SECURING MANET AGAINST INSIDER ATTACK-A BLACK HOLE ATTACK & ITS PERFORMANE ANALYSIS

Miss Bhandare A.S.[#1], Dr. Mrs Patil S.B.[#2],Mr. Pail B.S.[#3]
#1Dept. of Electronics & Telecomm Engg, JJMCOE Jaysingpur, 8308391322
#2 Dept. of Electronics Engg, JJMCOE Jaysingpur 9422618670
#3 1Dept. of Electronics Engg, PVPIT, Budhgaon, 98903055573

ABSTRACT

A Mobile ad hoc network (MANET) is a temporary network set up by wireless nodes usually moving randomly and communicating without a network infrastructure or any centralized administration. One of the principal routing protocols used in Ad-Hoc networks is AODV (Ad-Hoc On demand Distance Vector) protocol. Due to security vulnerabilities of the routing protocols, wireless ad-hoc networks are unprotected to attacks of the malicious nodes. The security of the AODV protocol is compromised by a particular type of attack called 'Black Hole' attack. It is due to malicious node present inside the network, called asInside Attacker. Since the data packets do not reach the destination node, on account of this attack, data loss will occur. In this paper, therefore, we attempt to focus on analyzing AODV against Black-hole attack imposed by both single and multiple black hole nodes(Co-operative Black-hole attack).and provides one solution to minimize it.

Key words: AODV, Black-hole attack, Co-operative black hole attack, MANET

Corresponding Author: Miss A.S. Bhandare

INTRODUCTION

Wireless ad-hoc networks are composed of autonomous nodes that are self- managed without any predefined infrastructure. 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 does the function of routing and relaying messages for other mobile nodes [5]. Ad-hoc networks have a dynamic topology such that nodes can easily join or leave the network at any time that makes it very difficult in developing secure ad-hoc routing protocols. The use of wireless links, lack of fixed infrastructure and the characteristic of dynamic topology associated with ad-hoc networks make it impossible to use wired network security mechanism as is most important networking operations include routing and network management [2]. Routing protocols can be divided into proactive, reactive and hybrid protocols, depending on the routing topology. Proactive protocols are typically table-driven. 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. 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 they are exposed to a lot of attacks. One of these attacks is the Black Hole attack.

Ad-hoc On-Demand Distance Vector (AODV) Routing Protocol

Ad-hoc On-Demand Distance Vector (AODV) [13] Routing Protocol is used for finding a path to the destination in an ad-hoc network. To find the path to the destination all mobile nodes work in cooperation using the routing control messages. Route Requests (RREQs), Route Replay (RREPs), Route Errors (RERRs) are control messages used for establishing a path to the destination. 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 [1].When the source node wants to make a connection with the destination node, it broadcasts an RREQ message. [3]. This RREQ message is propagated from the source, received by neighbors (intermediate nodes) of the source node. The intermediate nodes broadcast the RREQ message to their neighbors. This process goes on until the packet is received by destination node or an intermediate node that has a fresh enough route entry for the destination [3]. 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.

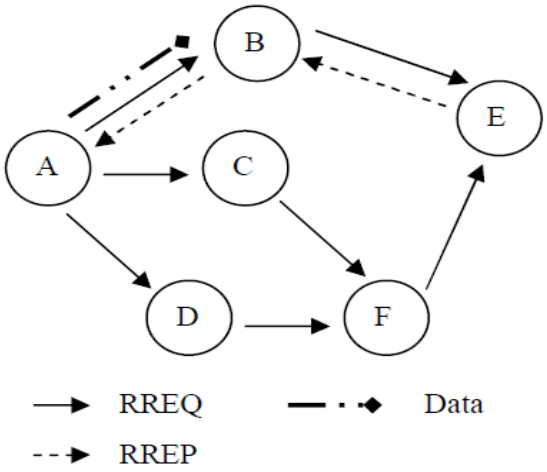

Fig 1. Propagation of RREQ and RREP from A to E

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. Above Fig 1 illustrate the operation.

Attacks to the wireless ad-hoc network in the networking layer usually have two purposes: not forwarding packets or adding and changing some parameters of routing messages; such as sequence number and IP addresses. Cryptography or authentication mechanisms protect the network against attacks that come from outside, but malicious 'insiders' which use one of the critical keys can also threaten the security [3].This paper consider one of such attack called as" Black hole attack"

Black Hole Attack

In a black hole attack, a malicious node sends fake routing information. To carry out a black hole attack, malicious node waits for neighboring nodes to send RREQ messages. When the malicious node receives an RREQ message, without checking its routing table, immediately sends a false RREP message giving a route to destination over itself, assigning a high sequence number to settle in the routing table of the victim node, before other nodes send a true one. Therefore requesting nodes assume that route discovery process is completed and ignore other RREP messages and begin to send packets over malicious node. [3] Malicious node attacks all RREQ messages this way and takes over all routes and all traffic will be routed through malicious node

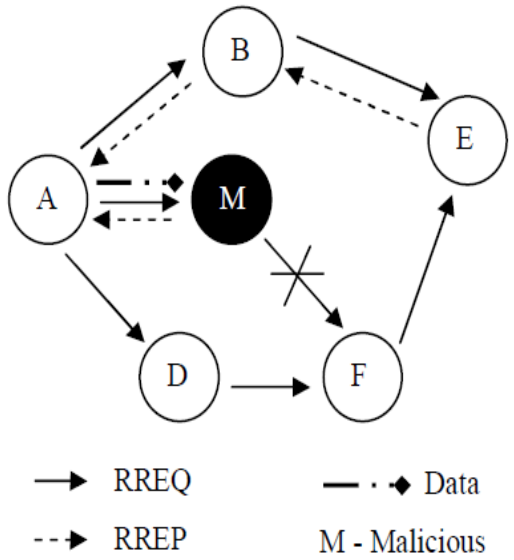

Fig2. Black hole attack in AODV

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'. Node 'A' assumes that the route through 'M' is the shortest route and sends any packet to the destination through it. When the node 'A' sends data to 'M', it absorbs all the data and thus behaves like a 'Black hole'. In the network there may be possibility that more than one black hole is present which is called as "Co-operative black hole attack"

Solution: System proposed to prevent Black hole attack in AODV

One of the main techniques utilized to prevent attacks against security threats is Intrusion Detection Systems (IDS). Intrusion detection is a process of detecting an adversary and preventing its subsequent actions. The proposed technique assumes every activities of a user

or a system can be monitored and anomaly activities of an intruder can be identified from normal activities. Hence, by identifying anomaly activities of an adversary, it is possible to detect a possible intrusion and isolate the adversary. This technique is called as Intrusion Detection using Anomaly Detection. Here IDAD is provided with a pre-collected set of anomaly activities, called audit data. Once audit data is collected and is given to the IDAD system, the IDAD is able to compare every activity of a host with the audit data. If any activity of a node resembles the activities listed in the audit data, the IDAD system isolates the particular node by avoiding it in further activities.
In a black hole attack, a malicious node deceives source nodes by sending a fake RREP message [3]. Fake RREP messages from a malicious node contain the following parameters:

I. maximum destination sequence number − to make the route up to date
II. single hop-count − to make a route with the shortest path
III. destination IP address − address of the destination node copied from RREQ
IV. time-stamp − the time the RREP was generated

These entries of an RREP message from a malicious node can be collected as audit data to differentiate anomaly activities from normalcy activities

Simulation Results

The simulation is done using NS-2 simulator. For simulation we use CBR (Constant Bit Rate) application with 25 numbers of nodes. The size of data payload is 512 bytes and simulation time is 150seconds.
Simulation results are summarized as follow

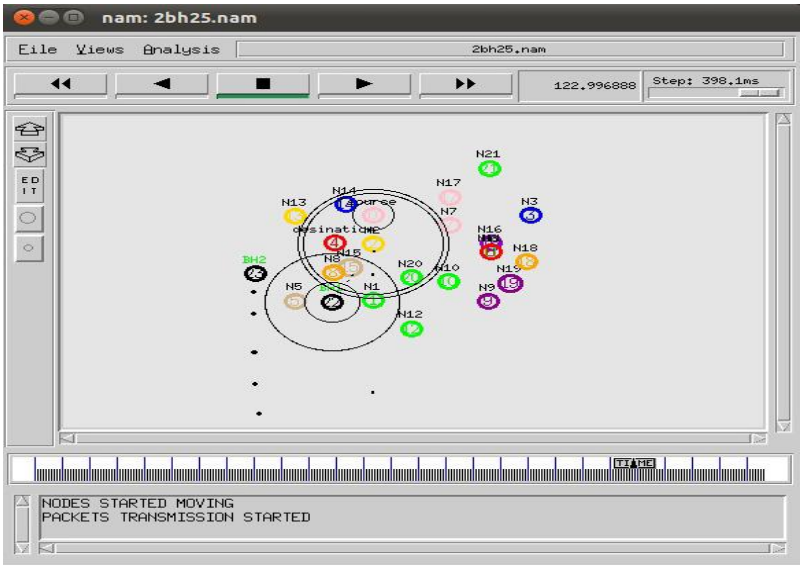

Fig1. Packets dropped due to black holes

Fig1. shows black hole scenario in NS-2 where Node 0 is source, node 4 is destination while Node 22 & Node 23 (black colored) are black hole nodes. From this Nam file we can see that these black holes drop the data packets instead of forwarding it to the Destination.

The parameters used to evaluate the performance of MANET without and with black hole (or holes) are number of Packets Generated, Number of Packets received, Packet Delivery Ratio,

Control Packets, Control Overhead, Average Throughput, and Average Delay. Then evaluate effects of the proposed solution (IDSAODV) with the help of same metrics.
The metrics are explained below [1]

i) 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.

ii) Throughput: Throughput is the average rate of successful message delivery over a communication channel.

iii) Routing Overhead: This is the ratio of number of control packet generated to the data packets transmitted

iv) 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. [1]

Table 1. Simulation results with and without black hole

Parameters	**Without black hole**	**With one black hole**	**With two black hole**
Generated Packets	21411	2442	1250
Received Packets	21357	1	1
Total Dropped Packet	54	2441	1249
Packet Delivery Ratio (%)	99.74	0.04	0.08
Data Packets	23531	4614	2366
Control Packets	23495	4614	2366
Control Overhead	99.84%	100%	100%
Average Throughput(kbps)	600.187	0.35	0.35
Average Delay(ms)	133.304	30.32	17.55

Form the table it is observed that packet delivery ratio goes on decreasing as no number of black hole nodes increases. The average throughput is also decreasing with black holes. The average delay is decreasing in presence of black hole node because it does not waste the time for checking the routing tables for giving RREP.

Table 2. Simulation results with IDSAODV

Parameters	**IDSAODV With one black hole**	**IDSAODV With two black hole**
Generated Packets	2442	1250
Received Packets	2441	1249
Total Dropped Packet	1	1
Packet Delivery Ratio (%)	99.95%	99.92%
Data Packets	4889	2507
Control Packets	4889	2507
Control Overhead	100%	100%
Average Throughput(kbps)	99.98	89.12
Average Delay(ms)	11.85	19.66

The above table shows that the packet delivery ratio increases with IDSAODV which improve the network performance. When IDSAODV protocol is used there is increase in the average end-to-end delay, compared to AODV. This is due to the time required for comparison with audit data.

CONCLUSION

Wireless ad hoc networks are vulnerable to various attacks due to the physical characteristic of both the environment and the nodes. One type of attack, due to malicious node present inside the network, Black hole attack causes serious damage to network. So to minimize the black hole effect one solution (IDSAODV) is proposed. Here every single mobile node is responsible for protecting itself effectively prevents a black hole attack regardless of the number of black hole nodes. The simulation results show that the performance of the network is improved under the co operative black hole attack also.

REFERENCE

[1] Tamilselvan,L.;Sankaranarayanan V.,"Prevention of Blackhole Attack in MANET," Wireless Broadband and Ultra Wideband Communications, 2007. Aus Wireless 2007. The 2nd International Conference on, vol., no., pp.21, 27-30 Aug. 2007.

[2] Yibeltal Fantahun Alem and Zhao Cheng Xuan , "Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection",2010 2nd International Conference on Future Computer and Communication.

[3] S. Dokurer "Simulation of black hole attack in wireless ad-hoc networks," Master thesis, September 2006, Atilim University, Turkey

[4] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," Sixth Annual International Conference on Mobile Computing and Networking (MobiCom'2000), Boston, August 6-11, 2000.

[5] H. Deng, W. Li and D. P. Agrawal,"Routing Security in Wireless Ad Hoc Networks". University of Cincinnati, IEEE Communication Magazine, October 2002.

[6] C. E. Perkins, E. M. B. Royer, and S. R. Das, "Ad hoc on-demand distance vector (AODV) routing," RFC 3561, July 2003

[7] P. Ning and K. Sun, "How to misuse AODV: A case study of insider attacks against mobile ad-hoc routing protocols," in Proceedings of the 4th Annual IEEE Information Assuranca Workshop, pp. 60–67, West Point, NY, USA, June 2003