD) is sent to the destination. The destination gets the message (M, EMD) and extracts the encrypted message digest (EMD). It then computes its own message digest (dMD) of the received message (M). It also decodes the received message digest (EMD) with the source's public key provided by DHA and gets the decoded message digest (dEMD). The destination node then compares both message digests (dMD==dEMD).

The Main Packet Transfer Phase: In this phase, the sender node transmits data to the receiving node by selecting the most reputed hop node that is next. As the data gets to the receiver, then the receiver nodes acknowledge the receiving of the message using a packet acknowledgement (PAC) packet to the sender node.

Shutdown Phase: In the shutdown phase, any node that misbehaves is demoted because it will be considered as malicious. The setup parameters that were used are given in Table 1.

Table 1. Parameter table.

PARAMETER	VALUE
Protocol Examined	AODV
Time of simulation	100 seconds
Range used in Simulation (m x m)	1200 x 1000
Nodes number used (varied)	5, 10, 15, 20, 25, 30, 35, 40, 45, 50
Type of traffic	CBR
Performance Parameter	Throughput, End to end delay (E2E), Packet Delivery Ratio, Overhead of network
Mobility Model	Random waypoint
Packet size (bits)	512
Number of malicious nodes	1
Type of Antenna	Omni Antenna
Channel used	Wireless channel
Type of Propagation	Two way ground
MAC used	MAC 802.11
Interference Queue	Queue/ Droptail/ PriQueue

EXPERIMENTAL RESULTS

This research work was conducted using Network Simulation version 2.35, and the results obtained from the simulation were analyzed by evaluating the performance of the proposed enhanced AODV, named Deffie Hellman Message Digest (DHMD), with an incorporated blackhole attack. Throughput, packet delivery ratio, end-to-end delay, and network overload were the evaluation parameters while varying the size.

Figure 3 depicts the data packet transmission rate, known as packet delivery ratio, simulated from a scenario embedded with 50 nodes containing 1 node for blackhole. The packet delivery ratio obtained from the simulation with a scenario consisting of nodes that vary from 5 to 50, including a blackhole node. The DHMD routing protocol with black hole nodes decreases as the number of nodes increases, as does AODV with blackhole. By comparison, AODV routing protocol with black hole nodes decreases from 34% to 3%, while DHMD decreases from 35% to 27%. Therefore, the simulation results show that DHMD protocol provides a higher packet delivery ratio in the presence of an increase in black hole nodes compared to AODV protocol with black hole nodes.

Furthermore, the simulation results suggest that the performance of DHMD protocol with the incorporated black hole attack outperforms that of the AODV protocol with the addition of a black hole attack in terms of packet delivery ratio. This implies that DHMD protocol with black hole nodes can provide better network security and stability in the presence of malicious nodes."

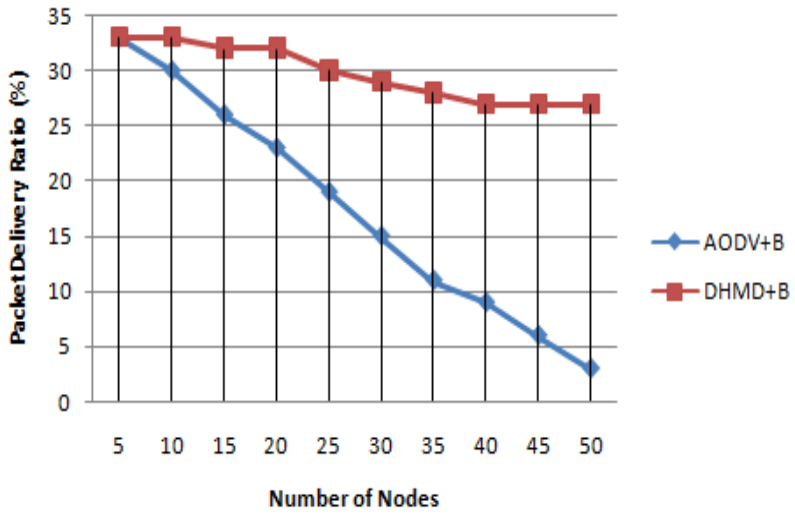

Figure 3. Packet Delivery Ratio of AODV+B AND DHMD+B against number of nodes.

Figure 4 plots the throughput of the routing protocols against the number of nodes on the same configuration. Here, a comparison is made between the AODV protocol with a black hole node and the DHMD protocol with a blackhole node. The graph shows that AODV with a blackhole started with 500kbps for 5 nodes and decreased to 120kbps, while DHMD

with blackhole decreased from 600kbps for 5 nodes to 390kbps for 50 nodes. Therefore, by comparison, the throughput in DHMD with blackhole is higher than that of AODV with blackhole.

The results of the simulation indicate that the proposed DHMD protocol provides a significant improvement in terms of network performance compared to the traditional AODV protocol with the addition of a black hole node. The DHMD protocol achieves a higher packet delivery ratio, lower end-to-end delay, and higher throughput while considering the management of memory space in the network. These results demonstrate the effectiveness of incorporating the Deffie Hellman Message Digest algorithm to enhance the security and performance of the AODV protocol in Mobile Adhoc Networks.

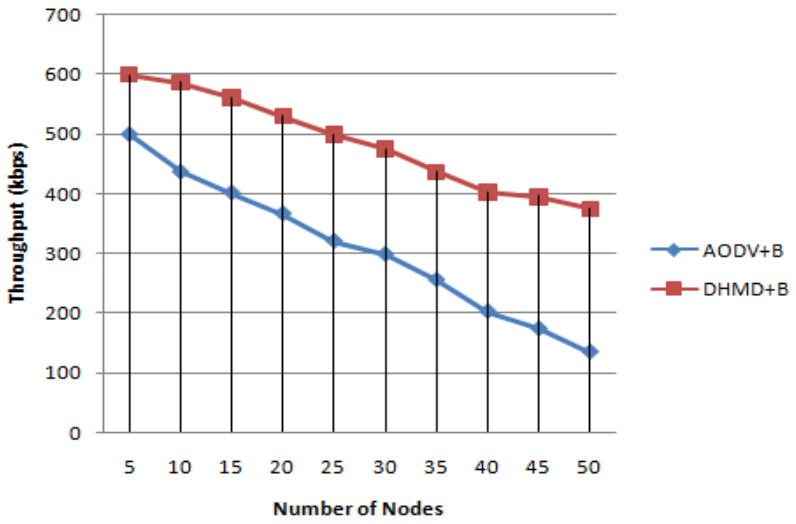

Figure 4. Throughput of AODV+B and DHMD+B against number of nodes.

Figure 5 shows the end-to-end delay of the routing protocols against the number of nodes in the same scenario. The comparison is also made between AODV protocol with black hole nodes and DHMD protocol with black hole nodes. The delay of the AODV protocol with a black hole attack is higher with a value of 0.4ms for 5 nodes and increases as the number of nodes increases to 0.81ms for 50 nodes. However, the DHMD protocol with black hole node provides a lower delay compared to AODV protocol with a black hole node, although it also increases from 0.3ms as the number of nodes increases to 0.52ms. The simulation results show that the delay of the DHMD protocol is less compared to AODV with a black hole attack. In conclusion, the simulation results indicate that the proposed DHMD protocol performs better than the AODV protocol with a black hole attack in terms of end-to-end delay. These findings suggest that the DHMD protocol can provide an effective solution for securing the Ad-hoc network against black hole attacks.

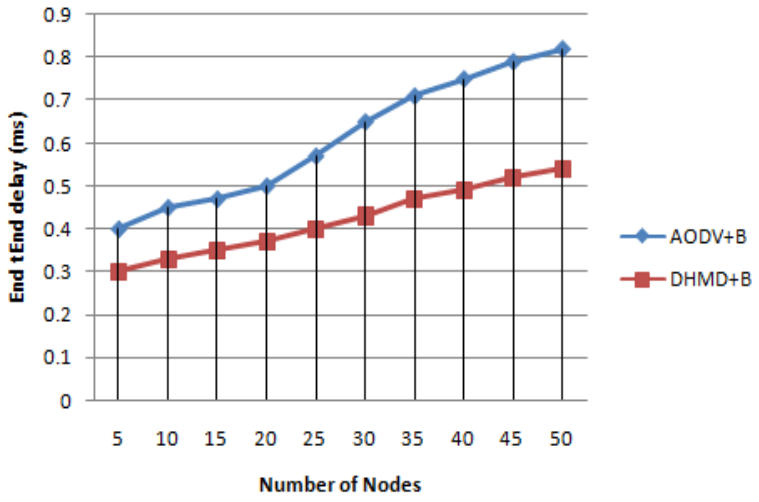

Figure 5. End to end delay of AODV+B and DHMD+B against number of nodes.

In Figure 6, the overhead of both AODV protocol with blackhole attack and DHMD protocol with blackhole attack are compared as the number of nodes increases. It is shown that the overhead of AODV protocol with blackhole attack starts at 0% for 5 nodes and rapidly increases to 38% for 50 nodes. On the other hand, the overhead of DHMD with blackhole attack starts at 0% for 5 nodes and increases to only 23% for 50 nodes. This indicates that the DHMD protocol with blackhole attack performs better than AODV with blackhole attack in terms of overhead. Overhead refers to the additional data used for control purposes, such as routing and maintaining network topology. Higher overhead can lead to congestion and decreased performance. In this case, DHMD with blackhole attack is more efficient at controlling overhead as the number of nodes increases compared to AODV with blackhole attack.

Overall, the results of the simulation suggest that DHMD with blackhole attack outperforms AODV with blackhole attack in terms of various performance metrics, such as throughput, packet delivery ratio, delay, and overhead.

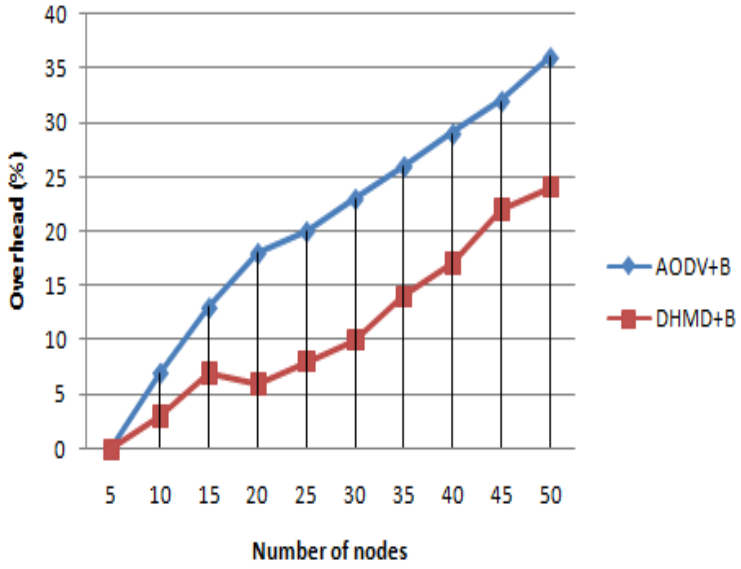

Figure 6. Overhead of AODV+B and DHMD+B against number of nodes.

CONCLUSION

In conclusion, the objective of this research was to enhance the security of MANET against black hole attacks. The proposed DHMD scheme is reactive in nature and can detect malicious nodes before the actual routing process and isolate them from the main packet sending. The simulation results revealed that DHMD outperformed AODV with black hole attacks in terms of evaluating the throughput, end-to-end delay, packet delivery ratio, and network overhead. This study aimed to improve the network overhead and memory space consumption, and the results demonstrated that the goal was achieved. Overall, the DHMD scheme can be a promising approach to enhancing the security of MANET against black hole attacks, and future work can explore the performance of the scheme under different network conditions and other types of attacks.

FUTURE WORK

Sequel to this research work, DHMD which is the work done in this research improves the security and the effect of throughput, Packet Delivery Ratio, End to end delay and Network Overhead, likewise this research work scope is for just a single blackhole attack, therefore, it is recommended that the future work should address and consider the use of multiple black hole attacks.

ACKNOWLEDGEMENT

The authors will like to appreciate Allah for His Favour then will like to appreciate the effort and contribution of Dr. Olanrewaju O. M. for her total support towards the success of this paper.

REFERENCES

[1] K. Ahmed, Al-Shammari, P., Ehkan, N. Y., "Future Barriers, Challenging Security Attacks and Secure Routing Issues in MANET", *Australian Journal of Basic and Applied Sciences*, Australia. pp. *20-25*, 2017, DOI:10.22587/ajbas.2017.11.15.4

[2] O. Afolayan, and , M. O. Oyenike,"Review of Mobile Ad Hoc Network Protocols" *IOSR Journal of Computer Engineering (IOSR-JCE)*, India. pp. 1-12, 2015, doi: 10.9790/0661-17220112

[3] S. Kumar, and K. Dutta, "Intrusion detection technique for black hole attack in mobile ad hoc networks". *International Journal of Information Privacy, Security and Integrity*, Switzerland. pp. 81, 2015, doi.org/10.1504/IJIPSI.2015.075435

[4] S. Yugarshi, P. Prashant,K. Arya, and K. Smit, A modified AODV protocol for preventing blackhole attack in MANETs", *Information Security Journal: A Global Perspective*, United State. pp. 240-248, 2017, doi.org/10.1080/19393555.2017.1358780

[5] V. Ashish., and Shrivastava S., "Security Enhancement in MANETs Using Fuzzy Based Trust Computation Against Blackhole Attacks", in *Information and Communication Technology*, Springer, Singapore, pp. 39-47, 2018, DOI:10.1007/978-981-10-5508-9_4

[6] D. Bisen, P. Suman, S. Sharma, and R. Shukla, "Effect of Pause Time on DSR, AODV and DYMO Routing Protocols in MANET," *International Journal of IT & Knowledge Management*, vol. 3, no. 1, pp. 1–6, 2010.

[7] S.Philomina, R. Ramesh, "Secure Routing-Solution to Diminish DOS Attack in AODV Based MANET*", International Journal of Chemical Sciences Research*, India, 15(4):188, 2017

[8] V. Ashwini and S. Kishor, "Blackhole Attack Detection And Prevention Mechanism Using Ns2 Simulation", *International Journal Of Scientific & Technology Research*, Volume 8, Issue 11, Europe, 2019.

[9] Md Ibrahim Talukdar, Rosilah Hassan, Md Sharif Hossen, Khaleel Ahmad, Faizan Qamar, Amjed Sid Ahmed, "Performance Improvements of AODV by Black Hole Attack Detection Using IDS and Digital Signature", *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 6693316, 13 pages, 2021. https://doi.org/10.1155/2021/6693316

[10] J. Sen, S.Koilakonda, and A. Ukil, "*A Mechanism for Detection of Cooperative Black hole Attack in Mobile Ad Hoc Networks"*, Proceedings of the Second IEEE International Conference on Intelligent Systems, Modeling and Simulation, ACTA Press, Canada. pp. 338-343, 2011, DOI:10.5013/IJSSST.a.12.04.04

[11] A.Baadache,. and A. Belmehdi, "Fighting Against Packet Dropping Misbehavior in Multi-hop Wireless Ad Hoc Networks", *Journal of Network and Computer Applications*, United State, pp. 1130–1139, 2012, doi.org/10.1016/j.jnca.2011.12.012

[12] M. Mohanapriya, and I. Krishnamurthi, "Modified DSR protocol for Detection and Removal of Selective Black hole Attack in MANET". *Computers and Electrical Engineering*, United Kingdom. pp. 530-538, 2014, doi.org/10.1016/ j.compeleceng.2013.06.001

[13] V. Kumar, ., and K. Somasundaram, .. "An Effective CBHDAP Protocol for Black Hole Attack Detection in Manet". *Indian Journal of Science and Technology*, India. 9(36), 2016, DOI:10.17485/ijst/2016/v9i36/95632

[14] I. Umar, Z. Hanapi, A.Sali, and A. Zulkarnain, "TruFiX: A Configurable Trust-Based CrossLayer Protocol for Wireless Sensor Networks". *IEEE Access*, pp. 2550-2562, 2017, doi: 10.1109/ACCESS.2017.2672827

[15] S. Kadry, A. Sayed and M. Abdelhady "Energy Efficient load balancing scheme of DSR protocol (EELB-DSR)", *International Journal of Computer Science and Mobile Computing (IJCSMC)*, North Lalaguda, India vol. 8 No. 1,2019.

[16] A. Abdulsalam, A. Hadeel and A. Areej "Blackhole attack prevention in MANET using Enhanced AODV protocol". Proceedings of the Second International Conference on Data Science, E-Learning and Information Systems, Association for Computing Machinery New York, NY, United States, pp 1-5, 2019, https://doi.org/10.1145/3368691.3368732