An Efficient Approach for Detection of Wormhole Attack in Mobile Ad-hoc Network

Shivangi Dwivedi
Dept of Computer Engg & Application
National Institute of Technical Teacher's Training and Research
Bhopal, India

Priyanka Tripathi
Dept of Computer Engg & Application
National Institute of Technical Teacher's Training and Research
Bhopal, India

ABSTRACT
Mobile ad hoc networks (MANETs) consist of a collection of wireless mobile nodes which dynamically exchange data among themselves without the reliance on a fixed base station or a wired resolution network. MANET nodes are typically well known by their precise power, transformation, and memory effects as well as high degree of mobility. In MANET mobile node is responsible for route establishment using wireless link where each node behave like both as a host and router. In such networks, the wireless mobile nodes may dynamically enter the network as well as go-ahead the network. Mobile ad hoc network is a group of many more devices or nodes with the capability of communication and networking. MANET encounter by number of security threat because of its open entrusted environment with little security settlement, even if security over MANET is not to be enhance up to satisfactory level because of its characteristics Security is an essential service for wired and wireless network communication. Due to its mobility and self routing effective nature, there are many deficiencies in its security. Various security threats show their impact at different layers, Among all of security thread worm hole is consider to be a very serious security thread over MANET. In wormhole two selfish node which is geographically very far away to each other, makes tunnel between each other to cover their actual location and try to believe that they are true neighbors and makes conversation through the wormhole tunnel. Wormhole attacks enable an attacker with limited resources and no cryptographic material to wreak havoc on wireless networks. For wormhole attack to have a best impact on the wired or wireless network, it must fascinate a huge amount of network traffic which is done by giving a shortest route to destination in the network. Therefore, the routes going through the wormhole must be shorter than alternate routes through valid network nodes. This Paper focuses on threat that wormhole attack possesses on network and also mentions few of the initiatives with their respective specifications to solve the problem of wormhole attack.

General Terms
Security, Encapsulation, Reactive Routing, Proactive Routing

Keywords
MANET, Wormhole attack, Wormhole detection technique, Wormhole Avoidance, Routing protocols, Wormhole attack modes.

1. INTRODUCTION
Wireless network refers to a network, in which all the devices communicate without the use of wired connection. Wireless networks [1] are generally implemented with some type of remote information transmission system that uses electromagnetic waves, for the carrier and self- configuring network that is formed automatically by a set of mobile nodes without the help of a fixed infrastructure or centralized management. Each node is prepared with a wireless transmitter and receiver, which allow it to interact with other nodes in its 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 interaction. Thus each node must accomplish as both a host and a router at the same time. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route transit. Such networks may achieve by themselves or may be connected to the larger internet. Privacy protection of mobile ad hoc networks is more demanding than that of wired networks due to the open nature and mobility of wireless media. A mobile Ad hoc network (MANET) is a collection of two or more devices or nodes equipped with wireless communication and networking capabilities [3].These node includes laptop, computers, PDAs and wireless phones etc, have a limited transmission range. In a MANET, nodes which are within each other's wireless transmission ranges linked directly, nodes that are farther from each other's range have to rely on some other nodes to transmit messages [4]. Thus, a multi-hop scheme develop, where several intermediary hosts broadcast the packets sent by the source host before they reach the final destination Due to the mobility in the ad hoc network, change of connective states and other effects of wireless transmission such as fading , multipath propagation, intervention etc.

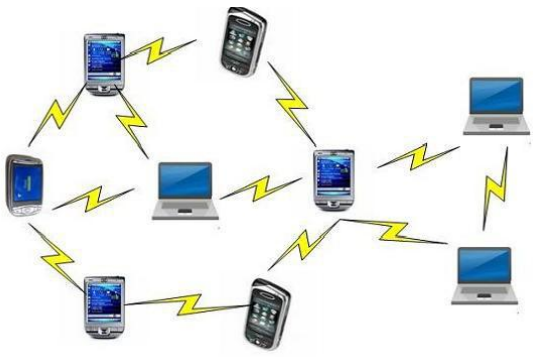
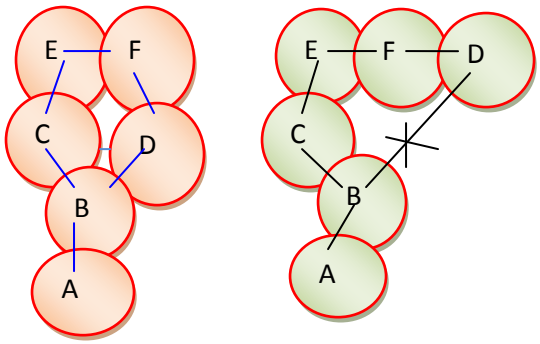


Figure.1 Mobile Ad-hoc Network

MANETs must have a secure way for transmission and communication which is a quite challenging and vital issue as there is increasing number of threats of attack on the wireless ad-hoc networks. In order to provide secure communication and transmission, the researchers must have to understand several different types of attacks and their effects on the MANETs environment. Wormhole attack, sinkhole attack, resource consumption attack, byzantine attack, routing table overflow attack, Denial of Service (DoS) , selfish node misbehaving, impersonation attack are the kind of attacks that a MANET can suffer from [5]. A MANET is characterized by having a effective, continuously modifying network topology due to mobility of nodes. A simple MANET example is illustrated in Figure2 [5].



Wireless links break between nodes B&D in fig (b)

(a) **(b)**

Figure 2 MANET Topology Changes

Circle shows the communication range of particularnode and nodes which are in direct communication range of other nodes are connected through wireless links. Here it is shown in ad hoc networks due to mobility wireless link breaks that origins change in the network topology. Initially, the network has the topology shown in Figure 2(a) but when node D moves out of the radio range of node B, the network topology changes to the one in Figure 2(b) when node D moves out of node B's radio range, network is damaged. Nevertheless, the network remains connected since node B can reach node D through nodes C, E, and F. Manet has some disadvantages, due to limited bandwidth, limited batter power of nodes and absence of infrastructure there are several chances for the attackers to break through the network and perform many attacks like Black hole attack, Flooding attack, Link withholding attack, Link spoofing attack, Replay attack, Colluding miserly attack and Wormhole attack. There are several kinds of routing protocols which are classified into two types.

1.1 Table driven routing protocols or Proactive routing protocols

In proactive routing protocols like Destination Sequenced Distance Vector (DSDV), Wireless Routing Protocol (WRP), Global State Routing, Fisheye State Routing, Hierarchical State Routing etc., the routes are calculated prior to the communication. All the nodes in the network maintain routing tables which contain routing information to all other nodes in the network and these tables are updated frequently in order to maintain consistency of the network. In proactive routing protocols whenever a node wants to send data it sends data immediately by taking a route from the routing table without any delay.

1.2 On-Demand routing protocols or Reactive routing protocols

In reactive routing protocols such as Ad hoc on demand Distance Vector (AODV), Dynamic Source Routing Protocol, Cluster Based Routing protocol (CBRP), Temporally Ordered Routing Algorithm (TORA), Ad-hoc On-demand Multipath Distance Vector (AOMDV) etc., the routes are calculated dynamically only when they are required. In this whenever a source node wants to send packets to destination node it initiates the route discovery mechanism to find the path to the destination. In reactive routing protocols the source cannot send the packets immediately, it requires some time to establish the route to the destination only then it can send the packets.

Section II describe about wormhole attack and types of wormhole attacks in section III we describe Related Work, in section IV we describe our proposed work, In Section V conclusion.

2. WORMHOLE ATTACK

Wormhole attack two selfish nodes join together. One node receives packets at one point and "tunnels" them to another attacker node via a private network connection, and then replays them into the network. Minimum two malicious nodes are required to perform this attack; more than two malicious nodes are also used to perform this attack In this attack the two malicious nodes resides in the two ends of the network and they form a link between them using an out-of-band hidden channel like wired link, packet encapsulation or high power radio transmission range [6].

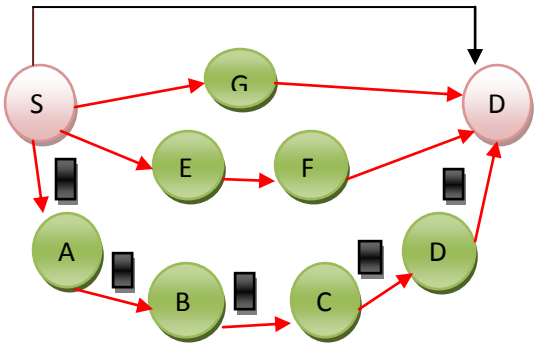


Figure 3 Wormhole Attack in MANET

Packet is travelling through the tunnel it reaches the destination speeder than other route and moreover the hop count through this path is going to be less so this path is established between the source and the destination [6] Once the path is established between the source and the destination through wormhole link they can misbehave in many ways in the network like continuously dropping the packets, selective dropping the packets, analyzing the traffic and performing Denial of Service attack.

2.1 Wormhole Attack Modes

Wormhole attacks can be launched using several modes, among these modes, we mention here-

2.1.1 Wormhole using Encapsulation: In this mode a malicious node at one part of the network and hears the RREQ packet. It channels it to a second colluding party at a distant location near the destination. The second party then rebroadcasts the RREQ packet; neighbors of the second colluding party receive the RREQ and drop any further legitimate requests that may arrive later on legitimate multi hop paths [7]. For example, consider Figure 4[7] in which nodes A and B try to discover the shortest path between A and B, in the presence of the two mischievous nodes X and Y. Node A broadcasts a RREQ packet , X gets the RREQ packet and encapsulates it in a packet destined to Y through the path that exists between X and Y (U-V-W-Z) Node Y de-marshals the packet, and rebroadcasts it again, which grasp B, due to the packet encapsulation, the hop count does not increase during the traversal through U-V-W-Z. Simultaneously, the RREQ packet travels from A to B through C-D-E. Node B have two routes, the first is four hops long (AC- D-E-B), and the second is apparently three hops long (A-XY- B). Node B will choose the second route since it appears to be the shortest while in reality it is seven hops long because it is not a actual route and showing like a short route because presence of wormhole attack . [7].

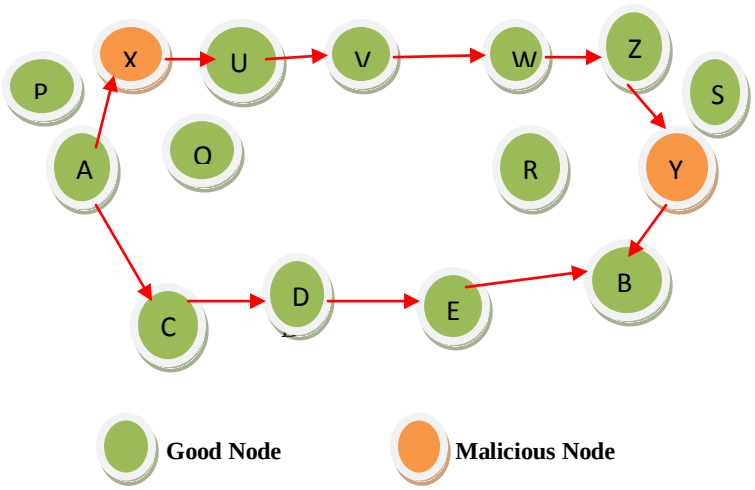


Figure 4. Wormholes through Packet Encapsulation

This mode of the wormhole attack is easy to launch since the two ends of the wormhole do not need to have any cryptographic knowledge, either they do not need any special efficiency, such as a high speed wired line or a high power source.

2.1.2 Wormhole using Out-of-Band Channel: The second mode for this attack is the use of an out of band channel. This channel can be accomplished, for example, by using a long range directional wireless link or a direct wired link. This mode of attack is more challenging to launch than the previous one since it needs specialized hardware capability. Consider the scenario depicted in Figure 5[7].

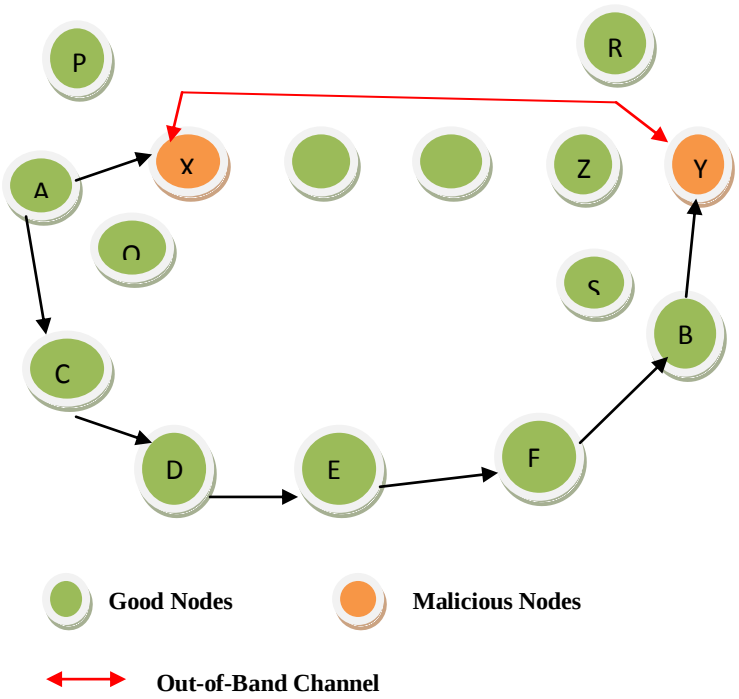


Figure 5. Wormholes through Out-of-Band Channel

2.1.3 Wormhole with High Power Transmission: Another method is the use of high power transmission. In this mode, when a single misbehaving node gets a RREQ packet, it broadcasts the request at a high power transmission, an efficiency which is not available to other nodes in the network. Any node that pick-up the high-power broadcast, rebroadcasts it towards the destination. By this method, the mischievous node increases its chance to be in the routes established between the source and the destination even without the participation of a colluding node.

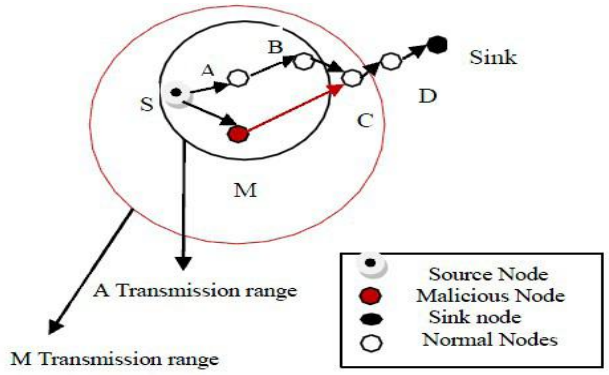


Figure 6. Wormhole Attack through high power transmission

2.1.4 Wormhole using Packet Relay: Wormhole using Packet Relay is another mode of the wormhole attack in which a malicious node relays packets between two distant nodes to convince them that they are neighbors. It can be sent by even one malicious node.

2.2 Wormhole Attack Threats

A wormhole tunnel could actually be useful if used for forwarding all the packets 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 systematically, etc. The attacker can also simply report the traffic for later analysis.

2.3 Impacts of Wormhole Attacks

The wormhole can solely peacefully transport all the traffic from one location within the network to a different location that's isolated, and 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.

2.4 Performance Metrics Considered For Evaluation

Here we have some metrics for evaluation is as follows-

Throughput: Throughput of any network scenario is defined as no. of knowledgeable packets or bits forwarded per second to the destination.

Packet loss: Packet loss is defined as no. of packets that are developed at source node but cannot be successfully delivered to the destination node within valid time.

Average end-to-end delay: Average end-to-end delay of the data packets is the interval between the data packet generation time and the time when the last bit arrives at the destination.

3. RELATED WORK

3.1 Prevention of Wormhole Attack

Sun Choi et al. in [8] considered that all the nodes will monitor the behavior of its neighbor. Each node will send RREQ messages to destination by using its neighbor list. If the source does not receive back the RREP message within a required time, it encounters the presence of wormhole and adds the route to its wormhole list. Each node maintains a neighbor node table which contains a RREQ sequence number, neighbor node ID, sending time and receiving time of the RREQ and count. Here the source node sets the Wormhole Prevention Timer (WPT) after sending RREQ packet and wait until it overhears its neighbor's retransmission. According to the author, the maximum amount of time required for a packet to travel one-hop distance is WPT/2. Therefore, the delay per hop value must not exceed estimated WPT. However, the proposed method does not fully support DSR as it is based on end-to-end signature authentication of routing packets.

Mahajan et al. [9] proposed some proposals to detect wormhole attacks like:

1) The crude decrease in the path lengths can be used as a possible symptom of the wormhole attack.

2) With the available displayed path instruction, if the end-toend path delay for a path can not 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 false exhibited link, yet they may use some nodes participate 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.

3.2 Detection and Avoidance of Wormhole Attack

Marti et al. proposed two techniques that improve throughput in an ad hoc network in the presence of selfish and malicious nodes [10]. The watchdog method is used for each node to detect misbehaving nodes in the network. When a node sends a packet to next hop, it tries to listen the packet forwarded by next hop. If it hears that the packet is forwarded by next hop and the packet matches the previous packet that it has sent itself, it considers the next hop node behaves well. Otherwise it considers the next hop node is misbehaving. In [11], authors study the impact of wormhole attacks on a real wireless mesh network test bed. Through theoretical analysis and comprehensive experiments, and find that when a path is under the control of wormhole links, standard deviation of RTT (stdev (RTT)) is a more efficient metric than per-hop RTT to identify wormhole attacks. Based on the observation, authors propose a neighbor-probe-acknowledge algorithm (NPA) to detect wormhole attacks by identifying the occurrence of large stdev (RTT). The evaluation results on test bed show that the proposed algorithm can achieve near 100% wormhole detection rate and zero false alarm rate both in light and heavy background traffic load scenarios. But, the parameters in NPA are static and not adaptive. So, in the future work on dynamic adjustment of algorithm parameters and routing algorithm that is resilient to wormhole attacks will be done. Furthermore, there will a possibility of adopt the observation to design a new routing protocol which can resilient to inside attacks without triggering the detection frequently to further decrease the overhead.

In [12] authors used the scheme called multi hop count analysis (MHA) with verification of legitimate nodes in network through its digital signature. Destination on node analyses the number of hop count of every path and selects the best path for replying. For checking the authentication of selected path, proposed methodology 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.

In [13] authors proposed E2SIW, a routing protocol immune to wormhole attacks. E2SIW uses a simple location information and alternate route finding techniques to detect and prevent wormhole attack in ad hoc networks. E2SIW has a high detection rate and less energy requirements compared to the De Worm protocol and also contributed in reducing the overhead associated with the control packets. Most of the work done so far in this topic assumes that the wormhole nodes are not capable of maliciously changing the data passing through them. But this may not always be the case. The design of the mitigation solutions keeping in mind that intelligent malicious nodes may exists is the need of the hour.

Table 1 Summary of Detection Methods of Wormhole Attack

METHOD	MOBILITY	QOS PARAMETER	SYNCHRONIZATION	FALSE DETECTION
HMTI	Handled Weakly, Topologicallly Robust	Jitter, Delay	Not Required Since PSD Profiling is done Locally	Use PSD to detect False Positive Alarm
Farid et al	Not Considered	Queue Delay Within Nodes	Sometime delay added to detect suspicious links	Not Handled
Delphi	Not Considered	Delay	Not Required	Not Handled
SAM	Cluster and Uniform Topology Considered	Not Considered	Not Considered	Not Handled
SAW	Not Considered	Not Considered	Not Considered	Failed to detect
DAW	Not Considered	Delay Parameter	Not Considered	Failed to detect
WAP	Maximum transmission distance is calculated	Delay Per hop	Only the source node is synchronized	Not handled

W. Wang et al. proposed a more generic approach [14] for end-to-end wormhole detection mechanism on a multi-hop route. In this detection approach all intermediate nodes will attach its timestamps and positions to the disclosure packets. After receiving a disclosure packet, the destination will check for the validation of these packets. If many successive detection packets are all lost or a wormhole is detected, then the destination node will broadcast a message which notifies the source to abort the current route and reinitiate the process.

Delay per Hop Indication (Delphi) [15] is another hop count analysis based solution that uses delay as a parameter for detecting Wormhole attack in MANET. The detection mechanism uses the delay/hop value for detecting wormhole attacks. The reason behind that under a wormhole attack, the delay that a packet experiences for propagating across false neighbors should be unreasonably high since there are in fact many hops between them.

Lazes et al. [16] has used a Local Broadcast Key (LBK) based method to set up a secure ad hoc network against wormhole attacks. In other words, there are two kinds of nodes in their network: guards and regular nodes. Guards access the location information through GPS or some other localization method and continuously broadcast location data. Regular nodes must calculate their location relative to the guards‟ beacons, thus they can distinguish abnormal transmission due to beacon retransmission by the wormhole attackers. All transmissions between node pairs have to be encrypted by the local broadcast key of the sending end and decrypted at the receiving end. In addition, special localization equipment has to be applied to guard nodes for detecting positions.

Another approach to detect closed wormholes is Packet Leash, which was proposed by Hue, Perrig and Johnson [17]. The leash is the information added into a packet to restrict its transportation distance. In the geographical leashes, the location information and loosely synchronized clocks together verify the neighbor relation. Each node, before sending a packet, affixes its current position and transmission time to it. The receiving node, on receipt of the packet, computes the distance to the sender and the time it took the packet to traverse the path. The receiver can use this distance anytime information to deduce whether the received packet passed through a wormhole or not. In temporal leashes, the packet transmission distance is calculated as the product of signal propagation time and the speed of light. In Temporal Leashes all nodes are required to maintain a tightly synchronized clock but do not rely on GPS information.

4. PROPOSED WORK

Our proposed work divide into two phases in phase 1 describe the generation of wormhole attack and in phase 2 describe a efficient approach for analyzing and prevention of wormhole attack.

Phase 1: Generation of Wormhole Attack

The wormhole attack is generated on mobile nodes in the Ad Hoc network. The two colluding nodes are connected through a tunnel. They generate illusive neighbors in the network. Hence, the Route request packets are misled by illusive neighbors. Malicious nodes receive route request and extract topology information. It may replay wormhole attack on other nodes in the Network.

Phase 2: Neighbor list Detection Approach for Wormhole Attack:

Step1: Sending RREQ message source find route to destination.

Step 2: RREQ packet is received by intermediate nodes and verifies destination address by checking if (d=RREQ) it means packets have destination address then intermediate nodes forward packet to destination.

Step 3: While receiving the RREQ packet, all intermediate nodes update their routing table.

Step 4: Once the destination node receives RREQ message from neighboring nodes, it unicasts the RREP message back to the source node. RREP message contains route reply count and neighbor lists.

Step 5: When the source node receives the RREP message, it records the route to the destination and the destination neighbor list and hop count between source and destination.

Step 6: When source node receives RREP message it will send additional message of route reply decision packet to destination node, It also contains source neighbor list NLs (NLs is stand for neighbor list for source).

Step 7: When source node send neighbor list entry NLs it is stored by destination node.

Step 8: Source node neighbor list stored in NLs and Destination node neighbor list stored in NLd.

Step 9: Compare both neighbor list source node and destination node and calculate the number of common neighbor nodes present between sources to destination by if {NLs(i)==NLd(j)}.

Step 10**:** While receiving the RREP message from destination node, source node stores the hop count between source and destination. Depends on the hop count value the threshold value is fixed.

Step 11: Number of common neighbors between source and destination exceeds the Threshold value then it will find out wormhole attacker nodes may present among the path.

Step 12: When it will find out wormhole attacker nodes present then Sender send worm announcement message to all nodes.

Step 13: All original nodes drop the wormhole attacker nodes.

Step 14: End

5. CONCLUSION

Wormhole attacks are severe attacks that can easily be launched even in networks with confidentiality and authenticity. Malicious nodes usually targets the routing control messages related to topology or routing information. In this paper, we introduced the wormhole attack along with its classification that can have serious consequences on many proposed ad hoc network routing protocols. Various methods and techniques used for the detection and prevention of wormhole attack along with their advantages and drawbacks are also discussed. In this paper the effects of wormhole attack in Mobile ad hoc network analyzed and prevented by using neighbor list based detection algorithm for wormhole attack in Manet. Finally we have proposed a new, energy-efficient algorithm is to detect wormhole attack in AODV protocol and also compare some factors end-to-end delay, throughput, packet delivery ratio etc.

6. REFERENCES

[1] Maulik, R.; Chaki, N., "A comprehensive review on wormhole attacks in MANET" IEEE 2010, Page 233-238.

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

[3] Perkins C. and Bhagwat P.: Highly dynamic destination-sequence distance vector routing (DSDV) for mobile computers, In Proceedings of ACM Conference on Communications Architectures, Protocols and Applications (ACM SIGCOMM 94), London, UK, pp. 234-244 (1994)

[4] Upadhyay S. and Chaurasia B. K.: Detecting and Avoiding Wormhole Attack in MANET using Statistical Analysis Approach, In the Second International Conference on Computer Science and Information Technology (CCSIT-2012), Springer, pp. (2012).

[5] Devinder Pal Singh et al.,’ INVESTIGATING THE EFFECT OF WORMHOLE ATTACK ON AODV in 2012.

[6] Azer, M.A., El-Kassas S.M., Hassan, A.W.F., El-Soudani M.S., “Intrusion Detection for Wormhole Attacks in Ad hoc Networks a Survey and a proposed Decentralized Scheme Marianne “ IEEE Third International conference on Availability, Reliability and Security, 2008.

[7] K. Issa, B. Saurabh, and B. S. Ness, "LiteWorp: Detection and Isolation of the Wormhole Attack in Static Multihop Wireless Networks," The International Journal of Computer and Telecommunications Networking vol. 51, pp. 3750-3772, 2007.

[8] S. Choi, D. Kim, D. Lee, J. Jung, “WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks”, Int’l conf. on Sensor Networks, Ubiquitous and Trustworthy Computing, pp. 343- 348, 2008.

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

[10] S. Marti et al. “Mitigating routing misbehavior in mobile ad hoc networks,” Proceedings of Sixth Annual IEEE/ACM Intl. Conference on Mobile Computing and Networking , April 2009,PP. 225-256

[11] Jie Zhou1, Jiannong Cao, Jun Zhang1, Chisheng Zhang and Yao Yu, “Analysis and Countermeasure for Wormhole Attacks in Wireless Mesh Networks on a Real Test bed” in 26th IEEE International Conference on Advanced Information Networking and Applications,2012

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

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

[14] X. Wang & J. Wong, (2007) "An End-to-end Detection of Wormhole Attack in Wireless Ad-hoc Networks", 31st Annual International Computer Software and Applications Conference - Vol. 1 - (COMPSAC 2007), pp. 39-48.

[15] H. S. Chiu & K. S. Lui, (2006) “Delphi: Wormhole Detection Mechanism for Ad Hoc Wireless Networks", Proc. of International Symposium on Wireless Pervasive Computing, pp-6-pp.

[16] Lazes, L.; Poovendran, R.; Meadows, C.; Syverson, P.; Chang, L.W. Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach. In *IEEE WCNC 2005*, Seattle, WA, USA, 2005; pp. 1193–1199.

[16] Lazes, L.; Poovendran, R.; Meadows, C.; Syverson, P.; Chang, L.W. Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach. In *IEEE WCNC 2005*, Seattle, WA, USA, 2005; pp. 1193–1199.

[17] Hu, Y.C.; Perrig, A.; Johnson, D.B. Wormhole Attacks in Wireless Networks. IEEE J. Sel. Area Comm. 2006, 24, 370–38