International Journal of Advance Engineering and Research Development (IJAERD)
Volume 1,Issue 5,May 2014, e-ISSN: 2348 - 4470 , print-ISSN:2348-6406

Detection of Black Hole Attack in MANET using Intrusion Detection System

[1]Nikhil Patel, [2]Avani Dadhaniya

[1]*Computer Department, KSV University,nikhil8441@gmail.com*
[2]*Assistant Professor, Computer Department, KSV University,avani26.22@gmail.com*
[1,2]*L.D.R.P Institute of Technology and Research, Ghandhinagar, India*

Abstract : Mobile Ad hoc networks (MANET) have been used in recent years, in many applications. They are more vulnerable to malicious attack. It is very tough to accomplish the complete security in the mobile ad hoc network. This is because of some of its unique characteristics. Besides the prevention methods, we need to detect the malicious nodes such as Black hole attack and take necessary actions to provide the security to these types of networks. For this purpose we are using many intrusion detection systems (IDSs). In this paper, we proposed Intrusion Detection System to identify the malicious node in AODV protocol suffering from black hole attack. As a result we can show the significant improvement of packet delivery ratio (PDR) and an average throughput.

Keywords: MANETs, AODV protocol, Black hole attack, Sequence Number

I. INTRODUCTION

MANETs being an emerging technological field is an active area of research and has found usage in a variety of scenarios like emergency operations, disaster relief, military service and task forces. Providing security to the nodes and their data Communication in such scenarios is critical. A mobile ad hoc network (MANET) is a self-configuring network that is formed automatically by a collection of mobile nodes without the help of a fixed infrastructure or centralized management. Each node is equipped with a wireless transmitter and receiver, which allow it to communicate with other nodes in its radio communication range. In order for a node to forward a packet to a node that is out of its radio range, the cooperation of other nodes in the network is needed; this is known as multi-hop communication. Therefore, each node must act as both a host and a router at the same time .The network topology frequently changes due to the mobility of mobile nodes as they move within, move into, or move out of the network [1, 3].

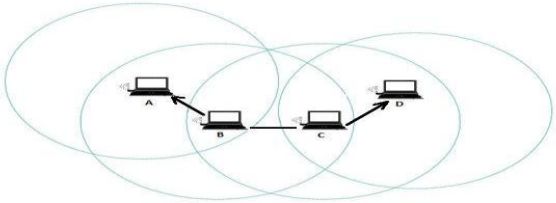

Figure 1 Mobile Ad-Hoc Networks [2]

The member nodes are themselves responsible for the creation, operation and maintenance of the network using single hop or multi hop communication. There are both passive and active attacks in MANETs. For passive attacks, packets containing secret information might be eavesdropped, which violates confidentiality. Active attacks, including injecting packets to invalid destinations into the network, deleting packets, modifying the contents of packets, and impersonating other nodes violate availability,

integrity, authentication, and non-repudiation. Proactive approaches such as cryptography and authentication [2, 3].The characteristics of MANET like dynamic topology, lack of fixed infrastructure, vulnerability of nodes and communication channel, lack of traffic concentration points, limited power, computational capacity, memory, and bandwidth make the task of achieving a secure and reliable communication more difficult. Attacks like sleep deprivation, jamming transmission channel with garbage packets, Black hole, Grey hole, Wormhole and DoS. The selfish nodes may not participate in routing and forwarding packets leading to loss of packets [2, 3]. Intrusion Detection Systems are detecting the malicious activity and give the alarm or alert to the other nodes. IDS system has two types. Anomaly based and Signature based, Both activity detect the malicious activity. In Signature based, some predefined data stored in database to detect the malicious activity. In Anomaly based, abnormal behavior detected in network than it gives the alert to the other nodes in the network.

II. AD HOC ON DEMAND ROUTING PROTOCOL (AODV)

AODV combines some properties of both DSR and DSDV. It uses route discovery process to cope with routes on-demand basis. It uses routing tables for maintaining route information. It is reactive protocol. It doesn't need to maintain routes to nodes that are not communicating. AODV handles route discovery process with Route Request (RREQ) messages. RREQ message is broadcasted to neighbor nodes. The message floods through the network until the desired destination or a node knowing fresh route is reached. Sequence numbers are used to guarantee loop freedom. RREQ message cause bypassed node to allocate route table entries for reverse route.

Route Request Message (RREQ):

Source node that needs to communicate with another node in the network transmits RREQ message. AODV floods RREQ message, using expanding ring technique. There is a time to live (TTL) value in every RREQ message, the value of TTL states the number of hops the RREQ should be transmitted [4, 5].

Route Reply Message (RREP):

A node having [4, 5] a requested identity or any intermediate node that has a route to the requested node generates a route reply RREP message back to the originator node.

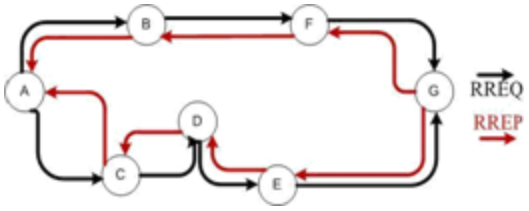

Figure 2 AODV Route Discovery [5]

Route Error Message (RERR):

Every node in the network keeps monitoring the link status to its neighbour's nodes during active routes. When the node detects a link crack in an active route, (RERR) message is generated by the node in order to notify other nodes that the link is down [4, 5].

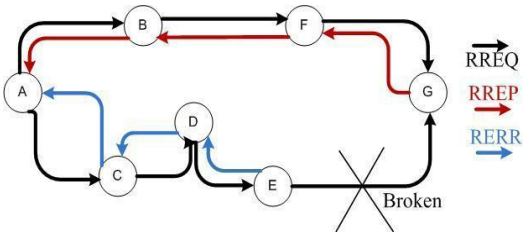

Figure 3 Route Error Message in AODV [5]

III. BLACK HOLE ATTACK

The black hole attack has two properties. First, the node exploits the mobile ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. Second, the attacker consumes the intercepted packets without any forwarding. However, the attacker runs the risk that neighboring nodes will monitor and expose the ongoing attacks. There is a more subtle form of these attacks when an attacker selectively forwards packets. An attacker suppresses or modifies packets originating from some nodes, while leaving the data from the other nodes unaffected, which limits the suspicion of its wrongdoing [5].

3.1 Black hole attack in AODV

In a black hole attack [6], 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. For example, in AODV, the attacker can send a fake RREP (including a fake destination sequence number that is fabricated to be equal or higher than the one contained in the RREQ) to the source node, claiming that it has a sufficiently fresh route to the destination node. This causes the source node to select the route that passes through the attacker. Therefore, all traffic will be routed through the attacker, and therefore, the attacker can misuse or discard the traffic. Figure 4 shows an example of a black hole attack [6], where attacker A sends a fake RREP to the source node S, claiming that it has a sufficiently fresher route than other nodes. Since the attacker's advertised sequence number is higher than other nodes' sequence numbers, the source node S will choose the route that passes through node A. However, a malicious node (performing a black hole attack) drops all data packets rather than forwarding them on.

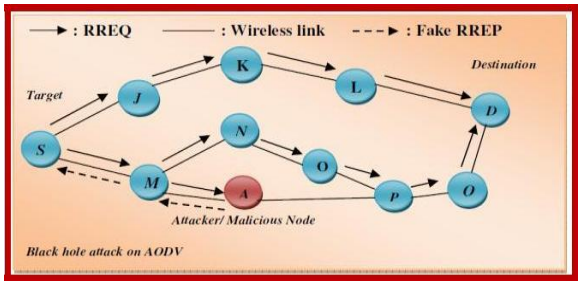

Figure 4 Black Hole Attacks on AODV [6]

IV. EXISTING WORK ON BLACK HOLE ATTACK

In [7] and [8], the author's have introduced the route confirmation request (CREQ) and route confirmation reply (CREP) to avoid the black hole attack. In this approach, the intermediate node not only sends RREPs to the source node but also sends CREQs to its next-hop node toward the destination

node. After receiving a CREQ, the next-hop node looks up its cache for a route to the destination. If it has the route, it sends the CREP to the source node. Upon receiving the CREP, the source node can confirm the validity of the path by comparing the path in RREP and the one in CREP. If both are matched, the source node judges 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 [9], authors Satoshi Kurosawa et.al. have introduced an anomaly detection scheme to detect black hole attack using dynamic training method in which the training data is updated at regular time intervals to express the state of the network. In this scheme, the average of the difference between the Dst_Seq in RREQ packet and the one held in the list are calculated and this operation is executed for every received RREP packet. The average of this difference is finally calculated for each timeslot and it taken as the feature. Hence, it consumes considerable amount time to do calculations for every RREP packet.

In [10] Authors Ming-Yang Su et.al discussed a mechanism known as ABM (Anti-Black hole Mechanism), which is mainly used to estimate the suspicious value of a node according to the amount of abnormal difference between RREQs and RREPs transmitted from the node. When a suspicious value exceeds the limit, the nearby IDS broadcasted a block message with id of IDS, the identified black hole node and the time of identification will place the malicious nodes on their blacklists to isolate the malicious node in the network cooperatively. The advantage of this method is that it can be able to detect cooperative black hole nodes in the MANETs. The main drawback of this technique is that mobile nodes have to maintain an extra database for training data and its updating, in addition to the maintenance of their routing table.
In [11] this scheme trust based communication in MANET using AOMDV-IDS against the black hole attack. AOMDV-IDS perform real time detection of attacks using AOMDV routing protocol. In AOMDV, RREQ transmission from the source to the target establishes multiple reverse paths both at intermediary nodes in addition to the destination. Multiple RREPs navigates this reverse route back to from multiple onward routes to the target at the source and intermediary nodes. Multiple routes revealed are loop-free and disjoint. AOMDV depends on the routing information previously available in the AODV protocol, thus preventing the overhead acquired in determining multiple paths.
In [12] authors Alem, Y.F et.al. proposed a solution based on Intrusion Detection using Anomaly Detection (IDAD) to prevent attacks by the both single and multiple black hole nodes. IDAD assumes every activity of a user can be monitored and anomaly activities of an intruder can be identified from normal activities. To find a black hole node IDAD needs to be provided with a pre-collected set of anomaly activities, called audit data. Once audit data collected and it is given to the IDAD system, which is able to compare every activity with audit data. If any activity of a node is out of the activity listed in the audit data, the IDAD system isolates the particular node from the network. The reduction of the number of routing packets in turn minimizes network overhead and facilitates a faster communication.

Herminder Singh et.al. [13] have discussed the AODV protocol suffering from black hole attack and proposed a feedback solution which comparatively decreases the amount of packet loss in the network. The black holes by examining the no of sent packets at that node which will always be equal to zero for most of the cases. After the malicious black nodes have been detected, we can adopt a feedback method to avoid the reacceptance of incoming packets at these black holes. The packets coming at the immediate previous nodes to black nodes are propagated back to the sender and the sender follows an alternative

safer route to the destination. However, it cannot detect black hole nodes when they worked as a group.

V. PROPOSED INTRUSION DETECTION SYSTEM

Here we proposed the Intrusion Detection System to detect the malicious activity and give alert to normal node. We know that there are three types of IDS system. I) Network Based IDS II) Host Based IDS III) Hybrid IDS. In our paper, we implemented the Host based Intrusion Detection System. In this, all nodes are IDS nodes. if in the network one node is malicious node than others are IDS nodes. In Proposed System, there are three steps for detecting the Black Hole Attacks. In our Proposed IDs, We detect the malicious activity using total time here TOTAL TIME (TT) is calculated by CURRENT_TIME (CT) and WAITING_TIME (WT).

Step 1: Route Request (RREQ)

In this Source node (SN) is broadcast the RREQ in the network. If the RREQ entry exists in the Route Table (RT) than find the other RREQ in the network. If entry does not exists in the RT than add a new entry in RT table. Here source node is also called as IDS node because we are using the Host Based IDs System.

Step 2: Route Reply (RREP)

In RREP, node sends the RREP to the RREQ node to have a highest DEST_SEQ (Destination Sequence) number for the fresh route to transfer the packet to the Destination Node (DN). If the CURRENT_TIME is less than TOTAL_TIME (CT <<<< TT) than it store the DEST_SQ number in RREP Table. Otherwise it selects the DEST_SEQ number from the RREP table. Selected DEST_SQ number is greater than the SRC_SQ number (Dest_sq >>>>> Src_sq) than it detect the malicious node and that malicious node id (M_ID) broadcast to all nodes. and all node has store the M_ID in their RT table.

Step 3: Block Message

After Detecting the Malicious node , IDS node send the Block message to other node in the network . if malicious node id entry already exists in the RQ table than it Delete all the entries from the RT table for malicious node. If not then add the malicious node into that list.

VI. SIMULATION RESULTS

For simulation, we used the Network Simulator NS2 (2.34).We took the simulation scenario.

Parameter	Value
Simulator	NS2-2.34
Simulation Time	500s
Number of nodes	20
Routing Protocol	AODV
Traffic Model	CBR
Network Area	700 * 700

Number of malicious nodes	2

In the First scenario Figure 5, we see the packets transfer over the network with attack and with attack using proposed IDS system. When normal activity the packets are received, routed (Forward) are normal. When one Black Hole node in the network than receiving packets are decreasing same as in two black hole node. When are using the IDS system then the ratio of packet receiving are increasing.

Packet Delivery Ratio (PDR): PDR is the ratio of the number of data packets received by the destination to the number of data packets sent by the source. The Figure 6 shows that PDR under Attack are very low. After Proposed IDS PDR ratio is going to increasing with compare to under attack.

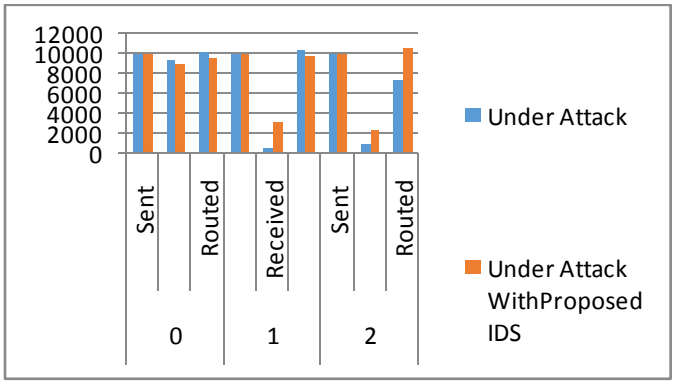

Figure 5 Sent, Received, Routed v/s Packets

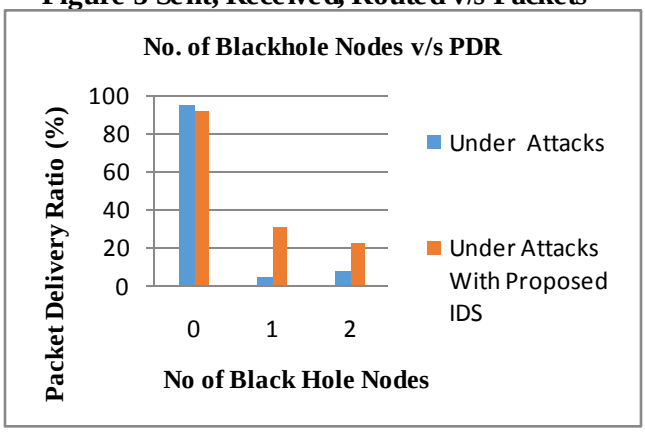

Figure 6 No. of Black hole Nodes v/s PDR

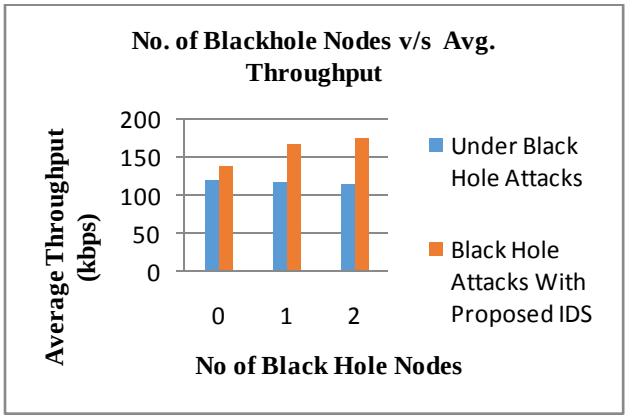

Figure 7 No. of Black hole Nodes v/s Avg. Throughput

Throughput is the no. of data packets delivered from source to the destination per unit of time. In Figure 7 under Black hole attacks the throughput are near about 120 kbps when we are using proposed IDS system then its increasing.

VII. CONCLUSION

In this Paper, We proposed the Host based approach to detect the black hole attack and a routing protocol to mitigate the effect of black hole attacks. We demonstrated through simulation that our method could effectively and efficiently detect the black hole attack. Simulation data shows that packet delivery ratio and Average throughput can be improved by 20 %. Future work will involve research into more robust and intelligent intrusion detection algorithms, as well as a choice of an anomaly detection model most appropriate for this type of IDS system. An intrusion detection system aims to detect attacks on mobile nodes or intrusions into the networks. However, attackers may try to attack the security system itself. Accordingly, the study of the defense to such attacks should be explored as well.

REFERENCES

[1] S. R. Murthy and B .S .Manoj," Ad Hoc Wireless Networks", Pearson Education, 2008.
[2] Y. Xiao, X. Shen, and D.-Z. Du," A Survey on Intrusion Detection in Mobile Ad Networks", pp. 170 – 196 °c 2006 Springer.
[3] Y. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure On-Demand Routing Protocol for Ad hoc Networks," Proceedings of the 8th Annual International Conference on Mobile Computing and Networking (MobiCom'02), pp. 12-23, September 2002.
[4] Perkins CE, Royer EM (1999),"Ad-hoc On-Demand Distance Vector Routing", Paper presented at the Second IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, Louisiana, 25-26 February 1999.
[5] IRSHAD ULLAH, SHOAIB UR REHMAN, "Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols", School of Computing Blekinge Institute of Technology, Sweden (2010).
[6] Dr. S. Tamilarasan, "Securing AODV Routing Protocol from Black Hole Attack", International Journal of Computer Science and Telecommunications [Volume 3, Issue 7, July 2012].
[7] Y.Zhang and W.Lee,"Intrusion detection in wireless ad-hoc networks", 6th annual international Mobile computing and networking conference proceedings, 2000.
[8] Seungjoon Lee, Bohyung Han, Minho Shin; "Robust Routing in Wireless Ad Hoc Networks" 2002, international Conference.
[9] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto; "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007, PP:338-346.
[10.] Ming-Yang Su; Kun-Lin Chiang; Wei-Cheng Liao, "Mitigation of Black-Hole Nodes in Mobile Ad Hoc Networks," Parallel and Distributed Processing with Applications (ISPA), 2010 International Symposium on, vol., no., pp.162-167, 6-9 Sept. 2010.
[11] Akanksha Jain,"Trust Based Routing Mechanism Against Black Hole Attack using AOMODV-IDS System In MANET Format" IJETAE, vol. 2, April 2012.
[12] Alem, Y.F.; Zhao Cheng Xuan; , "Preventing black hole attack in mobile ad-hoc networks using Anomaly Detection," Future Computer and Communication (ICFCC), 2010 2nd International Conference on , vol.3, no., pp.V3-672-V3-676, 21-24 May 2010.
[13] Herminder Singh, Shweta "An approach for detection and removal of Black hole In MANETS" International Journal of Researh in IT& Management (IJRIM) Volume 1, Issue 2 (June, 2011).