IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 13, Issue 3 (Jul. - Aug. 2013), PP 87-95
www.iosrjournals.org

Reactive Routing approach for preventing wormhole attack using hybridized WHOP

Miss Neha Jain[1], Associate Prof. Ashish Kr. Shrivastava[2]
[1](*M. Tech Scholar, Dept. of Computer Science Engineering, NIIST, Bhopal, India*)
[2](*Head PG Dept. of Computer Science Engineering, NIIST, Bhopal, India*)

Abstract : *Mobile Ad-hoc network is additionally a network that is self-organized and adaptive in nature. As a results of lack of centralized infrastructure several security problems are arises and malicious activity performed by offender. Here we've got an inclination to tend to denote specific attack referred to as wormhole attack , throughout that the degree offender with the help of malicious node to record packets at one location among the network and transmit to a distinct location by a secrete tunnel and retransmits them into the network. In previous research work have got process delay time is a lot of as compare to traditional process delay time because of some suspicious activity of wormhole attack. The aim of this research work is to reduce the process delay time, using the idea of hybridize WHOP protocol with time synchronization mechanism. The proposed approach provides efficient results to secure data packet transmission and reduce the process delay time while not use of any expensive hardware. We are going to work with DSR routing protocol that simulates the behavior of wormhole attack using network simulator NS-2.*

Keywords: *Ad Hoc Networks, DSR (Dynamic Source Routing), Malicious Node attacks, Wormhole attack, WHOP*

I. Introduction

A Mobile Ad-hoc Network (MANET) includes nodes that are organized and maintained in a distributed manner while not a fixed infrastructure. These nodes, like wireless phones, have a restricted transmission range. Hence, every node has the flexibility to communicate directly with another node and forward messages to neighbors till the messages reach the destination nodes i.e. the nodes act as both host and router at constant time, i.e., every node within the network may be independent. Since the transmission between two nodes should rely on relay nodes, several routing protocols [1, 2, 3, and 4] have been proposed for ad hoc networks. For basic infrastructure of MANET consider "Fig 1".

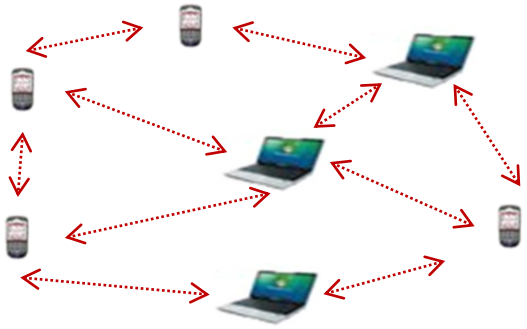


Figure1. Basic Infrastructure of MANET

In case of wormhole attack, attackers "tunnel" packets to a different area of the network bypassing traditional routes as shown in "Fig 2". The ensuing route through the wormhole could have a higher metric, i.e., a lower hop-count than traditional routes. With this leverage, attackers using wormholes will simply manipulate the routing priority in MANET to perform eavesdropping, packet modification or perform a DoS (Denial of Service) attack. The complete routing system in MANET will even be brought down using this attack. Its severity and influence has been analyzed [5].

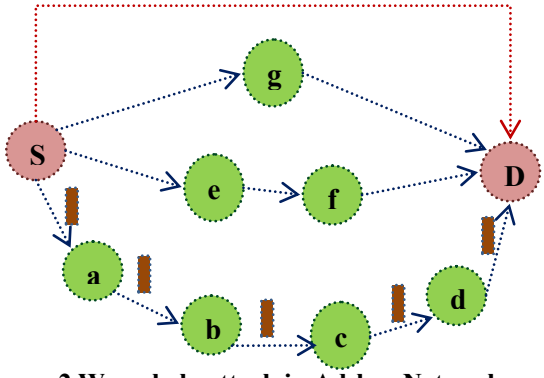


Figure 2.Wormhole attack in Ad-hoc Network

In wireless network many types of attacks are often initiated however most of them are relative simple to find because of their property of dramatically altering the network statistics however one completely different kind of attack we consider during this thesis. It's very important when considering security problems with network, is wormhole attack, that is tough to discover & will damage by leading important data to unauthorized nodes. Throughout the route discovery method, a wormhole will relay route request and response messages between distant nodes, making the appearance of shorter routes to destinations. Since the wormhole are often anyplace along a route, a source ought to discover its existence somewhere along the route when a node sets up the route (on-demand).

This paper is categorized as follows. Section 2 describes Problem Definition and section 3 presents related works concerning wormhole attacks. Section 4 presents proposed work. Section 5 provides evaluation of simulation results and analysis. At the end conclusion is provided in Section 6.

II. PROBLEM DEFINITION

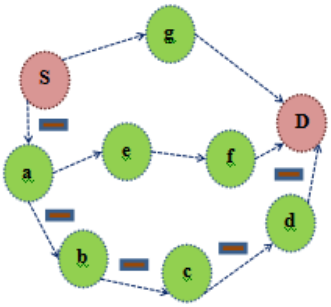


Figure 3a. Data transmission in Normal Network.

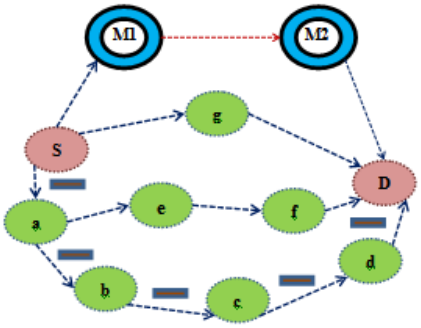
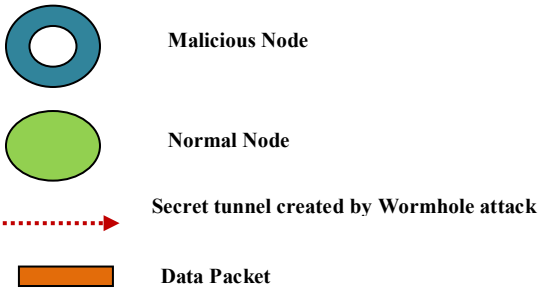


Figure 3b. Data transmission when Network under the effect of Wormhole attack



Ad-hoc or spontaneous wireless networks are vulnerable by a strong attack referred to as the wormhole attack. A Wormhole attack is often discovered with relative ease, however preventing one is tough. Establishes a wormhole or tunnel through that data will transfer quicker than it may on the first network.When setting up a wormhole, an attacker will disrupt routing to direct packets through the wormhole employing a technique referred to as selective forwarding. Within the wormhole attack, an attacker records packets (or bits) at one location within the network, tunnels them (possibly selectively) to different location, and retransmits them there into the network. The wormhole attack will form a serious threat in wireless networks, particularly against several ad hoc network routing protocols and location-based wireless security systems. To set up a wormhole

attack, an aggressor places two or a lot of transceivers at completely different locations on a wireless network as shown in "Fig. 3a" & "Fig. 3b".

We can easily see in fig 3a and 3b. When network is not affected by wormhole attack, the data packet would have followed the path S-a-b-c-d-D, while when network is affected by wormhole attack the data packet is transmitted by a secret tunnel(S-M1-M2-D), which is high speed link between two malicious nodes that perform malicious activity in the network.

III. RELATED WORK

A wide variety of wormhole attack mitigation techniques are proposed for specific types of networks: sensor networks, static networks, or networks wherever nodes use directional antennas. During this section, we have a tendency to describe and discuss such techniques, commenting on their usability and also the chance of their use normally ad-hoc network. Yih-Chun Hu propose a solution to wormhole attacks for ad-hoc networks within which they present a general mechanism, known as packet leashes, for detection and, so defensive against wormhole attacks, and additionally he gave the thought of a particular protocol, called TIK, that implements leashes and topology-based wormhole detection, and show that it's not possible for these approaches to detect some wormhole topologies. [6]

Saurabh Gupta [7] et al introduce new protocol WHOP network. Once the route discovery, source node initiates wormhole detection process within the established path that counts hop distinction between the neighbors of the one hop away node within the route. The destination node detects the wormhole if the hop distinction between neighbors of the nodes exceeds the suitable level. Our simulation results show that the WHOP is sort of wonderful in detection wormhole of enormous tunnel lengths.

Author[8] were introduced new objective is to prevent potential kinds of routing attacks are wormhole and rushing attack on location- primarily based geocasting and forwarding (LGF) routing protocol in Mobile Ad-hoc Network (MANET). The LGF protocol has proposed to the enforced in real MANET workplace that integration by global Positioning System (GPS)-free covered location tracking system with Geocast-enhanced Ad-hoc On-Demand Distance Vector (GAODV). Additionally wormhole and rushing attack are going to be generating the prevention techniques in LGF protocol and additionally realize the impact of attacks to beat the potential solutions. For Simulation of LGF protocol and attacks has been work done by GloMoSim-2.03 (NS) network simulator.

The approach is employed directional antenna to find and prevent the wormhole attack [9]. The technique is assumed that nodes maintain correct sets of their neighbors. So, an attacker cannot execute a wormhole attack if the wormhole transmitter is recognized as a false neighbor and its messages are neglected.

To estimate the direction of received signal and angle of arrival of a signal it uses directional antennas. This theme works providing two nodes are communication with one another, they receive signal at opposite angle. However this theme is unsuccessful only if the attacker placed wormholes residing between two directional antennas.

Statistical analysis scheme [10] is predicated on relative frequency of every link that is an element of the wormhole tunnel which is appears within the set of all obtained routes. This techniques is use to discover uncommon route selection frequency by victimization statistical analysis detected and can be employed in distinguishing wormhole links. This technique doesn't needs any special hardware or any changes in existing routing protocols. It doesn't need even the aggregation of any special information, since it uses routing data that's already accessible to a node the most plan behind this approach resides within the fact that the ratio of any link that's a part of the wormhole tunnel, are going to be a lot of higher than different traditional links.

To mitigate the wormhole attack in mobile ad hoc network, cluster primarily based technique is projected in [11]. During this approach clusters are formed to discover the wormhole attack. The complete network is split into clusters. These clusters will either be overlapped or disjoint. Member nodes of cluster pass the data to the cluster head and cluster head is no appointive dynamically. This cluster heads maintains the routing info and sends aggregative information to all or any members inside cluster. During this theme, there's a node at the intersection of two clusters named as guard node. The guard node has equipped with power to observe the activity of any node and guard the cluster from doable attack. The network is additionally divided into outer layer and inner layer. The cluster head of outer layer has the responsibility of informing all nodes of the inner layer regarding the presence of the malicious node.

To prevent and observe the wormhole attack most typical approach is mentioned in [10] and [12], referred to as packet leashes mechanism. During this paper, they're conferred two forms of leashes: geographic leashes and temporal leashes additionally given an authentication protocol. The authentication protocol is known as TESLA [12] with instant key revealing and this protocol, to be used with temporal leashes. In, geographic leashes every node access GPS information and supported loose clock synchronization. Whereas temporal leashes need a lot of tighter clock synchronization (in the order of nanoseconds), however don't tightly depend upon GPS information and temporal leashes that are enforced with a packet expiration time. The

observation of this scheme is geographic leashes are less economical than temporal leashes, due to broadcast authentication, wherever precise time synchronization isn't easily possible. Raj palSingh Khainwar et al were given new method which detects malicious nodes and works without modification of routing protocol; consider a hop-count and time delay analysis from the user's point of view without any special environment assumptions. The Research work is simulated in OPNET [13].

Khalil et al. [14] introduces LITEWORP within which they used the notion of guard node. The guard node will discover the wormhole if one in its entire neighbor is behaving maliciously. The guard node could be a common neighbor of two nodes to discover a legitimate link between them. During a sparse network however, it is not always attainable to search out a guard node for a specific link.

IV. PROPOSED ALGORITHM

This paper proposes a reactive routing approach for improving process delay time in previous research study. It is hybridized techniques of time synchronization with WHOP (Wormhole Attack Detection Protocol using Hound Packet), which is based on DSR [15] can efficiently found wormhole in the network and also the nodes that were making the wormhole. In this technique first sender send RREQ packet to destination node. This RREQ packet has destination node address and packet send time. When this packet arrived at the destination node then calculates the average delay time of packet that is:-

End to end delay = Packet receiving time - Packet sending time

Average delay time = End to end delay/no. of hop count

If this average delay time is not greater than 10 ms (that is take as threshold value), therefore route is not affected by malicious activity or wormhole attack. We consider this route for data transmission or if the average delay time is greater than 10 ms than in WHOP, a hound packet will be send after the route has been discovered using DSR routing protocol, the hound packet are processed by each node except nodes who were concerned in route from source to destination throughout path established. The preliminaries of the protocol are as follows:-

4.1 PRELIMINARIES

The Principal of WHOP is to take the help of others nodes (nodes who were not involved in path) after the path has been discovered to found worm hole in the network. Again In path discovery, the protocol uses DSR RREQ packet to find the path from source to destination, RREQ packet being broadcasted by all other node except the destination node. Each node replying back RREP to source node must store its identity into RREP packet. After the source node receives RREP packet, it creates packet called Hound Packet, before forwarding this packet source node computes its Message Digest (MD) and signed the MD with own private key and attached this information with hound packet.

4.2 RREP PACKET

WHOP modifies the packet structure of RREP packet shown in Fig 4. In WHOP protocol, each node stores its identity into RREP packet while sending it to the sender node using backward entry in the routing table. In this way the source node would have the information of each and every node which forms the route to the required destination node.

Type	R	A	Reserved	Prefix Size	Hop Count
Destination IP Address					
Destination Sequence Number					
Source IP Address					
Life Time					
Address [1] = Destination IP Address					
Address [2] = Intermediate Node IP Address					
.....					
Address [n] = Source IP Address					

Figure 4 RREP Packet Format

4.3 HOUND PACKET

The "processing bit" (P.B) can either be 0 or 1, initially all are 0, represents neighbor node of the entry has been visited or not, its value will only be set by the neighbor node of that entry. "Total hop count" field in the packet is used to prevent the packet looping in the network forever, if the value of this field reaches 20 (assuming source and destination would not be more than 20 hops far) then the node will not forward it and drop the packet.

Type	Flags	Reserved	Total Hop Count
Destination IP Address			
Destination Sequence No.			
Originator IP Address			
Originator Sequence No.			
Add [n-1]	Process Bit	Count to reach next hop	
Add [n-2]	Process Bit	Count to reach next hop	
Add [2]	Process Bit	Count to reach next hop	
Last Hop			

Figure 5 Hound Packet Format

"Count to reach next hop" (CRNH) represents the hop distinction between neighbors of one hop separated node, its value are increment by every node for the primary node entry whose processing bit is zero in the data packet. For identify the freshness of the hound packet utilized "Sequence Number" concept; node will cache the foremost recent sequence number packet whereas the previous has been discarded. Every node can cache the hound packet for threshold time to let the destination node discover wormhole within the route if exist at intervals that time. Nodes who receives hound packet first increments the CRNH field for the first node entry whose P.B is 0, second checks if any of the node listed in the hound packet is its neighbor then set all P.B in the packet till the node entry to which it is a neighbor otherwise forward it. Each node also checks if CRNH field in the packet for every entry in the packet are larger than the cached values than dropped the hound packet, otherwise update the smaller CRNH field value in the cache and broadcast the packet by incrementing the CRNH of corresponding entry in the packet.

The different hound packets received at destination node. Here destination node performs calculation on the received values of hound packet to detect wormhole in the pre-formed path between itself and sender. Destination node create table for each entry of hound packet, as it receives new hound packet, receiver adds one new row in each table.

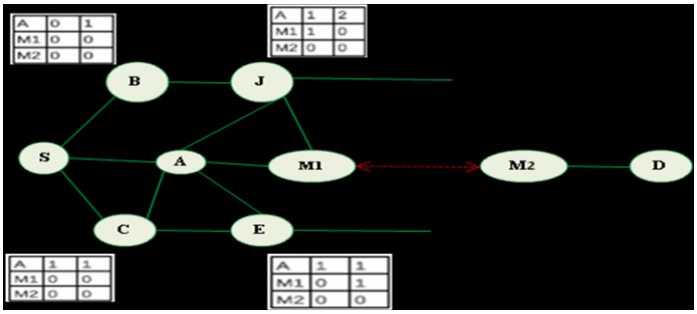


Figure 6 Hound Packet Processing

Figure 6 shows an example where source node S sends the Hound packet to each of its neighbor where node A will drop the packet because its identity included in the packet. When node C receives the hound packet founds it is the neighbor of node A, so it increments the CRNH field by 1 and set the P.B for the node entry A in the packet and forward the packet to node E. Node E founds it is also neighbor of node A but P.B for node A is already set then it increments the CRNH of entry M1. Similarly when node B gets the hound packet founds it does not have any node listed in the hound packet as its neighbor, it then increments the CRNH of the first entry in the packet whose P.B is zero i.e. Node entry A. and broadcast the hound packet. Node J receives the packet, founds it is the neighbor of entry A and M1 then it increments the CRNH field of entry A and set all P.B in the packet till the node entry to which it is a neighbor i.e. M1. Similarly, Hound packet entry will be updated by each node in the network and destination node will receive multiple hound packets with different values.

4.4 SECURITY ANALYSIS OF THE PROTOCOL

WHOP is very secure protocol against any malicious activity being done by node under scan of hound packet. Hidden wormhole attack cannot be doable in WHOP as a result of if node hides its identity whereas forwarding RREQ or RREP, the node who receives such packet once it, would discard the packet as a result of it might not realize the last hop entry within the packet as its adjacent node. So, malicious node must expose its identity while forming the route from source node to destination node. Figure 7 shows m1 is a malicious node forming wormhole with m2 in the path.

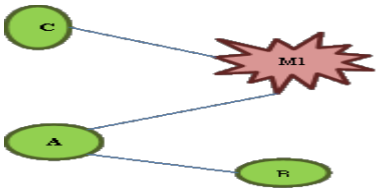


Figure 7 Security Analysis

When node C receives hound packet from previous neighbor, it will find node m1 as its one hop neighbor then node C broadcast the hound packet along with message digest (MD) of the packet encrypted by its private key. As other nodes receives the hound packet they will first decrypt the MD by node C public key, second compute the MD of the received hound packet then compare the result. Node will process the hound packet if comparison result is equal otherwise drop the hound packet.

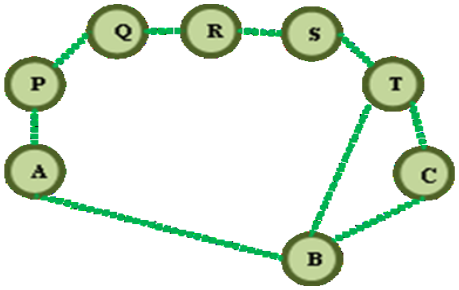


Figure 8 Actual Hop difference

If malicious node m1 try to forward the packet then, it would not forward packet with its own identity in the last hop field of hound packet because its neighbor would discard such packet? Consider Figure 7 If m1 has information about node B that it is a neighbor of node A to whom it is a neighbor node then it may send erroneous hound packet to node A with last hop entry in the packet contain node B identity but at node A message digest comparison will be failed because m1 do not know the private key of node B and node A use public key of node B to decrypt the attached message digest.

4.5 PITFALLS OF THE PROTOCOL

WHOP has major pitfall describes more illustratively in Fig 7 shown below. Suppose the path between Node A and B are part of route connecting source and destination node and they are not forming any wormhole.

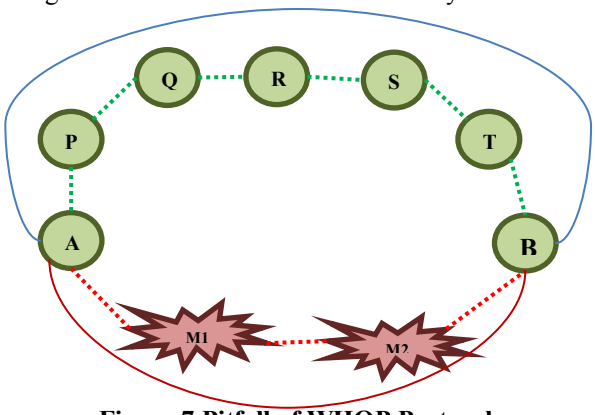


Figure 7 Pitfall of WHOP Protocol

Node A and B are also connected by path 1 (A-P-Q-R-S-T-B) and path 2 (A-M1-M2-B) respectively by their neighbors, while hound packet is traversing it would find both path 1 and path 2 and leads both path information to the destination node. Then wormhole between (node A and Node B) them would not be detected but if there is only path 2 exist then node A and B found as malicious nodes forming wormhole.

V. SIMULATION RESULTS

Simulation can be performed in terms of average End-to-End delay, routing Throughput, Packet delivery ratio

5.1 SIMULATION PARAMETERS

Table1: Simulation parameters

Parameter	Value
Physical Medium	Wireless Channel
Terrain area	670*670
Propagation Model	Two Ray Ground
Traffic model	CBR
Simulator	NS 2.34
Simulation time	120
MAC Protocol	IEEE 802.11
Routing protocol	DSR
No. of nodes	50
Queue Length	50

5.2 SIMULATION PERFORMANCE METRICS

The simulation was done to analyze the performance of the networks for various parameters. Different metrics are used to evaluate the performance of the network under wormhole attack.

5.2.1 Packet Delivery Ratio

The amount of the data packets delivered to the destinations to those generated by the traffic sources.

Packet Delivery Ratio = total data packet received / total routing packet.

5.2.2 Throughput

It is the rate at which a network sends and receives data. It is proportional to a good channel capacity of network connections and rated in terms bits per second (bit/s).

Throughput = Packet received / amount of forwarded packet (over certain time interval).

5.2.3 End to end delay

It refers to the amount of time taken for a packet to be transmitted across a network from source to destination

End to end delay D = packet received time – packet send time

5.3 SIMULATION GRAPH & RESULT ANALYSIS

The simulation result in terms of Packet Delivery Ratio Throughput End to end delay in various mode of network such as:-

- Simulate the Normal network based on DSR routing
- Simulate the Network under affection of wormhole attack.
- Simulate the network under the affection of wormhole attack and (Reactive routing approach) defense mechanism.

5.3.1. Experiment represents Throughput

5.3.1.1 Graphical representation

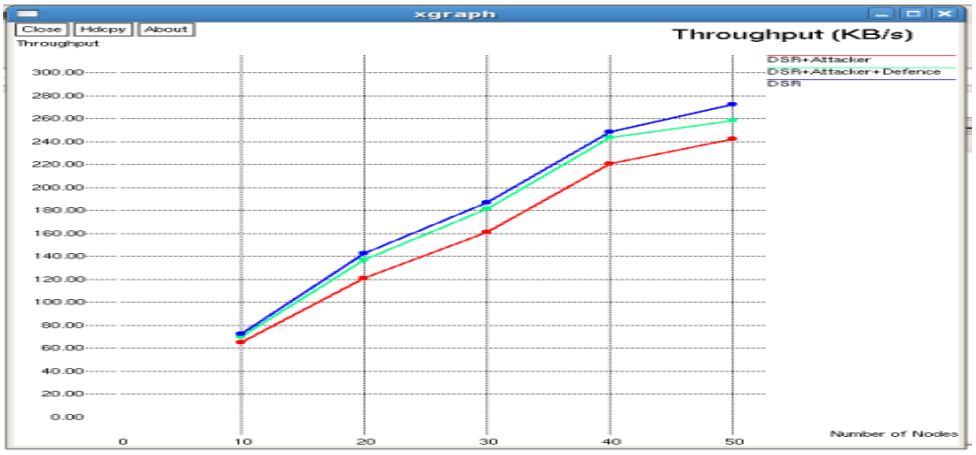


Figure 8 Throughput Analysis

5.3.1.2 Comparative Result of Throughput

S. No.	Throughput (kb/s)			
	Node	DSR	DSR +Attacker	DSR +Attacker + Defense
1.	10	75	62.32	74.5
2.	20	142	120	140
3.	30	182	160	180
4.	40	244	220	242
5.	50	268	240	260

5.3.2 Experiment represents Packet Delivery Ratio

5.3.2.1 Graphical representation

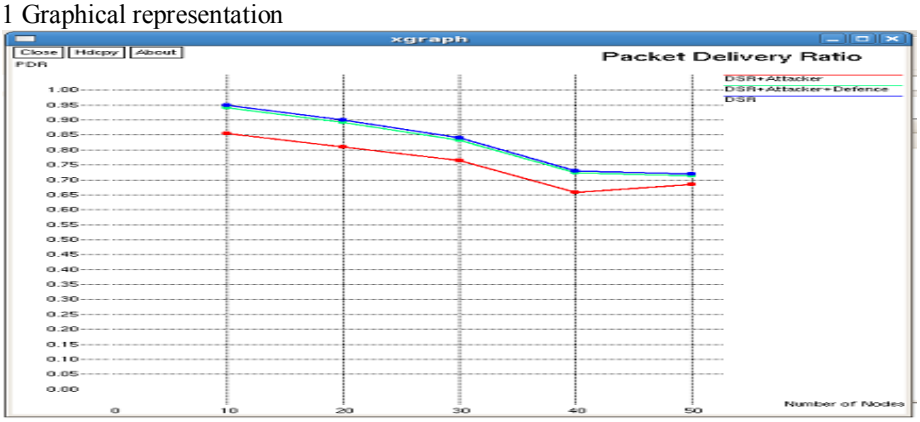


Figure 9 Packet Delivery Ratios

5.3.2.2 Comparative Result of Packet Delivery Ratio

S. No.	Packet Delivery Ratio			
	Node	DSR	DSR +Attacker	DSR +Attacker + Defense
1.	10	0.95	0.85	0.94
2.	20	0.90	0.82	0.89
3.	30	0.84	0.76	0.83
4.	40	0.74	0.66	0.73
5.	50	0.73	0.69	0.72

5.3.3 Experiment represents Average end to end delay

5.3.3.1 Graphical representation

Figure 10 Average end to end delays

5.3.3.2 Comparative Result of Average end to end delay

S. No.	Average end to end delay(ms)			
	Node	DSR	DSR +Attacker	DSR +Attacker + Defense
1.	10	5	7	5.2
2.	20	8	10	8.5
3.	30	28	34	30
4.	40	42	51	43
5.	50	45	56	47

VI. CONCLUSIONS

This research work analyzed the effects of wormhole attack in Mobile ad hoc networks. This work implemented a DSR protocol that simulates the behavior of wormhole attack in NS-2. This research have used very simple and effective way of providing security in DSR routing protocol against wormhole attack that causes the interception and confidentiality of the ad hoc wireless networks. This paper has overcome the drawback of previous approach [7] using hound packet to set up a new routing path every time. That causes long process delay time. The new approach that is hybridized WHOP with time synchronization mechanism to reduce process delay time has given better performance as compare to old approach.

References

[1] Perkins CE, Royer EM, Das SR. Ad hoc on-demand distance vector (AODV) routing, IETF internet draft. MANET Working Group.

[2] Johnson DB, Maltz DA, Hu YC.The dynamic source routing protocol for mobile ad-hoc network (DSR), IETF internet draft (work in progress); July 2004.

[3] P.G. Argyroudis and D. O'Mahony, "Secure Routing for mobile ad hoc networks", IEEE Communications Surveys & Tutorials, third quarter 2005, Vol. 7, no3, 2005 258 Authorized licensed use limited to: University of Allahabad.

[4] Secure Routing in Mobile Ad hoc Network Tirthraj Rai1 & Ashish Jain2, International Journal of Computer Science & CommunicationVol. 1, No. 1, January-June 2010, pp. 125-127.

[5] Hon Sun Chiu, King-Shan Lui. DelPHI: wormhole detection mechanism for ad hoc wireless

[6] Yih-Chun Hu, Member, IEEE, Adrian Perrig, Member, IEEE, and David B. Johnson, Member, IEEEWormhole Attacks in Wireless NetworksIEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO. 2, FEBRUARY 2006

[7] Saurabh Gupta, Subrat Kar, S Dharmaraja "WHOP: Wormhole Attack Detection Protocol using Hound Packet" 2011 International Conference on Innovations Technology IEEE

[8] Rajpal Singh Khainwar1, Mr. Anurag Jain2, Mr. Jagdish Prasad Tyagi3" Elimination of Wormhole Attacker Node in MANET Using Performance Evaluation Multipath Algorithm" ISSN 2250-2459, Volume 1, Issue 2, December 2011

[9] H.S. Chiu and K.S. Lui, "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks," in Proc. International Symposium on Wireless Pervasive computing, Phuket, Thailand, pp. 1-6, 2006.

[10] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks," in Proceedings of the Network and Distributed System Security Symposium.

[11] L. Lazos, and R. Poovendran, "SeRLoc: Secure Range- Independent Localization for Wireless Sensor Networks," in ACM WiSE'04, New York, NY, USA, pp. 73–100, October 2004.

[12] P. Michiardi and R. Molva, "CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks", In Proc. 6th IFIP Commune. And Multimedia Security Conf., Sept. 2002

[13] Pushpendra Niranjan, Prashant Srivastava, Raj kumar Soni, Ram Pratap "Detection of wormhole attack using Hop count and Time delay analysis" International Journal of Scientific and Research Publications, Volume 2, Issue 4, April 2012 1 ISSN 2250-3153

[14] I. Khalil S. Bagchi and N.B. Shroff. LITEWORP: a lightweight countermeasure for the wormhole attack in multihop wireless networks. International Conference on Dependable Systems and Networks, pages 612–621, 2005.

[15] C.E. Perkins and E. M. Royer. The ad hoc on-demand distance vector protocol. In C. E. Perkins, editor, Ad hoc Networking, Addison-Wesley, pages 173–219, 2000.