WIDPS: Wormhole Attack Intrusion Detection and Prevention Security Scheme in MANET

Priyanka Verma
Computer science and Engineering
SIRT- Excellence
Bhopal,India

Sumit Dhariwal
Computer science and Engineering
SIRT-Excellence
Bhopal,India

Harshvardhan Tiwari
Computer science and Engineering
SIRT-Excellence
Bhopal,India

ABSTRACT
Mobile Ad hoc network (MANET) is a collection of mobile nodes that form a temporary dynamic network without any fixed infrastructure and centralized administration. In this type of network it is difficult to have the reliable & secure communication in MANET. In this paper we proposed a scheme against wormhole attack in MANET. In this research we proposed Wormhole attack Intrusion Detection as well as prevention Security Scheme (WIDPS) against wormhole attack using the IDP nodes. Using the proposed algorithm for detecting the wormhole node, IDP node will analyze the behavior each nodes based on packets send by the nodes, will detect the node with abnormal behavior. After that we prevent wormhole attack using broadcasting the particular identification (ID) of attacker so that no node in network replies to that request and secure the mobile ad-hoc network communication. Through our proposed work we provide reliable as well as secure communication in network from wormhole attack and measure the network performance on the basis of network parameter like routing load, throughput and packet delivery ratio.

Keywords
MANET, WIDPS, routing, security, performance metrics, wormhole attack

1. INTRODUCTION
Mobile Ad-Hoc Network (MANET) is a network of mobile nodes having no infrastructure. In this type of network nodes change their location randomly and have dynamic topologies. A mobile ad hoc network (MANET) is a self organizing structure of mobile nodes .MANET uses intermediate nodes when two nodes are not directly connected and want to communicate, intermediate nodes in between those two nodes forwards their messages. In MANET routing is difficult because of mobile nodes, lack of predefined infrastructure, and limited transmission range. Due to open working environment and multi-hop routing, MANETs are vulnerable to attacks by 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. It is very difficult to find out the location of wormhole attack without having packet relay information or without known infrastructure of routing protocols.

The proposed WIDPS scheme is identified the misbehavior of wormhole attacker nodes. The attacker aim is to dump the whole performance of network through drop all the packets. But their identification through the WIDPS is block their misbehavior and their ID is also broadcast in network by that no sender and intermediate node will forward the packets to attacker and also ignores the route on that the attacker is present.

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 and simulation results. Section 6 is Conclusion and future.

2. OVERVIEW OF ROUTING PROTOCOL
The routing protocols [2] are required to established connection and data delivery in network. There are basically three types of routing protocols: reactive routing protocol, proactive routing protocol and hybrid routing protocol.

In proactive routing protocol, every node maintains one or more tables representing the entire topology of the network. These tables are updated regularly in order to maintain a up-to-date routing information from each node to every other node.

To maintain the up-to-date routing information, topology information needs to be exchanged between the nodes on a regular basis, leading to relatively high overhead on the network. One the other hand, routes will always be available on request.

The reactive or on demand protocols, a node initiates a route discovery throughout the network, only when it wants to send packets to its destination. 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 as well as reactive behavior among zones. Zonal Routing Protocol (ZRP) [3] is the example of that kind of routing protocol.

3. RELATED WORK

In the section of related work we mentioned the work that has been done in the field of wormhole attack prevention and detection and also the effect 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.

Short comings 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 that is totally need less.

Umesh kumar chaurasia and Varsha singh [4] proposed a 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.

Short comings 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 a work against Wormhole Attack in Ad Hoc Network using Digital Signature [5]. They presents a mechanism in which by verification of digital signatures by receiver can prevent wormhole attack in ad hoc network. A wormhole attack is a attack in which two malicious nodes creates a tunnel and take whole data from that tunnel. So to protect from wormhole attack they used a scheme called multi hop count analysis (MHA) along with verification of authorized nodes in network through its digital signature. Destination node selects the best path after analyzing the number of hop count. 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 Counter measures 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 performance of a small multicast group will mortify gravely under these types of attacks even the solution is available. The proposed algorithm provides protection against black hole attack in MANET.

K. S. Sujatha, VydekiDharmar, 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. This research work is staunch to study attacks and countermeasures in MANET. After introducing MANETs and network security they present a survey of various attacks in MANET concern to fail routing protocols in network. They also present 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. 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.

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 Sink hole attack, Selfish node behavior, black hole attack, hello flood, RREQ 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 WIDPS SCHEME

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. In our proposed wormhole attack detection and prevention divided into two modules

(1) Detection module
(2) Prevention module

(1) Detection Module:

In this module we create data set of normal communication data profile and pass the generate output to detection module, if data match that means no deviation of data else data are modified or corrupted, after the identification of mismatch data we find out the reason of data dropping or modification, if we get data incoming in w1 node and forward to w2 node and drop the data into w2 node that link is a suspicious link and set as wormhole link in between w1 to w2 and also both node as a wormhole attacker node.

Wormhole Attack Detection and Prevention Algorithm

Variable Initialization

M: Set of mobile node

S: Set of senders // M ⊑ S

R: Set of receivers // M ⊑ S

W1 and W2 : Wormhole node

Radio Range: 550 Meters

Antenna: Omani directional

Routing Protocol: AODV

IPS: Preventer Node

S broadcast search packet

If (Next Node in range && Node! =Receiver)

{

Receive Routing Packets

Forward Routing Packets to set R

}

Else

{Establish route and forward data to R}

Simulated generated data is stored in file.

Analyze behavior of each data

If (Sender ==W1 && next hop ==W2)

{Check W2 forward data or not

If (W2 not forward any data)

{W1 and W2 both is suspicious node}

While (W1 and W2 continuous data capture and not forwarded)

{Both as Attacker}

(2) Prevention Module :

Preventer node watch the all neighbour node and if they found node receives the data but not forward to particular receiver of next hop than that preventer node indentified their address and previous node whose send data to attacker node address so both node treat as a attacker node because w1 and w2 node work in collaborative manner (w1 data receives and w2 drop), than P-preventer block the both w1 and w2 node and inform all the sender to re-initiation of route discovery process whose new fresh route not contain and wormhole node and protect the data from attacker.

In built WIDPS module in ns-2

Create IPS simulator Setup

If (W1 and W2 both are in IPS node range)

{Detected as wormhole link

IPS node broadcast blocking message of W1 & W2 node

Sender receive message from IPS

}

If (W1 && W2 link in between S to R Link)

{

S change new link eliminate W1, W2 and new path established.

Send data to R node by new path

}

End if

Stop

The effect of proposed security scheme is visualized in results. The results are shows that the routing performance is almost equal as compare to normal AODV routing performance. The proposed scheme is identified the information of every neighbored and confirm the data delivery from every hop in network.

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.

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. These simulation parameters are decided on the basis of dynamic topology. In case of normal routing all the consider all 50 nodes but in case of wormhole

attack consider 2 nodes as a attacker and remaining 48 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 for simulation

Simulator Used	NS-2.31
Number of nodes	50
Preventer nodes	2
Wormhole Attacker	1
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	TCP, UDP
Node movement	random
Maximum Speed	20 m/s
Transmission range	550m

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 WIDPS.

5.1 Packet Delivery Ratio Analysis in Case of Normal, Wormhole and IPS

The PDF performance is evaluated the percentage of data per unit of time received at destination. The PDF performance in case of normal AODV routing, wormhole attacker and routing in presence of wormhole attacker and WIDPS is mentioned in this figure. Here the network performance in presence of wormhole attacker is negligible, that shows the zero packets receiving at destination but in presence of WIDPS the attacker activity is completely blocked through broadcasting the attacker identification (ADI). The proposed security scheme is provides the normal performance as nearly equal to normal AODV and improves the network performance in presence of wormhole attacker.

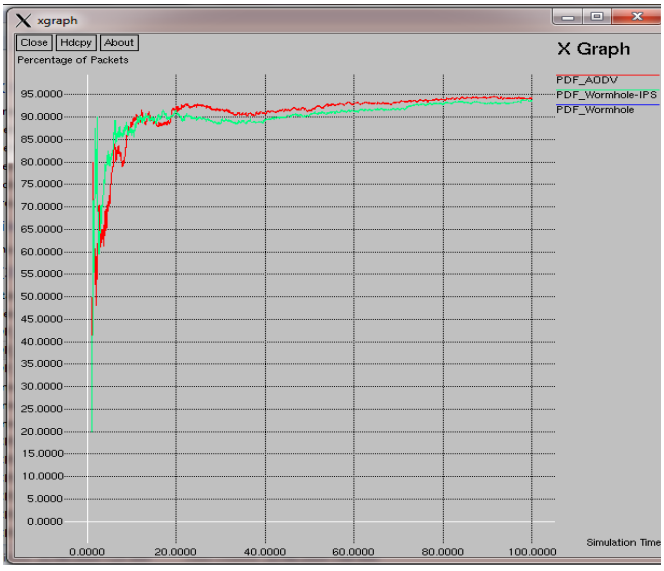

Fig 1: PDR Analysis

5.2 UDP Packet Receive Analysis in Case of Normal, Wormhole and IPS

The User Datagram Protocol (UDP) protocol is the connectionless end to end delivery transport layer protocol. This graph represents the UDP packets receiving analysis in presence wormhole attacker and proposed WIDPS scheme. The proposed scheme improves packets receiving and provides the better performance in presence of attacker. The packets receiving in case of wormhole attack is almost negligible. The packets receiving in case of WIDPS is about 620 packets at the end of simulation n that is about 620 times more in case of wormhole attacker.

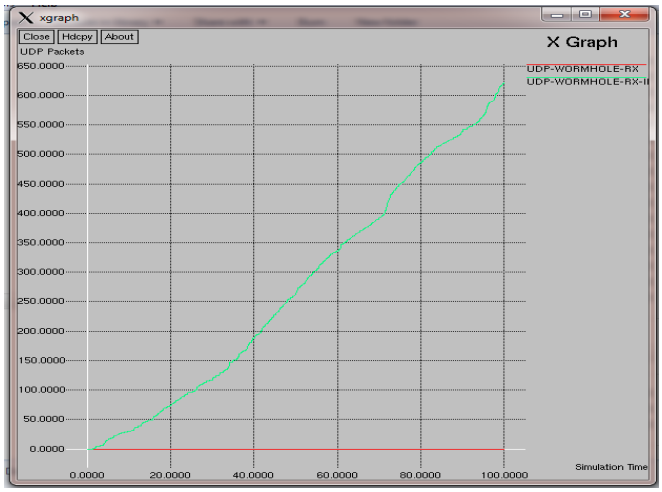

Fig 2: UDP packet received analysis

5.3 Infection from Wormhole

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 about 3050 packets are lost. At time about after 4 sec. the packets dropping is minimized because the complete packets are drop by attacker. But in WIDPS packet dropping is zero and not a single packet is affected by wormhole attack. WIDPS will block the whole activity of wormhole attack and remove the infection from network.

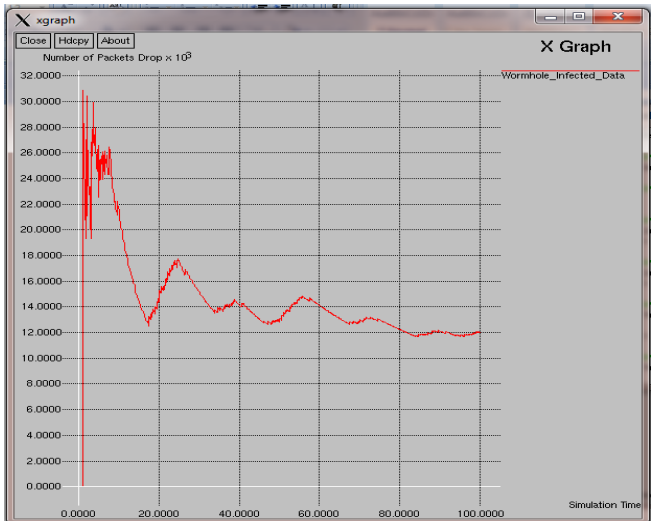

Fig 3: Infection Percentage

5.4 Throughput Analysis in of AODV, Wormhole and IPS

Throughput in measured to evaluated the packets receiving in per unit of time in network. This graph is illustrated the performance of normal AODV routing, wormhole and WIDPS routing. The throughput in presence of wormhole attack is negligible from start to end of simulation. The performance of WIDPS is about 850 packets / sec at the end of simulation and it is also higher about 1000 packets / seconds at time in between 17 seconds to 22 seconds. The proposed security scheme is provides the better performance in presence of attacker and completely block the misbehavior activity of wormhole attacker.

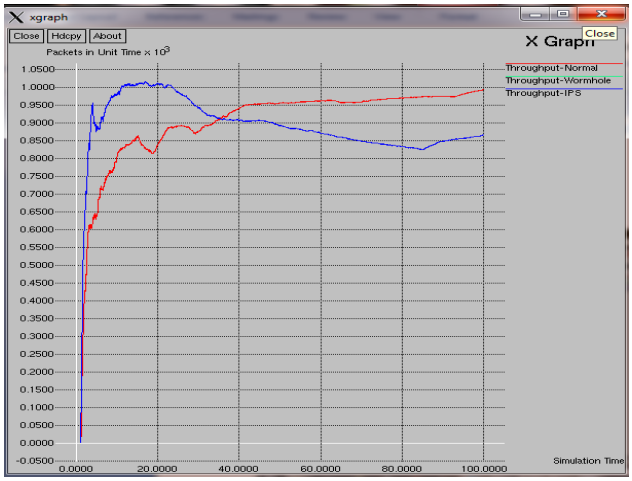

Fig 4: Throughput Analysis

5.5 Summary in Case of Normal Routing, Wormhole Attack and WIDPS Scheme

The Overall Performance of AODV routing protocol, wormhole attack and WIDPS are mentioned in Table 2. The normal AODV routing protocol is provides the performance in absence of attacker and rest of two performances are in presence of wormhole attacker. The effect of attacker in presence of WIDPS is completely nil but without WIDPS the attacker is majorly infected the routing performance that degrades the network performance. The proposed scheme is provides secure routing in presence of attacker and improves network performance.

Table 2 .Overall Summarized Analysis

Performance Parameters	Normal AODV Routing	Wormhole Attack	Proposed Security Scheme
SEND	4566	809	4897
RECV	4302	0	4586
ROUTINGPKTS	3883	0	4325
PDF	94.22	0	93.65
NRL	0.9	0	0.94
No. of dropped data (packets)	259	809	308

6. CONCLUSION AND FUTURE WORK

Security is such an important characteristic that it may well determine the success and widespread deployment of MANET. A variety of attacks have been identified in MANET and one of them is wormhole attack. 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 proposed WIDPS algorithm is to detect malicious nodes launching attacks and to prevent them from network. This WIDPS protection scheme provides the protection against wormhole attack and blocks the activities of attacker node. The packet dropping by attacker is huge in network but in case of WIDPS 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 WIDPS 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 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.

7. 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] MehranAbolhasan , TadeuszWysocki , ErykDutkiewicz "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] Umeshkumarchaurasia and Varshasingh, "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, VydekiDharmar, 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 conferenceon innovations Technology, IEEE 2011.

[11] HumairaEhsan, FarrukhAslam 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/.