Combined Approach for the Analysis of Black Hole and Worm Hole Attack in MANET

Sandeep Kumar Arora* and Himanshu Monga

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

Abstract

MANET is vulnerable to most of the security threats and we proposed a combined approach which is used to detect both the black hole and worm hole attack. We also carried out black hole and worm hole attack on MANET using Ad hoc On Demand Distance Vector (AODV) routing protocol and analyzed the performance parameters like Throughput, Packet Delivery Ratio (PDR) and Normalized Routing Load (NRL). After implementation of proposed technique, we found that the parameters for Quality of Services (QoS) in MANET improved significantly as compare to conventional techniques.

Keywords: AODV, IDS, Mobile Ad hoc Network, PDR, Routing Protocols, Quality of Services

1. Introduction

Black hole and worm hole are the network layer attack which reduces the Quality of Services\(^1\). Due to its dynamic topology and lack of central coordination MANET suffers from routing management and various security loopholes\(^2\). We proposed an algorithm which is helpful for the detection of black and worm hole attack. The watchdog identifier is helpful to predict the node misbehavior and inform, but this technique suffered from the problem of imperfect collisions and limited transmission power in DSR\(^3\). In MANET the nodes are communicating with each other with the help of various protocols. In this paper, we used AODV protocol for routing the packets from source to the destination.

2. Related Work

Denning proposed the first intrusion detection model in 1987 based on hypothesis that a security can be detected through system monitoring\(^4\). They also worked for securing the network from the intruders and eliminate single malicious node from the network. Two techniques have been proposed one is when the node is in administrator mode and inside the local neighborhood and another is when the node is out of the local neighborhood\(^5,6\). Black hole detection and removal also introduced by examining the sequence number in the Route Reply Packet (RREP)\(^7,8\). After that researchers created a modified protocol namely Multi Radio Adhoc On Demand Distance Vector (MR-AODV) based on the multiple radio support. It isolates the black hole and gray hole nodes and provides the path of secure routing between source and destination and a significant improvement over PDR has been found after implementing this protocol\(^9,10\). Black hole attack found in network layer in which node pretends that it has the path to reach to the destination but when source sends the data it drops all the data and decreases the packet delivery ratio\(^11\). Worm hole attack is also found in network layer but the behavior is totally different. In this nodes creates a malicious tunnel and relay all the traffic with the help of this tunnel\(^12\).

3. Proposed Technique

The main challenge in adhoc network is the routing of data packets from the source to destination. So we require a secure routing for the transmission of data. In this paper,
we considered two attacks deployment scenario. During the black hole attack, the malicious node attracts most of the traffic and provides the lower packet delivery ratio. In case of worm hole attack the malicious node will take more time as compared to the legitimate route. Therefore, the combined technique is required, which is having information of RTT (Round Trip Time), buffer length and packet drop ratio in routing strategy. The proposed Intrusion detection algorithm is defined as:

Consider N number of nodes in the network. Source node (S) is used to direct the packet to the Destination node (D). The source sends a request packet to all the nodes to search the path to the destination and timer T_r will be started. After receiving the route reply message from the destination the timer stopped and extract the T_d. Thus the path distance between the source and destination is defined by hop count is 2H_p, So for each hop the total time is given by equation (1):

\[ R_t = \frac{T_r - T_d}{2H_p} \]  

At the time of data transmission and reception the malicious route can be prevented using the Intrusion Detection System (IDS) in the following steps:

1. Sender sends the Route Request (RREQ).
2. Timer is initialized.
3. Receiver receives a RREP (Route Reply) and stop the timer.
4. Calculate the total time R_t.
5. For each node
   a. Transmit a hello packet.
   b. Record the acknowledgement time (ack_t).
   c. If the ack_t ≤ R_t and PDR ≤ Threshold.
   d. If buffer < threshold. Select the hop as next hop.
   e. End If
   f. Else
   g. Exit from the loop.
   h. End If
6. End for

4. Simulation and Results

4.1 Simulation Environment
NS-2.35 is used for the simulation environment. We simulated our model for 20 number of nodes using random waypoint mobility model in a rectangular field (600×600 m²). AODV protocol is used for routing of packets as shown in Table 1.

| Parameter   | Definition                  |
|-------------|-----------------------------|
| Protocol    | AODV, BLACKHOLEAODV, IDSAODV|
| MAC layer   | IEEE802.11                  |
| Simulation duration | 500s                      |
| Node placement | Random                     |
| Simulation area | 600m*600m                 |
| Size of data packet | 512bytes                  |
| Traffic sources | CBR/UDP                   |
| Number of nodes | 20                        |
| Version     | NS-2 2.35                   |

4.2 Analysis of Black Hole and Worm Hole Attack
We have taken the four scenarios for every parameter viz. Ideal case, Black Hole, Worm Hole and IDS. The following results in Figure 1 has been observed for the black hole and worm hole attack and it shows that this attack is having great impact on the quality of services like throughput, packet delivery ratio and normalized routing load. In case of throughput, it decreases randomly by the introduction of single black hole node. When we compare with worm hole it is less decreased as compare to the black hole attack. By the implementation of IDS, it is again restored by the removal of black hole and worm hole.
The other parameter for comparison is packet delivery ratio and it clearly depicted from the Figure 2. that in case of black hole node it falls to 70%. But in case of worm hole it is reduced to 40%. After the implementation of IDS, the network again restored to the ideal case. So it’s again depicted that in case of black hole attack, packet drop is more compared to the worm hole.

Lastly we compare one more factor that is normalized routing load as shown in the Figure 3. that the traffic rate is found more in case of black hole due to the high packet drop ratio. Worm hole is having a low latency path so the routing load is not so much affected in this case. IDS will again approximately restore the network to the ideal case.

5. Conclusion

We analyzed the routing of packets using AODV protocol. With the help of IDS the black hole and worm hole attack can be easily detected in the network. We also analyzed that black hole attack is more harmful in MANET as compared to the worm hole. In future we can propose some other technique which is useful for the detection and removal of these attacks.

6. References

1. Zhou L, Hass JZ. Securing ad hoc networks. IEEE Network Magazine. 1999; 13(6):24–30.
2. Karpjoki V. Security in ad hoc networks. Proceedings of the Helsinki University of Technology. Seminaron Network Security; 2000.
3. Marti S, Giuli JT, Lai K, Baker M. Mitigating routing misbehavior in mobile ad hoc networks. Proceedings of the 6th annual international conference on mobile computing and networking; 2000. p. 255–65.
4. Deng H, Wei L, Agarwal PD. Routing security in wireless ad hoc networks. University IEEE Communication Magazine; 2000. p.70–75.
5. Perkins CE, Royer B, Das SR. Mobile ad hoc networking group, Internet Draft; 2003.
6. Hu CY, Perrig A. A survey of secure wireless ad hoc routing. IEEE Security and Privacy. Special Issue on Making Wireless Network. 2004; 2(3):28–39.
7. Sen J, Chandra GM, Bala muralidhar P, Harihara GS, Reddy H. A distributed protocol for detection of packet dropping attack. Proceedings of IEEE International Conference on Telecommunications, Penang; 2007. p.75–80.
8. Mistry N, Jinwala CD, Averi MZ. Improving AODV protocol against black hole attacks. Proceedings of International Multi Conference of Engineers and Computer Scientists, Hong Kong; 2010; 2:1034–39.
9. Jhaveri HR. MR-AODV a solution to mitigate black hole and gray hole attacks in AODV based MANET. Proceedings of Third International Conference in Advanced Computing & Communication Technologies, India; 2013. p.254–60.
10. Shah N, Valiveti S. Intrusion detection systems for the availability attacks in ad hoc network. International Journal of Electronics and Computer Science Engineering. 2013; 1(3):1850–57.
11. Arora KS, Mantoo YM, Chishti M, Chaudhary N. Performance measurement in MANET. Proceedings of 5th International Conference on the Next Generation of Information Technology Summit, Noida; 2014. p.406–10.
12. Reji M, Raja PCK, Joseph C, Baskar R. Performance metrics of wormhole detection using path tracing algorithm. 2015; 8(17):1–9.