A Novel Nearest Neighbour Information based Security Scheme (SS) against Wormhole Attack in MANET

Sunil Kumar Sharma, Sitesh Kumar Sinha, Mukesh Kumar

Abstract— Mobile Ad hoc network (MANET) is a collection of nodes that are capable to form a temporary dynamic network without the support of any centralized administration and fixed infrastructure. Because of the absence of central controller it is difficult to determine the reliable & secure communication in Mobile Ad hoc network. That's why the security is the one of the most significant issue in MANET. Worm hole attack is a type of 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 and all the data pass through that tunnel. In this research we proposed detection as well as prevention Security Scheme (SS) against wormhole attack, for detection we use nearest neighbor information of hop count and get attacker node information like node number, number of attacker and infected packets it means trustful communication among the nodes by that the higher successful data communication process rates may well possible. After that we prevent wormhole attack using neighbor trust valuable base technique and secure the mobile ad-hoc network communication, through our proposal we provide secure as well as reliable communication in network from wormhole attack and measure the performance of network on the bases of network parameter like packet delivery ratio, throughput and routing load.

Index Terms— MANET, SS, routing, nearest neighbor, security, performance metrics, wormhole attack

1 INTRODUCTION

MOBILE Ad-Hoc Network (MANET) is an infrastructure less network of mobile nodes that can arbitrarily change their locations such that these networks have dynamic topologies and random mobility with constrained resources. They also have capability of network partition [1]. A mobile ad hoc network (MANET) is a self-organized multi-hop system comprised of mobile wireless nodes. Two nodes out of direct communication range need intermediate nodes to forward their messages. Routing in MANET' is difficult due to node mobility, lack of predefined infrastructure, and limited transmission range. Due to multi-hop routing and open working environment, MANETs are vulnerable to attacks by selfish or malicious nodes, such as packet dropping also called black-hole attacks and selective forwarding attack also called gray-hole attack.

It is assure that MANET is to solve or disputing real world problems continues to seek the attention from industrial and academic research projects. The most target area of research in mobile ad hoc networks is to provide a trusted environment and secure communication.

In wormhole attack the attacker record the packets 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.

In this paper, an efficient security scheme of to detect and prevention from wormhole attack called nearest neighbor based wormhole detection with AODV protocol has been proposed. Detection of wormhole attack is performed using number of hops in different paths from source to destination and hop information of each node in different paths from source to destination. The proposed Security Scheme (SS) is able to detect both kinds of wormhole attacks.

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 PROTOCOL

The routing protocols [2] are required to established connection and data delivery in network. Each protocol having a different routing mechanism to established the route in network. 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. The Destination Sequence Distance Vector (DSDV) is example of proactive routing protocol.

The reactive or on demand protocols, a node initiates a route

- *Sunil Kumar Sharma is currently pursuing masters degree program in computer science & engineering in AISECT"University,Bhoapl,INDIA, sunil.babloo.sharma@gmail.com*
- *Sitesh Kumar Sinha,(Dean of AISECT University) AISECT University Bhopal, India, siteshkumarsinha@gmail.com*
- *Mukesh Kumar is currently Assistant Professor in computer science & engineering in AISECT University, Bhopal, INDIA, goutam.mukesh@gmail.com.*

discovery throughout the network, only when it wants to send packets to its destination. 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. The Ad hoc On Demand Distance Vector Routing (AODV) protocol is the example of reactive routing protocol.
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. The Zonal Routing Protocol (ZRP) [3] is the example of that kind of routing protocol.

3 Related Work

As In the section of related we mentioned the work that has done in the field of wormhole attacker to prevent and detect and also affect of attack in routing protocols.
Ravinder Ahuja , Alisha Banga Ahuja and Pawan Ahuja, [1] evaluate the performance of AODV and DSR routing protocol under wormhole attack and compare the performance of these protocol without wormhole attack. Performance parameters are Average end to end delay, Throughput, and Packet delivery ratio (PDR). In future they provide solution that will detect and defend the wormhole attack so that network and routing protocols functioning is not disturbed.
Drawbacks of this research

- In this paper the routing performance is measured but only shows the affect of worm hole in AODV routing protocol and DSR routing protocol.
- In 50 nodes how much nodes are creating the tunnel and drop the packets are not detect.
- This scheme is only show the comparison of routing protocols in case of wormhole attack but there is totally need less.

Umesh kumar chaurasia and Varsha singh [4] proposed an efficient method to detect a wormhole attack called modified wormhole detection AODV protocol has been proposed. In Modified AODV (MAODV), a concept to detect wormhole attacks in the network by collecting both numbers of hop count and delay per hop information for different paths from source to destination, which offer a full general solution for both kinds of wormhole attacks. The reason behind is that under legitimate situation, the delay for each packet is similar along each hop in the path and the delay for each packet should be excessive for those nodes are involved in the wormhole attack because there can be many nodes between them or can be connected through a long link.
Drawbacks of this research

- The attacker effect is measured in light weight traffic. Moderate traffic and high traffic but here the comparison table is show in between normal traffic and attacker traffic not show in after applying security in network.
- This scheme is only detect the wormhole attack not prevent from attack in network.
- The wormhole attack is routing layer attack then why the routing load and throughput is not measured.
- On the basis of traffic loss, how it says the attacker is not completely affected the network.

Pallavi Sharma and Aditya Trivedi proposed an Approach to Defend against Wormhole Attack in Ad Hoc Network Using Digital Signature [5]. 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. Destination node analyzes the number of hop count of every path and selects the best path for replying. In this solution, if sender wants to send the data to destination, firstly it creates a secure path between sender and receiver with the help of verification of digital signature. If there is presence of any malicious node in between the path then it is identified because malicious node does not have its own legal digital signature.
Dr. N. Sreenath, A. Amuthan, & P. Selvigirija [6] 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 beside flooding and black hole attacks. This 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 proposed algorithm provides protection against black hole attack in MANET.
K. S. Sujatha, Vydeki Dharmar, R. S. Bhuvaneswaran [7] proposed Design of Genetic Algorithm based IDS for MANET. In this work the proposed scheme 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.
Dr Karim Konate, Gaye Abdourahime [8] proposed an Attacks Analysis in mobile ad hoc networks: Modeling and Simulation. In this research, work is dedicated to study attacks and countermeasures in MANET. After a short introduction to what MANETs are and network security they present a survey of various attacks in MANET pertaining to fail routing protocols in network. It also presents the different tools used by these attacks and the mechanisms used by the secured routing protocols to counter them. In this defined the concept of DoS like its various types. They presented several alternatives of DoS attacks met in MANET, their operating process thus the mechanisms used and the protocols which implement them to counter these attacks.
N. Gandhewar, R. Patel [9] proposed Detection and Prevention of Sinkhole Attack on AODV Protocol in Mobile Ad-hoc Network. This work is 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 efforts to catch the attention of most of network traffic towards it & degrade the performance of network. AODV is mainly analyzed under blowhole, wormhole & flooding attack, which needs to analyze under other kinds of attack also.

S. Gupta, S. Kar and S. Dharmaraja [10] proposed a Wormhole Attack Detection Protocol using Hound packet called WHOP for detecting wormhole attacks without using any special hardware or monitoring system. In this detection scheme after route discovery process source node uses a hound packet to detect wormhole attacks which counts hop difference between the neighbors of the one hop away nodes in the route. After the process the destination node detects the wormhole based on the hop, difference between neighbors of nodes exceeds the acceptance level.

Humaira Ehsan, Farrukh Aslam Khan [11] investigate in detail about some of the most severe attacks against Mobile ad hoc Network namely the black hole attack, sinkhole attack, selfish node behavior, RREQ flood, hello flood, and selective forwarding attack. It was observed through simulations that if the attacker node is in the path between the source to destination then selective forwarding and selfish node attacks can be very effective and it can cause a decline in the network performance. The only affect from attacker is measure here not work on any security scheme.

4 Proposed Scheme Against Wormhole Attack

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.

Wormhole Node spread route misbehaver module ;

```
Set misbehaver node = W1, W2; //W1 next to sender and W2 neighbour 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} ;
}
```

The proposed Intrusion Detection and Prevention system is identified the attacker and block their malicious activity through aware about the nodes about their particular information by that no will be receive the reply of attacker. The proposed scheme is identified the next hop information of every neighbored and confirm the data delivery from every hop in network.

The *true* and *true* values on any path show the reliable data delivery. The *true* and *false* and *false* and *true* is confirmed after the routing entry to next hop through SS. The *false* and *false* confirm no data delivery confirm by proposed SS. If the data delivery information through any node is *false* then in that case no data is delivering through that node on that hop. The number of routing packets delivery is confirmed by attacker then no need to find out. If the attacker replies the wrong information about data delivery then again confirm the information through nearest neighbor and in worm hole the nearest neighbor is also wormhole node and this node is not deliver the any data in network and SS again finding the *false* value against attacker. If the first wormhole node replies *True* then the nest hop is replies *false* the attacker is confirm. After confirmation of attacker the SS block the activity of attacker and also aware the network about that wormhole attacker nodes. The whole procedure of wormhole attack detection and prevention scheme is mentioned in proposed algorithm.

Proposed IDS Algorithm

```
Create mobile Node = M;              //Mobile Nodes
Sender Nodes = S;                                  // S € N ;
Destination Nodes = D;              // D € N;
Routing Protocol = AODV;
Set Simulation Time = T
While (S send RREQ_B)
 {       rtable -> insert(rtable->rt_nexthop);
        Add extra filed to rtable (next_hop , Through) //both value 1 , 0 formate
        If ((next_hop = true)&&(through == true) && (send_D_pkt==true))
   {
        True route ;
   }
        else if  (next_hop = false)&&(through == false)
    {
        In previous No data and route through that hop;
        Insert into ->rtable;        // for route to destination if shortest path
    }
        else if ((next_hop = true) && (through == false) && (send_D_pkt==true))
 {
  In previous data through that hop in wormhole nodes;
  But not exist in other nodes rtable entry; //Check reliability
```

```
If next hop(next_hop is unrelaible);
   {
    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 simulation is done by NS-2 (Network Simulator-2) Version 2.31[12] 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). The NS-2 is the opens source code that easily available. NS2 interprets the simulation scripts written in OTcl. The user writes his simulation as an OTcl script. Some parts of NS2 are written in C++ for efficiency reasons. The wormhole module and the security module is not be the part of simulator setup but it will be built-up after installation.

5.1 Simulation Parameters

The simulation of normal AODV, Wormhole attack and proposed Security Scheme (SS) are done the basis of following simulation parameters that has shown in table1.

These simulation parameters are decided on the basis of dynamic topology. In case of normal routing all the consider all 20 nodes but in case of wormhole attack consider 2 nodes as a attacker and remaining 18 are normal nodes and in case of proposed SS two nodes are Prevent the network and 2 nodes are attacker and rest of them are normal

TABLE 1
SIMULATION PARAMETERS USED

Simulator Used	NS-2.31
Number of nodes	20
Preventer nodes	2
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

TCP stands for Transmission Control Protocol, UDP stands for User Datagram Protocol, AODV stansd for Adhoc Ondemand Distance Vector routing protocol, m=meters, m/s=meters per second

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 Security scheme (SS).

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

This graph represents the Packet Delivery Ratio (PDR) analysis in case of normal AODV routing, in case of wormhole attack and in case of proposed Security 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. SS, the performance of network almost equal to normal means about 94% PDR are improves after applying security scheme against attack.

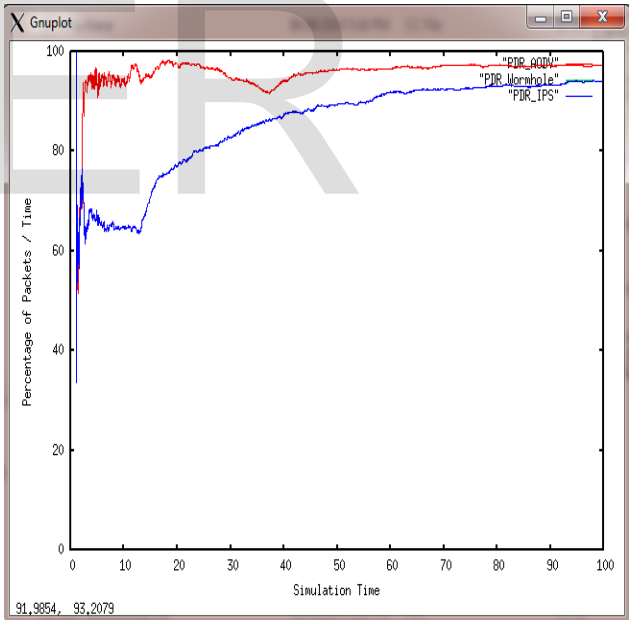

Fig. 1. PDR Analysis

6.2 Routing Load Analysis in case of Normal, Wormhole and SS.

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. The routing packets are important to know the information about the receiver. In this graph the routing load or number of routing packets in case of SS are very low about 600 routing packets are deliver in net-

ISSN 2229-5518

work then next in case of normal routing about 1200 routing packets are deliver in network but at last the routing load in case of wormhole attack are minimum about only 1200 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 proposed SS routing. In case proposed SS the routing packets are more deliver because of identifying the secure path for communication.

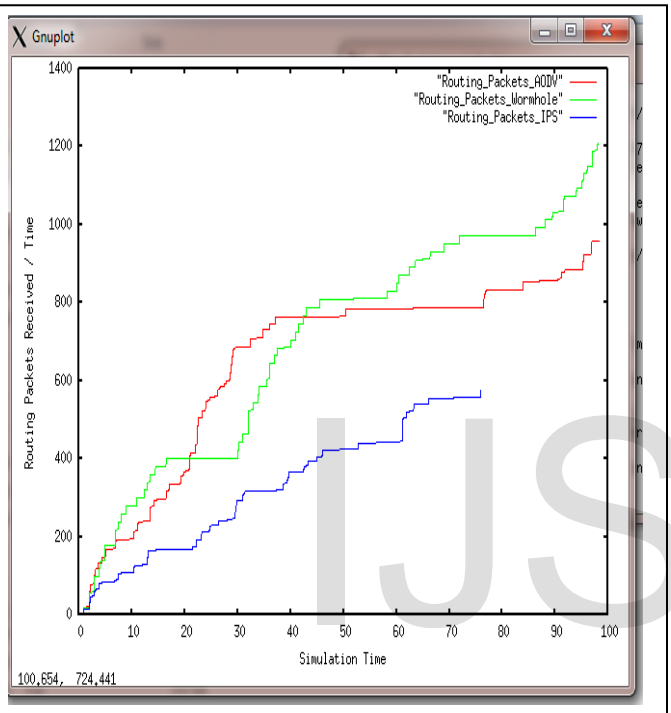

Fig. 2. Routing Load Analysis

6.3 UDP Packets Received Analysis in case of Normal, Wormhole and SS.

This graph represents the User datagram Protocol (UDP) Packet analysis in case of Normal, Wormhole attack and proposed Security 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, also provides high-quality performance. Here the UDP packets are almost equally received in case of attack and SS i.e. about 2200 and 2100 but in case of wormhole attack not a single packet is received, it means negligible packets are received at destination end in presence of attack.

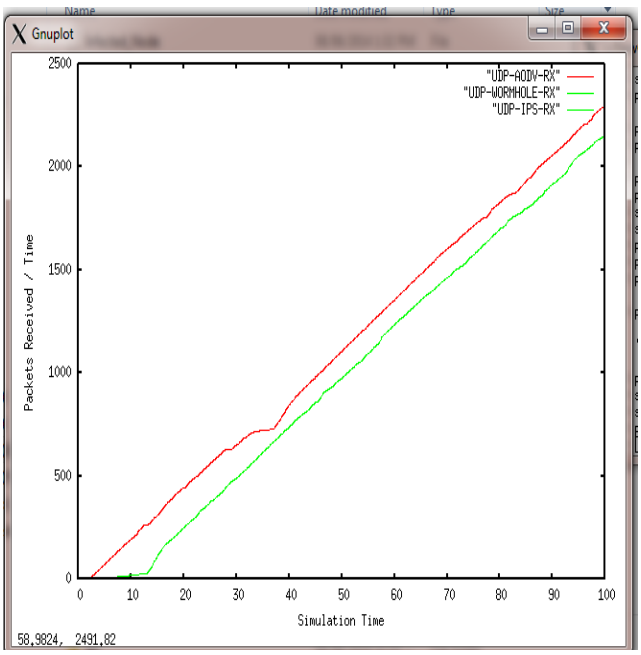

Fig. 3. UDP Packets Received Analysis

6.4 Infection from Wormhole Attack

Infection represents the number of packets are drop by attacker by that the receiver is not received the single packet in network w.r.t time. Infection in case of wormhole attack is continuously increases reach up to 5500 packets are lost. At time about after 4 sec. the packets dropping is minimized because the complete packets are drop by attacker. But in SS packet dropping is zero and not a single packet is affected by wormhole attack. SS will block the whole activity of wormhole attack and remove the infection from network.

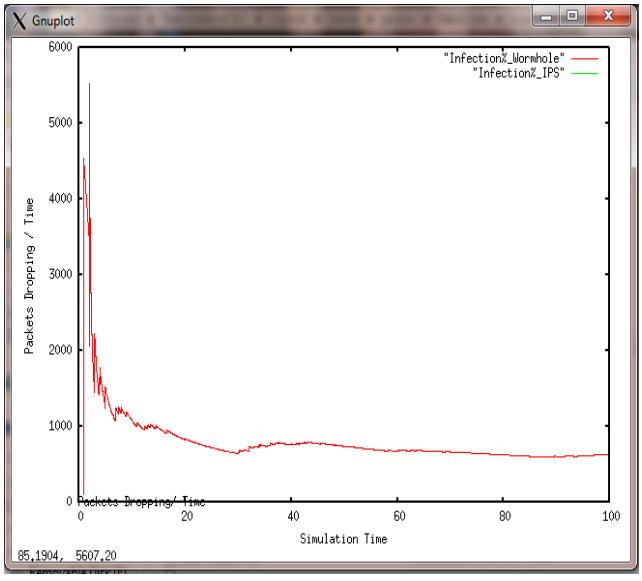

Fig. 4. Infection Analysis from Attack

6.5 Throughput Analysis in case of Normal, Wormhole and SS.

Throughput is depend on the total number of packets is send in network in per unit of time. In this graph the throughput analysis in case of normal AODV, wormhole and proposed Security Scheme are presents. Here we notice that the in case of normal routing the throughput is about maximum 1200 packets per second in network. But in case of wormhole the throughput is zero in network, means up to end of simulation not a single packet is received at destination but after applying SS the throughput value is increases up to 1100 packets/ sec. It means the proposed SS is definitely improves the network performance and proving the secure environment for communication.

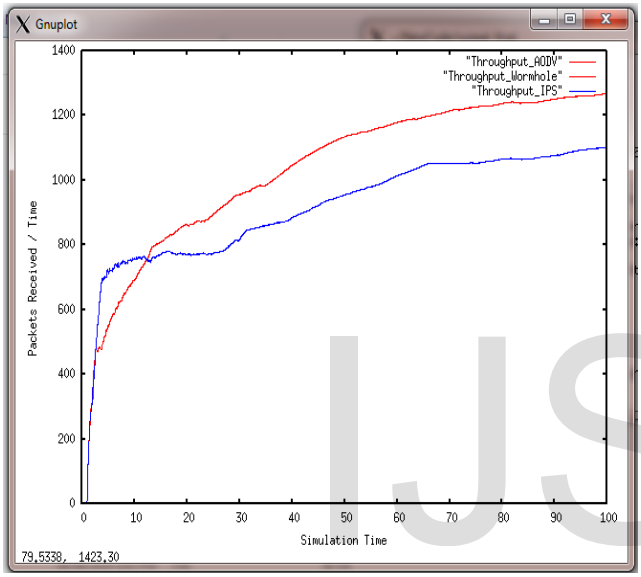

Fig. 5. Infection Analysis from Attack

6.6 Summery in case of Normal, Wormhole and SS.

TABLE 2
OVERALL SUMMERIZED ANALYSIS

Performance Parameters	Normal AODV Routing	Wormhole Attack	Proposed Security Scheme
Packets Send	7289	2480	6194
Packets Receive	7086	0	5821
Routing Packets	960	1209	575
PDF	97.21	00	93.98
NRL	0.14	00	0.1
Average e-e delay(ms)	262.55	00	324.62
Number of Data Drop	203	2480	373

PDF stands for Packet Delivery Ratio, NRL stands for Normal Routing Load

.

The table 2 presents the summery of or actually represents the performance of normal routing, wormhole attack and Security scheme. This summarized performance provides clear and exact performance of attacker and SS. The SS definitely improves the network performance i.e. degrades by wormhole attacker.

7 CONCLUSION AND FUTURE WORK

Security is an important feature for deployment of MANET. Security is such an important feature that it may well determine the success and extensive deployment of MANET. A variety of attacks have been identified. 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. The infection in case of security scheme is completely removes in network. The network performance is completely down by wormhole attacker and not a single packet is received in network but proposed Security Scheme improves performance nearly equal to normal routing. The proposed scheme is improves the performance of network and provides the attacker free environment from attack.

In future we also examine the behavior of other attacks like Sybil attack and Vampire 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.

REFERENCES

[1] Ravinder Ahuja , Alisha Banga Ahuja and Pawan Ahuja, "Performance Evaluation and Comparison of AODV and DSR Routing Protocols in MANETs Under Wormhole Attack", Proceedings of the 2013 IEEE Second International Conference on Image Information Processing (ICIIP), pp. 699-702, 2013.

[2] Mehran Abolhasan , Tadeusz Wysocki , Eryk Dutkiewicz "A review of routing protocols for mobile ad hoc networks" Elsevier, Ad Hoc Networks 2, pp. 1–22, 2004.

[3] Haas, Zygmunt J., Pearlman, Marc R.: The Performance of Query Control Schemes for the Zone Routing Protocol, IEEE/ACM Transactions on Networking, Vol. 9, No. 4, August 2001,

[4] Umesh kumar chaurasia and Varsha singh, "MAODV: Modified Wormhole Detection AODV Protocol", IEEE Sixth International Conference on Contemporary Computing (IC3), pp. 239 - 243, 8-10 August 2013.

[5] 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.

[6] [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.

[7] 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.

[8] 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.

[9] N. Gandhewar, R. Patel, "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.

[10] S. Gupta, S. Kar and S. Dharmaraja, "WHOP: wormhole Attack Detection protocol using hound packet". In the international conference on innovations Technology, IEEE 2011.

[11] Humaira Ehsan, Farrukh Aslam Khan "Malicious AODV: Implementation and Analysis of Routing Attacks in MANETs" IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, pp.1181-1187, 2012.

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