Review Research Study on Wormhole Attack in MANET

[1]Sonam gupta, [2]Garvita Gupta
BIST, Bhopal ,India
Email: Sonam21g@yahoo.com

Abstract :**A MANET (Mobile Ad-hoc network) is a self-configuring infrastructure less network of mobile devices connected by wireless. 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, Wormhole attack**

1. INTRODUCTION

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 defence, create them at risk of a wide range of security attacks. Fig1. Gives the 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).

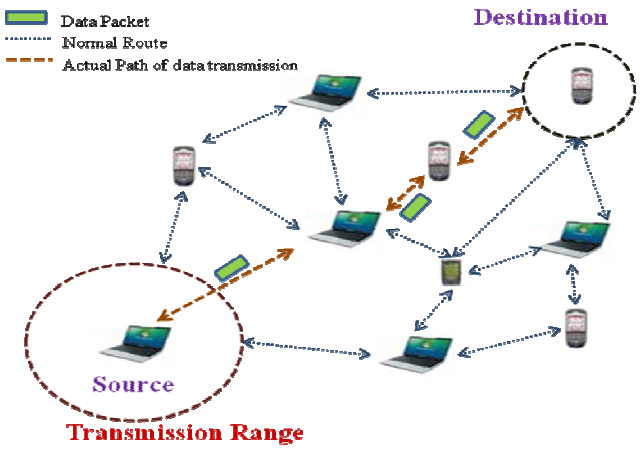

Figure 1 of MANET

The remaining section of this paper is as follows: sections 2 discuss the current state of art of wormhole attack, sections 4 discuss the defence mechanism against Wormhole Attack, sections 5 discuss the research scope and at last in section 6 is conclusion.

2. WORMHOLE ATTACK

2.1 Definition of Wormhole attack

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 neighbours 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.

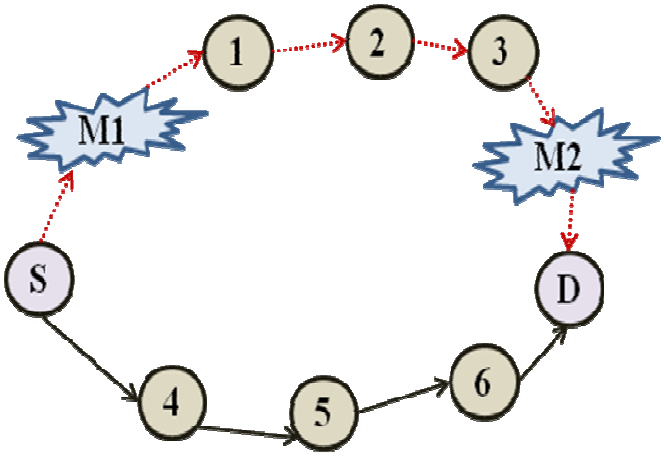

Figure2. Wormhole through packet encapsulation

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:

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.

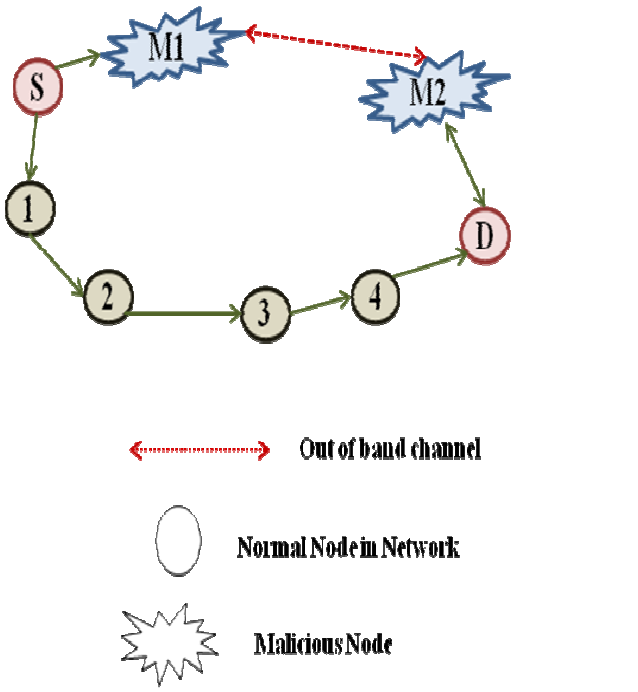

Figure 3.Wormhole through out-of-band channel

2.2 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.

2.3 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.

3. 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 [1]

Saurabh Gupta [2] 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 neighbours of the one hop away node within the route. The destination node detects the wormhole if the hop distinction between neighbours 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[3] 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 [4]. The technique is assumed that nodes maintain correct sets of their neighbours. So, an attacker cannot execute a wormhole attack if the wormhole transmitter is recognized as a false neighbour 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 [5] 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 [6]. 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 [5] and [7], 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 [7] 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 [8].

4. RESEARCH SCOPE

In Previous Research study we have got few techniques for detection and prevention of wormhole attack with some limitation such as:

- **Packet leashes (TIK Protocol)[1]:-** Only topological based detection And Time Synchronization Constant.
- **WHOP Protocol[2] :-** Process delay time is more
- **LGF Protocol[3]:-** Use other expensive hardware
- **Directional antenna [4]:-**It works providing two nodes are communication with one another (This is unsuccessful only if the attacker placed wormholes residing between two directional antennas.
- **Statistical analysis [5] :-**It works on relative frequency of every link & discriminate the normal link with wormhole link.
- **Hop-count and time delay [8]:-** 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 [2]. The aim of this research work is to improve the process delay time (due to AODV protocol because it is beaconless) which was pointed in research base paper [2]. 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 behaviour of wormhole attack using network simulator ns-2.

5. CONCLUSION

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 behaviour of wormhole attack in NS-2(Network simulator-2).

REFERENCE

[1] 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

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

[3] 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

[4] 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.

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

[6] 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.

[7] 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

[8] 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.