Wormhole Detection and Prevention using Profile base Mechanism in MANET

Gajendra Singh
Head of Department of Computer Science & Engineering
Sri Satya Sai Institute of Science &Technology
Sehore (M.P)

Amrita Gayakwad
Department of Computer Science & Engineering
Sri Satya Sai Institute of Science &Technology
Sehore (M.P)

ABSTRACT
A Mobile Ad hoc Network (MANET) is a collection of self-configurable mobile node connected through wireless links. Absence of central controller it is difficult to determine the reliable & secure communication in Mobile Ad hoc network. Worm hole attack that are work as to established path in between sender and receiver but if the sender has start data transmission then in that case the worm hole attacker has create a direct link, referred to as a wormhole tunnel between them, it means more of the number of trusted nodes it means higher successful data communication process rates may well expected. In this desertion we proposed detection as well as prevention technique against wormhole attack, for detection we use profile base detection technique and get attacker node information like node number, number of attack packet, attack time etc. after that we prevent wormhole attack using neighbor trust worthy base technique and secure the mobile ad-hoc network communication, through our proposal we provide secure as well as reliable communication and simulate through network simulator-2 and analyze the network behavior in attack and prevention case.

General Terms
We measure the performance of network on the bases of network parameter like throughput, packet delivery ratio, throughput, routing load etc.

Keywords
MANET, routing, performance metrics wormhole, NS-2

1. INTRODUCTION
Mobile Ad-Hoc Network (MANET) is an infrastructure less collection of mobile nodes that can arbitrarily change their geographic locations such that these networks have dynamic topologies and random mobility with constrained resources. Two nodes out of direct communication range need intermediate nodes to forward their messages. Due to multi-hop routing and open working environment, MANETs are vulnerable to attacks by selfish or malicious nodes, such as packet dropping (black-hole) attacks and selective forwarding (gray-hole) attacks. The most target area of research in mobile ad hoc networks is to provide a trusted environment and secure communication.

There are several applications of ad hoc network which need highly protected communication. Common applications of MANET are: military or police networks, business operations like oil drilling platforms or mining operations and emergency response operation such as after natural disaster like a flood, tornado, hurricane and earthquakes [1].

In wormhole attack the attacker record the packets (bits) at one location and tunnel them in another location in same network or in different networks. The attacker can transfer each bit directly, without waiting the entire packet. It is very difficult to find out the location of wormhole attack without having packet relay information or without known infrastructure of routing protocols.

This paper is organized as follows: Section 2 is the overview of routing protocols and Section 3 covers the related work. Section 4 is proposed scheme is defined in detail and Section 5 is the description of simulation environment. Section 6 is the explanation of simulation results in details and Conclusion and future work is given in Section 7.

2. OVERVIEW OF ROUTING PROTOCOLS
There are basically three types of routing protocols: reactive routing protocol, proactive routing protocol and hybrid routing protocol. In proactive or table-driven routing protocols, each node continuously maintains up-to-date routes to every other node in the network. Routing information is periodically transmitted throughout the network in order to maintain routing table consistency. Thus, if a route has already existed before traffic arrives, transmission occurs without delay. Proactive protocols suffer the disadvantage of additional control traffic that is needed to continually update stale route entries. Since the network topology is dynamic, when a link goes down, all paths that use that link are broken and have to be repaired. If no application is using these paths, then the effort gone in to repair may be considered wasted.

In contrast to proactive approach, in reactive or on demand protocols, a node initiates a route discovery throughout the network, only when it wants to send packets to its destination. For this purpose, a node initiates a route discovery process through the network. This process is completed once a route is determined or all possible permutations have been examined. Once a route has been established, it is maintained by a route maintenance process until either the destination becomes inaccessible along every path from the source or until the route is no longer desired. In reactive schemes, nodes maintain the routes to active destinations. A route search is needed for every unknown destination.

Finally in hybrid protocols, each node maintains both the topology information within its zone and the information regarding neighboring zones that means proactive behavior within a zone and reactive behavior among zones.

3. RELATED WORK
Pallavi Sharma [1] proposed an Approach to Defend against Wormhole Attack in Ad Hoc Network Using Digital Signature. They present a mechanism which is helpful in prevention of wormhole attack in ad hoc network is verification of digital

signatures of sending nodes by receiving node because each legitimate node in the network contains the digital signature of every other legitimate nodes of same network. A wormhole is one of prominent attack which is formed by two malicious nodes and a tunnel. In order to protect from wormhole attack we used the scheme called multi hop count analysis (MHA) with verification of legitimate nodes in network through its digital signature.

Hussain in this paper [2] proposed a Denial of Service Attack in AODV & Friend Features Extraction to Design Detection Engine for Intrusion Detection System in Mobile Ad hoc Network. In this work Denial of Service attack is applied in the network, evidences are collected to design intrusion detection engine for MANET Intrusion Detection System (IDS). True Positive generated by the detection engine is very high and False Positive is suppressed to negligible. True positive will be reported very fast in Lids & Friend list generated by Lids will be sent to the Gids module for further investigation. Global Detection Engine will generate the friend list according to trust level, higher the trust level of the node may be used for other different processes like routing, and deciding the cluster head for scalable ad-hoc networks. Feature extracted for Routing parameters and MANET Traffic generation parameters can be used for different routing protocols..

Jing-Wei Huang [3,] proposed Multi-Path Trust-Based Secure AOMDV Routing in Ad Hoc Networks. In this work uses a trust based multipath AOMDV routing combined with soft encryption, yielding our so-called T-AOMDV scheme. More precisely, this approach consists of three steps:

(1) In Message encryption the source node, the message is segmented into three parts and these parts are encrypted using one another using some XOR operations,

(2) In Message routing the message parts are routed separately through different trust based multiple paths using a novel node disjoint AOMDV protocol, and

(3) In Message decryption the destination node decrypts the message parts to recover the original message.

Shreenath [4], proposed Countermeasures against Multicast Attacks on Enhanced-On Demand Multicast Routing Protocol in MANETs. This work focus on improving the Secure Enhanced-On Demand Multicast Routing Protocol (EODMRP) to safeguard it against flooding and black hole attacks. The proposed mechanism is for flooding attack works even when the identity of the malicious nodes is unknown and does not use any additional network bandwidth. The performance of a small multicast group will degrade seriously under these types of attacks even the solution is available.

Sujatha [5], proposed Design of Genetic Algorithm based IDS for MANET. In this work a technique to analyze the exposure to attacks in AODV, specifically the most common network layer hazard, Black Hole attack and to develop a specification based Intrusion Detection System (IDS) using Genetic Algorithm approach. The proposed system is based on Genetic Algorithm, which analyzes the behaviors of every node and provides details about the attack. Genetic Algorithm Control (GAC) is a set of various rules based on the vital features of AODV such as Request Forwarding Rate, Reply Receive Rate and so on.

Konate [6], proposed an Attacks Analysis in mobile ad hoc networks: Modeling and Simulation. In this title we present work is dedicated to study attacks and countermeasures in MANET.They presented several alternatives of DOS attacks met in MANETs, their operating process thus the mechanisms used and the protocols which implement them to counter these attacks.

Gandhewar [7], proposed Detection and Prevention of Sinkhole Attack on AODV Protocol in Mobile Ad-hoc Network. This work mainly focuses on sinkhole problem, its consequences & presents mechanism for detection & prevention of it on the context of AODV protocol. Sinkhole is one of severe kind of attack which attempts to attract most of network traffic towards it & degrade the performance of network. It also shows performance of AODV with no sinkhole attack, under attack & after applying our mechanism in the form of simulation result obtained for certain variation of nodes in network, by considering performance metrics as throughput, PDR, End to end delay & Packet loss.

Sharma [8], proposed An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET. In this work a solution to the black hole attack in one of the most well-known routing algorithm, ad-hoc on demand distance vector (AODV) routing, for the MANETs. The black hole attack is one of such security risks. In this attack, a malicious node falsely advertise shortest path to the destination node with an intension to disrupt the communication. The proposed method uses promiscuous mode to detect malicious node (black hole).

Jian-Ming Chang [9], proposed CBDS: A Cooperative Bait Detection Scheme to prevent malicious node for MANET based on hybrid defense architecture. They presented a mechanism to detect malicious nodes launching black/gray hole attacks and cooperative black hole attacks, known as Cooperative Bait Detection Scheme (CBDS). It integrates the proactive and reactive defense architectures, and randomly cooperates with a stochastic adjacent node. By using the address of the adjacent node as the bait destination address, it baits malicious nodes to reply RREP and detects the malicious nodes by the proposed reverse tracing program and consequently prevents their attacks.

4. PROPOSED SOLUTION

Here we define algorithm for how the wormhole attack spread onto the network basically according to definition number of different way wormhole attack spread into the network name as packet encapsulation, out of band, high power transmissions and packet relay, in this algorithm we define wormhole attack on the bases of packet relay method and define through algorithm bases, first we set normal ad-hoc network parameter and set criteria of wormhole attack scheme and spread attack onto the network.

```
Set mobile Node = N;       //Mobile Nodes
Set Sender Nodes = S;          // S € N;
     Destination Nodes = D;            // D € N;
          Routing Protocol = AODV;
Set Simulation Time = T
Set Radio Range = RR;    // Initialize Radio Range
AODV_RREQ_B (S, D, RR)
        {
If ((rr<=550) && (next hop >0))
        {
        Compute route ()
        {
 rtable->insert(rtable->rt_nexthop); // next hop to RREQ source
        if (next_hop work correct route to destination )
                {
                next_hop(S,next_hop,D)
                                {
Next_hop_rtable=rtable ;  // if in future RREP Sends via
                        //link
                                }
Next_hop_RREQ_B -> till the Destinaion reachable ;
 rtable1->insert(rtable1->rt_nexthop); // nexthop to RREQ destination
        if (dest==true)
        {           send ack to source node with rtable1;
```

```
        Data_packet_send(s_no, nexthop, type)
                                        }
                                else    {

        destination not found;
                                        }
        }
     Else
    {// Wormhole Node spread route misbehaver module;
       Set misbehaver node = W1, W2; //W1 next to sender and
W2 neighbor of W1 both cooperatively work and both belong in
between S to D and W1 and W2 both set high transmission power
     If (W1 in radio range && active && transmission = =
        High)
        {
    If ( next hop W2 is next neighbour of RREQ_B Sender)
      {
    Update routing Table;
    Increase Hop count++;
        }
        Send W1 certainly RREP to S;
        S next RREQ to Next hop other Than W1 ;
        RREQ_Receive -> W2   //Other Than W1
        Send RREP (W1 is best path to destination)
    //Sender sends data packets through W1 ,W2 path to D
    Data_packet_send(s_no, nexthop, type)
         {
    if (Data type ==”UDP”)
              { discard data Pkts ;
        }
          Else { Block The data pakts ; }
         }
                                }

                        }
                        }
         Else {
                        destination un-reachable;
                         }
    }
```

4.1 Profile Base Prevent through Wormhole hole Attack

we apply profile base detection and route trust base prevention technique, for securing data communication. very first we generate normal activity profile and compare with new generated profile if not match that means our new arrival data is unsecure data and we get particular attacker node and if we found attacker node than we apply route trust mechanism and block the attacker node and prevent the our network communication against wormhole attack.

```
    While ( S send RREQ_B)
    {       rtable -> insert(rtable->rt_nexthop);
    Add extra filed to rtable (next_hop , Through)  //both value 1
, 0 formate
    If (new_profile == base_profile)
    {
    No any attack
    }
           Else If( (next_hop = true)&&
      (through == true)&&(send_D_pkt==true)&&
       (new_profile == base_profile))
                {
            True route ;
                }
    Else if  ((next_hop = false)&&
    (through == false)&&
    (new_profile != base_profile))
                 {
          In previous No data and route through that hop;
    Insert into ->rtable; // for route to destination if shortest path
        Cerate new Profile;
    }
Elseif ((next_hop = true) && (through == false) &&
(send_D_pkt==true))
    {
    In previous No data through that hop;
    But exist in rtable enetry ;
        //Check reliability
     if next hop(new_profile != base_profile);
                 {
    Block that Hop ;
    }
    else
    {
    Send RREQ_B till the Destination }
     }

    Else
    {
        Send_RREQ_B to next other hop ;
            Search destination D;
             }
     }
```

5. SIMULATION ENVIRONMENT

The entire simulations were carried out using ns 2.31[10] network simulator which is a discrete event driven simulator developed at UC Berkeley as a part of the VINT project. The goal of NS2 is to support research and education in networking. NS2 is built using object oriented language C++ and OTcl (object oriented variant of Tool Command Language). NS2 interprets the simulation scripts written in OTcl. The user writes his simulation as an OTcl script.

5.1 Simulation Parameters

The simulation of normal AODV, Wormhole attack and IPS scheme are done the basis of following simulation parameters that has shown in table1. In case of normal routing all the consider all 30 nodes but in case of wormhole attack consider 2 nodes as a attacker and remaining 28 are normal nodes and in case of IPS one node is IPD node, 2 nodes are attacker and rest of them are normal.

TABLE1. Simulation Parameters

Simulator Used	NS-2.31
Number of nodes	30
IPS node	1
Wormhole Attacker	2
Dimension of simulated area (meters)	800 × 600
Routing Protocol	AODV
Simulation time	100 sec.
Traffic type (TCP & UDP)	FTP & CBR
Packet size	512 bytes
Number of traffic connections	3 TCP, 2 UDP
Node movement at maximum Speed	random & 20 m/s
Transmission range	250m

6. SIMULATION RESULTS

Simulation results are evaluated on the basis of performance parameters like overhead, throughput etc. The simulation results are measured in case of normal AODV routing, in case of wormhole attack and after applying protection IPS scheme.

6.1 Packet Delivery Ratio analysis in case of Normal, Wormhole and IPS

This graph represents the Packet Delivery Ratio (PDR) analysis in case of normal AODV routing, in case of wormhole attack and in case of Intrusion Prevention System (IPS) scheme. Here the case of normal routing is only considered to match the network performance after applying protection scheme. Here we clearly visualized the effect of wormhole attack in network by that only about 30% packet delivery is possible in network at initial stage of simulation and after that the network performance are nearly zero and after about 50 second no PDF value is measure in network. But in case of after applying protection scheme i.e. IPS, the performance of network almost equal to normal means about 94% PDR are improves after applying security scheme against attack.

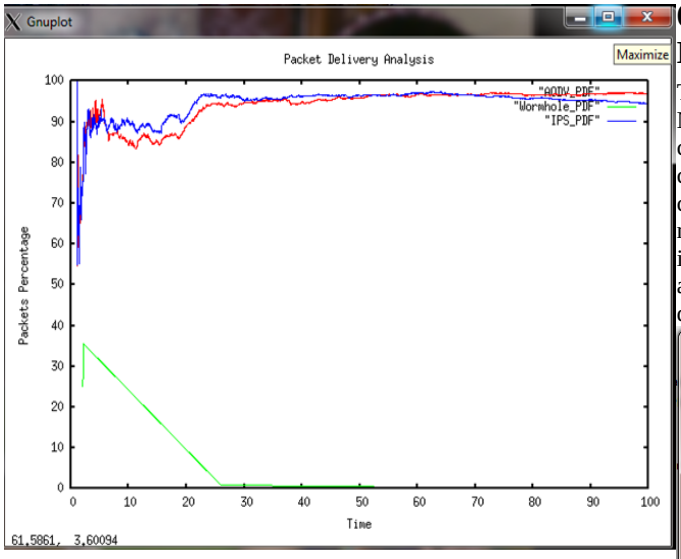

Fig. 1. PDR Analysis

6.2Routing load analysis

The routing load analysis is required to find the number of routing packets is delivering in network to established connection in between sender and receiver. In this graph the routing load or number of routing packets in case of IPS are high almost about 1300 routing packets are deliver in network then next in case of normal routing about 900 routing packets are deliver in network but at last the routing load in case of wormhole attack are minimum about only 500 packets are deliver in network. The important point of normal routing is the minimum value of routing packets are show the better performance in network and this performance is determine in case of attack and the important point is that in minimum routing packets the actual data packets are deliver in network are negligible as compare to normal and IPS routing. In case IPS the routing packets are more deliver because of identifying the secure path for communication.

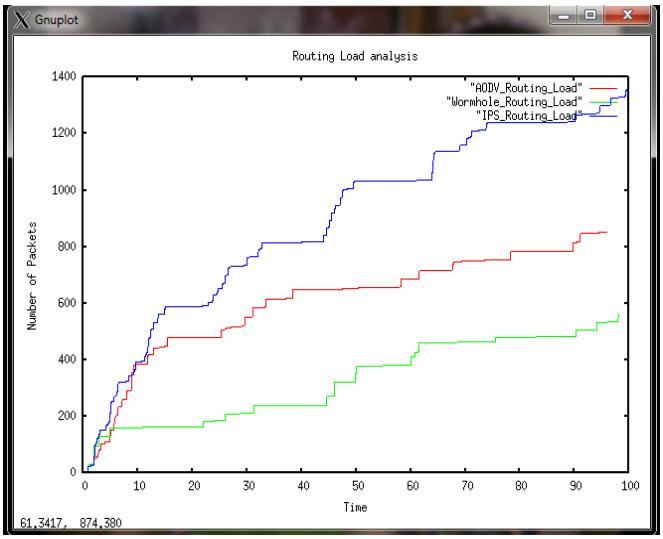

Fig. 2. Routing overhead Analysis

6.3 UDP Packet Receive analysis in case of Normal, Wormhole and IPS

This graph represents the UDP Packet analysis in case of Normal, Wormhole attack and IPS scheme. Because of the connection less nature the UDP protocol are not reliable for communication but network conditions are better than in that case the UDP. Here the UDP packets are almost equally received in case of attack and IPS i.e. about 2300 and 2200 but in case of wormhole attack only a single packet is received at about 60 seconds, it means negligible packets are received at destination end in presence of attack.

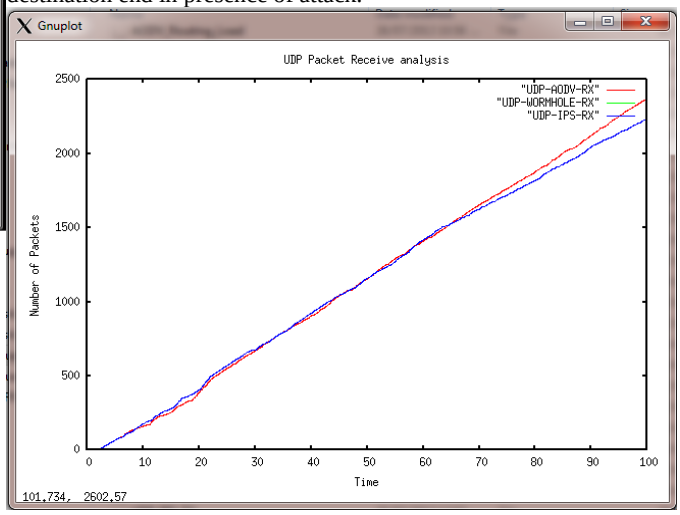

Fig. 3. UDP packet receive analysis

6.4 Infection from Wormhole

Infection percentage represents the infection percentage w.r.t time. Infection percentage in case of worm attack is continuously increases reach up to 49%. At time about after 4 sec. the infection are in maximum percentage value but at the time of IPS the infection percentage is zero and not a single packet is affected by wormhole attack.IPS will block the whole activity of wormhole attack and remove the infection from network.

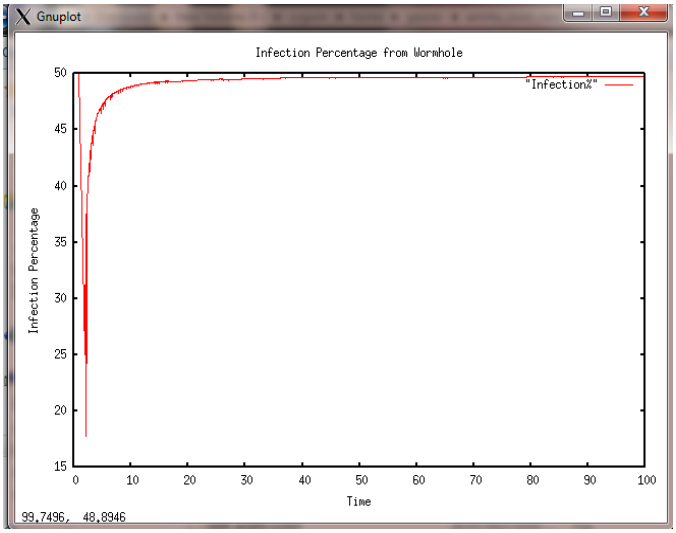

Fig. 4. Infection Percentage

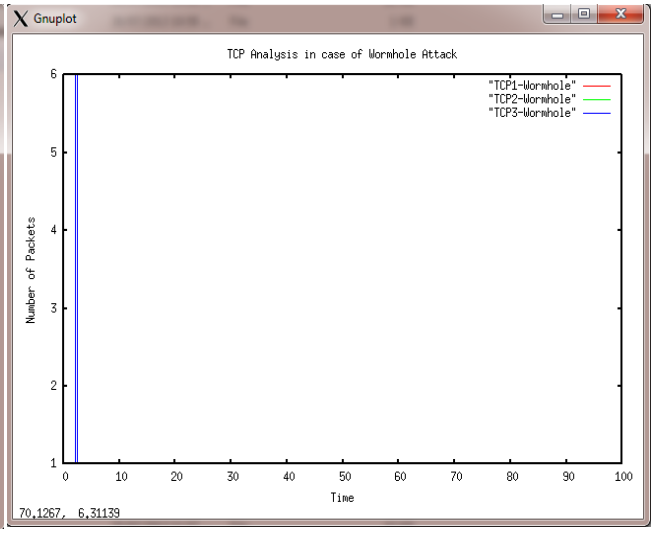

Fig.6. TCP packets delivery of IPS Scheme

6.5 TCP analysis of AODV Routing Protocol

Transmission Control Protocol (TDP) are the connection oriented reliable protocol for communication in network in between sender and receiver. There are three TCP connections are created in network and the performance of all the connections is measurable. The congestion window of TCP 2 connection are high means about more than 70 packets are deliver in network, after that the congestion window of TCP 1 are size of about 20 and at last the size of TCP 3 connection congestion window are about 1 packet.

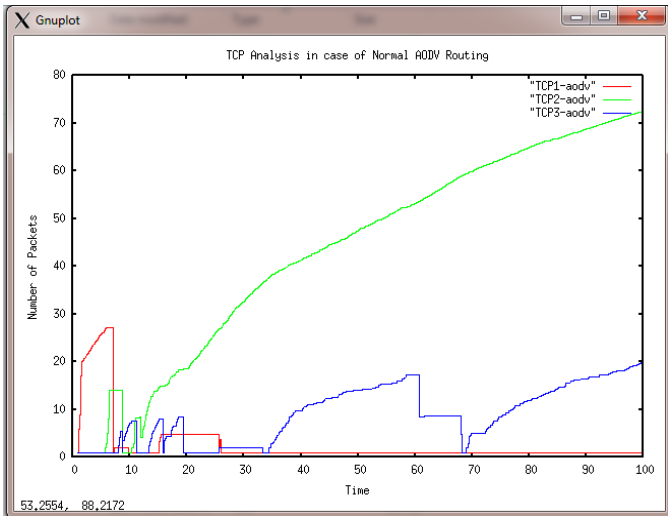

Fig.5. TCP packet performance of AODV Routing Protocol

6.6 TCP Packet Analysis in case of Wormhole Attack

In this graph the TCP 1, TCP 2 and TCP 3 connections packets are shown in this graph, only the 6 packets of TCP 3 connections at time about 2 seconds are deliver in network after that not a single packet are deliver in network. It means the wormhole attack completely fails the network performance of reliable protocol.

6.7 TCP Packet analysis in case of IPS Scheme

This graph represents the TCP packets analysis in case of applying prevention scheme against wormhole attack. Here we clearly notice the performance of all TCP connections. The size of congestion window is only varying but the packet delivery is almost same as normal routing i.e. shown in figure 5. The Protection IPS scheme is definitely improves the performance of network and blocks the misbehavior activity of wormhole attacker.

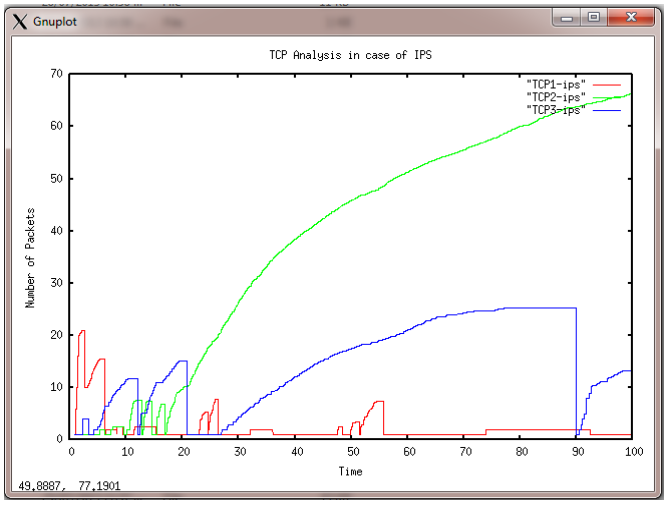

Fig.7. TCP packets delivery of IPS Scheme

6.8 Summary in case of normal routing, wormhole attack and IPS scheme

The table 2 presents the summery of or actually represents the performance of normal routing, wormhole attack and IPS scheme are presented here in the foam of performance parameters.

Table2.2

Table.3 Performance Parameters	Normal AODV Routing	Wormhole Attack	IPS Scheme
Packets Send	5946.00	2491.00	5691.00
Packets Receive	5762.00	7.00	5376.00
Routing Packets	853.00	563.00	1358.00
PDF	96.91	0.28	94.46
NRL	0.15	80.43	0.25
Average e-e delay(ms)	432.70	37.89	837.73
Number of Data Drop	179	2484	311

7. CONCLUTION AND FUTURE WORK

Mobile Ad Hoc Networks have the ability to setup networks in a cruel environment where it may not possible to deploy a traditional network infrastructure. Whether ad hoc networks have vast potential, still there are many challenges left to overcome.. Security is such an important feature that it could determine the success and wide deployment of MANET. The wormhole attack is a type of attack that performs the malicious activity by creating own link and avoids actual link i.e. the actual path for data delivery. The overall idea of this algorithm is to detect malicious nodes launching attacks and misbehaving links to prevent them from communication network. This protection scheme provides the protection against wormhole attack and blocks the activities of attacker node. In case of attack almost the network performance is completely down but proposed IPS scheme improves performance nearly equal to normal routing. This work explores a vigorous and a very simple idea, which can be implemented and tested in future for more number of attacks, by increasing the number of nodes in the network.

In future we also examine the behavior of other attacks like Gray hole attack and Black hole attack and try to make the protection schemes on it and also try to enhance the performance of routing protocol that has consider in this dissertation to improves their routing capability.

8. REFERNCES

[1] Pallavi Sharma, Prof. Aditya Trivedi "An Approach to Defend Against Wormhole Attack in Ad Hoc Network Using Digital Signature", 3rd IEEE International Conference on Communication Software and Networks (ICCSN), pp. 307 – 311, 2011.

[2] Husain. Shahnawaz, Gupta S.C., Chand Mukesh "Denial of Service Attack in AODV & Friend Features Extraction to Design Detection Engine for Intrusion Detection System in Mobile Ad-hoc Network", International Conference on Computer & Communication Technology (ICCCT-2011), pp. 292- 297, 2011.

[3] Jing-Wei Huang, Isaac Woungang, Han-Chieh Chao, Mohammad S. Obaidat, Ting-Yun Chi, Sanjay K. Dhurandher "Multi-Path Trust-Based Secure AOMDV Routing in Ad Hoc Networks", proceedings of IEEE Global Telecommunications Conference (GLOBECOM 2011), pp. 1-5, 2011.

[4] Dr. N. Sreenath, A. Amuthan, & P. Selvigirija "Countermeasures against Multicast Attacks on Enhanced-On Demand Multicast Routing Protocol in MANETs", International Conference on Computer Communication and Informatics (*ICCCI* -2012), pp. 1-7, 2012.

[5] K. S. Sujatha, Vydeki Dharmar, R. S. Bhuvaneswaran "Design of Genetic Algorithm based IDS for MANET", International Conference on Recent Trends in Information Technology (ICRTIT), pp. 28-33, 2012.

[6] Dr Karim KONATE, GAYE Abdourahime "Attacks Analysis in mobile ad hoc networks: Modeling and Simulation", 2011 Second International Conference on Intelligent Systems, Modelling and Simulation, pp. 367 – 372, 2011.

[7] Gandhewar, N., Patel, R. "Detection and Prevention of Sinkhole Attack on AODV Protocol in Mobile Adhoc Network", Fourth International Conference on Computational Intelligence and Communication Networks (CICN), pp. 714 – 718, 2012.

[8] Singh, P.K. Sharma, G. "An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET", IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 902 – 906, 2012.

[9] Jian-Ming Chang, Po-Chun Tsou ; Han-Chieh Chao ; Jiann-Liang Chen "CBDS: A Cooperative Bait Detection Scheme to prevent malicious node for MANET based on hybrid defense architecture", 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronics Systems Technology (Wireless VITAE), pp. 1-5, 2011.

[10] http://www.isi.edu/nsnam/ns/.