Performance analysis of ad-hoc networks under black hole attacks

Semih Dokurer
Department of Computer Engineering
ATILIM University Ankara, Turkey
E-mail: sdokurer@gmail.com

Y. M. Erten
Department of Computer Engineering
TOBB Economics and Technology University
E-mail:erten@etu.edu.tr

Can Erkin Acar
ProG Ltd
Ankara Turkey
E-mail:can.acar@pro-g.com.tr

***Abstract*— A wireless ad-hoc network is a temporary network set up by wireless nodes usually moving randomly and communicating without a network infrastructure. Due to security vulnerabilities of the routing protocols, however, wireless ad-hoc networks may be unprotected against attacks by the malicious nodes. In this study we inverstigated the effects of Black Hole attacks on the network performance. We simulated black hole attacks in Network Simulator 2 (ns-2) and measured the packet loss in the network with and without a black hole. We also proposed a simple solution against black hole attacks. Our solution improved the network performance in the presence of a black hole by about 19%.**

I. Introduction

Wireless ad-hoc networks are composed of autonomous nodes that are self- managed without any infrastructure. They usually have a dynamic topology such that nodes can easily join or leave the network at any time and they move around freely which gives them the name Mobile Ad hoc NETworks or MANETs. They have many potential applications, especially in military and rescue operations such as connecting soldiers in the battlefield or establishing a temporary network in place of one which collapsed after a disaster like an earthquake.

In these networks, besides acting as a host, each node also acts as a router and forwards packets to the correct node in the network once a route is established. To support this connectivity nodes use routing protocols such as AODV (Ad-hoc On-Demand Distance Vector) or DSR (Dynamic Source Routing).

Wireless ad-hoc networks are usually susceptible to different security threats and black hole attack is one of these. In this type of attack, a malicious node which absorbs and drops all data packets makes use of the vulnerabilities of the on demand route discovery protocols, such as AODV. In the route discovery process of AODV protocol, intermediate nodes are responsible to find a fresh path to the destination, sending discovery packets to the neighbor nodes. Malicious nodes abuse this process and they immediately respond to the source node with false information as though they have a fresh enough path to the destination. Therefore source node sends its data packets via this malicious node assuming it is a true path. Black hole behavior may also be due to a damaged node dropping packets unintentionally. In any case, the end result of the presence of a black hole in the network is lost packets.

In our study, we simulated black hole attacks in wireless ad-hoc networks and evaluated their effects on the network performance. We made our simulations using ns-2 (Network Simulator version 2). Having implemented a new routing protocol which simulates the black hole behavior in ns-2, we performed tests on different topologies to compare the network performance with and without black holes in the network. As expected, the throughput in the network deteriorated considerably in the presence of a black hole.

We also proposed a solution based on ignoring the first established route to reduce the adverse effects of the black hole node in an ad-hoc network using AODV as a routing protocol. We implemented the solution also in ns-2 and evaluated the results as we did for the black hole implementation. We presented the improvement due to our proposed solution in the proceeding sections.

The paper is organized as follows: section 2 describes the AODV protocol and black hole attacks are described in section 3. Network simulation results are presented in section 4 and the proposed solution is described in section 5 followed by conclusions in section 6.

II. AODV routing protocol

Ad-hoc On-Demand Distance Vector (AODV) [1] is an on demand routing protocol which is used to find a route between the source and destination node as needed. It uses control messages such as Route Request (RREQ), and Route Reply (RREP) for establishing a path from the source to the destination. Header information of these control messages are also explained in [1]. When the source node wants to make a connection with the destination node, it broadcasts an RREQ message. This RREQ message is propagated from the source, and received by neighbors (intermediate nodes) of the source node. The intermediate nodes broadcast 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 in its routing table. Fresh enough means that the intermediate node has a valid route to the destination established earlier than a time period set as a threshold. Use of a reply from an intermediate node rather than the destination reduces the route establishment time and also the control traffic in the network. This, however, leads to vulnerabilities as explained earlier.

Sequence numbers are also used in the RREP messages and they serve as time stamps and allow nodes to compare how fresh their information on the other node is. When a node sends any type of routing control message, RREQ, RREP, RERR etc., it increases its own sequence number. Higher sequence number is assumed to be more accurate information and whichever node sends the highest sequence number, its information is considered most up to date and route is established over this node by the other nodes.

III. Black hole attacks

In an ad-hoc network that uses the AODV protocol, a black hole node pretends to have a fresh enough route to all destinations requested by all the nodes and absorbs the network traffic. When a source node broadcasts the RREQ message for any destination, the black hole node immediately responds with an RREP message that includes the highest sequence number and this message is perceived as if it is coming from the destination or from a node which has a fresh enough route to the destination. The source assumes that the destination is behind the black hole and discards the other RREP packets coming from other nodes. The source then starts to send out its data packets to the black hole trusting that these packets will reach the destination.

Vulnerabilities of ad-hoc networks against black hole attacks are studied by different authors. Deng et.al. [2] addresses the black hole problem and proposes a solution based on modification of the AODV protocol. The authors propose to check the route through the next hop in the agreed upon path. This solution means that next hop information shall be added to the standard AODV header. Similar approach is adopted in [3] where the nodes are asked to send their neighborhood sets once the route is established. In [4] two solutions are proposed for detecting the black hole attack in ad-hoc networks. First solution involves sending a ping packet to the destination to check the established route. If the acknowledgement does not arrive from the destination, presence of a black hole is deduced. The other approach proposed is based on keeping track of sequence numbers as black holes usually temper with these sending packets with unusually high sequence numbers. A survey of intrusion detection methods against various attacks, including black hole attacks, are given in [6].

IV. Network Simulations

To investigate the effects of black holes we simulated the wireless ad-hoc network scenarios with and without 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 black holes adopted this protocol and behaved exactly like black holes as described above.

To test this protocol we used two simulations of a small network with 7 nodes. 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.

We used UDP protocol in both simulations and attached CBR (Constant Bit Rate) application that generates constant packets through the UDP connection. CBR packet size is chosen to be 512 bytes, and data rate is set to 1 Mbyte. Duration of the scenarios is 20 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 flat space. We manually defined appropriate positions of the nodes to show the data flow and also introduce a movement only to Node 1 to show the changes of the data flow in the network. A black hole node is included in the network for the second simulation. We observed that the protocol is functioning as it should hence it could be applied to larger networks.

We used 20 nodes in the actual test networks and UDP connections are established between even and odd numbered nodes. In this setup the even numbered nodes are the sending nodes and odd numbered nodes are the receiving nodes. For example Node 0 is transmitting to Node 1, Node 2 to Node 3, Node 4 to Node 5 etc. Node 18 and Node 19 are used as black holes during the simulations as needed. Thus, we could count the sent and received packets between any two nodes. We could also count the number of packets dropped at each node including the black hole nodes.

In all the 100 scenarios we tested, the same nodes are acting as a source and sending to the same destination but in each scenario, every single node is placed at different coordinates and exhibits different movements. Node positions and movements are randomly generated. For each scenario nodes move from a random starting point to a random destination with a speed that is randomly chosen in a 750 x 750 meter flat space. Total simulation time is set to 500 seconds and the CBR connections started at the first second of the scenario and lasts for 450 seconds. We allowed 50 seconds for the buffers to be emptied after the transmission ends. In our scenarios CBR parameters are set to have packet sizes of 512 bytes, and data rates of 10 kbits/sec..

For each scenario we performed two simulations. In the first one every node is working in cooperation with each other to keep the network in communication. The packet loss in an ad-hoc network without any malicious nodes is presented in Table I.

In the second we introduced one malicious node that carries out the black hole attack in the network. In this case node 18 acted as a black hole and node 19 was silent. We measured the number of packets sent by the source and received by the destination. We also tried to evaluate how many of the packets that could not reach the destination node are absorbed in the black hole. These are also shown in Table II.

We could then compare the results of these two simulations to understand the network and node behaviors. The results of the simulation show that the packet loss in the network with a black hole increases beyond that dropped by the black hole node. This we assumed to be due to increased congestion in the routes towards the black hole node.

We repeated these calculations for 2 black holes and the results are presented in Table III. The average of only 5

TABLE I

PACKET LOSS PERCENTAGES IN AN AD HOC NETWORK (AVERAGE OF 100 SCENARIOS)

Path	Packets Sent	Packets Received	% of Packets lost
Node 0-Node 1	974.05	931.84	4.33
Node 2-Node 3	1013.97	982.04	3.15
Node 4-Node 5	1020.27	979.22	4.02
Node 6-Node 7	1013.88	984.6	2.89
Node 8-Node 9	1044.7	1017.83	2.57
Node 10-Node 11	981.09	956.76	2.48
Node 12-Node 13	985.25	949.3	3.65
Node 14-Node 15	1019.86	978.41	4.06
Node 16-Node 17	1005.03	965.03	3.98
Total	9058.1	8745.03	3.46

TABLE II

PACKET LOSS PERCENTAGES IN AN AD HOC NETWORK WITH A SINGLE BLACK HOLE (AVERAGE OF 100 SCENARIOS)

Path	Packets Sent	Packets Received	Packets dropped at the black hole	% of Packets lost	% of Packets lost at the black hole
Node 0-Node 1	1047.33	68.43	489.9	93.47%	50.05%
Node 2-Node 3	1053.12	124.5	410.89	88.18%	44.25%
Node 4-Node 5	1067.54	92.58	488.95	91.33%	50.15%
Node 6-Node 7	1066.94	73.04	447.77	93.15%	45.05%
Node 8-Node 9	1069.7	136.25	469.14	87.26%	50.26%
Node 10-Node 11	1078.68	129.94	485.98	87.95%	51.22%
Node 12-Node 13	1059.39	115.15	472.52	89.13%	50.04%
Node 14-Node 15	1048.9	116.69	475.85	88.88%	51.05%
Node 16-Node 17	1058.01	103.27	452.24	90.24%	47.37%
Total	9549.61	959.85	4193.24	89.95%	48.82%

scenarios are used here and both node 18 and node 19 were assigned BlackholeAODV protocol.

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.

V. SIMULATION OF IDSAODV AND EVALUATION OF RESULTS

An ad-hoc network is basically a random graph. Some of the nodes are in direct communication if they are in the radio coverage area of each other. Other nodes communicate through the routing performed by their neighbors. It is not an easy task to calculate the probability of having a route from one node in the network to another even for special cases [7]. Hence the connectivity of the networks are usually determined through simulations or exhaustive search, and usually only connectivity for the nodes which are attempting to set up a connection is considered. In our case we generated random networks and created 100 scenarios this way. Our networks in the different scenarios changed over time as the nodes moved randomly. We tested the conductivity of the networks and the number of hops for different paths during the entire simulation period. Zero hops means there is no connection between a pair of nodes. Figure 1 shows the measured and calculated probability of different distances between nodes in the network. By distance we mean number of hops and the calculations are made assuming normal distribution. From the figure 10.8 % of the nodes are within 1 hop of each other and this is in close agreement with the results found in [8].

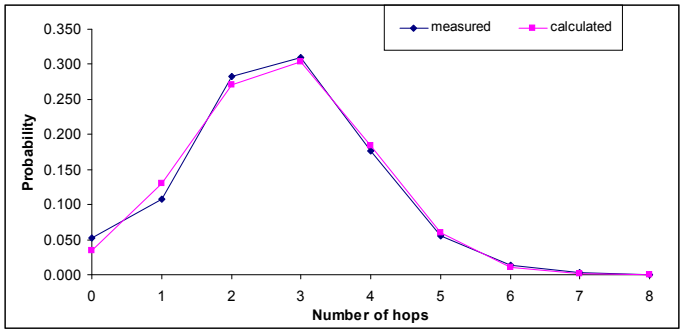

Fig. 1. Measured and calculated probability of different distances between nodes in the network (calculations are made assuming normal distribution)

We also manually checked the number of paths between the nodes under consideration as described in the previous section. We found out that for the scenarios we checked there were always a second route between the nodes which are communicating. We also made the following observations:

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 black hole node on average at t= 0.2059 seconds. It is reasonable to

TABLE III

PACKET LOSS PERCENTAGES IN AN AD HOC NETWORK WITH TWO BLACK HOLES WHERE AODV PROTOCOL IS USED (AVERAGE OF 5 SCENARIOS)

Path	Packets Sent	Packets Received	Packets dropped at the black hole 1	Packets dropped at the black hole 2	% of Packets lost	% of Packets lost at the black holes
Node 0-Node 1	1097	6	246	253	99.45	45.49
Node 2-Node 3	1110	49	294	578	95.59	78.56
Node 4-Node 5	1072	2	693	80	99.81	72.11
Node 6-Node 7	1111	1	311	42	99.91	31.77
Node 8-Node 9	1089	2	421	502	99.82	84.76
Node 10-Node 11	1130	6	460	519	99.47	86.64
Node 12-Node 13	1128	52	302	672	95.39	86.35
Node 14-Node 15	1113	18	158	578	98.38	66.13
Node 16-Node 17	1112	2	414	337	99.82	67.54
Total	9962	138	3299	3561	98.61	68.86

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. These examples may be extended according to the specific nodes in different network topologies.

TABLE IV

PACKET LOSS PERCENTAGES IN A NETWORK WHERE IDSAODV PROTOCOLIS USED (AVERAGE OF 100 SCENARIOS)

Path	Packets Sent	Packets Received	% of Packets lost
Node 0-Node 1	976.87	898.24	8.05
Node 2-Node 3	1005.62	930.32	7.49
Node 4-Node 5	1008.68	949.72	5.85
Node 6-Node 7	1008.99	922.51	8.57
Node 8-Node 9	1017.67	952.3	6.42
Node 10-Node 11	992.87	926.81	6.65
Node 12-Node 13	988.26	915.71	7.34
Node 14-Node 15	986.44	908.38	7.91
Node 16-Node 17	984.55	917.3	6.83
Total	8969.95	8321.29	7.23

Based on the above arguments and observations we chose to use the second route for message delivery and investigated if this approach improves the network performance under the black hole attacks in an ad-hoc network.

We implemented a new protocol which we called IDSAODV in ns-2. In this approach we used the first RREP message to initiate the data transfer but if a second RREP message arrived then we switched to the new route. To be able to evaluate if our solution improves the performance we used the same scenarios and simulation parameters as described previously. Table V shows that the proposed approach reduced the packet loss by about 19%, but the packet loss in the network without a black hole has also increased by about 4% (Table IV). The proposed protocol does not require any extra packets to be transmitted and the protocol packets have not been modified. Only the mechanism on which the protocol acts is modified.

Our calculations show that the probability of finding a disjoint third route from the source to the destination is negligible. To verify this, we modified the IDSAODV protocol further to check for a third RREP message (we called this protocol 3IDSAODV) and use the newly notified route if one is found. The network started communicating using the route established by the first RREP message, switched to the route indicated by the second if a second RREP arrived and then to the third one if one existed. The results of this approach with and without a black hole are presented in Tables VI and VII respectively. The results show that there is almost no difference between using the second or the third RREP messages. This is due to the scarcity of the third disjoint routes.

VI. CONCLUSIONS

In this study we analyzed the effects of black holes in ad-hoc networks. We implemented an AODV protocol that simulates the behavior of a black hole in ns-2 and we simulated 100 scenarios each involving different ad-hoc networks with 20 nodes each moving randomly. We introduced a black hole in each scenario and compared the performance of the networks with and without a black hole. We also tested a network with two black holes for only five scenarios. We then implemented a modified AODV protocol which responded to the second RREP message if it arrived assuming that it is more likely to have the first RREP arriving from the black hole if one exists in the network.

The results demonstrate that the presence of a black hole increases the packet loss in the network considerably. The network experienced 89.95% packet loss on average due to the introduction of a black hole. This loss is partially (48.82%) due to packets dropped in the black hole node and partially due to congestion in the network over the paths towards the black hole node.

The proposed modified AODV protocol reduced the packet loss due black hole attack to 71.09% which is an improvement of 18.86% compared to the AODV protocol. Using the third RREP message did not have any noticeable positive contributions to the packet loss in the network.

The proposed protocol does not make any modifications in the packet format hence can work together with the AODV protocol. Another advantage is that the proposed IDSAODV

TABLE V

PACKET LOSS PERCENTAGES IN AN AD HOC NETWORK WITH A SINGLE BLACK HOLE WHERE IDSAODV PROTOCOL IS USED (AVERAGE OF 100 SCENARIOS)

Path	Packets Sent	Packets Received	Packets dropped at the black hole	% of Packets lost	% of Packets lost at the black hole
Node 0-Node 1	1057.4	299.84	291.87	71.64	38.53
Node 2-Node 3	1057.02	333.04	278.84	68.49	38.51
Node 4-Node 5	1060.72	290.34	361.04	72.63	46.87
Node 6-Node 7	1020.97	275.86	293.14	72.98	39.34
Node 8-Node 9	1086.09	353.41	272.19	67.46	37.15
Node 10-Node 11	1071.22	233.14	310.32	78.24	37.03
Node 12-Node 13	1067.81	338.01	285.1	68.35	39.07
Node 14-Node 15	1059.61	295.79	311.87	72.09	40.83
Node 16-Node 17	1054.64	337.46	296.95	68.00	41.41
Total	9535.48	2756.89	2701.32	71.09	39.85

TABLE VI

PACKET LOSS PERCENTAGES IN AN AD HOC NETWORK USING 3IDSAODV PROTOCOL(AVERAGE OF 100 SCENARIOS)

Path	Packets Sent	Packets Received	Packets lost %
Node 0-Node 1	974.86	901.55	7.52
Node 2-Node 3	1006.89	930.9	7.55
Node 4-Node 5	999.52	942.07	5.75
Node 6-Node 7	1016.42	938.95	7.62
Node 8-Node 9	1014.12	961.02	5.24
Node 10-Node 11	992.5	932.28	6.07
Node 12-Node 13	987.00	915.92	7.20
Node 14-Node 15	985.36	904.71	8.18
Node 16-Node 17	989.88	923.24	6.73
Total	8966.55	8350.64	6.87

TABLE VII

PACKET LOSS PERCENTAGES IN AN AD HOC NETWORK WITH A SINGLE BLACK HOLE WHERE 3IDSAODV PROTOCOL IS USED (AVERAGE OF 100 SCENARIOS)

Path	Packets Sent	Packets Received	Packets dropped at the black hole	% of Packets lost	% of Packets lost at the black hole
Node 0-Node 1	1064.78	312.16	282.72	70.68	37.56
Node 2-Node 3	1049.88	372.19	260.09	64.55	38.38
Node 4-Node 5	1064.09	287.66	380.04	72.97	8.95
Node 6-Node 7	1035.6	277.28	283.06	73.23	37.33
Node 8-Node 9	1086.03	349.23	286.27	67.84	38.85
Node 10-Node 11	1069.81	267.9	307.19	74.96	38.31
Node 12-Node 13	1060.44	333.49	273.36	68.55	37.60
Node 14-Node 15	1068.93	301.67	325.94	71.78	42.48
Node 16-Node 17	1057.39	281.7	326.63	73.36	42.11
Total	9556.95	2783.28	2725.3	70.88	40.23

does not require any additional overheads such as sending a ping to the receiver or keeping a black hole list through a different protocol.

REFERENCES

[1] Perkins, C.E., Royer, E.M., "Ad-hoc on-demand distance vector routing", www.cs.ucsb.edu/~ravenben/classes/papers/aodv-wmcsa99.pdf

[2] Deng, H., Li, W., Agrawal, D., "Routing Security in Wireless Ad Hoc Networks" IEEE Communication Magazine (October 2002) pp. 70-75

[3] Sun, B., Guan, Y., Chen, J., Pooch, U.W., "Detecting black hole attack in Mobile ad-hoc networks",

[4] Al-Shurman, M., Yoo, S., Park, S., "Black hole Attack in Mobile Ad Hoc Networks", ACM Southeast Regional Conference (2004) pp. 96-97

[5] http://moment.cs.ucsb.edu/pub/rfc3561.txt

[6] Mishra, A., Nadkarni, K., Patcha, A., "Intrusion detection in wireless ad-hoc networks", IEEE Wireless Communications, February 2004, pp. 48-60.

[7] Papadimitratos, P., Haas, Z. J., and Sirer, E. G., " Path set selection in mobile ad hoc networks", Proceedings of the 3rd ACM international Symposium on Mobile Ad Hoc Networking Computing Lausanne, Switzerland, June 09 - 11, 2002 MobiHoc '02 pp. 1-11.

[8] Bettstetter, C.; Eberspacher, J., "Hop distances in homogeneous ad hoc networks," The 57th IEEE Semiannual Vehicular Technology Conference, 2003. VTC 2003-Spring. , vol.4, pp. 2286- 2290.