A NOVEL INTRUSION DETECTION SYSTEM FOR DETECTING BLACK-HOLE NODES IN MANETS

Baishali Goswami

Department of Computer Science and Engineering
Sikkim Manipal Institute of Technology
Sikkim, India

Abstract

Mobile ad-hoc networks (MANETs) are autonomous,infrastructure less, self-organized networks. In MANETs, nodes are not stationary and thus move arbitrarily, resulting in rapid and unpredictable topology changes in the network. Due to the limited transmission range of the nodes in the MANETs, these nodes are not capable of directly communicating with each other. Hence, routing paths in MANETs potentially contain multiple hops, and every node in it has the responsibility to act as a router.So, the presence of any intermediate node in the route, which is either highly congested or behaving as a malicious node, is likely to drop the packets. In computer networking, this type of attack is known as a packet drop attack or black hole attack which is a type of denial-of-service attack in which a router that is supposed to relay packets instead discards them. The proposed algorithm will detect black hole nodes in the network by implementing changes into the existing AODV routing algorithm. The implementation of the algorithm was being achieved using theNS-2 simulator.

Keywords

Ad-hoc AODV, Black Hole Attack, MANET, Destination sequence Number.

1. INTRODUCTION

A Mobile ad-hoc network (MANET) is a self-configured network that automatically forms from a collection of mobile nodes without the help of a fixed infrastructure or a centralized management. Each node is adorned with a wireless transmitter and receiver, which facilitates their communication with other nodes in its radio communication range. In order that a node can forward a packet to a node out of its radio range, the cooperation from other nodes in the network is needed. Hence, each node needs to act both as a host and a router simultaneously. The topology of the network may change frequently due to the mobility of the mobile nodes within, into, or out of the network. A MANET was originally developed for military purposes, as nodes are scattered across a battlefield and there is no infrastructure to help them form a network. These days, MANETs are being increasingly used in many applications, ranging from military to civilian and commercial uses, since setting up such networks can be done without the help of any infrastructure or less interaction with a human. Some examples are: search-and-rescue missions, data collection, and virtual classrooms and conferences where laptops, PDA or other mobile

DOI : 10.5121/jgraphoc.2016.8201

devices share wireless medium and communicate to each other. As MANETs are now widely used, their security issue has become one of the primary concerns. For example, most of the routing protocols proposed for MANETs assume that every node in the network is cooperative and not malicious where only one compromised node can cause the failure of the entire network.

The detection and prevention of the black-hole attack is very hard. It is a network layer attack. The Ad-hoc On-Demand Distance Vector (AODV) routing protocol is one of the routing protocols used in the ad-hoc mobile networks. AODV is a reactive protocol: the routes are created only when they are needed. It uses traditional routing tables, one entry per destination, and sequence numbers to determine whether routing information is up to date and to prevent routing loops. AODV besides being an efficient routing algorithm possesses some limitations due to which it is easily attacked by the external intruders. It cannot detect malicious nodes.

Intrusion detection can be defined as a process of monitoring activities in a computer or a network system. The mechanism by which this is achieved is called an intrusion detection system (IDS). An IDS collects the complete information regarding the network and uses it to analyze whether there are any activities that violate the security rules. Once an IDS realizes an unusual activity, it generates an alarm to alert the security administrator. In addition, IDS can also initiate a proper response to the malicious activity.Although there are several intrusion detection techniques for wired networks, they are not suitable for MANETs due to the differences in their characteristics. Thus, they need to be modified in order to be used in MANETs.

2.AD-HOC ON-DEMAND VECTOR ROUTING (AODV) PROTOCOL FOR MANETS-

AODV protocol, a pure on-demand data acquisition system, initiates route discovery process when a source node (SN) desires to send some traffic to an unknown destination node (DN). The SN broadcasts a Route Request (RREQ) to the neighbors who further broadcast to their neighbors until a node that has a fresh enough route to the DN is found. The freshness of the routes is ensured by destination sequence number (DSN). Each node maintains its own sequence number to the intended destination and an intermediate node can reply only if its destination sequence number is greater than or equal to that contained in the RREQ. The SN chooses that path from which it has received the first route reply (RREP) for the transmission of data packets to the DN and the RREP's that are further received are discarded.

As shown in the figure below, Node S needs a route to D.

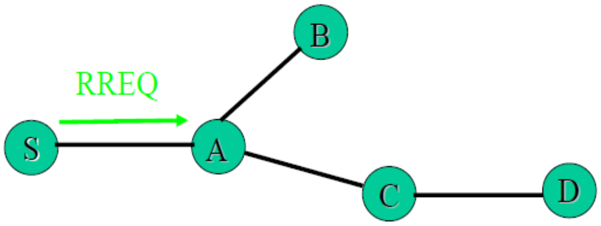

Figure 1: ‘S’ broadcast RREQ packet

It creates a Route Request (RREQ) message and enters D’s IP address, sequence number, S’s IP address, and sequence number, and initializes the hop count to 0. Node S broadcasts RREQ to neighbors. Node A receives the RREQ. It makes a reverse route entry for S with dest=S, nexthop=S, hopcount=1. As it has no routes to D, so it rebroadcasts the RREQ message.

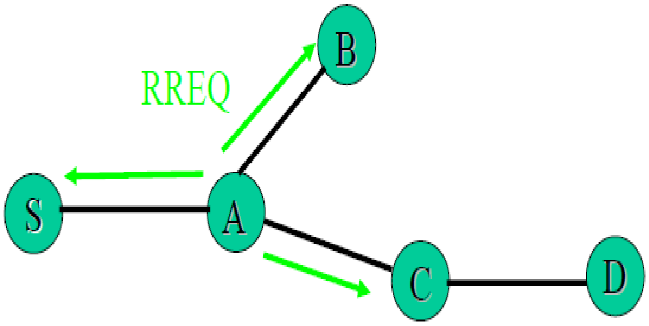

Figure 2: ‘A’ broadcast RREQ packet

Node C now receives the RREQ. It makes a reverse route entry for S with dest=S, nexthop=A and hopcount=2. It has a route to D, and the sequence number for route to D is >= D’s sequence number in RREQ.

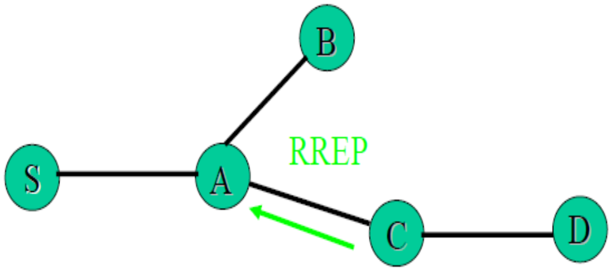

Figure 3: ‘C’ unicast RREP packet

Now, C creates a Route Reply (RREP) message and enters D’s IP address, sequence number, S’s IP address, and initializes hopcount to D (=1). C now unicasts RREP to A.

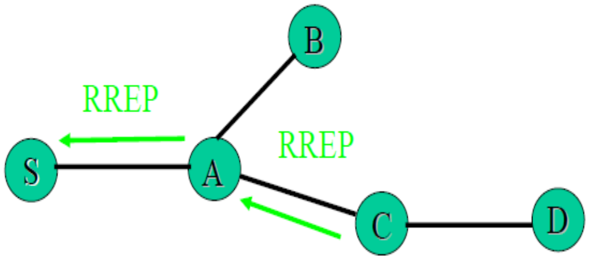

Figure 4: ‘A’ unicast RREP packet

Node A now receives the RREP. It makes a forward route entry to D with dest=D, nexthop=C, and hopcount=2. It then unicasts RREP to S.

When Node S receives the RREP it makes a forward route entry to D with dest=D, nexthop =A, and hopcount = 3. Thus node S sends data packet on route to D.

Since AODV has no security mechanisms to ensure that the packets have reached the destination, malicious nodes can perform Black-hole attacks just by not behaving according to the AODV rules. There is no acknowledgement procedure that is present and hence no validation.

3.BLACK-HOLE ATTACK IN MANETS-

In a Black-hole attack, a malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. This attack drops the data packets in the network. Thus the packets in the network from source never reach the destination. A Black Hole node forges the sequence number and hop count of a routing message to forcibly acquire the route, and then eavesdrop or drop all data packets that pass. A malicious node impersonates a destination node by sending a spoofed RREP to a source node that initiated a route discovery.

A Black Hole node has following two properties:

1. The node exploits the ad hoc routing protocol and advertises itself as having a valid route to a destination, even though the route is fake, with the intention of intercepting packets.

2. The node consumes the intercepted packets.

A Black hole attack is one of the active DoS (Denial-of-Service) attacks possible in MANETs. In this attack, a malicious node sends a false RREP packet to a source node that initiated the route discovery, in order to pose itself as a destination node or an immediate neighbor to the actual destination node. When a source node broadcasts the RREQ message in search of a destination node, the black hole node in the network immediately responds with an RREP message having the highest sequence number so that it is perceived to be coming from the destination or from a node which has a fresh enough rote to the destination. It lets the source assume that the black hole comes before the destination and thus it discards the other RREP packets coming from the other nodes. The source then starts to send out its data packets to the black hole trusting that these packets will reach the destination. A malicious node sends RREP messages without checking its routing table for a fresh route to a destination. As a result, the source and the destination nodes became unable to communicate with each other.

Let us consider the following scenario to see how Black-hole attack affects the normal behavior of AODV.

In black hole attack the malicious node “A” first detects the active route in between the sender “E” and the destination node “D”. The malicious node “A” then sends the RREP which contains the spoofed destination address including small hop count and large sequence number than normal to the node “C”. This node “C” forwards this RREP to the sender node “E”. Now this route is used by the sender to send the data and in this way data will arrive at the malicious node.

These data will then be dropped. In this way sender and destination node will be in no position any more to communicate in state of black hole attack.

An attacker node selectively drops RREQ/RREP packets. In AODV after receiving a RREQ message, an inside attacker may forge a RREP message as if it had a fresh route to the destination node. In order to suppress other legitimate RREP messages that the source node receives from other nodes, the attacker forges a faked RREP message by increasing the destination sequence number. An attacker may disrupt the route between the victim nodes to a given destination, or invade in the route between by suppressing other alternative routes. These kinds of nodes are known as Black Hole nodes.

In figure below, Node A which is a malicious node can forge a RREP message to the source node S. When source node S receives faked RREP message from node A, it updates its route to the destination node through attacking node. When node A receives the data packets it drops the packets as shown in fig below.

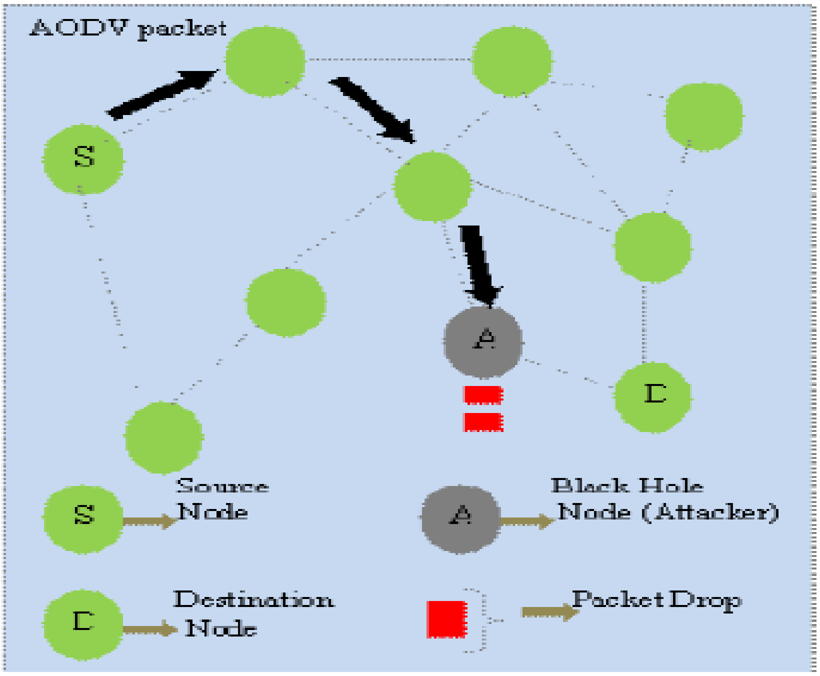

Figure 5: ‘A’ drops the packet

4.EXISTING WORK ON BLACK HOLE ATTACK-

In [4], Intrusion Detection Systems (IDS) are one of the primary techniques employed to thwart attacks against security threats. Intrusion detection can be classified as network based and host based. Network based IDS are installed on the data concentration points of a network such as switches and routers. In the mobile ad-hoc networks, we have no central device that monitors traffic flow, so the proposed technique of intrusion detection using anomaly detection (IDAD) used host based IDS schema. IDAD assumes every activity of a user or a system can be monitored and anomaly activities of an intruder can be identified from normal activities. To find a black hole, the IDAD needs to be provided with a pre collected set of anomaly activities, called audit data. Once audit data is collected and given to the IDAD system, the IDAD system is able to compare every activity with audit data. If any activity of a host is not among the activities listed in the audit data, the IDAD system isolates the particular node from the network. In this algorithm, they first broadcasted RREQ for route discovery, received RREP and matched the RREP with the audit data.If they match,the route is saved to the route table and the data is sent. Otherwise, the RREP is discarded and then again tried. In [2] [8], the authors introduced the route confirmation request (CREQ) and route confirmation reply (CREP) messages to thwart the effect of the black hole attack. In this methodology, the intermediate node sends RREPs to the source node as well as CREQs to its next-hop node towards the destination node. After receiving a CREQ, the next-hop node looks up at its cache for a route to the destination. If it finds a route, it sends the CREP to the source. After it receives the CREP, the source node confirms the validity of the path in RREP and the one in CREP. If both match, the source node confirms that the route is correct. One drawback of this approach is that it cannot avoid the black hole attack in which two consecutive nodes work in collusion, that is, when the next-hop node is a colluding attacker sending CREPs that support the incorrect path. In [5] authors have mentioned the AODV protocol and Black hole attack in MANETs and proposed a feasible solution for the black hole attacks that can be implemented on the AODV protocol. The Proposed method can be used to find the secured routes and prevent the black hole nodes in the MANET. As future work, author intend to develop simulations to analyze the performance of the proposed solution based on the various security parameters like packet delivery ratio (PDR), mean delay time, packet overhead, memory usage, mobility, increasing number of malicious node, increasing number of nodes and scope of the black hole nodes. In [5], the authors proposed a methodology that demands from a source node to wait until a RREP packet arrives from more than two nodes. Upon receiving multiple RREPs, the source node checks for the presence of a shared hop. If there is one, the source node concludes that the route is safe. The main drawback with this methodology is that it introduces time delay, because it must wait until multiple RREPs arrive. In [10], the authors analyzed the black hole attack and concluded that a malicious node must increase the destination sequence number amply, to convince the source node that the route provided is optimum. Based on this analysis, the authors proposed a statistical based anomaly detection approach to detect the black hole attack, based on differences between the destination sequence numbers of the received RREPs. The key advantage of this approach is that it detects the attack at low cost without introducing extra routing traffic, and it does not require modification of the existing protocol. In [14], according to author’s solution, information about the next hop to destination should be included in the RREP packet when any intermediate node replies for RREQ. Then the source node sends a further request (FREQ) to the next hop of replied node and asks about the replied node and route to the destination. By using this method we can identify trustworthiness of the replied node only if the next hop is trusted. However, this solution cannot prevent cooperative black hole attacks on MANETs. For example, if the next hop also cooperates with the replied node, the reply for the FREQ will be simply “yes” for both the questions.

5.PROPOSED ALGORITHM, DESIGN AND METHODOLOGY USED-

We are proposing a model for detecting black hole attack in MANETs using the AODV Routing Protocol. In the previous sections we have already discussed how a black hole attack affects the normal behavior of AODV. We have made changes into the normal algorithm of AODV. For this we have introduced a new table into the AODV algorithm which will work as follows:

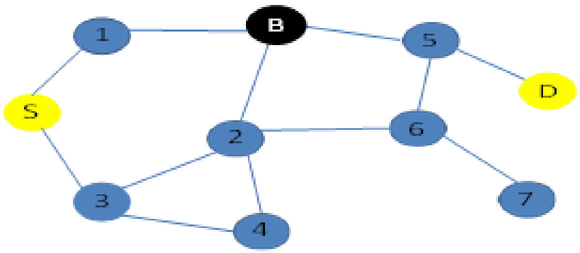

Figure 6: Assumed scenario

Here, in the above scenario, node S is the source node; node B is the black hole node and node D is the destination node. The rest of the nodes are numbered from 1 to 7.

We have assumed that our network is in promiscuous mode. When a network is in promiscuous mode, the nodes can intercept and read each network packet that arrives in its entirety. Therefore, node1will be informed when node S and B will send packets to its neighboring nodes. Moreover in our algorithm, each and every node will maintain its own table, which will be created as soon as a node sends a RREQ. A timer is set at each of the nodes which will check the expiry of the table that we have created. A flag field is maintained which is initially set to 1.

Step 1:

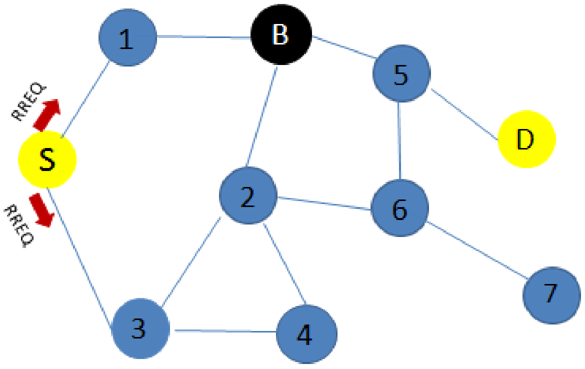

Figure 7: Source broadcasts RREQ

At first, node S needs a route to D. Therefore it creates a route request packet RREQ (1) that is RREQ with ID 1. The source node S broadcasts this RREQ (1) to its neighbors. As node 1and node 3 are its neighbors, they receive RREQ (1) from S. Let us assume the RREQ (1) broadcasting time from node S be t1.

Hence the following table will be maintained at node S:

Destination Address	RREQ Packet ID	RREQ Broadcasting time	RREQ Received from(LL)	RREP Received from	RREP Received time	Time-Out	Flag	Count
D	1	t1						

Step 2:

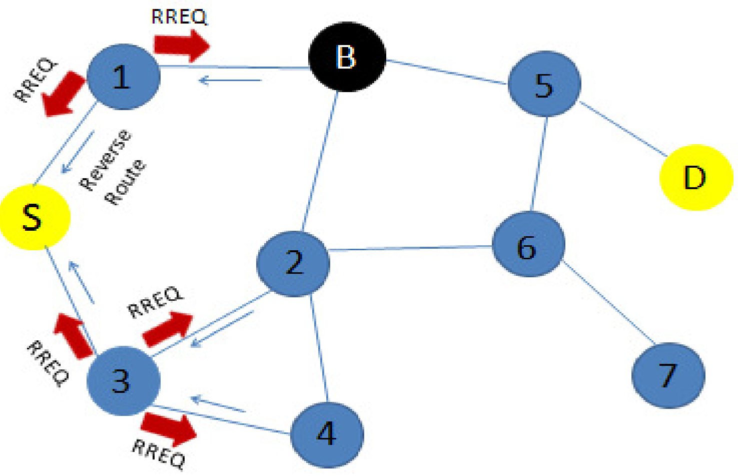

Figure 8: Nodes 1 and 3 makes reverse route entry and rebroadcasts RREQ

After receiving the RREQ(1), nodes 1 and 3 make a reverse route entry for S and check in its own routing tables whether they have a destination to node D. Since at the very moment of sending data packets for the first time, these nodes do not have any route to the destination node D, they rebroadcast RREQ (1) to their neighbors. Rebroadcasted RREQ (1) from node 1 reaches S and B and from node 3 to S, 2 and 4, and hence reverse route entries for S are made from B, 2 and 4. As S is the neighbor of 1 and 3, it received RREQ (1) from both of them. The nodes 1 and 3 will rebroadcast the RREQ (1) to its neighboring nodes at different time periods or at the same time say t2 and t3 respectively. Hence node 1 will maintain its table as follows:

Destination Address	RREQ Packet ID	RREQ Broadcasting time	RREQ Received from(LL)	RREP Received from	RREP Received time	Time-Out	Flag	Count
D	1	t2						

Table for node 3 will be maintained as:

Destination Address	RREQ Packet ID	RREQ Broadcasting time	RREQ Received from(LL)	RREP Received from	RREP Received time	Time-Out	Flag	Count
D	1	t3						

Step 3: As soon as node S receives the rebroadcasted RREQ (1) from 1 and 3, it fills up its column of "RREQ Received from" in its table. Thus, table for S after receiving RREQ (1) from 1 and 3:

Destination Address	RREQ Packet ID	RREQ Broadcasting time	RREQ Received from(LL)	RREP Received from	RREP Received time	Time-Out	Flag	Count
D	1	t1	1,3					

Step 4:

Since rebroadcasted RREQ(1) of node 1 reaches its neighbors, the black hole node we have assumed that is node B will also receive RREQ(1) from 1 being its neighbor. But immediately it will unicasts an RREP with high sequence number and least hop count to its immediate neighbor 1 at time say t4 instead of rebroadcasting the RREQ(1), since it is the black hole node.

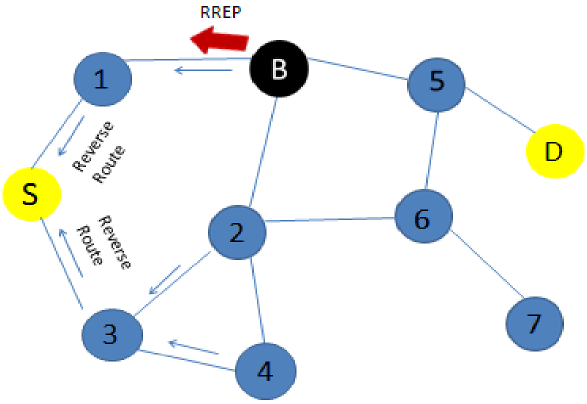

Figure 9: B unicasts RREP to S.

Thus node 1 after receiving the RREP from node B will immediately update its table by filling the column of "RREP Received from" as node B. Node 1 did not receive the rebroadcasted RREQ (1) from node B before receiving the RREP from B, hence B might be a malicious node.

So, this entry in the table of node 1 for node B cannot be deleted which is indicated by flag 1, since it needs to set a time out for B to check whether node B is forwarding the data packets within the time out period.

We have assumed a set of three time out periods which will be calculated by subtracting the RREQ (1) broadcasting time (of node 1) from the RREP unicasting time (of node B).

For node 1, RREQ (1) broadcasting was t2 and RREP unicasting time was t4. Thus, the set of time-outs will be:

1st time-out T_1 = t4-t2
2nd time-out T_2= 2*T_1
3rd time-out T_3 = 2*T_2

A count field is used which will be incremented by 1, each and every time the last calculated individual time-out period expires. When all the three time-outs expire i.e. when the count value exceeds 3, node B will be declared as the black hole node. The updated table of 1 will be:

Destination Address	RREQ Packet ID	RREQ Broadcasting time	RREQ Received from(LL)	RREP Received from	RREP Received time	Time-Out	Flag	Count
D	1	t2	-	B	t4	t4-t2	1	1

Step 5:

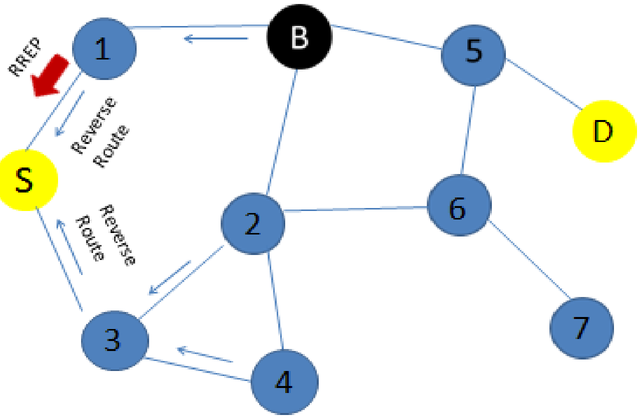

Figure 10: Node 1 unicasts RREP to S.

The unicasted RREP received by node 1from node B is unicasted to node S from 1. Since node S received the rebroadcasted RREQ (1) before receiving the RREP from 1, hence it can infer that node 1 is not a black hole node, and no ‘time-out period needs to be calculated for 1. Thus, the whole entry in the table of S is deleted, indicated by flag 0. Table for S will then be updated as:

Destination Address	RREQ Packet ID	RREQ Broadcasting time	RREQ Received from(LL)	RREP Received from	RREP Received time	Time-Out	Flag	Count
D	1	t1	1,3	1	t5		0	

6. EXPERIMENTAL RESULTS AND DISCUSSION

In this project, 4 sample scenarios were considered and were simulated to verify the performance of the detection algorithm which detects black hole nodes in MANETs. The simulation results are illustrated as below:

1. Scenario 1:

Parameters used:

Number of nodes (nn)	Number of connections	Assigned Black hole nodes (shows the node number)
5	2	1

True detection: Node 1.
False detection: No false detection.

2. Scenario 2:

Parameters used:

Number of nodes (nn)	Number of connections	Assigned Black hole nodes (shows the node number)
10	5	3,7

True detection: Nodes 3, 7.
False detection: No false detection.

3. Scenario 3:

Parameters used:

Number of nodes (nn)	Number of connections	Assigned Black hole nodes (shows the node number)
20	10	1,3,7,8,9.

True detection: Nodes 1, 3,7,8,9.
False detection: No false detection.

4. Scenario 4:

Parameters used:

Number of nodes (nn)	Number of connections	Assigned Black hole nodes (shows the node number)
50	20	2, 12, 17, 18, 34, 42, 25.

True detection: Nodes 2, 12, 18, 34, 42, 25.
False detection: Node 17 .

7. CONCLUSION

MANETs are widely used devices now-a-days. They have wide applications. However, their security is a major concern because of their mobility. They are very prone to security attacks. The routing protocols used in MANETs are also not secure. AODV routing protocol, the most widely used protocol in MANETs, which is considered one of the best routing protocols in terms of power consumption and establishing the shortest path also does not implement any security mechanisms. It cannot detect the presence of malicious nodes and hence cannot prevent any type of intrusions.

MANETs are susceptible to a variety of attacks thatprimarily target the protocols of the transport, network, and data-link layers. Currently, a large number of IDSs have been proposed that protect MANETs; however, the majority of them present limitations and weaknesses, which mainly derive from the fact that they are inherited from static or mobile networks. This paper proposes a novel IDS that attempts to address the limitations and weaknesses of the existing IDSs. We have designed an algorithm for detecting Black hole attack in MANETs, which is an active network layer attack. We have made changes into the existing AODV routing algorithm, so that it detects any black hole node in the network.

References

[1] A. Mishra, K. Nadkarni, A. Patcha, “Intrusion Detection in Wireless Ad Hoc Networks,” IEEE Wireless Communications, Vol. 11, Issue 1. 2004, pp. 48-60.

[2] D. Djenouri, L. Khelladi, N. Badache, “A Survey of Security Issues in Mobile Ad Hoc Networks,” IEEE Communications Surveys, Vol. 7, No. 4. 2005.

[3] H. Yang, H. Luo, F. Ye, S. Lu, L. Zhang, “Security in mobile ad hoc networks: challenges and solutions,” IEEE Wireless Communications Surveys, Vol. 11, No 1. 2004, pp. 38–47.

[4] S. Sen, J. A. Clark, “Intrusion Detection in Mobile Ad Hoc Networks,” Guide to Wireless Ad Hoc Networks, S. Misra, I. Woungang, S.C. Misra (Eds.), Springer 2009, pp. 427-454.

[5] D. Sterne, P. Balasubramanyam, D. Carman, B. Wilson, R. Talpade, C. Ko, R. Balupari, C-Y. Tseng, T. Bowen, K. Levitt, J. Rowe, “A General Cooperative Intrusion Detection Architecture for MANETs,” Proceedings of the third IEEE International Workshop on Information Assurance, pp. 57 – 70, 2005.

[6] K. Nadkarni, A. Mishra, “A Novel Intrusion Detection Approach for Wireless Ad Hoc Networks,” IEEE Wireless Communications and Networking Conference. vol. 2, WCNC 2004, pp. 831 – 836.

[7] B. Sun, K. Wu, Y. Xiao, R. Wang, “Integration of mobility and intrusion detection for wireless ad hoc networks,” International Journal of Communication Systems, vol. 20, Issue 6. pp. 695 – 721. 2007.

[8] L. Lovasz, “Random walks on graphs: a survey,” Combinatorics: Paul Erdos is eighty (Keszthely, Hungary, 1993), vol. 2, edited by D. Miklos et al., Bolyai Soc. Math. Stud. 2, J´ anos Bolyai Math. Soc. 1996, pp. 353–397.

[9] D. Kogias, K. Oikonomou, I. Stavrakakis, I., "Replicated Random Walks for Service Advertising in Unstructured Environments," 7th IFIP Annual Mediterranean Ad Hoc Networking Workshop Med Hoc-Net 2008, Palma de Mallorca, Spain.

[10] J. Daemen, V. Rijmen, "The Design of Rijndael, AES - The Advanced Encryption Standard," Springer Verlag 2002, pp. 238.

[11] V. Miller, "Uses of Elliptic Curves in Cryptography," Proceedings of Crypto '85, LNCS 218, Springer-Verlag 1986, pp. 417-426.

[12] S. Li, A. Ephremides, "Covert Channels in Ad-Hoc Wireless Networks," Elsevier Ad Hoc Networks 2009.

13] C-Y. Tseng, "A specification-based intrusion detection system for AODV," In proceedings. Of ACM Workshop on Security of ad hoc and sensor networks. 2003.

[14] C. H. Tseng, T. Song, P. Balasubramanyam, C. Ko, K. Levitt, "A Specification-based Intrusion Detection Model for OLSR," In proceedings of the 8th International Symposium, RAID 2005, Recent Advances in Intrusion.

[15] H. M. Hassan, M. Mahmoud, S. El-Kassas, "Securing the AODV protocol using specification based intrusion detection," In proceedings of the 2nd ACM international workshop on quality of service & security for wireless and mobile networks, Terromolinos, Spain 2006.

[16] Y. Huang, W. Lee, "Attack analysis and detection for ad hoc routing protocols," In proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection. RAID 2004.

[17] J. Orset, B. Alcalde, A. Cavalli, "An EFSM-based intrusion detection system for ad hoc networks," In proceedings of the 3rd international symposium on Automated technology for verification and analysis, ATVA 2005,Taipei, Taiwan.

[18] N. R. Potlapally, S. Ravi, A. Raghunathan, N. K. Jha, "A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols," IEEE Transactions on Mobile Computing, v.5 n.2. 2006, pp.128-14.