Study of Wormhole Attack in Mobile Ad-Hoc Network

Ashish Kr. Shrivastava
Associate Professor
NIIST BHOPAL

Neha Jain
Master of Computer Science & Engineering
NIIST BHOPAL

ABSTRACT

A wireless ad-hoc network could be a quickly set network by wireless mobile computers (or nodes) moving absolute within the place that don't have any mounted network infrastructure. The requirement for cooperation among nodes to relay every other's packets within the ad-hoc network exposes them to a wide range of security attacks. Ad-hoc wireless network is not secure to the attacks of malicious nodes ,out of all the attack cause by the malicious nodes, the foremost devastating attack is thought because the wormhole attack, within two or more malicious colluding nodes produce a higher level virtual tunnel(or secrete tunnel) within the network, that transport packets at one location within the network wherever the human records transmitted packets at one location, and transmit them into the network .Even if all communication provides authenticity and confidentiality, the wormhole attack is feasible. This paper presents a study on wormhole attack and its counter measures in ad-hoc wireless network, along with the future research scope.

Keywords

Ad Hoc Networks, Malicious Node attacks, Wormhole attack DSR (Dynamic Source Routing)

1. INTRODUCTION

A network is ad-hoc as a result of it doesn't have faith in a pre-existent infrastructure like routers in wired networks or access points in managed (infrastructure) wireless network. An ad-hoc network is self-organizing and adaptive networks formed on-the-fly, devices will leave and be a part of the network throughout its life. This network has the options of shared broadcast radio channel, Insecure operative atmosphere, absence of infrastructure, lack of central authority, lack of -association, limited resource accessibility, dynamical topology, resource violence and lack of clear line of defense, create them at risk of a wide range of security attacks. Fig1. Gives the basic infrastructure of MANET

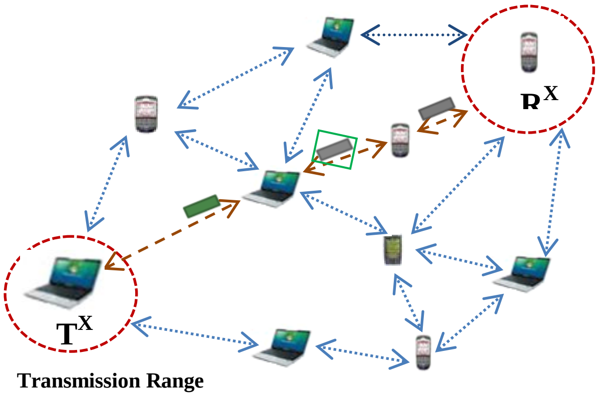

Figure1. Basic Infrastructure of MANET

Ad-hoc network are more vulnerable to the safety attack as compared to wired network or infrastructure based wireless network due to distributive nature. These networks are at risk of the wormhole attack launched through the compromised nodes (node that perform internal attacks).The remaining section of this paper is as follows: sections 2 discuss the various types of security attack in MANET and affected routing protocol, section 3 discuss the current state of art of wormhole attack, section 4 discuss the defense mechanism against Wormhole Attack, section 5 discuss the research scope and at last in section 6 is conclusion.

2. TYPES OF SECURITY ATTACKS IN MANET

Consider Table 1. Security Attacks on the ad-hoc network can be classified into two broad categories:-

Attacks in MANET	
Passive Attack	**Active Attack**
1.Traffic Analysis 2.Eavesdropping	1.Routing Attack 1.a Black-hole Attack 1.b Wormhole Attack 2. Session Hijacking Attack 3. SYN Flooding attack 4. Repudiation Attack

2.1 Passive Attack:-

A passive attack doesn't disrupt the conventional operation of the network; the attacker sleuth the data changed within the network while not altering it. Here the need of confidentiality gets violated. Detection of passive attack is extremely difficult that's why the operation of the network itself does not get affected [1]. Different Passive attacks are:-

2.1.2 Traffic Analysis & Monitoring:-Traffic analysis attack adversaries observe packet transmission to infer necessary information like a sender, destination, and sender-destination pair.

2.1.1 Eavesdropping:- Eavesdropping is another kind of attack that typically happens within the mobile ad hoc networks. It aims to get some confidential information that ought to be unbroken secret throughout the communication. The data could include the location, public key, personal key or maybe passwords of the nodes. As a result of such data is important to the security state of the nodes, they must be unbroken far away from the unauthorized access.

2.2 Active Attack:-

An active attack makes an attempt to alter or destroy the data being changed inside the network there by disrupting the traditional functioning of the network. Active attacks are going to be internal or external. External attacks are administrated by nodes that do not belong to the network. Internal attacks as a result of compromised nodes that are a part of the network. That's why the attacker is already present in the network, internal attacks are additional severe and exhausting to seek out than external attacks. Active attacks, whether or not or not administrated by an external advisory or an internal compromised node involve actions such as interception, modification, fabrication and replication [1].

These attacks may involve eavesdropping, message meddling, or identity spoofing. Several attacks are targeted at the data traffic by dropping all data packets (black-hole attack), by selection dropping data packets (gray-hole attack), and performing statistical analysis on the data) packets to get essential information, like the location of primary entities within the network. Alternately, the attacker are able to do such attacks by having a number of powerful adversary nodes that require not authenticate themselves to the network (i.e., external nodes). The attackers are able to do this by targeting specific control traffic within the network. Typical examples of control traffic are routing, watching aliveness of a node, topology determination, and distributed location discovery. A particularly severe control attack on the routing functionality of wireless networks, known as the wormhole attack [2][3][4], has been introduced within the context of ad-hoc networks.

2.2.1 Routing Attack: - There are several types of attacks mounted on the routing protocol which are aimed at disrupting the operation of the network. Black-hole and wormhole attack are under the category of routing attack.

a) Black hole Attack: The black-hole attack has two properties. First one is the node exploits the mobile ad hoc routing protocol, such as AODV Protocol(Ad hoc On-Demand Distance Vector Routing),to advertise itself as having a legitimate route to a destination node, even if the route is unauthentic, with the intention of intercepting packets. Second property is the attacker consumes the intercepted packets with none forwarding. However, the attacker runs the danger that neighboring nodes can monitor and expose the continued attacks. There's a lot of delicate form of these attacks once an attacker by selection forwards packets. An attacker modifies packets originating from some nodes, whereas leaving the data from the opposite nodes unaffected that limits the suspicion of its wrongdoing [4].

2.2.2 Session hijacking attack: Session hijacking takes advantage of the actual fact that almost all communications are protected (by providing credentials) at session setup, however not thereafter. Within the TCP session hijacking attack, the attacker spoofs the lost node IP address, determines the proper sequence number that's expected by the target, and so performs a DOS (Denial of Service) attack on the victim. Thus the attacker impersonates the lost node and continues the session with the target.

2.2.3 SYN flooding attack: The SYN flooding attack could be a denial-of-service attack. The attacker creates an oversized number of half-opened TCP connections with a victim node, however never completes the handshake to completely open the connection.

2.2.4 Repudiation attack: Repudiation attack: In the network layer, firewalls are often put in to keep packets in or keep packets out. Within the transport layer, entire connections are often encrypted, end-to-end. However these solutions don't solve the authentication or non-repudiation problems. Repudiation means to a deny participation in a section of the communications.

The wormhole attack is especially dangerous against several ad-hoc network Routing Protocols within which the nodes that hear a packet transmission directly from some node think about themselves to be in vary of (and, so a neighbor of) that node. Wormhole attack is under the category of routing attack. The nodes in Ad-hoc network perform the routing functions in another to the inherent function of being the hosts. The drawback with wireless transmission fluctuation needs the routing in multiple hops. The nodes rely upon one another for transmission of packets from sender nodes to destination nodes via the routing nodes. The nature of the networks places two elementary requirements on the routing protocols. First one is, it has to be distributed. Secondly, since the topology changes area unit frequent, it got to compute multiple, loop-free routes whereas keeping the communication overheads to a minimum. Supported route determination time, MANET routing protocols represent three general categories:

2.2.4.1 Proactive routing protocols: Proactive routing protocols can actively verify the layout of the network and it based on table-driven approach. The complete network is maintained at each node; therefore route selection time is lowest. But the mobility of nodes if high then routing info in the routing table invalidates terribly quickly, leading to many short lived routes. This additionally causes an oversized amount of traffic overhead generated once evaluating these inessential routes. For big size networks and therefore the networks whose member nodes build scattered transmissions, most of the routing information is redundant by nature. Energy conservation being terribly important in MANETs, the excessive expenditure of energy isn't desired. Thus, proactive painter protocols work best in networks that have low node mobility or wherever the nodes transmit data oftentimes. Examples of proactive MANET protocols embrace Optimized Link State Routing (OLSR), Topology Broadcast based on Reverse Path Forwarding (TBRPF), Fish-eye State Routing (FSR), Destination-Sequenced Distance Vector (DSDV), Landmark Routing Protocol (LANMAR), Cluster head entrance Switch Routing Protocol (CGSR) [5].

2.2.4.2 Reactive Routing Protocol: Reactive MANET protocols solely realize a route to the destination node once there's a necessity to send data. The sender node can begin by transmission route requests throughout the network. The sender can then wait for the destination node or associate intermediate node (that contains a route to the destination) to reply with a list of intermediate nodes between the sender and destination. This can be called the worldwide flood search, which successively brings a couple of significant delay before the packet is transmitted. It in addition desires the transmission of an enormous amount of management traffic. Thus, reactive MANET protocols area unit most suited to networks with high node quality Examples of reactive MANET protocols embrace ad hoc On-Demand Distance Vector (AODV), Dynamic source Routing (DSR), Temporally Ordered Routing algorithm (TORA), Dynamic MANET on Demand (DYMO) [5].

Basically DSR is a routing protocol which is example of reactive routing protocol. The Dynamic source Routing protocol (DSR) [Johnson 1994, Johnson 1996a, Broch 1999a] may be a straightforward and valuable routing protocol designed specifically to be used in multi-hop wireless ad hoc networks of mobile nodes [6].Using DSR, the network is totally self-organizing and automatic-construct, requiring no existing network infrastructure or administration. Network nodes (computers) collaborate to forward packets for every other to permit communication over multiple "hops" between nodes in a roundabout way among wireless transmission range of one another. As nodes within the network move regarding or be a part of or leave the network, and such as wireless transmission conditions like sources of interference modification, all routing is mechanically determined and maintained by the DSR routing protocol. Therefore the number or sequence of intermediate hops required to reach any destination could modification at any time, the resulting configuration is also quite made and quickly changing. The DSR protocol consists of two mechanisms that employment along to permit the invention and maintenance of source routes within the ad hoc network:

1. Route Discovery
2. Route Maintenance

2.2.4.3 Hybrid routing protocols: In MANET Both proactive and reactive routing protocols every work best in oppositely various type of problem, that's why we have best reason to develop hybrid routing protocols, which use a combination of each proactive and reactive routing protocols. These hybrid protocols may be wont to realize a balance between both (the proactive and reactive protocols). The basic plan behind hybrid routing protocols is consider proactive routing mechanisms in some areas of the network at limited times and reactive routing for the rest of the network. The proactive protocol operations are restricted to a little domain so as to reduce the control overheads and delays in network. The reactive routing protocols are very useful for locating nodes outside this domain, as this can be a lot of bandwidth-efficient in a very constantly dynamical network. Examples of hybrid routing protocols consider Core Extraction Distributed Ad Hoc Routing Protocol (CEDAR), Zone Routing Protocol (ZRP), and Zone Based Hierarchical Link State Routing Protocol (ZHLS) [5].

3. WORMHOLE ATTACK

3.1 Basically wormhole attack is finished by two or a lot of malicious nodes with conspiracy. Just in case of wormhole attack, two malicious nodes at totally different locations communicate to every alternative via a secrete channel. Thus the two malicious nodes are settled far from one another and that they initiate to be among one-hop count communication range. primarily this secrete tunnel is incredibly long as compare to traditional root from supply to destination however it's logically suppose united hop count. The tunnel like channel will be completed by two methods:

a.) Packet encapsulated channel or In-band channel:

When the Sender node broadcast the RREQ packet, a malicious node that's at one an area of the network receives the RREQ packet and it forward through the tunnels to a second colluding party that's at a faraway location near the destination, and then rebroadcasts it. The neighbors of the second colluding party receive the RREQ and drop to any extent further legitimate requests that may arrive shortly legitimate multi-hop ways. The result is that the routes between the Sender and thus the destination endure the two colluding nodes which are able to be same to possess formed a wormhole between them. And it prevents nodes from discovering legitimate ways in which are over more than hops away.

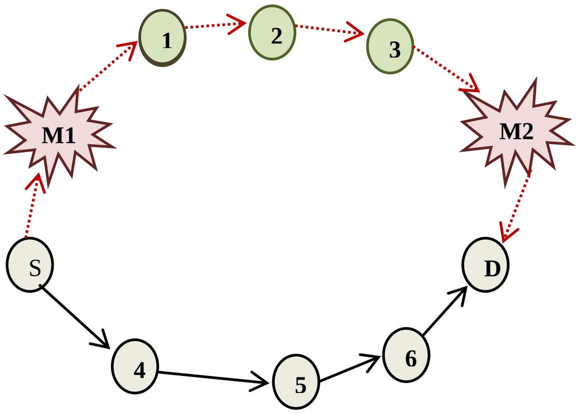

Figure2. Wormhole through packet encapsulation

In Figure 2 Node S is Sender node and D is that the destination node, each attempt to discover the shortest path between them, within the presence of the two malicious nodes M1 and M2. Node S broadcasts a RREQ, M1 gets the RREQ and encapsulates it in a packet destined to M2 through the trail that exists between M1 and M2 (1-2-3). Node M2 receive the packet, and rebroadcasts it once more, that reaches D. Note that as a result of the packet encapsulation, the hop count doesn't increase throughout the traversal through 1-2-3. At the same time, the RREQ travels from S to D through 4-5-6. Node D currently has two routes, the primary is Four hops long (S-4-5-6-D), and therefore the second is outwardly three hops long (S-M1-M2-D). Node D will choose the second route since it appears to be the shortest whereas basically it's seven hops a part. Any routing protocol that uses the metric of shortest path to choose the foremost optimal route is vulnerable to this mode of wormhole attack.

b.) Out of band channel:

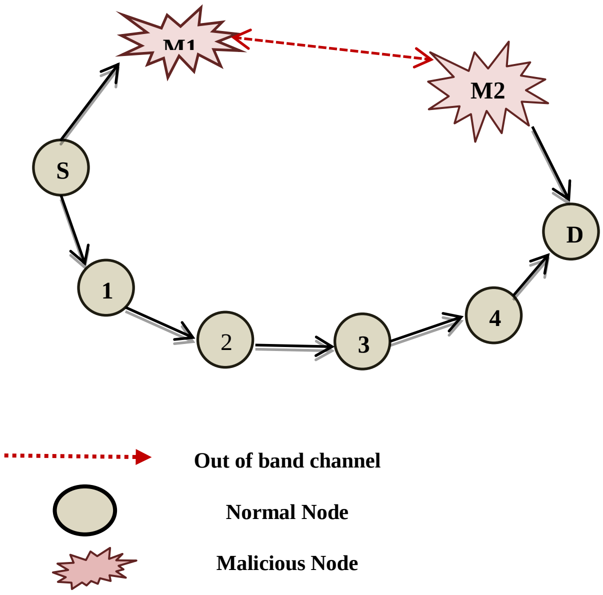

Figure 3.Wormhole through out-of-band channel

This mode of wormhole attack involves the utilization of an out of band channel. This attack is established by having an out of band high-bandwidth channel between the malicious nodes. This mode of attack needs specialized hardware capability. In Figure 3 Node S sends a RREQ to node D, and nodes M1 and M2 are malicious nodes having an out-of-band channel between them. Node M1 tunnels the RREQ to M2, which is a legitimate neighbor of D. Node M2 broadcasts the packet to its neighbors, including D. D gets two RREQs—S-M1-M2-D and S-1-2-3-4-S. The first route is both shorter and faster than the second, and is thus chosen by D.

3.2 Wormhole Attack Threats:-We can contemplate wormhole attack as a two phase method launched by one or many malicious nodes. Within the initial phase, the two malicious end points of the tunnel could use it to pass routing traffic to attract routes through them. Within the second phase, wormhole nodes may exploit the data in type of ways in which, they'll disrupt the data flow by selection dropping or modifying data packets, generating redundant routing activities by turning off the wormhole link periodically, etc. The attacker also can merely record the traffic for later analysis. Using wormholes an attacker also can break any protocol that directly or indirectly depends on geographic proximity. It ought to be noted that wormholes are dangerous by themselves, though attackers are diligently forwarding all packets with none disruptions, on some level, providing a communication service to the network. With wormhole in situ, affected network nodes haven't got a real image of the network, which might be disrupt the localization-based schemes, and thus lead to the inaccurate choices, etc. wormhole can also be used to merely combination an oversized range of network packets for the purpose of traffic analysis or cryptography compromise.

3.3 Impacts of wormhole attacks: If the wormhole can solely peacefully transport all the traffic from one location within the network to a different location that's isolated, then it may be helpful for the network operation because it will improve the network connectivity. Unfortunately if once the traffic is routed through the wormhole, the attacker can gain full management over the traffic. Then he will begin his malicious actions by selection dropping data packets which is able to lower the network throughput or store all the traffic and later perform cryptanalysis attacks. The attacker will decide once to drop data packets that go through the wormhole at some crucial situations. For instance, if the network is employed for a few alarm or surveillance systems, then the attacker will decide to time his packet dropping with a planned intrusion into the system. The wormhole attack was presented to have important impact on both proactive and reactive ad hoc routing protocols.

4. DEFENSE MECHANISM AGAINST WORMHOLE ATTACK

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 [7].

Saurabh Gupta [8] 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[9] were introduced new objective to prevent potential kinds of routing attacks are wormhole and rushing attack on location- primarily based geo-casting 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 geo-cast 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 [10]. 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. In this approach two nodes are communicating 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 [11] 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 [12]. 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 [11] and [13], 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 [13] 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 pal Singh 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 [14].

5. RESEARCH SCOPE

In Previous Research study we have got few techniques for detection and prevention of wormhole attack with some limitation, which we have summarized below in table 1.

Table2. Summary of detection & prevention method of Wormhole attack

Sr.	Research Finding	Research Scope
1.	Packet leashes (TIK Protocol)[7]	Only topological based detection & Time Synchronization Constant
2.	WHOP Protocol[8]	Process Delay time is more
3.	LGF Protocol[9]	Use other expensive hardware
4.	Directional antenna[10]	It works providing two nodes are communication with one another (This is unsuccessful only if the attacker placed wormholes residing between two directional antennas.
5.	Statistical analysis[11]	It works on relative frequency of every link & discriminate the normal link with wormhole link.
6.	hop-count and time delay[14]	Only use for detection of wormhole attack not give the concept for prevention of attack

In previous research study which is introduced by Saurabh Gupta et al they overcome the problem of time synchronization and using extra cost expensive hardware [8].

The aim of this research work is to improve the process delay time which was pointed in research base paper [8]. For solution of the problem discussed above we need to hybridize WHOP protocol with time synchronization mechanism. The proposed approach may give efficient results to secure data packet transmission and improving the process delay time. We will work with DSR routing protocol that simulates the behavior of wormhole attack using network simulator ns-2.

6. CONCLUSIONS

This paper presents survey of the various types of attack to the ad-hoc networks and also introduced the wormhole attack with detailed description. Here discussed threats of this attack, and summarized the effort done in the literature to combat this attack. Ethically, this type of wormhole analysis is important to account for possible new dangers and variations of this attack. This proposed work introduces new technique for preventing wormhole attack while not support of any hardware and clock synchronization. This work will be completed with DSR routing protocol that simulates the behavior of wormhole attack in NS-2(Network simulator-2).

REFERENCE

[1] Mariane A. Azer, Sherif M. El-Kassas, ―An Innovative Approach for the Wormhole Attack Detection and Prevention in Wireless Ad-hoc Network‖2010.

[2] Matthew Tan Creti,Matthew Beaman,Saurabh Bagchi,Zhiyuan Li,Yung-Hsiang Lu, ―Multigrade Security Monitoring for Ad-hoc Wireless Networks‖ ,2009IEEE.

[3] Bhargava, B.de Oliveira, R. Yu Zhang Idika, ―Addressing Collaborative Attacks and Defense in Ad Hoc Wireless Networks‖ 29th IEEE International Conference on Distributed Computing Systems, 2009

[4] Pradip M. Jawandhiya et. al. / International Journal of Engineering Science and Technology Vol. 2(9), 2010, 4063-4071.

[5] Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharma JOURNAL OF COMPUTING, VOLUME 3, ISSUE 1, JANUARY 2011, ISSN 2151-9617

[6] DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks David B. Johnson David A. Maltz Josh Broch

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

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

[9] 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

[10] 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.

[11] L. Hu and D. Evans “Using directional antennas to prevent wormhole attacks” In Proceedings of the Network and Distributed System Security Symposium.

[12] 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.

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

[14] 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.