Volume 4, Issue 5, May 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

# Analysis of Wormhole Attack Detection and Prevention Techniques in MANET

**Shivangi Dwivedi, Priyanka Tripathi**
Dept of Computer Engg & Application
National Institute Of Technical Teachers'Training and Research
Bhopal , India

***Abstract*— *MANET is a collection of autonomous system of mobile nodes connected with each other using wireless link and each node communicates with each other using wireless link that are within its transmission range. Mobile Ad-Hoc Network (MANET) is an infrastructure less self-configured collection of mobile nodes that can arbitrarily change their geographic locations such that these networks have dynamic topologies and random mobility with constrained resources. The network is unbounded by any fixed infrastructure or any central authority. The absence of any central coordination mechanism and open nature makes the Mobile Ad Hoc Network more vulnerable to security threats. Wireless networks are susceptible to many attacks, including an attack known as the wormhole attack .Wormhole attack is one such security threat at network layer which causes routing disruption. The attacker at one point in the network records the packet and forwards it through a high speed tunnel to the other attacker present at distant location giving an false impression to nodes in both the network that they are immediate neighbors. This paper presents a study on wormhole attack and various existing techniques to detect and prevent wormhole attack in MANET.***

***Keywords*— *Mobile ad-hoc Network (MANET), Security, Wormhole Attack, Types of Wormhole Attack, Reactive Routing Protocol.***

## I. INTRODUCTION

Mobile ad hoc networks (MANET) can be defined as a collection of large number of mobile nodes that form temporary network without help of any existing network infrastructure or central access point. Each node participating in the network acts both as host and as router. It allows the devices to maintain connections to the network as well as easily adding and removing devices in the network [1]. The nature of ubiquitous communication in Mobile wireless networks increases the demand in many application areas. MANET has a huge number of nodes that use no fixed infrastructure or fixed connectivity among them. Each node has small processing unit, memory, communication interface and limited residual power. Infrastructure of MANET is reconfigurable whenever the node changes its location. Communication among the nodes is possible by multi hop paths by using a number of intermediate nodes [2]. A MANET is also known as a mobile mesh networks that consists of wireless mobile nodes that dynamically self organized connected by wireless links. An Ad Hoc network is defined as —an autonomous system of routers and associated hosts connected by wireless links, the unions of which form an arbitrary graph. 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 standalone fashion, or may be connected to the larger Internet operating as a hybrid fixed/ad hoc network [3].

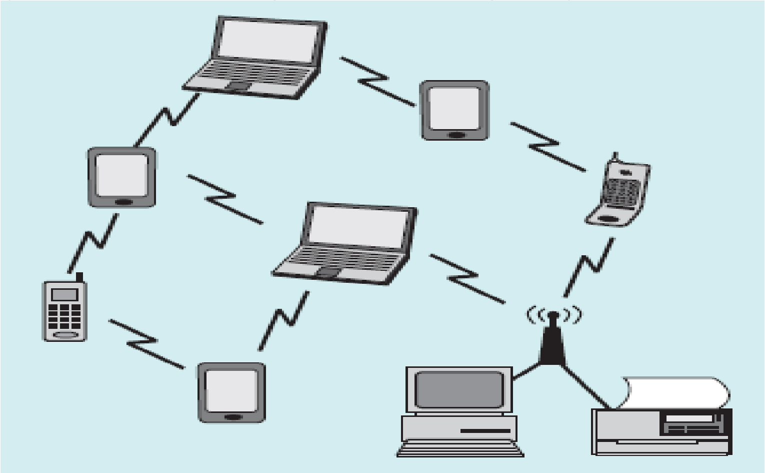

Fig.1-Mobile Ad-hoc Network [4]

In general, attacks are two types; active attacks and passive attacks. Wormhole attack [5] comes under active attack is depicted in fig.2.

Passive attack: These types of attacks are not disrupting the network. For example eavesdropping attacks and traffic analysis and monitoring etc.

Active attack: These types of attacks are disrupted the network, to alter or destroy data being exchanged in the network. These attacks can be internal or external. Wormhole attack is one of the major security threats that can cause major disruption in network communication where a malicious node captures packet from one location in the network, tunnels it to another malicious node at distant point, when then replays it locally Once the wormhole link is established malicious nodes can either drop the packet, perform eavesdropping Denial Service Attack.

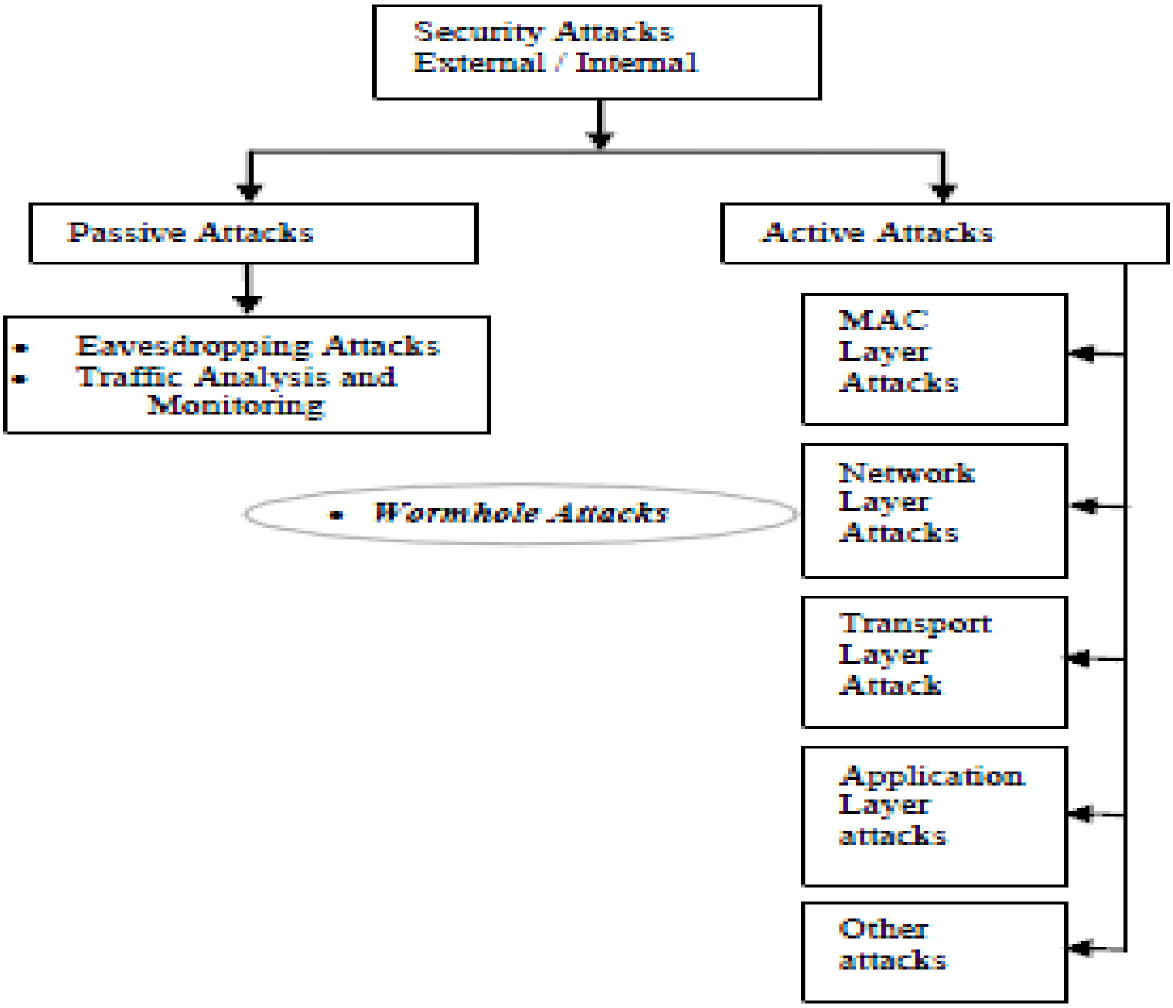

Fig.2-Categories of Attacks in MANET

The rest of the paper is organized as follows. Section II discusses the Wormhole attack in MANETs and its classification. Section III presents the various modes of wormhole attack. Section IV presents various detection and prevention techniques for wormhole attack. Section V presents our conclusion.

## II. **WORMHOLE ATTACK IN MANET**

The Wormhole attack, a route disrupting attack is one of the most serious security issue in MANET. It is a kind of tunneling attack in which a malicious node receives packet at a one location in the network, tunnels them to another location in the network and then replays them into the network from that point.

In wormhole attack [5], an attacker connects two distant points in the network, and then replays them into the network from that point. An example is shown in Fig. 3. Here S and D are the two end-points of the wormhole link (called as wormholes). In Fig. 3, wormhole attack is assumed between the node A and node H and their neighbours nodes, vice versa. The wormhole link can be established by many types such as by using Ethernet cables, long-range wireless transmissions and an optical link in wired medium. In a wormhole attack, a malicious node uses a path outside the network to route messages to another compromised node at some other location in the network. These attacks are relatively easy to undertake, and on the other hand they can cause serious consequences on the network, even if encryption or authentication techniques are used in routing. The attacker can tunnel request packet RREQ directly to the destination without the increase of hop-count value. In this way it prevents all other routes from being discovered.

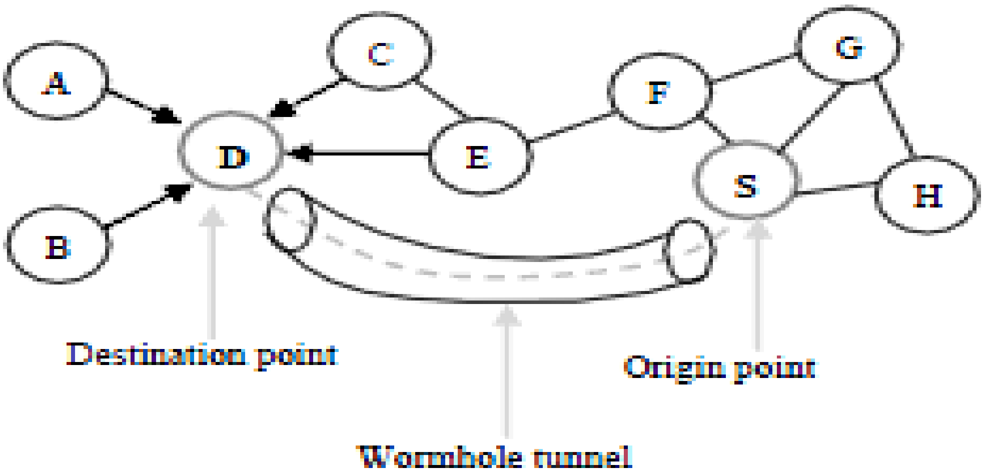

Fig.3-Wormhole Attack in a Network

Wormhole attack in reactive routing protocol is launched as shown in Figure 4[6], Node S, the source node wants to send packet to node D, the destination node. Node A1 and node A2 are two malicious nodes. The source node broadcasts an Route Request (RREQ) in order to find a route to destination node D. The neighbor node J and K receive and forwards the RREQ to its neighbors. The RREQ is then received by a malicious node A1 through node J. The malicious node A1 then records and tunnels the RREQ to another malicious node A2 through high speed tunnel. Malicious node A2 then rebroadcasts the RREQ which is later received by node P and then to the destination node D. As the RREQ through node P is received early at destination node D as compared to from node O, the destination node D choose the path from P i.e. D-P-J-S, to unicast the RREP to source S.

A single malicious node can launch this attack by broadcasting the route request at a high power level [7]. If multiple malicious nodes collude together to perform malicious acts, their activity of network disruption becomes even harder to detect. It creates an illusion that two remote nodes are immediate neighbors despite being located several hops away.

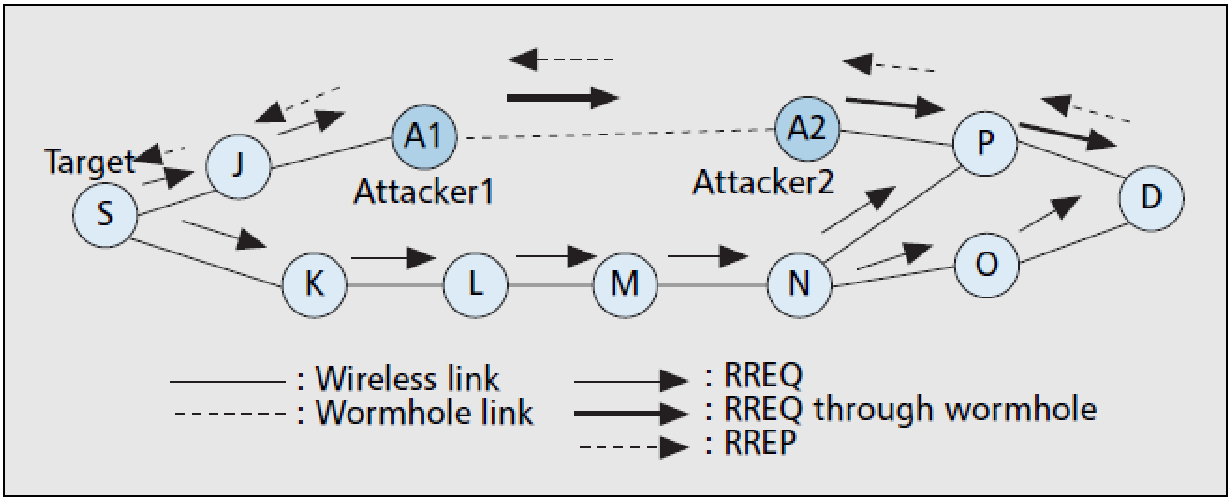

Fig.4- Wormhole Attack In Reactive Routing Protocol

*2.1- Classification of Wormhole Attack:* According to [8][9] wormhole attacks can be divided into two types:
1- In-band wormhole 2- Out-of-band wormhole attack.

An In-band wormhole does not use an external communication medium to develop the link between the colluding nodes but instead develops a covert overlay tunnel over the existing wireless medium. An in-band wormhole can be a preferred choice of attackers and can be potentially more harmful as it does not require any additional hardware infrastructure and consumes existing communication medium capacity for routing the tunnelled traffic, An Out-of-band wormhole, the colluder nodes establish a direct link between the two end-points of the wormhole tunnel in the network. This link is established using a wired link or a long-range wireless transmission. Due to the nature of wireless transmission, the attacker can create a wormhole even for packets not addressed to itself, since it can overhear them in wireless transmission and tunnel them to the colluding attacker at the opposite end of the wormhole. According to whether the attackers are visible on the route, the classification of the wormholes can be into three types [10] Closed Wormhole Attack, Half open Wormhole Attack, and Open Wormhole Attack.

In closed wormhole attack, the attackers do not modify the content of the packet, even the packet in a route discovery packet. Instead, they simply tunnel the packet form one side of wormhole to another side and it rebroadcast the packet.

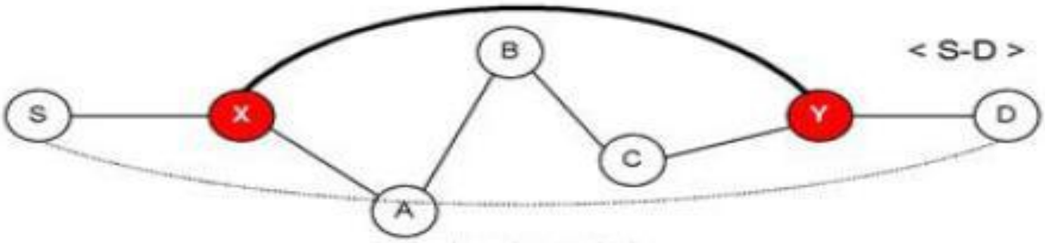

Fig.5-Closed Wormhole Attack

In half open wormhole attack, one side of wormhole does not modify the packet and only another side modifies the packet, following the route discovery procedure.

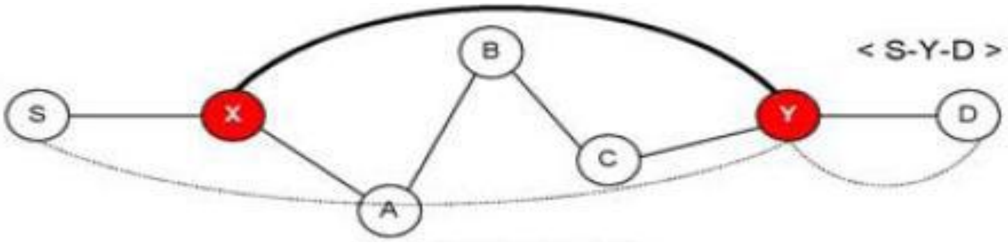

Fig.6-Half Open Wormhole Attack

In open wormhole attack, the attackers include themselves in the RREQ packet header following the route discovery procedure.

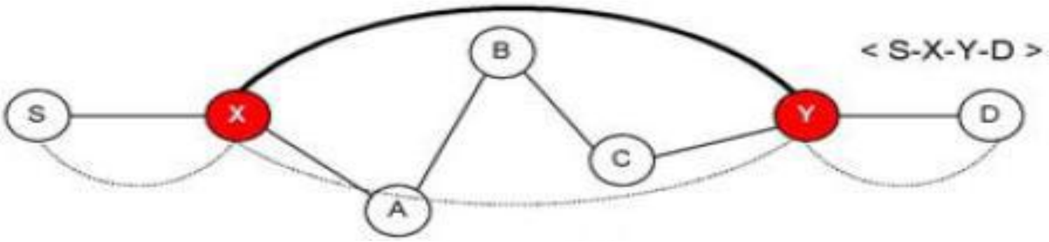

Fig.7-Open Wormhole Attack

Two different types of wormhole attacks have been discussed here: hidden wormhole attack and exposed wormhole attack [11] Hidden wormhole attack is the conventional wormhole attack in which the adversary records and replays packets. However, in hidden attacks, wormhole nodes do not update packets' headers as they should so other nodes do not realize the existence of them. This attack can be easily mounted using only hardware introduced by the attacker and without compromising any hosts in the network. In Exposed wormhole attack two end points are two compromised hosts. Then the adversary builds a virtual tunnel between the two compromised nodes. Wormholes are difficult to detect in MANET environment due to several reasons. The network is dynamic in terms of number of users, applications, their locations. Moreover devices are energy constrained with limited computing capability.

*2.2- Impact of Wormhole Attack:* Among various attacks, the wormhole is more dangerous as it does not exploit any node. The wormhole attack has significant impact on both type of routing protocols, i.e. proactive as well as reactive routing protocols. Once a wormhole is established, the attacker can get control of the routing traffic. The attacker can perform network disrupting operation such as packet dropping while results in low network throughput, eavesdropping and packet snooping. Though no harm is done if the wormhole is used properly for efficient relaying of packets, it puts the attacker in a powerful position compared to other nodes in the network, which the attacker could use in a manner that could compromise the security of the network.[12]

*2.3 -Metrics to detect Wormhole Attack:* To distinguish between different wormholes we need to have factors through which we can judge effect of a wormhole tunnel on a network here we will discuss about several metrics such as:

1-*Strength*: Strength is the number of end-to-end paths attracted by false link advertisements sent by the attacker. The larger the amount of attracted traffic, stronger can be the wormhole attack on the network traffic. The more is the number of traffic passing through the wormhole tunnel, the more effective is the wormhole attack.

2- *Difference between the advertised and actual path length*: If the advertised path has a path length of smaller number of hops as compared to that of actual path, this difference in the path length can be a useful metric to detect wormhole attack.
3- *Attraction*: This metric refers to the decrease in the path length offered by the wormhole. If the attraction is small then, the small improvements in normal path may reduce the strength of wormhole attack as the nodes may choose an alternative route that does not pass through the wormhole tunnel.
4-*Robustness*: Robustness of a wormhole refers to the ability of the wormhole to persist without significant decrease in the strength even in the presence of minor topology changes in the mobile ad-hoc network.
5- *Packet delivery ratio*: The Packet delivery ratio metrics refers to the ratio of total number of packets delivered to the total number of packed sent in the wireless network.

## III. Wormhole Attack Modes

1- *Wormhole attack using Encapsulation*: When the source node broadcast the RREQ packet, a malicious node which is at one part of the network receives the RREQ packet. It tunnels that packet to a second colluding party which is at a distant location near the destination, it then rebroadcasts the RREQ. The neighbors of the second colluding party receive the RREQ and drop any further legitimate requests that may arrive later on legitimate multi hop paths.

2-*Wormhole attack using out of band channel*: This channel can be achieved, by using a long range directional wireless link or a direct wired link.

3- *Wormhole attack using high transmission power*: Another method is the use of high power transmission. In this mode, when a single malicious node gets a RREQ, it broadcasts the request at a high power level, a capability which is not available to other nodes in the network. Any node that hears the high-power broadcast rebroadcasts it towards the destination.

4- *Wormhole attack using packet relay*: In this mode a malicious node relays packets between two distant nodes to convince them that they are neighbors.

5- *Wormhole attack using protocol deviation*: During the route request forwarding, the nodes typically back off for a random amount of time before forwarding. A malicious node can create a wormhole by simply not complying with the protocol and broadcasting without backing off. The advantage of this mode is that the control packet arrive faster, the challenge for this mode is that there is a possibility of collision to occur between transmissions of malicious nodes.

## IV. WORMHOLE DETETCION AND PREVENTION TECHNIQUES

Several works has been proposed to address the problem of wormhole attack by detecting, preventing or mitigating the wormhole attack in MANET, various detection strategies proposed and classified here:
1) Distance and location based solution
2) Special Hardware Based Approaches
3) Topology Based Solution
4) Hop Count and Delay Based Solutions
5) Synchronized Clock Based Solution
6) key based solution
7) Neighbor-Based solutions

Packet leashes and statistical based detection based methods are types of neighbor validation schemes, while end-to-end detection schemes detect wormhole based on round trip time (RTT), Hop count analysis (HC), frequency of nodes appearance in the route or location of the nodes. The neighborhood validation schemes are useful to detect Hidden mode wormhole attack while end-to-end scheme is useful to detect Participation mode wormhole attack [13] Most of the proposed wormhole solutions in the literature are based on location or time. A packet leash [14] is type of neighbor validation scheme. It is a mechanism to detect and defend the wormhole attack by restricting the time that packets can be transferred. There are two types of packets leashes: Temporal packet leash and geographic packet leash. The main idea is that by authenticating either an extremely precise timestamp or location information combined with a loose timestamp, a receiver can determine if the packet has traversed an unrealistic distance for the specific network technology used. In temporal leashes [14] each node based on the speed of light calculates the packet expiration time and appends it to the packet to restrict the packet from travelling further than a specific distance. The expiration of packet is checked by the receiver by comparing the current time and expiration time in the packet. A temporal leash requires tight clock synchronization and does not rely on GPS technology. In geographical leash[15] in which the sender inserts its own position and sending time into the packet, the receiver will estimate the maximum distance between the sender and itself based on its own position and receiving time. If the distance exceeds the transmission range, the packet will be discarded. Geographic leashes the nodes need not be tightly synchronized and reply on accurate measurement of GPS technology.

FEEPVR (First end-to-end protocol to secure Ad Hoc Networks with Variable range) [16] detects wormhole node based on the number of hops and location information. A path is suspected of wormhole if the number of hop count for a route is less than the minimum lower bound.

SEEEP (Simple and Efficient End –to –End protocol) [12] is a simple algorithm to secure ad hoc networks against wormhole attack based on the measurement of length of path between source and destination d and the communication range r. packet from source to destination must travel at least [d/r] hops [12] It does not require tight synchronization and has low computation and storage overhead.

DELPHI [17] (Delay Per Hop Indication) is based on the calculation of (delay/hop) value of disjoint paths. It is based on the fact that under normal condition, the delay a packet experiences in propagating one hop should be similar along each hop path, while in case of wormhole attack, the delay for propagating across false neighbors are high as there are many hops between them. It works for both I-B and O-B mode.

TTM [18] is a transmission time based approach based on the idea of calculating RTT (Round Trip Time) between two successive nodes in the network during route setup procedure. It is based on the fact that the transmission time between two malicious nodes is considerably higher than the normal nodes in the network which are within radio range of each other. MHA [21] (Multi- Hop Count Analysis) scheme is based on the hop count analysis to detect the wormhole attack. It examines the hop count values of all the routes and sets a set of safe route for data transmission .It is assumed that too low or too high hop-count is not healthy for the network.

WARP (Wormhole Avoidance Routing Protocol) [19] is based on anomaly detection technique to detect wormhole. It takes into consideration multiple link-disjoint paths but use only one path to transmit data packet. It enables the neighbors of wormhole nodes to discover that the wormhole nodes have abnormal path attractions. transmit data packet. It enables the neighbors of wormhole nodes to discover that the wormhole nodes have abnormal path attractions. As compared to other techniques, it achieves degradation in packet loss without any additional hardware support.[19]. It works for both I-B and O-B wormhole modes.

Mahajan et al [20] proposed some proposals to detect wormhole attacks like:
1) The abrupt decrease in the path lengths can be used as a possible symptom of the wormhole attack.
2) With the available advertised path information, if the end-to-end path delay for a path cannot be explained by the sum of hop delays of the hops present on its advertised path, existence of wormhole can be suspected.
3) Some of the paths may not follow the advertised false link, yet they may use some nodes involved in the wormhole attack. This will lead to an increase in hop delay due to wormhole traffic and subsequently an increase in end-to-end delay on the path.

In [22] A.Vani et al. proposed 3 different methods for Detection scheme has three techniques based on hop count, decision anomaly, neighbor list count methods are combined to detect and isolate wormhole attacks in ad hoc networks. That manages how the nodes are going to behave and which to route the packets in secured way. Hybrid routing algorithm is used to provide the common solution to three different techniques. This protocol is based on On-demand ad hoc routing protocol (AODV).In hop count based method one hop neighbors are calculated

Directional antennas [23] were also used to prevent the Wormhole attack. To ruin the wormhole, each node shares a secret key with every other node and maintains an updated list of its neighbors. To discover its neighbors, a node, called the announcer, uses its directional antenna to broadcast a HELLO message in every direction. Each node that hears the HELLO message sends its identity and an encrypted message, containing the identity of the announcer and a random challenge nonce, back to the announcer. Before the announcer adds the responder to its neighbor list, it verifies the message authentication using the shared key, and that it heard the message in the opposite directional antenna to that reported by the neighbor.

## V .CONCLUSION

In this paper, we introduced the wormhole attack along with its classification Various methods and techniques used for the detection and prevention of wormhole attack along with their advantages and drawbacks are also discussed. Wormhole attack is one of the major security concern of Mobile Ad Hoc Network as it disrupts the routing protocols by creating false routing paths during route discovery process by capturing and forwarding the packet from one location in the network to the other using high speed tunnel. The existing system on wormhole attack detection is either based on neighbor validation or end-to-end detection. But most of the existing techniques either has high computational complexity or need hardware or tight time synchronizations or is applicable only to specific wormhole detection modes. Wormhole attacks are severe attacks that can easily be launched even in networks with confidentiality and authenticity.

## REFERENCES

[1] C. Siva Ram Murthy & B.S Manoj, “Mobile Ad Hoc Networks- Architectures & Protocols” Pearson Education, New Delhi, 2004 .
[2] G. Carofiglio, C.-F. Chiasserini, M. Garettoy, and E. Leonard, “Route Stability in MANETs under the Random Direction Mobility Model”, International Journal of Engineering, 1(9), 2003.
[3] IRTF RRG Ad hoc Network Scaling Research Subgroup http://w3.antd.nist.gov/wctg/manet/adhoclinks.html
[4] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester, “An Overview of Mobile Ad Hoc Networks: Applications and Challenges” in 2005.

[5] Y.-C. Hu, A. Perrig, D. B. Johnson, "Wormhole Attacks in Wireless Networks, Selected Areas of Communications," in IEEE Journal on, vol. 24, no. 2, pp.370-380, 2006.

[6] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, Nei Kato, Tohoku University and Abbas Jamalipour, University of Sydney, "A Survey of Routing Attacks in Mobile Ad Hc Networks", Security in Wireless Mobile Ad Hoc Networks and Wireless Sensors, IEEE Wireless Communications, October 2007 .

[7] Gupta N, Khurana S,"SEEEP: Simple and Efficient End-to-End Protocol to Secure AdhocNetworks Against Wormhole Attacks", Proceedings of the 4th International Conference on Wireless and Mobile Communications (ICWMC'08); Athens, Greece. 27 July–1 August 2008; pp. 13–18."

[8] Viren Mahajan, Maitreya Natu, and Adarshpal Sethi: "ANALYSIS OF WORMHOLE INTRUSION ATTACKS IN MANETS" IEEE Military Communications Conference (MILCOM), 2008.

[9] Reshmi Maulik and Nanbendu Chaki: "A Study on Wormhole Attacks in MANET" International Journal of Computer Information System and Industrial Management Applications (IJCISIM), Vol.3 (2011), pp. 271-279.

[10] W. Wang, B. Bhargava, Y. Lu, and X. Wu, "Defending Against Wormhole Attacks in Mobile Ad Hoc Networks", Wiley Journal on Wireless Communications and Mobile Computing, vol. 5, pp. 1-21, 2005.

[11] Xia Wang and Hjony Wong: "An End to End Detection of Wormhole Attack in Wireless Ad-hoc Network" International Conference of computer Software and Applications, Vol.3 (2007), pp. 271-279.12-

[12] Gupta N., Khurana S., "SEEEP: Simple and Efficient End-to-End Protocol to Secure Ad-hoc Networks Against Wormhole Attacks", Proceedings of the 4th International Conference on Wireless and Mobile Communications (ICWMC'08); Athens, Greece. 27 July–1 August 2008; pp. 13–18."

[13] Jonny Karlsson, Laurence S. Dooley and Göran Pulkkis, "Identifying Time Measurement Tampering in the Traversal Time and Hop Count Analysis (TTHCA) Wormhole Detection Algorithm ", Sensors 2013.

[14] Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Packet Leashes: A Defence against Wormhole Attacks in Wireless Ad Hoc Networks", IEEE 2003.

[15] Ankita Gupta, Sanjay Prakash Ranga, "WORMHOLE DETECTION METHODS IN MANET", IJECBS INDIA, Vol. 2 Issue 2 July 2012.

[16] Khurana S., Gupta N,"FEEPVR: First End-to-End Protocol to Secure Ad hocNetworks with Variable Ranges Against Wormhole Attacks", Proceedings of the 2nd International Conference on Emerging Security Information; Cap Esterel, France. 25–31 August 2008; pp. 74–79.

[17] Chiu H.S., Lui K.-S. "DelPHI: Wormhole Detection Mechanism for Ad hocWireless Networks", Proceedings of the 1st International Symposium on Wireless Pervasive Computing; Phuket, Thailand. 16–18 January 2006.

[18] Phuong Van Tran1, Le Xuan Hung1, Young-Koo Lee1, Sung, Young Lee1, and Heejo Lee2, "TTM: An Efficient Mechansim to Detect Wormhole Attacks in Wireless Ad-Hoc Networks".

[19] Ming-Yang Su, "WARP:A Wormhole avoidance routing protocol by anamoly detetction mobile ad hoc networks", Miang Chuan Univeristy, Taiwan, Elsevier, 2009.

[20] V. Mahajan, M. Natu, A. Sethi. "Analysis of wormhole intrusion attacks in MANETS". In IEEE Military Communications Conference (MILCOM), pp. 1-7, 2008.

[21] Shang-Ming Jen, Chi-Sung Laih, Wen-Chung Kuo. "A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET", 9 (6), pp. 5022-5039, 2009.

[22] A.VANI , D.Sreenivasa Rao "An Algorithm For Detection And Removal Of Wormhole Attack for Secure Routing in Ad hoc Wireless Networks" International science And Engineering in 2007.

[23] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole attacks," in Network and Distributed System Security Symposium, 2