ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2013

Securing MANETs Routing Protocol under Black Hole Attack

Harmandeep Singh[1], Manpreet Singh[2]

Research Scholar, Dept. of Information Technology, GNDEC, Ludhiana, India[1]

Assistant Professor, Dept. of Information Technology, GNDEC, Ludhiana, India[2]

Abstract: Wireless or mobile network is the new generation of wireless network that is different from the wired approach in many aspects like power and energy efficient routing protocols, routing configuration, network infrastructure. There are several protocols proposed for the deployment of MANETs in fields like government, military etc. In this paper we are proposing a technique to identify attack i.e. black hole attack and solution to avoid the black hole attack by discover a safe route for secure transmission. In this paper we focus on improving the security of the one of the popular MANET Routing Protocol namely as AODV.

Keywords: Ad Hoc Network, Black Hole, security, AODV.

I. INTRODUCTION

Wireless networks have poor constrained like bandwidth and resources with no infrastructure. Time to time every node in such network has to take care of its routing module itself that enhance the importance of security in mobile ad-hoc network due to high probability of attacks[7]. A collection of independent mobile users is called a Mobile Ad Hoc network. In this network nodes can communicate with available bandwidth and limited power constraints. Mobile nodes in MANETs change the network topology rapidly. There is a no central role in the MANETs[6] so the possibility of attacks[7] in various manners that breech the security and any security approach may be disqualify due to this that rely on recovery administrative services.

II. ROUTING PROTOCOLS

In ad-hoc network nodes are moving freely from one location to another so mobility of node the path established by a source may not be exist after a short interval of time. Routing determines the path from source to destination so that the nodes can communicate[4]. Routing Protocols for ad-hoc networks are reactive, proactive and hybrid.

Reactive protocols are also known as demand driven protocol because they find path when necessary. These protocols discover the new route by sending route request (flooding) and receiving route reply. Only the active route is maintain by the nodes. Due to route discovery the major drawback of these protocols is delay[12].

Proactive protocols are also known as Table Driven Protocols. The network topology is constantly maintained by these protocols. In a network every node keeps the information of the neighbours in advance. The different tables are used to keep the routing information and these tables are updated according to the changes in the network topology. The topology information is also exchange by the nodes so that they can have route information any time when they needed[5].

The combination of proactive protocols with reactive protocols is a *hybrid protocols*. They use distance-vector for more precise metrics to establish the best paths to destination networks. In this network each node has its own routing zones and the size of the zone is defined by a zone radius i.e. number of hops in one zone[6]. Each node keeps a record of routing information for its own zone. In hybrid protocols, routers only maintain information about the adjacent routers. Source initiate the establishment of routes to a given destination on demand during reactive operation.

A. AODV 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. The most distinguishing feature of AODV[1] compared to the other routing protocols is that it uses a destination sequence number for each route entry. The destination sequence number is generated by the destination when a connection is requested from it. Using the destination sequence number ensures loop freedom. AODV makes

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2013

sure the route to the destination does not contain a loop and is the shortest path. Route Requests (RREQs), Route Replay (RREPs), Route Errors (RERRs) are control messages used for establishing a path to the destination, sent using UDP/IP protocols. When the source node wants to make a connection with the destination node, it broadcasts an RREQ message[8],[9]. This RREQ message is propagated from the source, received by neighbors (intermediate nodes) of the source node. The intermediate nodes broad cast 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. Figure 1show how the RREQ message is propagated in an ad-hoc network[2].

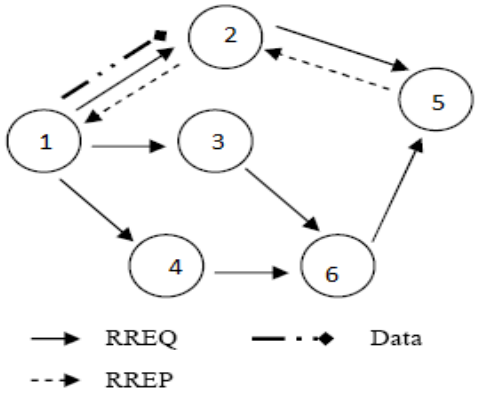

Fig. 1: RREQ & RREP Propagation from 1 to 5

Fresh enough means that the intermediate node has a valid route to destination formed a period of time ago, lower than the threshold. While the RREQ packet travels through the network, every intermediate node increases the hop count by one. If an RREQ message with the same RREQ ID is received, the node silently discards the newly received RREQs, controlling the ID field of the RREQ message[2]. When the destination node or intermediate node that has fresh enough route to the destination receive the RREQ message they create an RREP message and update their routing tables with accumulated hop count and the sequence number of the destination node. Afterwards the RREP message is unicasted to the source node.

III. BLACK HOLE ATTACK

In the following illustrated figure 2, imagine a malicious node 'M'. When node 'A' broadcasts a RREQ packet; nodes '2' '4' and 'M' receive it. Node 'M', being a malicious node, does not check up with its routing table for the requested route to node '5'. Hence, it immediately sends back a RREP packet, claiming a route to the destination. Node '1' Receives the RREP from 'M' ahead of the RREP from '2' and '4'.Node '1' assumes that the route through 'M' is the shortest route and sends any packet to the destination through it. When the node '1' sends data to 'M', it absorbs all the data and thus behaves like a 'Black hole'[7,12].

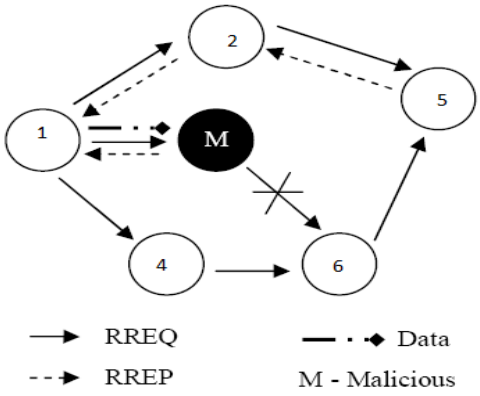

Fig.2: AODV BLACK HOLE ATTACK

IV. PROPOSED SOLUTION

To avoid Black Hole Attack[7] we enhance the basic AODV routing protocol. In this paper we proposed a solution to prevent any alternation in the default operation of either the intermediate node or that of the destination node. We basically modify the working of the source node by using additional function P_ReceiveReply(Packet P). We also

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2013

added a new table C_RREP_T, a timer M_WAIT_T and a variable M_Node to the data structures in the basic AODV protocol.

In AODV the source node accepts the first RREP request coming to it. According to our work we store all the RREPs in the newly created table i.e. C_RREP_T until the time, M_WAIT_T and we initialize this to be the half value of RREP_WAIT_TIME i.e. the time for which the source node wait for RREP control messages before regenerating RREQ. But according to our solution after receiving the first RREP control message source node has wait for M_WAIT_T and save all the coming RREP control messages in C_RREP_T table.

The source node analyses all the stored RREPs from C_RREP_T table and discard the request reply having very high destination sequence number. The node who sent the high sequence number is identify as malicious node and after that the source node selects a reply having highest destination sequence number from the C_RREP_T table. So with the help of our proposed solution the malicious node as M_Node is identified and in future source node can discard the message coming from that node and routing table for that node is not maintained[2].

```
At Source Node: AODV
1  ReceiveReply (Packet P){
2    if(P has an entry in Route Table){
3      select Dest_Seq_No from routing table
4        if(P.Dest_Seq_No > Dest_Seq_No){
5          update entry of P in routing table
6          unicast data packets to the route
           specified in RREP
7        }
8        else {
9            discard RREP
10       }
11     }
13     else {
14       if(P.Dest_Seq_No >= Src_Seq_No){
15         Make entry of P in routing table
16       }
17       else {
18         discard this RREP
19       }
20     }
21   }
```

Fig. 3: RecvReply pseudocode

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2013

```
The Proposed Algorithm : at Source Node:
1 Pre_ReceiveReply (Packet P){

2    t0 = get(current time value)
3    t1=t0 +   M_WAIT_T
4    while(CURRENT_TIME <= t1){
5      Store P.Dest_Seq_No and P.NODE_ID In
         C_RREP_T   table
     }
6    while ( C_RREP_T   is not empty) {
7      Select Dest_Seq_No from table
8      if (Dest_Seq_No >>>=Src_Seq_No){
9            M_Node=Node_Id
10         discard entry from table
11     }
12   }
13   select Packet q for Node_Id having
     highest value of Dest_Seq_No
14   ReceiveReply(Packet q)
15  }
```

Fig. 4 Pseudocode of Our Solution

The control messages are not added in the existing AODV so the normalized routing have minimum chance i.e. the ratio of number of control packets to data transmission in a simulation. The proposed solution is overhead in time in terms of the M_WAIT_T and the time required to execute the Pre_receivereply().

V. SIMULATION ENVIRONMENT

A. Criteria: For simulation, we have used NS-2[2.34] network simulator[10]. Mobility scenarios are generated by using a random way point model by varying 10 to 100 nodes moving in simulation area of 1000m x 1000m. We have used the following parameters.

TABLE 1
SIMULATION PARAMETERS

Simulator	NS-2 (version 2.34)
Simulation Time	200 (s)
Number of Nodes	10 to 60
Simulation Area	1000 x 1000m
Routing Protocol	AODV
Traffic	CBR (Constant Bit Rate)
Pause Time	5 (m/s)
Mobility	10-60m/s
Transmission Range	300m
No. Of Malicious Node	1

B. Metrics: The metrics used to evaluate the performance are given below:

1.) *Packet Delivery Ratio:* It is the ratio between the number of packets send by the sources and the number of packets received by the destination.

2.) *Average End-to-End Delay*: This is the average delay between the sending of the data packet by the sourceand its corresponding receiver. It includes all the delays caused during route acquisition, buffering andprocessing at intermediate nodes, retransmission delays in milliseconds.

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2013

3.) *Throughput:* Also known as normalized throughput. It is the ratio of overall the number of packets received by the CBR sink to the number of packets sent by the CBR source.

VI. SIMULATION RESULTS

After taking into consideration the simulation parameters mentioned in Table 1 we came across the following results:

TABLE 2
Simulation Results of AODV without Black Hole attack.

Protocol	Number of Nodes	Packet Delivery Ratio	Average End to End Delay	Throughput %
AODV without Black Hole Attack	10	81	0.12	78
	20	72	0.17	67
	30	61	0.21	57
	40	54	0.15	51
	50	52	0.33	49
	60	47	0.27	43

TABLE 3
Simulation Results of AODV with Black Hole attack

Protocol	Number of Nodes	Packet Delivery Ratio	Average End to End Delay	Throughput %
AODV with Black Hole Attack	10	68	0.04	66
	20	63	0.14	49
	30	54	0.17	46
	40	41	0.15	40
	50	37	0.23	35
	60	32	0.13	31

TABLE 4
Simulation Results of Secure AODV

Protocol	Number of Nodes	Packet Delivery Ratio	Average End to End Delay	Throughput %
Secure AODV	10	97	0.031	97
	20	90	0.13	87
	30	77	0.126	75
	40	75	0.183	73
	50	72	0.122	71
	60	69	0.155	67

VII. CONCLUSION

In this study we analyzed the effects of back holes in ad hoc wireless networks. We implemented an AODV protocol that simulates the behaviour of a black hole in NS-2.In this method we have used very simple and effective way of providing security in AODV against black hole attack that causes the interception and confidentiality of the ad hoc wireless networks. The solution detects the malicious nodes and isolates it from the active data forwarding. As from the graphs illustrated in results we can easily infer that the performance of the normal AODV drops under the presence of

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2013

black hole attack. Though the algorithm is implemented and simulated with AODV routing algorithm, we believe that the solution can also be used by other routing algorithm as well.

ACKNOWLEDGMENT

I express my sincere gratitude to my guide Mr. Manpreet Singh, for his valuable guidance and advice. Also I would like to thanks all the faculty members and colleagues for their continuous support and encouragement.

REFERENCES

[1]. Ilyas Mohammad," The Handbook of Ad Hoc Wireless Networks" ISBN-0-8493-1332-5, 2002.

[2]. Mishra Amitabh, "Security and Quality of service in Ad Hoc Wireless Networks" ,chapter 1-3, Handbook ISBN- 13 978-0-521-87824-1, 2005.

[3]. Singh Harmandeep, Singh Gurpreet and Singh Manpreet, " Performance Evaluation of Mobile Ad Hoc Network Routing Protocols Under Black Hole Attack", International Journal of Computer Applications, Vol. 42(18) , pp.1-6,2012.

[4]. Goyal Priyanka, Parmar Vinti, Rishi Rahul, " MANET: Vulnerabilities, Challenges, Attacks, Application", International Journal of Computational Engineering & Management (IJCEM), pp. 32-37, 2011.

[5]. Khare Shashank, Dixit Namrata and Agrawal Sumit,''Simulation and Analysis of Security inRouting Protocol to Avoid Threat of Black Hole Attack in MANET", VSRD-IJEECE, Vol. 2 (8),pp. 594-602, 2012.

[6]. Chandra Subash, Mandhata , Dr.Suryn Patro, "A counter measure to Black hole attack on AODVbased Mobile Ad-Hoc Networks", International Journal of Computer & Communication Technology (IJCCT), Volume-2, Issue-VI, 2011.

[7]. Singh Jatinder Pal, Gupta Anuj Kr., "Protocol Stack Based Security Vulnerabilities in MANETs", International Journal of Computer Applications, Volume 69– No.21, 2013.

[8]. Kurosawa Satoshi, Nakayama Hidehisa, Kato Nei, Jamalipour Abbas and Yoshiaki Nemoto,"Detecting Black hole Attack on AODV based Mobile Ad hoc networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, No.3, PP.338–346, 2007.

[9]. W. Li, H. Deng, Agrawal, D.P.,"Routing security in wireless Ad-Hoc networks", IEEE Communications Magazine, Vol.40, ISSN: 0163-6804, pp.70- 75, 2002.

[10]. Candolin, C. Kari, H. H., "A Security Architecture for Wireless Ad Hoc Networks", pp. 1095-1100, 2002.

[11]. Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", springer, pp. 1-38, 2006.

[12]. Loay Abusalah, Ashfaq Khokhar and Mohsen Guizani, "A Survey of Secure Mobile Ad Hoc Routing Protocols" IEEE Communications Surveys& Tutorials, VOL. 10, NO. 4, Fourth Quarter, 2008.

[13]. Gurjar A.A., Dande A. A., "Black Hole Attack in Manets: A Review Study", International Journal of IT, Engineering and Applied Sciences Research (IJIEASR) ISSN: 2319-4413 Volume 2, No. 3, 2013.

[14]. Şen Sevil, A. Clark John, E. Tapiador Jaun, "Security Threats in Mobile Ad Hoc Networks" Department of Computer Science,University of York, YO10 5DD, UK., pp. 1-22, 2010.

[15]. Gupta Anuj, Kaur Navjot, Kaur Amandeep, "A Survey on Behaviour of AODV and OLSR Routing Protocol of Manets under Black Hole Attack", IJCST Vol. 2, Issue 4, pp. 349-352, 2011.

[16]. Kumar Jaspal, Kulkarni M., Gupta Daya," Effect of Black Hole Attack on MANET Routing Protocols", I. J. Computer Network and Information Security, vol. 5, pp. 64-72, 2013.

[17]. Preeti Kamra, Singh Tanu Preet, Singh R.K, "Preventing Black hole Attacks in Mobile adhoc Networks: A Review", Recent Trends In Computing and Communication Engineering – RTCCE, PP. 285-287, 2013.