Detection and Prevention of Blackhole Attack in the AOMDV Routing Protocol

Abdelaziz Tami, Sofiane Boukli Hacene, and Moussa Ali Cherif

Original scientific article

***Abstract*—Mobile ad-hoc network is a collection of dynamically organized nodes where each node acts as a host and router. Mobile ad-hoc networks are characterized by the lack of preexisting infrastructures or centralized administration. So, they are vulnerable to several types of attacks, especially the Blackhole attack. This attack is one of the most serious attacks in this kind of mobile networks. In this type of attack, the malicious node sends a false answer indicating that it has the shortest path to the destination node by increasing the sequence number and decreasing the number of hops. This will have a significant negative impact on source nodes which send their data packets through the malicious node to the destination. This malicious node drop received data packets and absorbs all network traffic. In order overcome this problem, securing routing protocols become a very important requirement in mobile ad-hoc networks. Multipath routing protocols are among the protocols affected by the Blackhole attack. In this paper, we propose an effective and efficient technique that avoids misbehavior of Blackhole nodes and facilitates the discovery for the most reliable paths for the secure transmission of data packets between communicating nodes in the well-known Ad hoc On-demand multi-path routing protocol (AOMDV). We implement and simulate our proposed technique using the ns 2.35 simulator. We also compared on how the three routing protocols AOMDV, AOMDV under Blackhole attack (BHAOMDV), and the proposed solution to counter the Blackhole attack (IDSAOMDV) performs. The results show the degradation on how AOMDV under attack performs, it also presents similarities between normal AOMDV and the proposed solution by isolating misbehaving node which has resulted in increase the performance metrics to the standard values of the AOMDV protocol.**

***Index terms*—Mobile ad-hoc networks, AOMDV, Blackhole attack, Secure routing, Performance evaluation.**

I. INTRODUCTION

MOBILE ad-hoc network is a set of autonomous mobile nodes connected by wireless connections [1]. Without the help of an infrastructure or a centralized administration, the nodes move freely and form a dynamic topology. In this kind of network, the nodes have a wireless interface to communicate with each other where each node can act as a host or a router. Communication between nodes is established according to certain common rules in the form of a routing protocol which allows the discovery, establishment and choice of the route for the transmission of data packets between the source and the destination through intermediate nodes. However, due to these characteristics, mobile ad-hoc networks are exposed to different types of attacks and their security is a difficult task [2]. In this paper, we focus our study on multi-path routing protocols, in particular, the AOMDV routing protocol [3], [4]. This protocol can search for multiple paths and choose the right route to send data packets. However, this protocol has no protection mechanism against any kind of attack. The Blackhole attack is one of the most dangerous problems that disrupt the communication between nodes within a network. In this attack the malicious node announces itself as having freshest path to the destination node; it sends a false response packet to the source node. So the source node, as soon as it receives this false response, it begins the transfer of the data packets through the malicious node to the destination node and absorbs all by received data packets and all other reply packets issued from by other nodes. Blackhole attacks can degrade on how the routing protocols in a very serious way performs, by falsifying the way of managing communications between nodes in ad-hoc network. For that, security of the routing becomes a primordial task to fight against this type of attack. In this paper, we propose an effective and efficient technique to detect and isolate misbehaving nodes, it also, ensure the discovery of most reliable and secure paths between communicating nodes in AOMDV routing protocol.

The rest of this paper is organized as follows. We present the AOMDV routing protocol in the following section. Section III deals with the Blackhole attack mechanism. Section IV presents the existing mechanisms in literature to detect and isolate malicious nodes. Section V details our proposed security mechanism, this is followed by a detailed performance comparison study and results discussions in Section VI. Finally, in Section VII, we conclude our research work and present some perspectives.

II. AOMDV (AD-HOC ON DEMAND MULTIPATH DISTANCE VECTOR)

AOMDV is a distance vector reactive protocol and considered as an enhancement of the well-known AODV

Manuscript received October 29, 2019; revised October 12, 2020. Date of publication January 18, 2021. Date of current version January 18, 2021. The associate editor prof. Toni Perković has been coordinating the review of this manuscript and approved it for publication.

Authors are with the EEDIS Laboratory, Djillali Liabes University, Sidi Bel Abbes, Algeria (e-mails: {abaziz.tami, boukli, malicherif}@gmail.com, abdelaziz.tami@univsba.dz).

Digital Object Identifier (DOI): 10.24138/jcomss.v17i1.945

routing protocol [5], [6]. In the route discovery process, it discovers several paths loop-free and link-disjoint, but only one path will be considered as primary path and used when transmitting data packets; however, the remaining discovered paths are considered as alternative paths for the primary path when it becomes invalid. If all alternative paths become invalid, AOMDV starts a new route discovery process again. This protocol provides a set of route update rules to make sure that alternative paths are loop-free and link-disjoint. In the same way as AODV, AOMDV uses RREQ (Route Request) as a route discovery message, RREP (Route Reply) as a route response message, RERR (Route Error) as a route error message, and a HELLO message for monitoring the state of the links between the communicating nodes. In the route discovery process, the source node broadcasts the RREQ message in the network, so other nodes, either intermediate or destination, can accept duplicate RREQs and send multiple RREPs to the source node.

III. Blackhole Attack

The Blackhole attack is one of the most dangerous problems that disrupt the communication between nodes within a network [7]. In this attack, a malicious node upon receiving a RREQ, it responds immediately and without checking its routing table, that it has the shortest path, by announcing a fake RREP to the source node. In fact, this RREP has a high sequence number and a small hop count. However, other responses issued by other nodes arriving later to the source node will be ignored by the source node because it assumes that the malicious node has the freshest route to the destination node and that the route discovery process is complete. Then, the source node starts sending data packets to the malicious node in which drop them.

IV. Related Work

We present in this section the work related to our study. The problem of Blackhole attacks has been studied in several research studies. However, some work aims to find and secure the routing protocol against a single malicious node; so, other works are interested within the problem of several cooperative malicious nodes. There have been a number of solutions to overcome these security-related. On one hand, proposals that deal with the problem of routing security in terms of the behavior using control messages (RREP, RRER and RREQ) with respect to their contents, such as the number of hops and the destination sequence number. On the other hand, studies using cryptography for this kind of problem. In the following, we look at some related works. The solution proposed in [8] by Raj et al., performs an extra check to decide if RREP_seq_no is greater than a threshold value. At each time interval, the threshold value is dynamically updated. If the value of RREP_seq_no is greater than the threshold value, the node is suspected of being malicious and will be added to the blacklist. Thus, sending an ALARM control packet to its neighbors so that the RREPs coming from the malicious node will be ignored. The threshold value is the average of the difference in each time interval between the sequence number of the routing table and the sequence number in the RREP packet. The threshold value is updated each time a new node receives an RREP packet. This solution increases the Packet Delivery Ratio (PDR) with a minimum increase in the average end-to-end delay and normalized routing overhead. The main advantage of this technique is that the source node proclaims the malicious node to its neighbor's nodes to be ignored, but this method can also make mistakes when not malicious node may be entered into the blocked list according to its higher sequence number. On the other hand, this method can detect and drop simple and multiple Blackhole attacks, but it will be too complex for cooperative Blackhole attacks. Moreover, the routing overhead is considerably increased due to the updating of the threshold every time along with the forwarding of the ALARM control packet. To isolate malicious nodes and protect normal nodes from Blackhole attacks in the network, N. Mistry, et al. [9] proposed an improvement to the AODV protocol against Blackhole attacks. The advantage of this solution lies in the use of an extra function Pre_ReceiveReply (Packet P), the addition of a new table Cmg_RREP_Tab, a timer MOS_WAIT_TIME, and a variable (Mali_node) to the data structures in the AODV routing protocol. In the Pre_ReceiveReply (Packet P) function it keeps all the RREPs in the Cmg_RREP_Tab until time of MO_WAIT_TIME. The MOS_WAIT_TIME is initialized by half of the RREP_WAIT_TIME (during where the source node waits for the RREP) before regenerating the RREQ. However, the source node after receiving the first RREP waits for MOS_WAIT_TIME and during which it will save all future RREPs in the Cmg_RREP_Tab. Subsequently, the source node analyzes all the RREPs stored in the Cmg_RREP_Tab and ignores the RREP of the node whose destination sequence number is probably very high (this node is suspected to be malicious) and maintains identity of the malicious node, hence to ignore all the RREPs coming from this node in the future. Then, the selection of RREP with the highest destination sequence number in the Cmg_RREP_Tab that will be used in the recvReply (Packet P) function of the AODV to be used to send data packets. Additionally, to keep up the freshness of the Cmg_RREP_Tab, it is emptied as soon as an RREP is chosen. However, this solution does not add any control message to the AODV. The chance of increasing the normalized routing overhead is minimal. The PDR is increased with an acceptable end-to-end-delay. So, this solution can be used to detect and avoid simple and multiple Blackhole attacks, but introduces an increase in memory due to the use of Cmg_RREP_Tab. Mahmoud et al. [10] proposed a modified AODV routing protocol to avoid Blackhole attack in MANETs. Proposed Intrusion Avoidance System (IASAODV) detects and avoids the Blackhole nodes in two stages. The first step is based on counting RREQ and RREP control messages during route discovery. The second step is based on the Destination Sequence Number (DSN) of the RREP message, the number of RREP messages computed in the first step and the arrival time of RREP at the source. However, in the first step, a Route Reply Table is created to store all RREP messages from the destination node. The time to wait before data sending is considered twice the value of RREP_WAIT_TIME. As soon as the RREP_WAIT_TIME timer expires, the number of

RREP messages in the Route Reply Table (RRT) is checked in the second step. The existence of more than one RREP message in the RRT table signifies a Blackhole attack threat. In the case of receiving only one RREP message, the destination node is considered a trusted node and all data will be sent to it. The results obtained with this mechanism give better values for PDR, Throughput and Normalized Routing Load (NRL). This solution can detect and avoid simple and multiple Blackhole attacks, but introduces an increase in wait time and memory due to the doubled waiting of RREP_WAIT_TIME and the use of RRT. AOMDV routing protocol has also captured the interest of researchers in the field of detection and avoidance of Blackhole nodes. In [11], the authors proposed a detection mechanism for AOMDV. The proposed method is to send data packets across all possible routes after sending a random number of packets. In this solution, the destination node is modified to receive and compare the packets. If a malicious node causes an attack, the destination will know it because the data packet will not be received by it from the active route, and then send FINISH packet by another route to the source node.

TABLE I. LIMITATIONS OF EXISTING APPROACHES

Comparison Metric	Limitations of Existing Approaches
Detection of different types of Blackhole attacks	Proposed approaches [8], [9], [10], and [11] can detect and avoid single and multiple Blackhole attacks. Moreover, proposed approach [11] can detect cooperative Blackhole attacks, but it will be too complex for proposed approach [8] to detect cooperative Blackhole attacks.
Increase/decrease in performance metrics	In [10], the average end-to-end delay of the AODV protocol is less than the proposed IASAODV protocol due to the doubled waiting time. In [12], the packet delivery ratio is definitely highest with no malicious node in the environment. It decreases slowly with increasing number of malicious nodes. The average end-to-end delay increases gradually with incremented malicious nodes as time is taken by the encryption process with ECC. In [13], the end-to-end delay is higher in proposed scheme than the original AOMDV scheme when the number of malicious nodes is increased as time is taken by the splitting and encrypting of messages. The impact is present with higher data loss in the proposed scheme by increasing the malicious nodes. In [14], the packet delivery ratio stays holding the same amount (100%) in proposed scheme in the presence of any malicious nodes. The proposed scheme takes more time for delivering the packet, the throughput is higher in proposed scheme compared to the original scheme for the packet transmission. There is impact of multiple attackers in the proposed protocol because the scheme utilizes multiple paths simultaneously. The impact is present with higher data loss in proposed scheme by increasing the malicious nodes. The delay is higher for proposed scheme than the original AOMDV scheme when the number of malicious nodes is increased due to its procedures and security features.
Requirement of extra memory/database	Proposed approach [9] introduces an increase in memory due to the use of Cmg_RREP_Tab. Proposed approach [10] introduces an increase in wait time and memory due to the doubled waiting of RREP_WAIT_TIME and the use of Route Reply Table (RRT). Proposed approach [11] does not even require any extra memory.
Burden on intermediate nodes	In [11], no involvement of intermediate nodes is required for the proper functioning of the scheme thus preventing an extra burden on mobile intermediate nodes. Only sender and destination node is responsible for the proper functioning of approach. But, in [8], an extra burden on the energy of mobile nodes, due to the transmitted of ALARM messages to neighbors nodes. Also, in [13], and [14], every message is split into many parts, then the energy usage may increase because of the increased total size of the transmitted messages.
False detection ratio	False detection ratio of the proposed approach [8] is high, but it is negligible in the proposed approach [11] as it does not work on supposition.
Communication/routing overhead	In [8], the routing overhead is considerably increased due to the updating of the threshold every time interval along with the forwarding of the ALARM control packet. In [11], nominal communication overhead is present as the scheme does not involve additional control packets except the one which is sent only once. In [12], the normalized routing load grows with the number of Blackhole attacker nodes present in the situation, though the normalized routing load may vary depending on the number of packet transmission.

The source node after receiving FINISH packet, it stops sending data through the current route by purging the current entry from the routing table and starts sending packets through another route present in the routing table. This procedure will be repeated after sending data packets that are exponentially larger than the previous one until the entire transmission has been completed. This mechanism uses a counter that will be exponentially increased and it is possible to reduce the overhead of sending packets across all routes. The proposed approach has a negligible false detection ratio and can detect single, multiple and cooperative Blackhole attacks. It does not even require any extra memory and has nominal routing overhead. An Elliptic Curve Cryptography Based Data Transmission against Blackhole Attack in MANET mechanism was proposed by Sultana et al. [12]. In their solution, they implemented Elliptic Curve Cryptography (ECC) with the AOMDV routing protocol. In ECC, a public key cryptography mechanism that runs on a discrete logarithm problem with a smaller key size was used to encrypt the data packets to the source node before transmission. They have created a secure agent that generates the encrypted packet, then this packet reaches the destination by one of the selected multiple paths. In fact, the source node generates a private/public key pair. In the beginning, the source node chooses a random private key and generates a secret key from its own private key and the recipients public key. It encrypts the packet with the newly generated secret key and announces the public key. After that, the encrypted packet is sent through the AOMDV.

Upon receiving the encrypted packet by the destination node, it generates the same secret key using its own private key and the new public key of the source node. The destination node can decrypt the packet using its shared secret key and its private/public key pair to get the original data. In this case, it will be difficult for the malicious node to extract the private key from a secret key and the public key. The proposed mechanism ensures authentication and confidentiality for

secure data transmission. However, the main advantage with the use of ECC is, it takes less memory provides great security. So, this mechanism achieved a high-level of security. One of the challenges for this solution is the management and distribution of the keys as mobile nodes do not have a centralized administration. Authors in [13] proposed Secure and reliable data forwarding using homomorphic encryption against blackhole attacks in mobile ad hoc networks, in which there modified the earlier version [14] titled Securing Data Forwarding against Blackhole Attacks in Mobile Ad Hoc Networks. They extended AOMDV scheme to make data transmission be reliable and secure in the presence of malicious nodes in MANETs by distributing the parts of entire message into multiple paths and using a homomorphic encryption method for cryptography. The idea of this scheme is to assign a set of disjoint paths into a set of groups and several active disjoint paths are assigned to each group, where all disjoint paths are connected between a sender and a receiver. They split a message into many parts before the message is transmitted, and encrypt each part based on homomorphic encryption method. Then, the part of the message is transmitted to each group in order that only one encrypted part of the message is able to reach each group. Every node in each group can receive the same part of the message. Then, even if an intermediate node is misbehaving (dropping the part), the part of the message can be delivered to the destination through another path. Thus, the receiver is able to receive the whole encrypted parts of the message, decrypt the whole parts, combine them, and recover the whole message. The simulation results show that the proposed scheme provides a higher packet delivery ratio and throughput, which are good features for the emergency applications in MANETs. Moreover, the success rate of the proposed scheme to ensure and guarantee the delivery of the packet to the target is very high with many active paths in each group of the network. This scheme achieved a high level of security. One of the drawbacks for this solution is the increasing of the end-to-end delay due to the splitting and encrypting of messages. Table I shows limitations of existing approaches.

V. Proposed Mechanism

A. Working Principle of the Proposed Mechanism

The main goal of our IDSAOMDV is to detect, isolate and eliminate attacks from many malicious nodes. In the AOMDV, during the route discovery process, several paths can be discovered in order to choose one as main path for data packets transmission to the destination node. However, the selection criteria for this path is based on the sequence number and the hop count in order to get the shortest and freshest path. This criterion leads to threats that are used in Blackhole attacks. To overcome this problem, we have created a new function that returns two values, the first value (sum) is the sum of differences between the sequence number in the RREQ and the RREP packets and the second one (nrep) which is the number of received RREP packets. This function will be called from the standard recvRepp (p) function of the AOMDV protocol. The two values sum and nrep allow computing a threshold (TH) as a barrier against the sequence numbers announced by the Blackhole attackers and will secure the process of selecting main routes to transmit data packets. We recall that AOMDV protocol can choose a main path among several paths after checking the criterion: if (rt -> rt_seqno < rp-> rp_dst_seqno). However, in our technique, we changed this criteria as: if ((TH> rp -> rp_dst_seqno) && (rt -> rt_seqno< rp -> rp_dst_seqno)). This condition only allows keeping routes with a destination sequence number value lower than TH and at the same time higher than the sequence number defined in the routing table. However, the routing protocol might choose the appropriate route for data transmission. Thus, the other sequence number values will never be considered by the source node to avoid malicious nodes. So, this idea will allow finding secure routes and isolating Blackhole nodes from the network. A new additional table named ADDTABLE to store the RREP responses, and methods dealing with it, are implemented. The first function named (allrrep (p)) which records the RREPs in the ADDTABLE and it is called by the second function (prerrep (p)) which returns sum and nrep in order to compute the TH. The function (prerrep (p)) is called in the recvReply (p) function before the source node chooses the forwarding route. Fig. 1 shows the flowchart of our proposed mechanism.

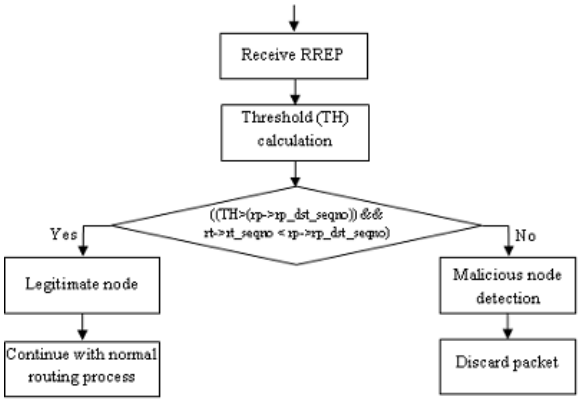

Fig. 1. Flowchart of the proposed mechanism

B. Proposed Algorithm

The following notations are used to express the proposed algorithm: SN: Source Node; DN: Destination Node; RREQ: Route Request; RREP: Route Reply; TH: Threshold; dif: Difference between sequence number of RREP and of RREQ; sum: Summation of dif; nrep: Replies number. The proposed detection and prevention algorithm are as follows:

```
Start the Route discovery process with SN and DN by using RREQ
and RREP packets;
Store all RREP packets in ADDTABLE;
while ADDTABLE is not emty do
    if rp- > rp_dst_seqno > rq- > rq_src_seqno
      then
          dif = ((rp- > rp_dst_seqno) - (rq- >
          rq_src_seqno));
          sum= sum + dif;
          nrep++ ;
      end
```

```
end
TH=sum/nrep ;
For all RREP responses;
if (TH > rp-> rp_dst_seqno) && (rt-> rt_seqno < rp-> rp_dst_seqno)
  then
      Legitimate node detection ;
      Continue with normal routing process;
else
      Malicious node detection ;
      Discard RREP;
end
```

Algorithm 1: Algorithm describing the detection and prevention mechanism

VI. Performance Evaluation And Result Discussions

To evaluate the performance of our mechanism, we have performed a detailed simulation study under the well known ns 2.35 simulator. We implemented three protocols AOMDV, BHAOMDV under Blackhole attacks, and our proposed solution IDSAOMDV.

A. Simulation Parameters

We use a random pattern of node mobility, where each node randomly moves in an area of 1500m_300m. The simulation time is 900 seconds, the pause time varied as (0s, 30s, 60s, 120s, 300s, 600s, 900s), the communicating nodes number varied as (10, 20, 30, 40) on 50 nodes of the network with 4 packets/second. The most speed is 20 m/s, the packet size is 512 bytes. The attacking nodes number varied from 1 to 5. We studied four scenarios, and the Gnuplot version 5.2 represents graphs. Table II shows the main simulation parameters.

Table II. Simulation Parameters

Parameter	Value
Simulation area (m × m)	1500 × 300
Number of nodes	50
Simulation time (s)	900
Mobility Model	Random way point
Maximum speed (m/s)	20
Pause time (s)	0, 30, 60, 120, 300, 600, 900
Number of communicating nodes	10, 30, 30, 40
Application layer	Constant Bit Rate (CBR)
Packet size	512 bytes
Packet rate	4 packet/second
Routing protocols	AOMDV-BHAOMDV-IDSAOMDV
Number of Blackhole nodes	1, 2, 3, 4, 5

B. Performance Metrics

- Packet Delivery Ratio (PDR) : Represents the ratio of the packets received number by the destination node to the packets sent number by the source node;
- Average End to End Delay (AEED): Represents the average end-to-end delay of sending packets by the source
- and receiving it by the destination;
- Drop packets (DP): Represents the packets lost number during the simulation;
- Forwarded packets (FP): Represents the packets transmitted number during the simulation.

C. Simulation Results

1) Packet Delivery Ratio: Figures 2, 3, 4, and 5 and tables IV, V, VI and VII respectively present the PDR evolution for the AOMDV, BHAOMDV, and IDSAOMDV with variation of the communicating nodes from 10 to 40 nodes, variation of the pause time from 0 to 900 seconds, and variation of the malicious nodes number from 1 to 5. In the first scenario where the communicating nodes number is 10 and with presence of a single malicious node, the PDR varied from 98.72% to 99.99% for AOMDV and from 61.57% to 96.56% for BHAOMDV. Thus, degradation of PDR in BHAOMDV varied from 3.16% to 37.39% when compared with the AOMDV. The AOMDV and IDSAOMDV have almost the same value of the PDR. Subsequently, performance of BHAOMDV is progressively degraded according to variation of the malicious nodes number. However, other scenarios behave the same way. Therefore, the four scenarios show performance degradation of the BHAOMDV and show also that the proposed IDSAOMDV gives similar results as the AOMDV, which denotes that our proposed mechanism detect all malicious nodes perfectly.

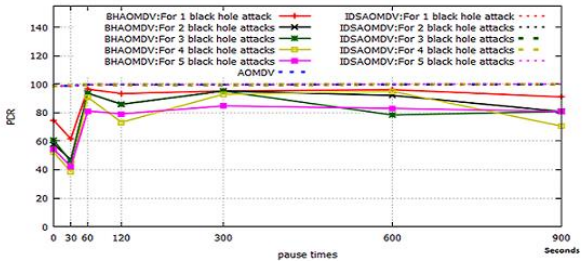

Fig. 2. Packet Delivery Ratio for 10 communicating Nodes

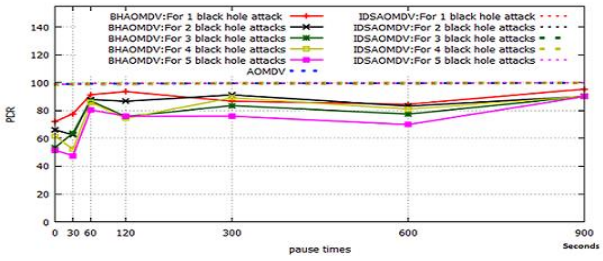

Fig. 3. Packet Delivery Ratio for 20 communicating Nodes

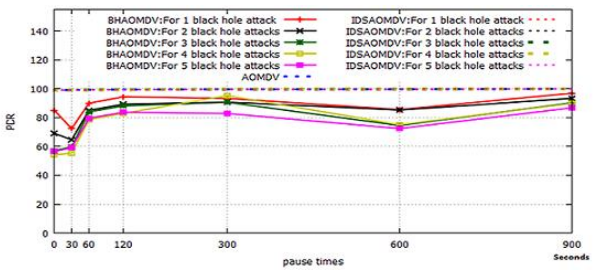

Fig. 4. Packet Delivery Ratio for 30 communicating Nodes

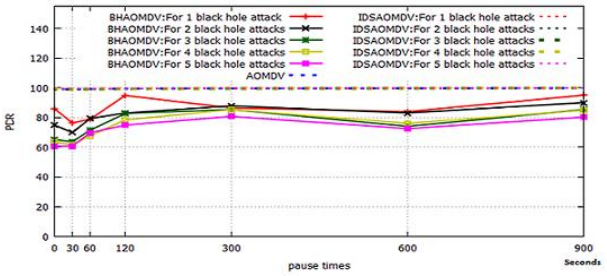

Fig. 5. Packet Delivery Ratio for 40 communicating Nodes

2) Average End to End Delay: We have also studied the end-to-end delay between source and destination nodes. The following graphs illustrated in Figures 6, 7, 8, and 9 and tables VIII, IX, X and XI respectively show performance of AOMDV, BHAOMDV, and IDSAOMDV in terms of end-to-end delay. Figures 6, 7, 8, and 9 depict clearly that AOMDV and IDSAOMDV give less end-to-end delay without and with Blackhole attacks. With presence of a single malicious node, and with 10 communicating nodes, the average end-to-end delay reaches up to 0.0011ms for AOMDV, 0.0011ms for IDSAOMDV and 0.0095ms for BHAOMDV. In this case, almost all the graphs are similar, with the exception for the pause time 0, where there is a variation in the value of the average end-to-end delay due to instability of the nodes in the communication at that time. But in scenarios where the nodes number varied from 20 to 40 (Figures 7, 8, and 9), the average

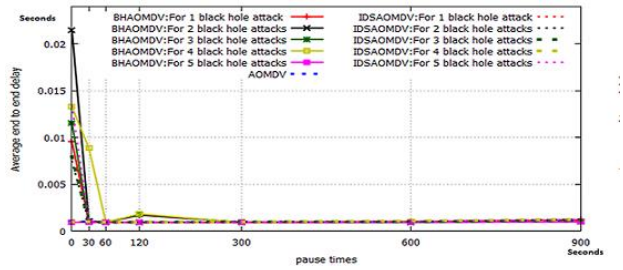

Fig. 6. Average End to End Delay for 10 communicating Nodes

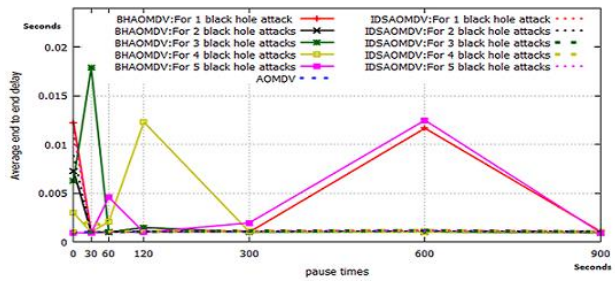

Fig. 7. Average End to End Delay for 20 communicating Nodes

end-to-end delay increases progressively according to variation of the nodes number in communication and simultaneously of variation of the malicious nodes number for BHAOMDV. As a result, the average end-to-end delay performance metric values are large and unstable for BHAOMDV. However, these values are very close and low for AOMDV and IDSAOMDV which denotes that our mechanism is lightweight.

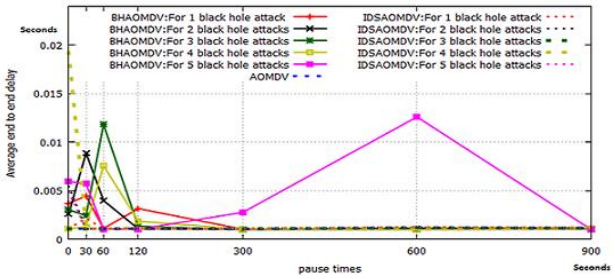

Fig. 8. Average End to End Delay for 30 communicating Nodes

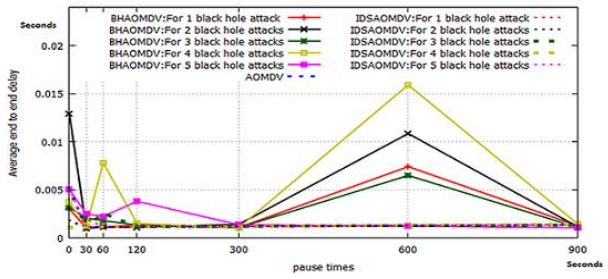

Fig. 9. Average End to End Delay for 40 communicating Nodes

3) Dropped Packets: Figures 10, 11, 12, and 13 and tables XII, XIII, XIV and XV respectively illustrate the lost packets number for AOMDV, BHAOMDV, and IDSAOMDV. The

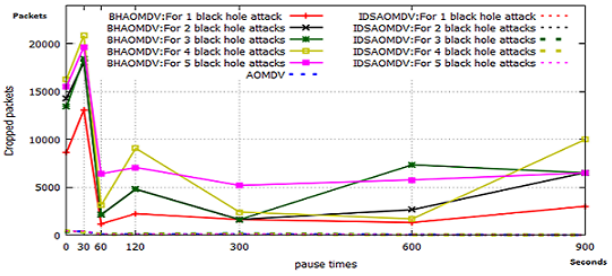

Fig. 10. Dropped Packets for 10 communicating Nodes

results show that IDSAOMDV based on our technique has fewer lost packets than in BHAOMDV, because malicious nodes have been identified and avoided in our solution, which reduces the lost packets number. According to Fig. 10, the lost packets number for AOMDV is 2 to 432, so the technique applied in our solution with the presence of a single malicious

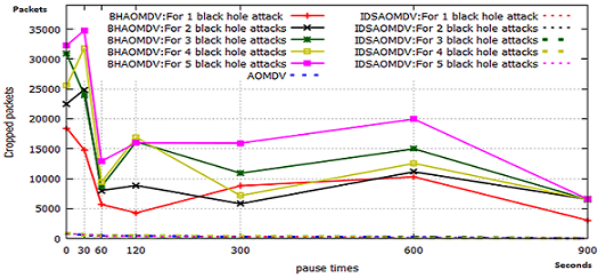

Fig. 11. Dropped Packets for 20 communicating Nodes

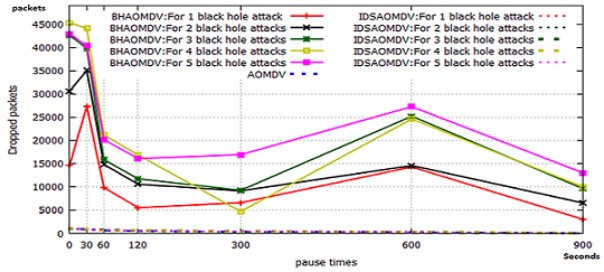

Fig. 12. Dropped Packets for 30 communicating Nodes

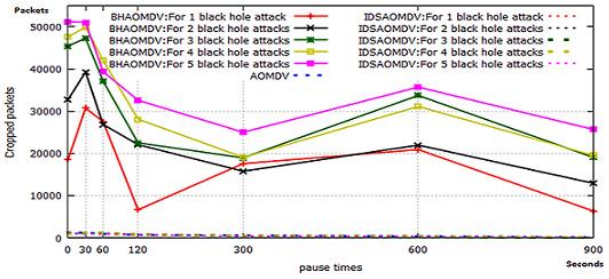

Fig. 13. Dropped Packets for 40 communicating Nodes

node generates results as 3 to 425 lost packets for IDSAOMDV, on the other hand in BHAOMDV with the presence of a single malicious node causes 1168 to 13082 lost packets. Thus, the lost packets number is greater in BHAOMDV when compared with AOMDV or IDSAOMDV. In the same figure (Fig. 10), and when there is an increase in the malicious nodes number, the lost packets number increases in BHAOMDV. We notice that the results behave in the same way as for 10 communicating nodes by varying the communicating nodes number from 20 to 40 nodes (Figures 11, 12, and 13), also, the increase in the communicating nodes number causes the progressive increase in lost packets for BHAOMDV. Moreover, this is an indication of better performance guarantees when the use of our proposed technique.

4) Forwarded Packets: In Figures 14, 15, 16, and 17 and tables XVI, XVII, XVIII and XIX respectively, we have illustrated the transmitted packets number in the case of AOMDV, BHAOMDV, and IDSAOMDV. In AOMDV, the chance of transmitting data packets increases in the presence of alternative paths in the network if the first path fails. In BHAOMDV, presence of malicious nodes in the network causes the loss of packets due to the malicious nodes misbehavior, thus the transmitted packets number is lower than in AOMDV. Applying our technique in IDSAOMDV, the transmitted packets number is greater than in BHAOMDV because our technique avoids malicious nodes to build the data packet transmission paths. In the case of Fig. 14, the transmitted packets number is 2847 to 10011 for AOMDV, 1420 to 10576 for BHAOMDV with presence of a single malicious node, and 2956 to 9967 for IDSAOMDV with the presence of a single malicious node. Thus, the transmitted packets number represents 94.35% to 157.68% more for AOMDV than for BHAOMDV. As the malicious nodes number increases, the transmitted packets number is much reduced for BHAOMDV. The transmitted packets number in the case of IDSAOMDV is very large compared to BHAOMDV. This shows that the transmitted packets number from the source to the destination has increased for IDSAOMDV, the reason is that if a malicious node presents itself in the network it causes the loss of packets in the case of BHAOMDV, but we apply our technique in IDSAOMDV, the malicious node is avoided before the protocol establishes the data packet transmission paths which maintains the paths reliability built from the source node to the destination node and improves the transmitted packets number. The results presented in Figures 15, 16, and 17 behave in the same way as for 10 communicating nodes, moreover, the increase in the communicating nodes number causes the progressive increase of the transmitted packets for AOMDV, BHAOMDV, and IDSAOMDV, that alternative paths can be used, also, more malicious nodes number is least, more transmitted packets is larger for BHAOMDV. The results obtained prove the effectiveness of our proposed technique.

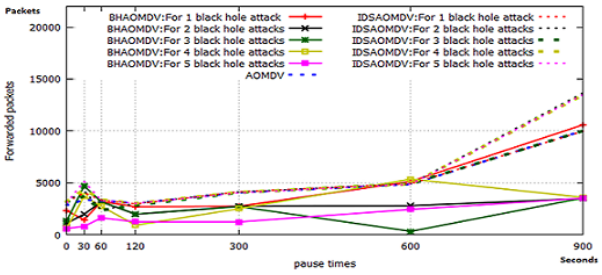

Fig. 14. Forwarded Packets for 10 communicating Nodes

D. Comparison with Others Solutions

In this section, we compare the performance of our proposed solution against others solutions described in Section IV ([11], [12] and [13]) that has similarities with the proposed solution. In [11], when their proposed approach is implemented then despite the presence of malicious nodes the Packet Delivery Ratio improved significantly and it roses to 94% when three malicious nodes were present and with an average growth of above 60%. In [12], the Packet Delivery Ratio is definitely highest with no malicious node in the environment, it reach 99.86%. It decreases slowly with increasing number of malicious nodes, it is 32% for one malicious node and it is 6% for three malicious nodes. In [13], the Packet Delivery Ratio is close to more than 70% for a single malicious node, and it is not less than 45% for 5 malicious nodes, but it is close to 90% without malicious nodes. In our solution as shown in the Section VI, in all scenarios the PDR for IDSAOMDV is not less than 98%. In [12], the average end-to-end delay increases gradually with incremented malicious nodes as time is taken by the encryption process with ECC. The Average end-to-end delay is 85655.8ms in the presence of a single malicious node, and is 85658.6ms in the presence of 3 malicious nodes, but it is 85652.4ms without malicious node. In [13], the end-to-end delay is higher in this scheme than the original AOMDV

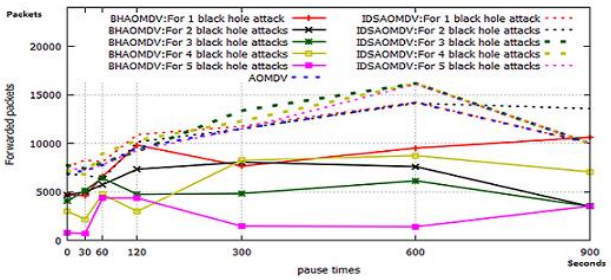

Fig. 15. Forwarded Packets for 20 communicating Nodes

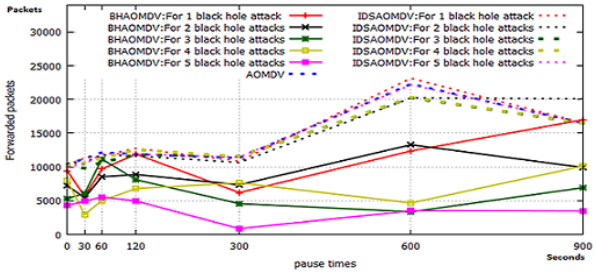

Fig. 16. Forwarded Packets for 30 communicating Nodes

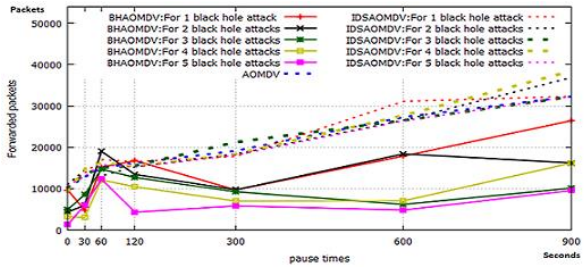

Fig. 17. Forwarded Packets for 40 communicating Nodes

scheme when the number of malicious nodes is increased due to its procedures and security features. In this solution, the message is divided and encrypted to achieve their feature. Due to this reason, it takes more delay for the delivery. In our solution as shown in the Section VI, in all scenarios the values of end to end delay are very close for IDSAOMDV when compared with AOMDV. In [13], there is an impact of multiple attackers because the scheme utilizes multiple paths simultaneously. Even though the impact is present with higher data loss in this scheme by increasing the malicious nodes, it delivers almost whole packet to the destination by distributing it into multiple paths to ensure the entire delivery through safe paths. In our solution as shown in the Section VI, in all scenarios the values of dropped packets are very close for IDSAOMDV when compared with AOMDV.

In summary, the comparison covers most scenarios like packet delivery ratio, average end-to-end delay, and dropped packets in the presence of Blackhole attacks. Based on the above performance comparisons, the proposed solution is very effective in most of the scenarios we tested. Table III summarizes the comparison of the proposed secure routing protocol with the some recent existing approaches.

VII. Conclusion

Mobile ad-hoc networks suffer from several types of attacks, in particular, the Blackhole attack. It is an attack where the malicious node can falsify the protocol response message to pretending it has the shortest path to reach the destination node. The mechanisms presented in the AOMDV routing protocol do not consider security. However, we have proposed an enhancement of the AOMDV to detect and isolate Blackhole attacks. In this paper, we have surveyed Blackhole attacks to prove our technique against this attack. In order to analyze its impacts on the AOMDV, we implemented BHAOMDV with several Blackhole attacks, and to detect and isolate malicious nodes, we have also implemented IDSAOMDV as a solution against Blackhole attacks. Our proposed technique works well even when multiple malicious nodes attack. The results show that the performances of the two protocols AOMDV and IDSAOMDV are almost equal. The results also prove the impact of Blackhole attacks on how the AOMDV performs and shows the validity of our proposed technique in the IDSAOMDV as a solution against Blackhole attacks.

Table III. Comparison of Routing Protocols

Approaches	Advantages	Disadvantages
Our approach	-Simple -No energy consumption problem -The comparison operation of destination sequence number with a threshold value on the route reply does not increase the communication delay. -The comparative performance evaluations prove that, by detecting and discarding the Blackhole nodes in the network, the delivery ratio increases without causing too much extra delay.	Unable to detect the malicious node if it does not use high destination sequence number. -Storage area problem due to the additional table.
[13]	-The security is high due to the uses of encryption/decryption algorithms. -The proposed method increases the delivery ratio and throughput.	-Complex -Energy consumption problem -Storage area and computation power problem -Adds a significant computational burden due to homomorphic encryption method. -The splitting and combining operation increases total end-to-end delay in the network.
[14]	-The security is high due to the uses of encryption/decryption algorithms. –All transmitted data packets are successfully received by the destination nodes. The delivery ratio is 100%. -The proposed method increases the throughput.	-Complex -Energy consumption problem -Storage area and computation power problem -Adds a significant computational burden due to homomorphic encryption method. -The splitting and combining operation increases total end-to-end delay in the network.

TABLE IV. PDR FOR 10 COMMUNICATING NODES

Pause time (s)	Packet Delivery Ratio (PDR (%))										
	AOMDV	BHAOMDV					IDSAOMDV				
		1	2	3	4	5	1	2	3	4	5
0	98.7285	74.6420	57.9616	60.5142	52.1060	54.3088	98.7563	98.6568	98.8950	98.6955	98.7382
30	98.9663	61.5744	47.0143	45.7525	38.5168	42.1662	98.9963	98.9359	99.1580	99.0896	98.7821
60	99.7350	96.5652	93.7301	93.8090	90.8596	81.1919	99.7379	99.6936	99.7447	99.7325	99.7769
120	99.7527	93.4371	85.9151	85.9777	73.2925	79.2274	99.6908	99.7419	99.6619	99.7269	99.7500
300	99.7148	95.2363	95.2231	95.2573	92.9374	84.7543	99.7389	99.6976	99.5559	99.6943	99.6330
600	99.8826	96.1559	92.2154	78.4048	95.0264	83.0457	99.9442	99.9499	99.8971	99.9558	99.8704
900	99.9941	91.1590	80.8108	80.8888	70.6140	80.8679	99.9912	100	99.9971	99.9941	99.9971

TABLE V. PDR FOR 20 COMMUNICATING NODES

Pause time (s)	Packet Delivery Ratio (PDR (%))										
	AOMDV	BHAOMDV					IDSAOMDV				
		1	2	3	4	5	1	2	3	4	5
0	98.8685	72.2105	66.0498	53.5555	61.4748	51.3834	98.9638	98.6953	98.7645	98.6928	98.8404
30	99.1385	77.7305	62.5638	63.8773	52.1095	47.5653	98.9214	99.2389	99.1209	99.1159	99.1095
60	99.3418	91.4575	87.9499	86.9325	85.8259	80.5110	99.4618	99.5047	99.4069	99.4391	99.3976
120	99.4297	93.5923	86.6752	75.6910	74.5705	75.9640	99.4689	99.3828	99.4249	99.3572	99.4611
300	99.5957	86.7648	91.2945	83.5935	89.2323	76.0011	99.5057	99.6869	99.6353	99.5137	99.6926
600	99.6995	84.5319	83.2606	77.4847	81.1189	69.9493	99.7442	99.7546	99.6812	99.8303	99.7485
900	99.9955	95.4349	90.1659	90.2322	90.1652	90.1162	99.9955	99.9940	99.9895	99.9985	99.9985

TABLE VI. PDR FOR 30 COMMUNICATING NODES

Pause time (s)	Packet Delivery Ratio (PDR (%))										
	AOMDV	BHAOMDV					IDSAOMDV				
		1	2	3	4	5	1	2	3	4	5
0	98.9558	85.0916	69.0720	56.9383	54.1597	56.5517	98.9936	98.9488	99.0288	98.9395	98.8569
30	99.1609	72.3800	64.6430	59.7985	55.4230	59.2101	99.0908	99.1885	99.1296	99.0980	99.2489
60	99.3752	90.0502	85.0218	83.9756	78.6148	79.6274	99.3467	99.4405	99.3035	99.4419	99.2091
120	99.5451	94.4363	89.3220	88.1569	82.9505	83.7378	99.4209	99.4565	99.4275	99.4482	99.5369
300	99.6941	93.3526	90.7633	90.6468	95.2586	82.8969	99.6847	99.7696	99.6626	99.7032	99.6024
600	99.7740	85.5735	85.2830	74.5554	75.1229	72.4488	99.6920	99.7531	99.7982	99.7891	99.7311
900	99.9737	96.9495	93.3827	90.2777	89.8830	86.8266	99.9778	99.9727	99.9879	99.9586	99.9838

TABLE VII. PDR FOR 40 COMMUNICATING NODES

Pause time (s)	Packet Delivery Ratio (PDR (%))										
	AOMDV	BHAOMDV					IDSAOMDV				
		1	2	3	4	5	1	2	3	4	5
0	99.0342	85.8032	74.8684	65.1513	63.4571	60.7235	99.1722	99.1917	99.1517	99.2423	99.0975
30	99.0878	76.4332	69.9047	63.7419	61.7247	60.8521	99.2336	99.2909	99.1398	99.1607	99.3015
60	99.2751	78.8718	79.3859	71.4968	67.7134	69.7698	99.2895	99.1473	99.1919	99.2190	99.2275
120	99.4735	94.9053	83.0678	82.7474	78.4579	74.9933	99.4985	99.4238	99.3926	99.4180	99.4619
300	99.6004	86.5031	87.8994	85.4669	85.3845	80.8191	99.7491	99.7214	99.6767	99.6894	99.6950
600	99.7392	83.9823	83.1621	74.1155	76.1286	72.6129	99.7683	99.7699	99.7507	99.8017	99.7574
900	99.9249	95.1220	90.0894	85.3920	84.9894	80.3074	99.9724	99.9240	99.9746	99.9309	99.9532

TABLE VIII. AEED FOR 10 COMMUNICATING NODES

Pause time (s)	Average End to End Delay (ms)										
	AOMDV	BHAOMDV					IDSAOMDV				
		1	2	3	4	5	1	2	3	4	5
0	0.000963	0.009554	0.021496	0.011568	0.013290	0.000920	0.000965	0.007438	0.007944	0.000970	0.013370
30	0.000964	0.000938	0.001035	0.000963	0.008872	0.000941	0.000986	0.000992	0.000972	0.001001	0.001025
60	0.000947	0.000950	0.000953	0.000953	0.000938	0.000905	0.000944	0.000920	0.000920	0.000951	0.000947
120	0.000938	0.001682	0.000914	0.001740	0.001839	0.000897	0.000932	0.000939	0.000933	0.000940	0.000939
300	0.000969	0.000937	0.000931	0.000930	0.000900	0.000889	0.000968	0.000968	0.000972	0.000970	0.000970
600	0.000993	0.001007	0.000945	0.000920	0.001027	0.000938	0.000999	0.000995	0.000995	0.001057	0.000995
900	0.001143	0.001185	0.000967	0.000974	0.000987	0.000969	0.001141	0.001250	0.001144	0.001243	0.001241

TABLE IX. AEED FOR 20 COMMUNICATING NODES

Pause time (s)	Average End to End Delay (ms)										
	AOMDV	BHAOMDV					IDSAOMDV				
		1	2	3	4	5	1	2	3	4	5
0	0.001025	0.012254	0.007292	0.006298	0.002950	0.000942	0.011245	0.008845	0.001048	0.001026	0.011316
30	0.001011	0.000974	0.000981	0.017858	0.000983	0.000911	0.001029	0.001006	0.001012	0.002325	0.001018
60	0.001018	0.000997	0.001005	0.000999	0.002068	0.004572	0.001018	0.000994	0.001027	0.001047	0.001018
120	0.001055	0.001446	0.001040	0.001466	0.012301	0.000975	0.001086	0.001064	0.001047	0.001081	0.001053
300	0.001079	0.000995	0.001030	0.000985	0.001034	0.001943	0.001092	0.001074	0.001109	0.001097	0.001092
600	0.001119	0.011663	0.001026	0.001035	0.001022	0.012491	0.001121	0.001119	0.001155	0.001183	0.001152
900	0.001039	0.001057	0.000933	0.000936	0.000996	0.000937	0.001035	0.001091	0.001043	0.001033	0.001040

TABLE X. AEED FOR 30 COMMUNICATING NODES

Pause time (s)	Average End to End Delay (ms)										
	AOMDV	BHAOMDV					IDSAOMDV				
		1	2	3	4	5	1	2	3	4	5
0	0,001072	0,003679	0,002597	0,003026	0,001085	0,005931	0,001075	0,005453	0,001062	0,019249	0,004846
30	0,001069	0,004448	0,008870	0,002410	0,001247	0,005707	0,002150	0,001063	0,001049	0,001063	0,001061
60	0,001070	0,001097	0,003983	0,011829	0,007575	0,001029	0,001063	0,001073	0,001062	0,001063	0,001076
120	0,001089	0,003145	0,001052	0,001318	0,001849	0,001022	0,001114	0,001086	0,001080	0,001098	0,001089
300	0,001073	0,001006	0,001004	0,000989	0,001021	0,002756	0,001061	0,001053	0,001070	0,001071	0,001075
600	0,001195	0,001089	0,001083	0,000984	0,000983	0,012601	0,001226	0,001169	0,001174	0,001196	0,001194
900	0,001145	0,001144	0,001062	0,001029	0,001073	0,000991	0,001142	0,001190	0,001140	0,001176	0,001140

TABLE XI. AEED FOR 40 COMMUNICATING NODES

Pause time (s)	Average End to End Delay (ms)										
	AOMDV	BHAOMDV					IDSAOMDV				
		1	2	3	4	5	1	2	3	4	5
0	0,005044	0,003027	0,012910	0,003165	0,003721	0,005041	0,001081	0,001835	0,001066	0,001057	0,005075
30	0,001107	0,001029	0,001026	0,002048	0,001198	0,002490	0,001928	0,001125	0,001120	0,001130	0,001120
60	0,001134	0,001122	0,001123	0,001785	0,007806	0,002229	0,001160	0,001115	0,002558	0,001152	0,001156
120	0,001156	0,001361	0,001104	0,001326	0,001508	0,003797	0,001169	0,001160	0,001162	0,001151	0,001155
300	0,001185	0,001056	0,001394	0,001051	0,001044	0,001362	0,001155	0,001169	0,001200	0,001168	0,001156
600	0,001260	0,007405	0,010854	0,006489	0,015920	0,001204	0,001317	0,001266	0,001266	0,001289	0,001267
900	0,001348	0,001253	0,001145	0,001088	0,001438	0,001058	0,001322	0,001389	0,001307	0,001425	0,001315

TABLE XII. DP FOR 10 COMMUNICATING NODES

Pause time (s)	Dropped Packets (packet)										
	AOMDV	BHAOMDV					IDSAOMDV				
		1	2	3	4	5	1	2	3	4	5
0	432	8624	14304	13424	16283	15515	425	459	376	444	429
30	353	13082	18049	18438	20884	19672	343	366	289	311	418
60	90	1168	2131	2111	3109	6397	89	105	87	91	77
120	86	2232	4800	4784	9080	7071	105	88	115	93	85
300	98	1619	1627	1610	2402	5193	89	103	152	104	126
600	40	1308	2648	7340	1689	5767	19	17	35	15	44
900	2	3013	6527	6502	9992	6503	3	0	1	2	1

TABLE XIII. DP FOR 20 COMMUNICATING NODES

Pause time (s)	Dropped Packets (packet)										
	AOMDV	BHAOMDV					IDSAOMDV				
		1	2	3	4	5	1	2	3	4	5
0	754	18444	22531	30870	25586	32314	690	870	820	875	772
30	574	14804	24871	23999	31830	34803	720	506	585	591	594
60	439	5666	8003	8676	9419	12915	361	329	396	376	402
120	383	4261	8865	16158	16904	15985	355	410	383	428	359
300	269	8794	5785	10910	7153	15935	328	208	242	324	204
600	200	10281	11129	14981	12546	19966	172	162	213	114	167
900	3	3032	6539	6491	6532	6576	3	4	8	1	1

TABLE XIV. DP FOR 30 COMMUNICATING NODES

Pause time (s)	Dropped Packets (packet)										
	AOMDV	BHAOMDV					IDSAOMDV				
		1	2	3	4	5	1	2	3	4	5
0	1035	14741	30652	42612	45299	42975	995	1047	969	1058	1135
30	835	27341	35041	39819	44129	40352	903	805	863	895	746
60	618	9851	14816	15844	21173	20158	650	555	694	559	784
120	454	5509	10566	11725	16857	16092	576	539	570	552	458
300	303	6590	9133	9250	4700	16931	314	228	335	294	395
600	225	14275	14575	25193	24602	27259	305	247	200	209	266
900	25	3020	6535	9630	10017	13021	22	27	13	42	13

TABLE XV. DP FOR 40 COMMUNICATING NODES

Pause time (s)	Dropped Packets (packet)										
	AOMDV	BHAOMDV					IDSAOMDV				
		1	2	3	4	5	1	2	3	4	5
0	1262	18531	32749	45439	47621	51213	1087	1057	1113	993	1178
30	1194	30739	39282	47287	49916	51020	1004	934	1127	1097	916
60	958	27541	26867	37146	42086	39396	930	1114	1072	1024	1024
120	689	6651	22078	22493	28111	32584	657	752	793	762	706
300	526	17589	15776	18961	19071	25019	328	363	422	408	400
600	343	20909	21966	33731	31116	35713	302	304	327	260	319
900	101	6360	12931	19050	19555	25687	36	103	34	93	61

TABLE XVI. FP FOR 10 COMMUNICATING NODES

Pause time (s)	Forwarded Packets (packet)										
	AOMDV	BHAOMDV					IDSAOMDV				
		1	2	3	4	5	1	2	3	4	5
0	2847	2294	1103	1353	629	588	3169	3229	3173	3202	3087
30	3356	1420	1965	4676	3704	796	4022	4227	3696	4352	5124
60	3284	3172	3153	3171	2728	1607	3315	2370	2337	3355	3298
120	3010	2695	1967	1968	901	1225	2956	2999	2826	3010	3005
300	4065	2729	2725	2696	2499	1219	4116	4106	4048	4082	4030
600	4860	5123	2784	311	5351	2428	4909	4892	4908	4876	4861
900	10011	10576	3472	3528	3589	3505	9967	13646	9998	13448	13472

TABLE XVII. FP FOR 20 COMMUNICATING NODES

Pause time (s)	Forwarded Packets (packet)										
	AOMDV	BHAOMDV					IDSAOMDV				
		1	2	3	4	5	1	2	3	4	5
0	6856	4664	4680	4036	2977	772	7567	6751	7717	7146	7416
30	7208	4611	4967	5146	2167	671	8281	6782	7408	6781	7240
60	7736	6566	5729	6393	4740	4374	8072	6268	7985	8939	7789
120	9542	9806	7327	4735	2975	4377	10899	10135	9179	10288	9271
300	11505	7647	8054	4817	8236	1450	11757	11500	13370	12282	11506
600	14201	9511	7591	6129	8729	1393	14229	14118	16166	16168	16092
900	10009	10615	3479	3481	7049	3522	10023	13581	9998	9989	10026

TABLE XVIII. FP FOR 30 COMMUNICATING NODES

Pause time (s)	Forwarded Packets (packet)										
	AOMDV	BHAOMDV					IDSAOMDV				
		1	2	3	4	5	1	2	3	4	5
0	10448	9435	7217	5344	7971	4327	10404	10468	10134	10203	10086
30	11222	5641	5454	6062	2948	4937	11334	10694	9832	10616	10397
60	12172	9698	8541	11183	5018	5548	11657	11801	10691	11352	12003
120	11911	11921	8885	8112	6818	4966	12773	11651	11837	12573	11926
300	11352	6203	7365	4573	7655	867	10877	10676	11575	11550	11466
600	22321	12395	13308	3354	4673	3523	23167	20260	20277	20341	22195
900	16510	17013	9932	6935	10143	3470	16554	20106	16506	16511	16523

TABLE XIX. FP FOR 40 COMMUNICATING NODES

Pause time (s)	Forwarded Packets (packet)										
	AOMDV	BHAOMDV					IDSAOMDV				
		1	2	3	4	5	1	2	3	4	5
0	10293	9646	4392	4972	3294	1321	11122	11050	10317	9487	10754
30	12827	4812	5944	8545	3007	6014	13771	14483	13490	14672	13009
60	15044	15221	19052	14720	12126	12320	17055	13113	15019	16255	15834
120	16217	16786	13438	12709	10468	4334	16564	15276	15582	15440	15214
300	19170	9699	9729	9258	7018	5820	17791	18389	21260	18370	18108
600	27327	17896	18412	6213	7058	4834	31127	26542	26533	27719	26438
900	32286	26447	16254	10120	16200	9562	32332	36893	32264	38467	32305

REFERENCES

[1] D. B. Johnson, "Routing in Ad Hoc Networks of Mobile Hosts," *in Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications*, pp. 158-163, Dec. 1994, DOI: 10.1109/MCSA.1994.513476.

[2] H. Yang, H. Y. Luo, F. Ye, S. W. Lu, L. Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions," *IEEE Wireless Communications*, Vol. 11, pp. 38-47, Feb. 2004, DOI: 10.1109/MWC.2004.1269716.

[3] M. K. Marina, S. R. Das, "On-Demand Multipath Distance Vector Routing in Ad Hoc Networks," *International Conference on Network Protocols*, pp. 14-23, 2001, DOI: 10.1109/ICNP.2001.992756.

[4] M. K. Marina, S. R. Das, "Ad Hoc on-Demand Multipath Distance Vector Routing," *Wireless Communications and Mobile Computing*, Vol. 6, pp. 969-988, 2006, DOI: 10.1002/wcm.432.

[5] C. E. Perkins, E. M. Royer, "Ad-hoc on-demand distance vector routing," *in Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA)*, pp. 90-100, Feb. 1999, DOI: 10.1109/mcsa.1999.749281.

[6] C. E. Perkins, E. M. Royer, S. R. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," *RFC 3561, Experimental*, pp. 1-37, Jul. 2003, DOI: 10.17487/rfc3561.

[7] H. Deng, W. Li, and D. P. Agarwal, "Routing Security in Wireless Ad-Hoc Networks," *in IEEE Communication Magazine*, Vol. 40, pp. 70-75, Oct. 2002, DOI: 10.1109/MCOM.2002.1039859.

[8] P. N. Raj, P. B. Swadas, "DPRAODV: A dyanamic learning system against blackhole attack in aodv based manet," *International Journal of Computer Science Issue*, Vol. 2, pp. 54-59, 2009.

[9] N. Mistry, D. C. Jinwala, M. Zaveri, "Improving AODV Protocol against Blackhole Attacks," *Proceeding of the International MultiConference of Engineers and Computer Scientists*, Hong kong, Vol. 2, pp. 1034-1039, March. 2010.

[10] T. M. Mahmoud, A. A. Aly, O. Makram, "A Modified AODV Routing Protocol to Avoid Black Hole Attack in MANETs," *International Journal of Computer Applications (0975-8887)*, Vol. 109, No. 6, pp. 27-33, Jan. 2015, DOI: 10.5120/19195-0809.

[11] N. Bhardwaj, R. Singh, "Detection and Avoidance of Blackhole Attack in AOMDV Protocol in MANETs," *International Journal of Application or Innovation in Engineering and Management (IJAIEM)*, Vol. 3, No. 5, pp. 376-383, May. 2014.

[12] J. Sultana, T. Ahmed, "Elliptic Curve Cryptography Based Data Transmission against Blackhole Attack in MANET," *International Journal of Electrical and Computer Engineering (IJECE)*, Vol. 8, No. 6, pp. 4412-4422, Dec. 2018, DOI: 10.11591/ijece.v8i6.pp.4412-4422.

[13] E. Elmahdi, S. Yoo, K. Sharshembiev, "Secure and reliable data forwarding using homomorphic encryption against blackhole attacks in mobile ad hoc networks, " *Journal of Information Security and Applications*, Vol. 51, p. 102425, April. 2020, DOI: 10.1016/j.jisa.2019.102425.

[14] E. Elmahdi, S. Yoo, K. Sharshembiev, "Securing Data Forwarding against Blackhole Attacks in Mobile Ad Hoc Networks, " *The 8th IEEE Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 463-467, Jan. 2018, DOI:10.1109/CCWC.2018.8301683.

Abdelaziz Tami is Assistant Professor at University of SAIDA -Dr. Moulay Tahar, SAIDA, Algeria. He received the M.S. degrees in Computer Science from the National Superior School of Computing of Algiers, Algeria, in 2012. He is currently pursuing the Ph.D. degree in Computer Science at Djillali Liabes of Sidi Bel Abbes, Algeria since 2016. He is a member of the Network and Communication research team of (Evolutionary Engineering and Distributed Information Systems) laboratory (EEDIS). His current research interests are networking, wireless ad hoc, and network security.

Sofiane Boukli Hacene is Full Professor in Computer Science Department of Djillali Liabes University (U.D.L) of Sidi Bel Abbes, Algeria. He received an engineering degree (first class honors) from U.D.L in 2002, M.S. degree from Al Al Bayt University at Mafraq, Jordan in 2005, the Ph.D. degree from U.D.L in 2012, and the habilitation to supervise research (HDR) in 2014. He is a head of the (Evolutionary Engineering and Distributed Information Systems Laboratory) and Network and Communication research team at the U.D.L. His research interests are in networking, including wireless ad-hoc, sensor networks, vehicular networks, IoT, 5G, network security and QoS.

Moussa Ali Cherif has received his Doctorate degree in Computer Science in 2014 and his Habilitation to Supervise Research (HDR) degree in 2016 from Djillali Liabes University (U.D.L) of Sidi Bel Abbes, Algeria. He is a scientific researcher and member of Network and Communication research team at EEDIS (Evolutionary Engineering and Distributed Information Systems laboratory) at U.D.L. He is also an Associate Professor of U.D.L. His research interests fall in the general area of Ad-hoc network, wireless sensor networks, acoustic Ad-hoc networks, vehicular network and routing based QoS.