Quest Journals
Journal of Electronics and Communication Engineering Research
Volume 2 ~ Issue 6(2014) pp: 07-16
ISSN(Online) : 2321-5941
www.questjournals.org

Research Paper

Worm Hole Attack Detection and Prevention Mechanism For Mobile Adhoc Network

Deepesh Namdev[1], Shikha Singhal[2]
[1]*HOD cum Associate Professor (E&C, EE), Gurukul Institute of Engg. & Technology, Kota (Raj), India*
[2]*Student of Gurukul Institute of Engg. & Technology, Kota (Raj), India*

Received 07 July, 2014; **A**ccepted 31 July, 2014 © The author(s) 2014. Published with open access at **www.questjournals.org**

ABSTRACT- *In Mobile Ad Hoc Network security plays an important role when data transmission is performed within un-trusted wireless environment. There are various kinds of attacks like Black Hole, White Hole, Gray Hole, Wormhole and many more have been identified & corresponding solution have been proposed. All these attacks are caused by the malicious node hence ad wireless network is unprotected from the attacks of the malicious node. Out of all these attacks the wormhole attack is harmful attack in which two or more malicious nodes create a virtual tunnel in the network. There are two types of wormhole attacks have been identified: Hidden attack and Exposed attack. For both types of attacks many detection mechanisms or algorithms are proposed by the researchers. In this paper we also proposes a mechanism and also gives a appropriate solution.*

Keywords – *MANET, Routing, Security Attacks, wormhole*

I. INTRODUCTION

Wireless Mobile ad hoc network is an infrastructure less network & dynamic in nature. An infrastructure network does not have any fixed infrastructure for the communication. Each node in such type of network can communicate directly with other nodes in the network & there is no requirement of any centralized network access point. An important thing about these types of networks is that these networks do not have any routers but the wireless nodes work as a routers & a host. These networks don't have any fixed or static topology [1] [2].

A mobile ad hoc network consists of mobile nodes that use wireless transmission for communication. In these type of networks the nodes are movable and the motion of nodes may be random or periodical [3]. Due to node mobility nature of nodes, the nodes have limited battery power & limited bandwidth.

In absence of centralized access point or administrator the source & destination communicate through multiple hops [2]. The MANET is also called a multi hop wireless network. A MANET is an autonomous collection of mobile nodes or users [4].

1.1 MANET VULNERABILITIES:

Weakness in security system is called vulnerability. An ad hoc network may be vulnerable to unauthorized access because the system does not verify a user's identity before allowing data access. Wireless MANET is more vulnerable than wired network. Some of the vulnerabilities are given below [5]:-

1 Absence of centralized management: Wireless MANET does not have any centralized monitor or management server or node. The absence of centralized management makes difficult to detect any type of attacks because it is not easy to monitor or manage the traffic in a highly dynamic and large scale MANET.

2 Scalability: Mobility nature of nodes in the ad hoc network is responsible for changing network topology all the time. So that in ad hoc network scalability is a major issue concerning security.

3 Cooperativeness: In MANET we assume that all nodes are cooperative and non-malicious because when data transfers from source node to destination node is performed all intermediate nodes between source and destination take part in data transfer. Due to this a malicious attacker can easily disrupt network operation.

4 Dynamic topology: Dynamic topology of MANET may disturb the trust relationship among nodes.

5 Limited power supply: All nodes in MANET are considered as a restricted power supply, which causes several problems. A node in MANET may behave like a selfish node, when node is finding that it has limited power supply.

6 Adversary inside the Network: The nodes in MANET are free to join or leave the network due to this topology of network changes dynamically. The nodes inside MANET also behave like malicious node. So it is very difficult to detect malicious node within the network. The internal attacks are more dangerous than external attack.

7 Undefined Boundaries: The MANET is infrastructure less network so we cannot define a physical boundary of the network. The nodes in MANET are free to join or leave the network due to this time to time physical boundary of the network are also changed.

1.2 Security Goals:

In MANET, routing and packet forwarding, are performed by nodes itself in a self-organizing manner. So it is a reason why ad hoc network is very challenging against security attacks. Points below indicate that existing MANET is secure or not [5, 6, 7]:

1 Availability: Availability means the data and services are available for authorized parties or nodes at appropriate times.

2 Confidentiality: Confidentiality means the data and services are accessed only by authorized parties or nodes at appropriate time. Maintaining confidentiality of the data and services, we require that the data and services are secret from all entities that do not have privilege to access them. Confidentiality is also defined as a secrecy or privacy.

3 Integrity: Integrity means data can be modified only in authorized way by authorized parties. Modification includes creating, writing, deleting and changing status. Integrity means the message received is same as it transferred or received message is not corrupted.

4 Authentication: The surety that the traffic you receive is sent by authorized parties. Authenticity means the authenticate user can produce a message that will decrypt properly with the shard key at receiver end.

5 Non repudiation: Non repudiation means the sender and receiver of a message cannot deny that they have ever sent or received such a message.
6 Authorization: Authorization means different access rights are given to different types of users.
7 Freshness: When malicious node capture a packet it does not resend previously captured packets.
8 Access control: Access control means protects unauthorized access of data and resources.

II. SECURITY ISSUES

Wireless Mobile Ad hoc networks are vulnerable to various attacks not only from outside attack but also from inside attacks (attacks within the network itself). In Ad hoc network mainly two different levels of attacks are discussed.
First level – based on the mechanisms of the ad hoc network called routing.
Second level – based on to damage the security mechanisms employed in the network.
The security attacks in MANETs are divided into two major types [7].

2.1. Passive attacks: In passive attack the attacker does not have permission to alter the data when data transmitted within the network. But attacker listen the network traffic. Passive attacker does not disrupt in the network but it attempts to find out important information from network traffic. It is very difficult to detect passive attack because passive attacker only listen the network traffic and it does not make any harm in the data. The proper solution to overcome such type of attacks is that user can use encryption algorithms for data encryption.

2.2 Active Attacks: Active attacks are very harmful attacks on the network. In Active attack attacker make unauthorized access on data as well as make changes such as modification of packets, DoS, congestion etc. in the data when data transmitted in the network. There are two types of active attack:

Active external attacks: this type of attack is performed by outsider source which do not belong to network.
Active internal attacks: this type of attack is performed by malicious nodes which belong to network.

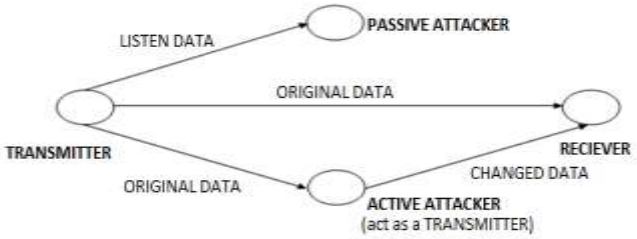

Fig 1: Active and Passive attacks in MANET

Generally active attacks are classified into four major groups:

1. Dropping Attacks: When source node has a packet for destination node then it select one of the route for sending packet. The route has selfish node which silently drop all packets and do not forward packets towards destination node .Due to this dropping attacks can stop end-to-end communications.
2. Modification Attacks: In modification attacks, the malicious nodes modify the packet and due to this it disrupts the whole communication between nodes. Sinkhole attack is the best example for modification attacks.
3. Fabrication Attacks: In fabrication attack, the attacker node send fake message to all its neighbors nodes without receiving any related message. When neighbors node request for route to destination then the attacker node can also send fake route reply message to all its neighbors.
4. Timing Attacks: In timing attacks, the attackers attract other nodes by advertising itself as a node closer to the destination node.

III. BACKGROUND

In MANET each node takes part in route decision to forward the packet, so it is very easy for malicious nodes to attack on MANET. In network layer attacks, the attackers inject itself in the active path from source to destination and also analyze the traffic flows between source node to destination node and harm the network operations. There are several network layer attacks performed by malicious nodes. Some network layer attacks are discussed below:

A. Black hole Attack:

Black hole attack is also called packet drop attack or it is a type of denial-of-service attack. Black hole define as a place in the network where all incoming traffic is silently dropped by malicious node, without informing to the source node. Black Hole attacks effects the packet delivery between nodes and also reduce the routing information available to the other nodes [8].

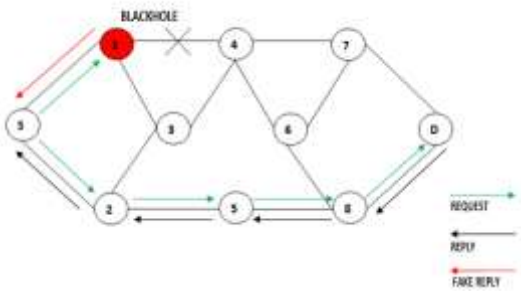

Fig 2: Black hole Attack

B. Rushing Attack:

These types of attacks corrupt the route discovery process. In rushing attacks when source node has data to transmit then it perform route discovery process from source to destination. When source node broadcast RREQ packet for finding optimal route, so packet travel through many intermediate nodes and when RREQ packet received by malicious node then it increases the transmission speed of RREQ packet by which packet forwarded by malicious node reaches first to destination node as compare to other nodes. At the same time malicious node keep copy of forwarded packet for future use and frequently forward copied packet to destination node by which destination node will be busy in receiving packet from malicious node. Figure below

shows the rushing attacks in the network, in the figure the S and D are source and destination respectively, attackers is NODE 4 called malicious node quickly broadcast the RREQ packet to ensure destination node that RREQ packet from itself arrive earlier as compare to other node. [9]

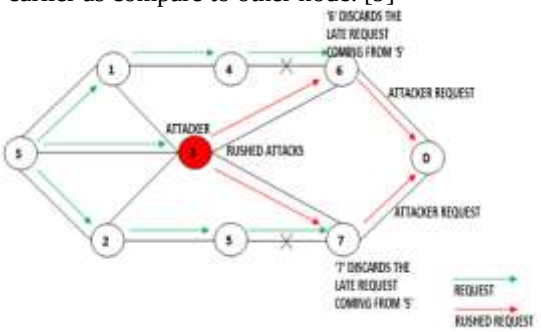

Fig 3: Rushing Attack

C. Wormhole Attack:

In wormhole attack, malicious node receive packet at one location in the network and tunnels them to another malicious node at another location. The tunnel exist between two malicious nodes is called wormhole. Attackers use wormholes in the MANET to make their nodes appear more attractive so that more traffic flow through their nodes. Figure.4 shows the wormhole, the nodes "2" and "7" are malicious node that forms the tunnel in MANET. The source node "S" when initiate the RREQ packet to find the route to destination node "D". The source node "S", forwards the RREQ packet to their respective neighbors "1" and "2". The node "2" when receive the RREQ packet it immediately share it with node "7" and later node "7" initiate RREQ to its neighbor node "D", through which the RREQ packet is delivered to the destination node "D". Due to high speed link, it forces the source node to select route <S-2-7-D> for destination. It results in "D" ignores RREQ that arrives at a later time and thus, invalidates the legitimate route <S-1-4-6-D>.[10][11][12][13]

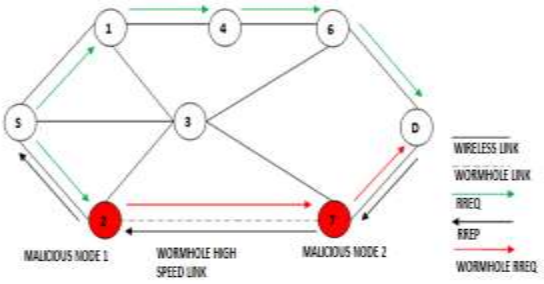

Fig 4: Wormhole Attack

D. Sinkhole Attack:

In sinkhole Attack, a malicious node advertises wrong routing information to produce itself as a specific node and receives whole network traffic. When malicious node receives whole network traffic then it modifies the secret information, such as changes made to data packet or discards them to make the network complex. A malicious node tries to collect all secure data from all its neighbor nodes. Due to this Sinkhole attacks affects the performance of MANET protocols. In this way the path presented through the malicious node appears to be the best available route for the nodes to communicate. Figure below shows the sinkhole attack. [5]

E. Replay Attacks:

In replay attack, a malicious node record control messages of other nodes and resends them later when needed. A replay attack is a form of network attack in which a valid data transmission is maliciously repeated or delayed. This is can be done by malicious nodes. These replay attacks are later misused to disturb the routing operation in a MANETs. [5]

F. Resource Consumption Attack:

In resource consumption attack, a malicious node can attempt to consume battery life by requesting excessive route discovery, or by forwarding unnecessary packets. These types of attacks are also called sleep deprivation attack.

IV. Wormhole Attack in MANET

Ad hoc networks are vulnerable to many attacks due to many reasons such as: wireless links between nodes, the absence of infrastructure, the Lack of a centralized monitoring or management, limited physical Protection, and the resource constraints. A particularly security attack which is called the wormhole attack, has been introduced in the ad-hoc networks [11], [12], [13]. In such type of the attack, a malicious node captures packets from one location in the network and tunnels the captured packets to another malicious node at another location, which replays them locally. This is shown in Fig 5.

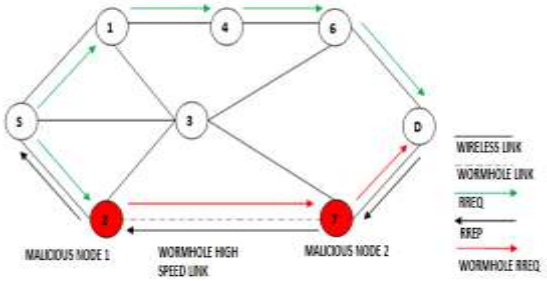

Fig 5: Wormhole Attack in Ad Hoc Network

A.Wormhole Attack Classification:

In a wormhole attack, two attackers work together. One receives the packets at one location in the network, tunnels the packets to its partner at another location in the network, and then the partner replays them into the network. There are two kinds of wormhole attacks. In the first type, malicious nodes hide the fact that they forward a packet, meaning that, legitimate nodes do not know their participation in packet Forwarding. In the second type, legitimate nodes are aware of the fact that the malicious nodes are forwarding packets; just do not know they are malicious. For the case of discussion, we refer the first type as hidden attack while the second types as exposed attack [11], [14], [15].

1. Hidden wormhole Attack:

The attackers do not modify the content of the packet and the packet header, even the packet is an AODV advertisement packet. Instead, they simply tunnel the packet from one point and reply it at another point. This kind of wormhole attacks makes the sender treat the receiver as its immediate neighbour [15]. As shown in fig. 6 the packet from S is received by M1, then M1 tunnels the packets to M2 and replies them to R, without modifying the packet header. Since M1 and M2 do not include themselves in the header, what R will find is that the pervious hop is S. the same observation can be obtained in the reverse path, such that S finds R as its immediate neighbour, and the path found is {S, R}.This is obviously not correct since S and R are Separated by node M1, node M2 and other node that are in the tunnel.

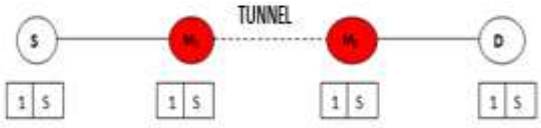

Fig 6: Hidden Wormhole Attack

2. Exposed Wormhole Attack:

In this kind of attacks, the attackers do not modify the content of the packet, but include themselves in the packet header following the route setup procedure. Other nodes are aware that the malicious nodes lie on the path but they would think that the malicious nodes are direct neighbours. Let's consider the situation where S wants to establish a route to R. As illustrated in Fig. 7, when M1 receives the packet, it modifies the pervious hop field to M1 and increases the hop count by 1. Then the RREQ packet is tunnelled to M2 and M2 performs the same setup procedure and broadcasts the RREQ packet to receiver R. Receiver R finds its previous hop is M2 with hop count equals to 3. The same thing happens in the reverse path. When S receives the RREP packet, it finds its pervious hop is M1 with hop count equals to 3. And the route is setup as {S, Ml, M2, R} [15].

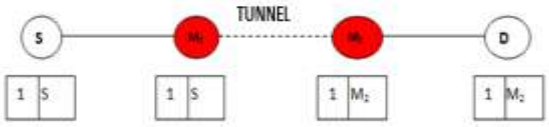

Fig 7: Exposed Wormhole Attack

A. **Wormhole Attack Modes:**

There are four wormhole attacks mode in ad hoc network [11], [14].

1. Wormhole Using Encapsulation:

In this mode a malicious (first Party) node hears the RREQ packet at one location in the network and tunnels it to another malicious (Second party) node at another location near the destination. The second party again rebroadcasts the RREQ packet. The neighbours of the second party receive the RREQ packet and drop any further legitimate requests that may arrive later on legitimate multi hop paths. Then the result is that the routes between the source and the destination go through the two malicious nodes that will be formed a wormhole between them. For example, consider Fig. 8 [13] Which shows Wormhole attack through Packet Encapsulation.

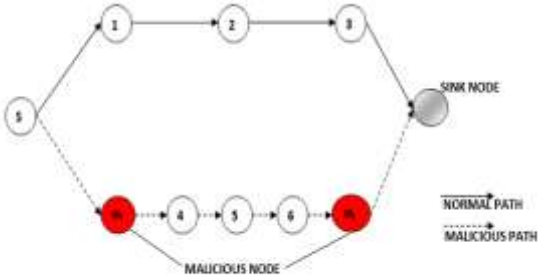

Fig 8: Wormhole Attack through Packet Encapsulation

2. Wormhole Using Out-of-Band Channel:

Out of Band Channel can be achieved by using a long range directional wireless link or a direct wired link. As compare to previous attack it is difficult to launch such mode of attack because it needs specialized hardware capability. For Example in Fig. 9 ,[13].

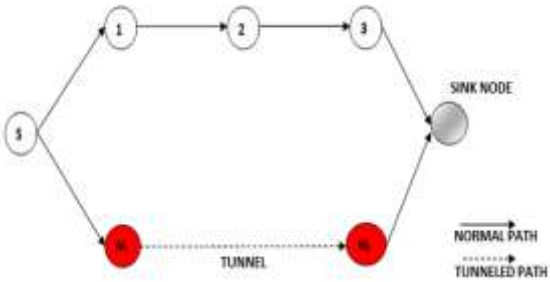

Fig 9: Wormhole Attack Through Out-of-Band Channel

3. Wormhole With High Power Transmission:

In this mode, when a single malicious node gets a RREQ, malicious node broadcasts the RREQ at a high power level so the malicious node increases its chance to be in the routes established between the source and the destination even without the participation of a another malicious node as compare to another nodes because other node does not have such high power level. For example fig. 10:

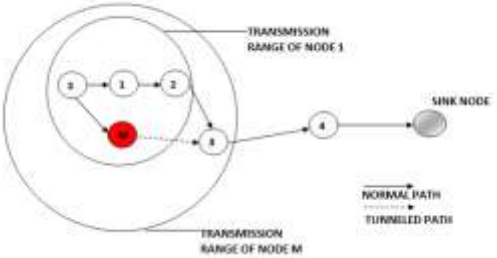

Fig 10: Wormhole Attack Through High Power Transmission

4. Wormhole Using Packet Relay:

Wormhole using packet relay is another mode of wormhole attack. In packet relay two malicious nodes relay packet between two nodes which are far apart from each other and convenience these nodes that they are neighbour.

V. RELATED WORK

A. In [16]Yih-Chun Hu, Adrian Perrig and David B. Johnson proposes a detection and prevention method in which there are basically two types of packet leashes:

1. GEOGRAPHICAL LEASHES
2. TEMPORAL LEASHES

Leash is a type of information that is added to a packet designed to restrict the packets maximum allowed transmission distance.

- Geographical Leashes: In Geographical Leashes the recipient of the packet is within a certain distance from the sender of the packet. For construction of geographical leash, each and every node must know its own location and all nodes must have loosely synchronized clocks. Use of geographical leash, when a sending node send a packet, it include its own location, p_s and the time at which it send a packet, t_s. When receiver node of the packet receives the packet the receiving node compares the values (p_s and t_s) to its own location, p_r and the time at which it received the packet, t_r. If the clocks of sender and receiver are synchronized to within $\pm \Delta$, and v is an upper bound on the velocity of any node, then at receiver end, the receiver can compute an upper bound on distance between sender and itself (receiver), d_{sr}. Which is based on the timestamp t_s (sending time of packet), t_r (time at which packet is received), δ (maximum relative error in location information), p_s (location of sender node) and p_r (location of receiver node).

$$d_{sr} \leq \| p_s - p_r \| + 2\, v.(t_r - t_s + \Delta) + \delta$$

Digital Signature scheme or some other authentication technique can be used to allow a receiver to authenticate the location and timestamp in the receiver packet.

- Temporal Leash: In temporal leash the packet has an upper bound on its lifetime, by which a packet is restricted to travel maximum distance, since the packet can travel at most at the speed of light.

For construction of temporal leash, all nodes must have tightly synchronized clocks. The maximum difference between any two nodes clocks is Δ. The value of the parameter Δ must be known by all nodes in the network. For temporal leashes the value of Δ must be on the order of few microseconds or even hundreds of nanoseconds. The level of time synchronization can be achieved by hardware such as LORAN-C, WWVB, GPS etc. Some other hardware such as cesium-beam clocks, rubidium clocks and hydrogen maser clocks are also be used for sufficiently accurate time synchronization for months. Use of temporal leash, when a sending node send a packet, it includes the time at which it send the packet, t_s. When receiver of packet receives the packet, the receiving node compares this value (t_s) to the time at which receiver node receives packet, t_r. At the receiver end the receiver is able to detect, if the packet traveled to far, based on clamed transmission time and the speed of light.

Advantage of geographical leashes over the temporal leashes is that the time synchronization is looser and another advantage is that geographical leashes uses the concept of digital signature scheme for successful secure delivery of packet at receiver end.

B. In [17] San Diego proposes a detection and prevention method in which Directional antenna system are used in ad hoc network for increasing the capacity and connectivity of ad hoc networks. Transmission of packet in particular direction gives a higher degree of spatial reuse of the shared medium. Directional antenna transmission system uses energy more efficiently. As compare to omnidirectional antenna, the transmission range of directional antennas is usually larger; which can reduce the number of hops in routing. Using directional antennas can increase spatial reuse and reduce packet collision and negative effect such as deafness. The directional antenna model assumes an antenna with N zones. Each and every zone has a conical shape or 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 may collectively cover the whole plane as shown figure below:

When a node is idle, in this condition the node listens the carrier in omni mode. When idle node receives a message, it determine the zone on which the received signal power in maximal and the node uses that zone to communicate with sender.

In directional antennas approach first protocol is Directional Neighbors Discovery, second protocol is to Verified Neighbor Discovery and finally Strict Neighbor Discovery will be performed.

C. Hon Sun Chiu and King-Shan Lui.In [15] Hon Sun Chiu and King-Shan Lui proposes a detection and prevention method in which, if mobile ad hoc networks, data transmission is performed within an untrusted

wireless environment. Different various kinds of attack have been identified and corresponding solutions have been proposed. Wireless Wormhole attack is one of the serious attacks which form a serious threat in the wireless networks, mainly against many ad hoc wireless routing protocols and location- based wireless security system. Generally we identify two types of wormhole attacks. In first type of attack, malicious nodes do not take part in finding routes, means legitimate nodes do not know their existence. In second type of attack, malicious nodes do create route advertisements and legitimate nodes are aware of the existence of malicious nodes, but legitimate node does not know they are malicious. Many researchers have proposed detection mechanisms for the first type. In this paper, author proposes an efficient detection method called Delay Per Hop Indication (DelPHI). By observing the delays of different paths to the receiver, the sender is able to detect both kinds of wormhole attacks. This method requires neither synchronized clocks nor special hardware equipped mobile nodes. The performance of the DelPHI is justified by simulations.

In this paper, author described an efficient algorithm for detecting wormhole attack in mobile ad hoc networks. We call it Delay Per Hop Indication (DelPHI). The advantages of DelPHI are that it does not require clock synchronization and position information, and it does not require the mobile nodes to be equipped with some special hardware's, thus it provides higher power efficiency. The performance of DelPHI has been evaluated by conducting various simulations using the ns simulator. It has been shown that DelPHI can achieve higher than 95% in detecting normal path and 90% in detecting wormhole attack, in the absence of background traffic. Simulations has also shown that DelPHI can maintain above 85% detection rate for both normal and tunneled paths given that there is background traffic. The message overhead of DelPHI has also been addressed in this paper. We compared it with AODV route setup procedures and found that the major factor is the triple request procedures in providing reliability. There is a trade off between providing reliability of DelPHI and minimizing the message overhead, and may need further investigation.

D. In [18] Tran Van Phuong, Ngo Trong Canh, Young-Koo Lee, Sungyoung Lee, and Heejo Lee proposes a detection and prevention method, in this mechanism when source node establishes a route to another node called destination, this mechanism will try to check whether there is wormhole link in the route or not by calculating round trip time between two successive nodes along the route. Each and every node in the established route will compute the Round Trip Time (RTT) between it and the destination and then send these values back to the source node. The source node collects all of these RTT values from different routes and calculates RTT's between two successive nodes of different routes and identify wormhole attack based on the fact that the RTT between two malicious or FAKE neighbors will be considerably higher than the two real neighbors.

E. In [19] Adel Saeed Alshamrani proposes a detection and prevention method, in this mechanism initially uses the same process of calculating the RTT's which we were already learn in transmission between two successive node (TTM) mechanism. In this mechanism the author adds some alteration when it is needed. The author's proposed mechanism is called Packet Travel Time (PTT), which is used to monitor all transmitted packets in the network. In this mechanism after forwarding the RREQ packet, each node will record the sending time (t_s) and save sending time (t_s) value in memory and also all nodes will record the time when it overhears its neighbor rebroadcast the RREQ packet (t_h). Further each node calculate the PTT value ($PTT=t_h-t_s$) and each node save the PTT value until it receives the RREP and append PTT value in the special part which is created by the destination. When source node receives the RREP, source node will make the calculation to obtain the RTT between every two successive nodes by the same process that has been discussed in TTM and then these values will be compare with the values of PTT's and find if there is any wormhole link in the route.

TABLE

Table below shows the sending and receiving time values of all nodes received by Source node and the calculation done by the source node:

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 values of PTT's will be received at source node

NODES	RREQ Sending Time	RREQ 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**	**-**	**-**

VI. PROBLEM

In Mobile Ad Hoc Network security plays an important role when data transmission is performed within un-trusted wireless environment. There are various kinds of attacks like Black Hole, White Hole, Gray Hole, Wormhole and many more have been identified & corresponding solution have been proposed. All these attacks are caused by the malicious node hence ad hoc wireless network is unprotected from the attacks of the malicious node. Out of all these attacks the wormhole attack is harmful attack in which two or more malicious nodes create a virtual tunnel in the network. There are two types of wormhole attacks first one is Hidden attack and second one is Exposed attack.

For both types of attacks many detection mechanisms or algorithms are proposed by the researchers. But the existing methods have some drawbacks.

The mechanisms DELPHI proposed by Hon Sun Chiu and King-Shan Lu [], able to tackle the both the wormhole attacks by calculating delay or hop value to serve as the indicator of detecting wormhole attacks.The DelPHI method avoids the need of synchronization & it does not require any special hardware there for it provides higher power efficiency but it has some drawbacks such as reliability & message overhead.

The another mechanism PTT: Packet Travel Time algorithm in Mobile Ad-hoc networks proposed by Adel Saeed Alshamrani [], also able to tackle both the wormhole attacks by calculating RTT (Round Trip Time) between two succesive nodes and PTT(Packet Travel Time). But this mechanism has some drawback like requires clock synchronization, calculating RTT of two successive nodes and observe the RREQ packet forwarding of its neighbours for calculating PTT.

In this paper we proposed a method which overcomes all above drawbacks.

VII. PROPOSED SOLUTION

In our proposed solution, First of all we will find out the Time to Leave (TTL) values and the same time we will also find out the hop count values between source nodes to destination node of each and every route. After finding the values of TTL & Hop Count we will find out the Delay per Hop (DPH) values of each & every route by using the values of TTL & Hop Count. After finding the value of DPH we will check the energy of each and every node previous to destination node.

1. Calculating of TTL: When source node calculates the value of TTL of every route from source node to destination node it generates RREQ packet marked with R flag, set Ts field (Sending Time of RREQ packet) & hop count is equal to zero initially & forward the RREQ packet to its all neighbors to establish a route. Neighbors node receives an RREQ packet, increases hop count value by one & forward RREQ packet to its neighbors. When the destination node receives RREQ packet it generates an RREP packet marked R flag to RREP flag, set hop count is equal to zero initially & forward the RREP packet to its all neighbors in reverse or backward route (route from destination node to source node).

Neighbors node receives an RREP packet, increases hop count value by one & forward RREQ packet to its neighbors in reverse direction.

Source node receives two or more RREP packets from different routes & calculates the Time to Leave (TTL) value of each & every route.

TTL=Tr-Ts, Where Tr is receiving time of RREP packet & Ts is sending time of RREQ packet.

2. Hop Count: When source node receives two or more RREP packets from different routes it gets the hop count value of every route.

3. Calculation of Delay per Hop(DPH): When source node gets the value of TTL & Hop Count it calculates the DPH(Delay Per Hop) value of each & every route by given formula DPH=TTL/2*Total Hop Count

4. Energy checking of nodes previous to destination: Now source node sends energy check packet through every route towards destination node & calculate the energy of last three nodes previous to destination node in each routes.

VIII. CONCLUSION

In ad hoc network wormhole attacks can degrade network performance significantly and harms the network security. Wormhole attacks detection is quite complicated. In this paper, we described types of security attacks. After describing security attacks, we discussed the existing wormhole detection techniques. Finally, by analyzing the advantages and disadvantages of all the existing techniques, we proposed an algorithm to detect wormhole attack in ad hoc networks.

Acknowledgement

First and foremost I would like to thank my parents for their support and to my guide Mr. Rakesh Verma for his valuable guidance and advice. Next I wish to express my sincere thanks to college authority. Finally special thanks to my friends for their support in completing this paper.

REFRENCES

[1]. A h highly topology adaptable ad hoc routing protocol with complementary preemptive link breaking avoidance and path shorting mechanisms Springer 2010.
[2]. K.A.Shah,M.R.Gandhi , "Performance Evaluation of AODV Routing Protocol with Link Failures" 978-1-4244-5967-4/10/ IEEE in 2010.
[3]. An efficient algorithm for detection of black hole attack in AODV based MANETs IJCA march 2013.
[4]. Distributed wireless links repair for maximizing reliability and utilization in multicast MANET IEEE 2008.
[5]. Priyanka Goyal, Vinti Parmar, Rahul Rishi," ApplicationMANET: Vulnerabilities, Challenges, Attack", IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011 ISSN (Online): 2230-7893.
[6]. Amandeep Kaur, Hardeep Singh," A Study of Secure Routing protocols", *International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 2, Issue 2, February 2013 ISSN 2319 – 4847.*
[7]. Gagandeep, Aashima, Pawan Kumar ," Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.
[8]. Puneet Kansal, Nishant Prabhat and Amit Rathee, "Black hole attack in Manet", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 3, March 2013 ISSN: 2277 128X.
[9]. ALshahrani, Abdullah Saad "Rushing Attack in Mobile Ad Hoc Networks" 978-0-7695-4579-0/2011 IEEE.
[10]. Ritesh Maheshwari , Jie Gao, Samir R das "Detecting Wormhole Attacks in Wireless Networks"1-4244-0732-x/2006 IEEE.
[11]. Pallavi Sharma, Aditya Trivedi, "An Approach to Defend Against Wormhole Attacks in Ad Hoc Network using Digital Signature". IEEE ISSN 978-1-61284-486-2/2011.
[12]. Reshmi Maulik and Nabendu Chaki, "A Study on Wormhole Attacks in MANET" International Journal of Computer Information Systems and Industrial Management Applications ISSN 2150-7988 Volume 3 (2011) pp. 271-279.
[13]. E.A. Mary Anita, V. Thulasi Bai, "Defending Against Wormhole Attacks in Multicast Roruting Protocols for Mobile Ad Hoc Networks" 978-1-4577-0787-2/2011 IEEE.
[14]. Marianne Azer, Sherif EI-Kassas, Magdy EI-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, IJCSIS Vol. 1, No. 1 May 2009.
[15]. Hon Sun Chiu and King-Shan Lui. "DelPHI Wormhole detection Mechanism for Ad Hoc Wireless Networks" 0-7803-9410-0/06.IEEE 2006.
[16]. Yih-Chun Hu, Adrian Perrig and David B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks", 0-7803-7753-2/03/IEEE in 2003.
[17]. Lingxuan Hu and David Evans, "Using Directional Antennas to Prevent Wormhole Attacks", In Network and Distributed System Security Symposium (NDSS 2004), San Diego, California, USA. February 2004.
[18]. Tran Van Phuong, Ngo Trong Canh, Young-Koo Lee, Sungyoung Lee, and Heejo Lee, "Transmission Time-based Mechanism to Detect Attacks", 0-7695-3051-6/07/ IEEE in 2007.
[19]. Adel Saeed Alshamrani, "PTT: Packet Travel Time Algorithm in Mobile Ad Hoc Networks", 978-0-7695-4338-3/11 / IEEE in 2011.