Available online at www.scholarsresearchlibrary.com

Scholars Research Library

European Journal of Applied Engineering and Scientific Research, 2012, 1 (4):84-90
(http://scholarsresearchlibrary.com/archive.html)

ISSN: 2278 – 0041

Black Hole Effect Analysis and Prevention through IDS in MANET Environment

Kamini Maheshwar; Divakar Singh

Dept. of Computer Science & Engineering, BUIT,BU, Barkatullah University, Bhopal

ABSTRACT

In Mobile Wireless Ad Hoc Networks (MANET) every node functions as transmitter, router and data sink is network without infrastructure. It must discover its local neighbors and through them it will communicate to nodes that are out of its transmission range. Various features like open medium, dynamic topology, lack of clear lines of defense, makes MANET vulnerable to security attacks. Ad hoc on-demand distance vector routing (AODV) is one of the best and popular routing algorithm. AODV is severely affected by well-known black hole attack in which a malicious node injects a faked route reply message that it has a fresh route to destination. In this paper Intrusion Detection and Response Protocol for MANETs have been demonstrated that perform better than AODV protocol in presence of Black Hole Attack, in terms of false positives and percentage of packets delivered. Security in MANET against Black Hole attack is provided by using IDSAODV routing protocol and the result are analyzed using an Optimized Network Engineering Tool NS-2, through various network parameter bases like TCP analysis , UDP analysis, Packet delivery ratio, Routing load etc.

Keywords: Mobile ad hoc network (MANET), AODV, Black Hole attack, Intrusion Detection System, IDSAODV**.**

INTRODUCTION

A mobile Ad Hoc Network is a collection of wireless nodes that are capable of communicating with each other without the help from a fixed infrastructure. It is formed dynamically by autonomous systems of mobile nodes that are connected wirelessly without support of any existing network infrastructure or centralized administration. MANET could be deployed in applications such as search and rescue, automated battlefields, disaster recovery, and sensor networks. A Mobile Ad Hoc Network is an autonomous system in which mobile hosts moves in a free and random manner. MANETs have some special characteristic features such as unreliable wireless media (links) used for communication between hosts, constantly changing network topologies and memberships, limited bandwidth, battery, lifetime, and computation power of nodes etc. While these characteristics are essential for the flexibility of MANETs, they introduce specific security concerns that are absent or less severe in wired networks. MANETs are vulnerable to various types of attacks [1].

A MANET can be examined on the basis of availability, confidentiality, authentication, integrity and non-repudiation. One of the most widely used routing protocols in MANETs is the ad hoc on-demand distance vector (AODV) routing protocol . It is a source initiated on-demand routing protocol. However, AODV is vulnerable to the well known black hole attack. Black hole attack is a type of denial of service attack in which a malicious node attract all the packets claiming a fresh enough route to the destination and dropping all the packets reaching at that node in the network. A black hole has two properties. First the node uses the ad hoc routing protocol, like AODV, to advertise itself as having a valid route to a destination, even though the route is fake , with the aim of intercepting packets and according to the second property node consumes the intercepted packets.

Intrusion is defined as "any set of actions that attempts to compromise the integrity, confidentiality or availability of resources". Intrusion detection systems (IDS) are mainly used to detect and call attention to suspicious behavior [2]. This paper discuss how to detect black hole behavior and malicious activity through the behavior analysis basis (using data filtering method) and also protection through black hole attack activity using intrusion prevention system (IPS) in AODV routing protocol. We made our simulations using NS-2 (Network Simulator version 2) simulation program.

The rest of the paper is organized as follows. Section II discusses some related work for security of MANET by routing attacks. Section III (A). describes overview of AODV protocol and Section III (B). Black hole Attack Working. Section IV presents the proposed algorithms. Section V discuss important results obtained in simulation. Section VI describes the conclusion of the paper.

II. RELATED WORK

The first intrusion detection model was developed in 1987 in which Denning proposed a model based on the hypothesis that security violations can be detected by monitoring a system check records for abnormal patterns of system usage [2]. In contrast to securing the routing layer of ad hoc networks, some researchers have also focused on simply detecting and reporting misleading routing misbehavior. Watchdog and Pathrater [4] use observation-based techniques to detect misbehaving nodes, and report observed misbehavior back to the source of the traffic. Pathrater manages trust and route selection based on these reports. This allows nodes to choose better paths along which to route their traffic by routing around the misbehaving nodes. However, the scheme does not punish malicious nodes; instead, they are relieved of their packet forwarding burden. CONFIDANT [5] detects misbehaving nodes by means of observation and more aggressively informs other nodes of this misbehavior through reports sent around the network. Each node in the network hosts a monitor for observations, reputation records for firsthand and trusted second-hand reports, trust records to control the trust assigned to the received warnings, and a path manager used by nodes to adapt their behavior according to reputation information [6]. Bansal and Baker [7] have proposed a scheme that relies on first-hand observations. Directly observed positive behavior increases the rating of a node, while directly observed negative behavior decreases it by an amount larger than that is used for positive increments. If the rating of a node dips below the faulty threshold, the node is added to a faulty list. The faulty list is appended to the route request by each node broadcasting it to be used as a list of nodes to be avoided. A route is rated good or bad depending on whether the next hop is on the faulty list. If the next hop of a route is in the faulty list, the route is rated as bad. As a response to misbehavior of a node, all traffic from that node is rejected. A second chance mechanism for redemption employs a timeout after an idle period. After a timeout, the node is removed from the faulty list with its rating remaining unchanged. Sen et al. have presented a scheme for detection of malicious packet dropping nodes in a MANET [8]. The mechanism is based on local misbehavior detection and flooding of the detection information in a controlled manner in the network so that the malicious node is detected even if moves out a local neighborhood.

III A. AODV Overview

AODV is a reactive routing protocol that does not require maintenance of routes to destination nodes that are not in active communication. Instead, it allows mobile nodes to quickly obtain routes to new destination nodes. Every mobile node maintains a routing table that stores the next hop node information for a route to the destination node. When a source node wishes to route a packet to a destination node, it uses the specified route if a fresh enough route to the destination node is available in its routing table [1]. Ad hoc on-Demand distance-Vector (AODV)[3] routing protocol uses on-demand approach for finding routes, that is, a route is established only when it is required by a source node for transmitting data packets. It employs destination sequence number to identify the most recent path. AODV works on the router request (RREQ)/routereply (RREP) query cycle. Route request packet (RREQ) is sent from source to destination node when routedoes already not exist between them. AODV uses a destination sequence number (DestseqNum) to determine an up-to-date path to destination. A node updating its path information only if the DestSeqNum of the current packet received is greater than the last destSeqnum stored at the node. In this case, a node unicast a RREP back to the source. If received RREQ is already processed simply they discard the RREQ and don't forward it. After receiving the RREP the source node will send the data packets to the destination node. If source node later receives the RREP of greater sequence number or same sequence number with less hop count then the routing table is updated and uses the better route to destination [9].

III (B). BLACKHOLE ATTACK WORKING

In Black Hole Attacks malicious nodes never send true control messages initially. To carry out a black hole attack, malicious node waits for neighboring nodes to send RREQ messages. When the malicious node receives an RREQ message, without checking its routing table, immediately sends a false RREP message giving a route to destination over itself, assigning a high sequence number to settle in the routing table of the victim node, before other nodes send a true one. Therefore requesting nodes assume that route discovery process is completed and ignore other RREP messages and begin to send packets over malicious node. Malicious node attacks all RREQ messages this way and takes over all routes. Therefore all packets are sent to a point when they are not forwarding anywhere. This is called a black hole similar to real meaning which swallows all objects and matter. To succeed a black hole attack, malicious node should be positioned at the centre of the wireless network. If malicious node masquerades false RREP message as if it comes from another victim node instead of itself, all messages will be forwarded to the victim node. By doing this, victim node will have to process all incoming messages and is subjected to a sleep deprivation attack.

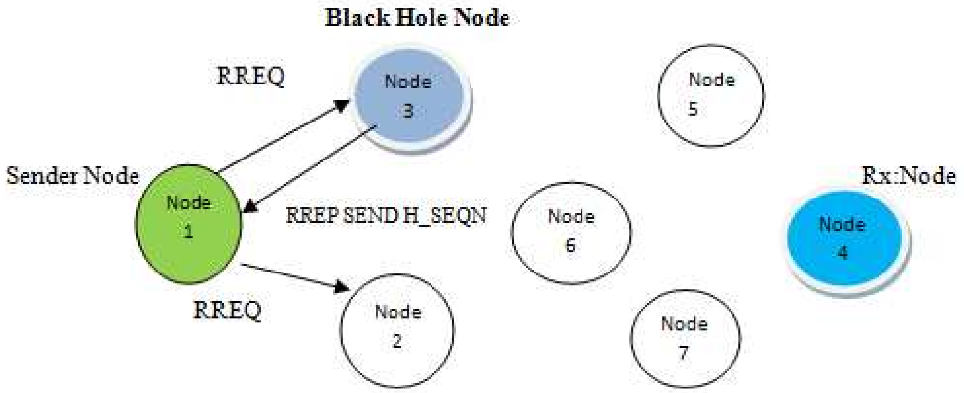


Figure 1 – Black Hole Attack scenario

In this Figure 1, we assume that Node 3 is the malicious node (Black Hole Node). Here shows node 1 as a sender node broadcast the route request packet to all radio range nearest neighbor, here node 3 malicious node certainly respond route reply packet to sender node 1 with maximum sequence number that means node 1 (sender node) assume this sequence number sends by the genuine receiver node number 4, and sender node 1 sends data packets (UDP, TCP) for node 4 (receiving node) but middle node 3 (gray hole node) capture all the UDP data packet , and can't sends TCP ACK to sender node so that TCP has Block via the Black Hole Node (3).

IV. THE PROPOSED ALGORITHM

In this section the algorithm for data processing which checks the network normal and abnormal behavior of the network is presented, first we create normal profile table then we apply algorithm for data filtering and filter the resultant part if any mislead happens in the network so node work as loop condition that means no any data receives by the genuine receiver.

IV (A). Algorithm for Behavior analysis through data processing (IDS module)

```
BEGIN {

    st[i]=0;     #Total no of Pkt send all node
    rt[j]=0;     # Total No of Mobile Node
    i=1;
    count1=0;
     node = 50;
    for(j =0; j<=node;j++)
```

```
                {
                 rt[j]=j;
                #printf("%d    %d\n",j ,rt[j]);
                }
    }
 {

        if (($1 == "s" || $1 == "d") && ($21 =="LOOP"))   // routing misbehavior module
        {
                        st[i]= $9;
                        count1 = i++;
        }
}
END {
        #for Tx
        printf("\t\t Infected Node Analysis \n\n")
        printf("\t Infected Node \t\t Total Infected Packets\n\n");
        for (j=0;j<=node;j++)
                {
             cn=1;
                for (i=1;i<=count1;i++)
                {
                        if (rt[j]==st[i])
                        {
                        s[j]=cn++;
                }
                }
                if ( s[j]>0)
                        {
                                printf("\t%d\t\t  %d \n",rt[j],s[j]);

                        }

                }
        }
```

IV(B). Algorithm for Preventing Blackhole Criteria(IPS module)

Here we implement IPS (intrusion prevention system) and call by the TCL(Tool Command Language) script in this case we internally design the algorithm for prevention of the network through the black hole behavior, IPS node acknowledge the sender node for mis-happen in the routing and also block the black hole node. All the work done under the AODV routing protocol and mobile ad-hoc network and one node created as IPS node and the network behavior through number of various parameter are analyzed.

```
        Set mobile node = M          //Total Mobile Nodes
        Set source node = S              //S Ɛ M
        Set Destination Node = D      // D Ɛ M
        Set Routing Protocol =AODV // routing protocol
        Set IPS Node = I                  // I Ɛ M
        Start simulation time = $t_0$
        Set radio range = rr;     //initialize radio range
```

RREQ_B(S, D, rr)

```
        {
If ((rr<=250) && (next hop >0))
        {
                Compute route ()
        {
            rtable->insert(rtable->rt_nexthop); // nexthop to RREQ source
            rtable1->insert(rtable1->rt_nexthop); // nexthop to RREQ destination
            if (dest =! true)
{   send ack to source node with rtable1;
    IPS (I, S , Ack )
        { send ack to sender about mislead node ;
     Block the Mis lead node that send's ACK pkt to S node;
     Comute Route ()
            if (dest == true)
            {   send ack to source node with rtable1;
            }
        Data_packet_send(s_no, nexthop, type)
         }
}
else      {
        destination not found;
      }
}
}
else { destination un-reachable ;
  }
}
```

V. SIMULATIONS

The experiments for the evaluation of the proposed scheme have been carried out using the network simulator ns-2. The simulation statistics is shown in table I. Performance of the three protocols are evaluated: (i) AODV protocol, (ii) Black hole node with AODV protocol, (iii) IDS AODV protocol i.e, Intrusion detection system based AODV protocol. Following metrics are chosen to analyze and prevent the impact of Black hole attack on the simulated network: (i) Packet delivery ratio (ii) TCP analysis (iii) UDP analysis(iv) Routing load. The chosen parameters for simulation are presented in

Table I: Simulation parameters

Simulation Duration	100 sec
Dimension of simulated area	800×600 m
Number of nodes	10 (9 normal,1 malicious)
Movement model	Random waypoint
Maximum Speed	1-25m/sec
Total number of flows	6
Traffic type	CBR, FTP
Packet rate	2 packets/sec
Data Payload	1024 byte/packet
Host pause time	10 sec.
Transmission range	250 m

Fig 1.shows the TCP1 Packet Flow Analysis graph. Red colored graph shows the no.of packets send in Normal condition using AODV protocol which is highest in this case , green colored graph shows the number of packets send in presence of black hole attack using AODV Protocol, here the loss percentage is very high and blue colored graph shows improved average packet send after applying our intrusion Detection Technique. Fig 2. shows the TCP2 Packet Flow Analysis graph. Red colored graph shows the no.of packets send in Normal condition using AODV protocol , green colored graph shows the number of packets send in presence of black hole attack , here packet are suddenly dropped after 30seconds because acknowledgment are not send back to the sender node in case of TCP due to black hole attack which is pretending to be the destination node and giving a faked route reply. Blue colored graph shows highest packet sending rate after applying our IDS Technique.

Fig 3.shows the UDP1 Packet Received Analysis graph. Red colored graph shows the no.of packets received using only AODV protocol which is highest in this case , blue colored graph shows the number of packets recieved in presence of black hole attack , which is negligible in this case and green colored graph shows improved rate of packet received after applying our IDS Technique.

Fig.4 shows the UDP PacketLost Ratio graph. Red colored graph shows minimum packet loss ratio in Normal condition using AODV protocol , blue colored graph shows the maximum number of packet loss in presence of black hole attack and green colored graph shows less packet loss ratio after applying our IDS Technique.

Fig.5 shows the Routing Load Analysis graph. Red colored graph shows the minimum routing load in Normal condition using AODV protocol , green colored graph shows more routing load percentage in presence of black hole attack using AODV protocol compare to normal condition and blue colored graph shows maximum routing load percentage after applying our intrusion Detection Technique. Here, the load increases with enhancement of AODV Protocol by Intrusion Detection System.Fig. 6 shows the Packet Delivery Ratio graph. Red colored graph shows the maximum no. of packets delivered in Normal condition using AODV protocol , green colored graph shows the minimum number of packets delivered in presence of black hole attack using AODV protocol and blue colored graph shows improved packet delivery ratio after applying our intrusion Detection Technique.

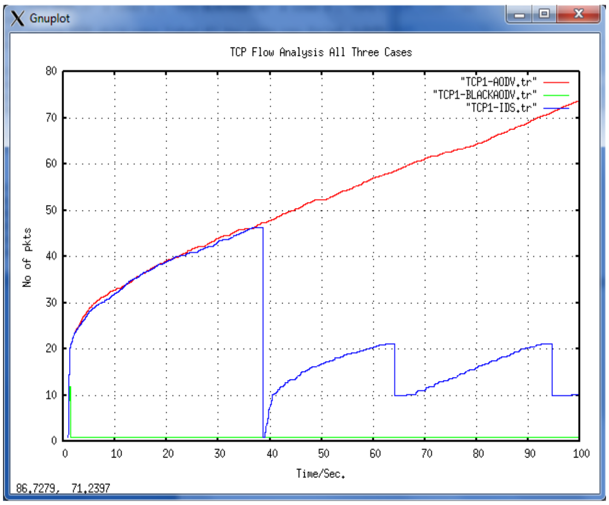


Fig 1.TCP Connection 1 Analysis

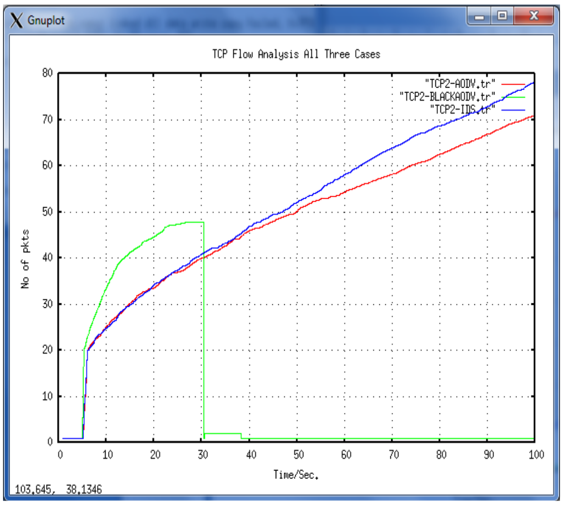
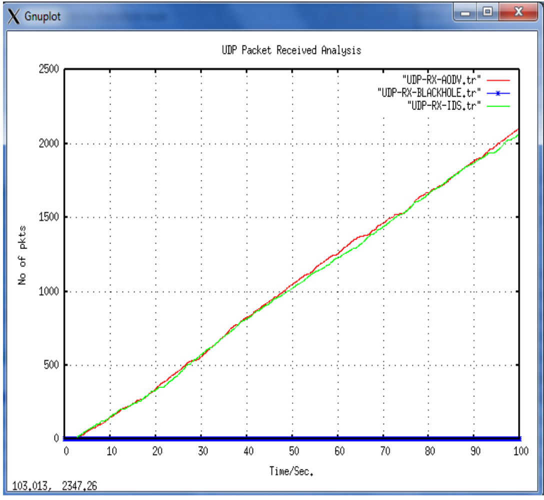


Fig 2.TCP Connection 2 Analysis



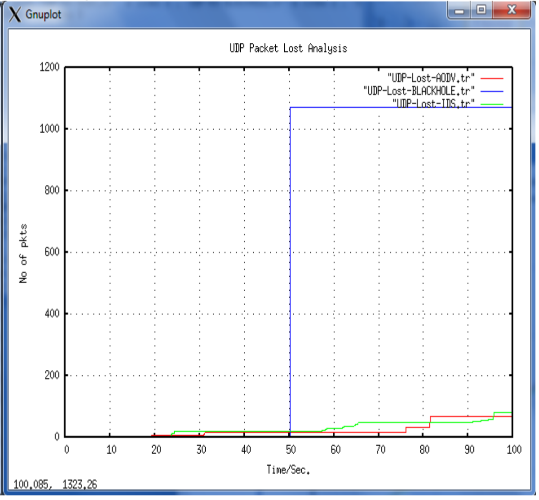
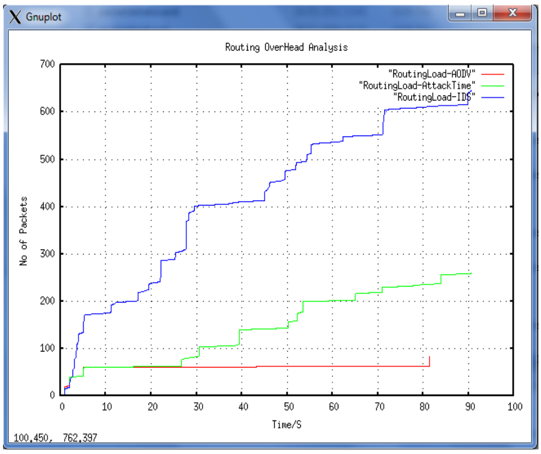


Fig.3 UDP Packet Received Analysis **Fig.4 UDP Lost Analysis**



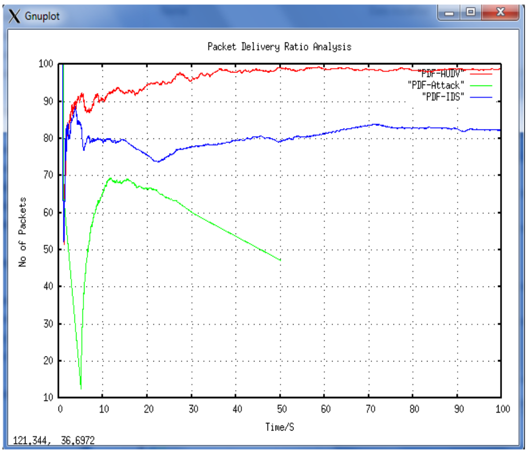


Fig 5.Routing Load Analysis Fig 6.Packet Delivery Ratio

CONCLUSION

In this Paper, detection of black hole behavior and malicious activity through the behavior analysis basis (using data filtering method) and also protection through black hole attack activity using intrusion prevention system (IPS) in AODV routing protocol are discussed. The proposed scheme has been evaluated by implementing it in the network simulator ns-2, and the results demonstrate the effectiveness of the IDS based AODV.

REFERENCES

[1] Jaydip Sen, Sripad Koilakonda, Arijit Ukil, “A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks”, Second International Conference on Intelligent Systems, Modelling, and Simulation, **2011**.

[2] L. Prema Rajeswari, R. Arockia Xavier Annie, A. Kannan, “ENHANCED INTRUSION DETECTION TECHNIQUES FOR MOBILE AD HOC NETWORKS”, IET-UK International Conference on Information and Communication Technology in Electrical Sciences (ICTES **2007**), Dec. 20-22, 2007. Pp.1008-101.

[3] C. Perkins, E. Belding-Royer, and S. Das, “Ad-hoc on-demand distance vector (AODV) routing”, Internet Draft, RFC 3561, July **2003**.

[4] S. Marti, T. Giuli, K.Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks”, In Proceedings of MOBICOM 2000, pp. 255-265, **2000**.

[5] S. Buchegger and J. Boudec,“Performance analysis of the CONFIDANT protocol: Cooperation Of Nodes-Fairness In Dynamic Ad hoc NeTworks”, In Proceedings of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing, Lausanne, CH, June,**2002**.

[6] S. Buchegger and J. Boudec, “The effect of rumor spreading in reputation systems for mobile ad hoc networks”, In WiOpt ’03: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, Mar **2003**.

[7] S. Bansal and M. Baker, “OCEAN: Observationbased cooperation enforcement in ad hoc networks”, Technical Report, Stanford University, **2003**.

[8] J. Sen, M. Girish Chandra, P. Balamuralidhar, S.G. Harihara, and H. Reddy, “A distributed protocol for detection of packet dropping attack in mobile ad hoc networks”, in Proceedings of IEEE International Conference on Telecommunications (ICT’07), May **2007**, Penang, Malaysia.

[9] A.Vani, D.Sreenivasa Rao, ”Removal of Black Hole Attack in Ad Hoc Networks to provide confidentiality Security Service”, International Journal of Engineering Science and Technology (IJEST), Vol. 3 No. 3, March **2011**.