Asian Journal of Information Technology 5 (10): 1070-1075, 2006

Routing Security in Mobile Ad-hoc Networks

[1]Latha Tamilselvan and [2]V. Sankaranarayanan
[1]Department of Information Technology, Anna University,
BSA Cresent Engineering College, Vandalur, Chennai, Tamilnadu, India
[2]Director, Tamil Virtual University, Elnet City, Chennai, Tamilnadu, India

Abstract: An Ad Hoc network is a collection of mobile nodes that dynamically form a temporary network. Unlike traditional wireless and mobile networks in which mobile nodes communicate with a centralized structure, an Ad Hoc network operates without the use of existing a network infrastructure. It is primarily used for military tactical communication applications with some commercial use. One important issue in Ad Hoc networks is security. The entire system of Ad-Hoc network works on the principle of Trust. If the neighbor's security is compromised or the node is itself hijacked then the security of the entire network is under threat. 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. This study provides routing security to the AODV routing protocol by eliminating the threat of 'Black Hole' attacks. Our solution utilizes the sequence numbers used in transmission and reception of data/control packets in AODV to identify the 'Black Hole' and isolate it from the network. Computer simulation using GLOMOSIM shows that our protocol provides better performance than the conventional AODV in the presence of Black Holes with minimal additional delay and hops.

Key words: Ad Hoc network, mobile nodes, routing security, black hole

INTRODUCTION

Ad-Hoc networks are temporary networks that are created between mobile nodes as and when needed. The difference between Ad-Hoc networks and conventional wireless networks is the absence of a fixed back-bone infrastructure in the study of Ad-Hoc networks[1]. Typical applications of Ad-Hoc networks are military, emergency and relief operations where the establishment of a central infrastructure may not be possible. There exists no central control through base stations or switching centers and 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 does the function of routing and relaying messages for other mobile nodes. Routing protocols play an important role in both the creation and maintenance of the routes in the network. The routing protocols developed for Ad-Hoc networks are generally classified into two categories[2]:

Proactive routing protocols: In proactive protocols, the routes are discovered before usage avoiding the latency incurred in finding the route. These protocols require the nodes to maintain routing and network topology information through one or more tables. Any change in the network needs to be reflected in these tables by propagating the changes throughout the network. Examples of this class include DSDV, WRP, GSR and FSR. Reactive routing protocols: Reactive protocols try to conserve the precious battery power of the nodes by discovering routes only when it is required. Only when there is a packet to be transferred, the route discovery protocol is initiated by the source and the route is found. Because of this nature, this class of routing protocols is also called as "Dynamic routing protocols". Examples of this class include DSR, AODV and CBRP.

Security is a major concern in all forms of communication networks, but Ad-Hoc networks face the greatest challenge due their inherent nature. This can be attributed to the following four characteristics of Ad-Hoc networks[3,4]:

- Limited bandwidth
- Dynamic topology
- Absence of central control
- Limited battery power

Corresponding Author: Latha Tamilselvan, Department of Information Technology, Anna University, BSA Cresent Engineering College, Vandalur, Chennai, Tamilnadu, India

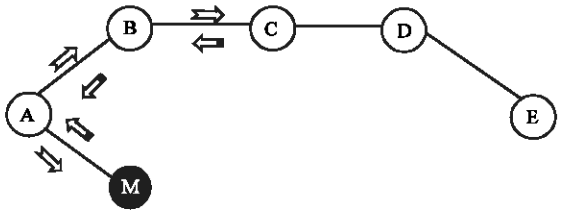
As a result, there exists a slew of attacks that can be performed on an Ad-Hoc network. The different attacks can be classified based on their nature as either passive or active attacks[5]. A passive attack attempts to illegitimately acquire valuable information by listening to the traffic without disrupting the operation of the routing protocol. Hence detection of passive attacks is highly difficult. On the other hand, active attacks alter the flow of data either by inserting false packets or by modifying the packet contents. Active attacks can further be classified into Internal and External attacks[6]. Internal attacks are caused by a node that belongs to the same network as the victim, whereas external attacks are caused by nodes that do not belong to that network.

The AODV protocol: The Ad Hoc on-demand Distance Vector (AODV) routing protocol is an adaptation of the DSDV protocol for dynamic link conditions[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.

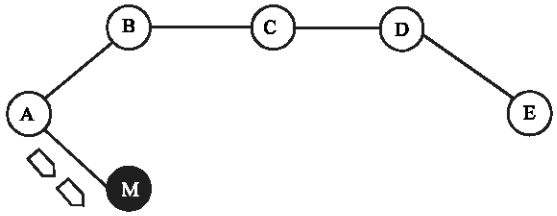
Black Hole attack: A Black Hole attack[4,5] is a kind of denial of service attack where a malicious node can attract all packets by falsely claiming a fresh route to the destination and then absorb them without forwarding them to the destination.

- RREQ packet
- RREP packet
- Data packet

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 the requested route to node 'E'.



Broadcast of RREQ Packet and Relay of RREP Packet with Black Hole



Transmission of Data Packets with Black Hole

RREQ packet **RREP packet**

Data packet

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 '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'.

Solution: BHR-AODV: We propose a solution that is an enhancement of the basic AODV routing protocol which will be able to identify and isolate Black Holes. The sequence numbers used in AODV for ordering the flow of data will be utilized in the solution.

Last seen and last sent sequence numbers: The solution requires the maintenance of two additional sequence numbers, namely 'Last Seen' and the 'Last Sent'

sequence numbers in each node's routing table. The Last Seen sequence number for a destination in a node's routing table is the sequence number of the last control packet (RREQ and RREP) issued by that destination intended for this node. It differs from the destination sequence number in that it is not updated by any intermediate node through which the control packet may traverse. To illustrate the difference, consider a node 'A' which broadcasts a RREQ for a particular destination 'D'. Any intermediate node that may receive a RREP packet in reply to the RREQ will update its destination sequence number for 'D', whereas only node 'A' can update the Last Seen sequence number for 'D'. The Last Seen sequence number will be updated:

- By the destination node, for the source, when it directly handles the route request.
- By the destination node, for the source, when it receives an intimation (Gratuitous Reply)[7] from the replying intermediate node.
- By the source, for the destination, when it receives the route reply.

Similarly, the Last Sent sequence number for a particular destination is the sequence number of the last sent control packet intended for that destination. The Last Sent sequence number will be updated:

- By the source node, for the destination, when it transmits the route request.
- By the destination node, for the source, when it directly transmits the route reply.
- By the destination node, for the source, when it receives an intimation (Gratuitous Reply) from the replying intermediate node.

The authenticity of a replying node is verified by comparing the last seen sequence number contained in the route reply and the last sent sequence number present in the routing Table.

Working of BHR-AODV: The initiator of the route discovery process needs to update the last sent sequence number for the destination in its routing table after sending a Route Request packet. But in order to ensure that the last sent sequence number is not updated when no route to the destination exists, it is copied on to a temporary structure until a route reply is received. When the intended destination receives the RREQ, it constructs and sends a RREP packet containing the last seen sequence number for the source.

It then updates the last seen and the last sent sequence numbers in its routing table. The last seen sequence number is updated to be the sequence number of the RREQ packet received and the last sent sequence number being the sequence number of the RREP packet sent. When an intermediate node that has a fresh route to the destination receives the RREQ packet, it constructs a gratuitous RREP packet containing the address of the next-hop neighbor toward the destination as one of the fields and sends it to the destination. The neighbor of the intermediate node which sent the gratuitous RREP packet does not relay this packet as such. Instead it checks if the 'next-hop' address contained in the gratuitous RREP packet matches with its own address. If it does, it looks up its routing Table 1 if it has a route to the specified destination.

If it contains a route, it then constructs an 'Authentication packet' containing the last seen sequence number present in its routing table corresponding to the source of the RREQ packet and sends it to the intermediate node which sent the gratuitous RREP packet. The node then relays the

Table 1: Working of BHR-AODV

```
Algorithm of BHR-AODV
Notations:
SN: Source Node          DN: Destination Node
IN : Intermediate Node NH: Next Hop of Intermediate Node
1. SN: Transmit (RREQ) broadcast
2. IN: Receive (RREQ)
      i. IF (IN has fresh route to destination) {
      Transmit (Gratuitous RREP) destination
      }
      ii. ELSE {
                  Relay (RREQ) broadcast
      }
3. NH: Receive (Gratuitous RREP)
      i. Transmit (Authentication Data) intermediate node
      ii. Relay (Gratuitous RREP) destination
4. DN: Receive (Gratuitous RREP)
      i. Update (last_seen, last_sent)
5. IN: Receive (Authentication Data)
      i. Transmit (RREP) source
6. SN: Receive (RREP)
      i. Compare (last_seen, last_sent)
      ii. IF (sequence numbers match) {
      Route_Date (secure route)
                  }
      iii. ELSE {
                  A. SN: Transmit (Probe) next hop
                  B. For each node in the suspected route
                        DO {
                        a. Receive (Probe)
                        b. Transmit (Check) previous hop
                        c. Transmit (Probe) next hop
                        d. Receive (Check)
                        e. Verify (Check)
                        } UNTIL [Verify (Check) =
FALSE]
                  C. Transmit (Alarm) broadcast
```

gratuitous RREP packet to the destination. The destination node after receiving the gratuitous RREP updates it routing table for both last seen and last sent sequence numbers. The intermediate node after receiving the 'Authentication data' packet from its neighbor constructs and sends a RREP containing the 'next-hop' address and the last seen sequence number from the authentication data packet to the source. The source node after receiving the RREP packet, extracts the last seen sequence number from it and compares it with its last sent sequence number corresponding the 'next-hop' node. If it matches, the node confirms that it is a valid route and starts sending packet across that node. If it does not match, the node assumes that there is a Black Hole in that route and initiates an Isolation process.

Isolation of the black hole: Once the source node identifies the presence of a Black Hole in a route, it initiates a process to identify and isolate the blackhole. The source node sends a 'Probe' packet to its neighbor in the suspected route and waits for a 'Check Packet' from the neighbor. If it is not received within 5* NODE_TRAVERSAL_TIME / 2, then the probe packet is resent for MAX_PROBE_RETRY times. The neighbor that receives a probe packet then constructs a check packet containing the last seen sequence number corresponding to the source node and sends it to the source node. In addition to this, the neighbor node sends a 'Probe' packet to its neighbor in the suspected route. So, the 'Probe' packet is relayed along the suspected route. Whenever a check packet is received, the authentication is carried out by comparing the last seen sequence number in the packet with the last sent sequence number for the replying node. Ultimately when a probe packet is sent to the malicious node, it can respond by either sending a check packet by fabricating a random last seen sequence number or fail to reply. If it fails to reply, then after resending the probe packets for MAX_PROBE_RETRY times the neighbor concludes that the next node is a Black Hole and broadcasts an alarm packet. If the malicious node fabricates the check packet, then the node which received the noncorrelating check packet identifies its neighbor as the 'Blackhole' and broadcasts an alarm packet with a TTL of NET_DIAMETER throughout the network and hence isolating the black-hole from the network.

Security of the solution: The security of the proposed solution is analyzed in this section. The security of the solution is achieved by authenticating the route claimed by the replying node. It is based on an assumption that authenticating the next hop of the replying intermediate node or the replying destination itself amounts to validating the route. The authenticity of the intermediate node or the destination is verified by comparing the last seen and last sent sequence numbers which act as a kind of shared key. Moreover, if the Black Hole tries to deceive by requesting the authentication data of any of its neighbor, it would fail as the neighbor first verifies that it has a route to the specified destination and only then sends the authentication data.

In addition to preventing malicious nodes from illegitimately absorbing data packets, the solution also tries to identify the Black Hole by using the probes. Once the Black Hole is identified, it can be isolated from the network and any further replies that it may issue can be discarded. The solution has the capability to identify and isolate any number of Black Holes present in the network with the exception of cooperative Black Holes.

Comparison with basic AODV: The solution secures the network from Black Hole attacks with minimum additional routing overhead and delay. The additional delay experienced by a source node before receiving a RREP is due to the additional hops incurred during the transmission of authentication data. The number of additional hops is one if an intermediate node replies and zero if the destination itself replies. The number of additional hops mentioned above remains the same for any number of nodes that may lie between the source and destination. In order to introduce even a minimal amount of security into the basic AODV protocol, it must be asserted that only the destination can reply for all route requests and the capability of the intermediate node to reply must be removed. Hence, the overhead associated rapidly increases as the number of nodes and hence the number of hops, increase in the network. This is much larger compared to the overhead involved in BHRAODV in the worst study. Moreover, the removal of the intermediate node's capability to reply does not guarantee freedom from Black Hole attacks, as the malicious node can claim to be the destination itself by sending an RREP packet. Since there is no authentication involved, there is no way that such behavior can be identified.

RESULTS AND DISCUSSION

For demonstrating the difference between AODV and BHR-AODV, a simulation with 6 nodes, node 1 to node 5 is run in the Glomosim simulator. The node 5 is assigned as the malicious node and node 0 is the source which transmits 1 data packet of 256 bytes each to every other legitimate node. The results of the simulation are tabulated (Table 2).

Table 2: Tabulation of simulation results for AODV and BHR AODV

Parameter	AODV	Bhr AODV
Number of Route Requests transmitted	4	4
Number of Routes Selected	4	4
Number of data packets transmitted	4	4
Number of replies fabricated by Malicious Node	4	4
Number of data packets absorbed	3	0
Number of Black Hole attempts detected	0	4
Number of data packets received	1	4

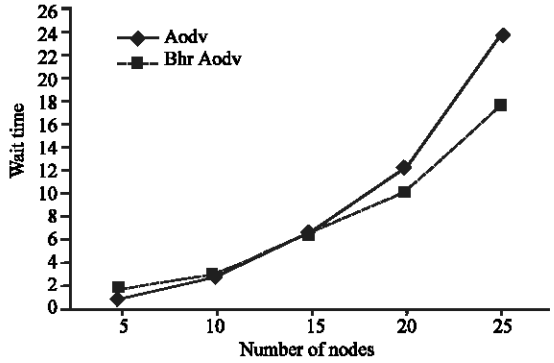


Fig. 1: Comparison of Average Wait Time between AODV and BHR AODV

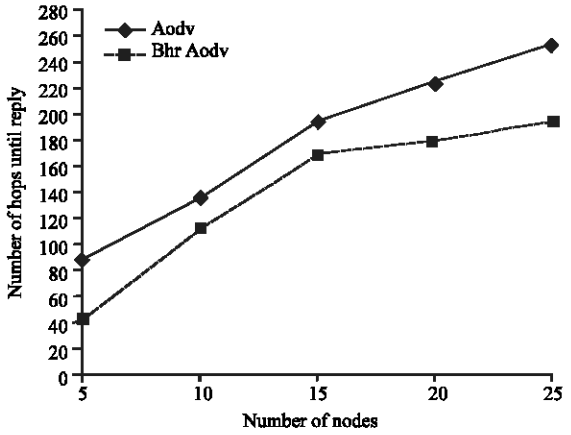


Fig. 2: Comparison of Average Number of Hops before RREP between AODV and BHR AODV

As is evident from the table below, three out four data packets is absorbed by the malicious Black Hole when the conventional AODV is employed. But the use of BHR-AODV results in the secure transmission of all data packets.

A more detailed comparison of the performance of AODV and BHR-AODV is done using the Glomosim simulator. Two parameters are measured for each of the protocols: The average wait time and the average number of hops before RREP. Both the parameters are directly related to the performance of the protocols. For the purpose of the simulation, measurements are made for a varying number of nodes ranging from 5 to 25. Also, the seed which is used for the generation of random numbers is also varied for consistency of the results.

Figure 1 the comparison of BHR AODV and AODV with number of nodes and wait time as X and Y axes respectively. It is evident from the graph that though the wait time for BHR AODV is slightly higher than AODV for lesser number of nodes, as the number of nodes increases, the wait time is much lesser when compared to AODV. This is because a smaller number of nodes imply more direct connections and hence the time saved from replies from intermediate nodes is not significant. But, the control overhead involved in BHR-AODV for a few nodes makes the delay greater than the delay for the basic AODV. But as the number of nodes in the network increase, the average distance between nodes in terms of the number of hops is much greater. Hence a huge amount of time in saved when an intermediate node replies. The time saved outweighs the additional overhead incurred heavily. Hence, the average wait time is much smaller compared to the basic AODV for more number of nodes.

Figure 2 illustrates the difference between AODV and BHR-AODV in terms of the number of hops traversed before a reply is issued. The X-axis contains the number of nodes in the network and the Y-axis contains the number of hops before RREP issued. It can be easily deduced from the graph that BHR-AODV consistently outperforms AODV in terms of the number of hops a RREQ packet must traverse before a reply is issued. Since BHR AODV provides security from Black Hole attacks without removing the ability of the intermediate nodes to reply, the average number of hops that a RREQ must traverse is much lesser than AODV. The difference in the number of hops becomes more significant as the number of nodes increase.

CONCLUSION

In this study we propose a strategy to counter the Black Hole attacks prevalent in Mobile Ad Hoc Networks. The solution is simulated using the Global Mobile Simulator and is found to achieve the required security with minimal additional delay and overhead. Our future work intends to be in the direction of simulating the protocol in a larger network and adapting this protocol for Ad Hoc networks susceptible to cooperative Black Hole and gray hole attacks and also to improve its efficiency during network start-up conditions.

REFERENCES

1. David B. Johnson, 1994. Routing in Ad Hoc Networks of Mobile Host, Proceedings of the IEEE workshop on Mobile Computing Systems and Applications.

2. Padmini Misra, Routing Protocols for Ad Hoc Mobile Wireless Networks, http://www.cis.ohio-state.edu/~misra.
3. Lidong zhou and Zygmunt J. Haas, 1999. Securing Ad Hoc Networks, IEEE network, special issue.
4. Hongmei Deng, Wei Li and Dharma P. Agarwal, 2002. RoutingSecurity in Wireless Ad Hoc Networks, IEEE Communications Magazine.
5. Yih-Chun Hu and Adrian Perrig, 2004. A Survey of Secure Wireless AdHoc Routing, IEEE Security and Privacy.
6. Dan Nguyen and Li Zhao, Pra-ornsiri Uisawang, John Platt, Secure Routing Analysis for Mobile Ad Hoc Networks.
7. Charles E. Perkins, Elizabeth M. Belding-Royer and Samir R. Das, 2003. Mobile Ad Hoc Networking Working Group, Internet Draft.
8. Jorge Nuevo, A Comprehensible GloMoSim Tutorial.