Broadcast ID based Detection and Correction of Black Hole in MANETs

Pooja Vij
Assistant Professor, Dept. of ECE
Amritsar College of Engineering & Technology, Amritsar,
Punjab-India-143001

V.K Banga, PhD.
Professor & HOD, Dept. of ECE
Amritsar College of Engineering & Technology, Amritsar,
Punjab-India-143001

Tanu Preet Singh
Associate Professor, Dept. of CSE
Amritsar College of Engineering & Technology, Amritsar,
Punjab-India-143001

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 research paper, we have detect the black hole node or unauthorized node on the based of broadcast ID. Firstly, to determine and propose routing algorithm for detection and correction of black hole in AODV.Secondly to implement this along on NS2 and analyze the result. Thirdly to obtain the comparison of the following parameters like End to End delay, Routing overheads and Packet delivery with the already proposed protocols. By doing this our proposed algorithm shows better performance than the conventional AODV.

Keywords

Routing protocol, Ad hoc Networks, AODV, Black Hole Attack, Broadcast ID

1. 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 include routing and network management [1].

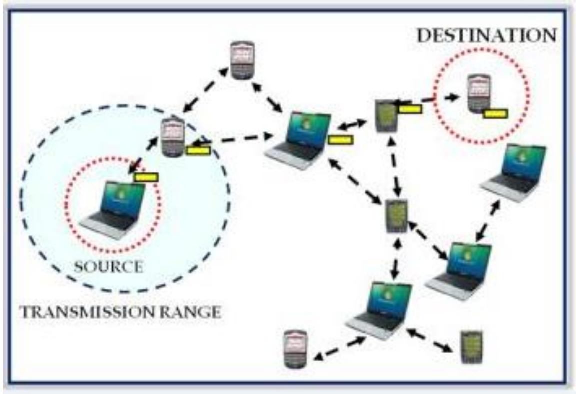


Fig 1: Mobile Adhoc Network

Routing protocols can be divided into proactive, reactive and hybrid protocols, depending on the routing topology. Proactive protocols are typically table driven. 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. Examples of this type include DSDV, WRP. 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. Hybrid protocols make use of both reactive and proactive approaches. Example of this type includes TORA, ZRP. Security is a major concern in all forms of communication networks, but ad hoc networks face the greatest challenge due to their inherent nature. As a result, there exist a slew of attacks that can be performed on an Ad hoc network. [2][3].

1.1 AODV Routing Protocols

1.1.1. The AODV protocol

The Ad Hoc On-Demand Distance Vector (AODV)

routing protocol is an adaptation of the DSDV protocol for dynamic link conditions [4][5]. 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. This is illustrated in figure 1.

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 AOD

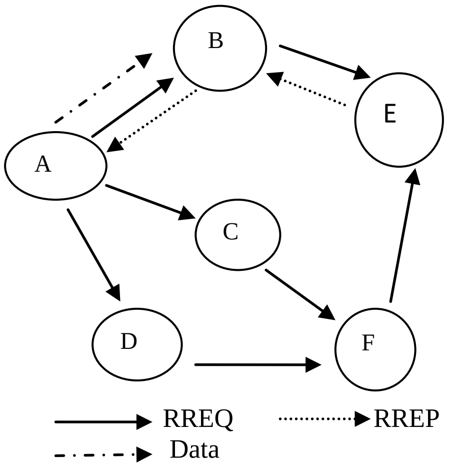


Fig:2 Propagation of RREQ & RREP from A to E

1.1.2. Black Hole Attack

A Black Hole attack [2],[6] 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

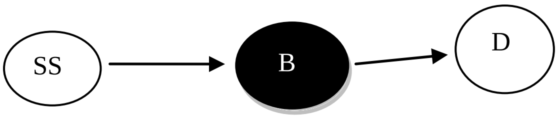


Fig 3: Single Black hole attack

Co-operative Black Hole Attack

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

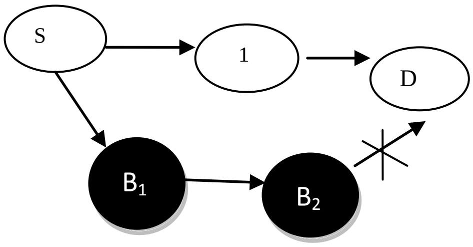


Fig 4: Co-operative Black hole node

When the source node wishes to transmit a data packet to the destination, it first sends out the RREQ packet to the neighboring nodes. The malicious nodes being part of the network, also receive the RREQ. Since the Black hole nodes have the characteristic of responding first to any RREQ, it immediately sends out the RREP. The RREP from the Black hole B1 reaches the source node, well ahead of the other RREPs, as it can be seen from the figure 2. Now on receiving the RREP from B1, the source starts transmitting the data packets. On the receipt of data packets, B1 simply drops them, instead of forwarding to the destination or B1 forwards all the data to B2. B2simply drops it instead of forwarding to the destination. Thus the data packets get lost and hence never reach the intended destination.

1.2. Related Work

Recently, a lot of research has focused on the security issue in MANET. Several related issues are briefly presented here. Researchers have proposed solutions to identify and eliminate a single black hole node [7]. 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 'timeout' 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. If there is no repetition select random route from CRRT.But again there is chance of malicious node. In paper [8] the proposed solution constructs different reputation properties and misbehaving reaction better suiting to AODV. 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. To reduce the probability it is proposed to wait and check the replies from all the neighboring nodes to find a safe route. The proposed approach to combat the Black hole attack is to make use of 'Fidelity Table' wherein ever y participating node will be assigned a fidelity level that acts as a measure of reliability of that node. In case the level of any node drops to 0, it is considered to be a malicious node, termed as a 'Black hole' and is eliminated. Computer simulation using GLOMOSIM shows that proposed protocol provides better security and also better performance in terms of packet delivery than the conventional AODV in the presence of Black holes with minimal additional delay and Overhead. In this paper, researchers have analyzed the black hole attack [9]. In this attack, a malicious node falsely advertise shortest path to the destination node. The intension of malicious node could be to intercept all data packets being sent to the destination node concerned. The proposed approach is to detect the black hole attack in Mobile Ad-hoc network. This approach is based on the AODV (ad-hoc on demand distance vector) routing algorithm. In this paper, by using the proposed algorithms enhance the security of the network [10]. 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. [11]In this paper, the security challenges in intrusion detection and authentication are identified and the different types of attacks are discussed. We propose a two-phase detection procedure of nodes that are not authorized for specific services and nodes that have been compromised during their operation in MANET. The detection framework is enabled with the main operations of adhoc networking, which are found at the link and network layers. [12] This paper presents a guard node based scheme to identify malicious nodes in Adhoc On-Demand Distance Vector (AODV) protocol. In this scheme each node calculates trust level of its neighboring nodes for route selection. Trust calculation process involves opinions of other nodes about the node whose trust level is to be determined. If a neighboring node has a trust level lower than a predefined threshold value, it is identified as malicious and it is not considered for route selection. The proposed model does not use any key distribution process and no changes are made in control packets of AODV. [13] This paper focuses on networks using the popular Ad-hoc On-demand Distance Vector (AODV) protocol and a secure extension to AODV, the Secure AODV (SAODV) protocol.SAODV is representative of a number of secure versions of the AODV protocol in that it relies upon the use of cryptographic mechanisms to protect the routing control messages of AODV from being forged and/or altered by attackers.

2. Solution: Efficient AODV

We propose a solution that is enhancement of basic AODV and others proposed routing protocols. Firstly the proposed protocol will detect the black hole attack and after detection it will make the authorized node.Accroding to the proposed solution the source node will send RREQ to the respective nodes or relaying nodes. Every intermediate node receives the RREQ from the source node. 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. Then source node check the route reply message. After this, the source node checks the entire RREP packet. If the RREP packet contain both the Sequence no and broadcast ID. Then source node transmits the data to this node. If some respective nodes sends only sequence no then it means these are unauthorized nodes or black hole nodes. The source node will request again to send the Broadcast ID.If the intermediate node will send Broadcast ID then it will consider it authorized node and transmit the data through this route. If it will not send the Broadcast ID after again requesting the source node then source node will eradicate it. This is illustrated in figure 3 .B_1 and B_2 are the black hole nodes.

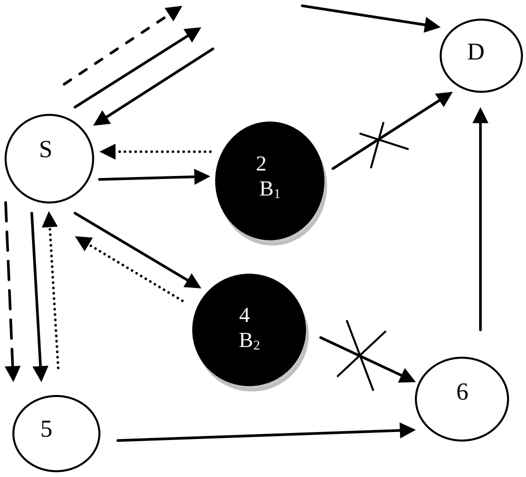


Fig 5: Propagation of the signal from source to destination node

A. Working principal of Efficient AODV

A.1.Black Hole node

The node which tries to capture the path of source node. As shown in the above figure B_1 and B_2 are the Black hole nodes.

A.2.Detection method

The node will be authentically decided on the basis of Broadcast ID and Sequence number.

A.3 Sending request

In the above figure 3, S wants to transmit to D. So it first transmits the route request to all the neighboring nodes. Here node 1, node B_1 node B_2 and node 5 receive this request. B_1 node and B_2 has no intention to transmit the DATA packets to the destination node D but it wants to intercept/collect the DATA from the source node S.

A.4 collecting response

The incoming responses are collected in a Routing table, namely, the Response table. The entries will have fields like, source address, destination address, hop count, next hop, lifetime, destination sequence number, Broadcast ID, source and destination's header address. The responses will be collected till a timer expiry event. As shown in the above figure node 1, node 5, node B_1 and node B_2 will give the response in the reverse route.

A.5 Choosing a response

All the responses are check that is collected from the respective nodes. If the responses from relaying nodes contains both the sequence no and broadcast ID then embedded this into routing table.

As shown in figure, the node 1, node 5 send the response with sequence no and broadcast ID.But node B_1 and node B_2 will send the only sequence no. The source node will be accept the request of only node 1 and node 5 and embedded into routing table and update it. Then the source node will be selecting the shortest path from the routing table. After selecting the shortest path, the source node will be check the link by sending the Hello packet which is simply ACK used to check the link from source to destination. This hello message again matches the Seq no. and BI of the relaying node that is already in routing table. If this condition is satisfied then metrics allowed sending data through this route.

A.5 Correction

From the above figure, node B_1 and node B_2 tries to capture the path of the source node when the source node is already transmitted the data through another node. Then the source node broadcast the RREQ to the black hole nodes (B_1 and B_2).Then the black hole node send the RREP.If the route reply contains both the sequence no and broadcast ID.Although the source node consider it authorize and transmit the data to this node. Otherwise remove the black hole node.

2.2. The Algorithm for proposed solution is as follows:

Perform Ring Search

```
1. Search network for source and destination.
2. Transmit RREQs and receive RREPs.
3. Network()
```

Network ()

```
1. Set Broadcast number for source and destination
2. Generate_Table (Broadcast Number($M_0$))
3. Check(Node_authenticity())
4. Compute_results()
```

Broadcast Number (M)

```
1. Assign_Broadcast ( for i=1 to N) ; N is the number
   of relaying nodes
2. Fetch(Adov:Broadcast(M, N)
3. Generate: send ACK---1
4. Transmit the Authenticity code (Node_authenticity)
```

Node_authenticity()

```
1. Consider Sender node
2. Check_broadcast_availabilty(broadcast table)
3. If (broadcast value==true)
4. Compute results()
5. Else
6. Send ACK—1 (node error)
7. Give error number to error node
8. Exit
```

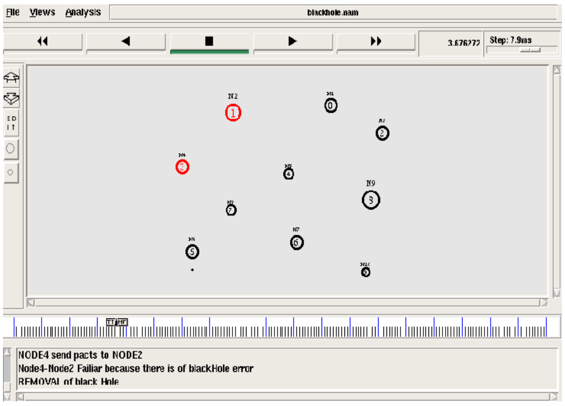
Compute_results()

```
1. Fetch packet received
2. Fetch packet lost
3. Merge to trace file
4. Compute graphical analysis
5. Compute end to end delays based on trace file
   parameter-VI
```

3. Simulation Results

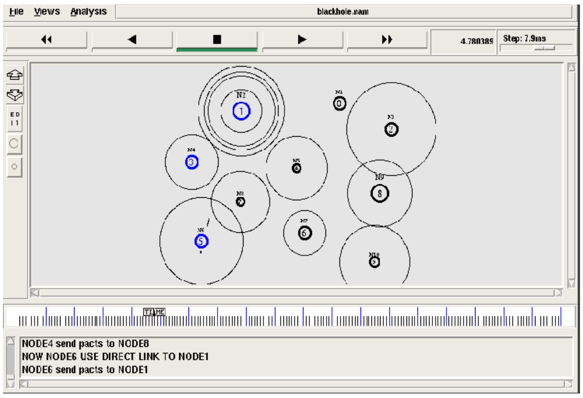
The simulation is done using NS2.34 simulator, to analyze the performance of the network by varying the nodes mobility. This paper has proposed a efficient AODV to detect and correct a black hole node. In an area of 2000×1000 meter, 10 nodes executing the EAODV (EfficientAODV) routing protocol randomly distributed, attack of two Black hole nodes are consider in this network topology.

In a simulated area 10 nodes are distributed and moved randomly. The blue color node shows that node is actively participating with less error. The green color node shows that node is actively participating with no error. Black color nodes are respective and receiving nodes. Fig 6 shows the detection of Black hole nodes. In this figure node 2, and node 4 are the black hole nodes. Fig 7 shows the correction of these black hole nodes. When these nodes sends the Broadcast ID then consider it authorized and transmit the packets to these nodes. In some cases black hole node tries to capture the path of source node. When the source sends the request for Broadcast ID.But this will not send the Broadcast ID because this node is actually a Black hole node.



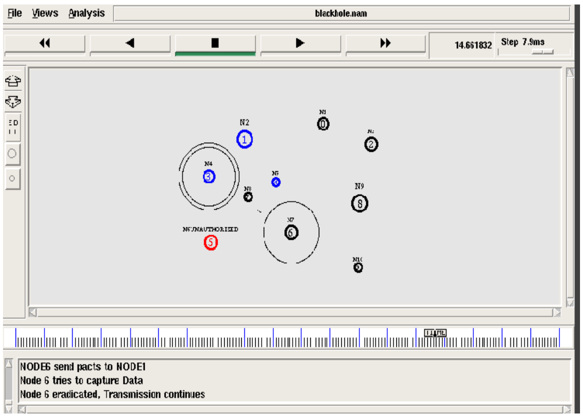
NODE4 send pacts to NODE2
Node4-Node2 Failiar because there is of blackHole error
REMOVAL of black Hole

Fig 6: Detection of Black hole nodes (shown in red color)



NODE4 send pacts to NODE8
NOW NODE6 USE DIRECT LINK TO NODE1
NODE6 send pacts to NODE1

Fig 7: Correction of Black hole nodes (shown in blue color)



```
NODE6 send pacts to NODE1
Node 6 tries to capture Data
Node 6 eradicated, Transmission continues
```

Fig 8:Removal of Black hole node

3.1.Simulation profile

The simulation profile is illustrated in the table 1.

Property	Value
Nodes	10
Simulation Time	25 ms
Mobility	10m/s
Packet size	512 bytes
Number of packet	50
Pause time	10ms
Simulation Area	2000×1000 meter

3.2.Metrics

The simulation is done using NS2(Network simulator 2) to analyze the performance of the network by varying the nodes mobility. The code of simulation is written in TCL (Tool Command Language).The metrics used to evaluate the performance are given below.

Packet Delivery Ratio: The ratio between the number of packets originated by the "application layer" CBR sources and the number of packets received by the CBR sink at the final destination.

Average End-to-End Delay: This is the average delay between the sending of the data packet by the CBR source and its receipt at the corresponding CBR receiver. This includes all the delays caused during route acquisition, buffering and processing at intermediate nodes, retransmission delays at the MAC layer, etc. It is measured in milliseconds.

Routing Overhead: This is the ratio of number of

Control packet generated to the data packets transmitted.

3.3.Comparision with basic AODV and SADOV

To evaluate the packet delivery ratio, simulation is done with 10 nodes with the source node transmitting 50 packets to the destination node. Each packet is of 512 bytes and is transmitted with an interval of 0.07ms. As it can be seen from the figure5, with SAODV the packet delivery ratio is more compared to AODV. Node mobility indicates the mobility speed of nodes. When the node mobility is very less then packet delivery ratio is very high. As shown in figure 1.When the node mobility is increased then packet delivery ratio is slightly decreased. The packet delivery ratio of EAODV is 95% compared to AODV and SAODV as shown in fig 1.The packet delivery ratio increases by using EAODV till 70m/s node mobility.

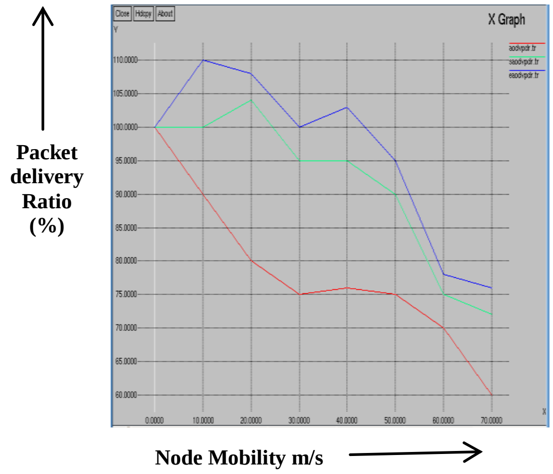


Fig. 9 Packet Delivery Ratio

From the figure-10 it can be observed that, when EAODV protocol is used there is decrease in the average end-to-end delay, compared to AODV and SAODV.

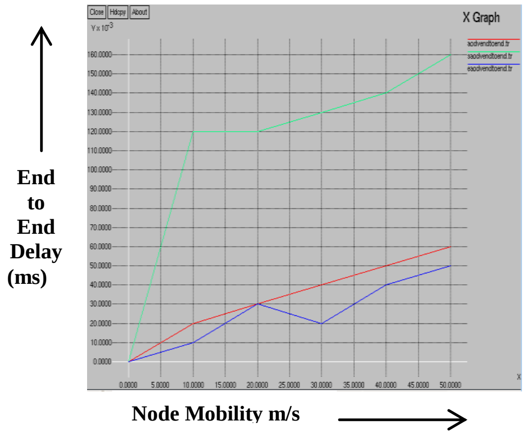


Fig.10.End to End Delay

From the fig 11. Shows the routing overhead. The number of transaction indicates number of flows initiated during a particular duration of time from same or different sources to same or different destinations within the considered network. If the number of transactions increase then overhead is increase due to the additional process is involved to avoid the selection of Black Hole node and to make the authorized node. As it can be seen from fig.11 the routing overhead of EAODV is slightly comparable to AODV.

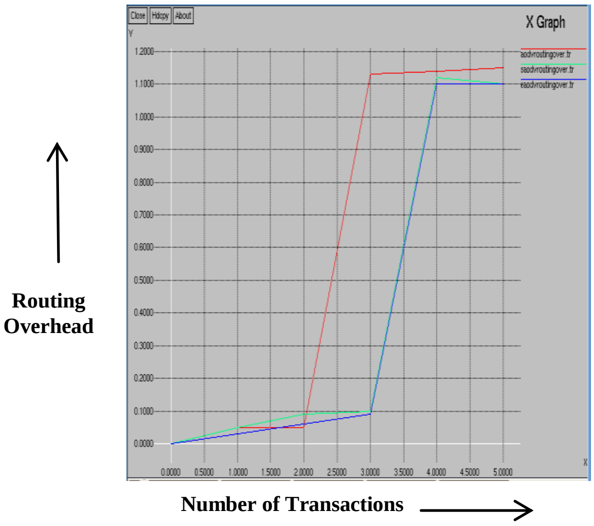


Fig.11.Routing Overhead

4.CONCLUSION AND FUTURE WORK

As already mentioned in the previous papers, the solutions have 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) or remove from the network. In this research paper we proposed a EAODV protocol that is enhancement of basic AODV.We compared the propose solution with basic AODV and already proposed work. By doing this we get the better result as compared to other solutions. Our proposed solutions firstly detect the Black Hole node then wait if this node sends the BI then consider it authorized node otherwise eradicate from the network. The solution is simulated using NS2 and is found to achieve the better security with minimal delay and overhead. The packet delivery ratio is also increase due this proposed solution. The future work is to practically implement.

5. REFERENCES

[1] V.Karpijoki, "Security in Ad Hoc Networks", Seminar on Network Security

[2] Hongmei Deng, Wei Li, and Dharma P. Agarwal, "Routing Security in Wireless Ad Hoc Networks", University of Cincinnati, IEEE Communications magazine, October 2002.

[3] Lidong Zhou, Zygmunt J. Haas, "Securing Ad Hoc Networks", IEEE network, special issue,, November/December 1999.

[4] 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-aodv-05.txt

[5] Charles E. Perkins, Elizabeth M. Belding-Royer, Samir R.Das, Mobile Ad Hoc Networking Working Group, Internet Draft, 17 February 2003.

[6] Yi-Chun Hu, Adrian Perrig, "A Survey of Secure Wireless Ad Hoc Routing", IEEE Security and Privacy May/June 2004.

[7] Latha Tamilselvan and Dr. V Sankaranarayanan, "Prevention of Black hole Attack in MANET",The Second international conference on wireless Broadband and Ultra Wideband Communications,2007.

[8] Latha Tamilselvan and Dr. V Sankaranarayanan, "Prevention of Co-operative Black hole attack in MANET", Journal of Networks, Volume No.5, May 2008.

[9] Govind Sharma and Manish Gupta, "Black Hole Detection in MANET Using AODV Routing Protocol "International Journal of Soft Computing and Engineering, ISSN: 2231-2307, Volume-1, Issue -6, January 2012.

[10] Ming-Yang Su, "Prevention of selective black hole attacks on mobile adhoc networks through intrusion detection systems", ELSEVIER, Volume 34, ppt: 107-117, Issue 1, 15 January 2011.

[11] Nikos Komninos and Dimitris vergados, "Detecting unauthorized and compromised nodes in mobile adhoc networks", ELSEVIER, Volume 5, ppt: 289-298, Issue 3, April 2007.

[12] Imran Raza and S.A Hussain**,** "Identification of malicious nodes in an AODV pure adhoc network through guard nodes" ELSEVIER, Volume 31, ppt: 1796-1802, Issue 9, 8 June 2008.

[13] Jan von Mulert, Ian Welch and Winston K.G. Seah, "Security threats and solutions in MANETs: A case study using AODV and SAODV", Journal of Network and Computer Applications, Volume 35, ppt: 1249-1259, Issue 4, July 2012.

[14] TheNetworkSimulator-ns-2, ttp://www.isi.edu/nsnam/ns/.