Wormhole Attack Detection Protocol using Time Stamp with Security Packet.

Chandraprabha Rawat

Department of Computer Application
Samrat Ashok Technological Institute Vidisha, India.

Abstract- **The Mobile Ad hoc Network (MANET) is a Self-organizing and Infrastructure-less Network In mobile ad hoc network data transmission is performed with in untrusted wireless environment. Mobile users communicate over dynamic nature of the network. MANET routing disrupts if participating node do not perform its intended function and start performing malicious activity. Because of dynamic nature of the MANET makes it vulnerable to various attacks that affect the network performance. One of the more complex attacks is called wormhole, in wormhole attacker node records the data from one location and tunnels them to another location and retransmits them into the rest network. Presence of wormhole attacker nodes into the network they decreases the performance of networks. In this paper we proposed a routing protocol named "Wormhole Attack Detection Protocol using Time Stamp with Security Packet " in this routing protocol firstly find out wormhole into the established path between source to destination use new added field Time Stamp. After that we use Security Packet followed by previous research WHOP to find out the position of malicious node. To simulate the results use a tool is called Network Simulator-2(NS2) in term of Throughput(KB/s),Packet Delivery Ratio, End-to-End Delay and also compare the results with WHOP. .**

Keywords:-**Routing Protocal,Mobile ad ho network,Wormhole attack.**

I. INTRODUCTION

Mobile Ad-hoc Network (MANET) is a collection of wireless mobile hosts without fixed network infrastructure and also no centralized administration. Communication in MANET is done via multi-hop paths. There are Lots of challenges (MANET) contains that different resources. Typically, the nodes act as both host and router at the same time i.e. each node participates in routing by forwarding data for other nodes and deciding to which nodes forward data next based on the network connectivity. Most previous ad hoc networks research has focused on problems such as routing and communication, assuming a trusted environment. However, many applications run in untrusted environments and require secure communication and routing such as military or police networks, emergency response operations like a flood, tornado, hurricane or earthquake. However, the open nature of the wireless communication channels, the lack of infrastructure, the fast deployment, and the Environment where they may be deployed, make them vulnerable to a wide range of security attacks. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a stand-alone fashion, or may be connected to the Internet. Multi hop, mobility, large network size combined with device heterogeneity, bandwidth, and battery power constraints make the design of adequate routing protocols a major challenge[11].

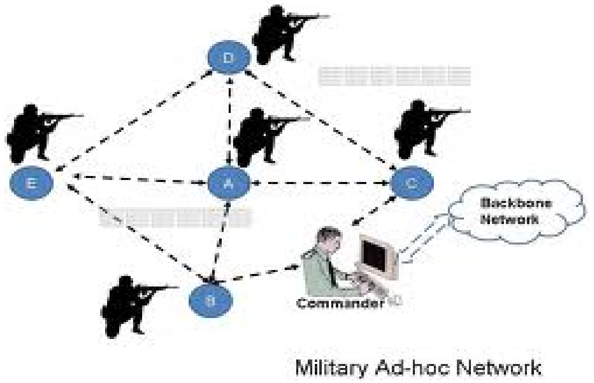


Figure1-ad hoc network.

II. RELATED WORK

In this section we will give a short overview of existing work, Several approaches have been proposed in the literature to defend wormhole attacks in wireless mobile ad hoc networks.

In [4] a new protocol called Multi-path Hop-count Analysis (MHA) is introduced based on hop-count analysis to avoid wormhole attack. It is assumed that too low or too high hop-count is not healthy for the network. The novelty of the hop-count analysis in detecting wormholes is however questionable. Similar works have also been reported earlier. As an example, Djenouri et al. [8] may be considered.

Hu et al. introduced *Packet Leashes* method to defenda gainst the wormhole attack. Two types of leash information was used *Geographical Leash and Temporal Leash.* In geographical leashes each node must have its accurate location information and loose clock synchronization. When node receives a packet, it calculates distance between previous node and itself by using send/receive timestamp. For temporal leashes, each node should have accurate clock synchronization. Every packet should be delivered to the next node within computed life time of a packet. Otherwise, the next node regards the path as a wormhole The packet leashes do not identify malicious nodes.[2]

Khalil et al. Introduces LITEWORP in which they used the notion of *guard node*. The guard node can detect the wormhole if one of its neighbour is behaving maliciously. The guard node is a common neighbour of two nodes to detect a legitimate link between them. In a sparse network, however, it is not always possible to find a guard node for a particular link.[3]

The Delay per Hop Indicator (DelPHI) proposed by Hon Sun Chiu and King-Shan Lui, can detect both hidden and exposed wormhole attacks. In DelPHI, attempts are made to find every available disjoint route between a sender and a receiver. Then, the delay time and length of each route are calculated and the average delay time per hop along each route is computed. These values are used to identify wormhole. The route containing a wormhole link will have a greater Delay per Hop (DPH) value. This mechanism can detect both types of wormhole attack; however, it cannot pinpoint the location of a wormhole. Moreover, because the lengths of the routes are changed by every node, including wormhole nodes, wormhole nodes can change the route length in a certain manner so that they cannot be detected.[5]

Su at al.proposed a routing protocol WHOP (Wormhole Attack Detection Protocol using Hound Packet), which is based on AODV, can efficiently found wormhole in the network and also the nodes who were making the wormhole. In WHOP, a hound packet will be send after the route has been discovered using AODV routing protocol, the hound packet will be processed by every node except nodes who were involved in route from source to destination during pathset up.[1]

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. In path discovery, the protocol uses AODV RREQ packet to find the path from source to destination, RREQ packet beingbroadcasted 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 MessageDigest (MD) and signed the MD with own private key and attached this information with hound packet. Compared with AODV, the proposed WHOP has the following differences in message format.

Hello Packet : WHOP modifies the function of hello packet. In the WHOP protocol, if a node receives a Hello message and does not find an entry of the neighbour node in its routing table, it would create an entry with the destination IP address being the neighbour node. Hello packet also used to broadcast the public key of a node among its one hop away neighbours. In another words, Hello messages will also affect the routing table as well as used to send the public key[1].

Pitfalls of the protocol-

WHOP has major pitfall describes more illustratively in Fig 2(a) 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. Node A and B are also connected by path 1 and path 2 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 them would not be detected but if there is only path 2 exist then node A and B found as malicious nodes forming wormhole. Fig2.

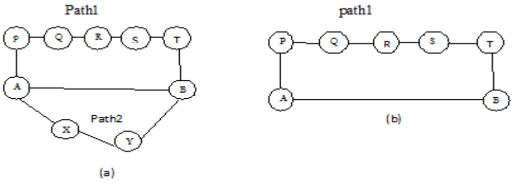


Figure2

III. WORMHOLE ATTACKS

In wormhole attack, a tunnel is created between two nodes that can be used to secretly transmit packets. In a wormhole attack an attacker node receives packets at one point in the network, and tunnels them to another point in the given network and then replays them into the network from that point. For tunneled distances longer than the normal wireless transmission range of a single hop, it is simple for the attacker to make the tunneled packet arrive sooner than other packets transmitted over a normal multihop route, for example through use of a single long range Directional wireless link or through a direct wired link to a colluding attacker. It is also possible for the attacker to forward each bit over the wormhole directly, without waiting for an entire packet to be received before beginning to tunnel the bits of the packet, in order to minimize delay introduced by the wormhole. If the attacker performs this tunneling honestly and reliably, no harm is done; the attacker actually provides a useful service in connecting the network more efficiently.

However, the wormhole puts the attacker in a very powerful position relative to other nodes in the network and the attacker could exploit this position in a variety of ways; the attacker can also still perform the attack even if the network communication provides confidentiality and authenticity and even if the attacker does not have any cryptographic keys.[8]

CLASSIFICATION OF WORMHOLE ATTACK

For example, in figure 1, the path from S to D via wormhole link (W1, W2) has the length of 5 when the normal path has the length of 11. Therefore, in most routing protocols prefers sending data to D along the path with wormhole link.[9] There are several ways to classify wormhole attacks. Here we divide wormhole attacks into 2 categories: hidden attacks & exposed attacks, depending on whether wormhole nodes put their identity into packets' headers when tunneling & replaying packets.[8]

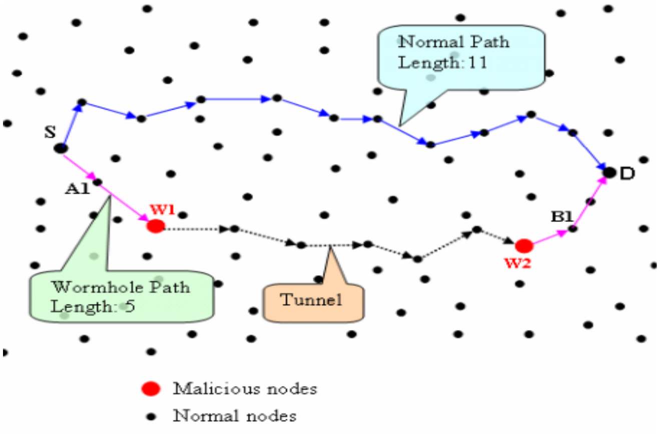


Fig.3-Wormhole Attack

Hidden Attacks-

Before a node forwards a packet, it must update the packet by putting their identity (MAC address) into the packet's header to allow receivers know where the packet directly comes from. However, in hidden attacks, wormhole nodes do not update packets' headers as they should so other nodes do not realize the existence of them. For example this kind of attack, a path from S to D via wormhole link W1, W2 will be (Fig. 3):

S _ A1 _ B1 _ D

In this way, B1 seems to get the packet directly from A1 so it considers A1 its neighbor although A1 is out of radio range from B1 (fake neighbors). General speaking, in hidden attacks nodes within W1's vicinity are "fake neighbors" of nodes within W2's vicinity and vice versa.

Exposed Attacks-

In exposed attacks, wormhole nodes do not modify the content of packets but they include their identities in the packet header as legitimate nodes do (figure 3). Therefore, other nodes are aware of wormhole nodes' existence but they do not know wormhole nodes are malicious. In case of exposed attacks, the path from S to D (figure 3) via wormhole will be:

S _ A1 _ W1 _ W2 _ B1 _ D

IV. Proposed Work

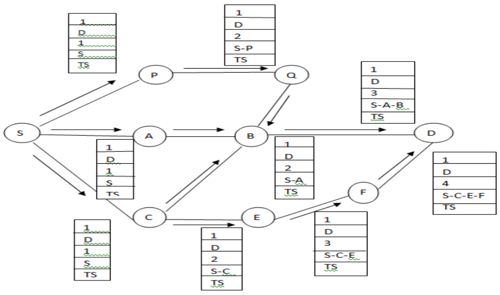
In this paper , we present a more efficient Routing Protocol named Wormhole attack Detection Protocol using Time Stamp with Security Packet. W-TSP allows to the receiver to check whether there are any malicious nodes sitting along its paths from sender to receiver and try to launch wormhole attacks. we obtain the average delay time and total hop count details of paths between the sender and the receiver and use this information to indicate that wormhole attack is subjected in this selected path among. The advantages of W-TSP are that it does not require any special hardware and clock synchronization.

We are detect wormhole in three ways first find out the path between sender and receiver and find out the presence of wormhole attack in this path . In second phase, we send a security packet if we are aware about malicious node which is present in established path between the source node and destination node to get the position of nodes that present in path. In third phase creates a detection table to find out the position of malicious node.

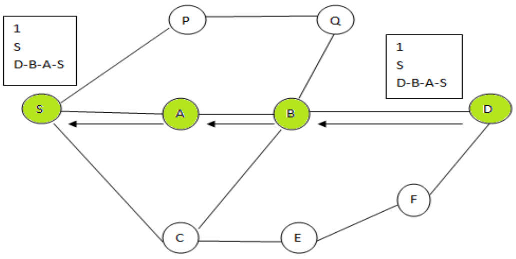
A-First Phase: Path Establishment

In this W-TSP routing protocol the path setup process start with DSR routing protocol using WRREQ packet to find the path from source to destination, firstly source node initiates a RoutRequestPacket(WRREQ) this Route request is flooded thought the network. Each and every node receiving this RouteRequestPacket(WRREQ) with additional field "Time stamp" which is neighbor of source node and all receiving nodes update time stamp value and its own entry and increases hop Difference then rebroadcasts the packet to our neighbor, but neighbor it's receive only when it does not still this type of packet otherwise it discard the packet. Source node generate a sequence number that carried by each RouteRequestPacket(WRREQ) and also carries a path that it has traversed and new updated field. When destination node receive RouteRequestPacket(WRREQ) firstly, It generate a WRRP packet(RouteReplyPacket) and send back to the source node using reverse path that traversed by the RouteRequestPacket.

Fig-WRREQ

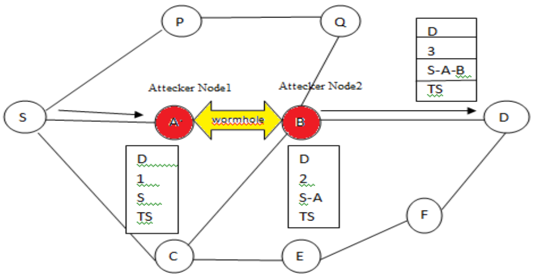


WRRP Packet: In this WRREP packet structure is modified. In the W-TSP protocol each node stores its identity into WRREP packet while sending it to the source node using reverse path in the route cache it is because of source node have knowledge about every node that make route source to destination.



After path setup source node send data packet form this route when destination node received data packet check time stamp field value and total hop difference in their route cache if time stamp value is greater than average time stamp of route cache but total hop difference is same .

It means occurs the problem in the path between sources to destination node. After that we follow the Security packet to find out the malicious node into the path between source to destination and also find out the position of the malicious node.



But some time it happens time stamp field increases time due to traffic that is create by the other node which are participating in this network. In this case we are send the same data packet three time and calculate the same and if two entry of data packet are same which is consider as the results mean we can able to justify values changed either due to traffic or presence of malicious activity.

B-Second Phase: Security Packet

To identify wormhole in the received path source node makes a Security packet which contain all nodes identity whose has been forming rout from source to destination node in currently discovered path.

In the Security packet some specific field are implement that can detected wormhole in the network first field is “Processing Bit (P.B.)” it can be either be 0 or 1, and initially all are 0.it’s represents neighbor node of the entry has been visited or not .the value of processing bit in the packet set by neighbor node entry. “Total Hop Count” field in the packet is used to secure from loop free network. Count to reach next hop (CRNH) represent the hop difference between two neighbor node the separated by one hop and its value will be increased by each node for the first node entry whose processing bit is set 0 in the packet. Sequence number is used to define freshness of the Security packet, node will be cache the newest sequence number of packet while destroy old sequence number. Every node will hold challenge packet for threshold time to detect worm hole in the route by the destination node, if exist within that time. The node that received the Security packet first increase the CRNH field value in the packet for first entry whose P.B. is 0. Second term is checks if any node is present in Security packet is its neighbor or node if is present then set all P.B. in the packet till the node entry to which its neighbor otherwise forward it.

Similarly the Security packet entry will be updated by every node that present in the mobile network and finally multiple packets receive by the destination node with different value.

Addre.	P.B.	CRNH
A	1	3
B	1	1
C	1	0

Addre.	P.B.	CRNH
A	1	4
B	1	0
C	1	1

Addre.	P.B.	CRNH
A	1	5
B	1	0
C	1	0

Table1-Security packets at destination node

C-Third Phase: Detection Table

The deferent Security packet that received by destination node. Destination node perform calculation on all Security packets that received by destination node for detecting wormhole node in the path that is found using DSR routing protocol. Destination node makes detection table for each entry which are included in Security packet. we are here defining a new entry in table called actual difference between nodes .Shows a table for node A that is create by the destination node, first entry show the number of hope, that required to reach the neighbor of c from neighbor of A. second column Shows the next entry in the Security packet whose neighbor node has been found after table node neighbor. The entry of the node filled by examine next entry in the Security packet which has non zero hop count. And finally third column indicate the actual difference between node A and next node which is included in actual path between source and destination node. if actual hop difference between nodes is found 4 or more than four then it mean that this node is creates malicious node which is make wormhole in the path.

Hop	Next node whose Neighbor found	Actual Difference
3	B	3
4	C	4-1=3
5	Destination	5-2=3

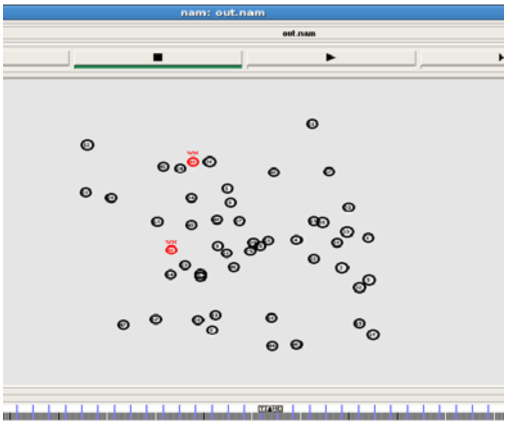
Table2-detection table of node A

In Table2 Where node C is the neighbor of node A hop difference is One. That is subtracted column value by one and similarly is row 1 and three

V. Implementation And Results

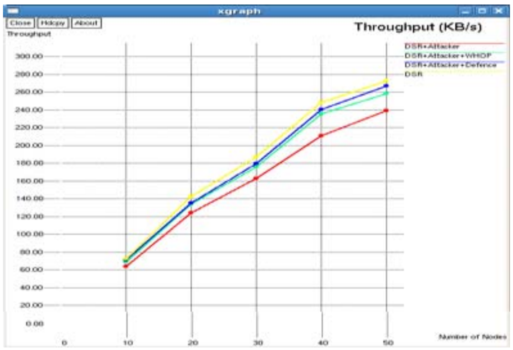
We implement our results in term of Throughput, Packet Delivery Ratio and End-to-End of the network. Using simulation tool is called Network Simulator-2(NS2), NS2 is simply an event-driven Simulation tool that has proved use full in studying the dynamic nature of communication networks. Simulation of wired as well as wireless network functions and protocols (e.g. routing algorithms ,TCP,UDP) can be done using NS2[12]

Figure below Shows the initial position of Mobile nodes in the NAM window:



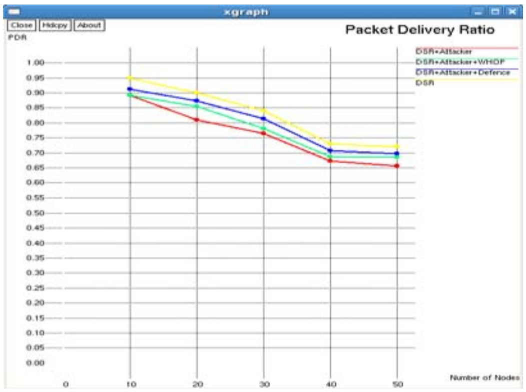
Simulation results of Wormhole attack shown in graphs 1,2,3 using W-TSP:

(A)Result analysis of throughput(KB/s) in case of W-TSP and also compare with previous research WHOP: The network throughput is calculated as the total number of packet received at destination node under given period of time that is articulate in kbps. In the Graph1 shows the results in the normal network with yellow line using DSR routing protocol, and then red line show result with (DSR+ attacker) node which is decrease the throughput. we applies W-TSP technique with new added field Time Stamp against attacker node then graph result is increased and reached around normal network graph and green line show the result of WHOP.



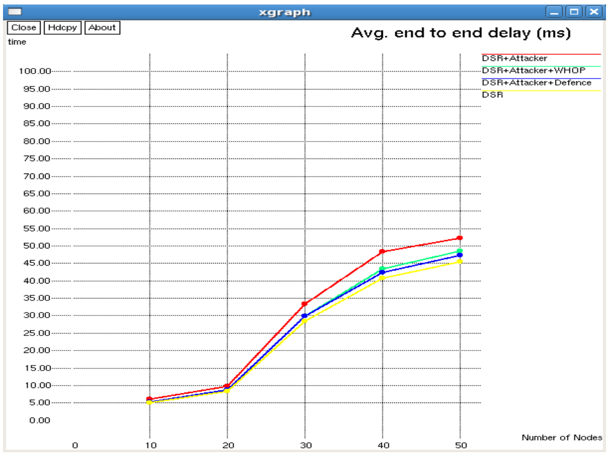
Graph1-Network throughput(KB/s)

(B)Result Analysis of packet delivery ratio (PDR) in case of W-TSP and compare with previous research WHOP : Packet delivery of ratio means that the ratio between packets which have generated by the source node and received at the destination node. Graph2 shows the result with wormhole attacker node and without wormhole node in the mobile ad hoc network .This nature is due to dropping the number of packets reached at destination node through malicious node it is known as packet delivery ratio. Shows in the graph decrement of the PDR due to presence of wormhole link.



Graph2-Packet Delivery Ratio

(C) Result Analysis of Average end-to end delay in case of W-TSP and also compare with previous research WHOP: Define end-to end delay as the time taken by the packet to pass through intermediate node from source and reach at destination node. And it's measured in seconds. Average end-to-end delay is defines as the total time taken over all received packets at destination. Graph3 shows the result of Average end-to-end delay that is increased in presence of wormhole link which very high. And then applies the W-TSP to minimize the Average end-to-end delay which reached around the normal network



Graph3-End-to-End delay

We can analyze the results with the help of table:-

a)Show the result of Throughput(KB/s) in tabular form.

No.of nodes	DSR	DSR+Attacker	DSR+Attacker +Defence-w-tsp	DSR+Attacker +WHOP
10	72.38	61.523	68.761	68.761
20	142.54	125.435	139.689	133.988
30	186.95	166.385	183.211	177.602
40	248.25	215.977	238.320	235.838
50	272.25	239.580	261.360	258.637

Table1

b)**Show the result of Packet delivery Ratio in tabular form.**

No.of nodes	DSR	DSR+Attacker	DSR+Attacker +Defence	DSR+Attacker +WHOP
10	0.95	0.855	0.912	0.902
20	0.90	0.837	0.864	0.855
30	0.84	0.781	0.806	0.798
40	0.73	0.679	0.694	0.679
50	0.72	0.648	0.698	0.684

Table2

c)**Show the result of Avg. end-to-end delay in tabular form.**

No.of nodes	DSR	DSR+Attacker	DSR+Attacker +Defence	DSR+Attacker + WHOP
10	5.075	6.192	5.227	5.380
20	8.324	10.155	8.740	8.740
30	28.450	34.141	29.873	30.158
40	40.678	50.441	42.713	43.119
50	45.478	53.665	47.753	48.753

Table3

VI. CONCLUSION

In this paper proposed a routing protocol to detect wormhole in the mobile ad hoc network. It has detected wormhole efficiently in the large number of mobile nodes, without any additional hardware. We need to changes in exiting DSR routing protocol, In this paper we use a additional field that is called “TIME STAMP” into the DSR Routing Protocol for detection of wormhole attack in the network. When we are create a mobile ad hoc network after that finding path setup using DSR routing protocol and then send this Security packet

to detect malicious node position which makes wormhole attack. Due to wormhole affected the network performance. Show the performance degradation of W-TSP through simulation in term of parameter like network throughput, packet delivery ratio and average end-to-end delay in the graphs. The main advantage of this proposed work we implement DSR Routing Protocol it is cost effective.

In our proposed work we are focus on detection of one wormhole link efficiently in DSR protocol additional field “TIME STAMP” with Security Packet mechanism for finding wormhole node position. In the future research we are focus on detection of multiple wormhole attacker links. Also use another routing protocol that is work more efficiently and cost effective

REFERENCES

[1] International conference on Innovations in Information Technology 2011.”Wormhole attack Detection Protocol using Hound Packet ” .

[2] Yih-Chun Hu , Adrian Perrig , David B. Johnson ,.Packet Leashes:A Defense against Wormhole Attacks in Wireless Ad Hoc Networks.

[3]Khalil, S. Bagchi, N. B. Shroff. LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks. In International Conference on Dependable System and Networks (DSN), Jul. 2005.

[4]Sun Chui ,Doo-young Kim.WAP:Woemhole Attack Prevention algorithm in Mobile Ad Hoc Networks.2008 IEEE International Conference on Sensor Network, Ubiquitous, and Trustworthy Computing.

[5]DelPHI:wormhole detection mechanism for ad hoc wireless network proposed by Hon Sun Chiu and King-Shan Lui in international Symposium on wireless Pervasive Computing ,Phuket,Thailand, 16-18 january 2006.

[6]Jun-Zhao Sun MediaTeam, Machine Vision and Media Processing Unit, Infotech Oulu P.O.Box 4500, FIN-90014 University of Oulu, Finland.

[7]Prevention ofWormhole Attack in MANET Latha Tamilselvan BSA Crescent Engineering College, Vandalur, Chennai, Tamilnadu, India.

[8]IRACST-Engineering Science and technology: An International Journal(ESTIJ),ISSN:2250-3498 Vol.2No,2,April 2012 “Wormhole attack in Mobile ad hoc Networks A Review”.

[9]September-2011, ISSN 2229-5518. | [9] Wenjia Li and Anupam Joshi, “ecurity Issues in Mobile Ad Hoc Networks - A Survey”.

[10]D B. Johnson, D A. Maltz, and Y. Hu. “The dynamic source routing protocol for mobile ad hoc network,", Internet-Draft, April 2003.

[11]Ullah.Master Thesis Electrical Engineering Thesis no: MEE 10:62 june 2010 “Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols”.

[12]Introduction to Network Simmulator NS2 Teerawat,Issariyakul,Ekram hossain,goolge book