An Assessment of Worm Hole attack over Mobile Ad-Hoc Network as serious threats

Vikas Kumar Upadhyay
Department of Computer Science & Engineering,
Sagar Institute of Research and Technology, Bhopal-462001
Email: erupadhyayvikas2010@gmail.com
Rajesh Shukla
HOD, Department of Computer Science & Engineering, SIRT, Bhopal-462001
Email: rkumardmh@gmail.com

ABSTRACT

Now these day Mobile Ad hoc networks vulnerable from number of security threats like black hole attack, DOS attack, Byzantine attack and wormhole attack. Wormhole attack is one of most important attack and having great attention in recent year. Wormhole attack, demonstrate a illusion over the network that show two far away node to be an neighbor node and attracted all traffic by presenting an greediness of shortest path over the network. This paper presents a bird eye over different existing wormhole deduction mechanism and their problem.

Keywords - Mobile Ad hoc Network, Selfish node, Malicious node, AODV

Date of Submission: 15, July 2013 Date of Acceptance: August 28, 2013

INTRODUCTION

Mobile ad hoc network [1] is infrastructure less network that self-configured automatically by mobile nodes without the help of any centralized management. In MANET nodes having special characteristics that each node in MANET behaves like receiver and transmitter and allow communicating with other nodes in its radio range. In order for a node to forward a packet to a node that is out of its radio range, the support of other nodes in the network is needed; this is known as multi-hop communication [2]. Therefore, each node must act as both a host and a router at the same time. The network topology normally changes due to the mobility of mobile nodes in the network.

In MANET each node can communicate with the help of its neighbor node that's comes in its radio range each node forward their packet to their neighbor node towards destination where path for transmitting massage packet is suggested by routing protocol as shortest path.

Every routing protocol concentrates over shortest path where some malicious node over network use this greediness of routing protocol and present an illusion of shortest path between two end point of network and attack major traffic over the network.

Wormhole attack attract massage packet and play number of misbehave with that routing packet like scanning of confidential message, drop, corrupt and change transmitted massage over network.

Figure 1 show the view of MANET where dashes line shows radio range of node. Where, each node makes a direct communication with their neighbor node that comes under its radio range. And each node has the capability of routing. So there is no need of any centralized device.

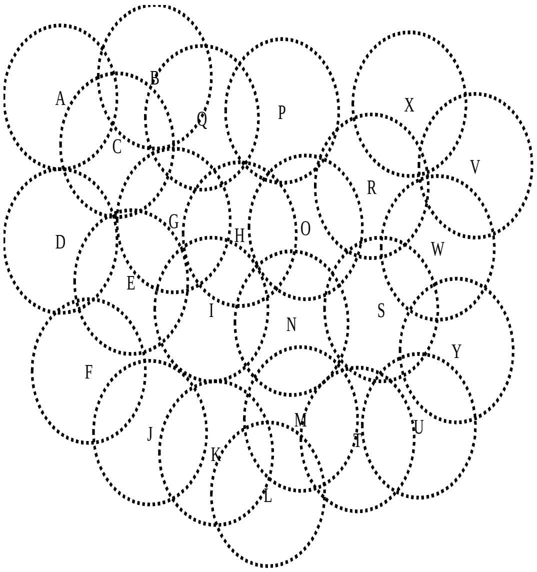

Figure 1: Mobile Ad-Hock Network

NETWORK & ITS CLASSIFICATION

In computer science network is a means of communication. Here more than one computer can connect with a connecting media and a protocol. This connection follows some structure which is known as the topology.

Basically the computer network has been using for the data communication from source to destination. As the time increases the technology also has increased. Initially there was the only way to connect the computers using the cable. But now there are other ways also available.

Advantages of Network

There are many advantages of network in the daily routine. But the most important facts are discussed here.

- Facility of communications
- Shearing Hardware
- Shearing data and information
- Shearing software

Apart from these advantages it also reduces to cost for the future. The communication with other make easy.

Classification of Network

Network is collection of nodes connected with networking devices and any connecting element. There are many types of network. Some of them discuss below.

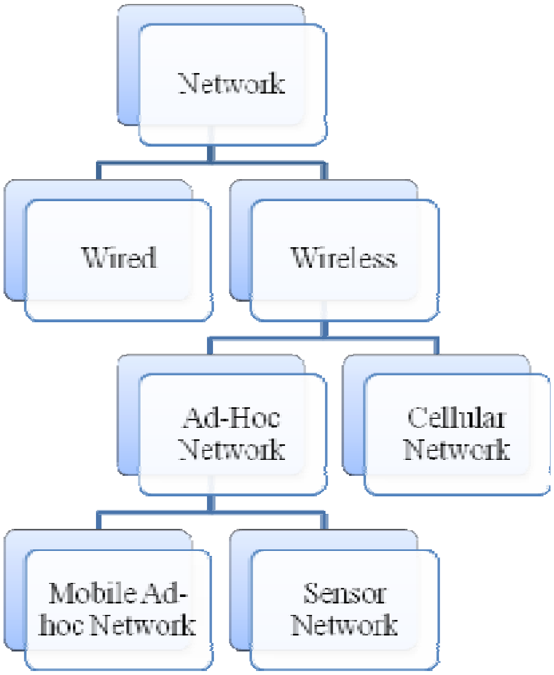

Figure2: Classification of Computer Network

The above figure shows the classification of computer network. This classification is specially based on the connecting media used by the network. Most of the time, the wired network has used in the commercial or home purposes.

The wireless network doesn't use any cable for the communication. This type of network always uses the some radio frequency as a connecting media. The greater mobility of wireless LANs helps offset the performance disadvantage. Mobile computers do not need to be tied to an Ethernet cable and can roam freely within the WLAN range.

The mobile ad-hoc network is the most popular in these days due to its flexibility.

MOBILE AD-HOC NETWORK

A mobile ad hoc network (MANETs) is a complex network which is a combination of self configured nodes. It is a type of wireless network. The arrangement of node is temporary so that it is called the Ad-hoc.

MANET is combination of node having the capability of processing the data to communicate. There is no static topology has used. The topology is dynamically changed every time. A mobile ad hoc network (MANET), sometimes called a mobile mesh network.

Figure3: Mobile Ad-Hoc Network

Each device in a MANET can freely and independently move in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic.

MANETs has the fowling issues, such as:

- Weaker in Security
- Device size limitation
- Battery life
- Dynamic topology
- Bandwidth and slower data transfer rate

Advantages of MANET

- **Wireless communication:** They provide access to information and services regardless of geographic position.
- **Mobility:** This is a type of wireless network so that the mobility is an important feature of this approach.
- **Infrastructure less:** These networks can be set up at any place and time. This type of network always uses the dynamic topology approach. These networks work without any pre-existing infrastructure.
- **Equipments:** In this network small and light equipments are used for the communication.

Disadvantages of MANET

- **Limited Resources:** In this network limited resource are used. Due to Limited resource invokes the problem of limited security.
- **Authorization Required:** the authentication is a necessary point to secure this network. Intrinsic mutual trust is vulnerable to attacks
- **Dynamic Topology:** Due to Dynamic, Volatile, and changeable topology node can move anywhere in the network. This makes hard to detect malicious nodes in the network.
- **Protocols:** the protocol which has already written for the wired network doesn't work in Mobile ad-Hoc Network. So that this is a constraint that we have to write to new protocols for mobile ad-hoc network.

Applications of MANET

As far as the wireless network is concert there are many applications of MANET. There are some applications like military, collaborative computing, emergency rescue, mesh network, wireless sensor network, multi-hop cellular network, wireless community network etc.

- **Military Battlefield:** Most of the time there is need to install the network on the spot but it is hard using the wired network. Its best solution is the mobile ad-hoc network. It is very easy to install at the moment.
- **MANET as a Commercial Purpose:** Now these days MANET is also used in Commercial places. As far as commercial purpose is consent it involves Ship to ship communication, Police department or the private security force in order to make people adherence of law.
- **Natural Digester:** when the natural digester take place then there is need to establish the network for the communication. This can install in small area at any time. These emergencies are may be like earthquake, heavy rainfall, flood, Sunami, Land Slide, fire etc. in such type of scenario most of the time it seems to be that the communication system plays an important role. But due to such type of digesters the infrastructure of communication system will fail. At that time there is need to use such sort of technology which is infrastructure less and less time consuming in installation. MANET is the best option in these conditions.
- **Local Level:** MANET has the ability of connecting itself to the multimedia network with the help of small computers like notebook computers or palmtop computers. These computers are using this facility in order to share the information among all other members of the local network.
- **Personal Area Network (PAN):** PAN is basically installed in limited area. So there is a need of short range of signals. MANET has the Short-range of signal which satisfied the intercommunication between small devices and mobile devices. It is very simple to install this network between cell phone, laptops, ear phones, wrist watches etc.

ATTACK IN MANET

MANET is vulnerable to various types of attacks. Some attacks affect to general network, some affect to wireless network, and some are particular to MANETs. These security attacks can be classified according to different criteria, such as the domain of the attackers, or the techniques used in attacks [3]. These security attacks in MANET and all other networks can be generally classified by the following criteria: passive or active, internal or external, different protocol layer, stealthy or non-stealthy, cryptography or non-cryptography related.

Attacks	Description
Passive Attack	This attack happened without the interrupting in the communication operations.
Active Attack	In this attack the node works as active node. It can perform the operations like interruption, modification, or fabrication, at the time of attack directly.
Internal Attack	Here nodes are the part of network in order to perform attack.
External Attack	Here nodes does not belong the network in order to perform attack.
Black hole Attack	A malicious user broadcast the message having the false information of shortest path. This shortest path is work for the attack.

Byzantine attack	In this attack node participates alone in the network. Some time it also makes the set of intermediate nodes and works as an attacker. The operation can perform like routing loops and forwarding packets dropping packets. It will degrade the quality of services.
Malicious code attacks	This attack can perform in the form of viruses, worms, spywares, and Trojan Horses in order to harm the operating systems and user applications as well.
Wormhole attacks	Here two nodes link together to make a tunnel. Using this tunnel it gives the illusion of shortest path and also able to bypass the other nodes of the network.

SECURITY CONSTRAINTS

Mobile Ad-Hoc network has several loop holes by which the attack in MANET is possible. This attack can do by any node of the network. These nodes itself take part in the malicious actions. This type of nodes called the active node and attack is known as active attack. On other hand some nodes do not involve in the malicious activity directly. This type of action is done by the passive node in passive attack. In both cases such type of node called the malicious node. In Mobile ad-hoc network there are some major concerns in order to secure the network. There all security should be applied in the province of data. These are the principle of network security [7,17].

Authentication: It is based on the right access of a user. In ad-hoc network there may be various anonymous user with the existing users. Which one is authorized to communication? This answer will find out by the authentication policies.

Confidentially: In this concept the message should only know to sender and receiver. None of the nodes have the information regarding the transmitting message.

Integrity: this concept ensures that the message hasn't any changes during the transmission in the network.

Availability: this is necessary for the sender's end. It shows the receiver is online or not.

Non-repudiation: it is concept to prevent the repudiation of message [7,8].

PROTOCOLS USED IN MANET

As the Mobile ad-hoc network in a wireless protocol so there is a need to use those protocol which can work in wireless environments. There are various wireless protocol has been developed. Routing protocol is a collection of rules to route the packet in the network. This route should be suitable to get the path of destination node. The Routing protocols are responsible to perform dynamic routing and information sharing as well.

Table Driven Protocol

In this type approach the protocol will store the table in order to get the route of destination. With the help of that table the route will decides and forward the packet to the destination node. There are many table driven protocol has developed like DSDV, WRP etc. this approach is also known as the proactive protocols.

On Demand Protocols

This is another approach to route the packet in the wireless network. This approach does not have any pre decided route. This approach works on the basis of current status of request.

Hybrid Protocol

This approach is used the combination of both protocols.

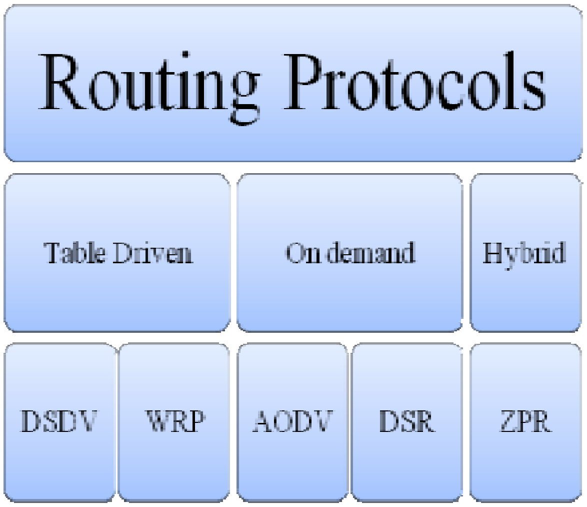

Figure4: Hierarchy of protocols

RELATED WORK

In recent year number of technique have been proposed for the wormhole detection that can be comes under the various category, In [1] Pallavi present an multi-hop count analysis (MHA) scheme for wormhole detection where digital signature is responsible for check the validity of any legitimate nodes over network .In MHA for authentication of selected path, MHA used verification of digital signature of all sending node by receiving node. If there is no malicious node between the paths from source to destination, then source node creates a path for secure data transfer. Whereas M.Nouri present an

IDS technique for wormhole detection[4] where decision is taking on the basis of voting , every trusted node make a participate in voting of suspect node and sending node decide which suspect node is malicious node on the basis of crusting technique. In [4] all decision is based on a value of K (threshold) if vote percentile is greater than k then suspect node is malicious but validation of k is not up to mark. Marianne [5] present a cost based scheme for wormhole avoidance scheme if any node (x) offer shortest path for any relative node (r) then cost of (x) has been increase gradually once node (x) cross threshold limit of cost node x has been avoided for route on the basis of theory that x try to attack network traffic, but this scheme not very help full for closed wormhole.

In [6]Author presented the design and performance analysis of a novel, efficient protocol, called TIK, In particular, a node needs to perform only between 3 and 6 hash function evaluations per time interval to maintain up-to-date key information for itself, and roughly 30 hash functions for each received packet. When used in conjunction with precise timestamps and tight clock synchronization, TIK can prevent wormhole attacks that cause the signal to travel a distance longer than the nominal range of the radio [6]. And wireless MAN technology could be sufficiently time-synchronized using either GPS or LORAN-C radio signals.

Mobile Ad Hoc Networks (MANETs) one of the most harmful attacks in MANETs, the wormhole attack remains a sizable challenge [12]. It seems to be that the number of wormhole detection technique depends on the specific hardware like GPS, different types of antennas etc. using these equipments the efficiency of detection in not up to the mark. To improve the performance of these detection techniques the author proposed a new approach using signal processing. This approach helps to detect the wormhole quickly and accurately. In this approach there is no need to any specialized hardware support. The simulation has done in the testbed.

One of the typical routing methods in MANET is on-demand routing approach [13]. In which routing is performed on the basis of current scenario. In this paper the author presents a new approach using Bayesian approach. The major issue in such a protocol is the route establishment cost. The author suggesting an efficient routing algorithm for mobile ad-hoc networks with a route establishment technique using Bayesian approach. The results shows that the delivery ratio, control packets overhead are batter in this approach.

WORM HOLE ATTACKS

Wormhole attack is serious threats in MANET, its attack the traffic of network and either scan, change or drops the entire confidential message inside the packet in the time of journey of packet over the wormhole tunnel. As shows in figure 5 in wormhole attack two malicious nodes of different network link together via some physical connection and form a tunnel and present an illusion[9] that node A of network X is neighbor of node B of network Y. Generally wormhole puts their malicious nodes at powerful position within the network as compared to other nodes so its attack maximum traffic of network and prevents other routes instead of the wormhole from being discovered, and thus creates a permanent Denial-of-Service attack by dropping all the data, or selectively discarding or modifying certain packets as needed [7].

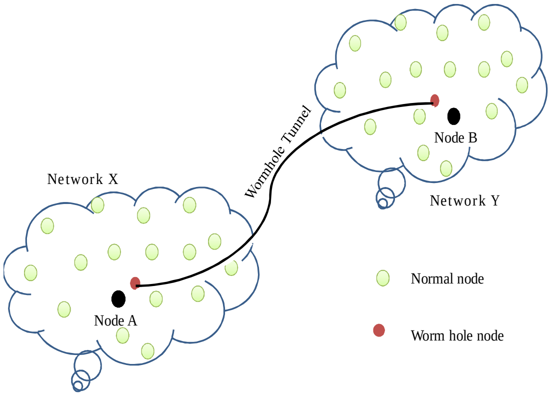

Figure 5: Worm Hole

ORGANIZATION OF WORMHOLE ATTACK

Wormhole attacks are organized in three different type namely closed, half open and open on the basis visibility of malicious node[10] in the route discover by routing protocol.

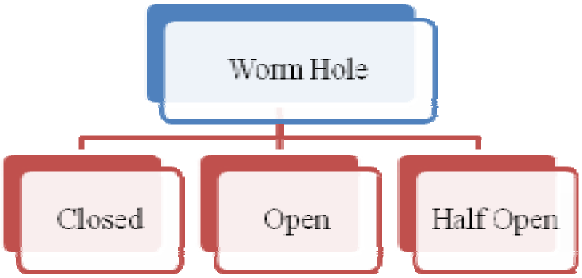

Figure 6: Classification of Wormhole Attack

As show in figure 5 consider two nodes of different network behave like end point of worm hole tunnel, and try to attack entire traffic of network.

Closed Wormhole: - Route discover by AODV is suffer from closed wormhole if both end point of wormhole tunnel not participate in hop count of route ie both the end point of wormhole tunnel hide them self as show in figure 7 and source node analysis destination node as their neighbor node[9].

Open Wormhole: - Where as in open worm hole attack both end point of wormhole tunnel consider in counting of hop count as show in figure 9 both end of wormhole tunnel participate in route suggested by routing protocol. .

Half Open Wormhole:-In half open wormhole only one of either end of wormhole tunnel participates in route hop count as show in figure 8 [8].

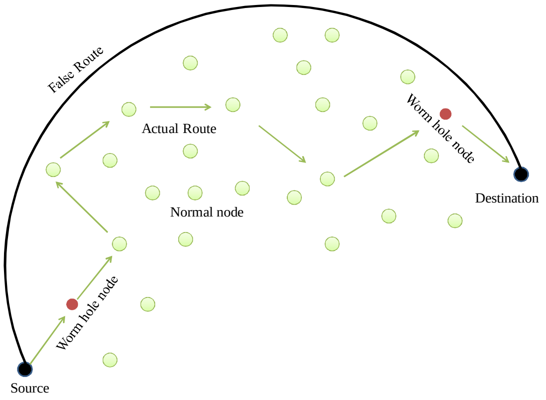

Figure 7: Closed Worm Hole

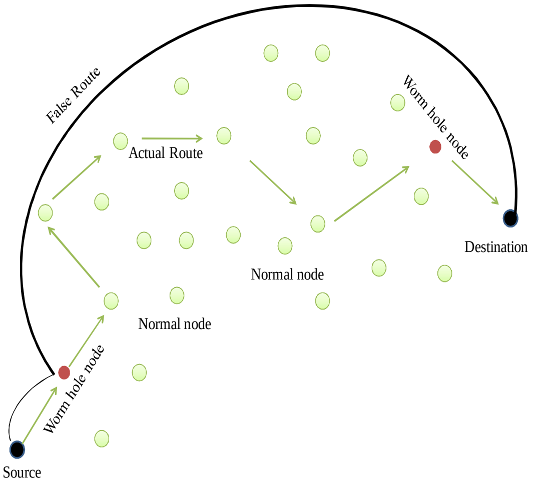

Figure 8: Half Open Worm Hole

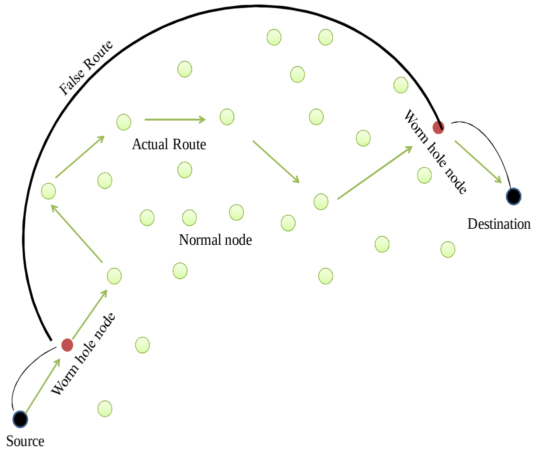

Figure 9: Open Worm Hole

SIDE EFFECT OF WORMHOLE ATTACK

Ad-hoc Network can install in three basic environments. 1) Open Environment 2) Localized Environment and 3) Organized Environment. Every node of Ad-hoc network exists in one of the above Environment. It seems to be that each Environment has its own security issues. These security issues leave some loop holes to attack in the Ad-hoc Environment. The figure 10 shows the various types effect over mobile ad-hoc network after wormhole attack [9,10, 11].

Modification: this type of attack use to customize the routing message. Here one malicious node will change the packet data during the forwarding that message. Here data or message will lose their integrity.

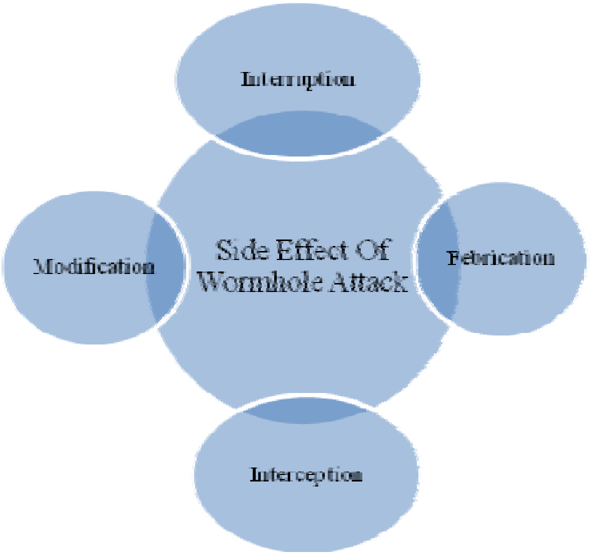

Figure 10: Effect of Wormhole Attack over Network Packet

Interception: this type of attack done by the unauthorized user. They show their self as a part of network but they are the malicious node. When they receive the packet of the network they can modify it and forward to next node. The malicious node can able to analyse the data of the packet. In this case the data integrity and confidentiality will lose.

Fabrication: Data modification is not only called the attack. Unused, unwanted packet generation is also comes under the attack. This is known as fabrication attack. Here the malicious node create the large number of packets and send it into the network. When the number of packets goes over the capacity of network then network will fail. Sometime this activity has done by the internal nodes of the network. These nodes are called as misbehaving nodes.

Interruption: In this type of attack the malicious node will prevent the message to receive by the destination node.

WORMHOLE DETECTION TECHNIQUE

There are many solutions to detect the wormhole but Most of them are based on location and time. Some of location and time based solutions are given below.

- Packet Leashes
- Using Directional Antennas

Packet Leashes: A leash is any information that is added to a packet designed to restrict the packet's maximum allowed transmission distance [11]. There are two types of packet leashes available. Geographical and temporal are the major types [4]. Packet leashing is mostly use to add in each packet on each link in order to restrict the transmission distance of the packet.

A) Location and Time Based Solutions

In recent year many of wormhole detection technique based on location and time based scheme where decision will taken on the basis of location and time information of node.he introduction of the paper should explain the nature of the problem, previous work, purpose, and the contribution of the paper. The contents of each section may be provided to understand easily about the paper

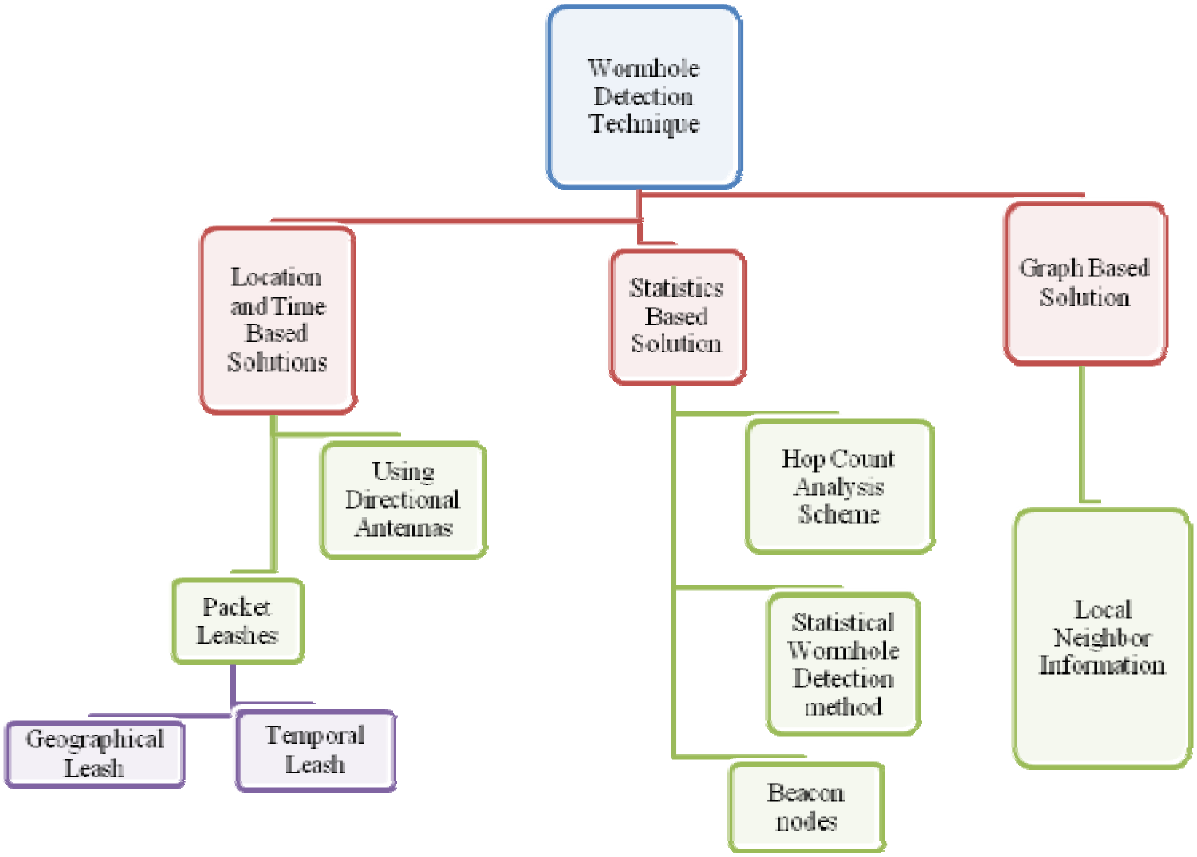
Wormhole Detection Technique
Location and Time Based Solutions
Statistics Based Solution
Graph Based Solution
Using Directional Antennas
Packet Leashes
Geographical Leash
Temporal Leash
Hop Count Analysis Scheme
Statistical Wormhole Detection method
Beacon nodes
Local Neighbor Information

Figure 11: Various Detection Technique of Wormhole

. Mostly in directional antenna and packet latch technique based on location and time based.

- **Packet Leashes:** Packet leashes scheme authenticate wormhole timestamp and location information that can transmitted by each node for each packet about the practical distance between two node for this type of authentication packet lashes scheme use two different packet namely [14] Geographical leash packet and temporal leash packet that can encapsulate as header to each packet for restricting the transmission distance of packet.
- **Using Directional Antennas:** This method used an special hardware called directional antenna at each mobile nodes antennas to defend against wormholes and maintain an directional scheme ie sender node sends packets in a given direction and receiver packet will get that packet from the opposite direction whole communication will performed only when the directions of both pairs match, the neighboring relation is confirmed [15]. This approach work only when system has only two end points does not prevent multiple endpoint attacks. Directional errors are possible.

B) Statistics Based Solution

Statistics based solutions for wormhole detection based on numerical facts collected from network structure. Statistics scheme is subdivide namely into Beacon nodes and Hop Count Analysis Scheme.

- **Beacon Nodes scheme**: Beacon node scheme based on a special type of node ie Beacon Node that's behave like wormhole detector. Beacon node generate alarm message to each of base station if its catch a wormhole node within their range [16]. Main disadvantage of beacon node scheme that its use GPS system to find location of another beacon node.
- **Hop Count Analysis Scheme** This method selects routes and "avoids" rather than "identify" the wormhole. This method first examines the hop-count values of all routes. Then they choose a safe set of routes for data transmission[17].

C) Graph Based Solution

Graph based scheme based on graph theories, where graph are used to detect wormhole in network. Neighbour node information scheme is one of graph theory based solutions.

- **Neighbour node information scheme** Threshold value selection is most important in this method. But algorithm does not provide optimal way to select threshold value. Overhead in each node is high[18]. This algorithm could not find wormhole, when multiple wormholes are in network.

XII. Conclusion and future scope

This paper is gives the detail about MANET. it also throw some light on the security constraints of MANET. This paper presented and discussed various security issues, attack and threats of mobile ad-hoc network. It also explains selfish node behaviors along with wormhole attack. It seem to be that the worm hole attack very harmful so there is huge need to identify the warm hole in the network. In future we plan to continue our work in field of secure routing over MANETs & wormhole detection and prevention technique which are present in the network in order to enhance the security of MANETs.

References

[1] Pallavi Sharma, Prof. Aditya Trivedi "An Approach to Defend Against Wormhole Attack in Ad Hoc Network Using Digital Signature" in IEEE ,2011

[2] Sebastian Terence J "Secure Route Discovery against Wormhole Attacks in Sensor Networks using Mobile Agents" in IEEE 2011

[3] Sanjay Kumar Dhurandher, Isaac Woungang , "E2SIW: An Energy Efficient Scheme Immune to Wormhole Attacks in Wireless Ad Hoc Networks" *26th International Conference on Advanced Information Networking and Applications* Workshops IEEE 2012.

[4] Mahdi Nouri, Somayeh Abazari Aghdam, Sajjad Abazari Aghdam "Collaborative Techniques for Detecting Wormhole Attack in MANETs" in *International Conference on Research and Innovation in Information Systems (ICRIIS),* 2011 ,IEEE

[5] Mariannne. A. Azer "Wormhole Attacks Mitigation" in *Sixth International Conference on Availability, Reliability and Security* ,2011,IEEE

[6] Katrin Hoeper and Guang Gong, "Pre-Authentication and Authentication Models in Ad Hoc Networks", Wireless Network Security Signals and Communication Technology, Springer, 2007

[7] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, "Wormhole Attacks in Wireless Networks" University of Illinois, Carnegie Mellon University, Rice University

[8] W. Wang, B. Bhargava, Y. Lu, and X. Wu, "Defending against wormhole attacks in mobile ad hoc networks: Research articles", *Wireless Communication Mobile Computing,* vol. 6, no. 4, pp. 483–503, ACM,2006.

[9] Ali Modirkhazeni , Saeedeh Aghamahmoodi , Arsalan Modirkhazeni , Naghmeh Niknejad "Distributed Approach to Mitigate Wormhole Attack in Wireless Sensor Networks" in *7th International*

Conference on Networked Computing (INC),IEEE,2011

[10] Ronggong song, Peter c. Mason, Ming li "Enhancement of frequency-based wormhole attack detection" in *Military Communications Conference*, 2011 - milcom ,IEEE 2011.

[11] Yih-Chun Hu, Adrian Perrig and David B. Johnson "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks" IEEE 2003.

[12] Ronggong Song, Peter C. Mason and Ming Li, "Enhancement of Frequency-based Wormhole Attack Detection", IEEE 2011, pp 1139-1145.

[13] Rusheel Jain, Murali Parameswaran and Chittaranjan Hota, "An Efficient on Demand Routing Protoco for MANETs using Bayesian Approach", IEEE 2011.

[14] Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks" IEEE, 2003.

[15] Hu, D. Evans, "Using directional antennas to prevent wormhole attacks", in Proceedings of the IEEE *Symposium on Network and Distributed System Security (NDSS)*, 2004.

[16] Marianne A. Azer, Sherif M. El-Kassas, Abdel Wahab F. Hassan, Magdy S. EI-Soudani "Intrusion Detection for Wormhole Attacks in Ad hoc Networks a Survey Proposed Decentralize scheme", in Proceeding of Third International Conference on Availability, Reliability and Security of the IEEE Computer and Communications Socieities, 2008.

[17] He Ronghui, Ma Guoqing, Wang Chunlei, and Fang Lan" Detecting and Locating Wormhole Attacks in Wireless Sensor Networks Using Beacon Nodes", World Academy of Science, Engineering and Technology, 55,2009.

[18] Shang-Ming Jen, Chi-Sung Laih and Wen-Chung Kuo" A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET" Sensors 2009, 9, 5022-5039, 2009.