Journal of Theoretical and Applied Information Technology
30th June 2013. Vol. 52 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AN OVERVIEW ON WORMHOLE ATTACK DETECTION IN AD-HOC NETWORKS

MOJTABA GHANAATPISHEH SANAEI[1], BABAK EMAMI ABARGHOUEI[2], HADI ZAMANI[3], MIRANDA DABIRANZOHOURI[4]

[1234]Faculty of Computer Science and Information System

Universiti Teknologi Malaysia (UTM), Johor 81310, Malaysia

E-mail: [1]ghanaatpisheh.m@gmail.com , [2]emami.babak@gmail.com , [3]hadii.zamani@gmail.com , [4]mirandabiran@gmail.com

ABSTRACT

An ad-hoc network is a group of wireless mobile nodes that shapes a temporary network without any infrastructure and centralized management. Each mobile node functions not only as base station but also as router forwarding packets for other mobile nodes in the network. One of the dangerous attacks in an Ad-hoc network is named wormhole attack which two or more destructive nodes record the packets at one point, and transmits them by a wired or wireless to another point in the network. Wormhole attack is so strong and detection of this attack is hard. Also, the wormhole attack may cause another type of attacks like Sinkhole or Select forwarding. Using a cryptographic technique is not enough to prevent wormhole attack. In this paper we are going to review some methods in wormhole detection and investigate the weaknesses and strengths of the methods.

Keywords: *Wormhole Attack detection, Wireless Ad-hoc Networks, prevention of wormhole attack, Mobile Ad-Hoc Network*

1. INTRODUCTION

Nowadays, by developing new technologies in the field of science, especially in Micro Electro Mechanical Systems (MEMS), applications of wireless sensors are increasing rapidly. Almost this application use in military and health monitoring proposes [1]. “Ad-hoc” is a Latin term that means “for this purpose”. This kind of network often used to define solutions that are expanded on-the-fly for a specific aim. Ad-hoc Networks are autonomous and decentralized wireless systems [2]. The nodes in Ad-hoc can be consisting of the systems or devices i.e. Mobile phone, laptop, Personal Digital Assistance (PDA), and a personal computer that is participating in the network. These nodes can act as host/router or both at the same time. Dynamic topology is the most important characteristics of Ad-hoc network caused by this nodes feature, flexibility and self-configuration feature also provided by this kind of behavior. By this ability, Ad-hoc network topology can be deployed urgently without any infrastructure.

Ad-Hoc networks are so flexible and every kind of communication between two and more nodes can be applied on it. For example if you want to send a file to your laptop friends, you can create a single session by an Ad-hoc network between your computer and your laptop’s friend to transmit the file. This work may be done using network cable or the wireless card to link with each other. If you need to transmit or share files with more than one workstation, you can launch a multi-hop ad hoc network, which could carry data over multiple nodes. Ad hoc network is a provisional network connection established for a specific object, such as sending data from one node to another node or one computer to one another.

Wireless Ad-hoc networks are involved three sub networks. Figure 1 shows the classification of wireless ad hoc network.

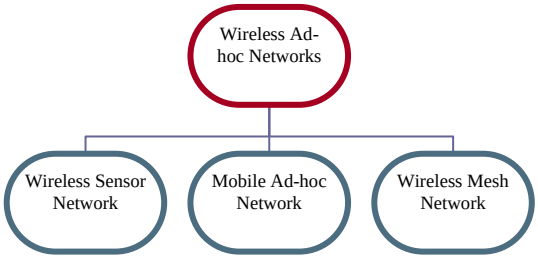

Figure 1: Classification of wireless Ad-hoc networks

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Wireless sensor network (WSN) is the first category. WSNs were firstly designed to facilitate military operations but today it's used for monitoring and recording the physical conditions of the environment and organizing, such as health, pollution levels, humidity, wind speed and direction, traffic, and many other consumer and industrial areas of collecting data at a central location [3].

Mobile Ad-hoc network (MANET) is the second parts of this category, it's a kind of ad hoc network, which can alter location and self-configure on the sky. MANET is mobile that use wireless link to connect to several networks [4]. MANET can be a standard Wi-Fi connection, like a cellular or satellite broadcast. Some MANETs are limited to a local area of wireless system, such as a group of laptops. A Vehicular Ad Hoc Networks (VANETs) is a kind of MANET that permits vehicles to connect with wayside [5].

The last portion of this category is Wireless Mesh Network (WMN). Mesh network made up through the link of wireless access points, which set at each local user's network. Every network user provides and forward data to the next node. Wireless mesh networking can let people living in faraway areas to connect their networks together for reasonable Internet links. Wireless mesh networks often involve gateways, mesh clients and mesh routers. In mesh network clients are often cell phone, laptops and other wireless devices, while the mesh network sends traffic to and from the gateways, do not need to connect to the internet. [6].

Wireless sensor nodes usually suffered from some limitation such as low power radios, short lifetime and limited memory; also the most secure algorithms that proposed for this issue are not perfect [7]. Generally, wireless sensor nodes are developed in an untrusted environment. For this reason security becomes one of the most important major in these small devices. Because of WSN limitation, providing the secure communication in an unreliable environment still is in challenging factor.

Node characteristics, dynamic topology without central monitoring system, provided different security threat on WSN routing protocol. Between all attacks, the wormhole is more dangerous than the other attack such as Sinkhole, Sybil attack, Selective forwarding attack, etc. because this type of attack does not need to compromise a sensor in the network and it can create the other type of attack easily.

2. WORMHOLE ATTACK

A wormhole is a kind of attack that typically happens with two or more malicious nodes in which the first malicious node eavesdrop or listen in packets at one location and then send them by tunnel to second malicious node in another area[8, 9]. Transferring the packets between these attackers can be done by using direct tunnel in wire/ wireless connection.

For example in Figure 2 the sender node (S) sends packets to destination node (D) through two ways; first by S, W1, W2, D and second by S, A, B, C, D. In first path the packet is sent to destination by five links that we call normal path (A-B-C-D) and the second path is wormhole link, which packet are sent to destination by three links (W1-W2-D). When the packets transmit through a node (W1), the data eavesdropped by the firs adversary node (W1) and tunneled the data to second malicious node (W2) and finally, W2 sends the packets to destination node (D) before they are arriving to node D from the normal path. So the destination node D dropped the packets that received from normal path.

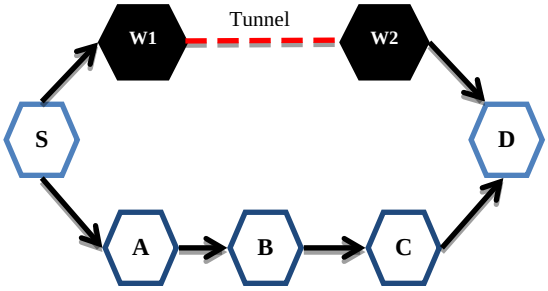

Figure 2: The simple model of wormhole attack

3. LITERATURE REVIEW

In quick view, wormhole attack is a kind of routing attack and in this paper tried to make quick comparisons between different current mitigation methods encountered with it. The common method for wormhole mitigation can be handed out in two main diversity; end to end detection by considering in extra devices on nodes as well as GPS (Geographic Position System), direct antenna and those methods which submitted on specific reading protocol.

3.1 Wormhole Detections by specialized hard-ware devices:

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.1.1 Geographical Leashes and Temporal Leashes

The overhead that is added to a packet designed in order to put a limitation on the packet's maximum allowed transmission distance is called leash. This method is divided into two categories such as geographic leashes and temporal leashes [10, 11, 12]. A geographic leash is based on this feature that the receiver of the packet is located within a certain distance from the sender, but a temporal leash is lifetime-oriented in which the maximum travel distance of each packet is restricted based on an upper bound on its lifetime.

3.1.1.1 Geographical Leashes

The geographical leash is a scheme that presented by Hu, Perrige and Johnson in 2003 to protect wireless Ad-hoc networks against one of the dangerous attack that called wormhole attack. It's a based on geographical leash that the receiver of the packets located in a specified distance from the source node. According to performance the geographical leash in Wireless Ad-hoc networks, should provide certain supplies that needed; for example: all nodes should (using GPS) to know itself location and every node must have loosely synchronized clocks to checking the time of sending. When the source node sends the packet to the destination node, the location (p_s) and the the sendert_s) of sender will be added to the header of the packet. After the packet received by destination node, the time (t_r) and the location (p_r) is compared by value of sender. In order to synchronized between two nodes, if the clock source and destination nodes are synchronized within ± Δ, thus, an upper bound distance between source and destination (d_{sr}) Is computed by the receiver.

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

In this formula (p_s) is location of sender, time of sender(t_s), location of receiver (p_r), time of receiver (t_r), light speed is (v)And maximum error that may be happened in finding location information that illustrated by (δ).

3.1.1.2 Temporal Leashes

Another scheme that is offered for avoiding of wormhole attack in sensor network is temporal leach; in this case we have an expiry time for each transmitted packet. The important element that should to consider is synchronized clock that every node must have a closely synchronizes clock. Most difference between any two nodes clock is shown by Δ. In this method the time is restricted and the sender of the packet should avoid broadcasting the packet more than distance L $(L_{min} = \Delta.c$, where the c is diffusion of light speed). The expiry time calculated $\left(t_e = t_s + \frac{L}{c} - \Delta\right)$by sender; before the packet is sent, the sender should to insert (t_e) to header of packet. Therefore, when the packet received by destination node, the time(t_r), is compared with the expiry time(t_e); if $(t_r > t_e)$ the packet is removed by receiver, also the receiver able to detect if the packet traveled too far, based on the claimed transmission time and the speed of light. In this method checking authentication of nodes is important requirements. Some techniques such as Hash-based Message Authentication Code (HMAC) and RSA authentication have problems; for these weaknesses, the TIK protocol is applied in temporal packet. TIK protocol is created base on TELSA that uses the symmetric cryptography. Similar a geographical lash, other authentication techniques such as digital signature can be used to authenticate a receiver.

The weaknesses of temporal leash using the TIK protocol, because TIK is not practical assumption. The synchronized time between every node in very difficult and delay can be a main problem with this method. So, for detecting wormhole attack these assumptions are a weak point.

3.1.2 An End to end Detection of Wormhole Attack in Wireless Ad-hoc Network (EDWA)

This method presented by Wang and Wong in 2007 that used end to end detection for identifying the wormhole attack in wireless Ad-hoc network, based on hope-count state to detect and prevent wormhole attacks in the DSR routing protocol. In this case our system needs some assumptions and requirements that should to consist, such as a set of mobile nodes that using radio transmission and bi-directional radio link between two nodes. Also each node must use Global navigation satellite system (GNSS) such as Global positioning system (GPS).Other assumptions is all nodes share pairwise secret keys or record authentic public key that established by key distribution scheme. We first describe the detection of wormhole by using estimate the shortest path length and then describe identifying the malicious nodes [13].

Journal of Theoretical and Applied Information Technology
30th June 2013. Vol. 52 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.1.2.1 Using Shortest Path Length Estimation to Detect Wormhole

After the destination node received the route request packet, it replays route request packet to sender. When a sender node received the packet, first checking the authenticity the packet, which came from destination node or not, then draw out the point of destination from the Route Request packet (RREQ); after that, the source node calculates the shortest path by using Euclidian distance model measure model. The distance between source and destination calculated by location of sender node(l_s), location of receiver(l_d) and the maximum relative error in location measurement is(δ). The below formula estimate minimum Euclidian distance between source and destination node:

$$d = \|l_d - l_s\| + \delta$$

The following notations specified our facilitated discussion:

d: Euclidean distance between a sender and receiver

l_s, l_d: Location of source and destination, respectively

δ: Estimate the maximum relative error in location measurement

As you can see in Figure 3, node A is one of the nearest nodes behind node S, also this node is the shortest Euclidean distance to reach the node D; therefore node A is chosen for delivery the packet through the shortest Euclidean distance to node D. According to position of nodes if the coordinates of node A be(x_a, y_a), in which x_i, y_i are arbitrary variables, so the formula for calculating the distance between nod A and D considered below:

$$e_a = \sqrt{(x_a - d)^2 + y_i^2}$$

Finally, the distance is calculated as:

$$E(e_A) = d - r \int_{d+r}^{d-r} \left(1 - P_{E_A}(e_A)\right)^{N\pi r^2} de_A$$

In order to above method, when $E(e_A)$ is calculated, it is easy to compute another node after node A. For instance for node B we can calculate $E(e_B)$ to estimate the distance.

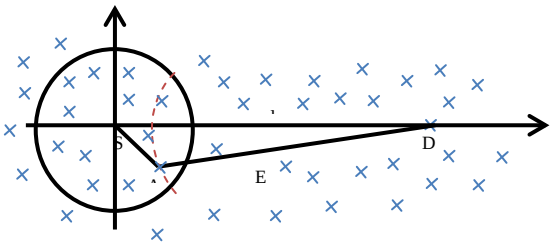

Figure 3: Estimate the first node of the shortest route

After the route replies were received by source nodes, it compares the hope counts of each route replay (h_r), with number of hope within the shortest path to destination(h_s). If $(h_r < h_s)$ so the wormhole happened during this path.

3.1.2.2 Using Shortest Path Length Estimation to Detect Wormhole

According to identify the tunnel between two or more malicious nodes, this method can help to find a wormhole. When the tracking packet send by destination node to source node thought the path, each intermediate node that belonging to path should receive the packet and transfer the Track response to the first node. The source node to identify the malicious node computes the shortest path to each intermediate node. After the shortest path selected by the source node, the sender transmits the packet to the destination from the trusted route. This situation will be performed, when the malicious node be diagnosed and be deleted from the path.

3.1.3 Defense scheme Against Wormhole attacks in Wireless Sensor Networks (DAWWSEN)

In order to defense against wormhole attack, DAWWSEN method proposed a new mechanism in wireless sensor network. It used hierarchical tree in which intermediate nodes are leaf nodes and the base station play role of the root node [14]. In this method root node sends a request message to discover the leaf nodes and location of them on the tree. Before the request message is broadcast to leaf nodes, two parameters: like hop count and ID of each node that emanates the request packet should put on header of the request message.

When the intermediate nodes receiving the first request message, they still have to wait for a period of time in order to collect a count of request messages since it is still difficult to know if a

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

received request message is replayed by a wormhole attacker or not. So, each node that receiving a request message inserts a new entry in its request list that includes the IDs of all the nodes from which it has received a request message and their corresponding hop count.

A Reply Timer is set to expire after a period of REPLY_DELAY seconds from the reception of the first received request packet. When the timer expires, the node sends a reply packet which contains its ID, the destination ID which is the ID of the first node in its request list and its corresponding hop count, and then updates its replay table. Then, it sets another timer, the Check Timer, which expires after a period of CHECK_DELAY seconds from the transmission of the reply packet.

During this period, the node sending this reply packet keeps listening to the transmitted reply packets, and increments the Num_Rep field for each received packet with source ID and destination ID respectively equal to its own ID and to the destination ID in the replay table. On the other hand, the node receiving a reply packet inserts in its reply list a new entry which contains the ID of the node sending the reply packet, its hop count, and the number of the identical received reply packets Num_reply which is set to one for a new received reply packet. Upon the reception of the first reply packet, the node sets the "Accept Timer" which expires after a period of ACCEPT_DELAY seconds from the reception of this packet.

For each received reply packet during this period, the nodes navigate over the reply list for a match of the NodeID. If an entry was found, its Num_reply field will be incremented by one; otherwise a new entry will be added to the list with Num_reply equal to one. Once its Accept Timer expires, the node sends for each entry in its reply list an equivalent accept packet which contains its own ID as a source ID, the NodeID in the reply list as the destination ID, and the Num_reply field which designated the number of repeated reply packets received by the destination node.

The node receiving an accepts packet should check the source ID that should be the same as the NodeID in its replay table. If this is not the case, this will mean that this packet was stored by an attacker during a previous construction of the routing tree and replayed now, and therefore should be dropped. If not, the node receiving this packet updates its replay table by setting the Recv_accept field to one and checks if the Num_reply field in the accept packet is one value greater than Num_Rep in the replay table of this node.

$$Num\_reply = Num\_Rep + 1 \quad (1)$$

If the above condition is not verified, a wormhole attack is detected by this node which will:

1. Delete the received accept packet.
2. Insert the ID of the creator of accepting packet to its NAP (Not Accepted Packets) list.
3. Update its replay list by setting the all values to zero.
4. And finally, the node can wait for another request packet or send another replay that is like to the second item in its request table if not available.

As a result, in this technique a hierarchical three-way handshake routing three can be created in wireless sensor network for multi-hop, to detect wormhole attack.

3.1.4 Prevention of Wormhole Attacks in Geographic Routing Protocol

This method presented by Poornima and Bindhu in 2011 to prevent and detect wormhole in the Boundary State Routing (BSR) protocol. In BSR routing, the Greedy-Bounded-Compass is used to transfer packet through destination in geographic routing. Two techniques designed in this model, firstly method using Reverse Routing Scheme (RRS) that try to detect intrusion action and secondly method checking Authentication of Node Scheme (ANS) which uses cryptography ideas to avoid and detect wormhole attack [14].

Reverse Routing Scheme (RRS) is a first method, which witness_value and witness_threshold and honest node are two terminologies that used. Each Ad hoc network includes some honest node and malicious node, and also these nodes can be placed in an arbitrary geographical location. In geographic routing nodes become candidates, that depends on geographic location. Routing path include a sequence of nodes that each of them responsible to send a message toward the geographical routing. In RRS scheme, when the source node sends a packet to a destination, the data-acknowledgment Data_ack will be send after the destination node received the packet from sender in the reverse pat. When the data are traversed from receiver node to sender node, called the reverse path. The Data_ack packet

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

is sent to the next node that is closer to the source and it is forwarded to the next nodes in reverse greedy forwarding method. If in greedy forwarding error is occurring, then Bounded Compass method is used. After the sender received the Data_ack from the destination, checks for the route in the packet and estimates the route from it to the destination according to the positions of the nodes in the network. If the estimated route is in deviation with the route in the packet, the source node comes to know the intrusion action.

Generally, this technic attempts to identify static wormhole by using a kind of hope-count method. Base on this technic, the number of hope from source to destination compared with the number of hope between the destination node and source node. If the witness value, the number of the same nodes in this to the path, was less than the minimum threshold, in result the wormhole attack is identified.

The second method is Authentication of Node shame (ANS), which uses digital signatures (RSA) to avoid wormhole attack. When the source node transmits the packet to the destination, each intermediate node that received the packet should insert its digital signature in the forwarding packet. If any packet reached to the malicious node, in order that malicious nodes do not have any key to sing, the destination node can identify the malicious node simply.

Therefore, in this technic some weaknesses are exits, such as digital signature, that is expensive, because uses asymmetric cryptography and it's not cost. Another weak point is expensive to receiver for adding its digital signature into packet and finally if the CPU is not powerful, thus creation and authentication of digital signature waste a time.

3.1.5 Detection Wormhole in Wireless Ad-hoc Networks

This method suggested by [15] in 2011 to enhance the RRS and NSA to detect wormhole in geographical routing protocol [15]. In this technique two approaches considered as follows:

Before any node transferring a packet to nearest next node through destination by using greedy or compass method, it should investigate the authentication of neighbor by using symmetric pairwise key distribution scheme. After the authentication of neighbor node is confirmed, the packet is transmitted; else the next neighbor node is selected from the table list that is located in each node. If this approach be used, the malicious node cannot impersonate or exploit authentication of nodes. This approach is kind of pre-processing level and will continue until the packet is received by destination. When the packet received to destination nod, the number of node that reached to packet is counted and base on pre-processing approach, the trusted path recognized. According to feature of geographical routing, every node can broadcast the radius range(R) and propagate the packet just to its neighbors. As we know, if the R*hope-count, so value will be larger than the distance between the source and destination. In order to inform the destination, destination node coordination is (x_d, y_d) and source node coordination is (x_c, y_c), the wormhole attack occurs if the following formula established:

$$\sqrt{(x_d - x_c)^2 + (y_d - y_c)^2} > R * Hop\_count$$

The comprehensive of this scheme shows that the pre-processing is one of the necessary levels to detect wormhole attack, because when the number of malicious nodes is more than threshold (λ), the attacker may impersonate or use the other node authentication.

3.2 Detection the wormhole attacks considering to the routing protocol:

3.2.1 Detecting and avoiding a wormhole attack in the OLSR routing protocol

In this procedure three methods will be reviewed, first mechanism is detection of wormhole attack in suspicious link, then verification of the wormhole and final timeout, which each of them described in separate parts:

3.2.1.1 Detect suspicious links in OSLR protocol

In this approach, packet latency is a base method to detect a wormhole in suspicious links. One of the important side effects of wormhole attack on the network is increasing delay compared to the normal wireless propagation latency on a single hop [16]. To distinguish suspicious links in this method on network, two new controls should be applied $HELLO_{req}$ and $HELLO_{rep}$, also both this control used in OLSR protocol. The sender puts expiry time in the packet before the $HELLO_{req}$ is transferred over the network. When the node received $HELLO_{req}$, it saves the sender address i and time Δi to sustain the packet till it is planned for sending its next $HELLO$ packet time to avoid overloading the network with too many $HELLO$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

answers. It should be noted that the default time transmission interval for $HELLO$ message is 2 seconds in piggy-backs and OLSR the answers to this $HELLO$ message. After this process, when the source node received $HELLO_{rep}$, its check the contain of respond packet and arrival time of the packet, that whether or not it has arrived within its scheduled timeout interval. If the packet did not come within its scheduled timeout, so the source node assumes that the malicious node is in route and communication not allows in link, as long as the wormhole verification method archive to the end point.

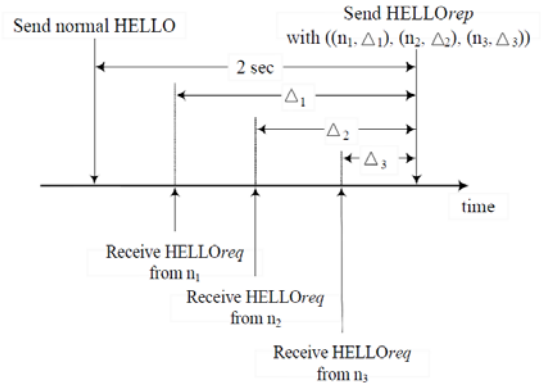

Figure 4: $HELLO_{rep}$ aggregation

3.2.1.2 Verification of wormhole

When the suspicious links was detected by the sender through the $HELLO_{req}$, $Probe$ packet is sent to all of the suspect nodes by source node and its waiting to ACK_{Probe} replies from them. This mechanism is similar to $HELLO_{req}$ and $HELLO_{rep}$ to detect wormhole tunnel. After the ACK_{Probe} received by sender, originator of $Probe$, compare the evaluation of its reputation status and reputations of the other end point in suspicious link. If the reputation of the remote node or the contents of ACK_{Probe} is occurred, that link is not trusted link.

Figure 5 shows the message exchanging between sender and receiver in this timing diagram. End to end authentication is needed to exchanging $PROBE$ and ACK_{Probe}, so to ensure the security is sufficient for $PROBE$ packet, the sender should select a large random number, that attacker cannot suppose, and use hashing or encrypting method for the message to send. After the node received the $PROBE$ packet from the sender decrypts the message and verifies the sender. If the authentication was successful the receiver creates the ACK_{Probe}, that contain the state of the sender and the large random number, which selected by the source node. In same method ACK_{Probe} is hashed and encrypted before sending to the source node. After the source node received ACK_{Probe}, it checks whether the ACK_{Probe} arrived within the required timeout or not.

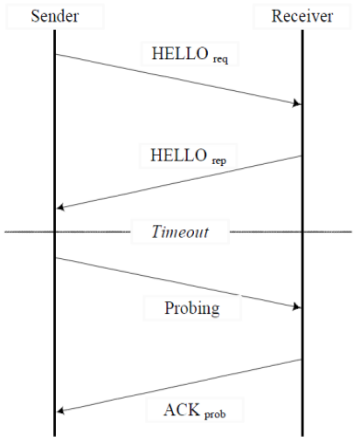

Figure 5: Detecting wormhole via message exchanging

3.2.1.3 Timeouts

The value of timeout is very important, because if calculated without accuracy, the mistake value can effect in decisions. For example, if the timeout is considered value too small, thus the rightful nodes can be suspected mistakenly. In the opposite, if the timeout is considered too big, certainly it becomes difficult to find malicious node. Timeout is calculated by follows formula:

$$\text{Timeouts:} = \frac{2R}{V} + T_{Proc}$$

The maximum transfer radio for every node is shown by R; also the speed of light is determined by V. The estimation of the packet processing and the queuing delays is shown by T_{proc}.

3.2.3 A Novel Trusted-base Scheme to Detect Wormhole Node

This technique presented by (Jain and Jain, 2010) that used trust model in Dynamic Source Routing (DSR) to detect wormhole attacks in the network [17]. In DSR protocol the packets contain the address list of each node that it has to traverse. In this method the wormhole attack identified by using

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

effort-return based trust model, which applied DSR protocol to derive and calculate respective trust levels in other nodes. To execute this model, must be done by following condition to exact perform:

1. Every node support irregular node proceeds.
2. The ranges of forwarding and receipt are comparable for the transceiver.
3. The ranges of forwarding and receipt are comparable for the transceiver.

All nodes perform a trust model, which correctitude and purity of them are measured by monitoring the neighbor nodes, that attendance in the packet forwarding mechanism. The verification of transmission node is different fields in the forwarded IP packet for prerequisite modifications through a sequence of integrity checks. If the integrity of node was successful, shows that this node is reliable, otherwise if the integrity checks, the error happened or the forwarding node does not pass the packet at all, its corresponding direct trust measure is decreased.

3.2.4 Detecting wormhole attack with DElPHI method

This method presented by [18], which called Delay per Hope Indication (DelPHI). This technique used the delay and the hop count information to find disjoint path between sender and receiver that wormhole attack subjected to these disjoint paths. The benefits are the Delphi does not need any extra devices or hardware and clock synchronization.

The main idea of this method is to collect hop count and delay Information decompose paths and evaluate the delay per hop to serve as the indicator of detecting wormhole attack, also this method is similar to the AODV route setup mechanism. These propose dividing into two phases to detect wormhole attack, in the first phase the hop information and delay are collected and in the second phase the sender analyzes the information in the first phase that whether the wormhole attack is happened or not.

In second phase that called data analysis and detection, the sender initiates the detection. When the Delphi request (DREQ) packets broadcasted through sender, at time t_s and received DelPHI reply (DREP) packet from intermediate node i at time t_i. Then the round trip time (RTT) of node $i$can define by$RTT_i = t_i - t_s$. If the hop count field in the DREP from node i I h_i, finally the delay per hop value (DPH) of the path to the receiver through node i will be calculated by following formula:

$$DPH_i = \frac{RTT_i}{2h_i} = \frac{t_i - t_s}{2h_i}$$

Delphi method has some advantages in opposed by the other methods. in this technique that able to detect both kind of hidden attack and exposed attack [18]; also DELPHI no need extra information such as, synchronization between two nodes or their position information. It can achieve higher than 98 percentages in detection normal path and 90 percentages in detecting wormhole attack, in the absence of background traffic.

The weak point of DELPHI method is unable to pinpoint the location of a wormhole, because this method just calculate the delay of each node in a path and observed that the DPH values of normal paths usually appear as small values when compared with those of tunneled paths. It can easily observe by that the DPH values of normal and tunnelled paths form two separate groups as shown in Fig. 6. The difference between "the smallest DPH in the tunneled group" and "the largest DPH in the normal group" is always larger than the gap between any two DPH values within the same group.

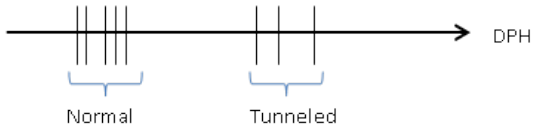

Figure 6: Relationship of normal and tunneled paths

4. CONCLUSION

In this paper, we reviewed the various Techniques against wormhole attacks in wireless Ad-hoc networks. The weak points of them are discussed and a qualitative comparison of these methods is summarized in Table 1.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1: Qualitative comparison of wormhole detection methods

Method	Require-ment(s)	QOS Parameter	Hop count Analysis
Geographical Leashes [10]	Time synchro-nization device and GPS coordinates of every node	Delay up to leashes factor	N/A
Temporal Leashes [10]	Loosely synchro-nized clocks	Delay up to leashes factor	N/A
EDWA [13]	N/A	TRACING the packet	YES
Prevention in Geographic Routing [14]	GPS	Greedy-Bounded-Compass	YES
Detection in geogra-phic Routing [15]	GPS	Symmetric pair-wise Key	YES
DelPHI Method [18]	N/A	Delay Per Hop	YES

REFRENCES:

[1] Yick, Jennifer, Biswanath Mukherjee, and Dipak Ghosal. "Wireless sensor network survey." Computer networks 52, no. 12 (2008): 2292-2330.

[2] Kontogiannis, Theofanis. "Ad-Hoc Sensor Networks for Maritime Interdiction Operations and Regional Security." PhD diss., Monterey, California. Naval Postgraduate School, 2012.

[3] Akyildiz, Ian F., Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci. "A survey on sensor networks." Communications Magazine, IEEE 40, no. 8 (2002): 102-114.

[4] Djenouri, Djamel, L. Khelladi, and N. Badache. "A survey of security issues in mobile ad hoc networks." IEEE communications surveys 7, no. 4 (2005).

[5] Hartenstein, Hannes, and Kenneth P. Laberteaux. "A tutorial survey on vehicular ad hoc networks." Communications Magazine, IEEE 46, no. 6 (2008): 164-171.

[6] Soni, Hariom, and Preeti Verma. "A Survey of Performance based Secure Routing Protocols in MANET." International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) 2, no. 1 (2013): pp-145.

[7] Al-Karaki, Jamal N., and Ahmed E. Kamal. "Routing techniques in wireless sensor networks: a survey." Wireless Communications, IEEE 11, no. 6 (2004): 6-28.

[8] Loo, Chong Eik, Mun Yong Ng, Christopher Leckie, and Marimuthu Palaniswami. "Intrusion detection for routing attacks in sensor networks." International Journal of Distributed Sensor Networks 2, no. 4 (2006): 313-332.

[9] Furht, Borko, and Mohammad Ilyas, eds. Wireless Internet Handbook: Technologies, Standards, and Applications. Vol. 7. Auerbach Publications, 2003.

[10] Hu, Yih-Chun, Adrian Perrig, and David B. Johnson. "Wormhole attacks in wireless networks." Selected Areas in Communications, IEEE Journal on 24, no. 2 (2006): 370-380.

[11] Malhotra, Amarjit, Deepti Bhardwaj, and Ankush Garg. "Wormhole attack prevention using clustering and digital signatures in reactive routing." In Networking, Sensing and Control (ICNSC), 2012 9th IEEE International Conference on, pp. 122-126. IEEE, 2012.

[12] Sen, Jaydip. "Security and Privacy Challenges in Cognitive Wireless Sensor Networks." arXiv preprint arXiv:1302.2253 (2013).

[13] Wang, Xia, and Johnny Wong. "An end-to-end detection of wormhole attack in wireless ad-hoc networks." In Computer Software and Applications Conference, 2007. COMPSAC 2007. 31st Annual International, vol. 1, pp. 39-48. IEEE, 2007.

[14] El Kaissi, Rouba, Ayman Kayssi, Ali Chehab, and Zaher Dawy. "DAWWSEN: a defence mechanism against wormhole attacks in wireless sensor networks." In Proc. 2nd International Conference on Innovations in Information Technology (IIT'05). 2005.

[14] Poornima, E., and C. Bindhu. "Prevention of WormholeAttacks in Geographic Routing Protocol." International Journal of Computer Network and Security (IJCNS) (2010): 42-50.

[15] M. Sookhak, M. R. Eslaminejad, M. Haghparast and I. FauziISnin. "Detection Wormhole in Wireless Ad-hoc Networks."

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

International Journal of Computer Science and Telecommunications 2, no. 7 (2011): 28-34.

[16] Naït-Abdesselam, Farid. "Detecting and avoiding wormhole attacks in wireless ad hoc networks." Communications Magazine, IEEE 46, no. 4 (2008): 127-133.

[17] Jen, Shang-Ming, Chi-Sung Laih, and Wen-Chung Kuo. "A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET." Sensors 9, no. 6 (2009): 5022-5039.

[18] Chiu, Hon Sun, and King-Shan Lui. "DelPHI: wormhole detection mechanism for ad hoc wireless networks." In Wireless Pervasive Computing, 2006 1st International Symposium on, pp. 6-pp. IEEE, 2006.