Profile Based Approach to Secure MANET from Wormhole Attack

Shashi Ranjan Kumar, Dr. Narendra Sharma, Mr. Ankit Navgeet Joshi

Department of CSE , SSSUTMS, Sehore, Madhya Pradesh, India,

ABSTRACT

Mobile ad hoc network (MANET) is an ad hoc network in which mobile nodes are connected via wireless links. Since there is no central controller, it is difficult to ensure reliable and secure communication in mobile ad hoc networks. Wormhole attack works by creating a path between the sender and the receiver, but if the sender has already started transferring data, the wormhole attacker creates a direct connection with them, this is called wormhole Tunnel, which means transfer of more data. Trusted nodes mean that a higher rate of effective communication can be expected. In this article, we introduce detection and protection technology for wormhole attacks. According to the detections, it uses data set detection technology and calculates the number of attack packages, execution time, etc. We receive attacker node information such as: We then protect against wormhole attacks using our community's reliable and secure mobile private network communications. We provide secure and reliable communications in line with our recommendations and simulate them with Network Simulator 2 (NS-2).

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

1. INTRODUCTION

Mobile ad-hoc networks (MANETs) are infrastructure-free collections of mobile nodes that can change their addresses randomly as the network follows a dynamic topology and service constraints. If two nodes are too far apart to communicate directly, the intermediate node must establish a connection. Multi-hop routing and open workstations make MANETs vulnerable to attacks from selfish or malicious actors. An important area of research in mobile ad-hoc networks is providing reliable and secure communications.

Some shared networks require secure communications. Common uses for MANETs include: military or law enforcement networks, industries such as oil rigs and mining, and emergency response

One exit In the case of a wormhole, the attacker collects information from one place and sends it to another. place it in the same place. network or any other network. 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 décor in such manners: Section 2 describe routing protocols analysis. Section 3 shows literature review. Section 4 describe proposed profile based approach of our work and Section 5 describes the simulation environment. Section 6 declare the details of simulation results and finally Conclusion and future work is given in Section 7.

2. ANALYSIS OF ROUTING PROTOCOLS

Here are basically three types of routing protocols: reactive routing protocols, proactive routing protocols, and hybrid routing protocols. A proactive or table-driven routing protocol allows each node to continuously maintain up-to-date routes to all other nodes in the network. Routing information is periodically sent across the network to keep routing tables consistent. So if the route already exists before the traffic arrives, the transmission happens without delay. Proactive protocols have the disadvantage of requiring additional control traffic to continuously update stale route entries. Network topologies are dynamic, so when a link fails, all paths using that link are broken and must be repaired. If there are no applications using these paths, repair efforts can be considered futile.

In contrast to the proactive approach, in reactive or on-demand protocols, a node initiates route discovery across the network only when it wants to send a packet to its destination. To do this, the node initiates a route discovery process through the network. The process is complete when the root is determined or all possible permutations have been explored. Once a route is established, it is maintained by a route maintenance process until the destination along each path from the source becomes inaccessible or the route is no longer needed. In a reactive scheme, nodes maintain routes to active destinations. A route search is required for each unknown destination.

Finally, in the hybrid protocol, each node maintains both topology information within a zone and information related to neighboring zones. This means active behavior within zones and reactive behavior between zones.

3. LITERATURE REVIEW

Pallavi Sharma et al. [2] describes a method that uses digital signatures to prevent wormhole attacks in ad-hoc networks. A wormhole attack on a private network occurs when the receiving node destroys the sender's digital signature because every legitimate node in the network has the digital names of every other legitimate node in the same network. It represents an idea that will facilitate analysis. Wormholes are one of the most important attacks and consist of both worms and holes. To defend against wormhole attacks, we used a scheme called Multi-Hop Counting Analysis (MHA) to verify legitimate nodes in the network through digital signatures.

Hussain et al. [5] suggested DoS Attacks in AODV & Friend Features Feature Extraction for Designing Detection Engines of Intrusion Detection Systems in Mobile Ad Hoc Networks. In this work, denial-of-service attacks are applied to networks, evidence is collected, and an intrusion detection engine is developed for the MANET Intrusion Detection System (IDS). The true positives produced by the detection engine are very high and the false positives are suppressed very little. True positives are reported very quickly in Lids, and the friends list generated by Lids is sent to the Gid engine for further investigation. The global search engine creates a list of friends based on trust level. For scalable ad hoc networks, one of the more reliable methods can be used for many processes such as teaching and decision making. The constraints and features extracted for MANET traffic generation can be used in many ways.

Huang Jingwei et al. [6] proposed multipath trust-based AOMDV security routing in ad-hoc networks. In this study, a concept called T-AOMDV has emerged by using trust-based multipath AOMDV routing together with software encryption.

(1) In message encryption, the message is basically divided into three parts and these parts are encrypted together using some kind of XOR operation.

(2) When sending the message, the messages sent from the message are separated into different trusts using the new AOMDV protocol extraction system.

(3) The goal in language decryption is to restore the original language by decrypting part of the language.

Shreenath et al. [7] describes a multi-attack attack on the development of a desirable multicast routing protocol for MANETs. This project focuses on the robustness of Security Enhanced Optional Multicast Routing Protocol (EODMRP) to prevent floods and black holes. Although the identity of the malicious actor is unknown, the flood attack mechanism works and does not consume additional network bandwidth. Despite solutions, the performance of small multicast groups drops significantly in such attacks.

Sujtha et al. [8] proposed a MANET IDS design based on genetic algorithm. In this paper, we analyze AODV's vulnerability to attacks, especially the black hole attack, which is the most common threat to network infrastructure, and build a custom-based intrusion detection system (IDS) using genetic algorithm. Create an improvement plan. . The planning process is based on a genetic process that defines the behavior of each cell and provides detailed information about the attack. Genetic Algorithm Control (GAC) allows AODV to send value request, response confirmation, etc. It is a different process based on physical properties such as.

Konate et al. [9] describes the model and simulation of intrusion detection in mobile ad-hoc networks. This name describes the effort to detect and attack MANET attacks. They suggested various methods for DOS attacks encountered in MANETs, their working methods, techniques used to combat these attacks and procedures to be followed.

Gandhewar et al. [10] describes Sinkhole attack detection and prevention of AODV protocol for mobile ad-hoc networks. This article focuses on the pooling problem and its consequences and describes methods for detecting and preventing this problem in the context of the AODV protocol. Sinkholes are one of the most aggressive types of attacks that attract large numbers of people to network connections and attempt to degrade network performance. Also PDR, end-to-end delay and packet loss

Sharma et al. [11] describes the effective protection of the black problem in the AODV routing protocol for MANETs. This paper presents a solution to black hole attack in Ad Hoc On-Demand Distance Vector (AODV) routing in MANETs, one of the most popular routing algorithms. Ground attack is one of these security risks. In this attack, the malicious node disrupts communication by imitating the shortest path to the target node. The proposed method uses a mixed model to detect malicious nodes (black holes).

Jian-Ming Chang et al. [12]. They proposed a mechanism called the Cooperative Second Tetch (CBDDS) to suppress the blast furnace/gordative ground attack. Combine active and unprotected architectures and work with neighbors randomly. By using the neighbor's address as the target's address, the malicious party is made to send back the RREP, and the malicious party is detected by the return request block attack.

4. PROPOSED APPROACH

In this section, we explain an algorithm which prevent the overall network from wormhole attack. Firstly we set normal ad-hoc network parameter and then set criteria of wormhole attack scheme and spread attack onto the network.

```
Set mobile Node = N; //Mobile Nodes
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 Oriented Prevention from 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

All simulations were performed using the network simulator ns 2.31[10]. This is a separate event-driven simulator. The purpose of NS-2 is to support networking research and education. NS-2 was built using the object-oriented language C++ and OTcl (the object-oriented variant of the Tool Command Language). NS-2 interprets simulation scripts written in OTcl. The user writes the simulation as his OTcl script.

5.1 Simulation Parameters

Table 1 shows the parameter that has been set during simulation. In case of normal routing, 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.

Table 1: 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 figure represents the packet delivery rate (PDR) analysis for normal AODV routing, for wormhole attacks, and for IPS (intrusion prevention system) schemes. Only considered if performance is deemed consistent. Application of protection schemes. Here we have clearly visualized the impact of a wormhole attack in our network. In the early stages of the simulation, only about 30% packet delivery is possible in the network, after which the network performance is almost zero, and then about 50%. Seconds The PDF value is not measured on the network. However, in the case of application of the protection scheme i.e. IPS, network performance is about the same as normal. This means that the PDR improved by about 94% after applying the security scheme against attacks.

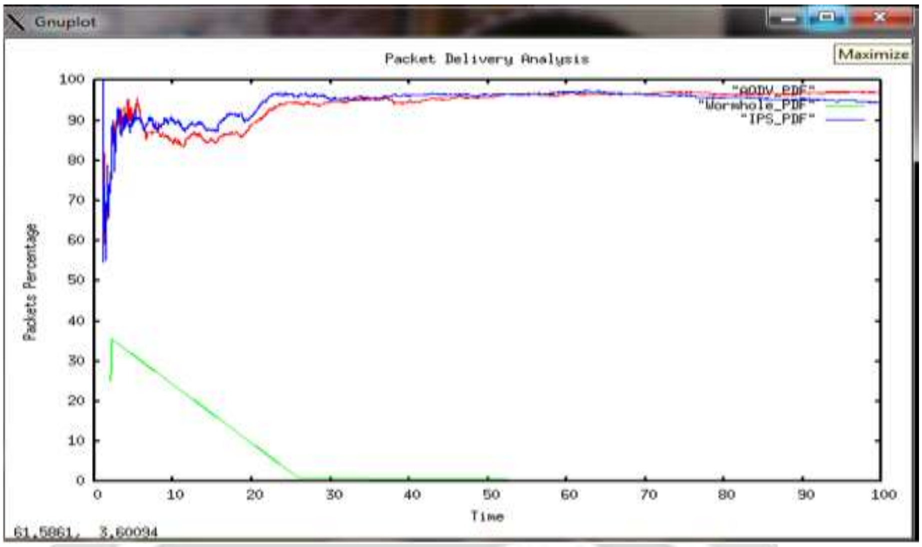

Fig. 1 PDR Analysis

6.2 Routing 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.

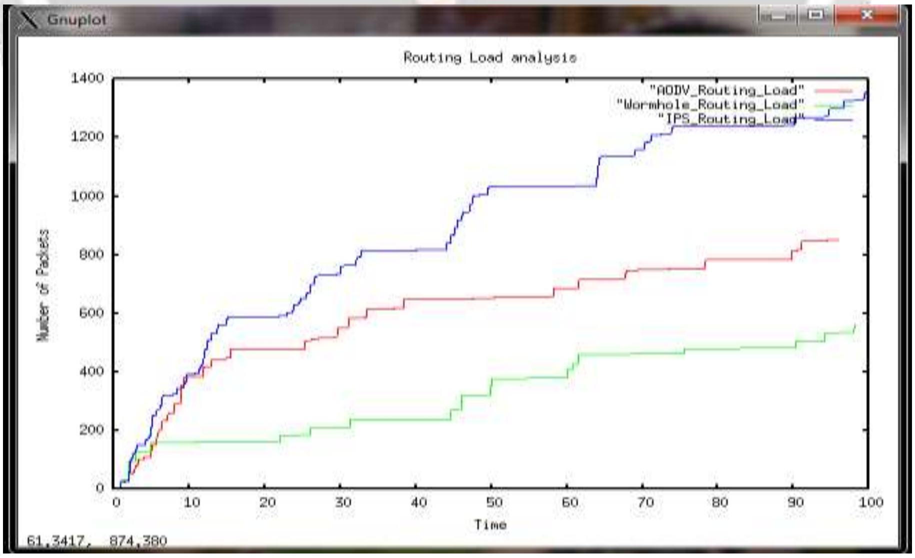

Fig. 2 Routing overhead Analysis

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.

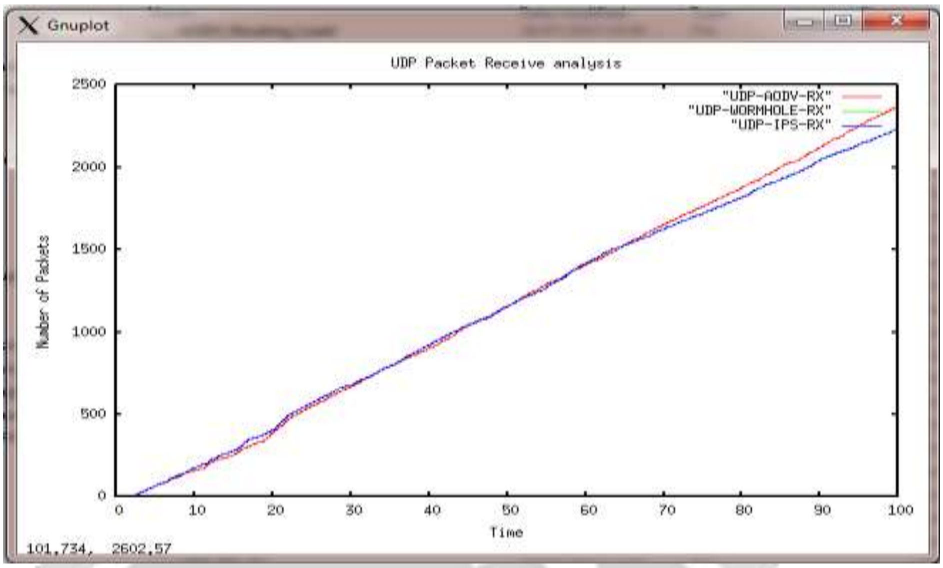

Fig. 3 UDP packet receive analysis

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.

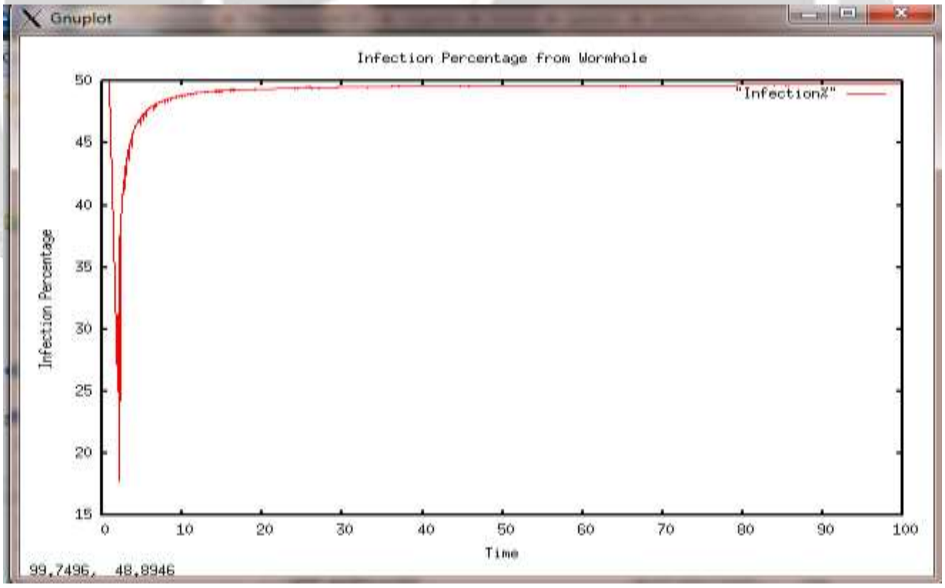

Fig. 4 Infection Percentage

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.

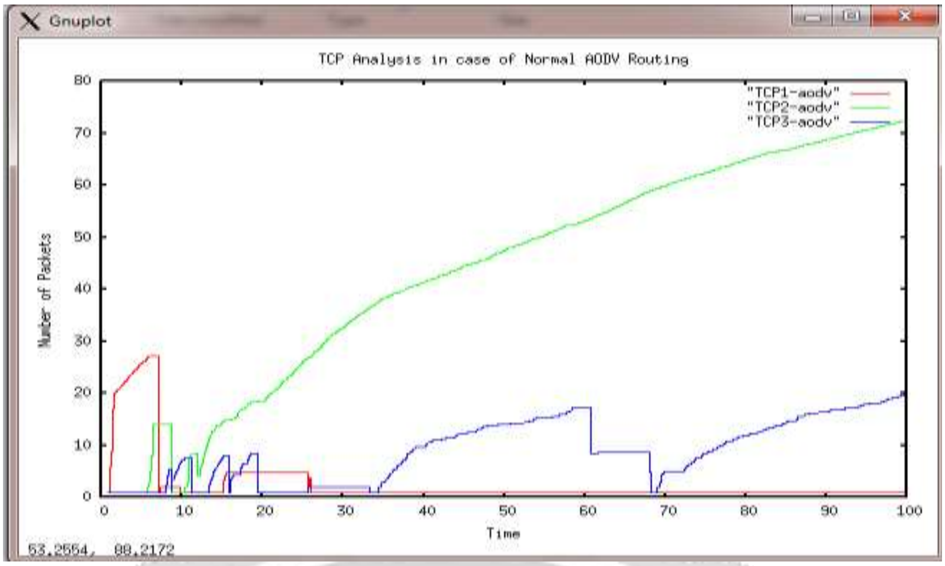

Fig.5. TCP packet performance of AODV Routing Protocol

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.

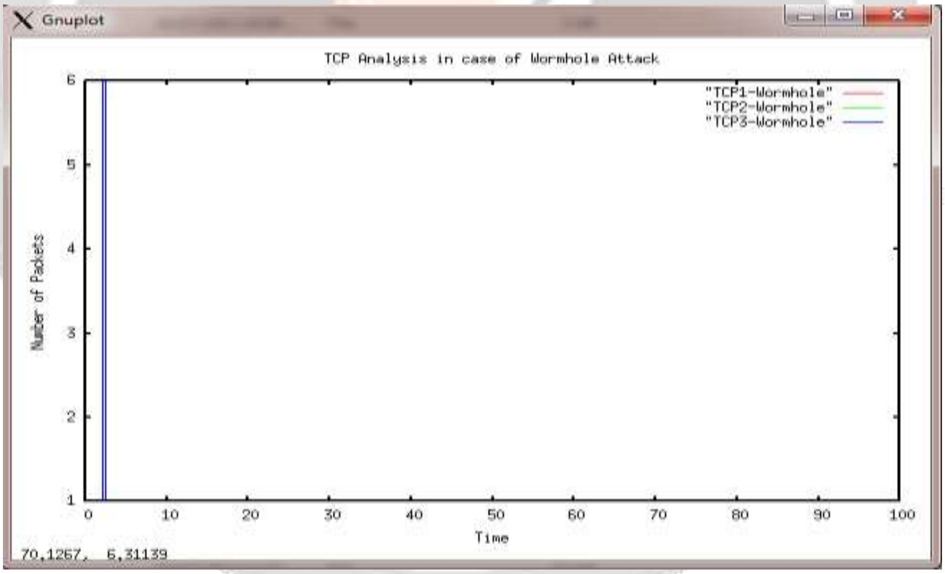

Fig.6. TCP Packet Analysis in case of Wormhole Attack

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 misbehaviour activity of wormhole attacker.

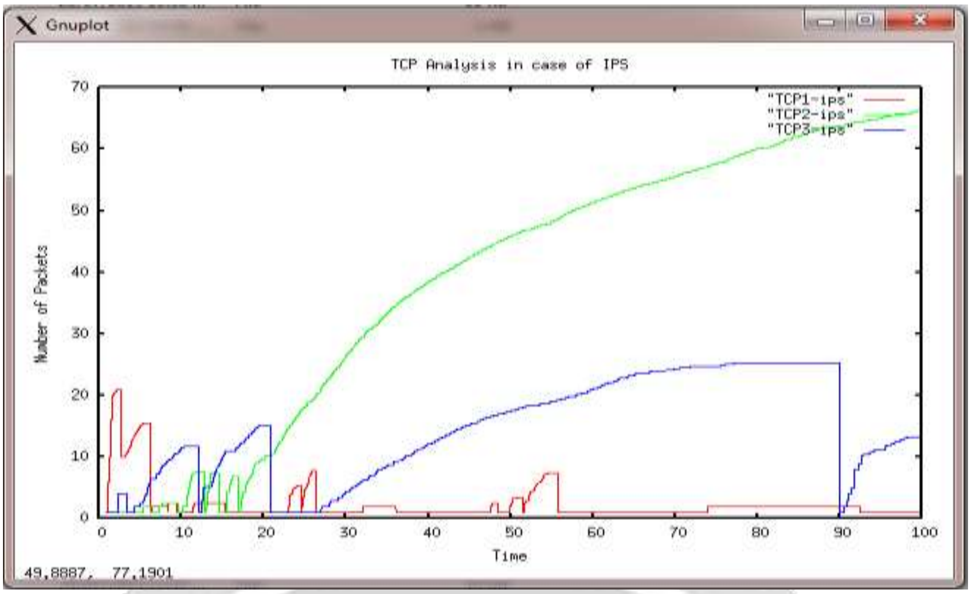

Fig.7. TCP packets delivery of IPS Scheme

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.

Table 2

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. CONCLUSION AND FUTURE WORK

Mobile ad-hoc networks have the ability to set up networks in harsh environments where traditional network infrastructure cannot be deployed. Regardless of the great potential of ad-hoc networks, there are still many challenges to overcome. Security is a very important feature and can determine the success and adoption of MANET. A wormhole attack is a type of attack that performs malicious activity by creating its own links and breaking the actual links. i.e. the actual path of data transmission. The basic idea of this algorithm is that malicious nodes launch attacks, detect link malfunctions, and disconnect them from the communication network. This protection scheme provides protection against wormhole attacks and blocks attacker node activity. In the event of an attack, the network performance would be almost completely lost, but the proposed IPS scheme would improve performance almost as much as regular routing. This work explores a vigorous and very simple idea that can be implemented and tested against more attacks in the future by increasing the number of nodes in the network.

In the future, we will also study the behavior of other attacks such as gray hole and black hole attacks, try to build protection schemes against them, and improve the performance of the routing protocols considered in this paper, trying to improve routing ability.

8. REFERENCES

[1] P Kaliyar, WB Jaballah, M Conti, C Lal – "LiDL: localization with early detection of sybil and wormhole attacks in IoT networks", Computers & Security, 2020 – Elsevier.

[2] 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.

[3] M Tahboush, M Agoyi, "A hybrid wormhole attack detection in mobile ad-hoc network (MANET)", IEEE Access, 2021

[4] M Shukla, BK Joshi, U Singh Mitigate Wormhole Attack and Blackhole Attack Using Elliptic Curve Cryptography in MANET Wireless Personal Communications, 2021 – Springer.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

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

[14] ZA Zardari, KA Memon, RA Shah, “A lightweight technique for detection and prevention of wormhole attack in MANET”, EAI Endorsed, 2021

[15] S Deshmukh Bhosale, S S Sonavane, “A real-time intrusion detection system for wormhole attack in the RPL based Internet of Things”, Procedia Manufacturing, 2019 - Elsevier