INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2022, VOL. 68, NO. 1, PP. 145–152
Manuscript received September 6, 2021; revised January, 2022. DOI: 10.24425/ijet.2022.139862

Lightweight Security Mechanism to Mitigate Active Attacks in a Mobile Ad-hoc Network

Uthumansa Ahamed and Shantha Fernando

***Abstract*—Mobile Ad hoc Network (MANET) is a type of Ad hoc network. General properties of MANET open the network to various security threats. Network layer-based Active attacks are widespread and destructive. Available security solutions contain complex calculations. Therefore, the objective of this research is to propose a lightweight security mechanism to enhance the security of data communications between source and destination nodes in a MANET from network layer-based active attack. Blackhole is used as a network layer-based Active attack. The network performance is evaluated using Packet Delivery Ratio (PDR), Average End-to-End Delay (AEED), Throughput, and Simulation Processing Time at Intermediate Nodes (SPTIN). The controller network was used to compare the performance of each network. During the experiment due to the impact of the blackhole attack, compared to the controller network, the PDR was found to be 0.28%, AEED was infinity and Throughput was 0.33%. The performance of the proposed security mechanism was compared with that of the controller network, and the values of PDR, AEED, Throughput, and SPTIN were found to be 98.0825%, 100.9346%, 99.9988%, and 96.5660%, respectively. The data packet delivery ratio was 100.00% compared to that of the controller network. The network that was affected by a blackhole attack showed a higher amount of ADDR than the controller network and the lowest amount of PDR. The network that was affected by the blackhole showed underperformance compared to the controller network. The proposed security mechanism performs well in PDR, AEED, and Throughput compared to the controller network. The AEED and SPTIN values prove that the proposed solution is free from complex calculations. The scope of the solution can be expanded into a lightweight Intruder Detection System to handle different types of security attacks in MANETs.**

***Keywords*—Blackhole; lightweight; mechanism; security; simulation**

I. Introduction

4G technology enables wireless devices to communicate themselves through a wireless medium without any predefined infrastructure.

These wireless devices can communicate among them if they are capable of listening to one another. This type of network is called an Ad Hoc Network [1]. MANET is a type of ad hoc network [2], [3]. The main characteristic of a MANET is node mobility [2]. Furthermore, mobile nodes join the network and leave the network without any constraints.

U. Ahamed is with Faculty of Applied Sciences, Rajarata University of Sri Lanka, Mihintale, Sri Lanka (e-mail: urmail2ahmed@gmail.com).

Shantha Fernando is with University of Moratuwa, Colombo, Sri Lanka (e-mail: shantha@cse.mrt.ac.lk).

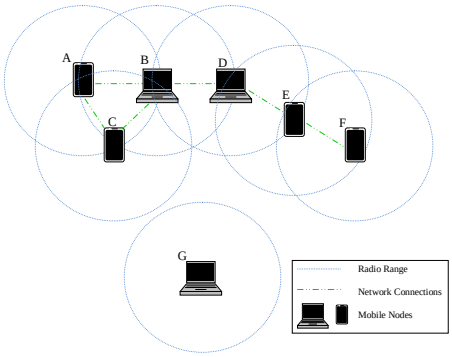

Fig. 1. A MANET

Therefore the network topology eventually changes. Three different types of nodes were identified in a MANET. These are the source, destination, and intermediate (routing) nodes. In the pure MANET paradigm, there was no fixed infrastructure.

As illustrated in Figure 1, the limited radio range of mobile nodes leads to finding the help of neighboring nodes (multi-hop) to communicate with the destination node that is not in the radio range of the source node [2], [3]. Nodes follow Open Systems Interconnection (OSI) model standards to communicate among them. In a multi-hop network, one or more intermediate nodes can be connected via a route between the source and destination nodes [1], [3]. The opportunistic nature of MANETs has attracted for attention to use on military and rescue agencies particularly in disorganized or hostile environments where infrastructure network services are unavailable because of disaster situations [1]. The relatively low cost of network deployment made MANET a more common and smart alternative even for commercial uses such as virtual classrooms [3]. MANET supports green networking concepts more than infrastructure networks do.

The general features of a MANET are mobile nodes, open network boundaries, infrastructure-less network nature, and limited resources. These features open the network to a large number of security threats. Security of MANETs is a critical issue. Researchers categorized security attacks on MANETs from different perspectives. Security attacks can be categorized based on the Open System Interconnection (OSI) layer that is operating on. Routing is the main function of MANET. Routing protocols help to establish a route between the source and destination nodes. Mainly, routing protocols

are two types: Proactive and Reactive. AODV is an example of a reactive routing protocol that is suitable for MANETs and performs better than other routing protocols. Routing attacks are oriented toward the network layer. Network layer attacks are more prominent and destructive. According to the impact of the attack, network layer attacks are categorized into: Active and Passive attacks. Active attacks degrade the network performance. Passive attacks either not degrade the network performance or enhance the network performance. Passive attacks are collect information from the network to form an active attack in the future. Blackhole and Grayhole attacks are network layer-based active attacks. Blackhole attacks drop all data packets. It inserts false information in the routing packets to become a part of the route or else to mislead the source node to send data packets to it. A Grayhole attack is an extensions of a blackhole attack. It drops data packets after a certain period of time or drops all data packets from a specific node.

The research study is an extension of our previous works [4], [5]. Related to the literature survey and the advantages of the MANET, we aimed to enhance the quality of a MANET by discovering a lightweight security mechanism to secure data communication. Therefore, the research problem can be stated as follows: "There is no lightweight security a mechanism in MANET to ensure secure data communication between a source and destination nodes from network layer-based active attacks". Moreover, the research objective can be formulated as "to propose a lightweight security mechanism to enhance data security communications between source and destination nodes in a MANET from network layer-based active attacks". The research question can be derived to achieve the research objective through an experiment. Therefore the research question can be formulated as follows, "What would be the appropriate lightweight security mechanism in a MANET to ensure data security for secure communication between a source and destination nodes from the network layer-based active attacks?" We designed an experiment to achieve the objective by finding the answers for the research question.

The remainder of the paper is organized as follows. The available literature related to solutions for blackhole attacks is reviewed in section 2. The proposed solution is described in section 3. The results of the performance of the proposed solution are presented in section 4. Section 5 presented the conclusion and future work of our research.

II. Literature Review

Researchers have proposed a large number of security solutions to prevent or identify security attacks in MANETs. Most of the solutions are based on the routing protocol. However, some researchers have proposed individual solutions for each security attack. Though, some researchers have proposed an Intruder Detection System (IDS) to handle a single attack or else to handle the number of attacks at once.

A. Specific solutions for blackhole attacks

Khamayseh, Y., et al, (2011) [6] proposed a solution for a blackhole attack using a new protocol. However, they only showed a modification of the AODV protocol. Furthermore, the graph that illustrated in figure 7 in their research paper, contradicts the definition of the blackhole attack in section 2 in their findings. The graph shows 60% of data received by the destination node in the presence of a blackhole attack. However, a blackhole attack does not allow any data packets to pass through it. Panos, C., et al. (2016) [7] proposed a comprehensive study on blackhole attacks and a mechanism to detect blackhole attacks. However, they made a poor assumption regarding a malicious node that is not available in the training phase in the detection mechanism. Semary & Diab (2019) [8] proposed a BP-AODV routing protocol to overcome cooperative blackhole attacks on AODV protocol. A new protocol was employed with five types of messages. Furthermore, an additional process called Confirm is available in the proposed protocol in addition to the AODV protocol. Therefore, BP-AODV is complex in operation and has a higher routing overhead than pure AODV.

Arathy & Sminesh (2016) [9] proposed a D-MBH algorithm to detect blackhole attacks using additional route requests with non-existent target addresses. The authors did not present any data or results. However, they concluded that the solution performed well without any evidence. Lachdhaf, Mazouzi & Abid (2018) [10] proposed an approach to detect and prevent blackhole attacks on a Vehicle Ad Hoc Network. They used Cyclic Redundancy Check 32-bit used as the hash function to store converted destination IP addresses in the Routing Request (RREQ) packet. If the IP address of the destination node is known then this approach will fail. Kumar, Tripathi & Agrawal (2018) [11] proposed a mechanism to secure the AODV protocol by proposing Symmetric Encryption Algorithm to mitigate blackhole attacks. However, the proposed mechanism contained more computation, calculations, and a higher delay. Hammamouche, A. et al. (2018) [12] proposed an approach that was based on a trust model that uses multi-hop acknowledgment and a reputation mechanism against blackhole attacks. the network overhead on each node in the network is the main drawback.

Dorri, Vaseghi & Gharib (2016) [13] proposed a novel approach called detection and elimination blackhole attacks that used a data control packet and an additional blackhole check table for detecting and eliminating malicious nodes. A data control packet is sent to verify the established route before sending the data packet. Therefore, verification through DCP is an additional and energy consumption process. Aziz, Alsaad & Hmood (2019) [14] proposed a new security scheme for MANETs. The scheme used the Trivium Lightweight Stream Cipher Algorithm in combination with Keyed-hash Message Authentication Code to secure routing control packets. The scheme performed well only in terms of throughput and packet loss ratio compared to pure AODV protocol. Rajendran, Jawahar & Priyadarshini (2019) [15] proposed a Cross Centric Intrusion Detection System for Secure Routing over blackhole Attacks in MANETs. From the results, they proved that the throughput of the network that is affected by a blackhole attack is higher than the network that is not affected by a

blackhole attack. Elmahdi, Yoo & Sharshembiev (2020) [16] proposed reliable and secure data transmission in MANETs under possible blackhole attacks based on modified ad hoc on-demand multipath distance vector (AOMDV) protocol. Their approach is with higher End-to-End Delay and complex calculations. Furthermore, needed to form three different paths to the destination.

B. Intruder Detection Systems

Shrestha, R. et al. (2010) [17] proposed a cross-layer intrusion detection architecture to discover the malicious nodes and different types of DoS attacks. They used Fixed Width Clustering Algorithm for the detection of the anomalies in the MANET. Though, they concluded that they can detect various types of UDP flooding attacks and sinkhole attacks efficiently. The same author [18] (Jhaveri, R, et al (2012b)) [19] presented a secure route discovery mechanism for MANETs using AODV against blackhole and Grayhole attack (Jhaveri, R, et al. (2012a)). Thought, same as their previous work, results are not realistic. Because PDR value remained the same in the presence of node mobility. Ibrahim, Omar & William (2015) [20] proposed a technique to detect and remove blackhole and Grayhole attacks including cooperative blackhole in AODV. A mobile backbone network constructed from randomly moving regular MANET nodes based on their trust value, location, and power. The proposed technique is divided into four phases. The mechanism to select the node for backbone network construction is not clearly defined. Therefore, a malicious node can be in the backbone network. Furthermore, this technique is complex and contains numerous calculations.

Dhaka, Nandal & Dhaka (2015) [21] proposed a scheme to identify the malicious node by the nodes' response for two types of control sequence packets to the neighbor nodes. Each intermediate node sends the Code Sequence Packet to all its neighbors. Then neighbors intern send their Response sequence Packet to the intermediate node. Therefore, these two types of packets will cause routing overhead. Subba, Biswas & Karmakar (2016) [22] proposed a new MANET IDS scheme consist of two components: MANET leader election mechanism and A hybrid MANET IDS. The proposed scheme consists of lightweight and heavyweight IDS. Vinayagam, Balaswamy & Soundararajan (2019) [23] proposed a novel Integrated Cross Interior Structure for IDS to secure a MANET from blackhole attacks. The proposed system contained complex calculations.

III. Proposed Solution

Proposed security mechanism contains three different phases: Protection, Pinpoint, and Prevention. This mechanism is designed based on the research outcomes of our previous two [4], [5] research studies.

As illustrated in Figure 2 the proposed security mechanism contains three different phases: Protection, Pinpoint, and Prevention. These three phases operate in chronological order or operated individually as per demand. Each phase is targeted to different functions of the AODV routing protocol.

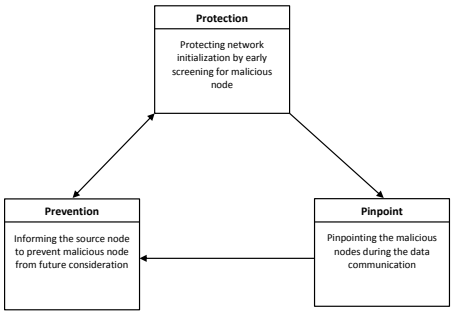

Fig. 2. Phases in Proposed Solution

Generally, there is a sequence between these phases. The functions of each phase are oriented to the operations of the specific functions of the AODV protocol. These functions are operating to provide secure transactions from start to end of a communication between the source and destination nodes.

Initially, the security mechanism is started to operate when a demand for a route from the source node to a destination node. The mechanism is oriented to the each routing packets (RREQ, RREP, and REER) of the routing protocol. Each phases working for screen malicious nodes from the route, detect malicious node, and preventing malicious nodes to join into the network. Protection is the initial phase. This phase is oriented to the Routing Reply (RREP) process of route establishment in the AODV routing protocol. The main task of this phase is selecting normal nodes to establish a secure route between the source and destination nodes by screening blackhole nodes to join the route. Blackhole nodes are inserting false routing information on RREP packets to trick the source node. Finally, the source node is cheated by the malicious node. Then the source node starts to transmit data packets to the malicious node. Therefore to prevent the misleading of the malicious node should be identified through initial protection to detect the false information in the RREP packets.

The protection process begins when a node receives RREP packets for the RREQ. A node waits for the response from its neighbors after transmitting an RREQ packet. A node can receive RREP packets from the destination node or the node that has the destination node as its next. According to the AODV routing protocol, the response for an RREQ will be a retransmission of the same RREQ packets or transmitting the RREP for the corresponding route request. If a node receives the same RREQ packets from its neighbor after transmitting RREQ packets then the node behaves genuinely. Because it is providing the cooperation to the communication by retransmitting the same RREQ packet after increasing hop count and source sequence no by one. If a node received an RREP packet as the response, then it needs to check the accuracy of the information in it.

Initially check for the availability of the IP address of the sender of the RREP packet in the malicious nodes list. If the IP address is available in the list, then the RREP packet will be discarded and then wait for the response from another neighbor

node. Moreover, if the IP address is not in the malicious list then check whether the RREP is from the corresponding destination node. If so, the RREP packet will be retransmitted to reach the source node. If RREP is not from the destination node then check similarity for the details of the source node and destination node of the RREP packet. If the details are different then the node retransmits the RREP packet. If details are the same then check for the destination hop count. If the destination hop count is more than one then the RREP packet is retransmitted. If the destination hop count is one then check for the validity of the destination sequence number as described in the following equation.

$$RREPSn_{n+1} \leq RREQSn_n + NoOfReply$$

RREPSn = Sequence number in the RREP
RREQSn = Sequence number in the RREQ
n = n^{th} node
NoOfReply = Number of possible RREP for an RREQ.

The value of the NoOfReply is changed according to the reply mechanism of a routing protocol. In AODV, RREP for an RREQ is sent by either the destination node or the node that has the destination node as its neighbor. Therefore NoOfReply value in AODV is two. The sequence number of an RREP packet should be equal to or lower than the sequence number of the RREQ packet plus two. If the sequence number of the RREP satisfies the above equation then the RREP packet will be retransmitted to its neighbor to reach the source node. If the destination sequence number is equal or lower than the sequence number of the specific RREQ plus two then it is retransmitted to reach the source node. If the sequence number is more than that then the IP address of the node is updated in the malicious list and RREP packets discarded. Moreover waiting for another RREP for the same route.

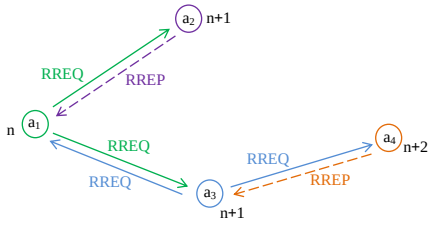

Fig. 3. Proposed Solution

For example, according to Figure 3 we assumed a_1, a_2, a_3, and a_4 set of nodes. a_2 and a_3 are in the radio range of a_1. a_1 and a_4 in the radio range of a_3. a_3 is in the radio range of a_4 and a_3. a_1 is in the radio range of a_2. a_1 retransmits RREQ for a specific source node as it is received. a_2 and a_3 receive the RREQ packet because a_2 and a_3 are in the radio range of a_1. Then a_1 waits for immediate responses from a_2 and a_3. a_3 retransmits the same RREQ packet after increasing the sequence number by one. Then a_1 and a_4 receive the RREQ packet. a_1 decides that a_3 is not a malicious node on this route selection. Because a_3 is not the destination and it will

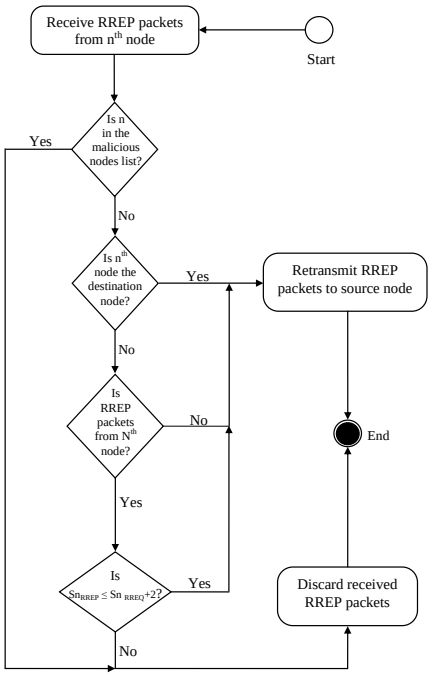

Fig. 4. Flow Chart

retransmit the RREQ packet. Though, a_1 may receive RREP as the response from the a_2 node. Then a_1 needs to validate the RREP packet sequence number. If the sequence number of the RREQ packet in a_1 is n then the sequence number of the RREP packet of a_2 should be lower than or equal to n+2. If the RREP packet of a_2 fulfills the condition then a_2 is a legitimate node else a_2 is a malicious node. Then a_2 updates its malicious list with the IP address of a_2. Then discard all packets from a_2 node. The flow chart of the protection phase can illustrate as in Figure 4. Moreover, to ensure the quickest response than the present, we can check the destination hop count first in the RREP packet. If the destination hope count is more than one then it indicates that the RREP packet is not from a direct neighbor. Therefore RREP packet needs to retransmit to reach the source node. Then, the IP address of the responding node is checked for availability in the malicious list.

Pinpoint is the second phase. This phase helps to detect malicious activities of neighbor nodes of a node. Retransmission is the main task expected from an intermediate node in the network. If a node failed to retransmit the data packet then the node is marked as the malicious node from the neighbor node. Finally, the prevention phase is executed after detecting a malicious node, the node sends RERR packets to the source node by inserting the malicious node's IP address. Then the source node updates its malicious table by the IP address of the malicious node.

IV. Experimental Design

Simulation methodology is known as the design of computer experiments which includes the design and analysis of simula-

tion experiments. Simulation is used to experiment with quantitative models. There are several specialized quantitative research methods and are based on agent-based simulations [24]. Furthermore, agent-based simulation provides a platform to inductively develop and examine theories in design that have the potential to inform experimental research [25]. Network Simulator 2 (NS2) [26] is used as the network simulator for design experiments in our research study. NS2 is a version of Network Simulator that is an agent-based discrete event simulator that is designed for network simulations. It enables to design of simulations for wired and wireless networks. NS2 is used in a massive amount of research studies [26], [27] for the simulator, visualization, and simulation scaling. Furthermore, NS2 is used as an Emulation which refers to the ability to introduce the simulator into a live network [26].

The NS2 is installed in the Personal Computer (PC). Configurations are "Intel® core i3-3217U CPU@ 1.80GHz x 4" processing power, 1.8 GB of memory, "Intel® Ivybridge Mobile x86/MMX/SSE2" graphics, and 169.4 GB size of the disk. The Operating System (OS) was the 32-bit type "ubuntu 14.04 LTS". The configuration of the PC was maintained unchanged throughout the experiment. The same PC was used for each experiment.

TABLE I
SIMULATION PARAMETERS

Parameters	Values
Simulator	NS2 (V.2.35)
Number of connected nodes in the network	10
Transmission range	250 m
Bandwidth	2.0 x 10^6 bps
Frequency	9.14 x 10^8 Hz
Antenna/ OmniAntenna X, Y, Z	0, 0, 1.5m
Traffic type	Constant Bit Rate (CBR)
Radio-propagation model	TwoRayGround
Network interface type	Phy/WirelessPhy
Routing protocol	AODV
Maximum packets in interface queue	50
Simulation time	5s

During the simulations following values are maintained for simulation parameters. The topography of X and Y is maintained as 1000 m and 1000 m. Distance between nodes is maintained the same between each node to emphasize the same signal strength. Moreover, Table I presenting simulator parameters that are maintained in each simulation experiment. The network performance is recorded only for 10 number of connected nodes in the network. Dependent variables are oriented to measure the network performance in the MANET that was modified by applying the proposed security mechanism. Moreover, the same network is affected by a malicious attack. PDR, EED, Throughput, and ADDR are considered as dependent variables. The network performance of different networks is measured. These networks are the controller network, the network that is affected by a malicious attack, and a network that is modified by applying the proposed security mechanism and affected by a malicious attack. A blackhole attack is considered in this experiment. Moreover, the position of the malicious node is changed, and observe the performance of the network that contained the proposed security solution. The positions are next to the source node, before the destination node, and central place in the network. Following assumptions are considered during the experiment.

- All nodes are considered to be identical in software and hardware configurations.
- All the nodes except malicious nodes show no malicious behavior during the communication.
- Distance between two nodes is identical in the network.
- During communication, the energy of a node is not the critical factor in the network.
- Nodes in the network are not involved in any other communication during the experiment.
- The updated routing protocol with the proposed security mechanism is available in the nodes in the network.
- No records are available in the malicious table in each node at the start of the simulation.

Network performance is measured using four different types of performance matrices. PDR is the ratio between the total number of packets sent by the source node and the total number of packets received by the destination node through the established route. This value is a percentage value. All the types of packets that are communicated between the source node and the destination node are considered to calculate the PDR value. Data packets and routing packets are counted to calculate the PDR value [4], [5] in MANET. AEED is an average amount of time [28] that is taken by a data packet to reach the destination node from the source node [4]. Units are seconds. Only data packets are considered to calculate the AEED value. Throughput is a ratio between the total number of packets received by the destination node over the total time taken to receive all packets [4], [29]. Units are bytes per second (bps). SPTIN is a ratio between the total processing time of all the connected nodes in the network and the number of connected nodes in the network [4].

V. RESULTS AND DISCUSSION

Figure 5 is a graph plotted between PDR values and three different networks that are mentioned earlier. Byte values of routing packets and data packets are considered to calculate the PDR value. The controller network shows nearly 84.00% of data delivery during the simulation. The network affected by a blackhole attack shows the lowest PDR value during the simulation due to the behavior of the blackhole attacking node which allows only routing packets but not data. After applying the solution same network shows 98.01% of data delivery

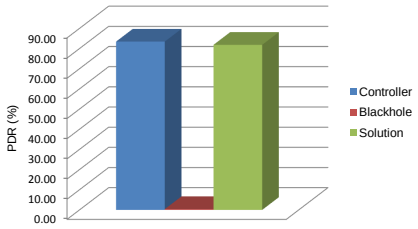

Fig. 5. The graph between PDR value VS different networks

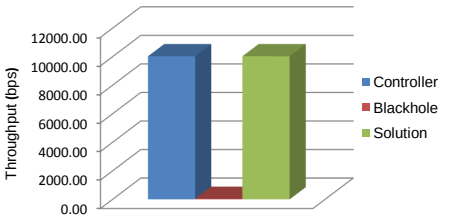

Fig. 7. The graph between Throughput value VS different networks

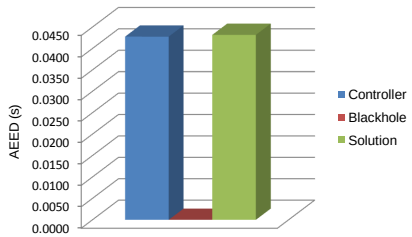

Fig. 6. The graph between AEED value VS different networks

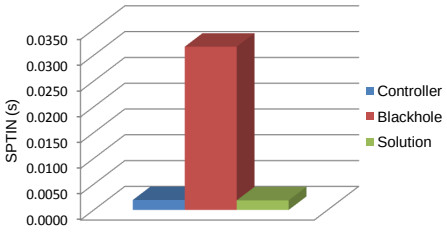

Fig. 8. The graph between SPTIN value VS different networks

compared to the controller network. The remaining bytes are dropped during the security enforcement in the network during the routing process. The packets which contain invalid and modified information are screened during the AODV routing process.

Figure 6 is a graph that is plotted between AEED values and three different networks: Controller network, blackhole attack affected network, and same network after applying the proposed solution. A data packet takes 0.0428 s to reach the destination node from the source node in the controller network. The network which is affected by a blackhole attack does not allow any data packets through it. Therefore AEED value is 0.00. Though, the data packet of the network in which the solution is applied takes approximately equal time as the controller network to reach from source to destination node. It is 100.9346% compared to the controller network.

Figure 7 is a graph plotted between Throughput values and three different networks: Controller network; blackhole attack affected network and same network after applying the proposed solution. Byte values of routing packet and data packets are considered to calculate the Throughput value. The controller network shows 10030.01 bps of Throughput value during the simulation. The network which is affected by the blackhole attack shows a 0.4471% Throughput value compared to the controller network. The throughput value of the network on which the solution is applied for the blackhole attack is 99.9988% compared to the controller network. The remaining portion of bytes is dropped because of the malicious screening process. These are routing responses from the blackhole node in the proposed solution.

Figure 8 is a graph plotted between SPTIN values and three different networks: controller network; blackhole attack affected network and same network after applying the proposed solution. THE highest SPTIN value is shown in the network that is affected by the blackhole attack. The total amount of data except routing packets are processed in the network that is affected by the blackhole node. Therefore SPTIN value is high. Though, 96.5660% of the SPTIN value is for the solution applied network compared to the controller network. Therefore it is equal to the performance of the controller network.

Table II shows the summary of the experiment. The results are converted into percentage values by comparing them with the values of the controller network. Empirical data show the impacts of blackhole attack on a network to degrade the network performances as defined in the theory. The proposed security mechanism to mitigate the blackhole attacks show approximately equal performances compared to the performances of the controller network. The reason behind the small amount of degraded performance of the proposed security mechanism is due to the discarding of routing packets from the blackhole node. The node that receives the RREP packet as the response from the blackhole node verifies the information in the RREP packet. The packets that contain infiltrated false information are screened from the proposed security mechanism. Therefore reply packets are discarded. Performances of the proposed security mechanism are acceptable compared to the performances of the controller network. These performances are nearly equal to the performances of the controller network. The Throughput value of the proposed solution proved that the data security is enforced in the communication between the source and the destination nodes in a MANET. Moreover, the AEED and SPTIN values of the proposed security solution proved that the proposed solution does not contain any complex calculations.

TABLE II
SUMMARIZED RESULTS

	Controller	Blackhole	Proposed Solution
PDR (%)	83.4400	0.4434	98.0825
AEED (s)	0.0428	∞	100.9346
Throughput (bps)	10030.0100	0.4471	99.9988
SPTIN (s)	0.001928103	1641.7073	96.5660

VI. Conclusion and Future Works

The results proved that the proposed security mechanism showed almost equal values of SPTIN and AEED compared to the controller network. Moreover, the Throughput value of the proposed solution confirmed that data delivery from the source node to the destination node was secured in the MANET. 99.99% of data were transferred from the source node reached destination node compared to the controller network. Therefore results proved that the proposed security mechanism is lightweight and secures the data in MANET between source and destination nodes. Therefore it is obvious that the main research objective of this research study is achieved.

Ability to join a node to a network depends on the decision made by its neighbor node. Therefore a node can control its neighbor node. Furthermore, the proposed security mechanism does not contain any features to evaluate or reconfirm the decision that was already made. The proposed security mechanism is failed to handle the cooperative blackhole attacks. Moreover, to protect a MANET from different types of network layer attacks, the security solution should be compatible to work on each layer of the OSI model. Updating the routing protocol is not enough to secure the network even from network layer attacks.

Our security mechanism is capable to detect any number of malicious nodes in any positions. It does not require any predefined conditions or predefined configurations. Moreover, the solution is flexible to use as a part of an IDS. The above paragraph concludes that the AODV routing protocol contains appropriate possibilities to alter the functions of route finding to apply for the screening of malicious nodes at route selection.

References

[1] Lee, F., "Routing in Mobile Ad hoc Networks". In Wang, X., (Ed.), *Mobile Ad-Hoc Networks: Protocol Design*, IntechOpen, 2011.

[2] Perking, P.E., & Royer, E., "Ad-hoc on-demand distance vector routing," In Proc 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, USA: IEEE, pp. 90-100, 1999.

[3] Rao, K.P.K., & Kalaiarasi, K., "A Survey on IEEE Standards for Mobile Ad Hoc Networks", In *IOSR Journal of Engineering*, 05(02), pp. 55-64, 2015.

[4] Ahamed, U., & Fernando, S,. Identifying the Impacts of Active and Passive Attacks on Network Layer in A Mobile Ad-hoc Network: A Simulation Perspective. In *International Journal of Advanced Computer Science and Applications(IJACSA)*, 11(11), 2020, https://doi.org/10.14569/IJACSA.2020.0111173

[5] Ahamed, U., & Fernando, S,. Identifying the Impacts of Node Mobility on Network layer based Active and Passive Attacks in Mobile Ad Hoc Networks: A Simulation Perspective. In Computing Science, Communication and Security. COMS2 2021. Gujarat, India: Springer, 2021, https://doi.org/10.1007/978-3-030-76776-1_18

[6] Khamayseh, Y., Bader, A., Mardini, W., & Yasein, M.B., "A New Protocol for Detecting Black Hole Nodes in Ad Hoc Networks." In *International Journal of Communication Networks and Information Security (IJCNIS)*, 3(1), 2011.

[7] Panos, C., Ntantogian, C., Malliaros, S., & Xenakis, C., "Analyzing, Quantifying, and Detecting the Blackhole attack in Infrastructure-less Networks", In *Computer Networks*, 2016, https://doi.org/10.1016/j.comnet.2016.12.006

[8] Semary, A.M.E., & Diab, H., "BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs Based on Chaotic Map," In *IEEE Access*, vol. 7, pp. 95197-95211, 2019, https://doi.org/10.1109/ACCESS.2019.2928804

[9] Arathy, K.S., & Sminesh, C.N., "A Novel Approach for Detection of Single and Collaborative Black Hole Attacks in MANET", In *Procedia Technology*, Vol. 25, pp. 264-271, 2016, https://doi.org/10.1016/j.protcy.2016.08.106

[10] Lachdhaf, S., Mazouzi, M., & Abid, M., "Secured AODV Routing Protocol for the Detection and Prevention of Black Hole Attack in Vanet", In *Advanced Computing: An International Journal (ACIJ)*, 9(1), 2018.

[11] Kumar, R., Tripathi, S., & Agrawal, R., "A secure handshaking aodv routing protocol (SHS-AODV)," In Proc. 2018 4th International Conference on Recent Advances in Information Technology (RAIT), Dhanbad, India, pp. 1-5, 2018.

[12] Hammamouche, A., Mawloud, O., Nabil, D., & Tari, A., "Lightweight reputation-based approach against simple and cooperative black-hole attacks for MANET," In *Journal of Information Security and Applications*, Volume 43, pp. 12-20, 2018, https://doi.org/10.1016/j.jisa.2018.10.004

[13] Dorri, A., Vaseghi, S., & Gharib, O., "DEBH: Detection and Elimination Black Holes in Mobile Ad Hoc Network," In *Computing Research Repository*, 2016.

[14] Aziz, N.W., Alsaad S.N., & Hmood, H.K., "Implementation of Lightweight Stream Cipher in AODV Routing Protocol for MANET," In Proc 2019 First International Conference of Computer and Applied Sciences (CAS), Baghdad, Iraq, pp. 210-215, 2016.

[15] Rajendran, N., Jawahar, P.K., & Priyadarshini, R., "Cross centric intrusion detection system for secure routing over black hole attacks in MANETs," In *Computer Communications*, Volume 148, pp. 129-135, 2019, https://doi.org/10.1016/j.comcom.2019.09.005

[16] Elmahdi, E., Yoo, S.M., & Sharshembiev, K., "Secure and reliable data forwarding using homomorphic encryption against blackhole attacks in mobile ad hoc networks," In *Journal of Information Security and Applications*, 51, 2020, https://doi.org/10.1016/j.jisa.2019.102425

[17] Shrestha, R., Han, K., Choi, D., & Han, S., "A Novel Cross Layer Intrusion Detection System in MANET," In Proc. 24th IEEE International Conference on Advanced Information Networking and Applications, Perth, WA, Australia, pp. 647-654, 2010, https://doi.org/10.1109/AINA.2010.52

[18] Jhaveri, R.H., Patel, S.J., & Jinwala-la, D.C., "A Novel Solution for Grayhole Attack in AODV Based MANETs". In Das, V.V., & Stephen, J., (Eds.) Advances in Communication, Network, and Computing. CNC 2012. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 108. Springer, Berlin, Heidelberg, 2012.

[19] Jhaveri, R.H., Patel S.J., & Jinwa-la D.C., "Improving Route Discovery for AODV to Prevent Blackhole and Grayhole Attacks in MANETs INFOCOMP," In *Journal of Computer Science*, 11(1), pp. 1-12, 2012

[20] Ibrahim, H.M., Omar, N.M., & William, E.K., "Detection and Removal of Gray, Black and Cooperative Black Hole Attacks in AODV Technique" In *International Journal of Advanced Computer Science and Applications (IJACSA)*, 6(5), 2015.

[21] Dhaka, A., Nandal, A., & Dhaka, R.S., "Gray and Black Hole Attack Identification Using Control Packets in MANETs," In *Procedia Computer Science*, Volume 54, pp. 83-91, 2016, https://doi.org/10.1016/j.procs.2015.06.010

[22] Subba, B., Biswas, S., & Karmakar, S., "Intrusion detection in Mobile Ad-hoc Networks: Bayesian game formulation," In *Engineering Science and Technology, an International Journal*, 19(2), pp. 782-799, 2016.

[23] Vinayagam, J., Balaswamy, C., & Soundararajan, K., "Certain Investigation on MANET Security with Routing and Blackhole Attacks Detection," In *Procedia Computer Science*, Volume 165, pp. 196-208, 2019 https://doi.org/10.1016/j.procs.2020.01.091

[24] Yilmaz, L., Toward Agent-Supported and Agent-Monitored Model-Driven Simulation Engineering. In Yilmaz, L., (Ed.), Concepts and Methodologies for Modeling and Simulation. Simulation Foundations, Methods and Applications. 2015, Springer, Cham, https://doi.org/10.1007/978-3-319-15096-3_1

[25] Sosa, R., Computational Modelling of Teamwork in Design. In Cash, P., Stanković, T., & Štorga, M., (Eds.), Experimental Design Research. 2016, Springer, Cham, 2016, https://doi.org/10.1007/978-3-319-33781-4 10

[26] The ns Manual [online]. Available at: http://www.isi.edu/nsnam/ns/nsdocumentation.html, 2011. [Accessed: Dec. 01 2021]

[27] Lan, K.C., SAMAN Publications/Talks. Available: https://www.isi.edu/saman/paper.html, 2003. [Accessed: Dec. 01 2020]

[28] Conti, M., "Body, personal, and local ad hoc wireless networks". The handbook of ad hoc wireless networks. CRC Press, Inc., USA, pp.3–24, 2003.

[29] Beraldi, R., & Baldoni, R., "Unicast routing techniques for mobile ad hoc networks". The handbook of ad hoc wireless networks. CRC Press, Inc., USA, pp. 127–148, 2003.