Wormhole Attack Detection Techniques: A Review

[1]Mahendra Dhole, [2]Anand Gadwal

[1,2]Dept. of Computer Science & Engineering, TCET Indore, MP, India

Abstract

Mobile ad-hoc network is self-organizing wireless network composed of different nodes communicate with each other without having established infrastructure. It generally works by broadcasting the information and used air as medium. Its nature of broadcasting and transmission medium also help attacker to disrupt network. Many kind of attack can be done on such Mobile Ad Hoc Network. The emphasis of this paper is to study wormhole attack, some detection method and different techniques to prevent network from these attack. This analysis able to provide in establishing a method to reduce the drawbacks like reliability, message overhead, delay and clock synchronization and to become more faster.

Keywords

Mobile Ad-Hoc Network, Attacks, Wormhole Attack, Detection Methods.

I. Introduction

Mobile ad hoc network is said to be an infrastructure less network and it is dynamic in nature. An infrastructure less network is not having any steady infrastructure for the communication. Each node in that type of network can communicate directly with other nodes in the network and there is no necessity of any centralized network access point. A significant thing about these types of networks is that these networks are not having any routers but the wireless nodes work as a routers and a host. These networks don't have any static or fixed topology.

A. Security Principles

Security includes a group of investments that are sufficiently funded. In MANET, each and every networking functions such as routing and packet forwarding, are execute by nodes themselves in a self-organizing manner. In favour of these reasons, securing a mobile ad -hoc network is extremely challenging. The goals to check if mobile ad-hoc network is secure or not are as follows:

1. Availability

Availability refers to assets which are accessible to authorized parties at proper times. Availability applies equally to data and to services. It gives the survivability of network service in spite of denial of service attack. It is also means sharing information so as to make sure consistency among redundant resources.

2. Confidentiality

Confidentiality makes sure that computer-related possessions are accessed only by authorized parties. It means, only those who should have access to somewhat will actually get that access. If we have to maintain confidentiality of some confidential information, we need to carry on them confidential and secret from all entities that do not have privilege to access them. Confidentiality is occasionally called secrecy or privacy.

3. Integrity

Integrity means that resources can be customized only by authorized parties or only in authorized manner. Modification includes writing, deleting and creating, changing status. Integrity assures that a message being passed is never corrupted.

4. Authentication

Authentication enables a node to make sure the identity of peer node it is communicating with. Authentication is fundamentally guaranteed that participants in communication are not impersonators they are authenticated. Authenticity is ensured because only the rightful sender can generate a message that will decrypt correctly with the shared key.

5. Non Repudiation

Non repudiation is the property which ensures that sender and receiver of a message cannot deny that they have ever sent or received such a message .This is useful when we want to discriminate if a node with a few undesired function is compromised or not.

6. Anonymity

Anonymity means all the information that can be used to recognize owner or present user of node should default be kept private and not be distributed by node itself or the system software. It provides the all probable information that can be used to identify the vendor.

7. Authorization

This property assigns dissimilar access rights to different types of users. For example a network management can be performed by network administrator only. Authorization is a procedure in which an entity is issued a credential which privileges and permissions it has and cannot falsify by the certificate authority. It is also used to allocate different access rights to different rank of users.

II. Wormhole Attack

Mobile ad hoc networks are open to many of the attacks due to many reasons such as wireless links between nodes, insufficiency in infrastructure, nonexistence of centralized monitor or management, limited physical Protection, and the resource constraints. A particularly security attacks called as wormhole attack is utilized in the ad-hoc networks [1-3]. One malicious node captures packets from one place in the network and tunnels the captured packets to another malicious node at another place as shown in the fig. 1, which replays them locally in the ad hoc environment.

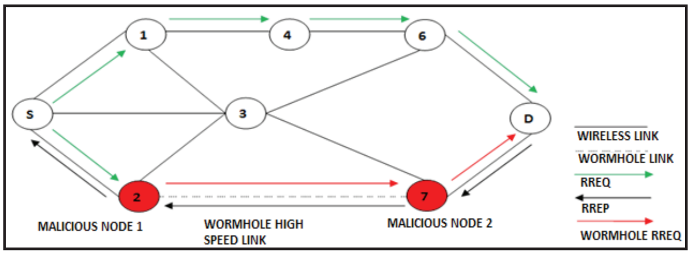


Fig. 1: Worm Hole Attack in Ad Hoc Network

A. Wormhole Attack Classification

Two of the attackers work together in a wormhole attack, in which first one receives the packets at one location in the network and tunnels the packets to its friend attacker at another location in the network. After that the friend attacker replays packets into the network. Two types of wormhole attacks have been identified. In first attack known as Hidden attack, legitimate nodes hide their identity in the network while forwarding packets. In the second type of attack which is known as exposed attack, Legitimate nodes show their identity but other nodes are not aware that they are malicious [1, 4-5].

1. Hidden wormhole Attack

The packet and the packet header do not modify by the attacker, but they only tunnel the packet from one place to another place. Sender end treats the receiver as its immediate neighbour in this type of attack [5]. As shown in Fig. 2 the packet from source node S is received by the malicious node M1, and it tunnels the packets to another malicious node M2 and replies them to receiver D, without transforming the packet header. As M1 and M2 are legitimate nodes they hide their identity in packet header thus D can only observes S as previous hop. The same phenomena happens in the reverse path, and S finds D as its immediate neighbour, so the path found is {S, D}.

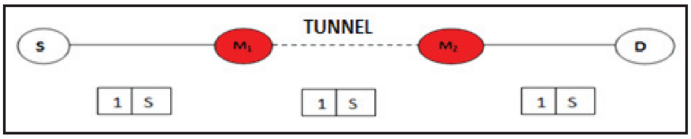


Fig. 2: Hidden Wormhole Attack

2. Exposed Wormhole Attack

In this type of attack malicious users do not change the content of the packet, but shows the presence in the packet header for the route setup procedure. Other nodes are known that the malicious nodes present in the path but they would assume that the malicious nodes are neighbours of each other. Let's consider the situation where source node S wants to establish a route to receiver node D. As shown in Fig. 3, malicious node M1 receives the packet from source node S, modifies the hop field value by M1 and increases the hop count value by 1. RREQ packet is tunnelled to malicious node M1 and M2 performs the same procedure and broadcasts the RREQ packet to receiver D. Receiver D discover that its immediate neighbour is M2 with hop count value equals to 3. The same phenomenon happens in the reverse path. As soon as S receives the RREP packet, it discovers its immediate neighbour is M1 with hop count value equals to 3. So the route establishes as {S, Ml, M2, D} [5].

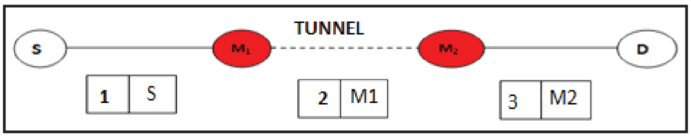


Fig. 3: Exposed Wormhole Attack

B. Modes of Wormhole Attack

There are four modes of wormhole attacks in ad hoc network [1, 4].

1. Wormhole Using Encapsulation

A first malicious node hears the packet RREQ at one location in the network and tunnels it to other which is second malicious node at another location near the destination in this mode type. The second malicious node again rebroadcasts the RREQ packet. The neighbours of the second malicious node receive the RREQ packet and drop every future legitimate request that will be arrive later on legitimate multi hop paths. Then the result is that the routes among source and destination go through the two malicious nodes that will be formed a wormhole between them. For example, Figure 4, which shows Wormhole attack through Packet Encapsulation [3].

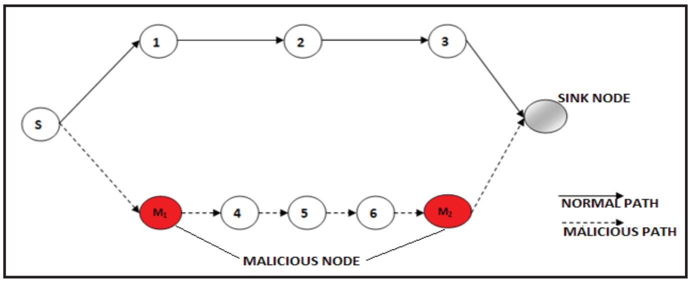


Fig. 4: Worm Hole Attack through Packet Encapsulation

2. Wormhole Using Out-of-Band Channel

The out of Band Channel can be created using a long range directional wireless link or a direct wired link as given in Figure 5. In comparison with previous attack it is complex to launch such attack mode because it needs dedicated hardware capability [3].

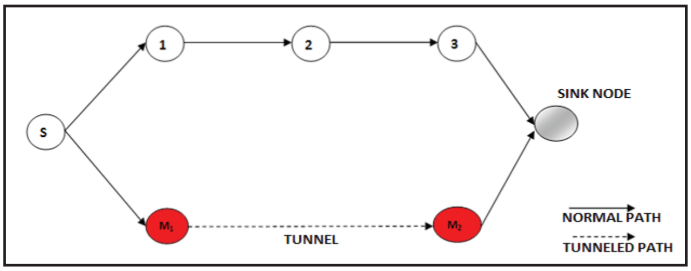


Fig. 5: Worm Hole Attack through Out-of-Band Channel

3. Wormhole with High Power Transmission

If a single malicious node obtains a RREQ, malicious node broadcasts the RREQ at a high power level therefore the malicious node gets chance to be in the routes establishment between the source node and the destination node, without need of any other malicious node because other node does not have such high power level as given away in the fig. 6.

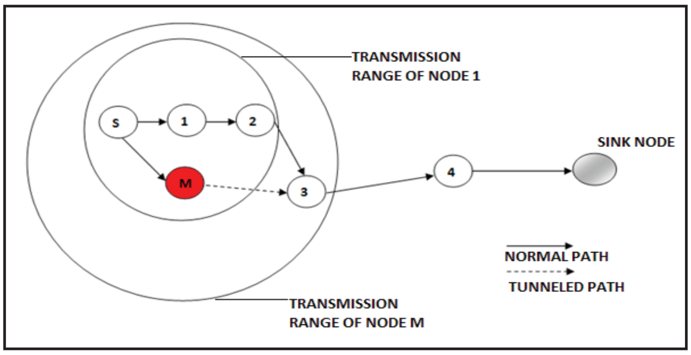


Fig. 6: Worm Hole with High Power Transmission

4. Wormhole Using Packet Relay

Packet relay is another mode of wormhole attack in which two malicious nodes which are apart from each other but likes that they are neighbours can relay packet between them.

III. Literatue Review

The goals of Ad hoc networks and mainly MANET have in current years not just seen widespread use in commercial and domestic application regions but have also become the focus of intensive study. Applications of MANET range from simple wireless home and office networking. Security aspects play an important role in all of these application scenarios given the vulnerabilities inherent in wireless ad hoc networking from the very fact that radio communication takes place. The above paper contents various literature surveys, which cover all dimensions of study.

A. Perrig, D. B. Johnson and Y. C. Hu [6] proposed a detection and prevention method in which there are two types of packet leashes:

1. Geographical Leashes
2. Temporal Leashes

Leash is information which is embedded in the packet at the time of designed to restrict the packets to travel maximum allowed transmission distance.

1. Geographical Leashes

The recipient of the packet is lie within an assured distance from the sender of the packet in Geographical Leashes. For the construction of geographical leash, each node mandatorily required to know its own location also all nodes mandatorily have clocks which are loosely synchronized. Use of geographical leash is defined as, when a sending node sends a packet, it includes its current location (ps) and the current time at which it send a packet (ts). When receiver node of the packet is receive the packet it compares the values (ps and ts) to its current location (pr) and the current time at which it received the packet (tr). In order to compute upper bound on distance between sender and itself (receiver), receiver required that clocks of sender and receiver are synchronized to within ± Δ where ν is an upper bound on the velocity of any node. Which is particularly based on the timestamp ts (packet's sending time), tr (time at which packet is received), □ (maximum relative error in location information), ps (location- sender node) and pr (location- receiver node).

$$dsr \le \| ps - pr \| + 2\ \nu.(tr - ts + \Delta) + □$$

Any authentication technique such as digital signature can be used to permit a receiver to authenticate the location of the receiving packet.

2. Temporal Leashes

The packet has an upper bound for its whole lifetime, by which a packet is restricted to travel maximum distance. The packet can travel with the speed of light in temporal leash. For construction of the temporal leash, all nodes must have clocks which are tightly synchronized. The maximum difference is Δ between any two clocks of the nodes. The value of the parameter Δ should be known to all nodes in the network. For temporal leashes the value of Δ must be on the order of a small amount of microseconds or even hundreds of nanoseconds. Level of the time synchronization can be achieved by hardware such as LORAN-C, WWVB, and GPS etc. Some other hardware such as rubidium clocks, hydrogen maser clocks and cesium-beam clocks are also used for sufficiently correct time synchronization for months. The use of temporal leash, when a sending node sends a packet, it includes the time at which it sends the packet, ts. When receiver of packet receives packet, receiving node compares this value (ts) to the time at which receiver node receives packet, tr. At the receiver end, if the packet traveled too far, the receiver is capable to detect packet based on clamed transmission time and the speed of light.

The advantage of geographical leashes over the temporal leashes is that the time synchronization is looser and the other advantage is that geographical leashes uses the concept of digital signature method for successful secure delivery of packet at receiver's end.

L. Hu and D. Evans [7] proposed the detection and prevention technique in which Directional antenna scheme is used in ad hoc network for increasing the capacity and the connectivity of ad hoc networks. Transmission of packet in particular direction gives. The directional antenna transmission system uses energy extra efficiently. In comparison with Omni directional antenna, the transmission range of directional antennas is generally larger which can decrease the number of hops in routing. Using directional antennas can increase spatial reuse and reduce packet collision and negative effect such as deafness. Directional antenna model assumes an antenna with N zones. Each of the zones are conical in shape and has a conical radiation pattern, spanning an angle of 2 /N radians. The model zones are fixed and non overlapping beam direction pattern; so that the N zones collectively cover the whole plane as shown fig. 7.

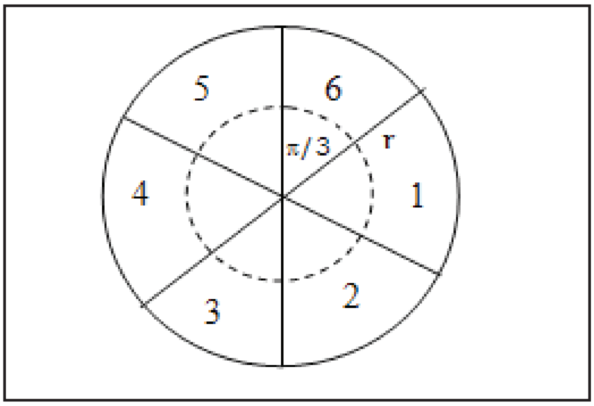


Fig. 7: Directional Antenna with 6 zones

When the node is idle, in this situation the node listens the carrier in omni mode. When the idle node receives a message, it determines the zone on which the received signal power in maximal and the node utilizes that zone to communicate with sender. Directional antenna scheme follows three steps: first is Directional Neighbors Discovery, second step is to verify Neighbor Discovery and finally Strict Neighbor Discovery will be performed.

Wormhole attack is one of the significant attacks which create a serious threat in the wireless networks, especially for location-based wireless security systems and ad hoc wireless routing protocols. H. S. Chiu and K. S. Lui [5] proposed a method for detection of wormhole attack called Delay per Hop Indication (DelPHI). The sender is capable to detect both kinds of wormhole attacks by discovering the delays of different paths to the receiver. This method does not requires synchronized clocks or special hardware furnish mobile nodes. The result analysis of the DelPHI has been examined by simulations. The result of simulation shows that DelPHI has gain greater than 95% in detecting normal path and gain greater than 90% in detecting wormhole attack, in the absence of background traffic. The result of simulations has also shown that DelPHI can gain greater than 85% detection rate for both normal and tunnelled paths with the background traffic. The problem of message overhead is the limitation of DelPHI which is also addressed in this paper.

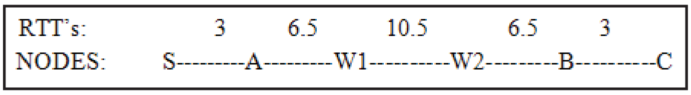
T. V. Phuong, N. T. Canh, Y. K. Lee, H. Lee, and S. Lee [8] proposed a prevention and detection method called TTM (Transmission Time Mechanism) for MANET. In this mechanism source node establishes a route to destination node. This technique checks whether there is a wormhole link present in the route or not by evaluating round trip time among two successive nodes along the route. Each and every node in the established route calculates the Round Trip Time- RTT between it and the destination and then sends these values back to the source node. The source node collects all RTT values from different routes and calculates RTT's between two successive nodes of different routes and then identify wormhole attack based on the fact that the RTT between two malicious or FAKE neighbors will be considerably higher in comparison to the two real neighbors.

A. S. Alshamrani [9] proposed a detection and prevention method called Packet Travel Time algorithm for MANET. This mechanism initially uses the same process of calculating the RTT's (round trip time) which are used in transmission time mechanism (TTM) among two successive nodes. Furthermore it monitors all of the packets transmitted in the network. When the RREQ packet is forwarded, then each and every node records the sending time (ts) and save sending time (ts) values in memory and the time when it overhears its neighbor rebroadcast the RREQ packet (th). Furthermore each node compute the PTT value with (PTT=th-ts) and each node save the PTT value until it receives the RREP and append PTT value in the particular part which is formed by the destination. When source node receives the RREP response, it calculates the Round trip time (RTT) between every two successive nodes by the similar process that has been discussed in TTM and then these values has compared with the values of PTT's and locate if there is any wormhole link in the route. Table 1 shows the sending and receiving time values of all nodes received by source node and the calculation done by the source node.

Table 1: Sending and Receiving Time Values of all Nodes

NODES	RREQ Sending Time	RREP Receiving Time	Calculation done by source node
S	0	32.5	32.5
A	1.5	31	29.5
W1	6.5	29.5	23
W2	12	24.5	12.5
B	13.5	19.5	6
C	15	18	3

RTT's between nodes are:



```
RTT's:          3       6.5        10.5        6.5       3
NODES:     S---------A---------W1----------W2---------B----------C
```

The value of PTT's received at source node shown in Table 2.

Table 2: Values of PTT's at Source Node

NODES	RREQ Sending Time	RREP Overhearing Time	PTT'S
S	0	1.5	1.5-0=1.5
A	1.5	6.5	6.5-1.5=5
W1	6.5	12	12-6.5=5.5
W2	12	13.5	13.5-12=1.5
B	13.5	15	15-13.5=1.5
C	15	-	-

M. M. Gore and G. K. Patnaik [10] proposed Trustworthy Path Discovery in MANET which is a Message Oriented Cross-correlation Approach. When source node established a route to destination node, this mechanism tried to check whether there is wormhole link in the route or not by discovering trustworthy path. The mechanism has two categories of nodes i.e. Trusted Mobile Node (TdMN) and Trustier Mobile Node (TrMN). TdMNs are trusted and every TrMN is associated with one of the TdMNs within its communication range pronounced as Associated Trusted Mobile Node (ATMn) [10]. And shows the trustworthy mechanism.

Mr. Susheel Kumar, Vishal Pahal and Sachin Garg [11] proposed a review of wormhole attack in MANET. It is normally works by broadcasting the information and used air as medium .It's transmission medium and broadcasting nature also help attacker, whose intention is to spy or disrupt the network. There are many type of attack can be done on such Mobile Ad-hoc network. The emphasis of particular research is to study wormhole attack, some different techniques and detection methods to provide a security to a network from these attacks. To demonstrate the impact of wormhole attacks in MANET, there is simulated randomly distributing nodes within a rectangular type of region and used the shortest path algorithm to locate the best route between any node pairs. If the wormhole is formed, some of the node pairs may find "shorter" path through the wormhole and therefore be controlled by the wormhole. During the first experiment, the base station is located at corner, one wormhole endpoint is close to the base station and another endpoint moves diagonally across the network.

Applying more hardware for increasing security may lead the better result, but can also be costly which may affect other networks need. Similarly some network require additional security like military area network as compare to just local communication network, it also depending on network type like wireless sensor network have less mobility and can be described in some standard model ,but most of other mobile ad hoc network are of infrastructure less ,in this way we can say the choice of detection method depend upon different situation.

Mobile ad hoc network is highly vulnerable to attack due to open error prone shared wireless medium. Mr. Sauabh Upadhyay and Aruna Bajpai [12] proposed an algorithm for avoiding and preventing the wormhole attacks in MANET using statistical analysis approach. Results of simulation shows that proposed algorithm provides better performance and security in the presence of wormhole attack than conventional AODV.

Statistical analysis approach is very useful if the satisfactory information about the routes is available from multi path routing. A simulation result shows that this algorithm is successful at detecting wormhole attacks and finding the malicious nodes. A result of simulation also shows that wormhole tunnel is avoided in route discovery process so that the effects of wormhole attack are minimized. This algorithm is light weight so it can be applied to many demands and limitations of MANET providing high efficiency.

Ms. Monika and Jyoti Thalor [13] proposed research review on Wormhole Attack Detection and Prevention Technique in MANET. Mobile Ad Hoc Networks refers in the direction of a multi-hop packet based wireless network composed of a set of mobile nodes that can communicate and move at same time, without using any type of fixed wired infrastructure. Ad Hoc network are useful and popular because of its infrastructure less environment. Ad-hoc Network is a collection of nodes, in this network individual nodes corporate by forwarding packets for each other to permit nodes to communicate beyond direct transmission range. Safety and security is primarily concern in order to offer protected communication between mobile nodes in hostile environments. A huge number of routing protocols for mobile ad hoc network has been proposed to enable quick and efficient network formation and restructuring.

Dr.Satbir Jain and Shalini Jain [15] gives the novel trust based method for isolating and identifying nodes that form a wormhole in the network without engaging any cryptographic means. They demonstrate that their scheme functions effectively with the help of extensive simulations in the presence of malicious colluding nodes and does not impose any needless conditions upon the network establishment and operation phase. The trust levels in neighbouring nodes based upon their sincerity in execution of the routing protocol. It derived trust is then used to influence the routing decisions, which in turn guide a node to stay away from communication through the wormholes.

Revathi Venkataraman, T. Rama Rao, M. Pushpalatha, and Rishav Khemka [17] proposed the graph-theoretic algorithm for detection of multiple wormhole attacks in mobile ad hoc networks. In this graph-theoretic algorithm if symmetric links are assumed, the upper triangle of the matrix is sufficient to store all the information of the neighborhood. The adjacency matrix requires n(n-1)/2 bits of storage. Alternatively, a linear array can be used to represent the set of neighbours of each node in an ad hoc network. A graph theoretic approach based on adjacency matrix of a network is proposed which easily detects the existence of wormholes in mobile ad hoc network. This method is beneficial since it does not increase the computation complexity in a mobile node which is resource constrained.

Issa Khalil et.al [19] presented a protocol called MOBIWORP for mitigating the wormhole attack in sensor networks and mobile multihop ad hoc networks. This incorporates two protocols CAP-CV and SMP for differing degrees of functionality afforded to a mobile node. They also proposed global and local isolation protocols that will neutralize the capability of the malicious nodes from launching further attacks after detection, at the current location or at a new location. They demonstrated the effect of MOBIWORP under different mobility patterns and network conditions using simulations.

Wormhole refers to an attack on mobile ad hoc network routing protocols in which colluding nodes make an illusion that two remote areas of a mobile ad hoc network are directly connected through nodes that appear to be neighbours but are actually distant from one another. A wormhole attack is a harsh attack on mobile ad hoc network routing where two attackers, connected by a high speed off-channel link, are tactically placed at different ends of a network. Wormhole attacks in mobile ad hoc network significantly degrade network performance and threat to network security and safety. Proposed approaches which will assist us in future to design a new approach for detecting the wormhole attack in Mobile ad Hoc network.

Table 3 Noteworthy contributions shows the summarized way of literature review from latest to older researches. It also shows the advantages and limitations of researches.

Table 3: Noteworthy Contributions

S.NO	TITLE OF PAPER	AUTHORS	YEAR	ADVANTAGE AND LIMITATIONS
1.	DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks.	H. S. Chiu, K. S. Lui	2013	It does not require clock synchronization and provides high power efficiency but it has some drawbacks like reliability & message overhead.
2.	Wormhole Attack Detection and Prevention Technique in Mobile Ad Hoc Networks: A review.	Monika, Jyoti Thalor	2013	It will help us in future to design a new approach for detecting the wormhole attack in MANET but it need GPS and Specialized Hardware which may increase cost.
3.	Avoiding and preventing the wormhole attacks in MANET using statistical analysis approach.	Sauabh Upadhyay, Aruna Bajpai.	2012	This approach is very useful if the sufficient information about the routes is available from multi path routing and can detect the wormhole .The algorithm is light weight so it can be applied to demands and limitations of MANET.
4.	Wormhole attack in MANET: A review.	Susheel Kumar, Vishal Pahal, Sachin Garg.	2012	Implementing more hardware for increasing security may lead the better result but can be costly.
5.	PTT: Packet Travel Time Algorithm in MANAT.	A. S. Alshamrani.	2011	It is able to tackle both the wormhole attacks by calculating PTT and RTT between two successive nodes but it requires clock synchronization.
6.	Trustworthy Path Discovery in MANET - Cross correlation.	G. K. Patnaik, M. M. Gore.	2011	This analysis shows significant improvement in packet delivery ratio of AODV in the presence of attacks, but finding the trustworthy path in MANET is still a real challenge.
7.	Detection and prevention of wormhole attack in MANET: novel trust based scheme for isolating nodes.	Shalini Jain, Satbir Jain.	2010	The trust model can efficiently locate reliable routes through the network in the presence of a wormhole in the network. The evasion of such wormholes in an ad-hoc network is still considered a challenging task.
8.	A Graph-Theoretic Algorithm for Detection of Multiple Wormhole Attacks in Mobile Ad Hoc Networks.	R. Venkataraman, M. Pushpalatha, T. Rama Rao, & Rishav Khemka.	2009	This approach is advantageous because it does not raise the computation complexity in a mobile node which is resource constrained. This mechanism will be accordingly modified to suite reactive protocols also.

9.	MOBIWORP: Mitigation of the wormhole attack in mobile multihop wireless networks.	Issa Khalil, Saurabh Bagchi, Ness B. Shroff.	2008	It neutralize the capability of the malicious nodes from launching further attacks after detection, whether at the current location or at a new location.
10.	Transmission Time Based Mechanism to Detect Attacks.	V. Phuong, N. T. Canh, Y. K. Lee, S. Lee &H. Lee.	2007	It is used to check the wormhole link in the route but It Requires Calculating round trip time (RTT).
11.	Using Directional Antennas to Prevent Wormhole Attacks.	L. Hu, D. Evans.	2004	It increasing the capacity and the connectivity of ad hoc networks but it requires Directional antennas on all nodes.
12.	Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks.	Y. C. Hu, A. Perrig, D. B. Johnson.	2003	Geographical leaches are less efficient then Temporal leaches, since they require broadcast authentication, but they can be used in networks where precise time synchronization is not easily achievable.

IV. Conclusion

Wormhole attacks can degrade network performance significantly in ad hoc network and harms the network security. The detection of wormhole attacks is quite complicated. In this paper we have basically surveyed the existing methods and approaches which will help us in future to design an enhanced approach for detecting the wormhole attack in Mobile Ad Hoc network. Overall a significant amount of work has been done on solving wormhole attack problem. It is the fact that we can’t say one solution is applicable to all situations. There is choice of solution available based on cost, need of security may lead better result, but can be costly, which may affect other networks necessities.

Similarly some network requires more security like the military area network. A standard and customary solution is still lacking, although several very useful solutions applicable to some networks have been described.

References

[1] P. Sharma, A. Trivedi,“An Approach to Defend Against Wormhole Attacks In Ad Hoc Network using Digital Signature”. IEEE, 2011.

[2] R. Maulik, N. Chaki,“A Study on Wormhole Attacks in MANET”, International Journal of Computer Information Systems and Industrial Management Applications, Vol. 3, pp. 271-279, 2011.

[3] E. A. M. Anita, V. ThulasiBai,“Defending Against Wormhole Attacks in Multicast Routing Protocols for Mobile Ad Hoc Networks”, IEEE, 2011.

[4] M. Azer, S. E. Kassas, M. E. Soudani,“A Full Image of the Wormhole Attacks towards Introducing Complex Wormhole Attacks In wireless Ad Hoc Networks”, International Journal of Computer Science and Information Security, Vol. 1, No. 1, May 2009.

[5] H. S. Chiu, K. S. Lui,“DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks”, IEEE, 2013.

[6] Y. C. Hu, A. Perrig, D. B. Johnson,“Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks”, IEEE, 2003.

[7] L. Hu, D. Evans,“Using Directional Antennas to Prevent Wormhole Attacks”, Network and Distributed System Security Symposium, San Diego, California, USA, February 2004.

[8] T. V. Phuong, N. T. Canh, Y. K. Lee, S. Lee, H. Lee, “Transmission Time Based Mechanism to Detect Attacks”, IEEE, 2007.

[9] A. S. Alshamrani,“PTT: Packet Travel Time Algorithm in Mobile Ad Hoc Networks”, IEEE, 2011.

[10] G. K. Patnaik, M. M. Gore,“Trustworthy Path Discovery in MANET - A Message Oriented Cross-correlation Approach”, IEEE, 2011.

[11] Mr. Susheel Kumar, Vishal Pahal, Sachin Garg, “wormhole attack in MANET: A review”. IRACST – Engineering Science and Technology: An International Journal (ESTIJ), Vol. 2, No. 2, April 2012.

[12] Mr. Sauabh Upadhyay, Aruna Bajpai,"Avoiding and preventing the wormhole attacks in MANET using statistical analysis approach”, International Journal on Cryptography and Information Security (IJCIS), Vol. 2, No. 1, March 2012.

[13] Ms. Monika, Jyoti Thalor,"Wormhole Attack Detection and Prevention Technique in Mobile Ad Hoc Networks: A review”. International Journal of Advanced Research in Computer Science and Software Engineering Vol. 3, Issue 2, February 2013, pp. 137-142.

[14] T. Sakthivel, R. M. Chandrasekaran,“Detection and Prevention of Wormhole Attacks in MANETs using Path Tracing Approach”, European Journal of Scientific Research, Vol. 76, No. 2, 2012, pp. 240-252.

[15] Shalini Jain, Dr. Satbir Jain,“Detection and prevention of wormhole attack in mobile adhoc networks”, International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010, pp. 78-86.

[16] S. Madhavi, K. Duraiswamy,“WAS-DP: Wormhole Attack in SAODV-Detection and Prevention”, European Journal of Scientific Research, Vol. 77, No. 4, 2012, pp. 560-569.

[17] Revathi Venkataraman, M. Pushpalatha, T. Rama Rao, Rishav Khemka,“A Graph-Theoretic Algorithm for Detection of Multiple Wormhole Attacks in Mobile Ad Hoc Networks”, International Journal of Recent Trends in Engineering, Vol. 1, No. 2, May 2009, pp. 220-222.

[18] Xu Su, Rajendra V. Boppana,“Mitigating Wormhole Attacks using Passive Monitoring in Mobile Ad-Hoc Networks”, IEEE Conferences, 2008, pp. 1-5.

[19] Issa Khalil, Saurabh Bagchi, Ness B. Shroff, “MOBIWORP: Mitigation of the wormhole attack in mobile multihop wireless networks”, Ad-Hoc Networks, 6, 2008, pp. 344–362.

[20] V. Singla, A. Kumar, R. Singla,“CBR and TCP based Performance Comparison of Various Protocols of MANET: A Review”, National Journal on Advances in Computing and Management, Vol. 1, No. 2, October 2010.

[21] R. H. Cheng, T. K. Wu, C. W. Yu,“Highly Topology Adaptable Ad Hoc `Routing Protocol with Complementary Preemptive Link Breaking Avoidance and Path Shorting Mechanisms”, Springer, 2010.

[22] A. Hinds, M. Ngulube, S. Zhu, H. A. Aqrabi,"A Review of Routing Protocols for Mobile Ad-Hoc Networks (MANET)", International Journal of Information and Education Technology, Vol. 3, No. 1, February 2013.

[23] M. Azer, S. E. Kassas, M. E. Soudani,"A Full Image of the Wormhole Attacks towards Introducing Complex Wormhole Attacks In wireless Ad Hoc Networks", International Journal of Computer Science and Information Security, Vol. 1, No. 1, May 2009.

[24] Jakob Eriksson, Shrikant V. Krishnamurty, Michalis Faloutsos 2006,"True link: A Practical Countermeasure to the Wormhole Attack in Wireless Networks" 14th IEEE International Conference on Network Protocols pp. 75-84.

[25] Ankita Gupta, Sanjay Prakash Ranga,"WORMHOLE DETECTION METHODS IN MANAT", International Journal of Enterprise Computing and Business System, 2012.

[26] Guoxing Zhan, Weisong Shi, Julia Deng,"Design and Implementation of TARF: A Trust Aware Routing framework for WSNs" IEEE Transactions for Dependable and Secure Computing, Vol. 9, Issue 2, pp. 184-197, 2012.

[27] Phuong Van Tran, Le Xuon Hung, Young-Koo Lee, "Mechanism to Detect Wormhole attacks in Mobile Adhoc Networks", Wireless Sensor Network Track at IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas USA, Jan 11-13-2007.

[28] Meghdadi M, Suat Ozdemir, Inan Guler,"A survey of Wormhole based attacks and Their Countermeasure in Wireless Sensor Networks", Vol. 28, pp. 89-102, 2012.

Mahendra Dhole received his B.E. degree in Computer Science from RGPV University and Vikrant Institute of Technology and Management, Indore, India, in 2013. Now he is persuing in M.Tech. Final Semester in Computer Science from RGPV University and TRUBA Collage of Engineering and Technology, Indore, India and his Research topic is "Detection of Hidden Tunnel Attack in Mobile Ad Hoc Networks". His other research interests include Software and Web Development and Data Mining techniques.