www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Vol.8, Issue.2, April 2020
Research Paper

Int. J. Sc. Res. in Network Security and Communication

E-ISSN:2321-3256

Reduce Impact Blackhole Attack in AODV Protocol

Z. Sh Alnadhery[1*], S. M. Baneamoon[2]

[1]Dept. of IT, College of Engineering & Information Technology, AL Rayan University, Hadhramout, Yemen
[2]Dept. of Computer Engineering, College of Engineering & Petroleum, College of Computers & IT, Hadhramout University, Hadhramout, Yemen

**Corresponding Author: z.alnodery@alrayan-university.edu.ye, Tel.: +00967-737679489*

Received: 19/Feb/2020, Accepted: 25/Mar/2020, Published: 30/Apr/2020

***Abstract*—** One of the most famous technologies in the networks is MANET technology, which is used in medical, military and other fields. MANET is a group of nodes that connect between them without the access point. AODV protocol is not provided with protection mechanisms because the primary purpose of this protocol is to quickly deliver packets to the destination. This is the main reason for its being attacked by malicious nodes. One of these attacks is a blackhole attack where the malicious node sends a fake message to the source that the shortest path to the destination passes through this malicious node. Then, the packets are dropped, which reduces the effectiveness and performance of AODV. In this paper, we proposed a SPAODV method to protect from blackhole attack and reduce its impact. In the SPAODV method, after the source node receives an RREP message, CHECKVERIFY will be sent to all proposed routes to confirm the route to the destination by the source node. The desired destination is the only node that can confirm the validity of the path by sending VERIFY to the source. Results of simulation by using NS2 showed that the SPAODV method better protection and better performance in AODV under blackhole attack networks compared to an EAODV method and a MAODV method.

***Keywords*—** AODV, SPAODV, Blackhole attack, Routing Overhead, NS2.

I. INTRODUCTION

Mobile Ad hoc Network (MANET) is a set of nodes that communicate among themselves without relying on infrastructure to maintain the network. Nodes may act as a source, destination or router [1]. Routing protocols in MANET are classified into three categories: Reactive routing protocol (on demand) like Ad hoc On-Demand Distance Vector Protocol (AODV), Proactive routing protocol (table-driven) like Optimized Link State Routing Algorithm (OLSR), and Hybrid routing protocol (mixed between Reactive and Proactive) like Zone Routing Protocol (ZRP) [2]. It can be used in military applications and wireless sensor network (WSN). AODV routing protocol is a reactive routing protocol, and it used in a lot of networks like e.g. (MANETs, mesh and sensor networks). AODV protocol is not provided with protection mechanisms because the primary purpose of this protocol is to quickly deliver packets to the destination and this protocol assumes that all nodes in its network are normal nodes, and not contain malicious nodes [3]. These the main reasons which made the protocol vulnerable to many attacks e.g. (black hole attack, gray hole attack, wormhole attack and so on).

The blackhole attack is effective and devastating and does not require complicated technologies in AODV networks [4]. This attack works during the process of detecting the path, the malicious node sends a fake message to the source that the shortest path to the destination passes through this malicious node. In this paper, the authors developed the MAODV method proposed in [5]. Our method is not concerned with searching for malicious nodes or deleting them from the network, but rather is interested in searching for safe paths to the desired destination node by adding some routing messages to reduce the impact of the malicious node. The authors used Safe Protection AODV (SPAODV) in our proposed method in this paper. The authors organized this paper as follows: section II dealt with an overview of AODV protocol, as well as a black hole attack on this protocol as the background of the paper. Discusses some of the previous literature and explains its limits in section III. Section IV gives details of the proposed model for processing a black hole attack. In section V, Results and discussion presented by simulation. Finally, section VI, Conclusion of the paper and the results of the implementation with some future work.

II. BACKGROUND

A. AODV Overview

In the AODV network, nodes do not care about the path to the other node unless there are packets to send. AODV has a set of routing control messages to complete the transfer of data between nodes these control messages are Route Request (RREQ), Route Reply (RREP), Route Error (RERR) and also hello Message [6]. As any protocol in the reactive routing protocol, AODV defines two main processes:

- Route discovery: When the source wants to send a packet to the destination, it looks for the path in the

routing table. If it does not find the path, it generates RREQ and sends it as a broadcast. Any intermediate node has the right path, or if the message reaches the destination, the node generates RREP that is sent as unicast to the source node.

- Route maintenance: If any node is out of the network or there is a break in the links, the neighbor node generates RERR then sends it to the source node to discover a new path.

B. Blackhole Attack Overview

AODV is not provided with protection mechanisms because the primary purpose of this protocol is to quickly deliver packets to the destination. This protocol assumes that all nodes in its network are normal nodes and not contain malicious nodes. These the main reasons which made the protocol vulnerable to many attacks for example (blackhole attack and warmhole attack). The blackhole attack is a type of denial of service attack where the malicious nodes send a fake reply to the source that contains it has a valid path and also the highest sequence number path to the destination [7]. One of the main disadvantages of the black hole attack is to reduce network performance because it deletes the packets that are attached to it. In the black hole attack, if it found a single malicious node, it called a single blackhole attack. The presence of more than a malicious node in the AODV network called a collaborative black hole attack [8]. In the blackhole attack, malicious nodes generate a fake RREP with a higher sequence number value, then send it to the nearest intermediate node and then forward it to the source nodes. The source will use the proposed path from the malicious node as the best and shortest path to the destination. When the data packet reaches the malicious node it drops and deletes it then does not reach it to the desired destination.

III. RELATED WORK

Here, the authors will present some suggested mechanisms for dealing with the black hole and then mention some limitations in their mechanisms.

A new method to immediately identify the blackhole attack and prevent it from occurring was introduced by M. Ebrahimi and S. Jamali (2016) [9]. In this method, the authors used the firefly algorithm. The firefly algorithm is biologically motivated. In this method, a timer is used to collect responses. The source store received a reply to the response table. In this table, a number is assigned to each node as the truth level. With every correct response, the value of the truth increases. The data is sent to the chosen path. The results of the simulation show that the proposed method has a better performance compared to AODV under the blackhole attack. The value of PDR is still relatively unacceptable because malicious nodes delete the nodes as usual until they are discovered and this decreases the overall network efficiency.

A trusted-fuzzy-ad-hoc routing protocol to upgrade the trust between the nodes to mitigate blackhole attacks was proposed by A. Sharma and P.K. Johari (2017) [10]. In this method, the source sends RREQ and then receives RREP messages. If it receives the RREP message with a higher sequence number, it sends a message to confirm that. if it receives the RREP message with a higher sequence number, the node will consider as the malicious node. Then block that node. This method showed improvement in PDR, Throughput and Routing Overhead compared with AODV with blackhole attack. However, the malicious nodes were able to delete lots of packets, approximately 45%. A large number of confirmation operations increased routing overhead. all of this affects the performance of the network.

A routing algorithm that calls EAODV that based on sending fake packets to detecting and removing malicious nodes was proposed by T. Delkesh and M. A. Jamali (2018) [11]. In this method, the source node sends fake RREQ, so any node that responds to this message is classified as a malicious node and added to the black hole list that is excluded from the network, then the source shares the list with the rest of the network nodes. Results of the method indicate that the PDR, throughput, and EED are better compared to the IDS method. However, fake route messages lead to an increase in routing overhead. Also, the entire network is busy looking for the alleged paths (which are not originally present), as this method is not practical in real life.

The modification in AODV that called the MAODV method to improve AODV under the blackhole attack was given by A. Chavan, D. S. Kurule and P. U. Der (2016) [5], the authors. The source sends a request packet to the desired destination. If the packet reaches the desired destination, a reply packet is created. An intermediate node that in the path creates verifies packet that is sent to the destination. When the reply message arrives at the source node it sends CHECKVRF to the destination as well. The requested destination compares the CHECKVRF packet to the VERIFY packet. If they match the FINALREPLY packet will send to the source. Malicious nodes cannot create the FINALREPLY packet, so the path is safe. PDR and throughput in the case of AODV and AODV after modifications are the same. However, the routing packets in the network resulted in a significant increase in routing overhead compared to AODV without malicious node.

Previous methods urge more effort to increase protection for AODV as well as to try to increase network performance in the presence of the attack.

IV. PROPOSED MODELLING

Failure to provide AODV with adequate protection left it vulnerable to numerous attacks. One of the most dangerous, simplest and most destructive attacks is the blackhole attacks. In this section, we will present the details of the proposed method in this paper called Safe Protection Ad hoc On-Demand Distance Vector (SPAODV). Through this method, we have tried to protect AODV from blackhole attacks with both single and collaborative types.

The proposed method “SPAODV” is shown in Fig. 1 as a flow chart, and as pseudocode in Fig. 2.

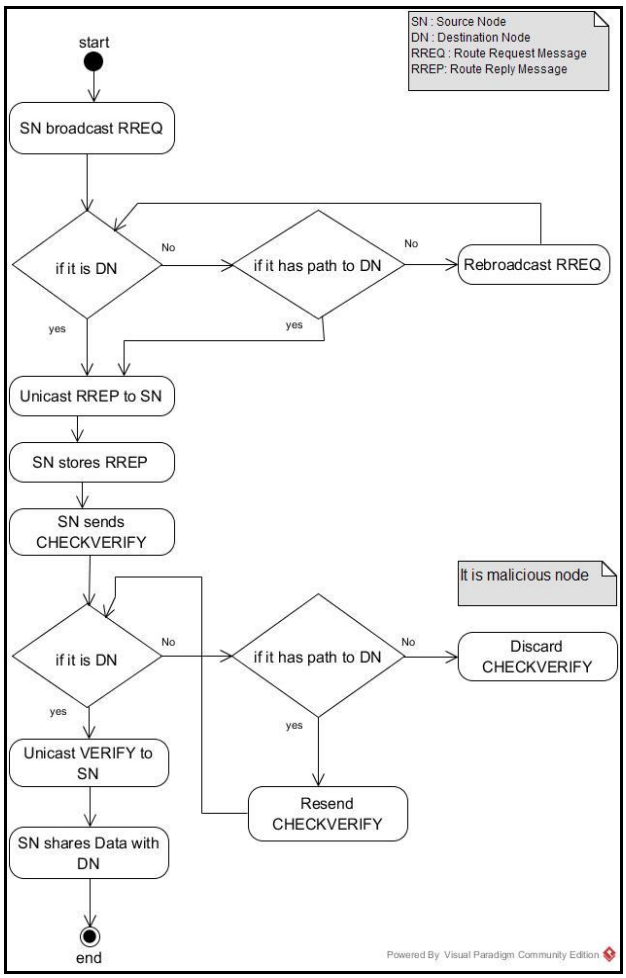

Figure 1. Flow Chart SPAODV Method

SN: Source Node
DN: Destination Node
IN: Intermediate
RREQ: Route Request
RREP: Route Reply
CHECKVERIFY: Check verify if the path leads to the destination
VERIFY: Confirm from destination

Begin
SN broadcast RREQ
If it is DN
Create RREP
Else
If IN has path to DN
Create RREP
Else Rebroadcast RREQ
End if
Send RREP as unicast to SN
SN stores RREP
For Each RREP do
SN sends CHECKVERIFY
If it is DN
Create VERIFY
Else
If it has path to DN
Resend CHECKVERIFY to DN
Else if it doesn't have path to DN or it is Malicious Node
Discard CHECKVERIFY
End if
End for
DN send VERIFY to SN
SN shares data with DN
End

Figure 2. Pseudocode of SPAODV Method

In our proposed method, the authors are not concerned with detecting or deleting malicious nodes that cause the blackhole attack. Rather, the SPAODV method looks for the safest paths that are free from malicious nodes to reach the desired destination. The SPAODV method is divided into three phases:

1) **Exploration phase:** When the source node wants to send packets to a specific node within the network, it sends a Route Request Message (RREQ) as a Broadcast to all the neighbor nodes in the range of source node. When the RREQ message arrives at the intermediate node, it is looking at its routing table. If it finds the short path that connects to the desired destination, it creates a Route Reply Message (RREP). Then send it to the source node as unicast. If it does not find the required path, it will resend RREQ as a broadcast to all neighboring nodes with an increase in the hop count by 1. If the RREQ message reaches the desired destination, then it will choose the shortest path to reach the source depending on two criteria, the first criteria are the lowest hop count and the second criteria is the highest sequence number from all RREQ that reaches to the destination from the different paths, then creates the RREP message and send it to the source node as unicast. At this point, the malicious nodes exploit the absence of a specific secure path to reach the desired destination, which will falsely claim that it has the shortest path to the desired destination, then creates a fake RREP message with an increase in the value of sequence number which is also sent to the source.

2) ***Verification phase****:* The source node collects RREP messages delivered to it from the intermediate nodes and the desired destination node, as well as from the malicious nodes in the network. In unprotected regular AODV networks, it will choose the shortest path and the highest in the sequence number, then send data via that path that was chosen, and usually, in the event of a malicious node, the nodes will be sent to it because it has a higher sequence number. As for our proposed method, the source node creates CHECKVERIFY message that will be sent via the proposed paths via RREP messages, and what distinguishes the CHECKVERIFY message is that it can only respond to it the desired destination and thus we will

prevent malicious nodes from exploiting the lack of protection in AODV networks in the false claim of paths to the desired destination. Once the CHECKVERIFY message reaches the desired destination node it creates the VERIFY message that is sent to the source node as unicast. The arrival of this message to the source node gives a guarantee to the source node that the message is sent by the desired destination node.

3) ***The Data Transmission phase:*** When the source receives the VERIFY message which is the guarantee of the path's security and that it is free of malicious nodes it starts sending data to the desired destination node.

This method will be successful as long as there is at least one safe path to reach to the desired destination node, but if all paths leading to the destination contain malicious nodes then the method will need to be supported with an additional mechanism that works to detect and isolate or delete the malicious nodes from the entire network.

V. RESULTS AND DISCUSSIONS

A. Performance Metrics

1) Packet Delivery Ratio: is the ratio of the total number of packets sent (PS) from the source node to the number of packets received (PR) to the destination node.

$$PDR = (\sum PR / \sum PS) * 100 \quad (1)$$

2) Throughput: This metric represents the total amount of data or actual packets received (PR) from the sender divided by the time (T) taken by the receiver to obtain the last packet.

$$Throughput = \sum ((PR) / T) * 0.008 \quad (2)$$

3) Average Delay: represents average end-to-end delay and refers to the average period time mean arrive time (TA) subtract from send time (TS) needed for delivering data (PR) from the source node to the destination node.

$$Average\ EED = \sum (TA - TS) / \sum PR \quad (3)$$

4) Routing Overhead: This describes the number of routing packets (RP) for path detection and path maintenance relative to the number of packets received (PR).

$$Routing\ Overhead = \sum RP / PR \quad (4)$$

B. Simulation Environment

To simulate SPAODV We used NS2. The area was estimated to be 1000 * 1000 m. The number of malicious nodes in the network is 1 and 5 nodes respectively to obtain results in both types of attack. static mode is used in this simulation. the proposed method can be applied in the mobile environment. The rest of the properties are shown in Table I.

TABLE I. SIMULATION PARAMETERS

parameter	value
Type of attack	Blackhole attack
Simulation tool	NS2.35
Simulation area	1000 * 1000
Simulation time	500s
Number of nodes	10,30,40,50,60,70,80,90,100
Transmission range	250m
Data rate	0.1 Mb
MAC type	IEEE 802.11
Mobility model	Static mode
Traffic type	UDP - CBR
Packet size	512
Routing protocol	AODV
No. of blackhole nodes	1 and 5 nodes
connection	5

C. Result

The authors proposed the SPAODV method to protect the AODV protocol from single and collaborative blackhole attacks. Then reduced the negative effects of the attack on the protocol. The results demonstrated the ability and effectiveness of the proposed method to protect the AODV protocol from the blackhole attack. In this study, SPAODV, EAODV, and MAODV methods were compared.

1) Packet Delivery Ratio: The malicious nodes that cause the blackhole attack aim to reduce network performance by claiming that they have the path to the destination and then delete Packets, which reduces the PDR. In AODV with single or cooperative blackhole attack, the PDR decreases significantly and reaches zero when these malicious nodes increase in the network.

The EAODV method attempted to address the blackhole attack and succeeded in raising the PDR but the malicious nodes were still able to delete some packets. Our method "SPAODV" succeeded in preventing malicious nodes from deleting packages that suggest fake paths to obtain the packages and then delete them by suggesting safe paths to the desired destination that be free of malicious nodes.

As shown in Fig. 3, the value of the PDR in the SPAODV method is 6% better than the EAODV method in AODV with the single blackhole attack while the results in the SPAODV method and MAODV method are very close.

In AODV with the cooperative blackhole attack (five malicious nodes in this study) as shown in Fig. 4, the value of PDR in the SPAODV method is 11% better than the EAODV method. Also, the results were close to the SPAODV method and the MAODV method.

This demonstrates that our proposed method in this study can protect the packets from deletion by malicious nodes which leads to raising the values of PDR and maintaining the quality and performance of AODV networks despite the presence of malicious nodes that cause single and cooperative blackhole attack.

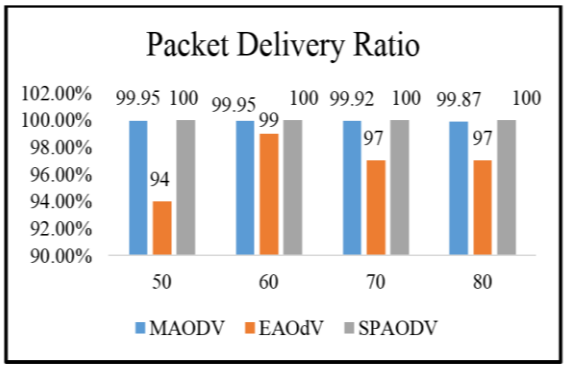

Figure 3. Packet Delivery Ratio with one malicious node

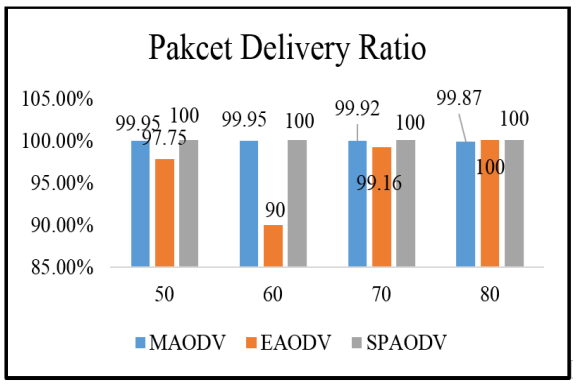

Figure 4. Packet Delivery Ratio with five malicious nodes

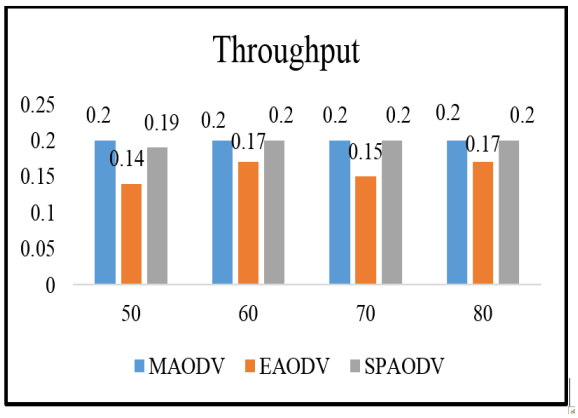

Figure 5. Throughput with one malicious node

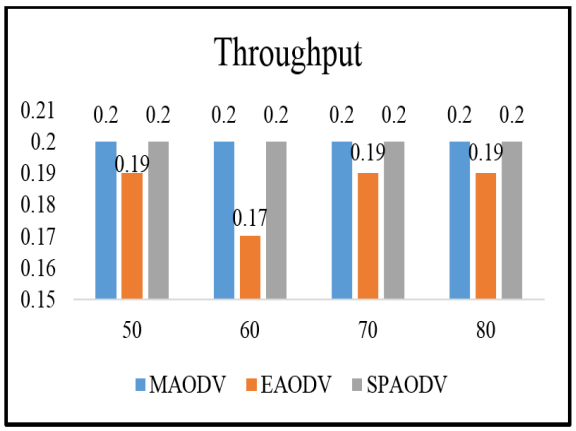

Figure 6. Throughput with five malicious nodes

2) Throughput: The most important factors affecting throughput in AODV networks are the ability to successfully deliver the most packets to the desired destination in the shortest possible time. In AODV networks with blackhole attack, these nodes delete the packets and do not deliver them to the correct path leading to the desired destination node. This leads to a decrease in the value of throughput too low rates, which negatively affects the performance of the network and may lead to network failure.

As shown in Fig. 5, it shows that the value of throughput in SPAODV and MAODV methods were not affected by the malicious nodes in AODV networks with single malicious node, so the results were almost equal, while in the EAODV method, the malicious node was able to delete many packets, which led to a decrease the value of throughput.

In AODV networks with the cooperative blackhole attack, the results of the EAODV method were not better than their results in AODV networks with the single blackhole attack. The results of the SPAODV method and the MAODV method were approximately equal in AODV networks containing five malicious nodes. As shown in Fig. 6.

3) Average End to End Delay: The distance between the nodes is one of the most important factors affecting average end to end delay, but the malicious nodes also delay the arrival of packets to the desired destination or we can say that the malicious nodes do not send the packets to the correct path, but delete them, which leads to an increase in average EED in AODV networks. The distance between the nodes is one of the most important factors affecting average end to end delay, but the malicious nodes also delay the arrival of packets to the desired destination or we can say that the malicious nodes do not send the packets to the correct path, but delete them, which leads to an increase in average EED in AODV networks.

As shown in Fig. 7, the SPAODV method was much better than the EAODV method because the malicious nodes sometimes managed to block the arrival of the beams to the desired destination in the EAODV method. As for the MAODV method, the SPAODV method was also better. This is for AODV networks with the single blackhole attack.

As for AODV networks with the cooperative blackhole attack (five malicious nodes) the SPAODV method gives a shorter timing than the MAODV method and also the EAODV method. As shown in Fig. 8.

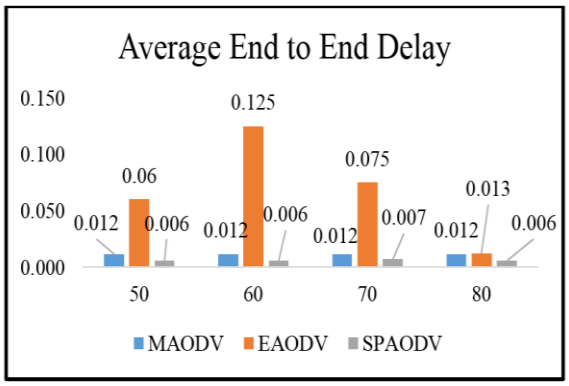

Figure 7. Average End to End Delay with one malicious node

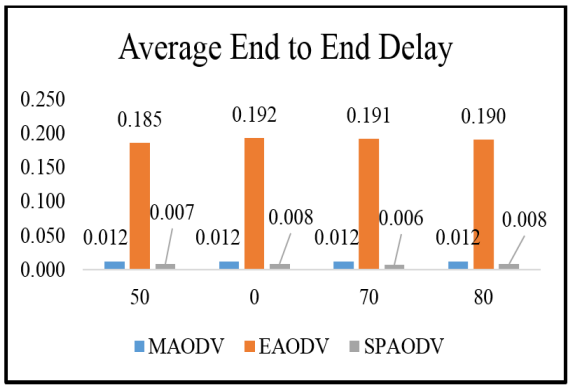

Figure 8. Average End to End Delay with five malicious nodes

4) Routing Overhead: The value of routing overhead increases when sending routing messages within the network increases. Malicious nodes generate fake routing messages then resend them to the intermediate nodes, which leads to an increase in the routing overhead value in the network. It is important to reduce the routing overhead value to keep the energy of nodes in the network.

The SPAODV method proposed in this study does not require lots of routing messages to determine the safe path to reach the desired destination, and this helped to reduce the routing overhead in AODV networks with single or cooperative blackhole attack.

The results showed a significant improvement in the value of routing overhead when applying the method of SPAODV compared to the method of MAODV that checks the path at each intermediate node and this is what led to an increase in the value of routing overhead in the networks applied in it. This improvement is 95% in the reduction of the routing overhead value in AODV networks with the single blackhole attack. As shown in Table II and Fig. 9.

Also, our method "SPAODV" reduced the value of routing overhead in single blackhole attack networks, as well as in cooperative blackhole attack networks, the SPAODV method gave lower values of the MAODV method by 96% as shown in also Table II and Fig. 10.

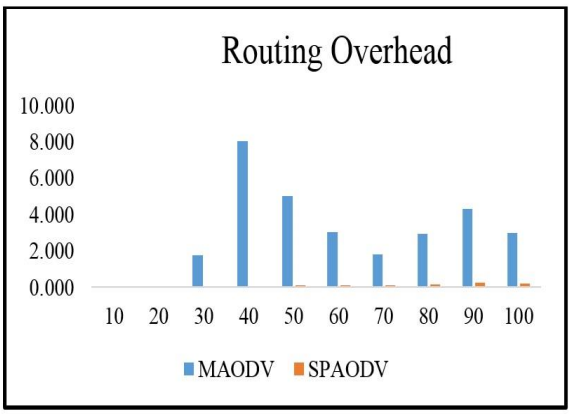

Figure 9. Routing Overhead with one malicious node

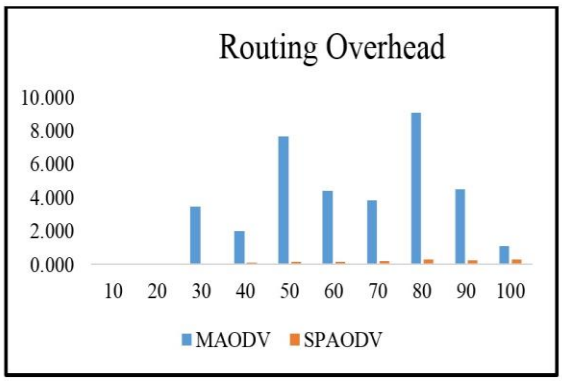

Figure 10. Routing Overhead with five malicious nodes

TABLE II. ROUTING OVERHEAD

Routing Overhead				
no	*One Malicious Node*		*Collaborative Malicious Node*	
	MAODV	SPAODV	MAODV	SPAODV (five malicious node)
10	0.00458	0.01642	0.00458	0.02530
30	1.75011	0.04712	3.46538	0.07688
40	8.01002	0.06610	1.99703	0.10243
50	5.02014	0.09101	7.67540	0.15640
60	3.01203	0.10870	4.42413	0.16876
70	1.80134	0.12655	3.82370	0.20152
80	2.91570	0.15801	9.04776	0.27766
90	4.31807	0.25923	4.50801	0.25949
100	2.98731	0.18115	1.09789	0.29674

Hence the authors conclude that the method proposed in this study called Safe Protection AODV is effective in reducing the negative impact of the malicious nodes that cause the blackhole attack in both types: single and cooperative blackhole attack.

VI. CONCLUSION

The malicious nodes that cause the blackhole attack in AODV networks negatively affect the performance of the network and most of the time lead to the destruction and stopped the network, and that the malicious nodes operate to raise routing overhead which exhausts the energy of the nodes without being able to send packets to the desired nodes to communicate with them. The SPAODV method

reduces the impact of malicious nodes that causes single and collaborative blackhole attack in AODV networks. Our method 'SPAODV, sends a confirmation message that called CHECKVERIFY to the desired destination. If the source node receives a VERIFY message, the path is safe and free of malicious nodes because the malicious nodes cannot respond to the CHECKVERIFY message. The result of the simulation showed a significant improvement in reducing Routing Overhead by over 96% compared to the MAODV method and also reducing the percentage of dropping packets to 10% compared to the EAODV method.

In future work, we try to find a uniform protection algorithm against blackhole attack, gray hole attack, and wormhole attack while reducing congestion in AODV.

REFERENCES

[1] D. Gorine and R. Saleh, "Performance Analysis of Routing Protocols in MANET Under Malicious Attacks," *International Journal of Network Security & Its Applications (IJNSA*), Vol.**11**, No.**2**, pp.**1-12**, **2019**.

[2] A. R. Mahlous, "The Effectiveness of Mobile Ad Hoc Routing Protocols Under a Gray Hole Attack," *International Journal on Information Technologies & Security*, Vol.**11**, No.**1**, **2019**.

[3] R. Kumari, P. Nand, "Performance Analysis of Existing Routing Protocols," *Int. Journal of Scientific Research in Computer Science and Engineering*, Vol.**5**, Issue.**5,** pp.**47-50**, **2017**.

[4] Ch. Panos, Ch. Ntantogian, S. Malliaros and Ch. Xenakis, "Analyzing, Quantifying, and Detecting the Blackhole Attack in Infrastructure-less Networks," *Computer Networks,* Vol.**113**, pp.**94-110**, **2016**.

[5] A. A. Chavan, D. S. Kurule and P. U. Der, "Performance Analysis of AODV and DSDV Routing Protocol in MANET and Modifications in AODV against Blackhole Attack," *In the Procedia Computer Science*, Vol.**79**, pp. **835-844**, **2016**.

[6] R. Rana and R. Kumar, "Performance Analysis of AODV in Presence of Malicious Node," *Acta Electronica Malaysia (AEM), Zibeline International Publishing*, Vol.**3**, No.**1**, pp.**1-5**, **2019**.

[7] M. Salehi, A. Boukerche and A. Darehshoorzadeh, "Modeling and Performance Evaluation of Security Attacks on Opportunistic Routing Protocols for Multihop Wireless Networks," *Ad Hoc Networks,* Vol.**50**, pp.**88-101**, **2016**.

[8] S. Ali, "Enhanced Virtual Private Network Authenticated Ad Hoc on Demand Distance Vector Routing*," International Journal of Innovative Engineering and Management Research*, Vol.**7**, Issue.**12**, pp.**190-197**, **2018**.

[9] M. Ebrahimi and S. Jamali, "Securing AODV Routing Protocol Against the Blackhole Attack Using Firefly Algorithm," *International Journal of Applied Operational Research*, Vol.**6**, No.**4**, pp.**53-64**, **2016**.

[10] A. Sharma and P.K. Johari, "Eliminating Collaborative Blackhole Attack by Using Fuzzy Logic in Mobile Ad-hoc Network," *International Journal of Computer Sciences and Engineering*, Vol.**5**, Issue.**5**, pp.**34-41**, **2017**.

[11] T. Delkesh and M. A. Jamali, "EAODV: Detection and Removal of Multiple Blackhole Attacks Through Sending Forged Packets in MANETs," *Journal of Ambient Intelligence and Humanized Computing*, Vol.**10**, No.**5**, pp.**1897-1914**, **2018**.

Authors Profile

Mr. **Zain Sharif Mohammed Zain Alnadhery** received B.Sc. degree in computer science from Taiz University, Taiz, Yemen in 2013. He is studying M.Sc. degree in Information Technology at AL-Rayan University, Hadhramout, Yemen now. He is interested in areas as network security, big data, and data mining.

Dr. **Saeed Mohammed Baneamoon** received the B.Sc. and the M.Sc. degrees in computer engineering from Technical University, Sofia, Bulgaria in 1996, the M.Sc. degree in computer science from University of Technology, Baghdad, Iraq in 2003 and the Ph.D. degree in Artificial Intelligence from Universiti Sains Malaysia, USM, Penang, Malaysia in 2011. He is an Associate Professor in Department of Computer Engineering, College of Engineering & Petroleum, Hadhramout University, Hadhramout, Yemen from 2018 till now. He is a Head of Computer Engineering Department, College of Engineering & Petroleum, Hadhramout University, Hadhramout, Yemen from 2014 till now. He is a Deputy Dean, College of Computers & Information technology Yemen from 2017 till now. His interest focuses on the field of Artificial Intelligence and Robotics. He has published several papers in journals and conferences.

