Wireless Netw (2017) 23:1767–1778
DOI 10.1007/s11276-016-1251-x

An EDRI-based approach for detecting and eliminating cooperative black hole nodes in MANET

Ali Dorri[1]

Published online: 23 March 2016

Abstract Mobile Ad hoc Network (MANET) is a self-configurable, self-maintenance network with wireless, mobile nodes. Special features of MANET like dynamic topology, hop-by-hop communications and open network boundary, made security highly challengeable in this network. From security aspect, routing protocols are highly vulnerable against a wide range of attacks like black hole. In black hole attack malicious node injects fault routing information to the network and leads all data packets toward it-self. In this paper, we proposed an approach to detect and eliminate cooperative malicious nodes in MANET with AODV routing protocol. A data control packet is used in order to check the nodes in selected path; also, by using an Extended Data Routing Information table, all malicious nodes in selected path are detected, then, eliminated from network. For evaluation, our approach and a previous work have been implemented using Opnet 14 in different scenarios. Referring to simulation results, the proposed approach decreases packet overhead and delay of security mechanism with no false positive detection. In addition, network throughput is improved by using the proposed approach.

Keywords Mobile Ad hoc Network (MANET) · Security · DRI table · Cooperative black hole attack · AODV

✉ Ali Dorri
alidorri.ce@gmail.com

[1] Department of Computer Engineering, Mashhad Branch, Islamic Azad University, Mashhad, Iran

1 Introduction

Mobile Ad hoc Network (MANET) is a self-configurable, easy and quick to setup network without any infrastructure. In this network, all nodes are mobile and free to join and leave the network [1]. This feature of MANET not only made it popular, especially for military and disaster management [2], but also made it highly challengeable. Routing packets [3], dividing network into clusters [4] and security [5] are among the most important issues in MANET. Special characteristics of MANET such as open network boundary, dynamic topology and wireless communications made security an important challenge in it. From a security design, MANET is vulnerable against various types of attacks. These includes, Denial Of Service [6] and Man-In-The-Middle [7].

One of the most critical issues in security of MANET is routing protocol's vulnerabilities. In this type of attacks, malicious nodes inject fault routing information packets to network in order to gain access to data packets. Gray hole [8], Worm hole [9] and black hole attack are among the most important attacks against routing protocols. Ad hoc On-demand Distance Vector (AODV) routing protocol is an on-demand routing protocol which uses additional routing packets and a sequence number to find a fresh enough route between source and destination [10]. AODV is highly vulnerable against a variety of attacks especially black hole attack. In black hole attack, malicious node injects fault routing information in order to leads packets toward it-self. Malicious node discards all data packets when it gains access to other node's packets [11].

In this paper, we proposed a security approach to detect and eliminate cooperative malicious nodes in AODV-based MANET. The proposed approach uses an additional data control packet and an Extended Data Routing Information

(EDRI) table in order to detect malicious nodes in selected path. Moreover, by broadcasting malicious node's ID, each source node, eliminate detected malicious nodes from the network. Furthermore, the proposed approach increases the number of trustable nodes in network by updating EDRI table entries during processing time of security mechanism. TCP connections are used in order to eliminate false positive detections. Simulation results show that the proposed approach decreases packet overhead and delay and eliminates false positive detections in security mechanism. Moreover, it increases network throughput in compare with our base work.

The rest of the paper is organized as follows: Sect. 2 presents a comprehensive review on AODV routing protocol and Black hole attack. Section 3 presents a literature review on existing detection and/or elimination approaches for black hole attack. Section 4 discusses the proposed approach in detail. Performance evaluation of the proposed approach is presented in Sect. 5. Finally Sect. 6 concludes the paper and discusses future research directions.

2 AODV and black hole attack

In this section, a brief overview of AODV routing protocol and black hole attack are presented.

2.1 Ad hoc on-demand distance vector (AODV) routing protocol

Ad hoc On-Demand Distance Vector (AODV) is a routing protocol which initiates the route discovery when a source node needs a path for transferring data packets [12]. Therefore, it is categorized as an on-demand routing protocol [13]. In AODV, each mobile node maintains a routing table and uses it to find its Next_Hop_Node (NHN) toward destination. Based on AODV routing protocol, the best path is a path with highest sequence number [14]. The sequence number is increased by either an Intermediate Node (IN) that generates Route Reply (RREP) or the source node that generates Route Request (RREQ).

Whenever, the source node wants to send data packets for destination, at first, it checks its own routing table. If the source has a fresh enough route to the destination, it sends data packets through the existing path. Otherwise, it initiates a route discovery phase to find a fresh enough path to the destination by using two different control packets which are: RREQ and RREP. The source node initiates a route discovery process by using a RREQ packet. The source puts the destination's ID and its own sequence number for the destination in the packet, then, broadcast it. By receiving RREQ, INs update their routing tables for reverse path. A RREP packet is generated by an IN, when either the IN is it-self the destination or it has a fresh enough route to the destination. Otherwise, the IN increases RREQ's hop count and re-broadcast it. The RREP generator unicast RREP packet through revers path to the source. After updating their routing table, all INs which received RREP, send RREP for their own NHN in the path toward the source node.

2.2 Back hole attack

Black hole attack is a kind of Denial of Service (DOS) attack; which, malicious node leads all packets toward it-self by taking advantages of routing protocols vulnerabilities [15, 16]. In AODV-based MANET, malicious node makes sure that the source node would send all packets for it by setting a high number as sequence number in RREP packet.

Regarding the number of malicious nodes in network, black hole can be studied on two different types of attack which are: single black hole and cooperative black hole. In single black hole attack, as shown in Fig. 1a, just one

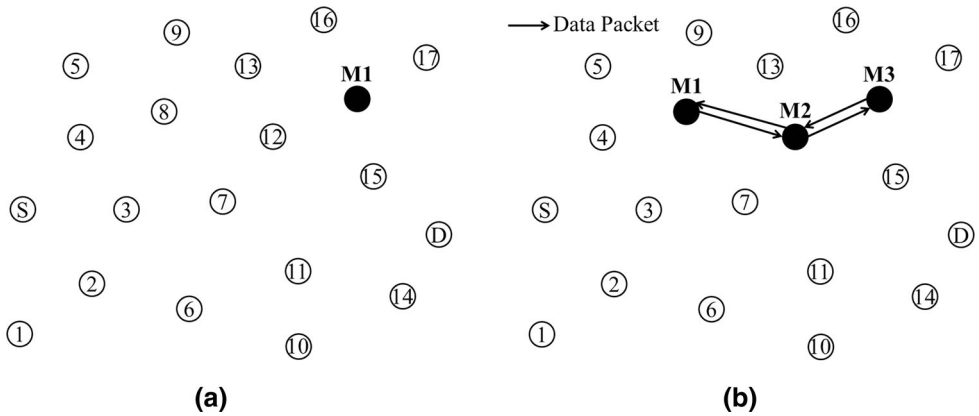


Fig. 1 Different types of black hole attack. **a** Single black hole, **b** Cooperative black hole

malicious node exists in network. As for cooperative attack, more than one malicious node participate in network, as shown in Fig. 1b, and each malicious node is aware of its neighbor's malicious nodes. Generally malicious node does not send any data packet for ordinal nodes; however, it could send data packets for its cooperative neighbors, as shown in Fig. 1b Moreover, each malicious node always set its next cooperative as its NHN in the path and claims that they have communicated data packets before.

Security mechanisms which can detect single black hole are unable to detect cooperative attack. Moreover, detecting cooperative attacks is much more complicated than single attack. Since, cooperative nodes use some mechanisms, like sending data packets for their cooperative neighbors, to cover their tracks.

3 Related works

In literature lots of detection and/or elimination approaches have been proposed. Authors in [17] presented an approach based on promiscuous mode. In this approach, each node monitors its neighbors and calculates a threshold in order to detect malicious nodes. This threshold is a ratio between received packets and forwarded packets. This approach is useful in order to detect one malicious node; however, it is useless in the case of cooperative malicious nodes. The reason is that, in cooperative black hole attack, malicious nodes can send data packets between each other in order to bypass the promiscuous based security approaches. Authors in [18] proposed a cluster-based scheme, called Black Hole Attack Prevention System in Clustered MANET (BHAPSC), which explores existence of malicious nodes and discovers their exact position at specific time. Each node maintains a Friendship Table for checking relationship of cluster head with its neighbor nodes. If Next Hop Node (NHN) is not a friend, then a false packet is sent to a stranger. A trust estimator invoked to calculate a trust value, and according to this value Friendship Table is updated. If trust value is out of tolerable range, stranger node is marked as malicious node. As for eliminating malicious node, a packet with malicious node's ID, is broadcasted to the network. Since the proposed approach uses false packet, it increases packet overhead and delay for security mechanism. Authors in [19] proposed a watchdog mechanism. Generally in watchdog mechanisms, each node uses promiscuous mode to detect a malicious node by monitoring its neighbor node's behavior. Each monitoring node maintains two extra tables which are; "Pending Packet Table" and "Node Rating Table". Each monitor node sniffs its neighbors and checks whether they forward packets which are not for them or not. In case that a node does not forward received packets, monitor node updates its table for considered neighbor node. In the proposed approach, a threshold is defined as ratio of the number of dropped packets to the number of forwarded packets. If total number of dropped packets exceeds the threshold, the monitoring node mark its neighbor as malicious nodes and aware all nodes of detected malicious node's ID. This approach has lots of benefits like low packet overhead; however, its drawbacks should not be ignored. This approach uses promiscuous mode in each node, which wastes node's energy. Furthermore, large cache memory and a wide range of calculations is needed and memory and processing overhead for each node is increased. Authors in [20] presented an advanced algorithm to detect and prevent cooperative black hole and gray hole attacks by using end-to-end checking with prelude and postlude messaging. In this approach, source node divides data packets to small, equal parts and sends them to NHN. Transmission of data packets in each path is monitored by the source node. If the number of dropped packets reaches to a threshold, a backbone network of trusted nodes collects the outcome of monitoring nodes. By using this information, malicious nodes are detected and eliminated from the network. Because of being in promiscuous mode, this approach wastes node's energy and is useless against cooperative attacks. In [21] authors presented a new approach based on estimating packet's sequence number. This approach uses three parameters for estimating maximum sequence number that can possibly be created in the network. These parameters are: RREQ sequence number, sequence numbers in each node's table and number of received RREPs. By receiving a RREP packet with higher sequence number than maximum possible sequence number, the Intermediate Node (IN) marks RREP generator as malicious node and drops RREP packet. This approach increases processing time in each node and wastes node's energy. In [22] authors presented a new way based on monitoring neighbor nodes. Each node, sniffs all its neighbors and cache all of their received packets. If a node receives a packet, which is for another node, and does not relay it, the monitoring neighbor increases the number of dropped packets for considered node. If the rate of received packets to dropped packets in a node reaches to a threshold,

the monitoring node suspects considered node as malicious node.

Beside discussed approaches, there are some papers based on Data Routing Information (DRI) table. Details of DRI table is discussed later in this paper. Authors in [23] proposed an Extended Data Routing Information (EDRI) based approach. In this approach three columns named, "BH", "Counter" and "Timer", have been added to normal DRI table. By selecting the freshest path using AODV protocol, the source node sends data packets for the destination. A NACK packet is sent for the source node in case that destination do not receive any packet. Then a refresh packet is sent by both the source and the destination in the suspected path. By detecting malicious nodes, they are eliminated from network using "BH" column in EDRI table. Moreover, "Counter" value is increased by one for detected node and a timer is set for considered node. During this time, detected node would be considered as malicious node and when the period is over, it becomes an ordinal node. Beside its plus, the proposed approach increases packet lost and decreases network throughput since it takes time for the destination to make sure that packets are dropped. Moreover, "Counter" column is useless and has no effect, neither on route selection, nor on detecting malicious nodes and just increases EDRI table size. The situation is the same for "timer" column. Giving a malicious node a second chance to join the network just increases network overhead and delay and decreases throughput dramatically. The reason is that malicious nodes always have the chance to return to network. However it could decrease the effects of false positive. Most of existing DRI based approaches suffer from the same challenges. To overcome these challenges authors in [24] proposed an approach based on a low size DRI table which decreases security overhead significantly in compare with other works. The proposed approach checks the safety of a selected path before sending data packets to make sure that there is no malicious node in the selected path. Each Intermediate Node which detects a malicious node will reject all response from marked node, so in case of false positive just one node marks a true node as malicious. However, its drawbacks should not be ignored. It cannot eliminate detected malicious nodes, so each source node has to run the security mechanism separately, which increases delay and packet overhead. Besides, it checks the path from RREP generator and suffers from false positive detection.

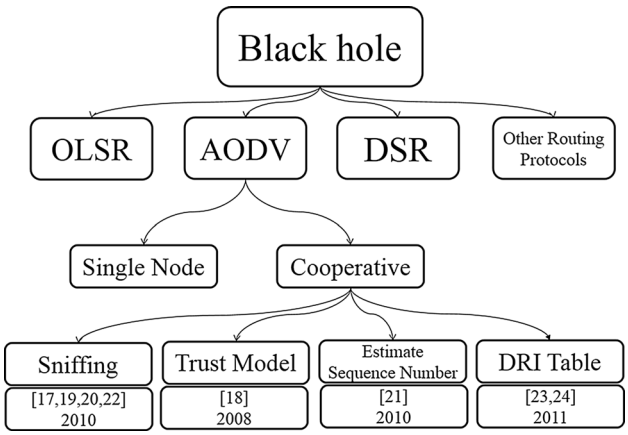


Fig. 2 Defeating approaches for cooperative black hole attack in AODV-based MANET

In this section, previous approaches for detecting and/or eliminating malicious nodes have been discussed. Figure 2 presents a summarization of discussed defeating approaches. At first, black hole attack is divided based on routing protocols. Since our concentration is on AODV routing protocol, AODV is divided in two types of black hole attack. However, different types of black hole attack exists for all routing protocols.

4 The proposed approach

This section provides details of our proposed approach. Using Data Routing Information (DRI) table is an effective way for detecting black hole nodes in MANET. The basic DRI table is presented in [25]. However, there are still lots of challenges, for instance, most of existing security approaches, checks the black hole nodes from RREP generator and suffer from large EDRI table which is useless and increases process overhead. Moreover, they suffer from false positive detections.

In order to overcome these challenges, a security mechanism which uses an Extended Data Routing Information (EDRI) table and a data control packet, is proposed. The proposed EDRI table is shown in Table 1. Each node

Table 1 The proposed EDRI table

Neighbor node's ID	Data routing information		BHN
	From	Through	
4	0/1	0/1	0/1
2	0/1	0/1	0/1

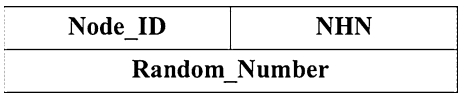


Fig. 3 The proposed data control packet

keeps and updates this table for its own neighbors. Due to dynamic topology of MANET, each node's neighbors are changing dynamically; however, each node keeps the record of its previous neighbors which are no longer its neighbors.

When an Intermediate Node (IN) receives data packet from its neighbor node, it has to set "From" column in its own EDRI table for the neighbor node as '1'. In the other side, when an IN sends data packets through its neighbor node, it has to set "Through" column in its own EDRI table for neighbor node as '1'. Original DRI table contains just these two columns. A Black Hole Node (BHN) column is added to DRI table for eliminating detected malicious nodes. If a node has been detected as malicious node, the "BHN" column will be set as '1' for detected node. Otherwise, "BHN" is '0' for ordinal nodes.

In black hole attack malicious nodes drop all received data packets. By using this feature a data control packet, which is shown in Fig. 3, is proposed for checking INs in a path. This data packet contains three parameters which are as follows:

Node_ID: This field refers to data packet generator's ID

NHN: This field refers to packet generator's Next Hop Node (NHN) in the path toward the destination

Random_Number: By starting security mechanism, the source node generates a small random number and puts it in this field. This number has to be constant in all data packets in a path

The proposed data control packet is a kind of data packet; therefore, malicious nodes can not forward it for ordinal nodes. However, they may relay this packet to their cooperative malicious nodes.

Beside the proposed data control packet, another control packet is used in our approach which is not a data packet and is transmittable by malicious nodes. At first, the proposed data control packet is used to check nodes in the selected path. Then, an ordinal control packet is used by the source node for checking a node which does not respond to data control packet. Our security mechanism is composed of following three steps:

Step 1 Finding freshest path
Step 2 Checking path
Step 3 Eliminating malicious nodes

Step 1 Finding freshest path The main aim of this step is finding a fresh path to the destination. The basic idea of finding fresh enough path in AODV was described in Sect. 2.1. By receiving RREQ packet, malicious node generates a RREP packet with high sequence number. Moreover, in the proposed approach, RREP generator must put its NHN and EDRI entries for NHN in RREP packet and send all for the source node. Malicious node introduces its next cooperative node as its NHN. In case that, it has been the last node in the path, it chooses a random ID and introduces it as its NHN. Furthermore, it claims that both "From" and "Through" columns are '1' for its NHN, whether it is its cooperative or is an ordinal node.

Step 2 Checking path In this step, the safety of selected path is analyzed by the source node. By choosing the freshest path, if the source node has trust to the RREP generator, then the path is safe; otherwise, it has to perform the security mechanism as described in Algorithm 1. Trustable node is defined as follows:

Definition 1 Node B is trustable node for node A, if both "From" and "Through" columns in node A's EDRI table, have been set as '1' for node 'B'.

In Algorithm 1, NHN refers to IN's NHN in each step and is dynamic, since IN is dynamic.

Algorithm 1: The process of proposed security mechanism

```
1:Source: Generate a random number
2:Source: Set source node as IN
3:IN: Generate data control packet and send it for NHN
4:IN: Wait for reply
5:IN: If reply is received
6:      {
7:      If received random number is the same with sent number
8:              {
9:              Update EDRI table
10:             If NHN is destination
11:                     {
12:                     Path is safe
13:                     End:
14:                     }
15:             Set NHN as IN
16:             Go to Line 3
17:             }
18:     Else
19:             {
20:             Mark NHN as malicious node
21:             Go to Line 28
22:             }
23:     }
24:Else
25:     {
26:     Go to Line 28
27:     }
28:IN: Aware Source node of NHN's ID
29:Source: Set NHN as IN
30:If IN is RREP generator
31:     {
32:     Set RREP generator's NHN as IN
33:     Go to Line 35
34:     }
35:Source: Find a route to IN
36:Source: ask for IN's NHN and EDRI entries
37:Source: check previous node for malicious
38:Source: If previous node is malicious
39:     {
40:     Mark as black hole
41:     Go to Line 49
42:     }
43:Source: If IN is trustable and placed after RREP generator
44:     {
45:     Path is safe
46:     End:
47:     }
48:Source: Go to Line 29
49:Source: Aware network of detected malicious nodes
```

The source begins the process by generating a random number and sending data control packet for its NHN (Lines 1–3). By receiving data control packet each node has to extract random number and generates a new data control packet with its own properties; then, it has to send it for both previous node and NHN. The data packet which is sent in reverse path, is considered as reply for data packet. By receiving random number, if received number is equal with sent number, the source updates its EDRI table and set both "From" and "Through" columns as '1' (Lines 5–9). The reason is that, data packets have been transmitted. The process is repeated (Lines 15–16) until one of the following situations happened:

(A) Data packet reaches to the destination: In this situation, the destination sends an ACK back in the reverse path for the source node, then the path is safe (Lines 10–14).
(B) Received random number is not the same with sent number: In this situation, NHN is marked as malicious node and IN aware the source node of its NHN's ID (Lines 18–22).
(C) An IN's NHN does not send reply for data packet (this could happen because of malicious node's activity or disappearing nodes or packet lost due to congestion): In this situation, IN send its NHN'ID for the source node and the source node continues the process with ordinal control packet (Lines 24–27).

In case that the source node has been aware of misbehavior activity, it uses an ordinal control packet and sends it in the path for noticed node and asks for its own NHN and EDRI entries for both its NHN and IN. Then, it has to check whether its previous node is malicious node or not (Lines 35–42). Checking malicious node is defined in Definition 2.

Definition 2 Node A will be marked as malicious by node C if "Through" column in node A is set as '1' and "From" column in node B is set as '0'(Node B is Neighbor of node A).

The process of checking nodes by ordinal control packet continues until one of the following situations happened:

(A) Previous node is marked as malicious (Lines 38–42): Using Definition 2, a node may mark as malicious node, therefore, all nodes between IN, which did not send reply for data packet, and detected node will be marked as cooperative malicious nodes.
(B) Reaches to a trustable node which is placed after RREP generator (Lines 43–47): In this situation the source node found a trustable node (a node which is trustable for the source node) which is after RREP generator and has a route to the previous nodes. The trustable node in this case acts like a security inductor.

In MANET it is strongly possible that a node gets out of range of its neighbor node due to dynamic nature. In this case our approach continues its work normally with no false positive detection. If a node's NHN gets out of range and does not send response to data control packet, simply the source node checks NHN with ordinal control packets and continues the algorithm. In case that NHN gets out of range during data packet transmission, IN does not receive any ACK packet and retransmits data packet and if it does not receive ACK again, the source node will generate a new path. So neither getting out of range, nor packet lost have negative impact on our proposed approach.

By doing described algorithm, all malicious nodes will be detected in each path by the first performing of algorithm. For more clear description an example from network which is presented in Fig. 1b is given. The freshest path is S-4-M1-M2-M3, which 'M3' is RREP generator. Table 2 shows IN and NHN's ID for process of Algorithm 1 in considered network.

Step 3 Eliminating malicious nodes After detecting malicious nodes, a packet containing the malicious node's ID, is generated by the source node for eliminating detected malicious nodes. By receiving this packet, each IN sets "BHN" column in its own EDRI table for detected nodes as "1", then re-broadcast the packet. By doing this, the malicious nodes will be eliminated from the network. When "BHN" column is set as '1' for a node, all INs drop all received packets from noticed nodes, without processing them.

By using described mechanism all malicious nodes are detected and eliminated from the network.

5 Evaluation

In this section, experimental setup, performance metrics, simulation results and analyses are discussed.

Table 2 Describing the process of algorithm 1

IN's ID	NHN's ID	Rules followed
S	4	1–9, 15, 16
4	M1	3–5, 24–30, 35–38, 43, 48
M1	M2	29, 30, 35–38, 43, 48
M2	M3	29, 30, 35–38, 43, 48
M3	6	29–41, 49

The "Rules Followed" column in this table indicates number of lines which the source node executed in each stage

5.1 Experimental setup

The experiments for evaluation of the proposed mechanism have been carried out by using the network simulator Opnet 14. Both approaches have been implemented in two different scenarios. Simulated approaches are: (1) The proposed approach in base work [24], (2) Our approach. Our goal is to show efficiency of the proposed approach in cooperative black hole attacks. Therefore, simulation is carried out under different densities of malicious nodes (2,3,5 and 7 malicious nodes) in different scenarios. Random waypoint model is used as mobility model and TCP is used for data transmission, however, control packets use UDP connections, in other word, TCP is used just after route establishment and for sending data packets. Nodes move within an area of 1000 m * 1000 m. Packet size of 512 byte/packet is used. Since time needed for rerouting has no effect on our approach's results, this time is passed out in our simulations. This time is important just in evaluation of routing protocols. Table 3 provides information on simulation parameters.

5.2 Performance metrics

Following metrics are used for evaluation of the proposed approach, and base work [24].

Packet overhead This metric refers to the number of additional packets which are generated by security mechanism. Packet overhead increases packet loss, congestion and collision probability and wastes node's energy. Since RREQ packet is flooding to the network, the number of RREQ packets generated by the source node, is used for evaluation of packet overhead. As it was mentioned before, our approach uses TCP connections for transmitting data packet, consequently, an additional ACK packet is used in this phase. This ACK is a low size packet which has low overhead on the network. Moreover, our focus is on security approaches overhead, therefore, we simply ignored it in our simulation results.

Delay This metric refers to delay caused by security mechanism. Also, it can be stated that it refers to packet delivery time. In our study, delay refers to time between starting security mechanism and delivering data packets to the destination. The reason is that, in some approaches security mechanism could not detect all malicious nodes in first performing of algorithm. Due to MANET's dynamic topology, time which is spent for each security mechanism is highly challengeable [5]. Link break, due to node's mobility, is strongly possible in MANET and this need rerouting process for finding new path.

Number of detected malicious nodes Since malicious nodes are cooperative, they may use some mechanisms in order to bypass the security mechanisms. By passing data packets between each other or generating RREP packet by the last node in the path, malicious nodes cover their cooperative. This parameter shows the ability of the security mechanism in detecting all malicious nodes in a path.

False positive This metric refers to true nodes which are detected as malicious node.

Throughput This metric refers to average number of delivered packets in compare with sent packets in different destinations.

Table 3 Simulation parameters

Parameter	Value
Simulation duration	600 s
Simulation area	1000*1000
Number of mobile nodes	30
Transmission range	200 m
Movement model	Random waypoint
Maximum speed	2–20 m/s
Data traffic type	TCP
Control packet traffic type	UDP
Packet rate	2 packets/s
Data payload	512 byte/packet
Number of malicious nodes	2/3/5/7
Host paused time	15 s

5.3 Simulation results and analyses

Simulation results are presented in this section. For increasing the accuracy of evaluation, the number of connections are increased from 5 to 30 in our simulation. It is assumed that the last malicious node in each path generates RREP in order to protect previous malicious nodes. For instance, in Fig. 1b, at first 'M3' generates RREP. When 'M3' has been detected by security approach, 'M2' generates RREP and if both 'M3' and 'M2' have been detected, 'M1' generates RREP. In the rest of this section the approach in [24] as is called "base work".

For measuring the first three parameters, which are: packet overhead, delay and the number of detected malicious nodes, simulation results from a single source node are used, however, for other two metrics simulation results from all nodes in network are used. Figure 4 shows the simulation results for the number of RREQ packets generated in the source node in different densities of malicious nodes.

In this diagram horizontal axis refers to the diversity of malicious nodes and vertical ones refer to the number of RREQ packets generated by the source node. In the first seconds of simulation both approaches generate RREQ to find the freshest path to the destination. The rest of RREQ

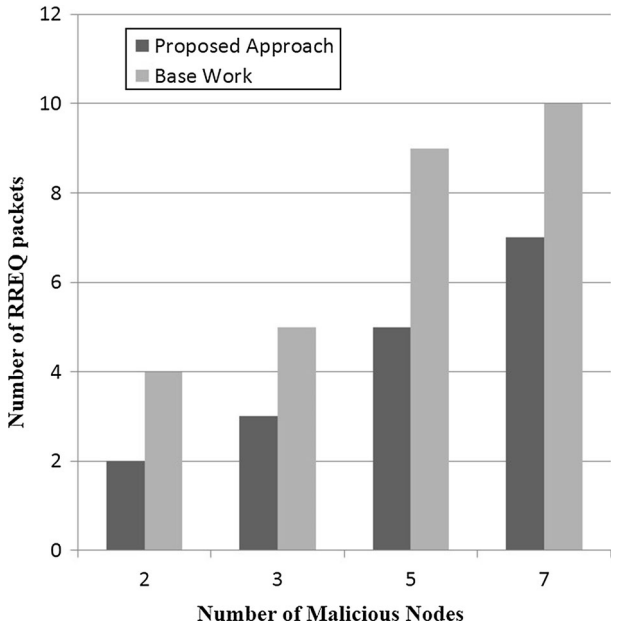


Fig. 4 Evaluation of the number of RREQ packets

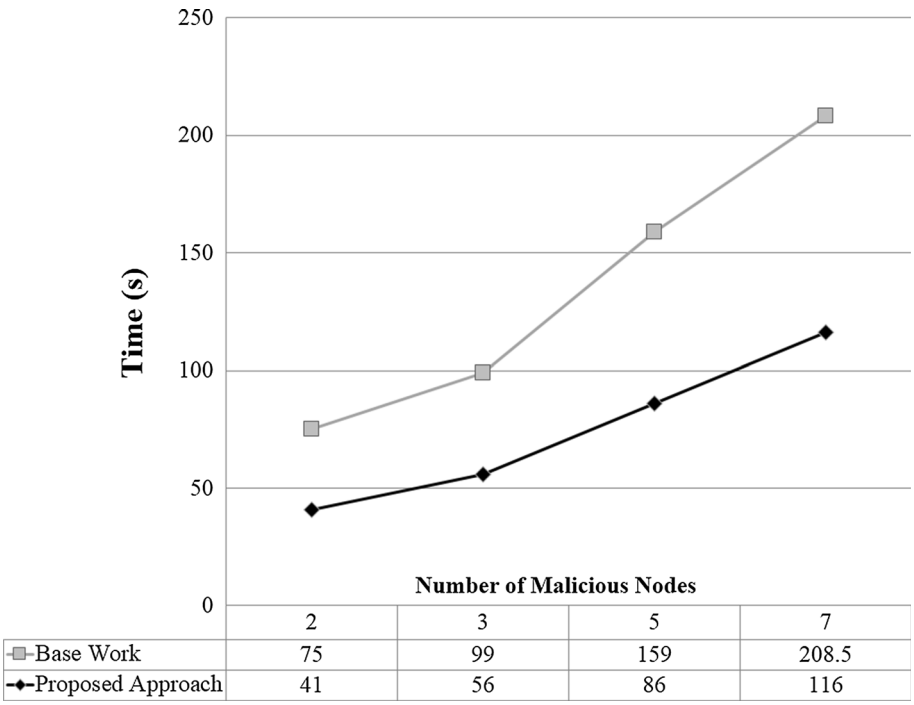
packets in our approach are generated for connecting to NHNs. While in base work the second RREQ is for connecting to NHN and others are for finding a new path. Based on AODV routing protocol, if the source node has a route to the destination, it uses existing path and there is no need to generate a RREQ packet.

Referring to simulation results given in Fig. 4 it is clear that the proposed approach generates lower RREQ packets in comparison with the base work; which decreases congestion, collision and packet loss probability. In addition, total energy consumption and the number of retransmitted packets are decreased in our work.

Simulation results for delay in both approaches are presented in Fig. 5. In Fig. 5 horizontal axis refers to the number of malicious nodes in each scenario and vertical one refers to delay caused by security mechanism for generating a safe path between the source and the destination.

Referring to simulation results given in Fig. 5, the proposed approach generates the safe path with lower delay in compare to base work. It is clear that sending data control packets hop-by-hop increases delay in our approach; but, overlay, our approach decreases delay, since it detects all malicious nodes in one running and the number of pauses for RREQ packets are decreased. Due to MANET's dynamic topology, reducing delay as low as possible is highly important. In order to achieve this goal, in our work EDRI table entries are updated by using data control packet. Therefore, the number of trustable nodes are increasing dramatically. By taking advantages of trustable nodes, delay and packet overhead of the proposed approach will be decreased over time. The reason is that, when the source reaches to a trustable node, placed after RREP generator, it can be sure that the path is safe (Algorithm 1, Lines 43–47).

Fig. 5 Evaluation of delay



	2	3	5	7
Base Work	75	99	159	208.5
Proposed Approach	41	56	86	116

Table 4 Evaluation of number of detected malicious nodes

Protocol	Malicious nodes density in network			
	2	3	5	7
Base work	1	1	1	1
Proposed approach	2	3	5	7

Delay reduction rate is depended on the number of trustable nodes and their position in the path.

Number of detected malicious nodes by security mechanism is presented in Table 4.

The base work starts checking path from RREP generator. In case that, last malicious node in each path generates RREP packet for protecting its cooperative nodes, the source node can detect just one of the malicious nodes in the path by each run. Next time when the source node starts checking path, it detects another node, and this will continue until all the malicious nodes are detected and eliminated from the network. Therefore, the security mechanism cannot detect all cooperative malicious nodes in its checking step.

Evaluation of false positive detection is given in Fig. 6. This diagram presents the average number of true nodes which are detected as malicious nodes in different densities. The horizontal axis refers to the number of connections in the network and vertical one refers to the number of false positive detections by security mechanism.

Due to dynamic topology of MANET, route breaking between nodes is strongly possible. This is one of the main reasons which causes false positive. Congestion and packet lost are the other two reasons for false positive. In order to overcome this challenge, TCP connections are used in our study; therefore, each node updates its EDRI table only if it receives the ACK of its neighbor.

Regarding throughput, simulation results are presented in Fig. 7. In this diagram horizontal axis refers to the number of connections and vertical one refers to average network throughput in different densities.

Network throughput is the number of packets reached to the destination. Each point in Fig. 7, is the average number of throughput for network with 2,3,5 and 7 malicious nodes. In our study each malicious node can send RREP packet for just one ordinal node and when all packets are received another RREP for another node in network could be sent. Also, all source nodes start sending packets simultaneously; therefore, each malicious node will drop just one node's packets. Each node sends 10 packets toward the destination. There is an example to make the process clear. When there are only 5 connections in the network for each density of malicious nodes the following situations will happened:

2 malicious nodes: In this case, 20 packets will drop by the malicious nodes and 30 packets will reach to the destination.

3 malicious nodes: In this case, 30 packets will drop and 20 packets will reach to destination.

5 and 7 malicious nodes: In these cases, all packets will drop by the malicious nodes.

Beside malicious nodes activity, congestion is influence in network throughout. By increasing the number of

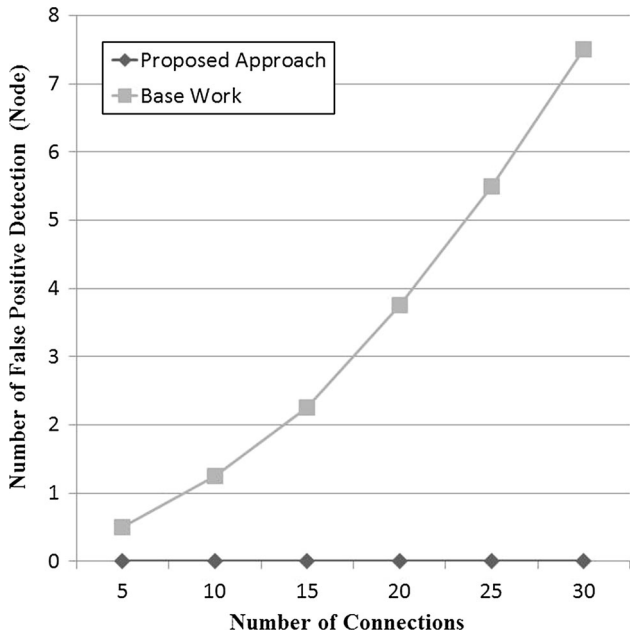


Fig. 6 Evaluation of false positive detection

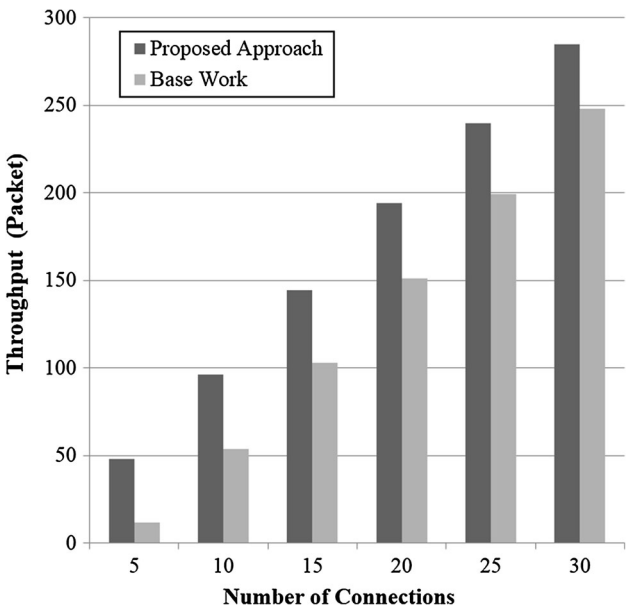


Fig. 7 Evaluation of network throughput

connections, congestion increases and network throughput decreases. However, congestion and packet lost rate is not very high.

It is clear from Fig. 7 that in the proposed approach, network throughput is by far higher than base work. The reason is that in base work just one of malicious nodes is detected by security mechanism. While in our work all malicious nodes are detected by each node.

Another benefit of the proposed approach is that it eliminates malicious nodes by using EDRI table. Therefore, after that one node is detected as malicious node, it would be isolated from the whole network by using "BHN" column in EDRI table. In consequence, other nodes disregard RREPs from marked nodes. Moreover, by taking advantages of trusted nodes and our EDRI table, overhead and delay for checking path decreases sharply by passing time and in the best situation a secure path may be generated without any overhead or delay. This is completely depends on the position of trusted nodes in the selected path.

In this section the simulation results of our approach and base work have been discussed and analyzed. We clarified that our approach is able to detect malicious nodes in selected path without false positive detection and eliminate them from the network by using an additional packet. EDRI table and trusted nodes are another plus of our work. Existing DRI based approaches extremely suffer from false positive detection while our work is safe against it. More importantly, in existing approaches by passing time packet overhead and delay may increase and has no reduction, since detected malicious nodes can return back to network, while in our work these parameters not only decrease significantly, but also could possibly reach to zero based on position of trusted nodes. As another noticeable advantage our approach could simply deal with nodes which are getting out of range of their neighbor without any additional control or delay. Furthermore, each node could be sure that its sent packets are received by its NHN.

6 Conclusion and future work

Mobile Ad hoc Network (MANET) is a kind of Ad hoc network with mobile, wireless nodes. Its special characteristics like open network boundary, dynamic topology and wireless communications made security highly challengeable. Black hole attack disrupts normal network functionality by sending bogus routing information during route discovery phases. In cooperative black hole attack, malicious nodes work together to defeat security mechanism.

In this paper, we proposed an approach for detecting and eliminating cooperative malicious nodes in ADOV-based MANET. An Extended Data Routing Information (EDRI) table and a data control packet are presented in order to reduce delay and packet overhead of security mechanism, in our approach, each node has to commence the security algorithm before sending data packets. Data control packet is sent hop-by-hop for checking the safety of path. Simulation results show that our approach generate the safe path with lower packet overhead and delay. False positive is eliminated in our study and network throughput is increased in comparison to our base work. Moreover, using data control packet and EDRI table, number of trustable nodes increases dramatically; therefore, delay and packet overhead will decreases (in best situation reaches to zero), and network throughout increases by passing time in network.

As a future scope of work, the proposed security approach can be extended to detect all malicious nodes in network; either they work cooperatively or not.

References

1. Kies, A., Mehar, S., Rodwane, B., & Maaza, Z. M. (2012). Self-organization framework for mobile ad hoc networks. In *8th international wireless communications and mobile computing conference (IWCMC)*.
2. Kaur, T., Toor, A. S., & Saluja, K. K. (2014). Defending MANETs against flooding attacks for military applications under group mobility. *Engineering and Computational Sciences (RAECS), 2014 Recent Advances in IEEE* (pp. 1–6). Chandigarh. doi:10.1109/RAECS.2014.6799499.
3. Zehua, W., Yuanzhu, C., & Cheng, L. (2014). PSR: A lightweight proactive source routing protocol for mobile ad hoc networks. *IEEE Transactions on Vehicular Technology, 63*, 859–868.
4. Zahidi, S. Z. H., Aloul, F., Sagahyroon, A., & El-Hajj, W. (2013). Optimizing complex cluster formation in MANETs using SAT/ILP techniques. *IEEE Sensors Journal, 13*, 2400–2412.
5. Dorri, A., & Nikdel, H. (2015). A new approach for detecting and eliminating cooperative black hole nodes in MANET. In *7th conference on information and knowledge technology (IKT)*, (pp. 1–6). 26.
6. Jhaveri, R. H., Patel, S. J., & Jinwala, D. C. (2012). DoS attacks in mobile ad hoc networks: A survey. In *Second international conference on advanced computing & communication technologies (ACCT)*. f.
7. Sharma, D., Gajkumar Shah, P., & Huang, X. (2010). Protecting from attacking the man-in-middle in wireless sensor networks with elliptic curve cryptography key exchange. In *NSS '10 proceedings of the fourth international conference on network and system security*.
8. Dorri, A., Kamel, S. R., & Kheyrkhah, E. (2015). Security challenges in mobile ad hoc network: A Survey. *International journal of Computer science and engineering survey (IJCSES),*. doi:10.5121/ijcses.2015.6102.
9. Khan, Z. A., & Islam, M. H. (2012). Wormhole attack: A new detection technique. In *International conference on emerging technologies (ICET)*.
10. Morshed, M. M., Ko, F. I. S., Dongwook, L., & Rahman, M. H. (2010). Performance evaluation of DSDV and AODV routing protocols in mobile ad hoc networks. In *4th international conference on new trends in information science and service science (NISS)*.

11. Jhaveri, R. H. (2013). MR-AODV: A solution to mitigate blackhole and grayhole attacks in AODV based MANETs. In *Third international conference on advanced computing and communication technologies (ACCT).*
12. Ismail, Z., & Hassan, R. (2010). Performance of AODV routing protocol in mobile ad hoc network. In *International symposium in information technology (ITSim)* (Vol. 1).
13. Dhurandher, S. K., Woungang, I., Mathur, R., & Khurana, P. (2013). GAODV: A modified AODV against single and collaborative black hole attacks in MANETs. In *27th international conference on advanced information networking and applications workshops (WAINA).*
14. Bagwari, A., Jee, R., Joshi, P., & Bisht, S. (2012). Performance of AODV routing protocol with increasing the MANET nodes and its effects on QoS of mobile ad hoc networks. In *International conference on communication systems and network technologies (CSNT).*
15. Jhaveri, R. H., Patel, S. J., & Jinwala, D. C. (2012). Improving route discovery for AODV to prevent black hole and gray hole attacks in MANETs. *INFOCOMP Journal of Computer Science, 11*(1), 1–12.
16. Mishra, A., Jaiswal, R., & Sharma, S. (2012). A novel approach for detecting and eliminating cooperative black hole attack using advanced DRI table in ad hoc network. In *IEEE*.
17. Jaisankar, N., Saravanan, R., & Durai Swamy, K. (2010). A novel security approach for detecting black hole attack in MANET. *Information Processing and Management Communications in Computer and Information, Science, 70*, 217–223.
18. Nath, I., & Chaki, R. (2012). BHAPSC: A new black hole attack prevention system in clustered MANET. *International Journal of Advanced Research in Computer Science and Software Engineering, 2*(8), 113–121.
19. Surana, K. A., Rathi, S. B., Thosar, T. P., & Mehatre, S. (2012). Securing black hole attack in routing protocol AODV in MANET with watchdog mechanisms. *World Research Journal of Computer Architecture, 1*(1), 19–23.
20. Jain, S., Jain, M., & Kandwal, H. (2010). Advanced algorithm for detection and prevention of cooperative black and gray hole attacks in mobile ad hoc networks. *International Journal of Computer Applications, 1*(7), 37–42.
21. Rutvij, H. J., Sankita, J. P., & Devesh, C. J. (2012). A novel approach for grayole and black hole attacks in mobile ad hoc networks. In *Second international conference on advanced computing and communication technologies*, IEEE.
22. Thachil, F., & Shet, K. C. (2012). A trust based approach for AODV protocol to mitigrate black hole attack in MANET. In *International conference on computing science*.
23. Bindra, G. S., Kapoor, A., Narang, A., & Agrawal, A. (2012). Detection and removal of cooperative black hole and gray hole attacks in MANETs. In *International conference on system engineering and technology*, IEEE.
24. Sen, J., Koilakonda, S., & Ukil, A. (2011). A mechanism for detection of cooperative black hole attack in mobile ad hoc networks. In *Second international conference on intelligent systems, modelling and simulation (ISMS).*
25. Weerasinghe, H., & Fu, H. (2007). Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation. In *Future generation communication and networking, FGCN* (Vol. 2).

Ali Dorri received his bachelor degree in Computer Engineering from Bojnourd University, IRAN, 2012. He then commenced his master degree in Computer Engineering in Islamic Azad University of Mashhad, IRAN, working on Mobile Ad hoc Networks and security issues rising from this sort of network. He now is a Ph.D. candidate in University of New South Wales (UNSW), Sydney. His current research interest covers security and privacy concerns in the context of Internet of Things (IoT), Wireless Sensor Network (WSN) and Vehicular Ad hoc Network (VANET). Moreover, he is working on fuzzy logic systems and routing protocols in wireless networks.