Detection and Removal of Gray, Black and Cooperative Black Hole Attacks in AODV Technique

Hosny M. Ibrahim, Nagwa M. Omar, Ebram K. William
Information Technology Department
Faculty of Computers and Information, Assiut University
Assiut, Egypt

***Abstract*—Mobile ad hoc network (MANET) is an autonomous self-configuring infrastructure-less wireless network. MANET is vulnerable to a lot of routing security threats due to unreliability of its nodes that are highly involved in the routing process. In this paper, a new technique is proposed to enhance the security of one of the most popular MANET routing protocols that is called Ad hoc on Demand Distance Vector (AODV) with minimum routing overhead and high packet delivery ratio. The proposed technique intends to detect and remove black, gray, and cooperative black hole AODV attacks depending on a mobile backbone network constructed from randomly moving regular MANET nodes based on their trust value, location, and power. The backbone network monitors regular nodes as well as each other to periodically estimate monitoring trust values which represent the reliability of each node in the network. The drop in the monitoring trust value of any node is used as a clue to its malicious behavior. The backbone network also tries to bait the malicious nodes to reply to a request for a route to fake destination address. The proposed technique uses the control packets of the AODV to exchange its control information which highly reduces the overhead. The simulation results show that the performance of the proposed technique is more secure than AODV and the other recently introduced techniques.**

Keywords*—MANET; AODV; Black Hole Attack; Gray Hole Attack; Cooperative Black Hole Attack

I. INTRODUCTION

Mobile ad hoc network (MANET) [1] is a set of mobile nodes communicate wirelessly to establish network without fixed infrastructure. MANET provides flexible communication when there are geographical or terrestrial constraints. Battlefields, military applications, emergencies and some disaster management situations need the existence of infrastructure-less network such as MANET [1].

MANET has a dynamic topology in which each node has unrestricted mobility, connectivity, and changes its links to other nodes frequently. In such networks the routing is not an easy task [1]. Routing in MANET is done cooperatively between nodes. Each node works as a router that forwards packets for other nodes. These infrastructure-less mobile nodes dynamically participate in an ad hoc route discovery process and create routes among themselves to form a wireless network on the fly. Due to the wireless communication nature and the collaboration of MANET nodes in finding routing paths, MANET is more vulnerable to security threats than ordinary wired networks [2]. Another characteristic of a MANET is its resource constraints, i.e., limited bandwidth and battery power of its nodes [1]. Dynamic Source Routing (DSR), Ad hoc On Demand Distance Vector (AODV), Optimized Link State Routing (OLSR), and Destination Sequence Distance Vector (DSDV) protocols are the most popular MANET routing protocols [1].

Many security techniques are introduced to prevent different MANET attacks [2]. Many of these techniques are directed to protect AODV [4] routing protocol from attacks because it is a popular reactive routing protocol designed for mobile ad hoc network. AODV is self-starting, multi-hop, has low processing and low routing overhead, and suitable for dynamic network changes [3] but it does not take security issues into consideration [5].

In this paper, a new technique is proposed to enhance AODV security. It uses a mobile backbone network to efficiently detect and remove the gray, black, and cooperative black hole attacks based on nodes' trust values. NS2 simulator [6] is used to evaluate the performance of the proposed technique. The simulation results show that, the proposed technique gives minimum routing overhead, minimum delay, and high packet delivery ratio compared with AODV and other routing techniques that are introduced to solve the security issues in AODV algorithm.

The rest of this paper is organized as follows: related work is presented in section 2. The proposed technique is described in section 3. Simulation and comparison results are presented in section 4. Finally, section 5 is a conclusion of the proposed technique.

II. RELATED WORKD

This section reviews the AODV routing protocol and its security attacks as well as the advantages and disadvantages of many algorithms that are recently introduced to solve the security issues in AODV.

A. AODV Routing Protocol

The AODV protocol consists of two important phases, Route Discovery and Route Maintenance. In Route Discovery, when a node wants to communicate with another node and there is no valid route in its routing table, it broadcasts a route request packet (RREQ). A node that receives a RREQ for the first time sets up a reverse route to the source node in its routing table. If the node is the destination or has a valid route to the destination, it unicasts a route reply (RREP) along the reverse path back to the source node. Otherwise, it will

increase the hop count in the RREQ by one and forward the RREQ to other nodes. In Route Maintenance phase, neighboring nodes periodically exchange HELLO messages to know its one-hop neighbors. If one node didn't receive a HELLO message from a neighboring node within a certain time interval, the node breaks the routing table information of this neighbor node and sends a Route Error (RERR) message to the nodes on a route with this neighbor.

B. AODV Security Attacks

The work in the current paper focuses on three types of attacks:

Black hole attack [3, 8, 9]: a black hole node is a malicious node that sends a false reply with an apparently valid route to the destination node. It replies every single RREQ with false sequence number, so it acquires the route, and then eavesdrops or drops all data packets that pass through it.

Gray hole attack (selective black hole) [8, 9]: looks like a black hole attack, but a malicious node randomly changes its state between regular node and black hole node. Accordingly, gray hole is harder to be detected by security techniques.

Cooperative black hole attack [9, 10]: two nodes or more in this attack cooperate to gain the path between the source and the destination nodes. When one node gains the path selectively drops or forwards the data packets to one of its cooperating nodes. Cooperation between black hole nodes helps malicious nodes to escape from monitoring techniques.

C. Fighting AODV Security Attacks

There are many techniques presented recently to mitigate security attacks in MANET [1], but this section reviews only some of the techniques that relate to the proposed technique.

Ming-Yang Su [11] presented an intrusion detection system (IDS) to detect and prevent selective black hole attacks. In IDS system, several fixed IDS nodes are distributed and set in sniff mode in order to estimate a suspicious value of a node. The simulation results show that the IDS technique can be used effectively to block the malicious nodes if a proper threshold is set, but IDS technique has some disadvantages: 1) it uses fixed, trusted, and powerful nodes to detect the malicious nodes, which violate the mobility feature of the MANET [12, 13] 2) the scheme suffers from high routing overhead.

The authors in [14] introduced a technique for detecting cooperative black and gray hole attack in MANET using a backbone network of strong nodes established over the ad hoc network. This backbone network monitors the overall traffic in the network with the help of regular untrusted nodes. The disadvantages of this algorithm are: 1) regular nodes can join the backbone based only on their power and location without taking into consideration their reliability and trust 2) the backbone nodes carry an end to end check based on regular nodes' request which can be used by malicious nodes to exhaust backbone recourses. 3) The backbone nodes ask normal nodes, which may be malicious to perform monitoring which give deceiving results. 4) Assuming that there is a difference between regular nodes and backbone nodes in terms of power and antenna range which is not suitable. 5) It is not proved that the backbone network is optimal in terms of minimality and coverage. 6) The technique suffers from high end-to-end delay and high routing overhead. 7) The technique executes an end-to-end check after every transmission of a block of data which is not an optimum solution. 8) The technique assumes that a node has strong neighbors more than malicious nodes, which may not be always satisfied [9, 12, 13].

Also, K. Vishnu, and A. J. Paul [15] presented a mechanism to detect and remove cooperative black and gray holes. It assumes that the network is divided into clusters and a backbone network is present in the MANET [14]. Each backbone node (BBN) knows a valid set of addresses that is used in the network. Only the backbone network in MANET is permitted to select the addresses for non configured hosts [16]. When the source node wants to transmit data, it asks the nearest BBN for non used IP in the network which is called restricted IP (RIP). The source node sends a RREQ for both the destination and the RIP simultaneously. If the source node receives a RREP for the RIP, it means that there is a black hole in that route. The source node sends a few dummy data packets to that destination. When a monitoring node finds that the loss in dummy data packets is more than the normal expected loss at an intermediate node, it informs the source node about this malicious node. Also, the neighbor nodes broadcast an alert message and add this malicious node to the black hole list. This technique has the following drawbacks: 1) regular nodes are assumed to be trusted by default. They participate in the monitoring process and take critical decisions to isolate other nodes, which is not secure [17]. 2) The authors didn't propose simulation results to test the performance of their scheme. 3) The mechanism will fail if malicious nodes keep asking the BBNs for RIP, save RIPs, and stop replying to RIP RREQs. 4) It suffers from routing overhead. 5) It detects black and gray hole nodes depending on the desire of the source node to send data to a destination node.

Authors in [10] presented an enhancement of the AODV to mitigate cooperative black hole attacks by introducing fidelity table wherein every node is assigned a fidelity level that acts as a measure of the reliability of that node. When the destination node receives the data packets, it sends an acknowledgment to the source and the fidelity level of the intermediate node is increased. If the fidelity level of any node drops to zero, it is considered as malicious node and is isolated. The algorithm can mitigate cooperative black hole, but it has many drawbacks [8]: 1) the fidelity tables of nodes are maintained and exchanged periodically among the participating nodes which increase the overhead and the processing delay. 2) Additional overhead and time delay are introduced due to the use of the acknowledgements.

III. THE PROPOSED TECHNIQUE

This paper proposes a technique to enhance AODV security. This technique attempts to detect and remove gray, black and cooperative black hole attacks with the aid of a network of mobile backbone nodes. The proposed technique is divided into four main phases:

*1) **Mobile Backbone Network Constructions:** in which, a mobile backbone network is constructed and updated based on nodes trust value*

*2) **MANET Formation:** in which, new clients join the MANET and the network nodes are grouped to give good performance.*

*3) **Detection of Malicious Nodes:** in which, two methods are implemented with the aid of the backbone network to detect malicious nodes.*

*4) **Removal of Malicious Nodes:** this phase starts after detecting malicious nodes; in which, the backbone network isolates the malicious nodes.*

These phases will be explained in more details in the next subsections.

B. Mobile Backbone Network Formation

The proposed technique intends to increase the security of AODV depending on the mobile network of secure backbone nodes. This backbone network should be trustable, have dynamic behavior, does not violate the mobility characteristic, structured of the regular MANET nodes, and has good coverage.

To achieve these characteristics, each node in the backbone network maintains two different values:

1) Monitoring trust value (MTV) for each of its neighbors that represents the reliability of the node.

2) Its trust value (TV), which is used to specify its operations and allowed decisions.

The estimation of the monitoring trust value varies in various introduced techniques. In [11], the estimation of trust value is not adequate since it depends only on the routing control packets and doesn't take dropping data packets into consideration. The techniques that are introduced in [10, 14] estimate the monitoring trust value based on the dropped data packets only but doesn't take into account the routing control packets. Also, they present high overhead and time delay.

The proposed technique in this paper introduces new criteria to estimate the monitoring trust value. The following equation is suggested to estimate the monitoring trust value for node (i):

$$MTV_i = \tanh(C_1 \frac{F\_DPs_i}{R\_DPs_i}) \tanh(C_2 \frac{R\_RREQs_i}{S\_RREPs_i}) \quad (1)$$

Where $0 \le MTV_i \le 1$, (F_DPs_i) is the number of the forwarded data packets that are not originated from the node , i, (R_DPs_i) is the number of the received data packets that is not targeted to the node, i, (R_RREQs_i) is the number of received route requests to the node, i, (S_RREPs_i) is the number of sent route replies from the node, i, and C_1 and C_2 are constants adjusted experimentally.

To increase the coverage of the backbone network, it should choose new nodes from the neighbors based on their MTVs, power and location to join the backbone network.

The new chosen nodes have lower level than the ones that choose them in the backbone hierarchy. The higher level backbone network nodes assign the lower level ones TVs. The trust value of the backbone network nodes is estimated using the following suggested equation:

$$TV_i = \frac{1}{L_j} * TV_j * MTV_i \ , \quad \text{where } 0 \le TV \le 1 \quad (2)$$

Where TV_i is the trust value of the new chosen node, i. TV_j is the trust value of the original backbone node, j. MTV_i is the monitoring trust value of the chosen backbone node, i. L_j is the level of the original backbone node. The backbone network node level is calculated using the following suggested equation:

$$L_i = L_j + 1 \quad (3)$$

Where L_i and L_j are the trust levels of the chosen backbone node, i, and the original backbone node, j, respectively. The highest level in the backbone network hierarchy is one.

The backbone network contains four types of nodes as follows:

*1) **Seed Backbone Nodes (SBBNs):** which face the difficulties in the backbone initialization. The mobile backbone network should have high trustable nodes at the start to judge the behavior of the new MANET clients. Accordingly, the backbone network needs to be initialized by powerful trustable mobile seeds before it reaches the autonomous mobile dynamic backbone structure. At least one SBBN is needed to construct the backbone network. SBNNs are distributed in the initialization step to cover the target area. SBNNs have trust value and level equal to one which are the maximum. Each SBBN has a pool of addresses that are used in the network. The SBBNs are the only nodes that have the permission to send addresses to the new nodes that join their clusters. Also, each SBBN monitors other nodes in its cluster to employ alternative backbone node based on its MTV, which is called a backbone node (BBN) and sends it the essential information then, SBBN enters a sleeping mode.*

*2) **Backbone Nodes (BBNs):** start as regular nodes, then are changed to take the role of SBBN to perform the monitoring function in their clusters and judge the other nodes behavior based on their MTVs. Every BBN employs the highest trusted nearest neighbor node to be its vice backbone node (VBBN) and periodically sends it its control information. To increase the coverage and improve the performance, BBNs can employ other nodes with high MTVs to be capable backbone nodes (CBBNs). There is one BBN in each cluster.*

*3) **Vice Backbone Nodes (VBBNs):** can take the role of BBN in case of BBN movement or power drop. There is one VBBN in each cluster*

*4) **Capable Backbone Nodes (CBBNs):** are employed to assist BBNs and to increase the coverage. CBBNs can employ other level of CBBNs.*

Each backbone network node (SBBN, BBN, VBBN, CBBN) assigns the new employed backbone node a trust value

and level using equations (2, 3) to specify the operations and allowed decisions for each node in the backbone network

The following steps illustrate the task of initializing the backbone network held by the SBBNs; assuming that initial mobile trustable seeds are equally distributed in the target area, can communicate with each other, know each other locations, contain a pool of addresses, and every SBBN is a seed for a cluster of MANET nodes:

1) If SBBN is not in a sleeping mode,
   a) If SBBN receives newly arrived clients requests to join the most powerful and closest distance SBBN,
      i. SBBN sends a reply to the client contains a unique address selected randomly from its pool of unused addresses. The process of assigning address to newly arrived clients is described in more details in section (3.5).
   b) SBBN continuously monitors its clients to judge their performance and sets them monitoring trust values (MTVs).
   c) For each node, obtain node's MTV,
      i. If node's MTV is less than experimentally chosen SUSPICIOUS NODE THRESHOLD,
         1. A node is considered suspicious.
      ii. Else if it finds a regular node that has MTV greater than experimentally chosen BBN THRESHOLD, the closest node to the SBBN, and it is the most powerful,
         1. SBBN employs this node to be the new mobile backbone node (BBN) for this cluster and takes SBBN role.
         2. SBBN sends to it the essential information.
         3. SBBN assigns the BBN's TV.
         4. SBBN starts wake up timer and enters a sleeping mode.
   d) Start rechecking nodes MTV timer.
   e) If rechecking timer elapsed,
      i. Go to step (1.c).
2) Else if SBBN is in a sleeping mode,
   a) If the wake up timer elapsed,
      i. SBBN wakes up to monitor the backbone network nodes and sets them monitoring trust values (MTVs).
      ii. For each node, obtain node's MTV,
         1. If the neighbor is BBN and its MTV is less than experimentally BBN THRESHOLD,
            a. The neighbor status is changed to be a regular one.
            b. Go to step (1.a).
         2. If the neighbor is VBBN/CBBN and its MTV is less than experimentally VBBN/CBBN node THRESHOLD,
            a. The neighbor status is changed to be a regular one.
            b. SBBN informs the BBN.
         3. Else if node's MTV is less than experimentally chosen SUSPICIOUS NODE THRESHOLD,
            a. A node is considered suspicious.
      iii. SBBN starts wake up timer and enters a sleeping mode.

The following points illustrate the operations of the backbone network held by the BBNs in every cluster taking into consideration that each cluster has only one BBN:

1) BBN takes the role of SBBN or BBN will be a cluster grouping point and the clients are regrouped to join this cluster.
2) Start regrouping timer.
3) If the regrouping timer elapsed,
   a) Each BBN will be a cluster grouping point and the clients are regrouped to join this cluster. Regrouping process is repeated based on the movement speed.
   b) Start regrouping timer.
4) Each BBN adds its neighbors to its MONITORED NODES LIST.
5) BBN receives newly arrived clients requests to join the most powerful, closest distance BBN.
   a) BBN sends a reply to the client contains a unique address selected randomly from its pool of unused addresses. The process of assigning address to newly arrived clients is described in more details in section (3.5).
6) Each BBN continuously monitors its neighbors including regular nodes and lower level backbone network nodes to judge their performance and sets them MTVs.
7) For each node, obtain its MTV,
   a) If the neighbor is VBBN/CBBN and its MTV is less than experimentally VBBN, CBBN node THRESHOLD,
      I) The neighbor status is changed to be regular one
      II) BBN removes the node's covered addresses from its MONITORED NODES LIST and starts the coverage process.
   b) Else if node's MTV is less than experimentally chosen SUSPICIOUS NODE THRESHOLD,
      I) A node is considered suspicious.
   c) Else if there are no VBBN and a regular node's MTV is greater than experimentally chosen VBBN THRESHOLD, the closest node to the BBN, and it is the most powerful,
      I) BBN chooses this node to be its vice backbone node.
      II) BBN assigns VBBN's TV and level.
8) Start rechecking nodes MTV timer.
9) If the rechecking timer elapsed,
   a) Go to step 7.
10) If there are VBBN,
   a. Each BBN periodically, based on HELLO message interval, sends the assigned addresses in its cluster and the MONITORED NODES LIST to its VBBN.
11) If the BBN suffers a low battery condition and there are VBBN,
   a. The BBN asks its VBBN to take its IP and role.
   b. The BBN changes its status to be regular node.
   c. End.
12) If BBN receives information about changing a backbone node status to a regular node,
   a. BBN removes the node's covered addresses from its MONITORED NODES LIST and starts the coverage process.
13) Each BBN periodically, based on HELLO message interval, asks the backbone network nodes in its cluster for their neighbors.
14) When BBN receives replies,
   a. Each BBN add not repeated replies to its MONITORED NODES LIST.
15) BBN periodically, based on HELLO message interval, checks its MONITORED NODES LIST.
16) If there are assigned addresses in BBN's cluster not in its MONITORED NODES LIST this is an indication that there are unmonitored nodes. In this case, the following is achieved to employ new backbone network nodes which are called CBBNs to monitor the uncovered nodes,
   a. Inform the backbone network nodes in its cluster with these addresses.
   b. If BBN finds regular nodes in its neighbors that have MTVs greater than experimentally chosen CBBN THRESHOLD,
      I) BBN asks if they have these addresses in their neighbor list.
      II) When BBN receives replies, The BBN,
         (1) Chooses the one with the highest MTV and

power to be the new CBBN.
(2) Adds the new covered address in its MONITORED NODES LIST.
(3) Assigns the new CBBN TV and level.
(4) Informs the backbone network with the CBBN's address.

c. If BBN receives suggestions for CBBNs,
I) BBN chooses the one with the highest MTV and power.
II) Adds the new covered address in its MONITORED NODES LIST.
III) BBN informs the backbone network in its cluster with the CBBN's address.

17) Else if there are no assigned addresses in BBN's cluster not in its MONITORED NODES LIST,
a. BBN ends the coverage process.

The following steps illustrate the operation of the backbone network held by the VBBN and CBBNs taking into consideration that each cluster can have only one VBBN and more than one CBBN:

1) If the VBBN discovers a BBN link failure,
a) It takes the IP and the role of BBN.
b) End.
2) Each VBBN/CBBN continuously monitors its neighbors to judge their performance and sets them monitoring trust values (MTVs).
3) For each node, obtain its MTV,
a) If the neighbor is CBBN and its MTV is less than experimentally CBBN THRESHOLD,
I) The neighbor status is changed to be a regular one and inform the BBN.
b) Else if node's MTV is less than experimentally chosen SUSPICIOUS NODE THRESHOLD,
I) A node is considered suspicious.
4) Start rechecking nodes MTV timer.
5) If the rechecking timer elapsed,
a) Go to step 3.
6) If VBBN/CBBN receives BBN request asks for its neighbors,
a) VBBN/CBBN replies with its neighbors.
7) If VBBN/CBBN receives request to be changed to a regular node,
a) VBBN/CBBN changes its state to be regular node.
8) Each VBBN periodically, based on HELLO interval, receives the assigned addresses and the MONITORED NODES LIST from its BBN.
9) If VBBN finds that there are assigned addresses in BBN's cluster not in the MONITORED NODES LIST OR If CBBN receives assigned addresses in BBN's cluster and not in BBN's MONITORED NODES LIST,
a) If VBBN/CBBN finds regular nodes in its neighbors that have MTVs greater than experimentally chosen CBBN THRESHOLD,
I) VBBN/CBBN asks if they have these addresses in their neighbor list.
II) When VBBN/CBBN receives replies, The VBBN/CBBN,
(1) It sends the BBN a suggestion carries information about the one with the highest MTV and power to be employed as new CBBN.
(2) If VBBN/CBBN receives BBN request to employ new CBBN,
a. VBBN/CBBN assigns the new CBBN TV and level.
10) Else if VBBN finds that there are no assigned addresses in BBN's cluster not in its MONITORED NODES LIST,
a) VBBN ends the coverage process.

As shown from previous tasks for every backbone network node type, the nodes of the backbone network monitor each other as well as the regular nodes that are located in their transmission range and set them MTVs which represent the reliability of each node in the network. The level of backbone network nodes can be changed based on MTV, power, movement, and coverage. Except the initial seeds, no backbone node is considered trusted forever. Increasing the number of BBNs and CBBNs helps in facing the dynamics of MANET, increases the coverage, increases the reliability, distributes the control, saves the nodes recourses, and speeds up the detection and the removal process.

The construction of the backbone network consumes low overhead because all control information that is exchanged between backbone network nodes is added to the AODV HELLO message as additional fields.

As shown from the discussion, the proposed multi-level backbone network is mobile, dynamic, trusted, powerful, has high coverage, reliable, distributes the control, saves the nodes recourses, and robust can face nodes failure. The backbone network uses multi-hop communication to communicate with each other as well as with regular nodes. Unlike the technique in [11], the proposed technique doesn't use permanent fixed nodes. Also, it is more secure and practical than the introduced backbone in [14] which chooses the backbone nodes based on their power and coverage assuming that all backbone nodes are powerful and trusted by default. The proposed backbone network is constructed and updated based on the nodes trust value in addition to power and coverage. Unlike the other techniques, the proposed technique has not considered any node to be trusted forever including the backbone nodes. Also, the backbone network nodes are the only nodes, that are permitted to monitor and judge the behavior of other nodes, which is considered more secure than the technique that is proposed in [17]. The monitoring process can be used for malicious node detection as well as for backbone construction.

C. MANET Formation

This section describes how new clients join the MANET. The proposed technique uses the BBNs as approximate centers of clusters to facilitate and speed up the communication process. Every BBN has a pool of unique addresses that is used to configure nodes in its cluster. The proposed technique follows the technique that is used in [15, 16] but it modifies the equation that is used by [16] to allocate the range of host addresses as follows:

$$\text{Range of addresses of } BBN_i = i * BaseValue + n \quad \text{for } 0 \le n < BaseValue; 0 \le i < K \tag{4}$$

Where K is the number of BBNs, and BaseValue is the maximum number of addresses that are supported by every BBN.

Newly arrived clients broadcast requests to BBNs to join the most powerful, closest distance BBN. The clients may be regrouped according to the node's movements. In each cluster, there are one BBN, one VBBN, and CBBNs to cover the cluster area. A lot of clustering techniques for MANET is

discussed in [18]. K-means [19] is one of the simplest algorithms that solves the clustering problem. Accordingly, it is used to group nearby nodes in the proposed technique. The proposed technique tries to keep the BBNs as cluster grouping points even if they are not located exactly in the cluster centers because BBNs are permitted to move randomly.

D. The Detection of black, gray, and cooperative black holes in AODV

Two methods are proposed in the current technique to detect malicious nodes:

1) The first method is based on the monitoring trust values (MTVs) which is estimated using equation (1).

2) The second method is based on baiting the malicious node to reply to requests for route to not existing destination in the MANET.

In the first method, the backbone network periodically checks neighbors MTVs. A node is considered malicious one if its MTV is less than experimentally chosen SUSPICIOUS NODE THRESHOLD. Each node in the backbone network has a suspicious node list. Each entry in this list contains suspicious node ID, discovering nodes TVs, discovering nodes IDs, and suspicious node MTV. The action that is taken by the discovering backbone network node is limited by its trust value.

The following points illustrate the steps executed by the backbone network nodes in the first method:

1) The backbone network node checks neighbors MTVs including the other backbone network nodes.
2) For each node, obtain next node's MTV,
   a) If node's MTV is less than experimentally chosen SUSPICIOUS NODE THRESHOLD,
      i) A node is considered suspicious.
      ii) If the discovering node TV is greater than experimentally chosen REMOVING NODE THRESHOLD,
         (1) The discovering node starts the removal process which will be described in detail in section 4.4.
      iii) Else if the discovering node TV is less than experimentally chosen REMOVING NODE THRESHOLD,
         (1) The discovering node searches its suspicious node list for the suspicious node ID.
         (2) If the discovering node does not find the suspicious node ID in its suspicious node list,
            (a) The discovering node adds an entry contains (discovering node ID, discovering node TV, suspicious node ID, and suspicious node MTV) to its suspicious node list. That entry fields are shown in Figure (4.3).
            (b) The discovering node informs the backbone network with that entry using additional control fields added to the HELLO message.
         (3) Else if the discovering node finds an entry of the suspicious node ID in its suspicious node list,
            (a) If this entry contains only the discovering node which can be happened if the discovering node added this entry before and the suspicious node is not removed yet,
               (i) The discovering node updates its TV and the suspicious node MTV in this entry.
               (ii) The discovering node informs the backbone network nodes.
            (b) Else if this entry contains another discovering nodes including or not including the discovering node which give indication that the discovering node received messages from neighbors confirm that they discover the same suspicious node,
               (i) The discovering node combines the TVs of all the discovering nodes in the entry including its new TV and calculates combined TV using equation (4.1).
               (ii) If the combined TV is greater than REMOVING NODE THRESHOLD,
                  1. The discovering node starts the removal process.
               (iii) Else if the combined TV is less than REMOVING NODE THRESHOLD,
                  1. If the discovering node is included in the entry,
                     a. The discovering node updates its new TV and the suspicious node MTV.
                  2. Else if the discovering node is not included in the entry,
                     a. The discovering node appends its ID, TV, and the suspicious node MTV in the entry.
                  3. The discovering node informs the backbone network.
3) Set up a timer for rechecking neighbors MTVs.
4) If the timer interval elapsed,
   a) Go to step 1.

The following steps illustrate the operation executed by the backbone network nodes in the first method upon receiving suspicious node entry:

1. The backbone network node receives the suspicious node information.
2. It searches its suspicious node list for the suspicious node ID.
3. If it does not find the suspicious node ID in its suspicious node list,
   a. It adds the received information as an entry to its suspicious node list.
   b. It informs the backbone network with that entry.
4. If it finds an entry of the suspicious node ID in its suspicious node list,
   a. It combines the TVs of all the discovering nodes in the entry with the new received information using equation (5).
   b. If the combined TV is greater than REMOVING NODE THRESHOLD,
      i. It starts the removal process.
   c. If the combined TV is less than REMOVING NODE THRESHOLD,
      i. It updates the suspicious nodes list entry using the received information.
      ii. It informs the backbone network.

As stated earlier, in some cases the backbone network nodes need to combine the TVs of all discovering nodes that are recorded in the entry including its new TV. The following equation is used to calculate the combined TV:

$$TV_{combined} = \tanh \sum_{i=1}^{n} TV_i \quad (5)$$

Where n is the number of the discovering nodes that are indicated in the entry.

As stated earlier, in addition to using the MTV value for detecting malicious nodes, the proposed technique uses another detection method. In this second method, the BBNs periodically perform a special check for malicious node detection. BBNs try to bait the attackers to send RREP to RREQ contains a fake destination address. As stated earlier in section (3.2), every BBN has a pool of disjoint unique addresses that is used to configure its clients in its cluster. This way of address allocation facilitates using the second method for malicious node detection.

The following points illustrate the steps held by the backbone network nodes of the second method:

1. BBN chooses a random unused address called restricted IP address (RIP).
2. BBN uses the AODV HELLO message to send this RIP to the backbone network which is considered as a sign for the backbone network to monitor any nodes that reply the RIP RREQ by RREP message.
3. The backbone network starts to monitor the neighbor nodes for any RREPs to that RIP.
4. BBN sends a RREQ to find a path to this fake destination.
5. If any backbone network node listens a RREP to that RIP RREQ,
   a. It saves the ID of the node that forwards the reply.
6. If the BBN receives a RREP for RIP RREQ,
   a. The BBN asks the backbone network for the monitoring information.
   b. The BBN figures out the source node of the RREP.
   c. The BBN moves into the removal process that will be described in section (3.4).
7. Set up a timer for baiting again malicious nodes.
8. If the timer interval elapsed,
   a. Go to step 1.

Using the two proposed methods to detect the malicious nodes, the proposed technique can mitigate black hole, gray hole, and cooperative black hole attacks. The black hole can be caught if it replies the RIP RREQs or if it drops data and sends a lot of RREPs compared to the RREQs. The gray hole attack can be detected by the same algorithm whenever it acts as a black hole node. Also, the proposed technique takes the history of the nodes into consideration when it estimates the MTVs which helps in detecting grayholes. Baiting malicious nodes to reply RIP RREQs can detect and isolate one node of the cooperative blackhole nodes whenever it tries to acquire the route. On the other hand in the monitoring process, if a source node needs to communicate with another node in the network, then the source node initiates the route discovery process by broadcasting RREQ. If one node of the cooperative blackhole nodes succeeds to acquire the route, then the source node starts to send its data packets. Upon the receipt of data packets, the black hole node starts to forward these data packets to other cooperating nodes. Other cooperating nodes forward these data packets to others and so on until one black hole node drops the data packets. In the proposed technique, the backbone network nodes can detect and isolate the black hole node which drops the data packets. After the isolation of one of the cooperative blackhole nodes, one of the remaining cooperative nodes has to reply RIP RREQs or drop data packets which facilitate its detection process by the proposed algorithm. The detection will continue in such way to catch the cooperative nodes one by one.

It can be shown that the proposed technique is more secure than [14, 15], because BBNs perform the security check periodically not based on a request from regular not trusted nodes, BBNs are the only nodes that perform the monitoring, detect and remove the malicious nodes, know the RIPs and send the RREQs for the RIPs.

The overhead of the proposed technique is lower than the other techniques in [10, 14, 15] because it doesn't use acknowledgments [10], it doesn't maintain and exchange a large amount of control data [10], it doesn't send dummy data [15], and it does not use special control packets to exchange its control information instead, it adds fields to the AODV HELLO message.

E. The Removal of Malicious Nodes

The removal process starts after detecting malicious nodes. The backbone network nodes that have the permission to isolate the malicious node start the removal process by adding the malicious node ID into its black list. Also the discovering node broadcasts the malicious node ID to other nodes in the network using additional control fields added to the HELLO message which is already implemented in AODV [7]. Each node receives the information that is integrated in HELLO message checks that the sender is one of the backbone nodes. After the validation step, the node adds the malicious node ID to its black list and adds the control information into its own HELLO message to redistribute the malicious node ID. Each node in the network ignores route replies (RREPs) and route requests (RREQs) that are received from any node in the black list to isolate the malicious nodes from the network. Also, each node deletes any route in its cash to any node in the black list. If all neighbor nodes around the malicious node do not forward their packets, the malicious node cannot communicate with the other nodes in the MANET and the malicious node is isolated from the network [20].

IV. SIMULATION RESULTS

NS2 simulator [6] is used in this paper to evaluate the performance of the proposed technique compared with other recent techniques such as IDS [11], hash-function [21], and AODV [7]. The simulation results are presented in the next subsections.

A. Comparison with IDS technique

In this subsection, the performance of the proposed technique is compared with Ming-Yang Su technique [11] as well as with the original AODV technique [7].

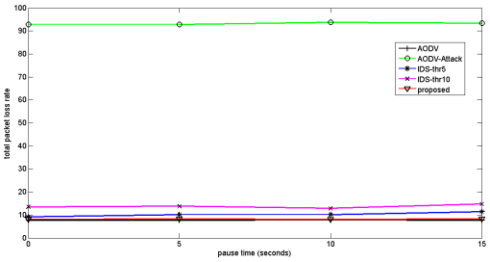
The current comparison is carried out using the same simulation parameters that are used in [11] except that the proposed technique doesn't use extra nodes. The used parameters are listed in Table (I). Random-way-point model [22] is used to allow nodes to move randomly. Each reading in the next figures is the average value resulting from a set of experiments under different scenarios of random movement. In [11], the total packet loss rates are calculated according to the ratio between the number of packets that fail to reach the destinations (missing packets) and the total number of packets that are transmitted from all source nodes of the entire network.

The results of the first comparison between the proposed, IDS, and AODV techniques are shown in Fig. 1. The total packet loss rates of one and two fixed selectively black holes (gray hole) are compared with IDS technique in case of IDS predefined thresholds of 5 and 10. The results are compared also with the ideal not attacked AODV as well as with AODV under attack. As shown from Fig. 1-a, when there is no attack, the mean total packet loss rate for all pause times by AODV is about 7.87%. When there is one fixed selective black hole node the rate by the attacked AODV raises to be about 92.40%. With IDS technique when the threshold value is set to 5, the rate is about 10.05%, and when the threshold is set to 10, the rate is about 13.04%. In the proposed technique the rate is successfully reduced to 8.14%. Fig. 1-b shows the mean total packet loss rate of all pause times when there are two fixed selective black hole nodes. The results are compared with the non attacked AODV in the case of the absence of selective black hole node. When there are no selective black hole nodes, the non attacked AODV gives a rate of about 7.73%, which increases to be about 97.32% when there are two fixed selective black hole nodes. IDS technique gives rate about 11.28% and 14.76% when the threshold values are set to 5, 10 respectively. The rate is successfully reduced to be about 9.83% in the proposed technique. It can be shown from the results that the proposed technique has the lowest mean total loss rate in case of one and two fixed gray hole nodes compared with AODV under attack and IDS. It can be shown that the proposed technique loss rate is very close to the rate of the ideal non attacked AODV.

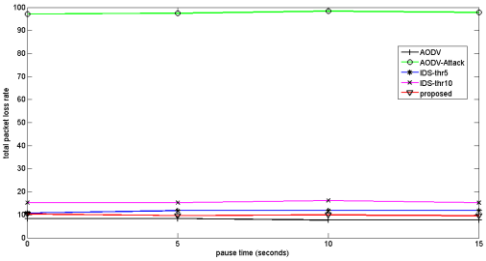
The second comparison between the proposed technique, IDS, and AODV, is carried out when there are one and two random moving selective black hole nodes, the results are illustrated in Fig. 2. As shown from Fig. 2-a, when there is one randomly moving a selective black hole node, the mean total loss rate in AODV under attack is about 86.53%. IDS technique gives rate about 10.29% and 12.55% when the threshold value is set to be 5 and 10 respectively. While in the proposed technique the mean rate is successfully reduced to be about 7.52%, which is close to the ideal non attacked AODV. Also, as shown from Fig. 2-b when there are two randomly moving selective black hole, AODV under attack gives mean total packet loss rate for all pause times about 94.64%, while IDS technique gives rates about 12.03%, and 14.57% with threshold values of 5 and 10 respectively. The rate is successfully reduced to 10.08% in the proposed technique. Also, it can be shown from this comparison that the proposed technique gives the lowest packet loss ratio which is also close to the ideal non attacked AODV ratio.

TABLE I. SIMULATION PARAMETERS

Parameter	Value
Area size	1000 m×1000 m
Normal nodes	50 (distributed and moving randomly)
Connections	20 pairs (40 nodes)
Transmission range	250 m
Traffic type	UDP-CBR (Constant Bit Rate)
Packet size	512 bytes
Mobility	Random-way point model
Maximum speed	20 m/s
Simulation time	500 s
Pause times	0s, 5s, 10s, and 15s
Malicious node(s)	one/two grayhole (fixed/moving)
Traffic rate	5 Kb/second

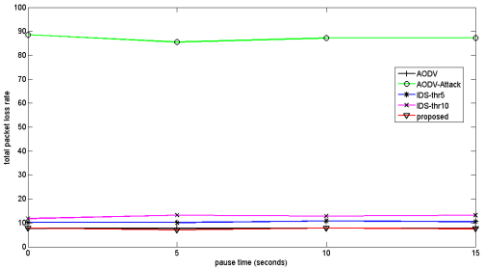


(a) One fixed selective black hole

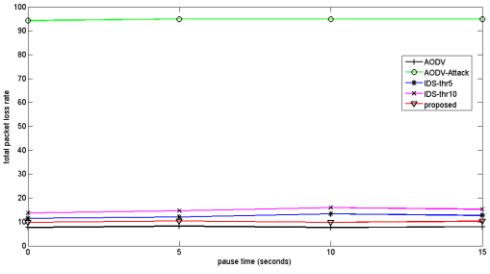


(b)Two fixed selective black holes

Fig. 1. Comparing total packet loss rate in AODV, IDS, and the proposed technique in case of fixed one and two selective black hole (gray hole)



(a)One randomly moving selective black hole



(b)Two randomly moving selective black hole

Fig. 2. Comparing total packet loss rate in AODV, IDS, and the proposed technique in case of randomly moving one and two selective black holes

The authors in [11] give a summary of the true positive rate and false positive rate. A true positive (TP) is defined in [11] as a selective black hole node being correctly judged as a black hole; whereas, a false positive (FP) is a normal node being misjudged as a black hole [11]. The TP rate is defined as the ratio between the number of the TP and the number of black hole nodes while the FP rate is defined as the ratio between the number of the FP and the number of the normal nodes. The results of the comparison between the proposed and IDS techniques are listed Tables (II, III). The results in case of fixed selective black hole(s) are listed in Table (II) and for randomly moving selective black hole(s) are listed in Table (III). As illustrated, the FP and TP of the proposed technique are 0% and 100% respectively in all cases which are better than IDS which gives worst FP rates in some cases. Also, the time of blocking in the proposed technique is better than IDS.

It can be seen from previous comparisons that the proposed technique gives better results than IDS technique and close to the ideal non attacked AODV behavior.

TABLE II. COMPARING TP RATE FP RATE IN IDS, AND THE PROPOSED TECHNIQUE IN CASE OF FIXED 1 AND 2 SELECTIVE BLACK HOLES

(a) TP rate and FP rate for one fixed selective black hole.

Pause time (s)	FP rate			TP rate			Time of blocking (s)		
	IDS (5)	IDS (10)	proposed	IDS(5)	IDS(10)	proposed	IDS (5)	IDS (10)	proposed
0	0(0%)	0(0%)	0(0%)	1(100%)	1(100%)	1(100%)	16.54	21.07	4.65
5	0(0%)	0(0%)	0(0%)	1(100%)	1(100%)	1(100%)	20.13	23.09	5.45
10	0(0%)	0(0%)	0(0%)	1(100%)	1(100%)	1(100%)	21.42	23.08	5.07
15	0(0%)	0(0%)	0(0%)	1(100%)	1(100%)	1(100%)	21.23	21.29	5.75

(b): TP rate and FP rate for two fixed selective black hole.

Pause time (s)	FP rate			TP rate			Time of blocking(s)		
	IDS(5)	IDS (10)	proposed	IDS(5)	IDS(10)	proposed	IDS (5)	IDS (10)	proposed
0	0(0%)	0(0%)	0(0%)	2(100%)	2(100%)	2(100%)	20.60	21.39	5.65
5	0.3(0.6%)	0(0%)	0(0%)	2(100%)	2(100%)	2(100%)	21.68	23.06	5.35
10	0(0%)	0(0%)	0(0%)	2(100%)	2(100%)	2(100%)	21.31	22.76	5.6
15	0.2(0.4%)	0(0%)	0(0%)	2(100%)	2(100%)	2(100%)	21.27	23.03	5.76

TABLE III. COMPARING TP RATE FP RATE IN IDS, AND THE PROPOSED TECHNIQUE IN CASE OF RANDOMLY MOVING 1 AND 2 SELECTIVE BLACK HOLES

(a): TP rate and FP rate for one randomly moving selective black hole.

Pause time (s)	FP rate			TP rate			Time of blocking (s)		
	IDS(5)	IDS (10)	proposed	IDS(5)	IDS (10)	proposed	IDS (5)	IDS (10)	proposed
0	0(0%)	0(0%)	0(0%)	1(100%)	1(100%)	1(100%)	21.08	23.19	5.34
5	0(0%)	0(0%)	0(0%)	1(100%)	1(100%)	1(100%)	21.19	21.99	6.14
10	0.2(0.4%)	0(0%)	0(0%)	1(100%)	1(100%)	1(100%)	21.06	21.24	5.21
15	0(0%)	0(0%)	0(0%)	1(100%)	1(100%)	1(100%)	21.19	21.37	5.45

(b): TP rate and FP rate for two randomly moving selective black hole.

Pause time (s)	FP rate			TP rate			Time of blocking (s)		
	IDS(5)	IDS (10)	proposed	IDS(5)	IDS(10)	proposed	IDS (5)	IDS (10)	proposed
0	0.1(0.2%)	0(0%)	0(0%)	2(100%)	2(100%)	2(100%)	21.24	21.23	5.72
5	0.1(0.2%)	0(0%)	0(0%)	2(100%)	2(100%)	2(100%)	21.27	27.7	5.75
10	0(0%)	0(0%)	0(0%)	2(100%)	2(100%)	2(100%)	21.22	23.58	5.48
15	0(0%)	0(0%)	0(0%)	2(100%)	2(100%)	2(100%)	21.17	21.43	5.85

B. Comparison with Hash-Function Technique

In this subsection, the proposed technique is compared with the technique that is introduced in [21]. The technique uses hash function and message authentication to mitigate black hole attack. The simulation parameters are the same parameters that are used in [21]; these parameters are the same parameters which are listed in Table (I) except that the simulation time is 600 s, the pause times are 0s, 100s, 200s, 300s, 400s, 500s, and 600s, the malicious node is one randomly moving black hole, and the traffic rate is 4 packets/second.

Random-way-point model [22] is used to allow nodes to move randomly. Each reading in the figures is obtained as an average of a set of experiments under different scenarios of random motion.

Authors in [21] use three performance measures; packet delivery ratio, time delay, and normalized control packet overhead. They defined Packet Delivery Ratio as the ratio between the number of data packets successfully delivered to the destinations and the total number of data packets in the network. They defined Time Delay as the difference between the time when the source node broadcasts a RREQ message and the time when the first data packet is received by the destination node. They considered that Normalized Control Packet Overhead is the ratio between the size of all the routing packets and the size of all received data packets.

In the following comparisons, the proposed technique is compared with Hash-Function [21] and AODV [7] techniques

In the first comparison, the packet delivery ratio is obtained for different pause times, the comparison results are shown in Fig. 3. It can be shown that the proposed technique gives the highest packet delivery ratio.

The second comparison is carried out to compare the Time Delay; the results are shown in Fig. 4. It can be shown that the proposed technique introduces the lowest time delay. This comparison is not fair to the proposed technique because the delay is considered for the packets that reach the destination and doesn't take into consideration the packets that will be dropped by the black hole. The delay should be related to the delivery ratio which is not considered by [21].

Fig. 5 shows the results of the third comparison in which the Normalized Control Packet Overhead is compared. As shown, the proposed technique gives the lowest normalized control packet overhead which is close to non attacked AODV.

C. The backbone network security and coverage

The simulation parameters that are used in this subsection are the same parameters that are used in the previous subsection. The first experiment is carried out to see if a malicious node can deceive the backbone network and join it as backbone member. The experiment is carried out with number of malicious nodes equals to 20%, 30%, 40%, 50% of the total number of nodes. The results proved that there is no malicious node could join the backbone network.

In the second experiment, the backbone network coverage is tested and the result is illustrated in Fig. 6. As shown from the figure, by using a low percentage of the backbone nodes, the proposed technique gives high coverage percentage.

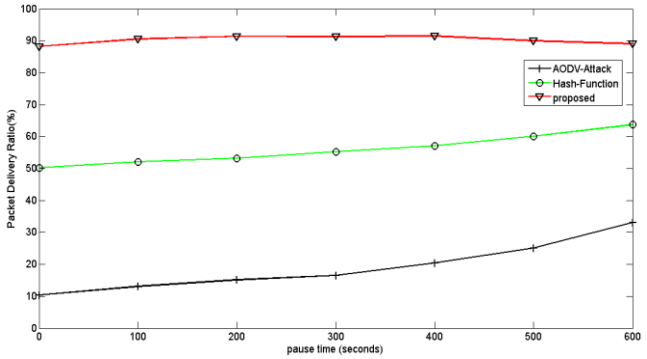


Fig. 3. Total packet delivery ratio for proposed, Hash-Function, and AODV techniques

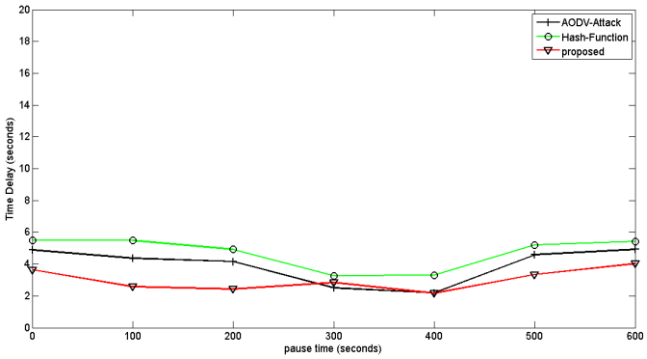


Fig. 4. Time delay for proposed, Hash-Function, and AODV techniques

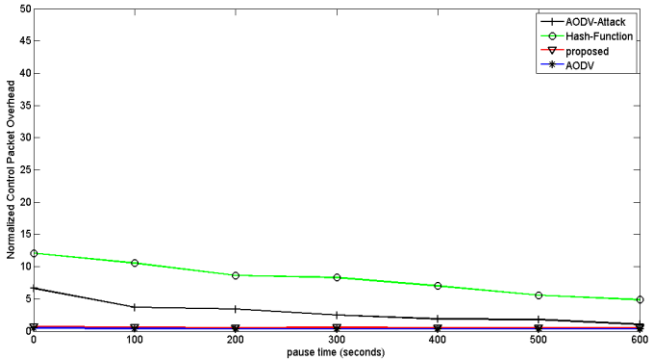


Fig. 5. Normalized Control packet overhead for proposed, Hash-Function, and AODV techniques

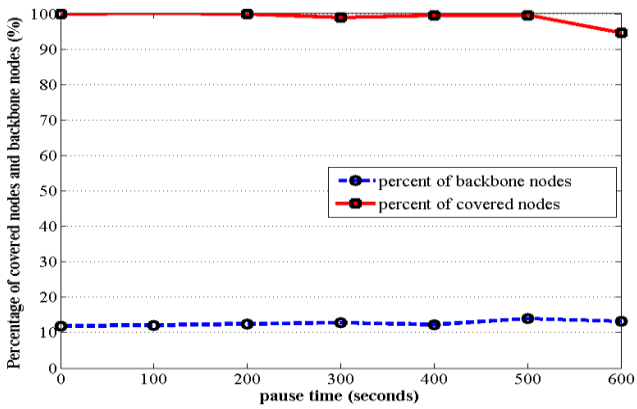


Fig. 6. Backbone network coverage

V. Conclusion

A reliable technique is proposed to detect and prevent black, gray, and cooperative black hole attacks in AODV. The proposed technique uses a multi-level mobile backbone network constructed of randomly moving regular MANET nodes chosen based on their trust value, location and power. The backbone network monitors each other as well as regular nods to estimate monitoring trust value for each node. This value is used as an indicator of malicious behavior. Also, higher level backbone nodes bait the malicious nodes to reply a request for a route to non existing IP. AODV HELLO messages are used to isolate the suspicious node and to exchange the control information. The performance of the proposed technique is compared with AODV, IDS and hash-function techniques. The simulation results show that the backbone network is secure and has high coverage. The proposed technique can highly detect and remove the malicious nodes. It gives the lowest packet loss rate, the lowest end-to-end delay, and the lowest packet overhead.

References

[1] S. Basagni, M. Conti, S. Giordano, and I. Stojmenovic, “Mobile ad hoc networking”, Wiley, 2004.

[2] D. Djenouri, L. Khelladi, and N. Badache, “A survey of security issues in mobile ad hoc networks”, IEEE communications surveys, Vol. 7, No. 4, pp. 2-28, 2005.

[3] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, “A survey of routing attacks in mobile ad hoc networks”, Journal of Wireless communications, IEEE,Vol. 14, No. 5, pp. 85-91, 2007.

[4] N. Badache, D. Djenouri, and A. Derhab, “Mobility impact on mobile ad hoc routing protocols”, ACS/IEEE International Conference on AICCSA, Vol. 3, 2003.

[5] D. Cerri, and A. Ghioni, “Securing AODV: the A-SAODV secure routing prototype”, Communications Magazine, IEEE, Vol. 46, No. 2, pp. 120-125, 2008.

[6] The Network Simulator ns-2, http://www.isi.edu/nsnam/ns/.

[7] C.E. Perkins, E. Beliding-Royer, S. Das, “Ad hoc on-demand distance vector (AODV) routing”, IETF Internet Draft, MANET working group, Jan. 2004.

[8] S. Kamboj, and M. Dua, “Comparison Study of Various DoS Node Detection Schemes in MANETs”, International Journal on Computer Science and Emerging Trends (IJCSET), Vol. 2, No. 1, pp. 8-15, 2013.

[9] S. Jain, J. Singhai, and M. Chawla, “A Review Paper on Cooperative Blackhole And Grayhole Attacks in Mobile Ad hoc Networks”, International Journal of Ad Hoc, Sensor & Ubiquitous Computing, Vol. 2, No. 3, 2011.

[10] L. Tamilselvan, and V. Sankaranarayanan, "Prevention of co-operative black hole attack in MANET", Journal of networks, Vol. 3, No. 5, pp. 13-20, 2008.

[11] M. Su, "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems", Journal of Computer Communications, Elsevier, Vol. 34, No. 1, pp. 107-117, 2011.

[12] H. R. Jhaveri, S. J. Patel, and D. C. Jinwala, "Improving route discovery for aodv to prevent blackhole and grayhole attacks in manets", INFOCOMP Journal of Computer Science, Vol. 11, No. 1, pp. 1-12, 2012.

[13] M. B. Jani, and H. Patel, "Mitigation of Blackhole for AODV (Ad hoc On Demand Distance Vector)", International Journal of Computer Science and Mobile Computing, Vol. 2, No. 5, pp. 338-345, 2013.

[14] P. Agrawal, R. K. Ghosh, and S. K. Das, "Cooperative black and gray hole attacks in mobile ad hoc networks", Proceedings of the ACM 2nd international conference on Ubiquitous information management and communication, pp. 310-314, 2008.

[15] K. Vishnu, and A. J. Paul, "Detection and Removal of Cooperative Black/Gray hole attack in Mobile Ad Hoc Networks", International Journal of Computer Applications, Vol. 1, No. 22, pp. 38-42, 2010.

[16] S. Indrasinghe, R. Pereira, and J. Haggerty, "Conflict free address allocation mechanism for mobile ad hoc networks", In IEEE 21st International Conference, vol. 1, pp. 852-857, 2007.

[17] F. H. Tseng, L. D. Chou, and H. C. Chao, "A survey of black hole attacks in wireless mobile ad hoc networks", Journal of Human-centric Computing and Inf. Sciences, Springer, Vol. 1, No. 1, pp. 1-16, 2011.

[18] R. Agarwal, and D. Motwani, "Survey of clustering algorithms for MANET", International Journal on Computer Science and Engineering , Vol. 1, No. 2, pp. 98-104, 2009.

[19] J. MacQueen, "Some methods for classification and analysis of multivariate observations", fifth Berkeley symposium on mathematical statistics and probability, Vol. 1, No. 281-297, p. 14, 1967.

[20] P. Yi, Z. Dai, Y. P. Zhong, and S. Zhang, "Resisting flooding attacks in ad hoc networks", IEEE International Conference on Information Technology: Coding and Computing (ITCC), Vol. 2, pp. 657-662, 2005.

[21] P. Sachan, and P. M. Khilar, "Authenticated Routing for Ad-Hoc On-Demand Distance Vector Routing Protocol", Advances in Network Security and Applications, Springer, pp. 364-373, 2011.

[22] C. Bettstetter, G. Resta, and P. Santi, "The node distribution of the random waypoint mobility model for wireless ad hoc networks", IEEE Transactions on Mobile Computing, Vol. 2, No. 3, pp. 257-269, 2003.