Volume 5, Issue 12, December 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Intrusion Detection System for Blackhole in MANETs

[1]Devendra Singh, [2]Anuj Singh, [3]S.S. Bedi

[1, 2] Department of Computer Science and Engineering, IFTM University, Moradabad, Uttar Pradesh, India

[3] MJP Rohilkhand University, Bareilly, Uttar Pradesh, India

Abstract*—A Wireless ad-hoc network is a makeshift scoop net set up by wireless mobile computers (or nodes) moving licentious-in the places that have no network facilities. Since the nodes demonstrate with each other, they bear company, by forwarding data packets to other nodes in the network. Thus the nodes find a driveway to the right way node using routing protocols. However, due to rampart permeability of the routing protocols, wireless ad-hoc networks are unsafe to invasion of the felonious nodes. One of these attacks is the Black Hole Attack anti,network righteousness intriguing all data packets in the network. Since the data parcel do not reach the right way node on account of this attack, data damage will occur. There are lots of Investigate and security mechanisms to Dismissal pusher, that carry out the black hole assail. In this thesis, i simulated the black hole attack in various wireless ad-hoc network under plot and have tried to find a reactant system in simulations.

Keywords*— Black Hole Attack; Intrusion Detection System; protecting; Simulation; Wireless Ad-hoc Network;

I. INTRODUCTION

Wireless ad-hoc networks are easily of self governing nodes that are oneself- managed without any infrastructure. In ad-hoc networks have a dynamic topology such that nodes can very-easily link or break the network at any time. They have various probable applications, in particular, in military and rescue areas such as joining soldiers men on the battlefield or placed a new network instead of a network which collapsed after a disaster like an earthquake. Ad-hoc networks are suitable for areas where it is not construct easily to set up a fixed infrastructure. Since the nodes communicate with each other without an infrastructure, the communication between the nodes by forwarding packets over themselves. To support this, nodes using some routing protocols (AODV, DSR, DSDV). Besides acting as a host, every node also acts as a router to search a path and transfer packets to the correct node in the network. As wireless ad-hoc networks lack of infrastructure, they are very prone to attacks. One of these attacks is the Black Hole attack. In this attack, intruder node absorbs all packets in itself, similar to a hole which sucks in everything in. In this way, all packets in the network are dropped. An intruder node drops all the traffic in the network. An intruder node makes use of the permeability of the route search packets of the on demand protocols, such as AODV. In route search process of AODV protocol, in-between nodes are responsible to find a new path to the right way, sending search parcel to the neighbor nodes. Malicious nodes do not use this process and instead, they quickly respond to the source node with wrong information as though it has fresh enough path to the destination nodes Therefore parcel sending node sends its data parcel via the intruder node to the destination, assuming it is a right path. Black Hole attack may occur due to a injured node which is deliberately wrong behave, as well as a injured node interface. In any case, nodes in the network will constantly try to search a path for the end station, which makes the node consumes its battery in joining to losing packets. We simulated the Black Hole attack in wireless ad-hoc networks and evaluated its damage in the network. We built up our simulations using NS-2 simulation program that consists of all network protocols to simulate many of the current network topologies. Even though NS-2 contains wireless ad-hoc routing protocols, it does not have any modules to emulate felonious protocols. Thus, to simulate blackHole offensive, we first joining a new protocol into the NS-2. We open our study by writing a new AODV protocol using C++. Having implemented a fresh routing protocol which simulates the blackhole we performed tests on different topological to compare the network equally with and without blackhole in the network. As expected, the flow capacity in the network was deteriorated considerably in the impendence of a blackhole. Afterwards, we proposed an IDS solution to eliminate the blackhole effects in the AODV network.

Rest of the paper is organized as follows. Section 2 present the background of blackhole detection in Manets. Section 3 discusses the blackhole attacks. Section 4 discusses the proposed solution to the attack. Section 5 discusses the simulation parameters used in simulation part. Section 6 discusses the IDS for blackhole. In section 7, results and analysis are discussed. Finally, conclusion and future work are discussed in section 8.

II. BACKGROUND

Nital Mistry et. al.[1] has proposed an algorithm to counter blackhole attack against the AODV routing protocol. It has been observed that the proposed modification to secure AODV is indeed effective in preventing the blackhole attacks with marginal performance punishment. A blackhole attack is one of the active DoS attacks believable in MANETs.

Jaspal Kumar et. al. [2] have been analyzed the effects of Black hole attack on mobile ad hoc routing protocols. AODV and maximize AODV have been fully considered. Simulation has been performed on the basis of performance parameters and effect has been analyzed after adding blackhole nodes in the network. It is an enhanced version of AODV and is hybrid in nature

Sarita Choudhary et.al. [3] proposed a complete protocol for detection & removal of networking Black/Gray Holes by using OPNET network simulator 14.5; considering two another networks with 15 nodes and 35 nodes in network and evaluating a security attack against MANET as a network, another statistics or performance metrics Packet loss, Packet delivery ratio and Average end to end delay has been used

Akanksha Saini et. al [4] includes the behavior of the Black Hole node studied by considering different scenarios. Performance of the Black Hole ADOV protocol has been analyzed by varying the number of mobile nodes and black hole nodes. The protocol is analyzed on different performance metrics like packet loss, packet delivery ratio and average end to end delay. It is observed that the impact on packet loss is much lower as compare to effect on delay.

In [5], authors proposed a sequenced based method which is stored in the RREP table, calculating the difference between the sequence numbers of nodes. If there are high difference in the sequence number then it comes under the doubted case. To analysis the performance PDR and packet loss have been used.

III. ATTACK IN MANET

A blackhole attack is one of the active DoS attacks possible in MANETs. In Figure 1, a malicious node(9) sends a false RREP packet to a source node(7) that initiated the route discovery, in order to pose itself as a destination node(10) or an immediate neighbor to the actual destination node. In such a case, the source node(7) would forward all of its data packets to the malicious node(9), eventually may never forward any of the data packets to the genuine destination(10). As a result, therefore, the source and the destination nodes became unable to communicate with each other. Since AODV treats RREP messages having higher value of destination sequence number to be fresher, the malicious node will always send the RREP having the highest possible value of destination sequence number. Such RREP message, when received by source node is treated a fresh. The fallout is that there is a high probability of a malicious node attempting to orchestrate the blackhole attacks in AODV. A blackhole is a malicious node that not right way replies the route requests that it has a fresh route to destination and then it drops all the receiving packets. The impairment will be serious if malicious nodes work team wise as a group. This type of attack is called cooperative black hole attack.

IV. PURPOSED METHOD (SECUENCE NUMBER)

Sequence Numbers serve as time stamps and allow nodes to compare how fresh their information on the different node. A node sends any type of routing control message, RREQ, RREP, RERR etc., it maximize its own sequence number. Max sequence number is more truly information and whichever is considered and path is established over this node

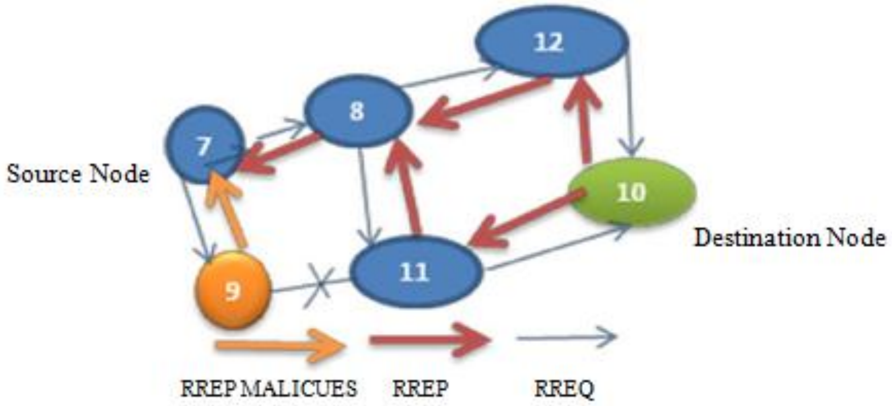


Figure 1. blackhole attack in network

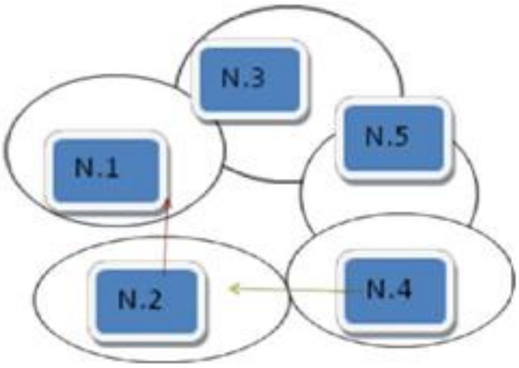
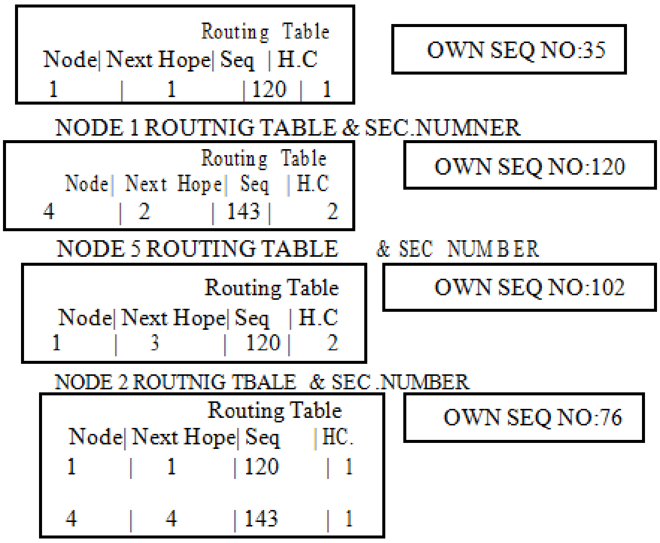


Figure 2. Sequence number and routing table for nodes

NODE 3 ROUNTING TBALE & SEC NUMBER



Routing Table
Node| Next Hope| Seq | H.C
1 | 1 | 120 | 1

OWN SEQ NO:35

NODE 1 ROUTNIG TABLE & SEC.NUMNER

Routing Table
Node| Next Hope| Seq | H.C
4 | 2 | 143 | 2

OWN SEQ NO:120

NODE 5 ROUTING TABLE & SEC NUMBER

Routing Table
Node| Next Hope| Seq | H.C
1 | 3 | 120 | 2

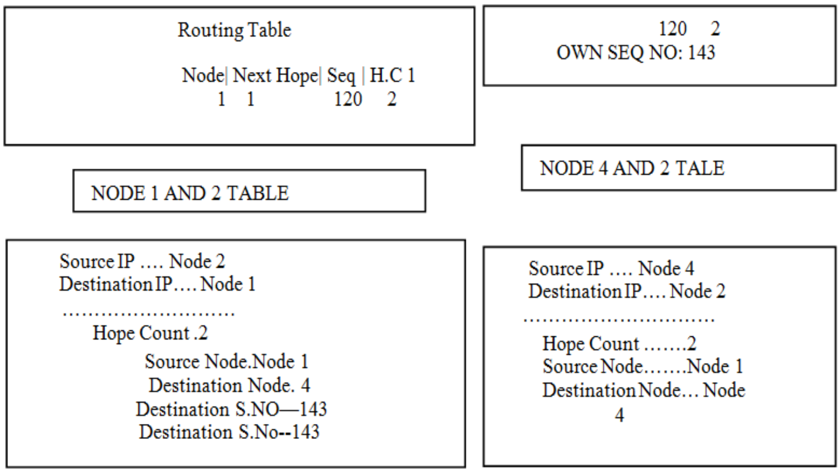
OWN SEQ NO:102

NODE 2 ROUTNIG TBALE & SEC.NUMBER

Routing Table
Node| Next Hope| Seq | HC.
1 | 1 | 120 | 1
4 | 4 | 143 | 1

OWN SEQ NO:76

NODE 4 ROUTING TABLE & SEC.NUMBER



Routing Table

Node| Next Hope| Seq | H.C 1
1 1 120 2

120 2
OWN SEQ NO: 143

NODE 1 AND 2 TABLE

NODE 4 AND 2 TALE

Source IP .... Node 2
Destination IP.... Node 1
....
Hope Count .2
Source Node.Node 1
Destination Node. 4
Destination S.NO—143
Destination S.No--143

Source IP .... Node 4
Destination IP.... Node 2
....
Hope Count 2
Source Node.......Node 1
Destination Node... Node 4

by the another nodes. The sequence number is a 32-bit unsigned integer value (i.e. 4294967295). If the sequence number of the node reaches the possible highest sequence number, 4294967295, then it will be set to zero (0) again. If the results of subtraction of the currently stored sequence number in a node and the sequence number of incoming AODV route control message is lower than zero, the stored sequence number is changed with the sequence number of the incoming control message In Figure 2, while Node 2 forwards the RREP message coming from Node 3, compares its own previously stored sequence number with that of Node 3. If assessment that the sequence number is newer than its own, then it modify its route table entry as necessary.

V. NETWORK SIMULATIONS

To examine the effects of black holes we simulated ad-hoc network scenarios with barring a black hole node present in the network. To be able to do that we introduced a new protocol, which we called "BlackholeAODV" into the ns-2. Nodes which are marked as blackholes adopted this protocol and behaved exactly similar blackholes as described above. To test this protocol we used 2 simulations of a small network. In the first scenario, we did not use any black hole nodes and in the second scenario, we added a black hole node to the simulation. We then compared the results of the simulations. CBR is used in both that generates constant packets through the UDP connection. CBR packet size is select to be 512 bytes, and data rate is set to 1 Mbt. Duration of the scenarios is (18+2)seconds and the CBR connections started at time equals to 1.0 seconds and continued until the end of the simulation in a 500 x 500 meter. A black hole node is included in the snare for the second simulation. In this setup the even numbered nodes are the sending nodes and odd numbered nodes are the receiving nodes. For example Node 6 is transmitting to Node 7, Node 8 to Node 9, Node 10 to Node 11,Node 12 to Node 13,Node 14to Node 15,Node 16 to Node 17Node 18 to Node 19. Node 22 and Node 23are used as black holes. Thus, we could numerate the sent and received packets between any two nodes. We could also numerate the number of packets dropped at each node including the black hole node. The packet loss in an ad-hoc network without any felonious nodes is presented in Table 1. In the second we introduced one malicious node that carries out the blackhole attack in the network. In this case node 24 acted as a blackhole and node 25 was silent. We measured the number of parcel sent by the source node and received by the destination node. We also tried to evaluate how many of the packets that could not reach the destination node are exploited in the black hole. These are also shown in figure 3.

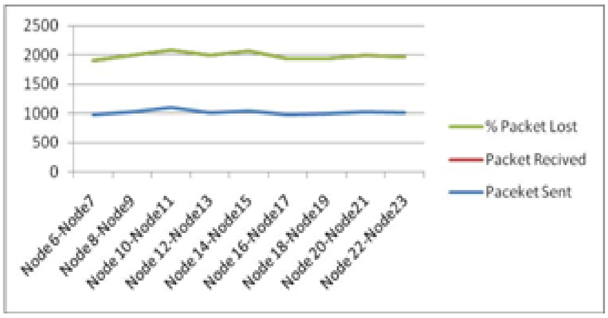
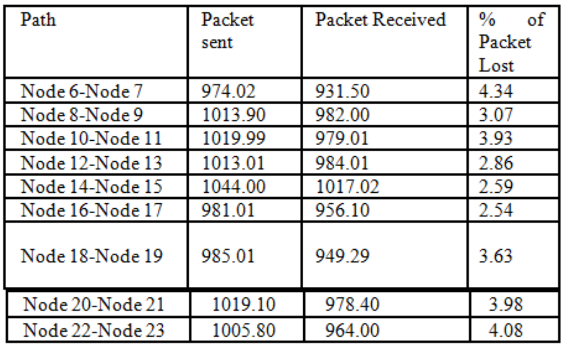


Figure 3. Packet sent, Packet Recieved and Packet Lost

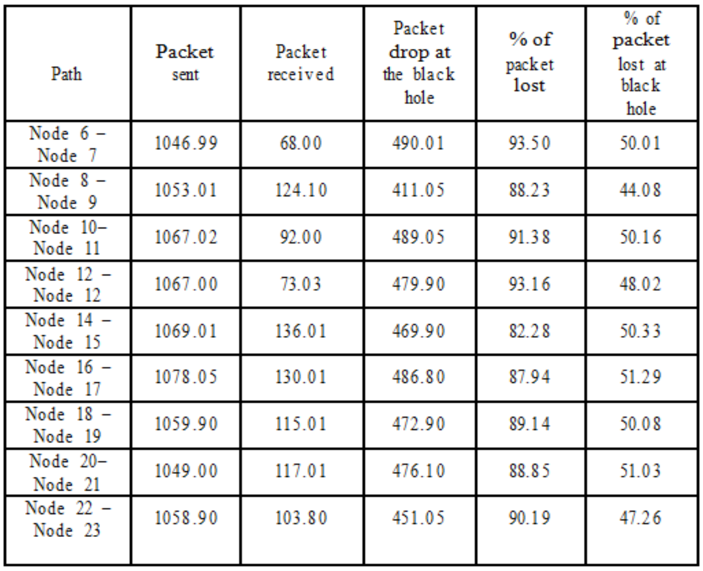
Table1. Packet loss percentages in an ad hoc network



Path	Packet sent	Packet Received	% of Packet Lost
Node 6-Node 7	974.02	931.50	4.34
Node 8-Node 9	1013.90	982.00	3.07
Node 10-Node 11	1019.99	979.01	3.93
Node 12-Node 13	1013.01	984.01	2.86
Node 14-Node 15	1044.00	1017.02	2.59
Node 16-Node 17	981.01	956.10	2.54
Node 18-Node 19	985.01	949.29	3.63
Node 20-Node 21	1019.10	978.40	3.98
Node 22-Node 23	1005.80	964.00	4.08

The results of these two simulations to understand the network and node behaviour. The results of the simulation demonstrate that the packet loss in the network with a black hole maximize beyond that dropped by the blackhole node. This we assumed to be due to maximized congestion in the routes towards the black hole node. We use these calculations again and again for 2 black holes and the results are presented in Table 2. The average of only 5 scenarios are used here and both node 24 and node 25 were assigned Black hole. Ad hoc networks may also experience packet loss due to parameters employed. In our 100 simulations of a normal AODV network, we saw that data loss showed variations of up to %40 as the network parameters such as the distribution of the nodes changed.

Table 2. Packet loss percentages in an ad hoc network with two black holes



Path	Packet sent	Packet received	Packet drop at the black hole	% of packet lost	% of packet lost at black hole
Node 6 – Node 7	1046.99	68.00	490.01	93.50	50.01
Node 8 – Node 9	1053.01	124.10	411.05	88.23	44.08
Node 10– Node 11	1067.02	92.00	489.05	91.38	50.16
Node 12 – Node 12	1067.00	73.03	479.90	93.16	48.02
Node 14 – Node 15	1069.01	136.01	469.90	82.28	50.33
Node 16 – Node 17	1078.05	130.01	486.80	87.94	51.29
Node 18 – Node 19	1059.90	115.01	472.90	89.14	50.08
Node 20– Node 21	1049.00	117.01	476.10	88.85	51.03
Node 22 – Node 23	1058.90	103.80	451.05	90.19	47.26

VI. SIMULATION OF IDSAODV AND EVALUATION OF RESULTS

When AODV protocol is used, RREP message arrived from different possible routes and in the cases we tested for example one arrived at the source on average at t= 1.2765 seconds as opposed to the RREP message arriving from the blackhole node on average at t= 0.2059 seconds. It is reasonable to assume that an RREP message will arrive from the black hole earlier than the actual destination with a higher probability as the black hole does not waste any time by checking the tables. In some cases, this idea may not work. For instance the second RREP can be received at the source node from an intermediate node which has stale information about the destination node or the second RREP message may come from the black hole node. If the real destination node is nearer than the black hole node. Based on the above reason and scan we chose to use the second route for message delivery and investigated if this approach increase the network performance under the black hole attacks in an ad-hoc network. We implemented a new protocol which we say IDSAODV in ns-2. In this approach we used the first RREP message to initiate the data shifting but if a second RREP message arrived then we switched to the new path. To be able to evaluate if our solution increase the performance we used the same scenarios and simulation parameters as described already. Table 3 shows that the proposed approach reduced the packet loss by about 5.14%, The proposed protocol does not requisiteness any more packets to be transmitted and the protocol packets have not been modifed

Table 3. packet loss percentages in an ad hoc network using idsaodv protocol

Packet	Packet Sent	Packet Received	Packet Lost %
Node 6 – Node 7	975.05	901.90	7.50
Node 8 – Node 9	1007.10	930.95	7.56
Node 10– Node 11	1000.15	942.10	5.79
Node 12 – Node 13	1016.80	939.12	7.57
Node 14 – Node 15	1014.80	961.95	5.14
Node 16 – Node 17	993.12	932.40	6.11
Node 18 – Node 19	987.10	916.50	7.15
Node 20– Node 21	985.90	905.10	8.12
Node 22- Node 23	989.20	923.15	6.66

VII. CONCLUSSION & FUTURE WORK

Finally after doing various comparisons, it can be concluded that the blackhole effects the AODV protocol. Effect on packet loss is much lower as resemblance to effect on delay. As malicious node is the main security threat that effects the performance of the AODV routing protocol. Even though, the packet loss can be happen due to network issues for this reason we implement a Intrusion Detection System to detect the malicious node(s) from the network. It is proved that our IDS does not affect the performance of the network and does not create extra traffic in the network. Detection of intruder node is the main matter of concern. Therefore the work can be extended by implementing some mechanisms to detect the Black Hole attack. Improvement for overcoming the effect of Black Hole should orient towards controlling the delay. In future some techniques should be proposed for lessen the effect of Black Hole. Also Black hole for AODV routing algorithm can be implemented in real life scenario and its analysis can be compared with the analysis result and its analysis can be compared with the analysis result.

REFERENCES

[1] Mistry N, Jinwala DC, IAENG, Zaveri M (2010) Improving AODV Protocol Against Blackhole Attacks. Paper presented at the International MultiConference of Engineers and Computer Scientists, Hong Kong, 17-19 March, 2010.

[2] Jaspal Kumar, M. Kulkarni, Daya Gupta,” Effect of Black Hole Attack on MANET Routing Protocols”, Published Online April 2013 in MECS (http://www.mecs-press.org/), I. J. Computer Network and Information Security, 2013, 5, 64-72http://moment.cs.ucsb.edu/pub/rfc3561.txt

[3] Sarita Choudhary, Kriti Sachdeva,” Discovering a Secure Path in MANET by Avoiding Black/Gray Holes”,published in International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-1, Issue-3, August 2012

[4] Akanksha Saini, Harish Kumar,” Effect Of Black Hole Attack On AODV Routing Protocol In MANET”, International Journal of Computer Science and Technology.

[5] Vipan Chand Sharma, Atul Gupta, Vivek Dimri,” Detection of Black Hole Attack in MANET under AODV Routing Protocol”, Volume 3, Issue 6, June 2013 International Journal of Advanced Research in Computer Science and Software Engineering.

[6] http://en.wikipedia.org/wiki/Personal_area_network, 25 July 2005.

[7] T. Franklin, “Wireless Local Area Networks”, Technical Report http://www.jisc.ac.uk/uploaded_documents/WirelessLANTechRep.pdf. July2005

[8] http://certifications.wi-fi.org/wbcs_certified_products.php 25 July 2005.

[9] P. Misra,. “Routing Protocols for Ad Hoc Mobile Wireless Networks”, http://www.cse.wustl.edu/~jain/cis788-99/adhoc_routing/index.html, 14 May 2006.

[10] http://en.wikipedia.org/wiki/Personal_area_network, 25 July 2005.

[11] J. Reynold, “Going Wi-Fi”, Chapter 6, The Wi-Fi Standards Spelled out, Pg. 77.

[12] http://certifications.wi-fi.org/wbcs_certified_products.php 25 July2005