Analysis and Detection of Black Hole Attack in MANET

Swati Saini¹, Vinod Saroha²

¹BPSMV University, School of Engineering and Science, Khanpur, Sonipat, India
²BPSMV University, School of Engineering and Science, Khanpur, Sonipat, India

Abstract: An Ad hoc network is the network with no fixed infrastructure. There is no central administrator so any node can come and move in and outside of the network in a dynamic manner. This makes it more dynamic and complex which makes it more prone to attacks. They can attack either active or passive. Some effects of malicious nodes are Denial of service, Routing table overflow, Impersonation, Energy consumption, Information disclosure etc. A black hole attack node attracts all packets by falsely claiming a fresh route to the destination node and absorbs them without forwarding them to destination. In this paper a mechanism based on FUZZY LOGIC is proposed to detect the black hole attack in MANET with AODV protocol. An introduction of black hole in MANET with NS2 (2.35) is done, after applying the detection technique result reflects the performance. This paper is intended for audience having prior knowledge about network routing protocols and its related quantitative performance metrics.

Keywords: Ad hoc Network, Black hole Attack, AODV, NS2.35, Detection Technique

1. Introduction

Ad hoc network has no predefined structure and no any fixed topology. All nodes can move freely in network. There is no any centralized control to control transmission and movement of nodes. All the nodes in network participate in network management task, Hence network management is done in distributed manner. Each node in the network works both as router and host. As all nodes are movable so this changes topology of the network dynamically, that brings more challenges in security of Ad hoc network.

2. Black Hole Attack

A black hole node that attracts all the packets by falsely claiming that it has valid route to destination node. [8] It disturbs the routing protocol by deceiving other nodes about the routing information. A black hole node works in the following scheme: once receiving RREQ messages, the attacker replies RREP messages directly and claims that it is the destination node or had valid route to destination node. Under these circumstances, the source node sends data packets to the black hole instead of the destination node. When the source node transmits data packets through the black hole, the attacker discards them without sending back a RERR message.

3. AODV (Ad hoc On-Demand Distance Vector)

AODV is reactive protocol Routing information is collected only when it is needed, and route determination depends on sending route queries throughout the network. When a route to a new destination is needed, the node broadcasts a RREQ to find a route to the destination. Each node receiving the request caches a route back to the originator of the request, so that the RREP can be unicast from the destination along a path to that originator. A route can be determined when the RREQ reaches a node that offers reach ability to the destination (e.g., the destination itself).

Figure 1: AODV Protocol Messaging

The route is made available by uncasting a RREP back to the origination of the RREQ. For nodes monitoring the link status of next hops for active routes, when a link break in an active route is detected, the broken link is invalidated and a RERR message is typically transmitted to notify other nodes that the loss of that link has occurred. The RERR message indicates the destination that is no longer reachable by way of the broken link.

4. Related Works

Shafinaz Buruhanudeen, Mohamed Othman, Mazliza Othman, Borhanuddin Mohd Ali [1] discuss about the existing MANET Routing Protocols in paper author highlight the important routing matrices required in evaluating the performance of the protocol in terms of reliability and efficiency. In paper they discuss some of the factor which affects the routing algorithm like such as variable wireless link quality, propagation path loss, fading; multi-user interference, power expended and topological changes become important issues.

Jiwon CAI, Ping YI, Ye TIAN, Yongkai ZOHU, Ning LIU [8] has proposed & simulated some of the attacks for DSR protocol using NS2.
Ioannis Broustis Gentian Jakllari Thomas Repantis Mart Molle[2] discuss the performance of routing protocols for large scale mobile ad hoc network larger throughput lower end to end delay fewer lost data packet. They perform the simulation on DSR, TORA, AODV, LAR in the paper discuss result derived from extended simulation and compare the efficiency of the above four protocols using NS-2 and Qualnet.

Satoshi Kurosawa, Hidehisa Nakayama [3] has been analyzed the blackhole attack which is one of the possible attacks in ad hoc networks. In a blackhole attack, a malicious node impersonates a destination node by sending a spoofed route reply packet to a source node that initiates a route discovery. By doing this, the malicious node can deprive the traffic from the source node. In order to prevent this kind of attack, it is crucial to detect the abnormality occurs during the attack. After analysis he proposed an anomaly detection scheme using dynamic training method in which the training data is updated at regular time intervals.

Md. Anisur Rahman, Md. Shohidul Islam [4] compared the performance of two prominent on-demand reactive routing protocols for mobile ad hoc networks: DSR and AODV, along with the traditional proactive DSDV protocol. A simulation model with MAC and physical layer models have been used to study interlayer interactions and their performance implications. The On-demand protocols, AODV and DSR perform better than the table-driven DSDV protocol.

Lidong Zhou [5] studied the threats an ad hoc network faces and the security goals to be achieved. After that he identified the new challenges and opportunities posed by this new networking environment and explore new approaches to secure its communication.


6. Detection Technique

The proposed work is about the prevention of blackhole attack. The proposed system is based on fuzzy based parametric analysis while performing the next node selection. The fuzzy parameters taken here are the loss rate, transmission rate and the network delay. The fuzzification on these all parameters is performed to identify the critical node as well as the safe node. On each node, the fuzzy rule is implemented to identify the safe path. The process is repeated on each node till the destination is not achieved. The system is providing better throughput and less packet loss over the network. The system is implemented in a wireless network with AODV protocol. In this system a neighbor node analysis is performed under different parameters to provide the network security in case of blackhole attack.

6.1 Algorithm for Detection of Blackhole Attack

/* S is the source node and D represents the Destination Node over the network*/
{
    1. As transmission begins it will search for all the intermediate nodes and send data on to it.
    2. The intermediate node failed forwarding the probe message to the next node;
    3. It will check the RESPONSE time for the intermediate node

    If (Response Time > HopTime + Threshold)
    
    Volume 2 Issue 5, May2013
    www.ijsr.net
The Attacker Node is detected.

Update Neighbor Node Table & Routing Table for the Intermediate Nodes

4) The unresponsive node is incapable of responding to the probe message.
5) The diagnosis algorithm will then be called to decide which one is the case.

7. Result Analysis after Applying Detection Algorithm

7.1 Analysis of Packet Lost

The figure is showing the comparison graph to represent the number of packets lost over the network. Here X Axis represents the simulation time and the y axis represents the number of packets lost in the network. In case of proposed network, the fuzzy logic is implemented. The results shows that the presented work gives the packet lost initially, but as the algorithmic approach is implemented and the route reconfiguration is done, after that no more data lost is there.

7.2 Analysis of Last Packet Time

The figure is showing the graph to represent the last packet time over the network. Here X Axis represents the simulation time and the y axis represents the last packet time. The results here shows that the in both kind of network the communication is performed on same rate but the difference is in terms of packet forwarding and rerouting of the network.

7.3 Analysis of Packet Loss Rate

The figure is showing the comparison graph to represent the number of packets lost over the network. Here X Axis represents the simulation time and the y axis represents the loss rate in the network. The results show that the presented work gives the packet loss initially, but as the algorithmic approach is implemented and the route reconfiguration is done, after that no more data lost is there.

7.4 Analysis of Bit Rate

The figure is showing the graph to represent the bit rate over the network. Here X axis represents the simulation time and the y axis represents the bit rate of data transmission.

7.5 Analysis of Packet Delay

The figure is showing the comparison graph to represent the number of packets delay over the network in Existing and Proposed Approach. Here X Axis represents the simulation time and the y axis represents the number of packets delay in the network. The results shows that the packet delay in proposed work is reduced.

8. Conclusions

This paper presents a fuzzy based detection analysis with black hole attack by using AODV routing protocol in
different scenario. This analysis is performed in wireless ad hoc network. After completion of all simulation results were analyzed in X-graph. The system is providing better throughput and less packet loss over the network. Hence detection is supported.

9. Future Work

The proposed system can be enhanced in future by other researchers in the following ways. We have performed the work only with black hole attack; the work can be enhanced by implementing some other attack such as worm hole, DOS etc. We have presented the work with a clustered approach in a wireless network. The work can be implemented on some specific network such as PAN, WiMax etc.

References

[11] ACM 978-1-4503-1310-0/12/10