International Journal of Computers &Technology
Volume 4 No. 2, March-April, 2013, ISSN 2277-3061

A Simulated Novel Approach for Identifying Black Hole Attack in AODV based MANET

Kanika Lakhani
Assistant Professor, Manav Rachna College of Engineering, Faridabad
kanikalakhani@yahoo.co.in

Abstract: Security is an essential requirement in mobile ad hoc networks to provide protected communication between mobile nodes. Due to unique characteristics of MANETS, it creates a number of consequential challenges to its security design. To overcome the challenges, there is a need to build a powerful, multifeatured security solution that achieves both broad protection and desirable network performance. MANETs are vulnerable to various attacks, blackhole, is one of the possible attacks. Black hole is a type of routing attack where a malicious node advertise itself as having the shortest path to all nodes in the environment by sending fake route reply. By doing this, the malicious node can deprive the traffic from the source node and can be implemented as a denial-of-service attack where the packets can be dropped later on. In this paper, a solution is proposed to identify the malicious node and implanting security against the threats of blackhole by notifying other nodes in the network of the incident. The simulation of the proposed algorithm demonstrates that the solution prevents the nodes in the network from blackhole attack and also improves the overall performance of AODV in the presence of black hole attack.

Keywords: MANETs, AODV, Routing protocol, blackhole attack.

I. Introduction

A mobile ad hoc network (MANET) is a collection of mobile nodes that can instantly establish a network, whenever they coexist in the same neighborhood without the need of any fixed infrastructure or centralized administration. The routing protocols in an ad hoc network allow the source node to find various routes to the destination with the cooperation of other nodes within the network. Due to the random movement of the nodes, the network topology changes rapidly and arbitrarily. So, the routing protocol is expected to be able to react to these changes and must facilitate the nodes to identify new routes in the network to maintain connectivity. The problem of security in MANETs[2][3] represents a serious challenge. This issue arises mainly due to the highly vibrant nature of the ad hoc network and also due to the need to operate efficiently with limited number of resources, including network bandwidth, CPU processing capacity, memory and battery power (energy) of each individual node in the network. Rapid and frequent routing protocol interaction between nodes is required. As wireless ad-hoc networks lack an infrastructure, they are exposed to a lot of attacks and one of these kinds of attacks is the Black Hole attack.

In the Black Hole attack, a malicious node absorbs all data packets in itself, similar to a hole which sucks in everything in. In this way, all packets in the network are dropped. A malicious node that drops all the traffic in the network makes use of the vulnerabilities of the route discovery packets of the on demand protocols, such as in AODV. In this paper, a new approach is defined to identify the malicious node and all the nodes in the network is intimated of the malicious node. The packet is then resend and security architecture is applied to the network. The application of security architecture serves as the future work.

II. AODV Routing Protocol

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. Malicious node attacks all RREQ messages this way and takes over all routes. Therefore all packets are sent to a point when they are not forwarding anywhere. This is called a black hole similar to real meaning which swallows all objects and matter. To succeed a black hole attack, malicious node should be positioned at the center of the wireless network. If malicious node masquerades false RREP message as if it comes from another victim node instead of itself, all messages will be forwarded to the victim node. If this is done, victim node will have to route all incoming messages and is subjected to a sleep deficit attack.

III. Security in Ad-Hoc Networks

The security characteristics of ad-hoc networks are very different to those of traditional infrastructure based wireless networks. The absence of a fixed infrastructure due to node mobility implies that nodes cannot rely on information from trusted servers such as certification authorities. In this section, we will examine the security challenges facing ad-hoc networks.

One of the most distinct feature of MANET's from other static networks is the fact that each node of the networks contributes in making up routes from various sources to destinations or groups of nodes acting as destination. However, this distinct feature poses a number of serious threats to the security and privacy of the overall network as well as the individual nodes making up the network. The openness of ad hoc networks offers greater flexibility in terms of functionality, but it also provides an open path for any malicious node or intruder to gain access to the network and perform activities

such as eaves dropping, spoofing, Denial of service attacks, flooding, link failure and many more. To ensure safe operation of an ad hoc network, the following minimum constraints should be met

- **Authentication** of a node is very important so that the node can be trusted as a valid and trusted node, and malicious, eavesdropping nodes are denied access into the network.
- **Data integrity** is an important issue, so as to ensure the data communicated between nodes has not been tempered or altered by any malicious node.
- **Privacy** is also necessary, to ensure that no intermediate node can access the data that is meant for the destination of that message.
- **Non-repudiation** ensures that the origin of the message cannot deny having sent the message Non-repudiation is useful for detection and isolation of compromised nodes. When a particular node receives an erroneous message from another node, non-repudiation allows the receiver to accuse sender using this message and to convince other nodes that the sender is compromised

IV. Black Hole Attack

Mobile ad-hoc networks are vulnerable to various kinds of attacks. These attacks include threats against the routing mechanism involving the functioning of physical layer, MAC and network layer. These attacks serve the purpose of not forwarding the packet and modifying several parameters such as sequence number. Commonly an opponent can cause the non-forwarding of a message to other nodes. SO, if the opponent node is selected as a route to send the data packet, it denies providing the routing path. Similarly, in the case of Black hole attack, the opponent or the malicious node waits for route request (RREQ) packet from its neighboring node and on receiving; it sends a false route reply (RREP) packet with a customized sequence number. This gives an illusion to the sender node about the new route to the destination. This makes the sender node to ignore the RREP packet from other neighboring node in the network and forwards the data packet to the opponent node. The opponent node routes all the packets towards itself and blocks the packets to be forwarded anywhere on the network.[15]

In the following illustrated hypothetical situation, imagine a malicious node ‘M’. When node ‘A’ broadcasts a RREQ packet ,both nodes ‘B’ and ‘M’ receive it .Node ‘M’, being a malicious node ,does not check up with its routing table for 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 ‘C’ node

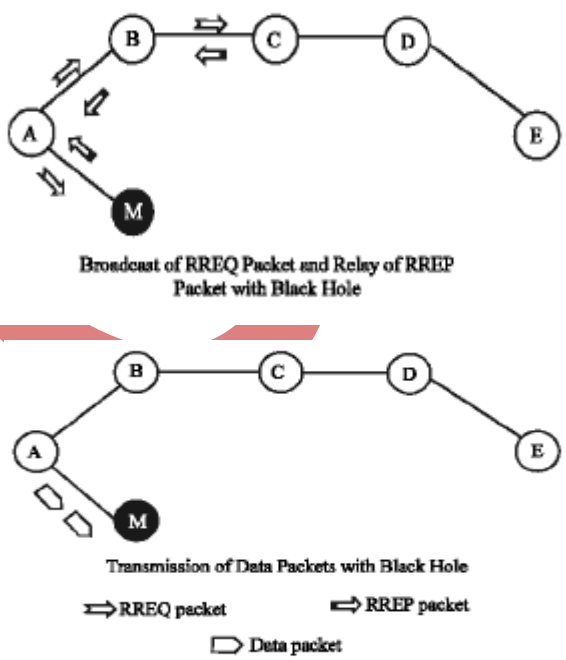

Figure 1: Blackhole Attack

‘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.

V. Proposed Solution

The proposed solution exploits the packet sequence number included in any packet header. The node in this situation needs to have two extra tables; the first table consists of the sequence numbers of the last packet sent to the every node in the network, and the second table for the sequence number received from every sender. During the RREP phase, the

intermediate or the destination node must include the sequence number of last packet received from the source that initiates RREQ. Once the source receives this RREP, it will extract the last sequence number and then compare it with the value saved in its table. If it matches the transmission will take place. If not, this replied node is a malicious node, so an alarm message will be broadcast to warn the network about this node. Every packet in MANETs has a unique sequence number. This number is an increasing value, i.e., the next packet must have higher value that the current packet sequence number. The node in regular routing protocols keeps the last packet sequence number that it has received and uses it to check if the received packet was received before from the same originating source or not.

In this solution, every node needs to have two additional small-sized tables; one to keep last-packet-sequence-numbers for the last packet sent to every node and the other to keep last-packet-sequence-numbers for the last packet received from every node. These tables are updated when any packet is arrived or transmitted. The sender broadcasts the RREQ packet to its neighbors. Once this RREQ reach the destination, it will initiate a RREP to the source, and this RREP will contain the last-packet-sequence-numbers received from this source. When an intermediate node has a route to the destination and receives this RREQ, it will reply to the sender with a RREP contains the last-packet-sequence-numbers received from the source by this intermediate node. This solution provides a fast and reliable way to identify the suspicious reply. No overhead will be added to the channel because the sequence number itself is included in every packet in the base protocol.

Prelims: The implementation consists of several modules as the packet is broadcasted through route agent from the source node.

- AODV_Host-1 to AODV_Host-m are the 'm' number of nodes in the network; Host-n is the destination node; Host-u is the malicious node.
- Check AODV_pkt_Type checks the type of packet sent
- Blackhole_AODV_Host-u() module depicts the working of malicious node
- pkt_alloc() is the module for packet allocation
- RA_pkt_init() is the module for packet initialization by the Route Agent
- pkt_recv() is the module for packet receive
- pkt_resolve()is the module for resolving the destination node

VI. Pseudo Code

1. Set Route Agent RA
   {
   pkt_alloc(); //Packet is allocated to RA
   RA_pkt_init(); //RA initializes the packet for transmission
   Forward to AODV_Host-1 //Packet is forwarded to host1
   }
2. AODV_Host-1
   {
   pkt_recv(); //Host1 receives the packet
   pkt_resolve(); //Host1 checks if the packet is meant for itself
   if(Reply_Recvd== NONE)
   then forward the packet to AODV_Host-2
   }
3. The packet is kept forwarded to next node if no reply for acceptance is received from the intermediate nodes.
4. AODV_Host-n //Host-n is the destination node
   {
   pkt_recv();
   broadcasts msg "Packet Received"
   }
5. If (Reply_Recvd== NONE)
   packet is assumed to be lost

Before Resending

6. Locate Lost_Packet
   {
   Check AODV_pkt_Type
   Check Source Routing Table
   }
7. Apply Security Constraints
8. Resend Lost Packet
9. If (Reply_Recvd=="Packet Received")
   EXIT

International Journal of Computers &Technology
Volume 4 No. 2, March-April, 2013, ISSN 2277-3061

```
Blackhole_AODV_Host-u
{
  pkt_recv();
  pkt_resolve();
  {
    If(pkt==data_pkt)
      Drop
   }
   Packet is Lost
  }
```

```
Check AODV_pkt_Type
{
  If AODV_pkt_Type==RREQ)
        recvReq(x);
  else if AODV_pkt_Type==RREP)
        recvReply(x);
  else if AODV_pkt_Type==ERROR)
        recvError(x);
 else if AODV_pkt_Type==”HELLO”)
        recvHello(x);
  else print”(Invalid Type”)
}
```

```
Check Source Routing Table
{
  Check Last_Packet_Sequence_Number Table for    every node
  Identify Malicious Node
  If (identified)
  Broadcast Msg “Malicious Node AODV_Host-“%n””)
}
Apply Security Constraints.
```

VII. Explanation

An agent bound to the specific node allocates the packet and initializes the content of the packet. Afterwards the packet is handled by the AODV routing mechanism. First the routing handler receives this packet. This is done locally. Afterwards the route for the packet is detected. When a suitable route is found, the packet is forwarded to the next hop within this route[12]. The pkt_recv() method is the first method called. This method calls first the pkt_resolve() and the forward() method.

This simulation consists of ‘m’ hosts that are located in a line, so that Host 1 and Host 3 are not able to communicate directly. Within this simulation one TCP packet is send from Host 1 to Host 3 and the reply is send from Host 3 to Host 1. AODV resolves the route to Host 3 by sending a special request packet. This packet is broadcasted as long as the destination of the packet replies. The reply is also broadcasted through the network. Each forwarded request packet also triggers the intermediate nodes to send additional request packets.

Therefore in the beginning of the simulation there is a high amount of AODV related network traffic. After that phase, there is only a few additional AODV network traffic required. Detected routes are cached within this implementation, so that not every send packets requires a related AODV route request. After the detection of the route, the packet is send.

International Journal of Computers &Technology
Volume 4 No. 2, March-April, 2013, ISSN 2277-3061

Evaluation of Results

Each scenario has two simulations. In the first one every node is working in cooperation with each other to keep the network in communication. The second simulation has one malicious node that carries out the Black Hole Attack. To evaluate the packet loss, the number of packets that are sent are counted by the sending nodes and how many of them reached the receiving nodes.

The tables below compares the normal and Black Hole networks. In the tables, the second column shows how many packets are sent by sending nodes and the third column shows how many of them reached the receiving nodes. By calculating the difference between the tables of normal and Black Hole AODV network we try to evaluate how many of the packets which could not reach the destination node are absorbed in the Black Hole Node.

Packets lost in the Black Hole Node are shown in the fourth column of the table of the Black Hole network. The rest of the columns show percentage of the packets lost and additionally in the table of Black Hole network, we added percentage of loss packets which are absorbed in the Black Hole Node.

We noticed that the percentage of data loss of the Black Hole AODV is increased more than the normal AODV network simulations in all scenarios.

Sending Node -> Receiving Node	Sent Packets	Received Packets	Loss %
Node 0 -> Node 1	1103	1067	3.263826
Node 2 -> Node 3	1098	1002	8.743169
Node 4 -> Node 5	1117	1075	3.760072
Node 6 -> Node 7	993	959	3.423968
Node 8 -> Node 9	911	887	2.634468
Node10->Node11	1045	998	4.497608
Node12->Node13	868	862	0.691244
Node14->Node15	1092	1023	6.318681
Node16->Node17	1073	1043	2.795899

Table 1: Results of AODV in Scenario 1

Sending Node -> Receiving Node	Sent Packets	Received Packets	Loss %
Node 0 -> Node 1	1089	1069	1.836547
Node 2 -> Node 3	1175	1123	4.425532
Node 4 -> Node 5	845	798	5.56213
Node 6 -> Node 7	278	265	4.676259
Node 8 -> Node 9	756	733	3.042328
Node10->Node11	1178	1056	10.35654
Node12->Node13	965	945	2.072539
Node14->Node15	1098	1062	3.278689
Node16->Node17	1149	1102	4.090513

Table 2: Results of AODV in Scenario 2

Sending Node-> Receiving Node	Sent Packets	Received Packets	Packet Drop	Loss %
Node 0 -> Node 1	1091	29	277	97.34189
Node 2 -> Node 3	1103	62	563	94.37897
Node 4 -> Node 5	1031	27	732	97.38118
Node 6 -> Node 7	1100	116	118	89.45455
Node 8 -> Node 9	1115	87	897	92.19731
Node10->Node11	1167	98	665	91.6024
Node12->Node13	1103	64	598	94.19764
Node14->Node15	1154	99	456	91.42114
Node16->Node 7	1134	56	778	95.06173

Table 3: Results of Blackhole AODV in Scenario 1

Sending Node -> Receiving Node	Sent Packets	Received Packets	Packet Drop	Loss %
Node 0 -> Node 1	998	23	546	97.69539
Node 2 -> Node 3	1067	98	778	90.81537
Node 4 -> Node 5	1134	49	559	95.67901
Node 6 -> Node 7	1189	23	734	98.0656
Node 8 -> Node 9	1100	67	621	93.90909
Node10-> Node 11	1078	45	443	95.8256
Node12-> Node 13	998	33	507	96.69339
Node14-> Node 15	1023	96	740	90.61584
Node16-> Node 17	1178	56	489	95.24618

Table 4: Results of Blackhole AODV in Scenario 2

VIII. Conclusion

In this study, the effect of Black Hole attack is analyzed in an AODV Network. For this purpose, AODV protocol is implemented that behaves as Black Hole in NS-2. Two scenarios have been implemented where each one has 20 nodes that use AODV protocol and also simulated the same scenarios after introducing one Black Hole Node into the network. Moreover, a solution has also been implemented that attempted to reduce the Black Hole effects in NS-2 and simulated the solution using the same scenarios. Having simulated the Black Hole Attack, it is observed that the packet loss is increased in the ad-hoc network. The tables of simulation results show the difference between the number of packets lost in the network with and without a Black Hole Attack. This also shows that Black Hole Attack affects the overall network connectivity and the data loss could show the existence of the Black Hole Attack in the network.

It can be seen from Tables, AODV network has normally 5.65 % data loss and if a Black Hole Node is introduced in this network data loss is increased to 95.5 %. As 5.65 % data loss already exists in this data traffic, Black Hole Node increases this data loss by 89.85 %. When we used secure AODV protocol in the same network, the data loss is decreased.

Proposed solution for blackhole attack is further enhanced so that blackhole node once identified can be blacklisted in a network in a way that every other node in the network is aware of blackhole nature of this particular node and avoids sending/receiving data to/from this node.

Future Work

Future work includes implanting security constraints on the network so that the communication with the malicious node can be strictly avoided. Implementation of this enhancement requires certain changes in AODV protocol.

References

[1] Das, S. R.(2000). Performance Comparison of Two On-demand Routing Protocols for Ad Hoc Networks

[2] Hongo Zhou," a survey on Routing Protocols In Manets", Technical report, MSU-CSE-03-08 Mar 28,2001.

[3] L. Zhou and Z.J.Haas," Securing Ad Hoc networks" IEEE Net. Vol. 13, Nov./Dec. 1999.

[4] Hu, Y. C.(April 2003) The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks(DSR), IETF Draft.

[5] Srdjan Capkun, Levente Butty´an, and Jean-Pierre Hubaux, "Self-Organized Public- Key Management for Mobile Ad Hoc Networks," Technical Report at EPFL http://ic2.epfl.ch/publications/documents/IC_TECH_REPORT_200234.pdf.

[6] S. Marti et.al. ." Mitigating Routing Misbhevaior in mobile Ad Hoc Networks," 6th Intl. Conference on Mobile Computing Net.(MOBICOM)August 2000, p.p 255-265.

[7]V.Karpijoki ,"Security in Ad Hoc networks" http://www.hut.fi/~vkarpijo/netsec00_manet_sec.ps.

[8] J.Lundberg,"Routing Security in mobile Ad Hoc Networks", Helsinki University of Technology , http"://citeseer.nj.nec.com/40096/html

[9] Jean-Pierre Hubaux, Lvnt Buttyan, S. Capkun." The Quest for security in mobile Ad Hoc Networks, proceedings of the ACM 2001".

[10]IETF MANET Working Group http://www.ietforg/html.charters/manet- charter.html

[11] D. Johnson, D. Maltz," Dynamic Source routing in Ad Hoc Wireless Networks in Mobile Computing Chapter –5, p.p 153-181, 1996.

[12]B. Dahill, B.N. Levine" A secure routing protocol for Ad Hoc Networks",Proc.10th IEEE Conf.Network Protocols (ICNP), IEEE Press, 2002, pp 78-87.

[13] T. Camp, J. Boleng and V.Davies, " Mobility models for Ad hoc Network research" Wireless Communications and Mobile Computing(WCMC) , special Issue on Mobile Ad Hoc networking: Research Trends and Applications, 2002.

[14] M. Guerrero Zapata and N. Asokan ," Securing Ad Hoc Routing protocols" , in Proceedings of the ACM Workshop on Wireless security (WiSe), September 2002.

[15] P. Papadimitratos and Z. J. Haas, "Secure Routing For Mobile Ad Hoc Networks" in Proceedings of the SCS Communication Networks and distributed Systems Modeling and Simulation Conference(CNDS), January 2002.

[16] W. Lou, W. Liu and Y. Fang SPREAD: Enhancing data Confidentiality in Mobile Ad Hoc Networks" in Proceedings of IEEE INFOCOM' 04 HongKong, China, March 2004

[17]Y. Zhang, W. Liu and W.Lou Anonymous Communications in Mobile Ad Hoc Networks" in Proceedings of the IEEE INFOCOM' 05 Miami, FL, March 2005

[18]Rivest, A. Shamir, L.Adleman, " A method for obtaining digital signatures and public key Cryptosystem, Communications of the ACM 21(2) Feb. 1978p.p 120-126.

[19]Haiyun Luo, Petros Zerfos, Jiejun Kong, Songwu Lu and Lixia Zhang, "Self-securing Ad Hoc Wireless Networks,"http://www.cs.ucla.edu/~jkong/publications/ISCC02.pdf.

[20]T. S. Rappaport, Wireless Communication: Principles and Practice, Prentice Hall October 1995

[21] Seung Yi, Prasad Naldrug, Robin kravets: A security Aware routing protocol for Wireless Ad hoc Networks in the Proceedings of 3rd ACM International Conf. of mobile ad hoc networking and Computing pp 226-236, 2002

[22] Monis Akhlaq, M Noman Jafri, Muzammil A khan, Baber Aslam "Addressing Security Concerns Of Data Exchange in AODV Protocol" in the proceedings of World Academy of Science, Engineering and Technology .Vol. 16, November 2006.