ISSN 2394-3777 (Print)
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) ISSN 2394-3785 (Online)
Vol. 2, Issue 10, October 2015
Available online at www.ijartet.com

# Efficient Dynamic Source Routing Protocol for MANET's Based on Black Hole attack Prevention

M.Janaki
Joe Suresh Engineering College
Tirunelveli
**tornando66@gmail.com**

***Abstract*—A black hole attack on a MANET refer to an attack by a malicious node, which forcibly acquires the route from a source to a destination by the falsification of sequence number and hop count of the routing message. A selective black hole is a node that can optionally and alternately perform a black hole attack or perform as a normal node. In this paper, several IDS (intrusion detection system) nodes are deployed in MANETs in order to detect and prevent selective black hole attacks. The IDS nodes must be set in sniff mode in order to perform the so-called ABM (Anti-Black hole Mechanism) function, which is mainly used to estimate a suspicious value of a node according to the abnormal difference between the routing messages transmitted from the node. When a suspicious value exceeds a threshold, an IDS nearby will broadcast a block message, informing all nodes on the network, asking them to cooperatively isolate the malicious node. This study employs ns2 to validate the effect of the proposed IDS deployment, as IDS nodes can rapidly block a malicious node, without false positives, if a proper threshold is set.**

## 1. Introduction

In a wireless mobile ad hoc network (MANET), there are no basic network devices, such as routers or access points; data transfer among nodes is realized by means of multiple hops, and rather than just serving as a single terminal, every mobile node acts as a router to establish a route. When a source node intends to transfer data to a destination node, packets are transferred through the intermediate nodes, thus, searching for and quickly establishing a route from a source to a destination node is an important issue for MANETs. The currently available routing protocols are mainly categorized into proactive routing protocols and reactive routing protocols.

In a proactive routing protocol, every node proactively searches for routes to other nodes, and periodically exchanges routing messages, in order to ensure that the information in the routing table is up-to-date and correct, such as DSDV (Destination Sequence Distance Vector)
[1] and OLSR (Optimized Link State Routing Protocol)
[2]. Each node in a MANET is limited to a certain power and bandwidth, thus, continuous transmission of routing messages would lead to congestion of the network. In a reactive routing protocol, a route is searched and established only when two nodes intend to transfer data; and therefore, it is also called an on-demand routing protocol, such as AODV (Ad hoc On-Demand Distance Vector)
[3] or DSR (Dynamic Source Routing) [4]. A source node generally broadcasts a route request message to the entire network by means of fooding, in order to search for and establish a route to the destination node.

The AODV [3] is the most popular routing protocol and has been extensively discussed in research papers; therefore, this study deploys and evaluates the proposed IDSs on AODV-based MANETs. MANETs are generally used for communication during natural disasters, on the battlefield, and a business conference, which illustrates the importance of guaranteed safety of data transfer between two nodes, thus, more secure routing protocols [5-8] have been recently proposed. Most secure routing protocols are designed to prevent hazards to safety properties, such as:
(1) Identity authentication and non-repudiation;
(2) Availability of resources;
(3) Integrality; and
(4) Confidentiality and privacy. By forging a routing message a black hole attack is intended to scramble the route, and then, further eavesdrop or drop the packets, posing a possible threat to safety properties (2),(3),and (4). Due to its easy-to-operate behavior, a black hole attack is common in MANETs, making it very important to efficiently prevent black hole attacks.

A black hole attack can be achieved by a single-node or by several nodes in collusion. A single-node black hole attack forges the sequence number and hop count of a routing message in order to forcibly acquire the route, and then eavesdrop or drop all data packets that pass. Fig. 1 depicts the behavior of a black hole attack, wherein source node S is intended to establish a route to destination node D. In an AODV [3] routing protocol, node S would broadcast a Route Request (RREQ) packet to search for destination node D; the normal intermediate nodes would receive and continuously broadcast the RREQ, rather than the black hole node. As shown in Fig.1 (a), the black hole node would directly reply through an RREP with an extremely large sequence number and hop count of 1 to source node S. When receiving RREQs from normal nodes, the destination node D would also select a route with a minimal hop count, and then, return a Route Reply (RREP) packet, as shown in Fig. 1(b). According to the AODV design, a source node would select the latest (largest sequence number) and shortest route (minimal hop count) to send data packets upon receipt of several RREPs packets. Thus, a route via a black hole node would be selected by node S. The black hole node will then eavesdrop, or directly drop the received data packets, as shown in Fig. 1(c). Moreover, a black hole attack colluded by two malicious nodes, is referred to as a cooperative black hole attack, as shown in Fig. 1(d). The difference of a single malicious node lies in that, after obtaining the route, B1 may select to directly drop the data packets or send to malicious node B2, enabling B2 to eavesdrop or drop the packets. The main purpose of separating the packets dropped by B1 is to reduce the probability of being discovered.

Black hole attacks have serious impact on routing algorithms, which uses sequence numbers to determine whether a message is fresh, and selects the shortest route of minimum hops, such as AODV [3] or DSR [4]. Dokurer et al. [9], revised the AODV routing protocol to reduce

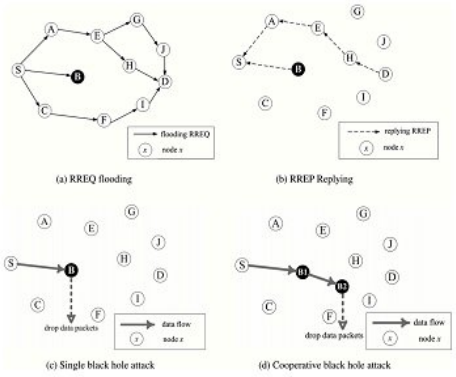



Fig. 1. Diagram of a black hole attack.

opportunities for a black hole node to acquire a route, namely, the source node drops the first returned RREP, or the first two returned RREPs, but selects any subsequent RREP packets, because RREP replies by a black hole node are generally the first or the second one to arrive at the source node, thus, method [9] is very useful to prevent a black hole node being located nearby a source node. Another AODV- based approach proposed by Tamilselvan et al. [10] is as follows; a source node does not immediately send out a data packet upon receipt of the first RREP, but waits in order to collect subsequent RREPs from its neighboring nodes. After comparing all RREPs, the source node selects one (from the neighboring nodes that forward RREPs to the source node), which has the same next hop as other alternative routes (i.e., a node with a distance of 2 from the source node), and begins to send out data packets.

Tamilselvan et al. [11] also proposed a revised AODV routing protocol, called PCBHA (Prevention of a Co-operative Black Hole Attack), in order to prevent cooperative black holes. First, it provides each legal user with a default fidelity level, and after broadcasting a RREQ, a source node waits to receive returned RREPs from the neighboring nodes, and then selects a neighboring node of a higher fidelity level, which exceeds the threshold value, for passing the data packets. The destination node will return an ACK message after receiving data packets, and the source node may add 1 to the fidelity level of the neighboring node, upon receipt of an ACK response. If no ACK response is received, 1 is subtracted from the fidelity level, which indicates a possible black hole node on this route, and data packets are dropped before reaching the destination node.

Kurosawa et al. [12] proposed a dynamic learning method to detect a black hole node. It is required to observe if the characteristic change of a node exceeds the threshold within a period of time. If yes, this node is judged as a black hole node, otherwise, the data of the latest observation is added into dataset for dynamic updating purposes. The characteristics observed in [12] include, the number of sent RREQs, the number of received RREPs, and the mean destination sequence number of the observed RREQs and RREPs. However, [12] it does not involve a detection mode,
such as revising the AODV protocol or deploying IDS nodes, thus, it does not isolate black hole nodes.

Luo et al. [13] added an authentication mechanism into the AODV routing protocol, by combining hash functions, message authentication codes (MAC), and a pseudo random function (PRF) to prevent black hole attacks. Djahel et al. [14] proposed a routing algorithm based on OLSR (Optimized Link State Routing) [2] to prevent the attack of cooperative black holes, by adding two control packets, namely 3 hop_ACK and HELLO rep. Mahmood and Khan [15] also surveyed recent research papers involving black hole attacks on MANETs, and described seven previous methods, and analyzed their advantages and disadvantages.

In this paper, IDS nodes are deployed in MANETs to identify and isolate black hole nodes. An IDS node observes every node's number of broadcasted RREQs, and the number of forwarding RREQs in AODV, in order to judge if any malicious nodes are within its transmission range. Once a black hole node is identified, the IDS node will send a block message through the MANET to isolate the malicious node. The remainder of this paper is organized as follows. Section 2 describes the AODV routing protocol; Section 3 presents the implementation of IDS nodes; Section 4 discusses the experimental data and analysis of ns2; and conclusions are given in Section 5.

## 2. Background

AODV [3] provides a rapid, dynamic network connection, featuring low processing loads and low memory consumption. AODV uses a sequence number to distinguish whether the routing message is fresh. Routing messages in a network can be divided into path discovery and path maintenance messages. The former includes Route Request (RREQ) and Route Reply (RREP), while the latter includes Route Error (RERR) and Hello messages. Since the RREQ and RREP are directly and largely involved in the proposed IDS of this Paper, their formats are shown in Fig. 2(a) and (b), respectively. The formats of RERR and Hello message can be found in [3]. In addition, each node maintains a routing table, the contents of which are updated while receiving a routing message. The fields of the routing table are shown in Fig. 2(c). When a source needs to send data to a destination, but its routing table path to the destination is out of date, or there is no path, then, the source would broadcast a RREQ to all nodes in the network. Each intermediate node receiving a RREQ would first judge whether it is the source, or if such an RREQ is repeated; if yes, this RREQ would be dropped, if no, the RREQ would be processed and re-broadcasted.

In processing the RREQ, an intermediate node first checks if a corresponding reverse route exists in its routing table, if not, the node would create an entry for a reverse route. The purpose of a reverse route is to allow the intermediate node to send a RREP back to the source. If there is a reverse route, the intermediate node checks the content of this entry, and if the destination sequence number in this entry is smaller than the source sequence number in the RREQ (a larger number means newer information), or if the two sequence numbers are the same, but the hop count recorded by the routing table is larger (smaller hop count means shorter path), then, the information in the entry would be replaced by the information in the RREQ. Then, if this intermediate node has a route to the destination, and the route is not expired, then, the intermediate node would return the RREP to the source by the reverse route. However, if the intermediate node does not have a (forward) route to the destination, it will broadcast the RREQ

Fig. 2. Formats of RREQ, RREP, and routing table entry.

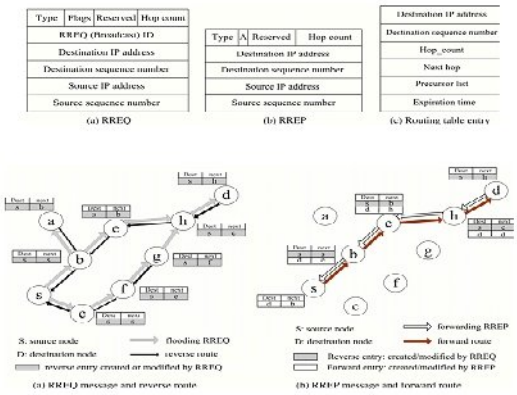



Fig. 3. Path discovery in AODV.

to continue searching a route to the destination node.

An example is shown in Fig. 3(a), where s and d represent the source node and the destination node, respectively, the gray lines represent the tracks of the RREQ, and the black lines represent reverse routes, as reserved in the routing tables of the intermediate nodes. Each node only needs to know the following node, and does not need to know all nodes of the entire route. Taking the node g for example, the following node back to s is node f. Node h would receive two RREQs, transmitted from e and g. In this case, it is assumed that the RREQ from e arrives first; therefore, the RREQ from g, which arrives later, would be immediately dropped. Fig. 3 only shows a portion of the fields in the routing table.

When the destination node, or some intermediate node, which knows a route to the destination, receives an RREQ, it would reply an RREP to the source by a unicast method, rather than the broadcast method, as shown in Fig. 3(b). If the intermediate node receiving the RREP does not have a forward entry in its routing table, it would create a forward entry and store the data of the RREP into the new entry. If there is a forward entry, the destination sequence number in this entry would be compared with that in the RREP. If the latter is larger, then the intermediate node would update this entry according to the RREP, and then send the RREP back to the source via the reverse route, which was created upon the receipt of the RREQ. In Fig. 3(b), the entries with a white background are forward entries. Once the source receives a RREP, it can transmit the data packets to the destination along the forward route.

In AODV, each mobile node would periodically send Hello messages, thus, each node knows which nodes are its neighboring nodes within one-hop. If one node has not received a Hello message from a neighboring node within a certain time, the node would send an RERR message to the nodes recorded in the corresponding precursor list of the routing table, which records a list of the nodes on a route with a disappeared node. The nodes receiving an RERR would remove the compromised route from their routing tables

AODV routing protocol, despite its excellent packet arrival rate, cannot fight the threat of black hole attacks, because during the phase of route searching, malicious nodes may counterfeit a sequence number and hop count in the routing message; thereby, winning an opportunity to acquire the route, eavesdropping or dropping all data packets as they pass.

## 3. The proposed intrusion detection system

All IDS nodes in this study execute a mechanism, called an ABM(Anti-Blackhole Mechanism), which is mainly used to estimate the suspicious value of a node according to the amount of abnormal difference between RREQs and RREPs transmitted from the node. When a suspicious value exceeds the predefined threshold, a block message is broadcast by nearby IDS, giving notice to all nodes on the network to cooperatively isolate the malicious node. The Block message contains the issuing IDS, the identified black hole node, and the time of identification. Upon receipt of a Block message issued by IDS, normal nodes will place the malicious node on their blacklists, thus, the AODV routing protocol for normal nodes must be slightly revised. There are three assumptions in this paper, as follows.

Assumptions:

1. Two neighboring IDS nodes are located within each others transmission range in order to forward Block messages to each other
2. An authentication mechanism exists in MANETs, wherein, a node ID cannot be forged, and a block message, sent by an IDS node, cannot be modified or counterfeited.
3. Every IDS is set in promiscuous mode in order to sniff all routing packets within its transmission range.

Detailed authentication mechanisms in MANETs can be found in [16], thus, this portion will not be addressed in this paper. There are three types of nodes in the network topology of this paper, which separately perform three algorithms, as follows.

- Malicious node: selectively executes the BAODV (Black hole AODV) routing algorithm for black hole attacks.
- Normal node: executes a slightly revised AODV, called MAODV (Modified AODV), to conduct normal routing, and also blocks the malicious nodes in collaboration with IDS node.
- IDS node: executes ABM (Anti-Black hole Mechanism) to detect black hole nodes, and issues a Block message, if necessary.

Generally, a malicious node behaves like a normal node, and conducts normal routing by performing MAODV(modified AODV).In the event of an attack occurrence, the malicious node turns to perform BAODV (Black hole AODV), set RREP with an extremely large sequence number, and 1 hop count in response to RREQ, which makes it possible to quickly acquire the route. When receiving data packets, BAODV will directly drop them, and generate a black hole attack.If a malicious node is detected by IDS, it will broadcast the malicious node's ID, through a Block message, to all nodes within the transmission range. When a normal node receives a Block message the malicious

**Table 1**
Block table.

| IDS node | Malicious node | Time |
|---|---|---|
| IDS_A | 1 | 2009/02/19 12:51 |
| IDS_C | 6 | 2009/02/19 12:55 |

**Table 2**
RQ table and SN table.

| Route | | | Maximal hop count | Broadcasting nodes | Expiration time |
|---|---|---|---|---|---|
| Source | Destination | Src_seq | | | |
| *(a) RQ Table* | | | | | |
| 1 | 6 | 3001 | 2 | 2, 4, 5 | 02:41:12 |
| 3 | 5 | 5012 | 4 | 1, 6 | 02:44:34 |
| Node ID | | | Suspicious value | | status |
| *(b) SN table* | | | | | |
| 3 | | | 1 | | inactive |
| 4 | | | 6 | | active |

```
//When an IDS node sniffs a RREQ transmitted by node N, does the following:
//RQT: RQ Table, RQTE: an entry of RQT

01 search RQT for the entry with (Src, Dest, Src_seq) =
                    (RREQ.src_ip, RREQ.dest_ip, RREQ.src_seq);
02 if the RQTE exists
03      store N to the RQTE.broadcasting_nodes field;
04      if RREQ.hopcount > RQTE.max_hopcount
05          RQTE.max_hopcount ← RREQ.hopcount;
06          RQTE.expiration_time ← RQTE.expiration_time + 3;
07      endif
08 else
09      create a RQTE and store data of the RREQ into the new entry;
10      RQTE.expiration_time ← CURRENT_TIME + 15;
11 endif
12 return;
```

Fig. 4. Procedure of ABM for RREQ.

node's ID is added to the Block table, as listed in Table 1, which lists malicious Node 1 identity, as issued by IDS_A; and malicious Node 6 identity, as issued by IDS_C, as well as their timestamps. Every normal node must authenticate the Block messages from IDSs before updating its own Block table, thus, with the exception of the IDS nodes, nodes cannot broadcast validated Block messages

The implemented routing algorithm of MAODV for normal nodes is basically the same as AODV, with the exception that, intermediate nodes may not reply to RREQs; the difference lies in that:

1) One Block table is added in addition to a routing table, and is used to record a list of malicious nodes;
2) When receiving a Block message broadcasted by IDS, a normal node will add the malicious node stored in the Block message into the Block table;
3) When forwarding a RREP packet, a normal node will drop an RREP if its neighboring node that forwards the RREP is found in the Block table.

Next, the ABM (Anti-Black hole Mechanism) algorithm implemented for IDS nodes is described in detail. ABM employs two tables, which are the RQ and SN tables, as shown in Table 2(a) and (b).

The RQ table records RREQ messages of a watched IDS node within its transmission range, for instance, the first row in Table 2(a) indicates RREQ for (source node, destination node, source sequence) = (1,6,3001), wherein, the IDS has observed that nodes 2,4, and 5 broadcasted this RREQ with a maximal hop count of 2. SN (suspicious node) table, Table 2(b), is used for an IDS node to record the suspicious values of nodes within its transmission range. The suspicious value of a node is an important benchmark to judge a malicious node. In principle, if an intermediate node is not the destination node, and it never broadcasts a RREQ for a specific route, but forwards a RREP for the route, then its suspicious value will be increased by 1 in a nearby IDS's SN table. For instance, the current suspicious value of node 3 in Table 2(b) is 1, which does not exceed the threshold, thus, it is

```
//When an IDS node sniffs a RREP transmitted by node N, does the following:
//S: source node, D: destination node
//RQT:RQ Table, RQTE: an entry of RQT
//RPT:RP Table, RPTE: an entry of RPT
//SNT:SN table, SNTE: an entry of SNT

01 if N is not D
02   search RQT for the entry with (Src, Dest) = (RREP.src_ip, RREP.dest_ip)
03   Case 1: the RQTE does not exist
04        drop the RREP;
05        return;
06   Case 2: the RQTE exists and N is in RQTE.broadcasting_nodes field
07        drop the RREP;
08        return;
09   Case 3: the RQTE exists and N is not in RQTE.broadcasting_nodes field
10        search SNT for the entry with Node_ID = N;
11        if the SNTE exists
12             if SNTE.status = "active";    //already known
13                  drop the RREP;
14             else //SNTE.status = "inactive"
15                  SNTE.suspicious_value++;
16                  if ( SNTE.suspicious_value >= threshold) //a new black hole nod
17                       SNTE.status ← "active";
18                       broadcast a Block message;
19                  endif
20             endif
21        else //the SNTE does not exist
22             create a SNTE and store (N, 1, "inactive") to the new entry;
23        endif
24 endif
25 return;
```

Fig. 5. Procedure of ABM for RREP.

considered as in an "inactive" state; the suspicious value of node 4 is 6, which is assumed as having reached the threshold, thus, it is in an "active" state and blocked.

The procedure for IDS nodes, namely, ABM (Anti-Black hole Mechanism), is described in three parts.

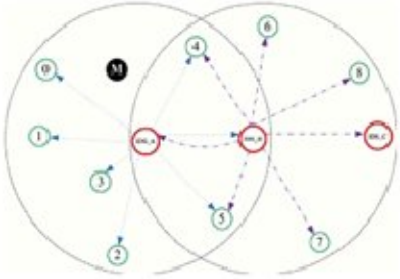
(i)When an IDS sniffs an RREQ: The RQ table is inquired at both ends of the route, as well as the Source sequence number, i.e., (Src node, Dest node, Src_seq), in the RREQ. In case of an absence of this entry, an entry is added; the two ends of the route, Src_seq, hop count, and the ID of the RREQ broadcasting node are copied into the new entry, and Expiration time" is set as the current time + 15 s. The 15 s may be assumed to include the RREQ flooding the entire network to reach the destination node as well as the RREP forwarded back to the intermediate node.

```
//When an IDS node sniffs a RREP transmitted by node N, does the following:
//S: source node, D: destination node
//RQT:RQ Table, RQTE: an entry of RQT
//RPT:RP Table, RPTE: an entry of RPT
//SNT:SN table, SNTE: an entry of SNT

01 if N is not D
02   search RQT for the entry with (Src, Dest) = (RREP.src_ip, RREP.dest_ip)
03   Case 1: the RQTE does not exist
04        drop the RREP;
05        return;
06   Case 2: the RQTE exists and N is in RQTE.broadcasting_nodes field
07        drop the RREP;
08        return;
09   Case 3: the RQTE exists and N is not in RQTE.broadcasting_nodes field
10        search SNT for the entry with Node_ID = N;
11        if the SNTE exists
12            if SNTE.status = "active";    //already known
13                drop the RREP;
14            else //SNTE.status = "inactive"
15                SNTE.suspicious_value++;
16                if ( SNTE.suspicious_value >= threshold) //a new black hole node
17                     SNTE.status ← "active";
18                     broadcast a Block message;
19                endif
20            endif
21        else //the SNTE does not exist
22            create a SNTE and store (N, 1 , "inactive") to the new entry;
23        endif
24 endif
25 return;
```

Fig. 5. Procedure of ABM for RREP.

Fig. 7. Functions of block message.



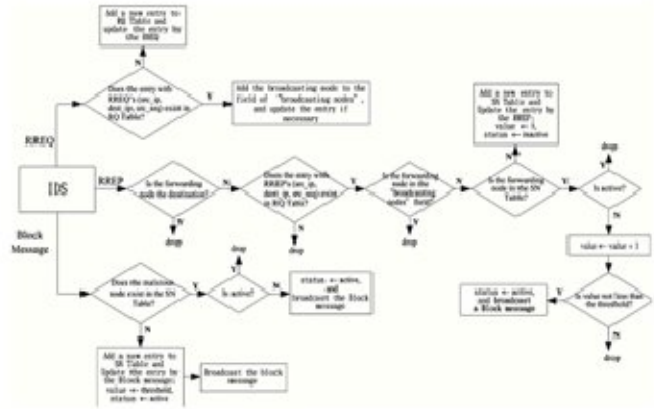



Fig. 8. Flow diagram of ABM (Anti-Blackhole Mechanism).

In cases of the presence of this entry, the ID of the broadcasting node is added into the "Broadcasting nodes" field, and then, judgment to determine whether the hop count in RREQ is greater than Maximal hop count of this entry. If yes, this field value is replaced with the RREQ's hop count, and then, the "Expiration time" is added with 3 s to prolong the lifetime of the entry. The routing protocol itself will, at a preset time interval, clear the outdated entries in RQ table according to the expiration times listed. The algorithm of ABM while sniffing a RREQ is shown in Fig. 4.

(ii) When an IDS sniffs an RREP: Checks if RREP forwarding node is the destination node, if yes, no processing is required; if not, then (Src node, Dest node) in RREP are indexed to inquire of theRQ table in the following three cases.

Case1. If there is no corresponding entry in the RQ able, it indicates the RREP forwarding node is not within the transmission range of the IDS that previously broadcasted the corresponding RREQ. The algorithm stops without subsequent processing.

Case2. If there is corresponding entry in the RQ table, and the "Broadcasting nodes" field contains the ID of a RREP forwarding node; it indicates that this is a reasonable reply to RREQ. The algorithm stops without subsequent processing.

Case3. If there is a corresponding entry in the RQ table, and the "Broadcasting nodes" field does not contain the ID of the RREP forwarding node; it indicates this is not a reasonable RREP reply, thus, it must inquire about the SN table by this RREP forwarding node, by searching the "Node ID" column in Table 2(b),with two possible case results as below.

Case 3.1. This entry exists in the SN table - checks if the status is active. If active (already blocked), it stops with no further handling. Otherwise, the suspicious value of the entry in the SN table is added with 1, and then checks if this value reaches the threshold. If yes, the status is set as active and a Block message is broadcasted.

Case 3.2. This entry does not exist in the SN table - a new entry is added in SN table, and the ID of the RREP forwarding node is entered, the suspicious value is set as 1, and the status is set as inactive.

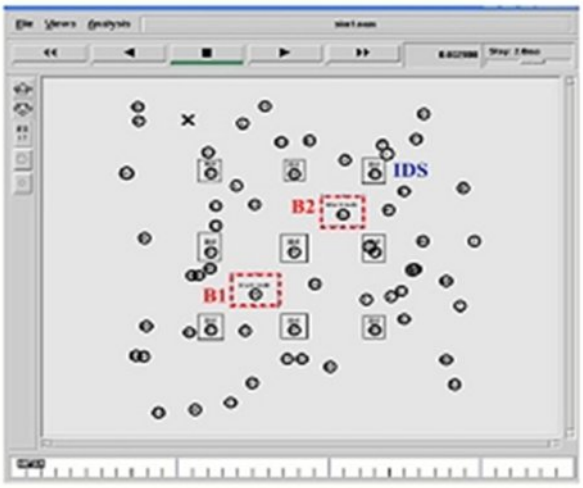
The algorithm of ABM for monitoring a RREP is shown in Fig. 5.

j Communications between IDSs: In aforementioned Case 3.1when the suspicious value of a node is found to have reached the threshold, the detected IDS will broadcast a Block message to notify other normal nodes in its transmission range, in order to update their Block tables (see Table 1). This procedure is shown in Fig. 6(a). Simultaneously, nearby IDSs can hear this Block message, according to Assumption 1. When an IDS node hears a Block message, the following steps are taken. Check if "Node ID" field of SN table has the malicious node ID stored in the Block message. If there is such a node and the status is inactive (a fresh black hole node), change the status to active, and re-broadcast this Block message to notify the normal nodes and nearby IDSs within the transmission range.

When there is such node, and the status is active (a known black hole node), it is dropped without handling, and when there is no such node, create a new entry, store the identified node in the SN table, and set the Suspicious value as the threshold value and the Status as active, and then, re-broadcast this Block message. This procedure is shown in Fig. 6(b).

For example, as shown in Fig. 7, when IDS_A locates malicious node M within its range, it will broadcast a Block message containing the node ID as M, to notify the surrounding nodes 0, 1, 2, 3, 4 and 5 (including malicious node M) to update their Block tables. Simultaneously, the nearby IDS_B also receives this Block message, according to Assumption 1. If this message was not seen before, the IDS_B will re-broadcast to nodes 4, 5, 6, 7, and 8. During broadcasting by IDS_B, both IDS_A and IDS_C will receive the Block message. IDS_A will directly drop it, while IDS_C will continuously re-broadcast.

A complete diagram of ABM (Anti-Black hole Mechanism) is shown in Fig. 8.

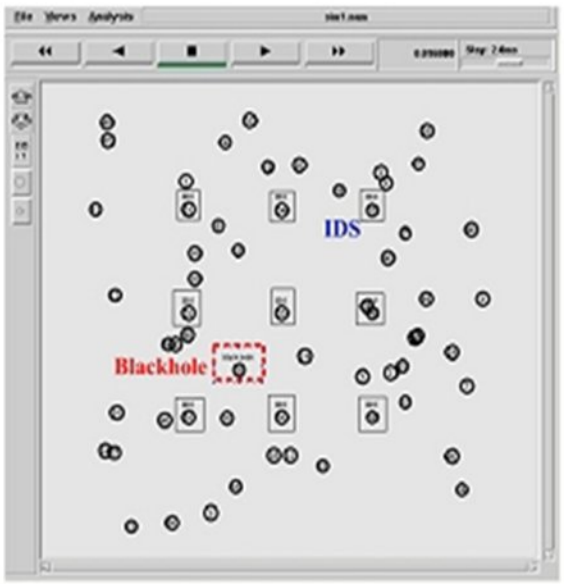



(b) Two black hole nodes (B1 and B2)

Fig. 9. 50 normal nodes and 9 IDS nodes in the simulation.

able 3
Experimental parameters.

| Parameter | Value |
|---|---|
| Coverage area | 1000 m by 1000 m |
| Normal nodes | 50 (random scattered and moved) |
| Malicious node(s) | 1 or 2 (fixed/moved) |
| IDS nodes | 9, 5, 4, 3, 2, or 1 (fixed) |
| Transmission range | 250 m |
| Simulation time | 500 s |
| Mobility | Random-way point model |
| Connections | 20 pairs (40 nodes) |
| Traffic type | UDP, CBR (constant bit rate) |
| Packet size | 512 bytes |
| Maximum speed | 20 m/s |
| Pause time | 0, 5, 10, and 15 s |




(a) One black hole node

## 4. Experimental data and analysis

This paper applied ns2 [17] to validate the detection and isolation efficiency of the proposed IDS against black hole nodes. In an area of 1000 m 1000 m, 50 normal nodes executing the MAODV (Modified AODV) routing protocol were randomly distributed, and a couple of malicious nodes, selectively performing black hole attack, i.e., executing alternatively MAODV or BAODV (Black hole AODV), are randomly located, along with several fixed IDS nodes, which execute ABM (Anti-Black hole Mechanism). Twenty pairs were randomly chosen for data communication, each sending 5 kb UDP-CBR (Constant Bit Rate) per second. All normal nodes were moved in a Random-way point model, with random speeds ranging between 0 and 20 m/s. In addition, four types of pause times of the normal nodes, 0 s, 5 s, 10 s, and 15 s were separately considered. Pause time refers to the time that a moveable node can remain in one place, and then continue moving. For example, in the case of pause time 0, it means all nodes continuously moved, without any temporary stops. Pause time also denotes the frequency of network topology changes. It is first assumed in Section4.1 that, all IDSs nodes can cover most of the simulation area, and then in Section 4.2, IDS nodes are insufficient to cover most of the simulation area. The major parameters of all ns2 experiments are listed in Table 3, and all experimental data in this section refer to an average value, which result from the 10 experiments.

### 4.1. All IDSs can cover most of the simulation area

In a simulated area of 1000 m _ 1000 m, 9 fixed IDS nodes are arranged to cover most of the area, and ensure message transfer can be realized between IDS nodes. In addition to 50 normal nodes distributed and moved randomly (maximum speed is 20 m/s), 1 or 2 black hole nodes in a network topology are considered separately, as shown in Fig. 9(a) and (b), wherein, those with real line frames are IDS

nodes, and those with broken line frames are black hole nodes, and the remaining are normal nodes.

First, it is assumed that black hole nodes are fixed. The total packet loss rates, of one black hole node and two black hole nodes, are as shown in Fig. 10(a) and (b), respectively, and depict the total packet loss rates when the nodes are at different pause times. The total packet loss rates are calculated according to the ratio of missing packets to sent packets; in other words, the number of packets that failed to reach their destinations, to the total number of packets transmitted from all source nodes of the entire network. A MANET may have missing packets due to the mobility of nodes, even without an existing black hole attack. In Fig. 10(a), in the event of the absence of a black hole node, the mean total packet loss rate for all pause times by AODV is about 7.87%; with one black hole node fixed at the position in Fig. 9(a), the rate rises sharply to about 92.40%. With the deployment of the proposed IDS nodes, the rate can be successfully reduced to about 10.05%, with a threshold value set as 5; and about a 13.04% rate, with the threshold set to 10. Fig. 10(b) shows that the mean total packet loss rate for all pause times by AODV is about 7.73%, in the event of an absence of a black hole attack; and about 97.32%, when there are two black hole nodes fixed at the positions shown in Fig. 9(b). With the proposed IDS nodes, the rate can be successfully reduced to about 11.28% (threshold 5) or 14.76% (threshold 10).

It is noted that each dot in Fig. 10 is obtained from an average of 10 experiments, under different random movement scenarios. For every dot in Fig.10(a) and (b), its variance is shown in Fig. 11(a) and (b), respectively. The variance is computed as the average squared deviation of each number from its mean, where l is the mean, and N denotes the number of experiments.

The true positive rate and false positive rate for fixed black hole(s) are listed in Table 4. A true positive (TP) is a 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. The TP rate, computed by #TP/# black hole node in total * 100%, is the ratio of black hole nodes being orrectly judged.

. Similarly, the FP rate, computed by #FP/ # normal node in total * 100%, is the ratio of normal nodes being misjudged. Table 4(a) shows that for one fixed black hole node with the use of a network topology, as shown in Fig. 9(a), it can be successfully detected and blocked in any threshold and pause time settings without false positives. Since there is only one black hole node in the entire network, the TP rate reaches 100% only if the black hole node can be detected and isolated. As shown in Table 4(a), the black hole node is detected and isolated within the first 24 s, during a 500s simulation process. Table4 (b) shows that when two black hole nodes with the use of the network topology, as shown in Fig. 9(b), they can be successfully detected and blocked, with the exception of false positive of 3 nodes in 10 experiments, when the threshold was set as 5, and pause time was 5 (i.e., mean #FP is 0.3, and mean FP rate is 0.3/50=0.6% since there were 50 normal nodes in each experiment). In addition, false positive of 2 nodes existed in 10 experiments, when the threshold was set as 5, and pause time was 15 (i.e., mean #FP is 0.2, and mean FP rate is 0.2/50 = 0.4%). In the case of Table4 (b), the TP rate reaches 100% only if both malicious nodes are detected. Finally, according to Table 4(a) and (b), the influence of the threshold setting directs that, malicious node(s) with a smaller value can be blocked more quickly, but false positives may increase.

Then, the black hole nodes are considered to move randomly at maximum 20 m/s, as normal nodes. As shown in Fig. 12(a), when there is a moveable black hole node, the total packet loss rate is about 86.53%; after deploying IDS nodes, the packet loss rate is reduced to about 10.29%, when anomaly threshold is set to 5, or 12.55% when anomaly threshold is set to10.When there are two moveable black hole nodes, as shown in Fig. 12(b), the total packet loss rate is about 94.64%. With the IDS nodes, the packet loss rate is reduced to about 12.03%, when the anomaly threshold is set to 5, or 14.57% when the anomaly threshold is set to 10.

As shown in Table 5(a), for one black hole node, randomly moving at maximal 20 m/s, as a normal node, the TP rate is still 100%. False positives exist in 2 nodes of the 10 experiments, when the threshold is set as 10 and pause time is 10; with a mean #FP of 0.2, and mean FP rate of 0.4%. No false positives occurred in other parameter settings. If two moveable black hole nodes are considered at the same speed of other normal nodes, the TP rate and FP rate are listed in Table 5(b).

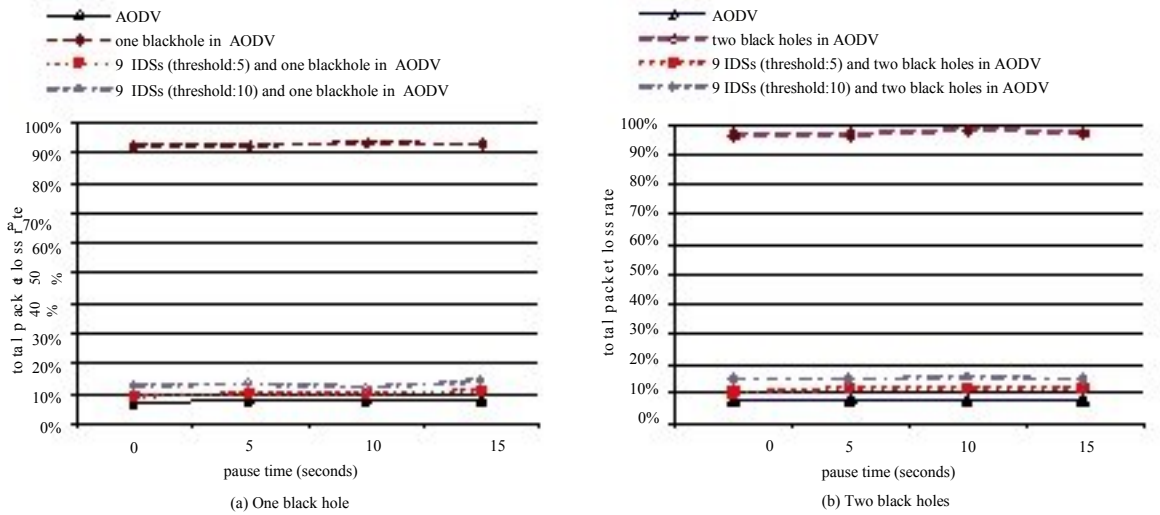



Fig. 10. Total packet loss rates for fixed black hole(s).

### 4.2. All IDSs can only cover part of the simulation area

Nine IDS nodes are arranged in the experiment of Section 4.1,with its coverage occupying 92.23% of the entire simulation area, as shown in Fig. 13(a), thus, excellent preventative effects are obtained.

In this section, 5, 4, 3, 2, or 1 IDS node arranged in the same area is considered, the coverage for the entire simulation area is 64.25%, 48.38%, 41.25%, 30.44%, and 19.63%, respectively, as shown in Fig. 13(b), (c), (d), (e), and (f), respectively.

When there is one black hole node that can move randomly at max. 20 m/s, like normal nodes, the total packet loss rate under different numbers of IDSs, are shown in Fig.14(a), with the anomaly threshold set as 5, or as shown in Fig. 14(b), with anomaly threshold set as 10. On the whole, the growing number of IDS nodes means a lower packet loss rate. For example, the case of a pause time of 10s, as shown in Fig. 14(a). The packet loss rate of AODV itself is 7.93% in the absence of black hole attacks, while the packet loss rate for one moveable black hole is 92.90%.

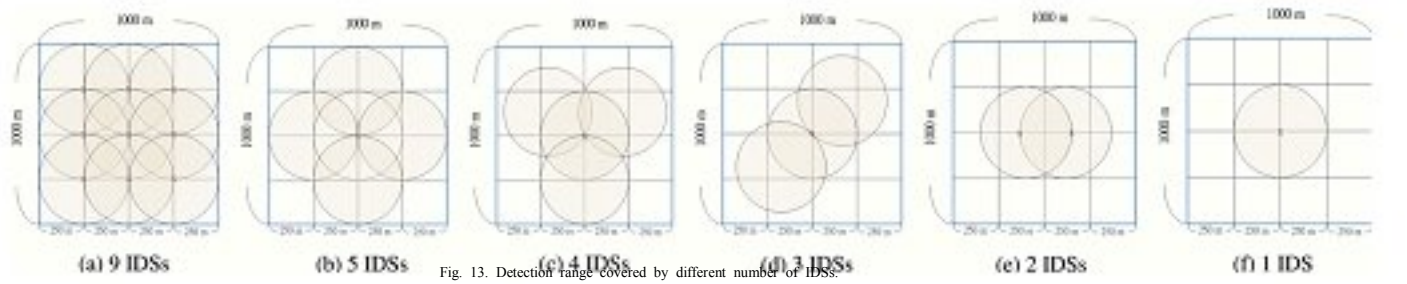
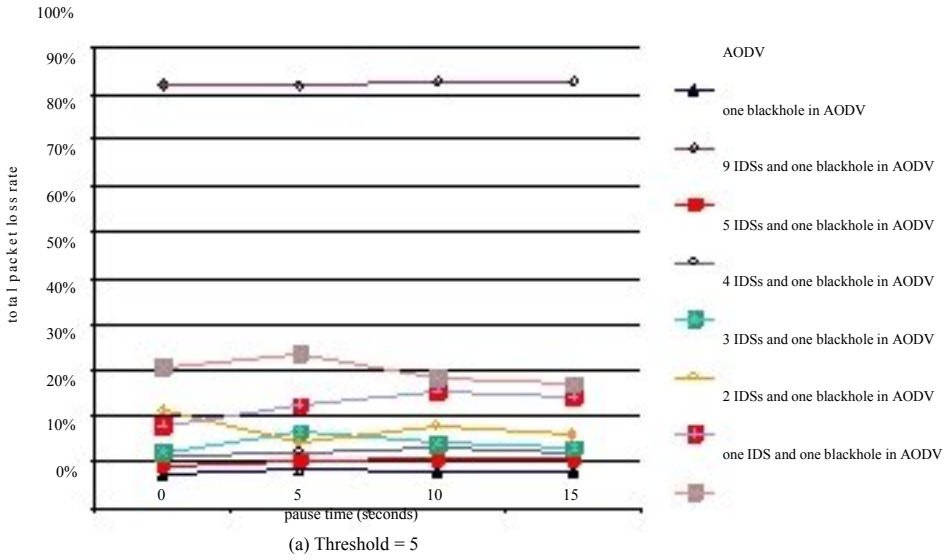
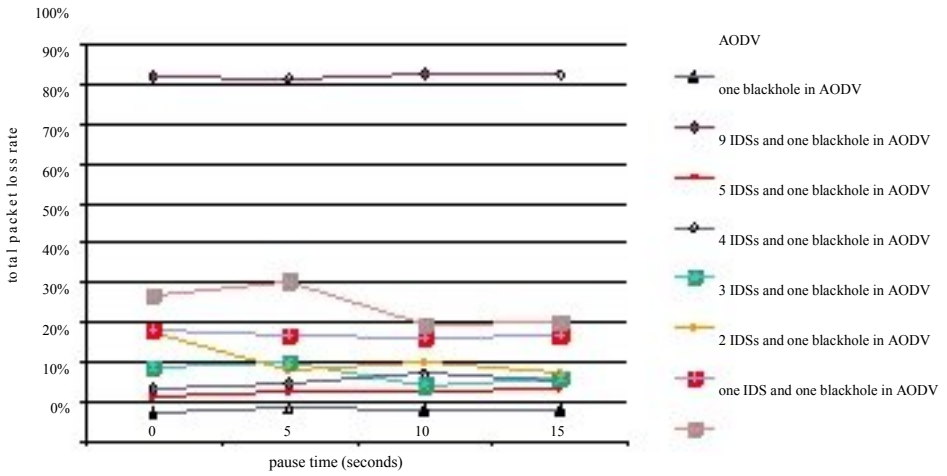



Fig. 13. Detection range covered by different number of IDSs.




(a) Threshold = 5




(a) Threshold = 10

Fig. 14. Packet loss rates for different number of IDSs.

The total packet loss rate will decline gradually with the growing number of IDSs; from 1, 2, 3, 4, 5, to 9 IDS nodes, the packet loss rate is 28.40% 25.66%, 18.00%, 14.11%, 13.13%, and 10.94%, respectively. Even when only one IDS is deployed, the total packet loss rate can be reduced from 92.90% to 28.40%.

## 5. Conclusions

This paper attempts to detect and separate malicious nodes, which selectively perform black hole attacks by deploying IDSs in MANETs (mobile ad hoc networks). All IDS nodes perform an ABM (Anti-Black hole Mechanism), which estimates the suspicious value of a node, according to the amount of abnormal difference between RREQs and RREPs transmitted from the node. With the prerequisite that intermediate nodes are forbidden to reply to RREQs, if an intermediate node, which is not the destination and never broadcasts a RREQ for a specific route, forwards a RREP for the route, then its suspicious value will be increased by 1 in the nearby IDS's SN (suspicious node) table. When the suspicious value of a node exceeds a threshold, a Block message is broadcasted by the detected IDS to all nodes on the network in order to cooperatively isolate the suspicious node. In the ns2 experiments, the total packet loss rate for AODV itself is about 7.8% in the event of an absence of black hole attacks. When there is one fixed (or moveable) black hole node, the total packet loss rate rises sharply to about 92.40% (or 86.53%); for the case of two fixed (or moveable) black hole nodes, the total packet loss rate is about 97.32% (or 94.64%). With the deployment of the proposed IDSs, the total packet loss rate can be greatly improved. For example, the total packet loss rate can be successfully reduced to about 10.05% (threshold set as 5) or 13.04% (threshold set as 10) by using 9 IDSs in order to cover most of the simulation area. In all experiments with 9 IDSs, the detection rate was 100%, and the false positive rate was 0% in most cases. Even if the number of IDS is not enough to cover most of the area, the proposed IDS can perform very well. For example, with only one IDS deployment, the total packet loss rate for one moveable black hole in the MANET can be reduced from 92.90% to 28.40% in the ns2 experiments

## 6. Acknowledgments

This work was partially supported by the National Science Council with contracts NSC 97-2221-E-130-014, 98-2221-E-130-
007, and 99-2628-E-130-003.

## References

[1] Charles E. Perkins, Pravin Bhagwat, Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers, SIGCOMM (1994).

[2] T. Clausen, P. Jacquet, Optimized Link State Routing Protocol (OLSR), IETF RFC 3626, October 2003.

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

[4] D.B. Johnson, D.A. Maltz, Y.-C. Hu, "The Dynamic Source Routing Protocol for Mobile Ad-hoc Network (DSR)," IETF Internet Draft, July 2004.

[5] Manel G. Zapata, N. Asokan, "Securing Ad-hoc Routing Protocols", in: Proc. of the ACM Workshop on Wireless Security (WiSe), 2002.

[6] Kimaya Sanzgiri, Bridget Dahill, Brain Neil Levine, Clay Shields, Elizabeth Belding-Royer, "A Secure Routing Protocol for Ad hoc Networks", in: Proc. of the IEEE International Conference on Network Protocols (ICNP'02), November 2002.

[7] Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", in: Proc. of the ACM Conference on Mobile Computing and Networking (MobiCom), pp. 12-23, 2002.

[8] Panagiotis Papadimitratos, Zygmunt J. Hass, "Secure Routing for Mobile Ad Hoc Networks", in: Proc. of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS),January 2002.

[9] Semih Dokurer, Y.M. Erten, Can Erkin Acar "Performance Analysis of Ad-hoc Networks under Black Hole Attacks", in: Proc. of the IEEE SoutheastCon, pp. 148-153, 2007.

[10] Latha Tamilselvan Dr. V. Sankaranarayanan, 'Prevention of lackhole Attack in ANET", in: Proc. of the International Conference on Wireless Broadband and Ultra Wideband Communication, 2007

[11] Latha Tamilselvan, Dr.V. Sankaranarayanan, Prevention of co-operative black hole attack i MANET, Journal of Networks 3 (5) (2008) 13-20.

[12] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, Yoshiaki Nemoto, Detecting blackhole attack on AODV-based Mobile Ad Hoc Networks by dynamic learning method, International Journal of Network Security 5 (3) (2007) 338-346.

[13] Junhai Luo, Mingyu Fan, Danxia Ye, "Black Hole Attack Prevention Based on Authentication Mechanism", in: Proc. of the IEEE Singapore International Conference on Communication Systems (ICCS), pp. 173-177, 2008.

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

AUTHORS BIOGRAPHY

M.JANAKI, Pursued ME Communication Systems having 7. 67 CGPA in JOE Suresh Engineering College, Tirunelveli, India. In 2012 he graduated in Electronics and communication engineering at Jayaraj Annapackiam CSI College of engineering, India. He had done a project in networks named as “Zigbee based two level surveillance system using Asynchronous sensor networks” in his bachelor degree.


IJARTET