Enhancing the Routing Security in Mobile Ad-hoc Networks

N.Madhuri[1], Dr.B. Ananda Krishna[2]

[1]*Student, M.Tech, DECS, Gudlavalleru Engineering College, Gudlavalleru,*

[2]*Prof., ECE Department, Gudlavalleru Engineering College, Gudlavalleru*

Email:[1]madhu.honey57@gmail.com, anand_bk@rediffmail.com[2]

Abstract: Mobile adhoc networks assume no existing infrastructure is available for routing packets end-to-end in a network and instead rely on intermediary peers. There are many routing protocols that establish the routes between the nodes in the network. The control toward the management of the nodes in the MANET is distributed. This feature does not give assurance towards the security aspects of the network. Routing protocols, data, bandwidth and battery power are the common targets of various attacks that occurs in MANET. The routing attack addressed in this paper is the black hole attack. Most of the routing protocols do not address the issues of the routing attack. This paper proposes a solution strategy which will overcome the black hole attacks in MANETs, adapted on AODV protocol.

Keywords MANET, AODV, Black hole attack.

1. Introduction

A Mobile Ad hoc Network (MANET) consists of a set of mobile hosts that carry out basic networking functions like packet forwarding, routing, and service discovery without the help of an established infrastructure. Nodes of an ad hoc network rely on one another in forwarding a packet
to its destination, due to the limited range of each node's wireless transmissions. MANET provides a possibility of creating a network in situations where creating infrastructure is impossible or prohibitively expensive. Unlike a network with fixed infrastructure, mobile nodes in adhoc networks do not communicate through the fixed infrastructures.

2. Challenges of MANETS

The following list of challenges shows the inefficiencies and limitations that have to be overcome in a MANET environment [8]:

- Limited wireless transmission range
- Routing Overhead
- Battery constraints
- Asymmetric links
- Time-varying wireless link characteristics
- Broadcast nature of the wireless medium
- Packet losses due to transmission errors
- Mobility-induced route changes
- Potentially frequent network partitions
- Ease of snooping on wireless transmissions (security issues)

3. Types of Routing Protocols in MANETs

MANET routing protocols are classified as following:

3.1 Table Driven (Proactive) Routing protocols:

In these protocols, every node maintains one or more tables containing routing information to every node in the network. All nodes update these tables so as to maintain a consistent and up-to-date view of the network. These protocols are also called as proactive because routing information is maintained by them even before it is required. Since, these protocols maintain node entries for each and every node in the form of table; it causes more overhead in the routing table which leads to more bandwidth consumption. So these protocols are not unsuitable for larger networks. Table Driven Protocols are: Destination Sequence Distance Vector (DSDV) routing, Cluster-head Gateway Switch Routing (CGSR) and Wireless Routing Protocol (WRP). There are some differences among the protocols on the basis of routing information being updated in each routing table. [9]

3.2 On Demand (Reactive) Routing protocols:

On demand protocols obtain routes only on demand basis rather than maintaining a complete list of routing information all the time. The routes are created when desired by the source node. Whenever a node requires a route to destination a route discovery is initiated within the network. This process is completed once a route is found. Once a route is established, it is maintained by a route maintenance procedure till the destination becomes inaccessible or the route is not desired. On demand routing protocols include: Dynamic Source Routing (DSR) protocol, the Adhoc On demand Distance Vector (AODV) protocol, the Temporally Ordered Routing Algorithm (TORA), and the Associatively Based Routing (ABR) protocol [9].

3.3 Hybrid Routing Protocols:

In this, various approaches of routing protocols are combined to form a single protocol. ZRP (Zone Routing Protocol) is one of the hybrid protocols which are the combination of table-driven and on-demand routing protocol. It has the characteristics of adaptive to network conditions [10].

4. Overview of AODV Routing Protocol

AODV routing protocol uses a broadcast route discovery mechanism and it depends on dynamically established route. AODV builds routes by using a route request (RREQ)/ route reply (RREP) query cycle. When a source node requires a destination route for which it does not have a route already, it broadcasts RREQ packet across the network. The nodes receiving this packet update the information for the source node and sets up backward pointer information for the source node in the routing table [9], [10].

5. Attacks on Ad Hoc Networks

5.1 Black Hole Attack — in this attack, a malicious node uses the routing protocol to advertise itself as

having the shortest path to the node whose packets it wants to intercept. The attacker will then receive the traffic destined for other nodes and can then choose to drop the packets to perform a denial-of-service attack, or alternatively use its place on the route as the first step in a man-in-the-middle attack by redirecting the packets to nodes pretending to be the destination.

5.2 Spoofing — a node may attempt to take over the identity of another node. It then attempts to receive all the packets destined for the legitimate node, may advertise fake routes, and so on. This attack can be prevented simply by requiring each node to sign each routing message (assuming there is a key management infrastructure). Signing each message may increase the bandwidth overhead and the CPU utilization on each node.

5.3 Modifying Routing Packets in Transit — a node may modify a routing message sent by another node. Such modifications can be done with the intention of misleading other nodes. For example, sequence numbers in routing protocols such as AODV are used for indicating the freshness of routes. Nodes can launch attacks by modifying the sequence numbers so that recent route advertisements are ignored. Typically it is particularly difficult to detect the node which modified the routing message in transit. Requiring each node to sign each routing message can prevent these types of attacks. In such a case, if a node modifies routing packets, then it might escape undetected, but it will not be able to mislead other nodes because the routing messages will not have the appropriate signature. Other nodes can detect illegal modifications in the packet via the cryptographic protection mechanisms.

5.4 Packet Dropping — a node may advertise routes through itself to many other nodes and may start dropping the received packets rather than forwarding them to the next hop based on the routes advertised. Another variation of this attack is when a node drops packets containing routing messages. These types of attacks are a specific case of the more general packet dropping attacks.

6. Related Work

There indeed have been numerous attempts published in the literature that aim at countering the Black attacks. We survey them in the following. Many researchers have addressed the black hole attack problem in MANET. All the solutions proposed and implemented were based on AODV and DSDV protocol.

In [1]Karlsson *Jonny, Laurence S.Dooley et al.* proposed a contemporary review of MANET routing protocols is briefly presented. An overview of active attacks based that occur in MANET is presented. The importance of cryptography and trust in secure MANET routing is also outlined, with relevant security extensions of existing routing protocols for MANETs described and assessed. A comparison of existing secure routing protocols form the main contribution in this paper, while some future research challenges in secure MANET routing are discussed.

In [2] *Luo Junhai et al.* proposed a method to prevents the black hole attack by authentication mechanism. The authentication mechanism, based on the hash function, the Message Authentication Code (MAC), and Pseudo Random Function (PRF), is proposed for black hole prevention on top of Ad-hoc On-demand Distance Vector (AODV).

In [3] *M. Khalili shoja et al*. proposed a hash chain mechanism to prevent the black hole attack. Black hole attack is based on alteration of sequence number and hope count. In this mechanism, when an intermediate node receives RREQ or RREP, check an extra field to verify sequence number and hop count. The hash RREQ and hash RREP fields are add with RREQ and RREP field respectively. A seed value should be choose randomly for calculating hash function.

In [4] *K. Selvavinyaki et al*. uses the route discovery scheme of DSR to issue security certificates. Since there is no fixed infrastructure, nodes carry out all required tasks for security solutions including routing and authentication in a self organized manner.

In [5] *Mohammad Al.Shurman and Seong- Moo Yoo et al*. proposed two solutions for the black hole problem. The first is to find more than one route to the destination. The second is to exploit the packet sequence number included in any packet header. Computer simulation shows that compared to the original AODV routing scheme, the second solution can verify 75% to 98% of the route to the destination depending on the pause times at a minimum cost of the delay in the networks. Here, they had studied only one node attack to be in the route (not a group of attackers). The group attack for this problem should be studied.

In [6] Shabir Sofi , Eshan Malik, Rayees Baba, Hilal Baba , Roohies Mir et al. proposed the new algorithm for finding the intentional selective dropping attack by a node in the Black hole and Grey hole attack. The algorithm successfully attempted to detect and prevent Black Hole and Gray hole attacks using the concept of probability of attacks in AODV protocol, but with coplexity O(n).

In [7] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall et al. had studied the routing security issues and described the cooperative black hole attack that can be mounted against a MANET and proposed a feasible solution for it in AODV, to identify the multiple black hole nodes cooperating with each other in MANET and also to discover secure paths from source to destination by avoiding multiple black hole nodes acting in cooperation. Their future work is to study the impact of Gray hole nodes and techniques for their identification.

7. Security Mechanism

We provide a framework for avoiding Black hole attack in the Ad hoc On-demand Distance Vector (AODV) routing protocol. We have designed the mechanism that will ensure the proper data packet transmission and reception between the source and destination.

7.1 Route Discovery Process in AODV

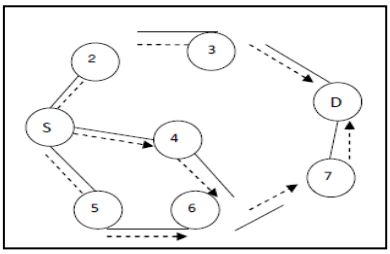

Fig. 1: Route Discovery Process

When a node needs to determine a route to a destination node, it floods the network with RREQ packets. The originating node broadcasts a RREQ packet to its neighboring nodes, which broadcast the packet to their neighbors, and so on as shown in figure 1. As these requests spread through the network, intermediate nodes store reverse routes back to the originating node. Since an intermediate node could have many reverse routes, it always picks the route with the smallest hop count.

When a node receiving the request either knows of a "fresh enough" route to the destination or is itself the destination, the node generates a RREP packet, and sends this packet along the reverse path back towards the originating node as shown in the figure 2. As the RREP packet passes through intermediate nodes, these nodes update their routing tables, so that in the future, packets can be routed through these nodes to the destination. Notice that it is possible for the RREQ originator to receive a RREP packet from more than one node. In this case, the RREQ originator will update its routing table with the most "recent" routing information; that is, it uses the route with the greatest destination sequence number.

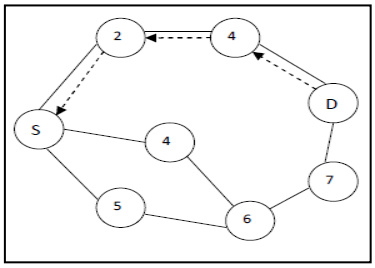

Fig. 2: Propagation of RREP Packet

8. Black Hole Problem in AODV

Consider an Ad Hoc Network in which the Source node (1) wants to send data packets to the Destination node (6). The Intermediate node (3) is assumed to be a Black Hole with no fresh enough route to node 5. Before transmitting the data packets, the node1 initiates a Route Discovery Process as shown in the figure 3.

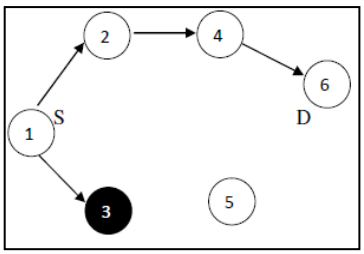

Fig. 3: Route Discovery Process

As node 3 is a Black Hole, whenever it receives a RREQ packet, it immediately sends a RREP packet stating that it has the shortest route to the destination node as shown in the figure 4.

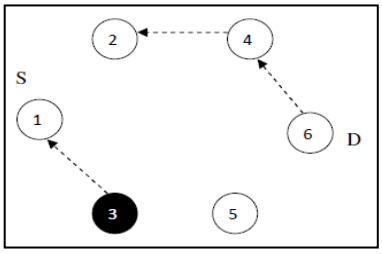

Fig.4: Propagation of RREP Packet

If the reply from a normal node reaches the source node of the RREQ packet first, everything works well; but the reply from node 3 could reach the source node first, since it is nearer to the source node. Moreover, a Black Hole does not need to check its routing table when sending a false message; its response is more likely to reach the source node first. This makes the source node to think that the route discovery process is complete, ignore all other reply packets, and begin to send data packets as shown in the figure 5. As a result, all the packets through the black hole are simply consumed or lost. This problem is called as the "Black Hole Problem" and in this way the Black Hole can misroute a lot of network traffic to it, and could cause an attack to the network.

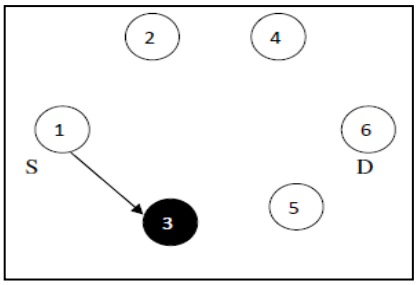

Fig. 5: Transmission of Data Packets

9. Proposed Solution

In our proposed method, every node in the network is required to append the one's complement of its own IP address in every RREQ packet it transmits. The node receiving the packet checks the authentication of its source by adding the appended one's complement and the source IP address known to it to get all ones. Any malicious node sneaking into the network does not know that it has to append the one's complement of its IP

address and thus any packet from such nodes get dropped by its neighbors. Also, once a node fails the test for authenticity, a broadcast is made to the whole network, warning all the nodes in the network of the presence of a malicious node and its IP address. This saves processing time, as any node receiving any packet from the malicious node can simply discard it without any further checking. Thus the malicious node is isolated from the network.

Along with the one's complement of IP address, we also install a TIMER in all the nodes. The Timer is switched ON when a RREQ packet is sent and the Timer is switched OFF when a RREP packet is received by the same node. Thus, the Timer's value denotes the time for receiving a Route Reply from its neighboring node. As the Black Holes immediately reply without checking the routing table and one's complement of IP address, the IP address doesn't matches and the Timer's value will be less when compared with a normal node. But the Timer's value will also be less when the destination node is nearer to the source node. To avoid this problem, the Timer's value is compared with the Threshold value. The Threshold value is the time required for receiving the route reply from a normal node. If the Timer's value is lesser than the Threshold value, then the node, which sent the RREP packet, is assumed to be a Black Hole. The strength of the proposed algorithm lies in

- One's complement of IP address gives simple authentication
- Without the knowledge of one's complement the malicious nodes can reply immediately lesser than the threshold value.

The algorithm for identification of malicious nodes and possible acts of the malicious nodes are given in the algorithm1, 2 and 3. To confirm the node to be a Black Hole, we do the following process shown in the figure 6.

Algorithm 1: Identification of malicious nodes

1. *Find the 1's complement of node's IP address*
2. *Switch on Timer and transmit RREQ packet*
3. *Neighboring nodes verify IP address by appending 1's complement and forward RREQ to the destination node*
4. *Destination node sends RREP packet*
5. *RREP reaches the source node*
6. *Check the received time and compare with the threshold value*
7. *Discard the RREP if the calculated time is much less than the threshold value*
8. *Raise the alarm and warn the neighboring nodes*

Algorithm 2: Malicious nodes without the knowledge of 1's complement

1. *Assume that malicious node enters the network*
2. *Receives the RREQ packet and sends RREP immediately acting as the destination without appending the 1's complement of IP address*
3. *RREP receives by a particular node confirms that it was sent by the malicious node*
4. *Immediately raise the alarm to the neighboring nodes*

Algorithm 3: Malicious nodes with the knowledge of 1's complement

1. *Assume that malicious node enters the network*
2. *Receives the RREQ packet and appends 1's complement on IP address and sends the RREP immediately acting as the destination*
3. *Source node calculate the receiving time and compares with the threshold value*
4. *If the calculated time < threshold value, confirms as malicious*
5. *If the calculated time > threshold value, source node yet to confirm*
6. *Perform further request and reply operation*

Figure 6: Proposed Algorithm

9.1 Further Request

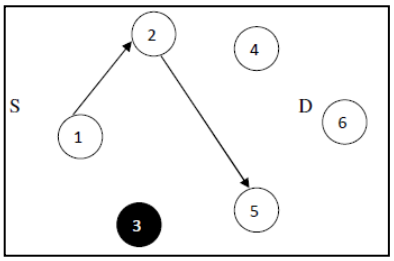

Fig. 7: Transmission of Further Request

In the proposed method, we require each intermediate node to send back the next hop information when it sends back a RREP packet. Thus, node 3 sends back the next hop information when it sends the RREP packet to source node 1. Here we assume the next hop it sends back is node 5. When node 1 receives the RREP packet from node 3, it does not send the data packets right away, but extracts the next hop information from the reply packet and then sends a Further Request to the next hop (node 5 as shown in the figure 7) to verify that it has a route to the intermediate node which sent the RREP packet, and that it has a route to the destination node. In response to the *Further Request*, the inquired intermediate node sends back a *Further Reply*.

9.2 Further Reply

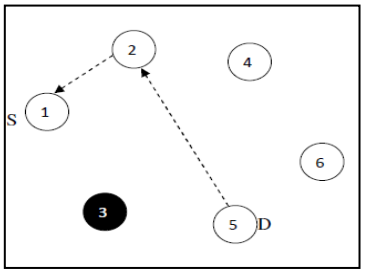

Fig. 8: Transmission of Further Reply

To avoid the problem of recursiveness, only the requested next hop can send back a Further Reply packet, which includes a Check Result. In our method, we ignore the Further Reply packet from the inquired intermediate node (node 3 as shown in the figure 3.10). Thus, we avoid the situation of the intermediate node taking further action such as fabricating the reply packet on behalf of the next hop node. When the source node receives the Further Reply from the *next hop*, it extracts the Check Result from the reply packet.

9.3 Check Result

The Check result may be of three types as follows:

Check Result	Explanation
1	Intermediate node is a Black Hole
2	Intermediate node is not a Black Hole
3	Initiate a new Route Discovery Process

Table 1: Values of Check Result

10. Implementation and Expected Results

The proposed security model is going to implement in the Glomosim with the following metrics to evaluate the efficiency in addition to the effectiveness of the protocols.

(i) **Average throughput**: Measured as the ratio of data packets delivered to the destinations to data packets originated by the sources. This number presents the routing efficiency of the protocol.

(ii) **Packet delivery ratio**: Measured as the ratio of the data packets delivered to the receivers to those data packets expected to be delivered.

(iii) **End-to-end delay:** Measured as the time interval from the moment that the source node sends a first message until the moment that the destination node in the network receives this last message. It also includes all possible delays caused by queuing at the interface, retransmission delays, and propagation and transfer times.

(iv) **Control overhead**: Measured as the number of control packets transmitted by all the nodes during the entire simulation.

(v) **Total overhead**: Measured as the ratio of the total packets transmitted (i.e., sum of control packets and data packets) to the data packets delivered.

11. Conclusion and Future Work

Our proposed security mechanism hopes to score over others by the fact that it is a very simple form of authentication avoiding complex cryptographic calculations reducing the processing overhead on the intermediate nodes. The work is going to implement Glomosim and to be analyzed.

REFERENCE

[1] Karlson, Jonny; Dooley, Laurence S. and Pulkkis, Goran (2012). Routing Security in Mobile Ad-hoc Networks. In: Informing Science and Information Technology Education 2012 Conference (InSITE'12), 22-27 June 2012, Montreal, Canada (Forthcoming).

[2] Junhai Luo, "Black Hole attack prevention based on authentication", In Communication Systems ICCS 2008, pages 173-177.

[3] M. khalili Shoja, Taheri,H.Vakilina, Iranian Conference Of Electrical Engineering,"Preventing Black Hole Attack Through Using A Hash Chain",May-2011,pages 1-6.

[4] K. Selvavinayaki, K.K Shyam Shankar, Dr. E.Karthikeyan, "Security enhanced DSR protocols to prevent black hole attacks in MANET", International Journal of Computer Applications (0975-8887) VOL7 NO-11, October-2010.

[5] Mohammad Al. Shurman and Seong –Moo Yoo, "Black Hole Attack in mobile adhoc Network", University of Albama.

[6] Shabir Sofi, Eshan Malik, Rayees Baba, Hilal Baba, Roohie Mir, "Analysis Of Byzantine Attacks In Adhoc Networks And Their Mitigation".

[7] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard, "Prevention Of Cooperative Black Hole Attack In Wireless Adhoc Networks".

[8] Kapang Lego, PranavKumar Singh, Dipankar Sutradhar, "Comparative Study Of Adhoc Routing Protocol AODV, DSR and DSDV in Mobile Adhoc Network" International Journal of Computer Science and Engineering VOL.1 NO.4364-371.

[9] E. M. Royer and C. K. Toh, "A Review of Current Routing Protocols Ad Hoc Mobile Wireless Networks", IEEE Personal Communications, April 1999, Volume 6, Number 2, pp: 46-55.

[10] C. E. Perkins and E. M. Royer, "Ad-hoc On-Demand Distance Vector Routing", Proceedings of the second IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, L.A.,1999, pp: 90-100.

[11] Ravinder Ahuja, "Simulation Based Performance Evaluation and Comparison of Reactive, Proactive and Hybrid Routing Protocols Based on Random Waypoint Mobility Model", International Journal of Computer Applications, October 2010, Volume 7, Number 11, pp: 20-24