Indian Journal of Science and Technology, *Vol 9(20), DOI: 10.17485/ijst/2016/v9i20/85588, May 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Detection and Analysis of Black Hole Attack using IDS

Sandeep Kumar Arora, Shivani Vijan and Gurjot Singh Gaba*

Department of Electronics and Communication Engineering, Lovely Professional University, Jalandhar - 144411, Punjab, India; sandeep.16930@lpu.co.in, shivanivijan@gmail.com, gurjot.17023@lpu.co.in

Abstract

Mobile Ad-hoc Network (MANET) has no clear line of defense; i.e., no built-in security. Black hole attack found in network layer pretends that it has a shortest route to reach to the destination but actually consumes all the packets sent by the source. In this paper, Intrusion Detection System is implemented using NS-2 by modifying the original AODV protocol and removing the black hole node which drops the maximum packets. We also proposed a method of activating the promiscuous mode by selecting the path of highest sequence number which is helpful in achieving the better Quality of Services (QoS). The study was conducted to analyze the performance of the IDS technique over existing techniques which revealed that the Packet Delivery Ratio is improved by 60%.

Keywords: Detection, Intrusion Detection System (IDS), Normalized Routing Load (NRL), Packet Delivery Ratio (PDR), Sequence Numbers

1. Introduction

An ad hoc network is a collection of nodes that do not rely on a predefined infrastructure to keep the network connected. So the functioning of ad hoc networks is dependent on the trust and co-operation between nodes. Nodes help each other in conveying information about the topology of the network and share the responsibility of managing the network. Hence in addition to acting as hosts, each mobile node does the function of routing and relaying messages for other mobile nodes[1]. The most famous type of attack in MANET is black hole attack which used network layer and drop most of the packets by decreasing its performance. From a security point of view, Ad-hoc has no specific area of protection. After detecting the black hole attack using IDS and data is sent to the original destination by bypassing the black hole nodes[2,3].

The security issues of network layer are vital for Ad-hoc network that protecting the functionality of network to transfer the packets between the mobile nodes through multiple hop forwarding of packets. Thus, they required to ensure that the routed packet is transferred between authorized nodes along with the specification of protocols and forward the packets to each node of the network[4,5]. Due to its characteristics that are inherent of MANET, they undergone several issues that are related to security as compared with the already existing normal networks. MANET is likely to be attacked passively or actively by a multiple or single adversaries. Attacks that are more prone i.e., black hole in which it severely drops the data and as a result of this, it affects the entire operations of network as discussed in this paper. Black hole attack is most prone attack which develops and absorbs all information of routing. In black hole attack, a corrupted node transmits malicious information of routing and claims efficient path to the destination node and thus affects the other routes of the nodes and transfer packets through the corrupted node[6]. Malicious node sends frequent fake RREP message to source node claiming that it has new and shortest route to the destination node. As a result of this, source node routes its data traffic to this node and following this, malicious node drops all data traffic and doesn't forward it to the destination node. Considering an

*Author for correspondence

example in AODV, the intruder transmits a fake RREP (that includes a wrong sequence number of destination which is assumed to be higher or equal than as present in the RREQs) of the node that set to be source initially and claims that it has an efficient new path to reach the destination node as shown in Figure 1.

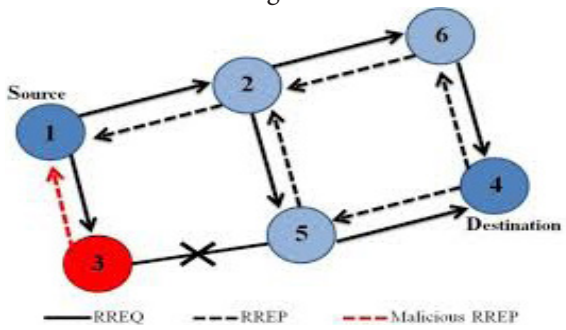

Figure 1. Effect of black hole attack in network.

This further affects the source node to attain the route send by corrupted node which is generated by the attacker. As the result of this, all packets are transferred by including the malicious node and thus the intruder will misuse the entire traffic and drop all packets[7]. According to this, the already existing methods are categorized into two main categories: secure packet forwarding protocols and secure ad hoc routing protocols. Network goals are achieved like as confidentiality, authentication, non-repudiation, availability and integrity[8,9]. Apart from the routing protocols, node density plays an important role in affecting the QoS parameters of the network. Sparse networks (with few mobile nodes) have difficulty in sending and receiving packets as nodes are not in communication range with one another[10]. Many researchers have attempted to compare the performance of these protocols by incorporating Quality of Service (QoS) metrics (viz., delay, throughput, jitter, packet delivery ratio), and other performance metrics like memory/overhead metrics and Stability based metrics. In[11] method is proposed which enables to detect the malicious nodes using valid and invalid addresses, without triggering false detection across the network. Studies reveal that AODV protocol is wisely preferred due to its ability to generate a route with minimal delay and overhead, high packet delivery ratio and throughput[12].

2. Research Methodology

The algorithm given below gives us idea of the proposed technique implemented:

Algorithm:

Step 1: Root Discovery Process

The source node S starts the route discovery phase by broadcasting the RREQ packet to the neighboring node.

Step 2: Collecting Replies

The Source node store all the replies arrived from the destination node or the intermediate nodes in terms of their DSN and NID and arrange them in terms of the decreasing DSNs in RR – Table

Step 3: Identification of Black Hole Node

Case 1: When a node is Idle:

If (CI >Th)
{Idle node Prepares 3 packets and send them as 0, 1 and 1 ms, respectively. i.e., Fcntsrc1=0; Fcntsrc2=1; and Fcntsrc3=1;
Do
{Call the procedure (Blackhole_ Detection)
Fcntsrc 1= Fcntsrc 2;
Fcntsrc 2= Fcntsrc 3;
Fcntsrc 3= Fcntsrc 1+ Fcntsrc2;}
While (Fcntsrc3 <= Fth)}
Else
{Reset Fcntsrc with the initial value}

Case 2: When a node is not Idle:

Source node retrieves the top entry from RR-Table.
Call the Procedure Blackhole_Detection
Procedure (Black hole_ Detection)
If (DSN >>> SSN)
{
Set x[Node_id] =1;
}
Else if(x[Node_id] = =1)
{Malicious node= x[Node_id];
Go to step 4}
Else
The node is not an attacker node

Step 4: Removal of Black Hole node and remove the entire malicious node(s) from RR-Table detected through Black Hole detection procedure.

Step 5: Node selection process for secure routing and sort the contents of RR-Table entries according to the DSN in decreasing order and select the node which has highest DSN.

Step 6: Continue default routing process and continue with the normal procedure of AODV.

The Abbreviations used in the above algorithm are: SSN - Source Sequence Number DSN -Destination

Sequence Number NID - Node ID CI - Communication Interval Th - Threshold Value for CI R-R Table-Route Reply Table Fth- Flow CountThreshold x[Node_Id] =Suspicious or Black Hole Node

3. Results and Analysis

The results for the following simulation parameters are presented in Table 1.

Table 1. Simulation parameters Output for Network without Attack

Simulation Parameters	Specification
Simulation Area	900×900
Simulation time	20s
Channel Type	Wireless
Antenna Model	Omnidirectional
Radio Propagation	Two Way Ground
Number of Nodes	20 and 25
Number of black hole nodes	1
Packet Size	512 bytes
Traffic Type	Constant Bit Rate (CBR)
Mobility	Random Waypoint(RWP)

In normal AODV Network for 20 and 25 nodes, as the destination node is far away from the transmitting source node, the data packets are passed through the intermediate nodes by having the parameters shown in Table 2 and Table 3 respectively.

Table 2. Comparison of different parameters for 20 nodes

Parameters (For 20 nodes)	Ideal case	Black hole attack	After removal of Black hole attack by IDS
Average Throughput (Kbps)	446.11	102.16	778.63
PDR (Packet Delivery Ratio)	0.9926	0.2271	0.9762
NRL (Normalized Routing Load)	0.19	2.785	0.061

3.2 Output for Black Hole based Network

Black hole based AODV Network for 20 and 25 nodes are studied. As the destination node is out of the range of the source node, then data packets are passed through the intermediate nodes and most of the packets are dropped by blackhole node present in the scenario. Quality of Services affected as shown in the Table 2 and Table 3. As you can see the Packet Delivery Ratio for 20 and 25 nodes respectively reduced by 76.5% and 68.5%.

Table 3. Comparison of different parameters for 25 nodes

Parameters (For 25 nodes)	Ideal case	Black hole	After removal of Black hole attack by IDS
Average Throughput (Kbps)	446.47	138.89	786.21
PDR (Packet Delivery Ratio)	0.9935	0.3089	0.9857
NRL(Normalized Routing Load)	0.212	0.645	0.053

3.3 Output after the Removal of Blackhole Attack by IDS

According to Table 2 and Table 3, when we implemented the IDS algorithm for 20 and 25 nodes it will remove the vulnerable node from the network and improve the Quality of Services (QoS). It is also described that the PDR in the IDS case is improved by 76.2% and other parameters also improved.

3.4 QoS for 20 Nodes

Figure 2, Figure 3 and Figure 4 shows that the throughput, PDR and NRL for ideal case, black hole and IDS respectively. It clearly shows that the Throughput and PDR is decreased when blackhole attack is simulated and after the removal of black hole node the value of the Throughput and PDR improved again by IDS. But when we talk about NRL which is less in the ideal and IDS case because of less overhead in the network but it is having high value in the case of black hole attack.

3.5 QoS for 25 Nodes

Figure 5, Figure 6 and Figure 7 shows that the Throughput, PDR and NRL for ideal case, black hole and IDS respectively. It clearly shows that the throughput and PDR is decreased when blackhole attack is simulated and after the removal of black hole node the value of the Throughput

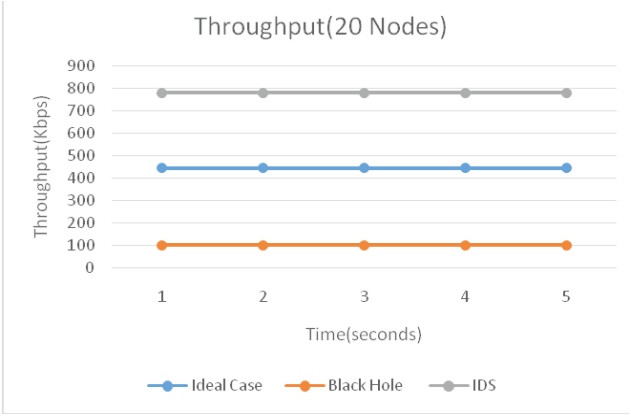

Figure 2. Throughput for three different scenarios.

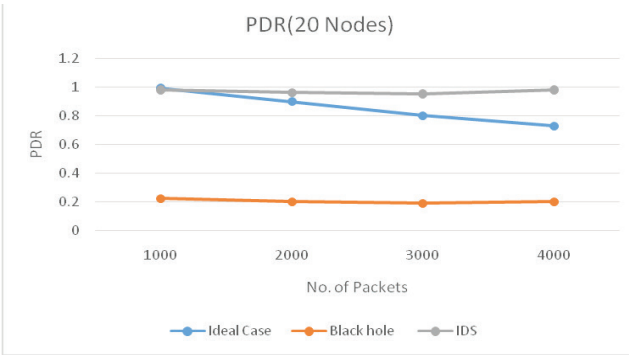

Figure 3. PDR for three different scenarios.

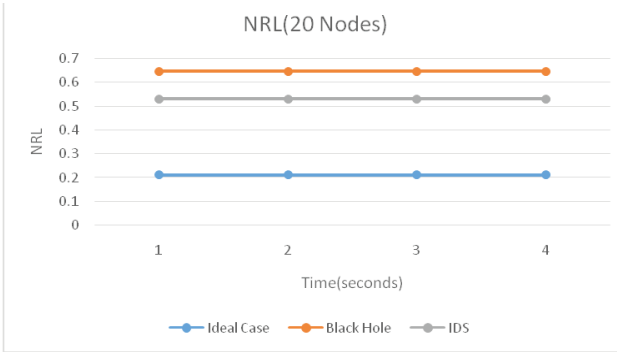

Figure 4. NRL for three different scenarios.

and PDR improved again by IDS and it approximately achieve the same value as it was present for ideal case. But when we talk about NRL which is less in the ideal and IDS case because of less overhead in the network but it is having high value in the case of black hole attack.

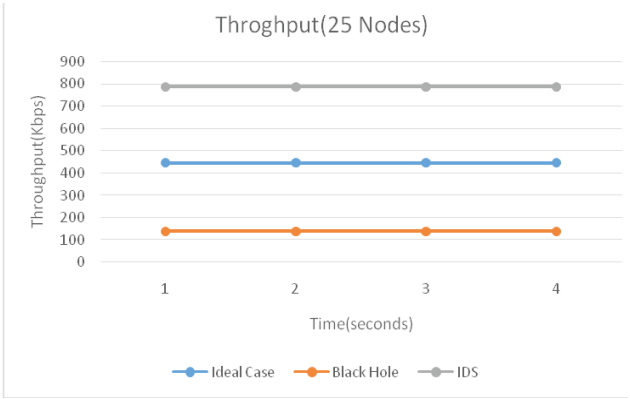

Figure 5. Throughput for three different scenarios.

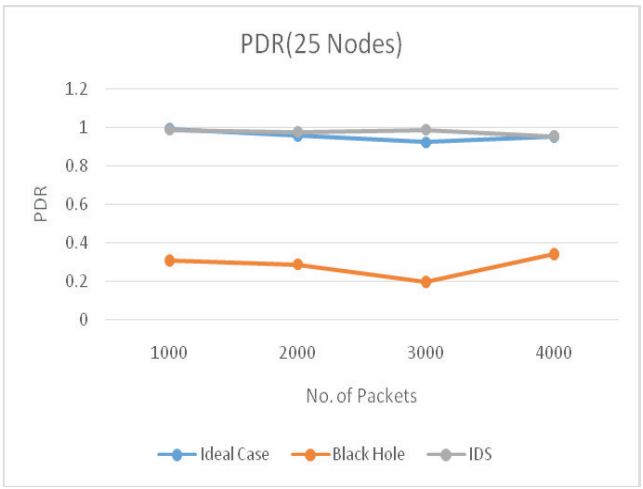

Figure 6. PDR for three different scenarios.

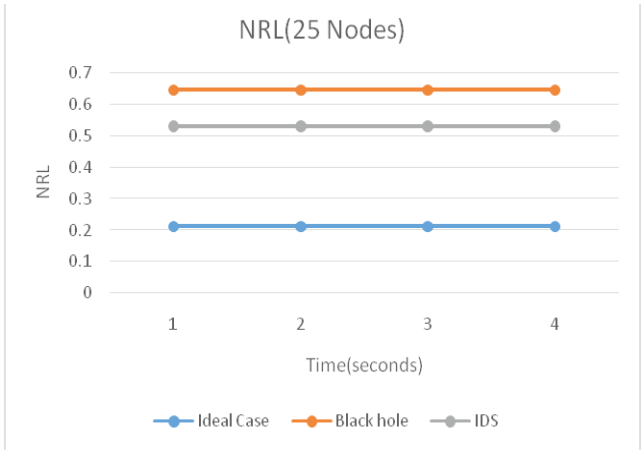

Figure 7. NRL for three different scenarios.

4. Conclusion

According to the issues of MANET security, the Black hole attack is discussed. Attack like black hole is type of Denial of Services attack in which corrupted node drop all packets by claiming new path to the destination node and after that drop all packets instead of transmitting to the node which is set to be destination. As the results obtained, it is found that the corrupted node inside the network has affected the PDR and Throughput of the system which is overcome by IDS implementation. IDS help to detect the vulnerable node which affects the QoS and removes it from the network. After implementation of IDS, improvement in QoS can be clearly seen. In future, we can simulate more attacks like wormhole, jellyfish and hijacking and will analyze the various QoS.

5. References

1. Roopak M, Reddy BVR. Performance analysis of AODV protocol under black hole attack. International Journal of Scientific and Engineering Research. 2011; 8(8):1–6.
2. De I, Roy DB. Comparative study of attacks on AODV-based mobile ad hoc networks. International Journal on Computer Science and Engineering. 2011; 3(1):313–22.
3. Saetang W, Charoenpanyasak S. CAODV free blackhole attack in ad hoc networks. International Conference on Computer Networks and Communication Systems. 2012; 35(2):63–8.
4. Jhaveri RH, Patel AD, Dangarwala KJ. Comprehensive study of various DoS attacks and defense approaches in MANETs. Proceedings of IEEE International Conference on Emerging Trends in Science, Engineering and Technology; India. 2012 Dec 13-14. p. 25–31.
5. Patel M, Sharma S. Detection of corrupted attack in MANET a behavioral approach. Proceedings of IEEE International Conference on Advance Computing Conference; India. 2013 Jun 14-15. p. 388–93.
6. Ghonge M, Nimbhorkar SU. Simulation of AODV under blackhole attack in MANET. International Journal of Advanced Research in Computer Science and Software Engineering. 2012; 2(2):1–6.
7. Bhosle AA, Thosar TP, Mehatre S. Black-hole and worm-hole attack in routing protocol AODV in MANET. International Journal of Computer Science, Engineering and Applications. 2012; 2(1):1–5.
8. Gupta H, Shrivastav S, Sharma S. Detecting the DOS attacks in AOMDV using AOMDV-IDS routing. Proceedings of IEEE 5th International Conference on Computational Intelligence and Communication Networks; Mathura. 2013 Sep. 27-29. p. 380–4.
9. Jeni PR, Juliet AV, Parthasarathy R, Bose AM. Performance Analysis of DOA and AODV routing protocols with black hole attack in MANET. Proceedings of IEEE International Conference on Smart Structures and Systems; Chennai. 2013 Mar 28-29. p. 178–82.
10. Rao M, Singh N. Performance evaluation of AODV nth BR routing protocol under varying node density and node mobility for MANETs. Indian Journal of Science and Technology. 2015; 8(17):1–9.
11. Amiri R, Rafsanjani KM, Khosarvi E. Black hole attacks detection by invalid IP addresses in mobile ad hoc networks. Indian Journal of Science and Technology. 2014; 7(4):1–6.
12. Persis JD, Robert PT. Ant based multi-objective routing optimization in mobile ad-hoc network. Indian Journal of Science and Technology. 2015; 8(9):875–88.