Techniques to Discover Black Hole nodes in Mobile Ad Hoc Networks using AODV Protocol

Ms. Puja
Department of Electronics & Communication Engineering
Amritsar College of Engineering & Technology
Amritsar, India

Dr. V.K Banga
Department of Electronics & Communication Engineering
Amritsar College of Engineering & Technology
Amritsar, India

Tanu Preet Singh
Research Scholar Student,
Uttarakhand Technical University,
Dehradun

Prof. R.K Singh
Professor & OSD
Uttarakhand Technical University
Dehradun, India

Abstract: **A wireless Adhoc network is a collection of mobile nodes with no pre-established infrastructure, forming a temporary network. In the absence of a fixed infrastructure, nodes have to cooperate in order to provide the necessary network functionality. One of the principal routing protocols used in Ad hoc networks is AODV (Ad hoc On-Demand Distance Vector) protocol. The security of the AODV protocol is compromised by a particular type of attack called 'Black Hole' attack [1]. In this attack a malicious node advertises itself as having the shortest path to the node whose packets it wants to intercept. It is proposed to wait and check the replies from all the neighboring nodes to find the Black hole nodes. In this paper, we detect the Black hole nodes or malicious nodes and after detecting it we will remove those nodes and also find the shortest path from source to destination by using GLOMOSIM. We propose that our protocol is increase the throughput, security and life time of the network by reducing the delay than the other conventional AODV protocols.**

Keywords: **- MANETS, black hole attack, malicious node, routing protocols.**

I. INTRODUCTION

An ad hoc network is a collection of nodes that do not rely on a predefined infrastructure to keep the network connected. So the functioning of Ad-hoc networks is dependent on the trust and co-operation between nodes. Nodes help each other in conveying Information about the topology of the network and share the responsibility of managing the network. Hence in addition to acting as hosts, each mobile node. **In Infrastructure less or Ad Hoc wireless network**, the mobile node can move while communicating, there are no fixed base stations and all the nodes in the network act as routers. This type of network can be shown as in fig. 1. Most important networking operations involves Networking.[2].

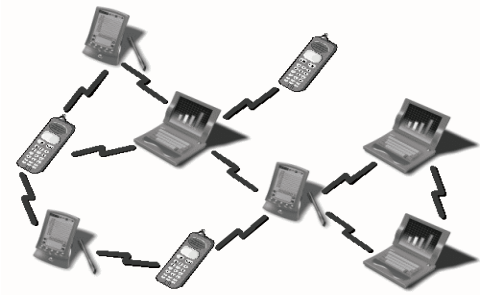


Fig 1: Mobile Ad Hoc Networks

Types of Black Holes

A Black Hole attack [1],[4] is a kind of denial of service attack where a malicious node can attract all packets by falsely claiming a fresh route to the destination and then absorb them without forwarding them to the destination.

Single Black Hole Attack

In single black hole attack only one malicious node attack on the route.

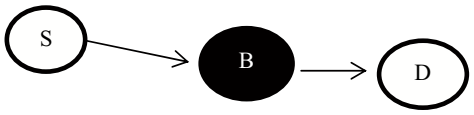


Fig 2: Single Black hole attack

Co-operative Black Hole Attack

Co-operative Black Hole means the malicious nodes act in a group.

Proc. of the Intl. Conf. on Advances in Electronics, Electrical and Computer Science Engineering — EEC 2012
Edited by Dr. R. K. Singh.

ISBN: 978-981-07-2950-9

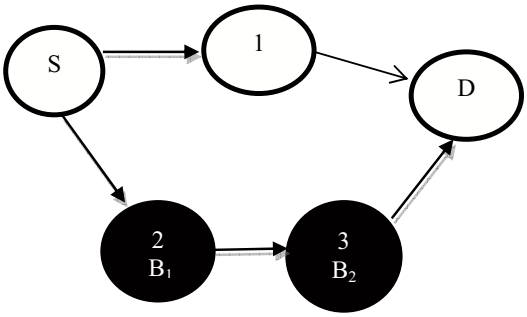


Fig 3: Co-operative Black hole node

Routing protocols can be divided into proactive, reactive and hybrid protocols, depending on the routing topology.

Classification of Routing Protocols

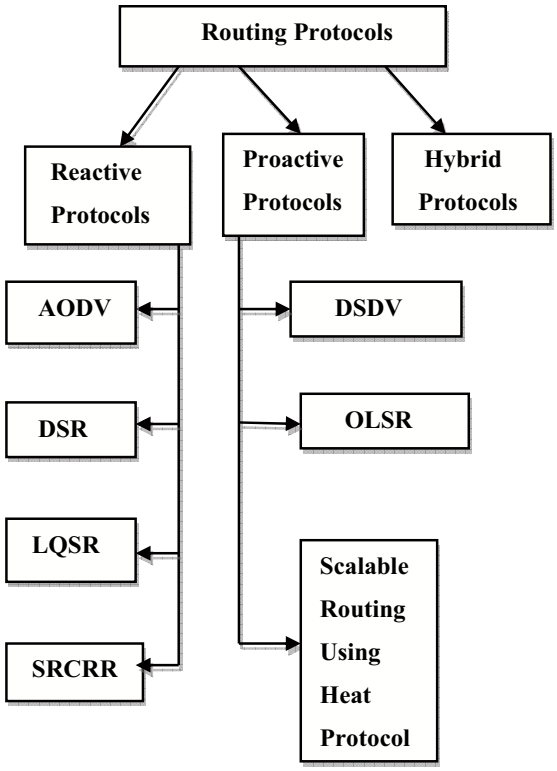


Fig: 4 Classification of Routing protocols

There exists a large number of wireless mesh network routing protocols. They can be broadly classified into three categories as shown in Figure 4. In this study, we focus on two types of protocols: Proactive and Reactive Routing Protocols.

1. Proactive Protocols

Proactive protocols are typically table-driven. Examples of this type include DSDV, WRP. In these types of routing protocols, each node maintains a table of routes to all destination nodes in the network at all times. This requires periodic exchange of control messages between nodes. Since the route to every destination already exists, there is little or no initial delay when first sending data. However, periodic control traffic competes with data transfer to gain access to the channel. The Proactive protocols are classified into Destination Sequence Distance Vector, Optimized Link State Routing, Scalable routing using heat protocols.

a) Destination Sequence Distance Vector (DSDV)

DSDV is a proactive type of routing protocol. DSDV table-driven DV routing scheme for MANET, DSDV based on the Bellman-Ford algorithm with adaptations that are specifically targeted for mobile networks. The Bellman-Ford algorithm uses the distance vector approach, where every node maintains a routing table that records the —next hop for every reachable destination along the shortest route and the minimum distance (number of hops). Whenever there is any change in this minimum distance, the information is reported to neighboring nodes and the tables are updated as required [9] To make this algorithm adequate for mobile ad hoc networks, DSDV added a sequence number with each distance entry to indicate the freshness of that entry. A sequence number is originated at the destination node and is incremented by each node that sends an update to its neighbors. Thus, a newer routing table update for the same destination will have a higher sequence number. Routing table updates are periodically transmitted throughout the network, with each node updating its routing table entries based on the latest sequence number corresponding to that entry. If two updates for the same destination have identical sequence numbers but different distances, then the shorter distance is recorded. The addition of sequence numbers removes the possibility of long-lived loops and also the “counting-to-infinity” problem, where it takes a large number of update message to ascertain that a node is not reachable [9].

b) Optimized Link State Routing(OLSR)

OLSR protocol is a proactive routing protocol. The Optimized Link State Routing (OLSR) protocol was first introduced in [10]. The current OLSR Version 11 is the definitive RFC 3626. It provides optimization of a pure link state algorithm tailored to the requirements of a mobile wireless LAN (OLSR protocol optimized for MANET but can also be used in WMNs). The

concept used in the protocol is that of multipoint relays (MPRs). MPRs are selected nodes which forward broadcast messages during the flooding process. This technique provides two key optimizations [10]. First, it reduces the size of the control packets, that is, instead of all links, it declares only a subset of neighbouring links designated as the MPRs. Secondly, flooding of the control traffic is minimized by using only the selected nodes to propagate its messages in the network. Only the MPRs of a node retransmit its broadcast messages. Such procedures substantially reduce the message overhead as compared to pure flooding mechanisms where every node re-transmits each message when it receives the first copy of the packet.

2. Reactive Protocols

Reactive or source-initiated on-demand protocols, in contrary, do not periodically update the routing information. It is propagated to the nodes only when necessary. Example of this type includes DSR, AODV and ABR. In reactive routing protocols, the route is calculated only when a node needs to send data to an unknown destination. Thus, route discovery is initiated only when needed. This saves overhead in maintaining unused routes. However, this may lead to larger initial delays. During route discovery, the query is flooded into the entire network and the reply from the destination (or intermediate nodes) sets up the path between the source and destination. The Reactive protocols are classified into Ad-hoc on Demand Distance Vector, Dynamic Source Routing, SRCRR, Link Quality Source Routing, and Multi radio Link Quality Source Routing.

a) Dynamic Source Routing Protocol

Dynamic Source Routing (DSR) is a routing protocol for wireless mesh networks. It is similar to AODV in that it establishes a route on-demand when a transmitting mobile node requests one. However, it uses source routing instead of relying on the routing table at each intermediate device. Dynamic source routing protocol (DSR) is an on-demand, source routing protocol, whereby all the routing information is maintained (continually updated) at mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration. The protocol is composed of the two main mechanisms of "Route Discovery "which work together to allow nodes to discover and maintain routes to arbitrary destinations in the ad hoc network. An optimum path for a communication between a source node and target node is determined by Route Discovery process. Route Maintenance ensures that the communication path remains optimum and loop-free according the change in network conditions, even if this requires altering the route during a transmission. Route Reply would only be generated if the message has reached the projected destination node (route record which is firstly contained in Route Request would be inserted into the Route Reply).To return the Route Reply, the destination node must have a route to the source node. If the route is in the route cache of target node,
the route would be used. Otherwise, the node will reverse the route based on the route record in the Route Reply message header (symmetric links). In the event of fatal transmission, the Route Maintenance Phase is initiated whereby the Route Error packets are generated at a node. The incorrect hop will be detached from the node's route cache; all routes containing the hop are reduced at that point. Again, the Route Discovery Phase is initiated to determine the most viable route.The major dissimilarity between this and the other on-demand routing protocols is that it is beacon-less and hence it does not have need of periodic hello packet (beacon) transmissions, which are used by a node to inform its neighbors of its presence. The fundamental approach of this protocol during the route creation phase is to launch a route by flooding Route Request packets in the network. The destination node, on getting a Route Request packet, responds by transferring a Route Reply packet back to the source, which carries the route traversed by the Route Request packet received.

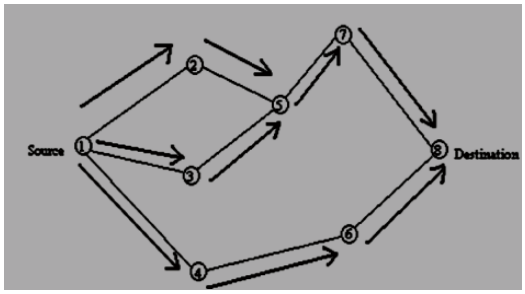


Fig 5: Propagation of Request (PREQ) packet

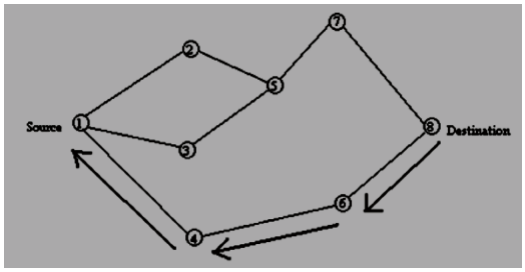


Fig 6: Creation of Route in DSR

A destination node, after receiving the first Route Request packet, replies to the source node through the reverse path the Route Request packet had traversed. Nodes can also be trained about the neighboring routes traversed by data packets if operated in the promiscuous mode. This route cache is also used during the route construction phase. If an intermediary node receiving a Route Request has a route to the destination node in its route cache, then it replies to the source node by sending a Route Reply with the entire route information from the source node to the destination node.

b) Ad Hoc On-Demand Distance routing Protocol (ADOV)

The Ad Hoc On-Demand Distance Vector (AODV) routing protocol is an adaptation of the DSDV protocol for dynamic link conditions [5][6][7]. Every node in an Ad-hoc network maintains a routing table, which contains information about the route to a particular destination. Whenever a packet is to be sent by a node, it first checks with its routing table to determine whether a route to the destination is already available. If so, it uses that route to send the packets to the destination. If a route is not available or the previously entered route is inactivated, then the node initiates a route discovery process. A
RREQ (Route REQuest) packet is broadcasted by the node. Every node that receives the RREQ packet first checks if it is the destination for that packet and if so, it sends back an RREP (Route Reply) packet. If it is not the destination, then it checks with its routing table to determine if it has got a route to the destination. If not, it relays the RREQ packet by broadcasting it to its neighbors. If its routing table does contain an entry to the destination, then the next step is the comparison of the 'Destination Sequence' number in its routing table to that present in the RREQ packet. This Destination Sequence number is the sequence number of the last sent packet from the destination to the source. If the destination sequence number present in the routing table is lesser than or equal to the one contained in the RREQ packet, then the node relays the request further to its neighbors. If the number in the routing table is higher than the number in the packet, it denotes that the route is a 'fresh route' and packets can be sent through this route. This intermediate node then sends a RREP packet to the node through which it received the RREQ packet. The RREP packet gets relayed back to the source through the reverse route. The source node then updates its routing table and sends its packet through this route. During the operation, if any node identifies a link failure it sends a RERR (Route ERRor) packet to all other nodes that uses this link for their communication to other nodes. In the following illustrated figure 7, imagine a malicious node 'M'. When node 'A' broadcasts a RREQ packet, nodes 'B' 'D'and'M' receive it. Node'M', being a malicious node, does not check up with its routing table for the requested route to node 'E'.Hence, it immediately sends back a RREP packet, claiming a route to the destination. Node 'A' receives the RREP from 'M' ahead of the RREP from 'B' and 'D'. Since AODV has no security mechanisms, malicious nodes can perform many attacks just by not behaving according to the AODV rules. A malicious node *M* can carry out many attacks against AODV.This Solutions provides routing security to the AODV routing protocol by eliminating the threat of 'Black Hole' attacks

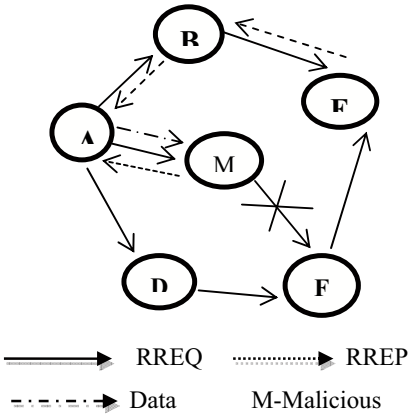


Fig 7: Black hole Attack in ADOV

A Comparison of the Characterstics of the Adhoc routing protocols is given in Table.1

Table:1 Adhoc Network Protocol Comparisons

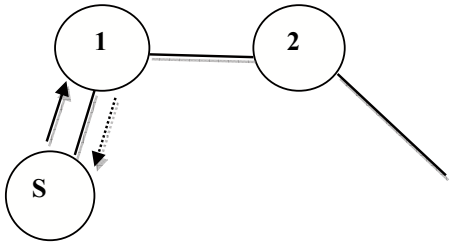
Protocol Property	DSR	DSDV	AODV
Loop free	Yes	Yes	Yes
Multicast	Yes	No	No
Distributed	Yes	Yes	Yes
Unidirectional Link Support	Yes	No	No
Multicast	No	No	Yes
Periodic Broadcast	No	Yes	Yes
QoS Support	No	No	No
Route Maintained in	Route Cache	Route Table	Route Table
Reactive	yes	No	Yes

II. TECHNIQUES TO DISCOVER BLACK HOLES

2.1. Solution to Black Hole Attack (SAODV)

According to this proposed solution the requesting node without sending the DATA packets to the reply node at once, it has to wait till other replies with next hop details from the other neighboring nodes. After receiving the first request it sets timer in the 'TimerExpiredTable', for collecting the further requests from different nodes. It will store the 'sequence number', and the time at which the packet arrives, in a 'Collect Route Reply Table' (CRRT). The time for which every node will wait is proportional to its distance from the source. It calculates the'time out'value based on arriving time of the first route request. After the timeout value, it first checks in CRRT whether there is any repeated next hop node. If any repeated next hop node is present in the reply paths it assumes the paths are correct or the chance of malicious paths is limited.

Then it chooses any one of the paths with the repeated node to transmit the DATA packets. If there is no repetition select random route from CRRT. Here again the chance of malicious route selected is reduced .The proposed solution is illustrated in figure 8.



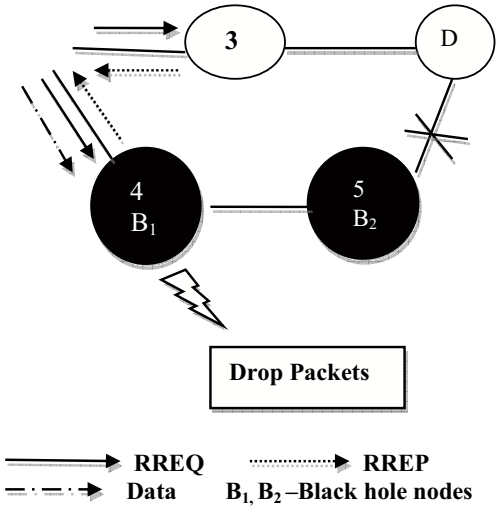


Fig 8: Co-operative Black hole nodes Attack

2.2 SIMULATION RESULTS

A. Metrics

The simulation is done using GloMoSim (Global Mobile Simulator) [11][12], to analyze the performance of the network by varying the nodes mobility. The metrics used to evaluate the performance.

B. Simulation Profile

Property	Value
Nodes	25
Simulation Time	5M
Mobility	Random way point model speed– 30 m/s pause time – Node mobility varied between 10 S to 90 S
Load	300 items, Data pay loads 512 Bytes. Interdeparture time of 1S.
Coverage Area	800 m by 800 m

Table 2.Simulation Profile

C. Comparison with basic AODV

To evaluate the packet delivery ratio, simulation is done with 25 nodes with the source node transmitting 300 packets to the destination node. Each packet is of 512 bytes and is transmitted with an interval of 1 second. As it can be seen from the fig 9, with SAODV the packet delivery ratio is more compared to AODV. Node mobility indicates the mobility speed of nodes.

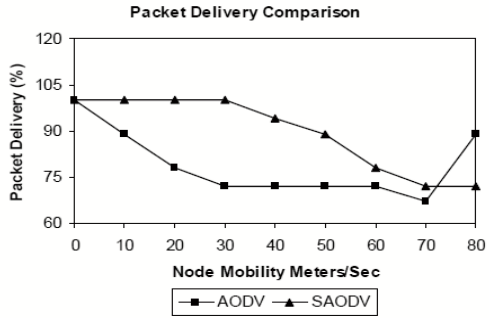


Fig 9: Packet Delivery (%)

Fig 10 shows the packet delivery ratio in the presence of malicious node. Consider Source 1 sends packet to Destination 5. Here assume 2 is the malicious node. In AODV the packet delivery ratio is reduced to 30%. But in SAODV the packet delivery ratio is around 90 to 100%.

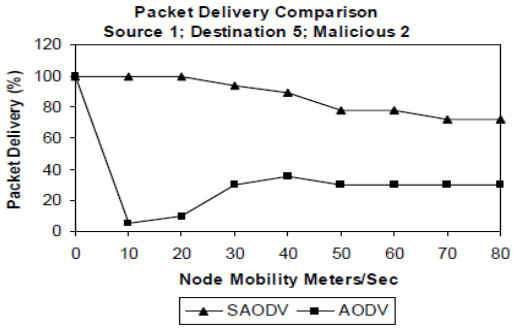


Fig: 10 Packet Delivery (%) in presence of malicious node near the source node

Figure-11 shows the packet delivery ratio in the presence of malicious node away from the source. In AODV the packet delivery ratio is increased to around 80%.

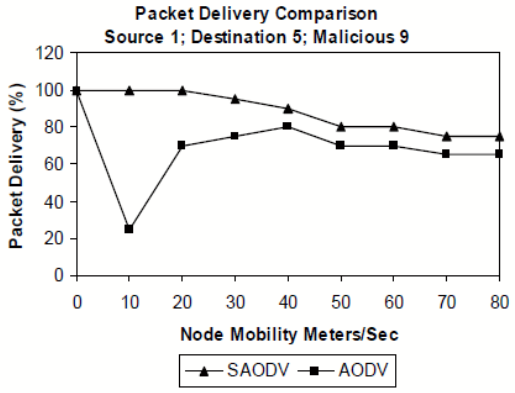


Fig: 11 Packet delivery (%) in presence of malicious node away from source node

This is because before the reply from the malicious reaches the source, nearby node to the source transmits the reply. Again in SAODV the packet delivery ratio is around 90 to 100%. From the figure-12 it can be observed that, when SAODV protocol is used there is increase in the average end-to-end delay, compared to AODV. From the figure-13 &14 it can be observed that, when SAODV protocol is used there is only slight increase in the average end-to-end delay, compared to AODV.

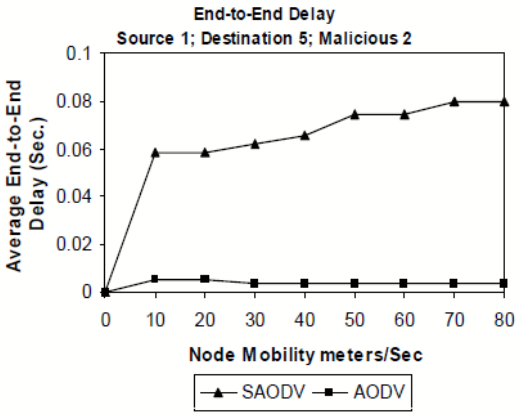


Fig: 12 End to End Delay

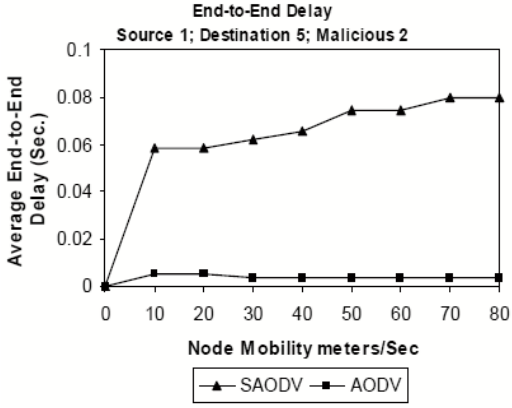


Fig: 13 End-to-End delay in presence of malicious node near the source node

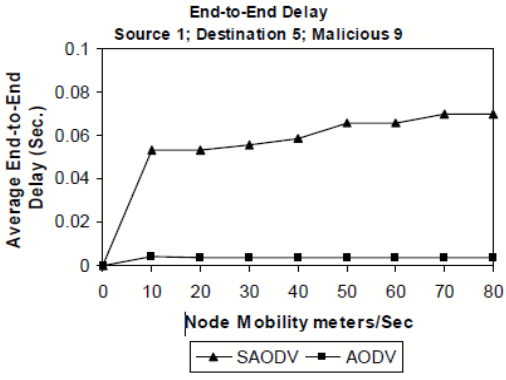


Fig: 14 End to End delay in presence of Malicious node away from source node

Figure-15 shows the routing overhead. To evaluate the routing overhead. As it can be seen from the figure11, with SAODV the routing overhead is slightly more compared to AODV. This is due to

the additional process involved to avoid the selection of malicious node.

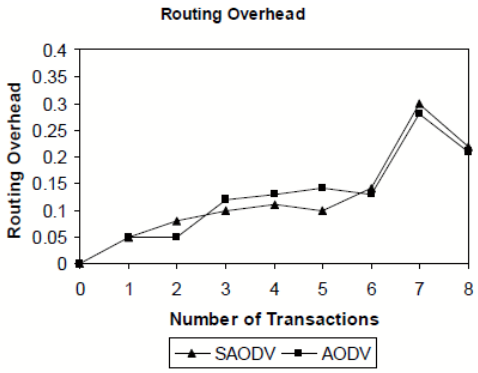


Fig: 15 Routing overhead

III. THE **PROPOSED INTRUSION DETECTION SYSTEM (PIDS)**

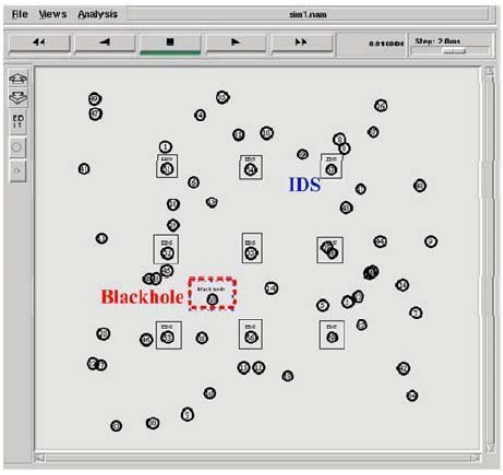
In this study, every IDS node executes a mechanism, called an ABM (Anti-Black hole Mechanism), which is mainly used to estimate the suspicious value of a node according to the amount of abnormal difference between RREQs and RREPs transmitted from the node. When a suspicious value exceeds a threshold, a block message is broadcasted 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, (1).Detaile authentication mechanisms in MANETs can be found in [8], thus, this portion will not be addressed in this paper. 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 node's ID is added to the Block table, as listed in Table 1, which lists malicious Node 2 identity, as issued by IDS_A; and malicious Node 5 identity, as issued by IDS_B, 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.

IDS	Malicious Node	Time stamp
IDS_A	2	22:26
IDS_B	5	22:59

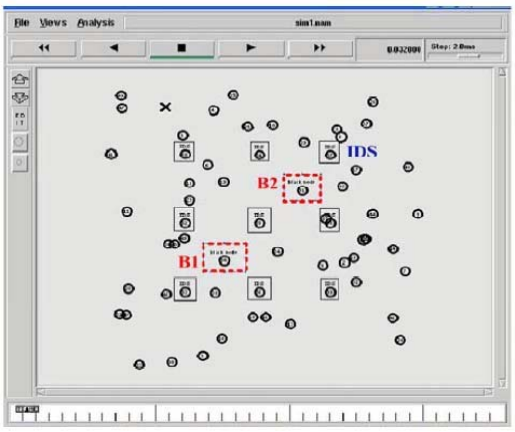
Table 3: Block table

3.1 Experimental Data and Analysis

This paper applied ns2 [13] to validate the detection and isolation efficiency of the proposed IDS against black hole nodes. In an area of 1000m × 1000m, 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). All experimental data in this section refer to an average value, which result from the 10 experiments. In a simulated area of 1000m × 1000m, 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 20m/s), 1 or 2 black hole nodes in a network topology are considered separately, as shown in Figure 16(a) and 16(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.



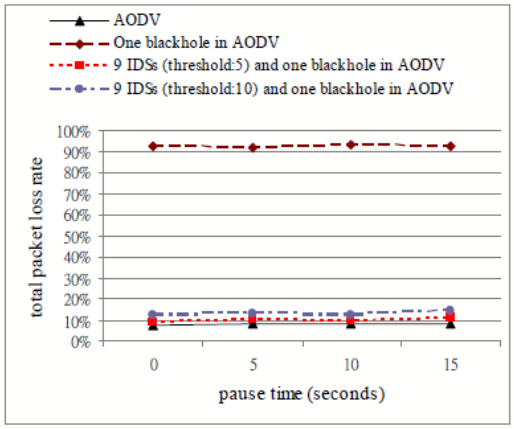
(a) One Black Hole node



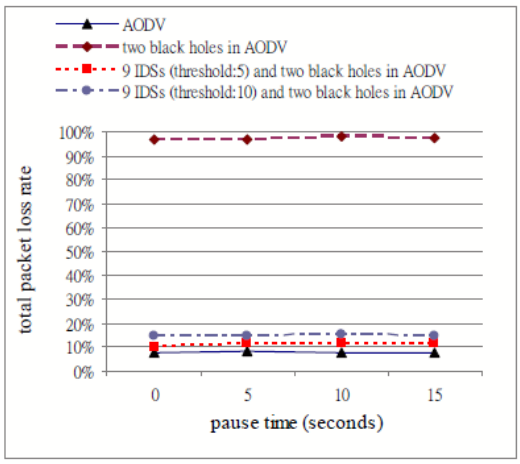
(b) Two Black Hole nodes

Fig: 16 50 normal nodes and 9 IDS nodes in the Simulation

In Figure 17(a), in the event of the absence of a black hole node, the total packet loss rate in AODV is about 7.87%; with one black hole node fixed at the position in Figure 16(a), the total packet loss rate rises sharply to about 92.40%.With the deployment of the proposed IDS nodes, the packet loss rate can be successfully reduced to about 10.05%, with the threshold set to 5, or 13.04% with the threshold set to 10. Figure 17(b) shows that the total packet loss rate in AODV is about 7.73%, in the event of absence of a black hole attack, and about 97.32%, when there are two black hole nodes fixed at the positions shown in Figure 16(b). With the proposed IDS nodes, the total packet loss rate can be successfully reduced to about 11.28% (threshold 5) or 14.76% (threshold 10).



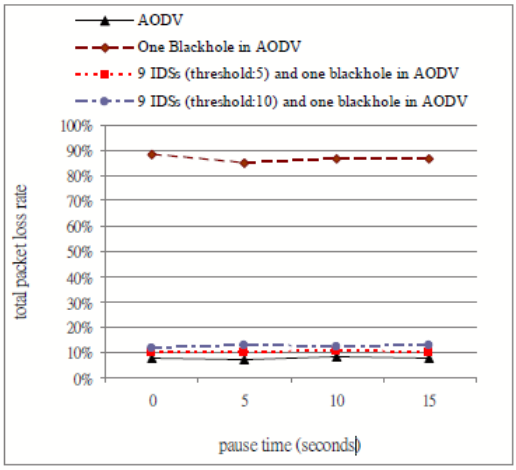
(a) One Black Hole



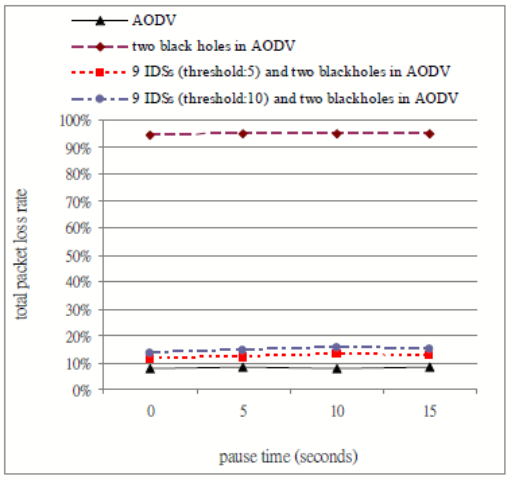
(b) Two Black Hole nodes

Fig: 17 Total packet loss rates for fixed black node (s)

Then, the black hole nodes are considered to move randomly at maximum 20m/s, as normal nodes. As shown in Figure 18(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 to 10. When there are two moveable black hole nodes, as shown in Figure 18(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.



(a) One Black hole



(b) Two black holes

Fig:18 Total packet loss rates for randomly moved black hole(s)

IV. CONCLUSION AND FUTURE SCOPE

As already mentioned in the previous papers, the solutions has been proposed by using various techniques to attempt to detect the single black hole and co-operative black hole nodes. After detecting these black hole nodes, the data packets had not being send through this route(i.e. to avoid black hole nodes).To reduce the probability it was proposed to wait and check the replies from all the neighboring nodes to find a safe route. We propose a solution that is enhancement of all the proposed solutions. We will implement the modified AODV routing protocol in order to detect the black hole nodes and after detecting it we will remove those nodes and also find the shortest path from source to destination. By doing this we will be able to improve the throughput, end to end delay and packet delivery ration of the network thus it increases the lifetime of the network structure.

REFERENCES

[1] Hongmei Deng,Wei Li,and Dharma P.Agrawal, "Routing Security in Wireless Adhoc Networks", University of Cincinnati,IEEE Communications magazins, October 2002.

[2] V.Karpijoki, "Security in Ad Hoc Networks", Seminar on Net Work Security, HUT TML 2000.

[3] Lidong zhou Zygmunt J. Haas. "Securing Ad Hoc Networks", IEEE networks, special issue on network security, Vol.13,no.6,November/December 1999.

[4] Yi-Chun,Adrian Perrig, "A Survey of Secure Wireless Ad Hoc Routing",IEEE Security and Privacy,1540-7993/04/$20.00 2004 E.May/June 2004.

[5] C.E. Perkins, S.R Das, and E.Royer, "Ad-Hoc on Demand Distance Vector (AODV)",March 2000, http:/www.ietf.org internet-drafts/draft-ietf-manet-05.txt

[6]Yi-Chun,Adrian Perrig,David B.johnson, "Ariadna: A secure On-Demand Routing Protocol for Ad Hoc Networks", sparrow.ece.cmu.edu/~adrian/Projects/secure-routing/ariadne.pdf,2002.

[7] Charles E.Perkins, Elizabeth M.Belding-Royer,Samir R.Das, Mobile Ad Hoc Networking Working Group, Internet Drafts, February 2003.

[8] Kimaya Sanzgiri,Daniel LaFlamme,Bridget Dahill, Brian Neil Levine, Clay Shields,and Elizabeth M.Belding-Royer,rAutenticated Routing for Adhoc Networks," IEEE journal on Selected Areas in Communications,Vol.23 No.3,pp.598-610, 2005.

[9]http:/web2.blogtells.com/2008/09/17/ Proactive-routing-protocols-destination-sequenced-distance/

[10]P.jacquet,P.Muhlethaler,T.Clausen, A. Laouiti, A.Qayyum and L. Viennot, "OLSR Protocol for Ad Hoc Networks", IEEE INMIC, pp.62-68, Dec 2001, last accessed on Oct 2005.

[11]Jorge Nuevo, "A Comprehensible GloMosim Tutorial" INRS-universitedu Quebec.nuevo@inrstelecom.uquebec.ca. March4,2004.Abstract www.sm.luth.se/csee/courses/smd/161_wireless/glomoman.pdf

[12]Tony Larson, "Nickles Hedman, "Routing Protocols in Wireless Ad-hoc Networks- A Simulation Study", Masters thesis in computer science and engineering, Lulia University of Technology, Stockholm, 1998.

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