A Systematic Analysis For Blackhole Intrusion Detection in MANET Using Dynamic Training Method

Iniyan E U[1], Shalini[2], Bhavani [3]
[1]Assistant Professor, Dept of ECE
[2, 3]Dept of ECE
[1]Prathyusha Engineering College,Thiruvallur, TamilNadu
[2,] TJS Engineering College,Thiruvallur, TamilNadu

Abstract- *Mobile Adhoc Network (MANET) is a Collection of Mobile host without the regained interaction of any existing infrastructure or centralized access point such as destination. Causing packet loss due to attacks by malicious nodes is one of the most important problems in MANETs. There are many ways by which loss can occur in MANETs such as broken links, transmission errors, no route to the destination and attack by malicious node. Black hole attack is also called sequence number attack because it is created using and modifying sequence number field in routing control packets. Then performed the attack and its detection method on MANETs network using Ad Hoc Distance Vector (AODV) routing protocol. In a Black Hole attack a Malicious node impersonates a destination node by sending a spoofed route reply packet to a source node that initiates a route discovery. In conventional schemes, anomaly detection is achieved by defining the normal state from static training data. In this project, presented a AODV, algorithm for the operation of such ad-hoc networks. A new routing algorithm is quite suitable for a dynamic self-starting network, as required by users wishing to utilize ad-hoc networks. In this project, an anomaly detection scheme using dynamic training method in which the training data is updated at regular time intervals. Performance analyses like Packet Delivery Ratio (PDR), Jitter, Constant Bit Ratio (CBR), Goodput, End-to-end delay are done.*

Keywords- Black hole attack, AODV, Dynamic training method, Constant Bit Ratio, Jitter.

I. INTRODUCTION

A. MANET

A Mobile Ad-hoc Network (MANET) is a dynamic wireless network that can be formed without the need for any pre-existing infrastructure in which each node can act as a router. A mobile ad hoc network (MANET) is a collection of mobile devices that can communicate with each other without the use of a predefined infrastructure or centralized administration. In addition to freedom of mobility, a MANET can be constructed quickly at a low cost, as it does not rely on existing network infrastructure. Due to this flexibility, a MANET is attractive for applications such as disaster relief, emergency operations, military service, maritime communications, vehicle networks, casual meetings, campus networks, robot networks, and so on. Unlike the conventional network, a MANET is characterized by having a dynamic, continuously changing network topology due to mobility of nodes. This feature makes it difficult to perform routing in a MANET compared with a conventional wired network. Another characteristic of a MANET is its bandwidth and limited battery power. This characteristic makes routing in a MANET an even more challenging task. Therefore, early work in MANET research focused on providing routing service with minimum cost in terms of bandwidth and optimized battery power.

B. BLACKHOLE ATTACK

In this attack, a malicious node acts like a Black hole, dropping all data packets passing through it as like matter and energy disappears from our universe in a black hole. If the attacking node is a connecting node of two connecting components of that network, then it effectively separates the network into two disconnected components as shown in Fig 1.1.

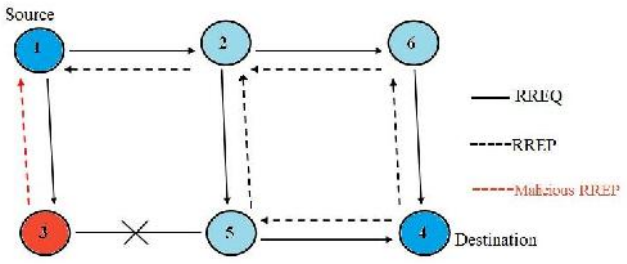

Fig 1.1 Black hole attack problem

Few strategies to mitigate the problem occurring in Black hole attack problem in MANET:

i. Collecting multiple RREP messages (from more than two nodes) and thus hoping multiple redundant paths to the destination node and then buffering the packets until a safe route is found.
ii. Maintaining a table in each node with previous sequence number in increasing order. Each node before forwarding packets increases the sequence number. The sender node broadcasts RREQ to its neighbors and once this RREQ reaches the destination, it replies with a RREP with last packet sequence number. If the intermediate node finds that RREP contains a wrong sequence number, it understands that somewhere something went wrong.

C. AODV ROUTING PROTOCOL

Each mobile host in the network acts as a specialized router and routes are obtained as needed, thus making the network self-starting. Each node in the network maintains a routing table with the routing information entries to its neighboring nodes, and two separate counters: a node sequence number and a broadcast-id. When a node (say, source node 'S') has to communicate with another (say, destination node 'D'), it increments its broadcast-id and initiates path discovery by broadcasting a route request packet RREQ to its neighbors. The (source-address, broad case-id) pair is used to identify the RREQ uniquely. Then the dynamic route table entry establishment begins at all the nodes in the network that are on the path from S to D. As RREQ travels from node to node, it automatically sets up the reverse path from all these nodes back to the source. Each node that receives this packet records the address of the node from which it was received. This is called Reverse Path Setup. The nodes maintain this info for enough time for the RREQ to traverse the network and produce a reply to the sender and time depends on network size. If an intermediate node has a route entry for the desired destination in its routing table, it compares the destination sequence number in its routing table with that in the RREQ.

II. EXISTING AND PROPOSED SYSTEM

A. EXISTING SYSTEM

Black hole Attack is a type of Denial-of-services (DOS) attack. This is also called Sequence Number Attack (SNA) because it is created by sequence number. Sequence number is monotonically increasing number and maintained by originator node of the RREQ and RREP message in the network. AODV routing protocol includes key features such as RREQ and RREP (For route discovery), RERR and HELLO message (For route maintenance), sequence number and hop count. AODV routing protocol has every route entry is assigned by destination sequence number in the routing table. RREQ and RREP message contains several of fields.

B. DISADVANTAGES OF EXISTING METHOD

- The energy consumption is a critical issue in the design of the Ad hoc networks.
- Limited bandwidth and Limited wireless connectivity range.
- Weak connectivity and remote server latency

C. PROPOSED SYSTEM

In order to detect this attack, the destination sequence number is taken into account. In normal state, each node's sequence number changes depending on its traffic conditions. When the number of connections increases the destination sequence number tends to rise, when there are few connections it tends to be increased monotonically. However, when the attack took place, regardless of the environment the sequence number is increased largely. Also, usually the number of sent out RREQ and the number of received RREP is almost the same. From these reasons we use the following features to express the state of the network.

- Number of sent out RREQ messages.
- Number of received RREP messages.
- The average of difference of Dst Seq in each time slot between the sequence number of RREP message and the one held in the list.

Here, the average of the difference between the Dst_Seq in RREQ message and the one held in the list are calculated as follows. When sending or forwarding a RREQ message, each node records the destination IP address and the Dst_Seq in its list. When a RREP message is received, the node looks over the list to see if there is a same destination IP address. If it does exist, the difference of Dst_Seq is calculated, and this operation is executed for every received RREP message. The average of this difference is finally calculated for each time slot as the feature. Comparing the proposed method (ΔT= 600(s)) with using initial training data only, the average detection rate is increased by more than 8% and the average false positive rate is decreased by more than 6%.From this result, the detection rate and false positive rate has been improved.

In the proposed method, by updating the training data it can adapt to the changing environment in MANET, while using initial training data only using only the initial training data can not adapt to the dynamically changing environment.

Therefore, that the proposed scheme is effective in anomaly detection.

D. ADVANTAGES OF PROPOSED METHOD

- It prevents security threats of black hole intrusion by notifying other nodes in the network of the incident.
- Our method not only detect black hole intrusion but also improves the overall performance of the network.

III. ATTACK METHODOLOGY

A. BLACK HOLE ATTACK ON AODV

When source node S wants to send data packet to destination node D. It creates route discovery process by using RREQ message having destination sequence number suppose 6 send to neighboring node P, Q and R. Figure 3.1. shows an example of Black Hole attack on AODV routing protocol. When neighboring node receive RREQ message from source node S it updates routing table and further rebroadcast to their neighboring nodes. Each RREQ message is uniquely identified by using RREQ Id and Source IP address that eliminate duplicates. Route reply message (RREP) is generated by either any intermediate node having fresh route information to the destination or destination node.

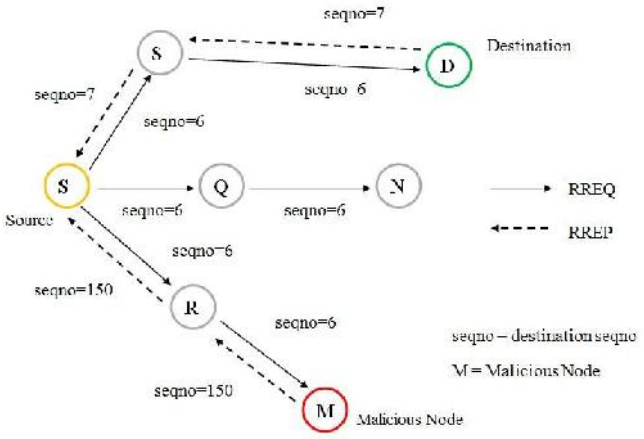

Fig 3.1 Black hole attack on AODV

B. DYNAMIC TRAINING METHOD:

Dynamic source routing (DSR) protocol is an on-demand routing protocol that is based on the concept of source routing . Mobile nodes are required to maintain route caches that contain the source routes of which the mobile is aware. Entries in the route cache are continually updated as new routes are learned.

The protocol consists of two major phases: route discovery and route maintenance. When a mobile node has a packet to send to some destination, it first consults its route cache to determine whether it already has a route to the destination. If it has an unexpired route to the destination, it will use this route to send the packet. On the other hand, if the node does not have such a route, it initiates route discovery by broad- casting a route request packet. This route request contains the address of the destination, along with the source node's address and a unique identification number. Each node receiving the packet checks whether it knows of a route to the destination. If it does not, it adds its own address to the route record of the packet and then forwards the packet along its outgoing links. To limit the number of route requests propagated on the outgoing links of a node, a mobile only forwards the route request if the request has not yet been seen by the mobile and if the mobile's address does not already appear in the route record. By the time the packet reaches either the destination or such an intermediate node, it contains a route record yielding the sequence of hops taken. This technique is called as dynamic updated training method.

IV. SOFTWARE REQUIREMENTS

A. ANALYTICAL APPROACH

Analytical modeling approach is to first come up with a way to describe a system mathematically with the help of applied mathematical tools such as queuing and probability theories, and then apply numerical methods to gain insight from the developed mathematical model. When the system is simple and relatively small, analytical modeling would be preferable . The numerical solutions to this model in effect require lightweight computational efforts.

B. SIMULATION APPROACH:

Simulation is widely-used in system modeling for applications ranging from engineering research, business analysis, manufacturing planning, and biological science experimentation, just to name a few. Compared to analytical modeling, simulation usually requires less abstraction in the model (i.e., fewer simplifying assumptions) since almost every possible detail of the specifications of the system can be put into the simulation model to best describe the actual system. When the system is rather large and complex, a Straight forward mathematical formulation may not be feasible.

C. SIMULATION PARAMETER

The following Fig 4.3 has been set up in NS2 as simulation parameters.

V. RESULT ANALYSIS

A. PERFORMANCE ANALYSIS

Network performance refers to the service quality of a communications product. There are many different ways to measure the performance of a network, as each network is different in nature and design. In this chapter, the results obtained from simulation on various scenarios are presented and discussed in detail. We have simulated Black hole attack and determined effect of attack on performance metrics such as Packet Delivery Ratio(PDR), End-to-End Delay (EED) by varying number of nodes, good put, jitter, constant bit rate(CBR), number of malicious nodes and mobility speed of nodes. Simulation parameters used to build the scenarios are shown in simulation setup. Simulations are performed using latest release of NS-2.

Fig 4.1 Terminal window

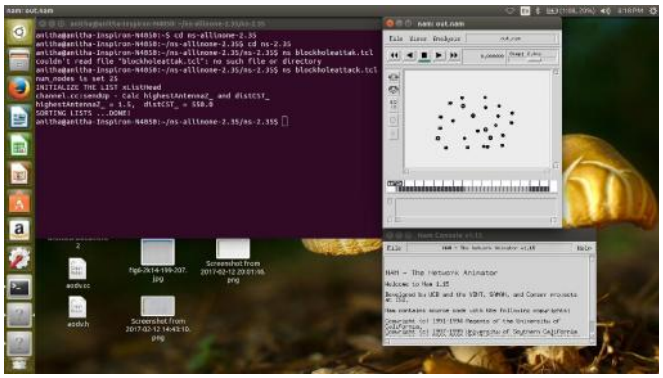

Fig.4.2 Nam console v1.15

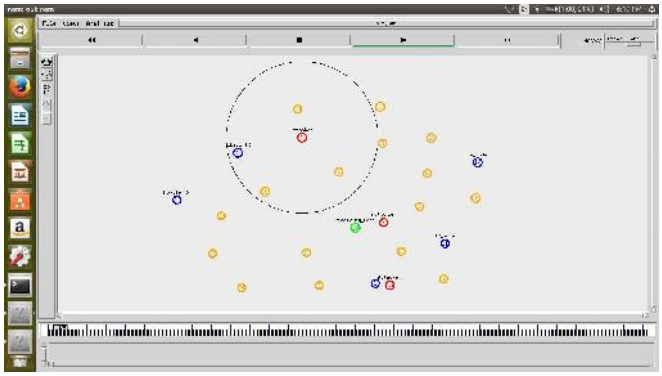

Fig 4.3 Indication of source, malicious and destination nodes

- **Packet delivery ratio**

The packet delivery time or latency is the time from when the first bit leaves the transmitter until the last is received. In case of a network connection mediated by several physical link and forwarding nodes , the network delivery time depends on the times of each link , and also on the packet queuing time and the processing delay of the forwarding nodes in wide area networks , the delivery time is in the order of milliseconds.

PDR = Number of packets transmitted successfully / Number of packets transmitted.

= 500/1242

= 0.40257649.

- **Jitter:**

Jitter is defined as a variation in the delay of received packets. The sending side transmits packets in a continuous stream and spaces them evenly apart. Because of network congestion, improper queuing, or configuration errors, the delay between packets can vary instead of remaining constant.

- **End-to-End delay:**

End-to-end delay or one-way delay (OWD) refers to the time taken for a packet to be transmitted across a network from source to destination. It is a common term in IP network monitoring, and differs from Round-Trip Time (RTT). There are basically 3 delays in end to end network.

- **Goodput**:

Goodput is the term that determines the amount of packets which is successfully received .It is also defined as the ratio between delivered amount of information, and the total

delivery time. The formula to derive goodput is,goodput=(received Size/(stopTime-startT ime))*(8/1000). The following figure shows the successful amount of packet received.

- **Constant bit rate (CBR):**

Constant Bit Rate is the rate of measure of constant number of packets transmitted between nodes in a network. Constant bit rate (CBR) is a term used in telecommunications, relating to the quality o f service. When refers to codec's, constant bit rate encoding mean that the rate at which a codec's output data should be consumed is constant.

B. STRUCTURE OF TRACE FILES

Fig 5.1 shows the structure of trace files. NS simulation can produce visualization trace as well as ASCII file corresponding to the events that are registered at the network. While tracing ns inserts four objects: EnqT, DeqT, RecvT & DrpT. EnqT registers information regarding the arrival of packet and is queued at the input queue of the link. When overflow of a packet occurs, then the information of the dropped packet is registered in DrpT. DeqT holds the information about the packet that is dequeued instantly. RecvT hold the information about the packet that has been received instantly.

Fig 5.1 Structure of trace files

Event	Time	From node	To node	Pkt type	Pkt size	Flags	Fid	Src addr	Dst addr	Seq num	Pkt id

C. GRAPH ANALYSIS

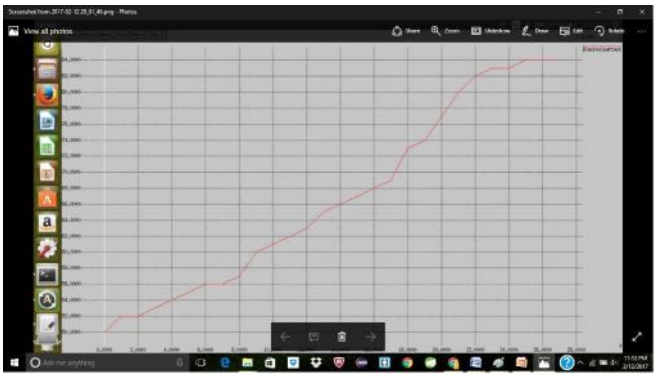

Fig 5.2(AODV) With Black hole attack

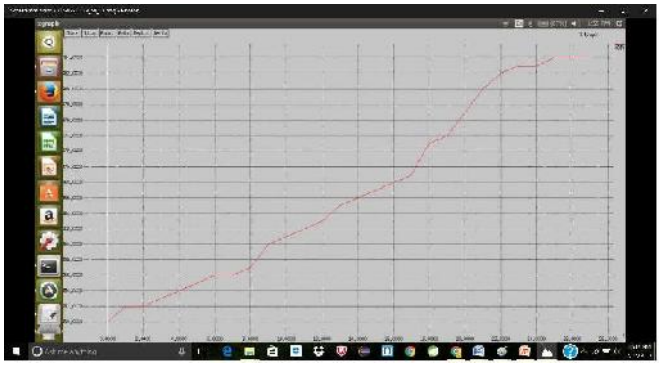

Fig 5.3(AODV)Without Black hole attack

From the above two graphs, we can see the packet loss is occurred when Black hole intrusion is present. If we take the path between node 1 to node 2, the packet loss is 45.49% when transferring packets, in the meanwhile the packet loss from node 2 to 3 is 78.56%, that depends on activity of malicious node.

Table 5.1.Packet Loss Tabulation

Path	Packet sent	Packets received	Packets drop at the blackhole 1	Packets drop at the blackhole 2	%of packet loss	%of packets lost at the blackhole
Node0-1	1097	6	246	253	99.45	45.49
Node2-3	1110	49	294	578	95.59	78.56
Node4-5	1072	2	693	80	99.81	72.11
Node6-7	1111	1	311	42	99.91	31.77
Total	4390	58	1544	953	394.76	227.93

VI. CONCLUSION

Black hole attack is one of the most important security problems in MANET. It is an attack that a malicious node impersonates a destination node b y sending forged RREP to a source node that initiates route discovery, and consequently deprives data traffic from the source node. In this project, analyzed the black hole attack and introduced the feature in order to define the normal state of the network. We have presented a new detection method based on dynamically updated training data .Through the simulation, our method shows significant effectiveness in detecting the black hole attack. Also considering performance metrics such as End-to-End Delay, Packet Delivery Ratio, Routing Overhead to implement any detection techniques in routing protocol. So here we have implemented detection module in AODV at source node. This technique does not change more functioning of the AODV routing protocol but introduces additional delay due to preprocess.

REFERENCES

[1] Nikhil Patel, Avani Dadhaniya. Detection of Black Hole Attack in MANET using Intrusion Detection System. International Journal of Advance Engineer ing and Research Development (IJAERD) Volume 1,Issue 5,May 2014.

[2] A. Bhattacharya, H. Nath Saha. A Study of Secure Routing in MANET: various attacks and their Countermeasures. IEMCON 2011 organized by IEM. January 2011.

[3] Ms A.Naveena, Dr. K.Rama Linga Reddy International Journal of Engineering Research and Applications (IJERA) Vol. 2, Issue 6, November- December 2012.

[4] Meenakshi Patel, Sanajy Sharma. Detection and prevention of Routing Attacks in MANET using AODV. In International Journal of Advanced Research in Computer Science and Electronics Engineering, 2012.

[5] A.Boukerche. Performance Evaluation of routing Protocol for AdHoc Wireless Network, Mobile Network and Application, 2004.

[6] Md.Arafatur, Jannatul Naeem. A Simulation Based Performance Comparison of routing Protocol on Mobile Ad-hoc Network. In International Conference on Computer and Communication, 2010.IEEE.

[7] Z.Ahmad, K.A.Jalil. Blackhole effect Mitigation in AODV Routing Protocol. In 2011 IEEE.

[8] Kumar B.R.Lokanatha, C.Reddy, Prakash S.Hiremath. Performance Comparison of Wireless Mobile Ad Hoc Network Routing Protocols. In International Journal of Computer Science and Network Security, June 2008.

[9] Suresh Kumar, Diwakar Pandey. Traffic pattern based Comparison of Two Reactive Routing Protocols for Ad Hoc Networks. 2009 IEEE International Conference, pages 369-373, 2009.

[10] S. Bhargava, D.P. Agrawal. Security Enhancements in AODV protocol for Wireless Ad Hoc Networks. In 2001 IEEE.