Review Paper on Wormhole Attack

Garima Kadian
CSE Department, DCRUST
DCRUST, Murthal, Sonipat, India
Dinesh Singh, PhD
Assistant Professor
DCRUST, Murthal, Sonipat, India

ABSTRACT

A Wireless Networks are more accessible to different types of attack than wired Network. One such attack is Wormhole Attack, in which traffic is forwarded and replayed from one location to another through the Wormhole tunnel without negotiating any cryptographic techniques over the network. Thus, it is challenging to defend against this attack. In this paper we review WSN concept and Wormhole Attack. Then we discuss classification of wormhole Attack and also mention few of the initiatives to detect the Wormhole Attack.

Keywords

Wireless Sensor Networks, Wormhole Attack.

1. INTRODUCTION

A wireless network is that network which uses wireless data connections for connecting network nodes [1].Wireless Network can be classified into two types named as Infrastructure based and Ad-hoc network. In Infrastructure based network, every user needs to communicate with an access points or base stations whereas in Ad-hoc network, nodes create and maintain the intercommunication links without the help of a pre-existing infrastructure. Lack of infrastructure in network means lack of central entities. Security in Ad hoc network is difficult because network topology is dynamic as well as links between nodes is unreliable. Wireless network are more prone to attacks ranging from eavesdropping to interfering. Wireless Sensor Network (WSN) as a part of MANET consists of a large number of tiny sensor nodes that continuously monitors the environmental conditions. Sensor nodes perform various tasks such as signal computation, processing, and self-configuration of network which help in expanding network coverage and strengthen its scalability. A WSN is composed of tens to thousands of Sensor Nodes distributed in a wide area. These sensors are tiny and are able to sense, process data and communicate through radio frequency channel with each other,. Each Sensor Node (SN) is composed of four basic components, named as sensing unit, processing unit, transceiver unit and power unit shown in “Figure 1”. They also have additional optional components which are application dependent such as a location finding system, a power generator and a mobilize. The Sensing unit is composed of two subunits: sensors and Analog to Digital Converters (ADCs). The Analog signals are converted to digital signals with the help of ADC and then go into the processing unit. The processing unit is associated with a small storage unit and manages the operation that makes the SN collaborate with the other SNs to carry out the assigned tasks. The function of transceiver unit is to connect the node with the network. Power unit may be supported by a power rummage unit such as solar cells. Some application dependent subunits are also present in SN. Each node has the ability to sense element of its environment and can perform simple computations and communicate with its peers or directly to an external (Base Station) BS. These BS may be a fixed node or a mobile node which is capable of connecting the WSN with the actual communications infrastructure or with the Internet where a user can access the reported data [2].

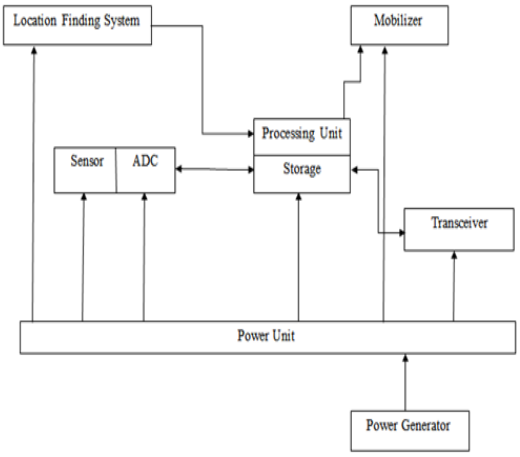


Fig 1.Components of Sensor Node

WSNs generally operate in remote areas and contain a large number of sensor nodes. These nodes have strictly limited resources such as memory, energy, communication and computation due to which, reliability and accuracy of a single sensor node is somewhat low thereby requiring collaborative data collecting and processing [3]. WSNs are liable to security attacks due to the transmission medium nature (broadcast nature). Furthermore, WSNs nodes are mostly placed in a dangerous or hostile environment where they are not protected physically. Attacks are of two types named as active attacks and passive attacks. In Active Attack, the attacker’s monitors, listens and alter the data stream in the communication channel. Some of the attacks that are active in nature are as follow:

1. Routing Attacks in Sensor Networks
2. Message Corruption
3. Node Malfunction
4. Physical Attacks
5. Node Outage
6. Denial of Service Attacks
7. Node Replication Attacks
8. False Node
9. Node Subversion

When unauthorized attackers monitors and listen the communication channel it is called passive attack. Any attack against privacy is passive in nature [4].

2. WORMHOLE ATTACK

In **Wormhole Attack**, two or more malicious attacker receives data packets from one location of network, forwards them through the wormhole tunnel and releases them into another location which gives two distant nodes the illusion that they are close to each other. For better understanding let us consider a multi-hop Ad hoc network irrespective of whether nodes in network are mobile or static as shown in (Figure 2). In this figure, a node or a user of network is denoted by circle whereas line represents the connection between the two nodes. Suppose node 2 wants to transmit message to node 9. But before sending message, source node will decide a path to send message by using Predefined Routing Protocols which may be Proactive or Reactive in nature. If node 2 that is source node had already maintained a routing table (i.e. proactive routing) then it will maintain routing information regarding each and every node in network which will be used to send message to destination but if source node uses reactive routing protocol then it will not have any routing table hence it needs to find routing information before transmitting any message. In Reactive routing protocol sender broadcasts a RREQ message to its one-hop away neighbors in network. All nodes that receive RREQ message will check whether RREQ is intended for itself or not and if not then it will retransmit RREQ message after altering its node identity in message and when request message is received by destination node it will unicast route reply message with route information to sender through same route from which request message had arrived to node. Mostly routing protocols decide path that is shortest because of nodes in ad hoc network have limited bandwidth and power. Hence we can say the node 2 will send the message through the node 2-5-6-8-9.In the network, the intermediate nodes act as routers that send the message to destination. Let us assume that ad hoc network mentioned above is under wormhole attack. Suppose that two attackers are placed in vicinity of node 2 and node 9 and these attackers are connected with each other through a high speed bus. It may be possible that attacker may not be part of network but still it can overhear message due to the open nature of ad hoc network. Whenever any of attackers receives message transmitted by nodes on whose vicinities attacker lies, retransmission of message is done by the other attacker in network. Thus nodes where attackers lies which are node 2 and node 9 are made to believe that both of them are connected to each other directly. Hence a fake link is created by the attacker in a network i.e. between node 2 and node 9. Due to this fake link node 2 will send message to node 9 directly through wormhole tunnel. Hence now the path is 2-9. All routes in network that had to pass through node 2-5-6-8-9 are now replaced by node 2-9. Hence maximum numbers of messages in network are directed through wormhole which puts the attacker in a very powerful position as compared to other nodes in the network. Attacker can misuse the fake link by storing all messages passing through it which can be used to analyze content even if the attacker has no cryptographic keys. Attacker can also selectively drop or modify the message of any node at any time which affects the availability and integrity factors of security. Thus Wormhole attack is dodging for more attacks like eavesdropping, congestion, spoofing packet loss and so on [5]. Wormhole attack is one of the Denial-of-Service attacks which affect the network even without the knowledge of any cryptographic techniques. That is why wormhole attack is very difficult to detect. It can be launched by two or more nodes. In two ended wormhole, packets are tunneled through wormhole link from source to destination node and on receiving packets, destination node retransmit them to the other end.

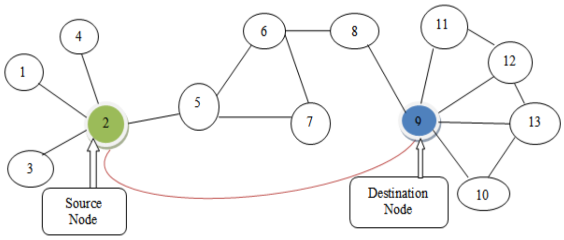


Fig 2: Wormhole Attack in Ad-hoc Network

2.1 Classification of Wormhole Attack

Depending on whether the attackers are visible on the route and packet forwarding behavior of wormhole nodes as well as their tendency to hide or show the identities, wormholes attack is classified into three types: open, half open, and closed. In the following cases S is the source node and D is the destination node. Malicious Nodes are represented by M1 and M2.

2.1.1 *Open Wormhole*

In this mode, attackers include themselves in the packet header following the route discovery procedure. In it, nodes in network are aware about the presence of malicious nodes on the path but they would imitate that the malicious nodes are direct neighbors. As shown in the (Figure 3) Source (S) and destination (D) nodes and wormhole ends M1 and M2 are visible whereas nodes A and B on the traversed path are kept hidden.

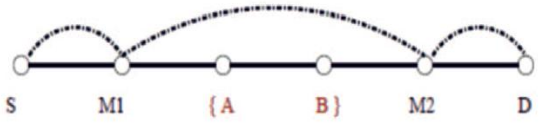


Figure 3: Open Wormhole Attack

2.1.2 *Half-Open Wormhole*

In this mode, the attackers do not modify the content of the packet. They simply tunnel the packet form one side of wormhole to another side and then rebroadcast the packet. As shown in the (Figure 4), malicious node M1 near the source (S) is visible, while second end M2 is set hidden which leads to path S-M1-D for the packets sent by S for D.

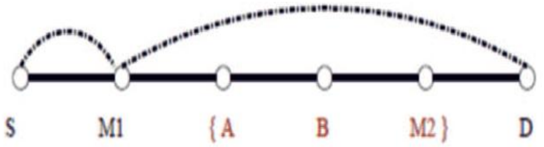


Figure 4: Half Open Wormhole Attack

2.1.3 *Closed Wormhole*

In this mode, identities of all the intermediate nodes (M1, A, B, M2) on path from S to D are kept hidden. In it, both source and destination feels themselves just one-hop away from each other. Hence fake neighbors are created.

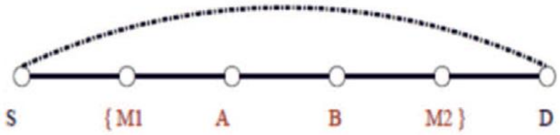


Figure 5: Closed Wormhole Attack

Based on the techniques used for launching attack, Wormhole Attack can be classified into five categories

2.1.2.1 Wormhole using Packet Encapsulation

In wormhole using encapsulation, attackers crumble the routing information and send it through the other nodes to its cooperator. In this type of wormhole attack at least two attackers are needed and as tunnel made via usual nodes in the network, there is no need to any additional tools. In this type of attack actual hop count does not increases during traversal. Routing protocols that uses hop count for path selector are particularly susceptible to encapsulation- based wormhole attack (Figure 6**)** presents an example of encapsulation-based attack. Consider that nodes S (source) and Sink (destination) try to discover the shortest path between each other, in the presence of the two malicious nodes M1 and M2. Node S broadcasts an RREQ (Route Request Message), M1 gets the RREQ and encapsulates it in a packet destined to M2 through the path that exists between M1 and M2 (E-F-G). Node M2 turns the packet into its previous state, and rebroadcasts it again. Due to the encapsulation of the data packet, the hop count does not increase when RREQ travels between M1 and M2 (E-F-G). At the same time, another copy of the RREQ travels from S to sink over the path that includes nodes A-B-C. Now, there are two routes from S to Sink: the first one is four hops long (S-A-B-C-Sink), and the second one appears to be three hops long (S-M1-M2-Sink), while in reality it is six hops long (M1-E-F-G-M2-Sink). The sink chooses the second route since it appears to be the shortest path.

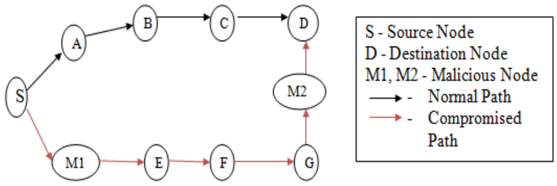


Figure 6: Wormhole Attack Using Packet Encapsulation

2.1.2.2 Wormhole using High-Quality or Out-of-Band Channel

In this, attacker use long range wireless or wired link. In this type of attack, once malicious attacker receives a route request message, it broadcasts the message with high power signal which is not available to the usual nodes in the network and which will establish tunnel, through itself, from source to destination. This mode of attack requires specialized hardware capability. (Figure 7) presents an example of high quality channel based attack. Sensor nodes M1 and M2 are malicious nodes and they have an out-of-band channel between themselves. Let us assume that source node (S) sends a RREQ to sink node and nodes A and M1 are neighbors of S. Node M1 tunnels the RREQ to M2 and M2 broadcasts the packet to its neighbors, which may include the sink node. Sink node gets two RREQs: (S-M1-M2-Sink) and (S-A-B-C-Sink), the first route is both shorter and faster than the second one, thus it is chosen by the sink node [6].

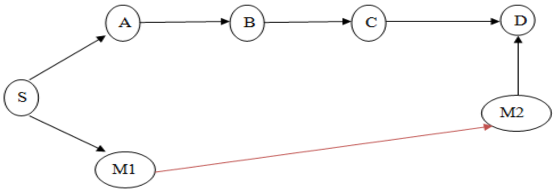


Figure 7: Wormhole Attack using tunnel between two nodes

2.1.2.3 Wormhole Using High-Power Transmission Capability

In this type of wormhole attack, one malicious node with high-power transmission capability exists in the network and this node can communicate with other normal nodes from a long distance. When a malicious node receives an RREQ, it broadcasts the request at a high-power level. Any node that hears the high-power broadcast rebroadcasts the RREQ towards the destination. By this method, the malicious node increases its chance to be in the routes established between the source and the destination even without the participation of another malicious node [7].

2.1.2.4 Wormhole Using Packet Relay

This type of attack can be launched by one or more malicious nodes. In it, malicious node relays data packets of two distant sensor nodes and convinces them that they are neighbors. In this way fake neighbors are created. This attack is also called as “Replay-Based Attack” in the literature. For example, in (Figure 9(a)), sensor node A and sensor node B are two non-neighboring nodes with a malicious neighbor node M1. Node M1 can relay packets between sensor nodes A and B to make them believe that they are neighbors. As shown in (Figure 9(b)), if there are several cooperating malicious sensor nodes, sensor nodes that are multiple hops away from each other can be victims of this attack [7]

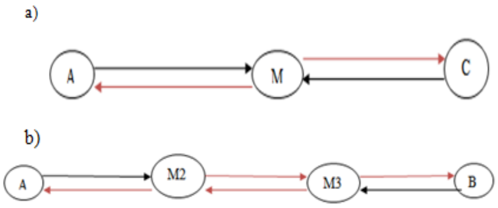
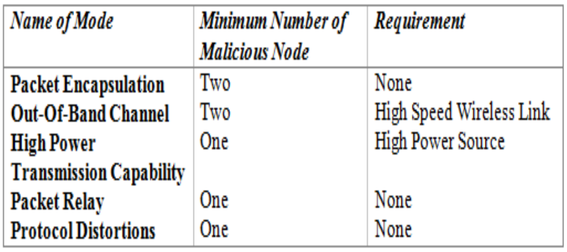


Fig 8: Replay Based Attack Using (a) one malicious node or (b) two malicious node

2.1.2.5 Wormhole Using Protocol Distortion

In this mode of attack, single malicious node tries to attract network traffic by distorting the routing protocol. This attack does not affect the network routing much and hence is harmless. Also it is known as “rushing attack” in the literature [3]. Routing protocols that are based on the 'shortest delay' instead of the 'smallest hop count' is at the risk of wormhole attacks by using protocol distortion [7].

Table 1: Summary of Wormhole Attack Modes



Name of Mode	*Minimum Number of Malicious Node*	*Requirement*
Packet Encapsulation	Two	None
Out-Of-Band Channel	Two	High Speed Wireless Link
High Power Transmission Capability	One	High Power Source
Packet Relay	One	None
Protocol Distortions	One	None

2.2 Detection of Wormhole Attack

Wormhole attacks are difficult to detect as the malicious nodes replays valid data packets into the network. Moreover, majority of wireless sensor network routing protocols employ lightweight cryptographic solutions to prevent unauthorized nodes from injecting false data packets into the network. Hence, in wormhole attacks, the replayed data packets pass all cryptographic checks. Mostly protocols were proposed using synchronized clocks, directional antennas or positioning devices. Several approaches have been developed to detect wormhole attacks in Mobile Ad-hoc Network.

2.2.2 Based On Special Hardware

Hu, Perrig and Johnson [9] proposed a mechanism, named packet leashes.

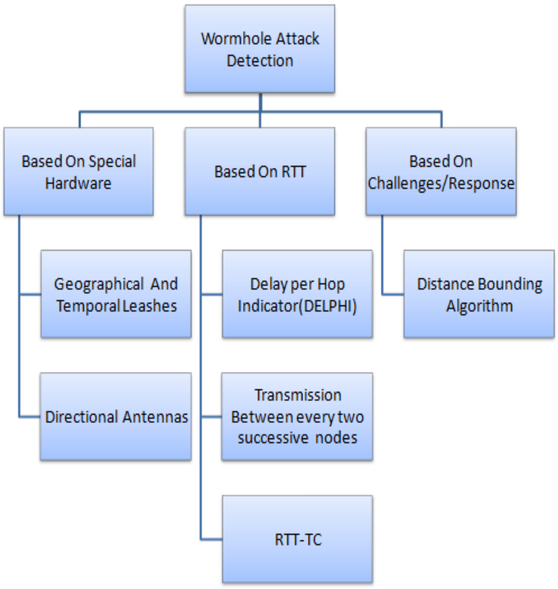

Wormhole Attack Detection
Based On Special Hardware
Based On RTT
Based On Challenges/Response
Geographical And Temporal Leashes
Delay per Hop Indicator(DELPHI)
Distance Bounding Algorithm
Directional Antennas
Transmission Between every two successive nodes
RTT-TC

Figure 9: Classification of Wormhole Attack Detection Mechanism

In it packets are prevented from travelling farther than transmission range. In it, leashes are classified of two types: Geographical and Temporal .In Geographical Leashes, every node in the network knows its precise location and all nodes have loosely synchronized clocks to determine the neighbor relation. Before sending a packet, node affix its current position and transmission time to it. When the receiving node receives the packets it computes the distance with respect to the sender and the time required by the packet to traverse the path. Then the receiver can use this distance information to deduce whether the received packet passed through a wormhole or not [5]. For the construction of geographical leash, each node must know its own location which requires the need for a Global Positioning System [7].In Temporal Leashes, all nodes must have tightly synchronized clocks. Then the receiver will compare the receiving time with the sending time attached with the packet. Special hardware is needed to achieve recognize time synchronization between the nodes which makes the setup complex and costly. This mechanism considers the processing and queuing delays to be negligible and does not take congestion into account [7]. In it, every node maintains a tightly synchronized clock but does not depend on GPS information [5].

Hu and Evans suggested the method of directional antennas [9]. It is based on the fact that in ad-hoc networks with no wormhole link, if one node transmits packets in a given direction, then its neighbor will receive that packet from the opposite direction. Hence, only when the directions are matching in pairs, then neighboring relation is confirmed. In it, each node requires a special hardware i.e. directional antenna [5].Directional antennas based on the zone of the incoming signal were proposed to detect wormhole attacks. The zones around each sensor are numbered 1 to N clockwise starting with zone 1 facing east .This method is based on the co-operation between nodes in sharing directional information .When a sensor node accept a signal from a sensor node for the first time, the sensor node get the inexact direction of the signal and identify the foreign sensor node by its zone. Then the sensor node cooperates with its neighboring nodes and verifies the legitimacy of the unknown node [6]. This method requires no location information or clock synchronization but requires special hardware with each node in the network and suffers from antennas directional errors [7].

2.2.3 Based on RTT

Hon Sun Chiu and King-Shan Lui proposed Delay per Hop Indicator (Delphi) [10] method which can detect both hidden and exposed wormhole attacks. In Delphi, sender node detects wormhole attack by finding delays of different paths to the receiver. Hop count and delay information of disarrange paths are collected and delay per hop value is computed to serve as an indicator of detecting wormhole attacks. Hop count is the minimum number of node-to-node transmissions. Under normal scenario, the delay that the packet sense in propagating one hop should be similar along each hop in the path. But, under wormhole attack the delay is unreasonably high because of the presence of malicious nodes along the path. Therefore if a path has high delay per hop value, it is governs the wormhole attack. By comparing the delay per hop values among these disarrange paths, a wormhole can be identified. This method cannot locate wormhole attack. Since the length of the paths can be changed by each node, wormhole nodes could alter the path length in a way that makes them unable to detect [7].

Tran et.al [11] proposes a transmission-time-based mechanism (TTM) to detect wormhole attacks during the route setup procedure by calculating transmission time between every two consecutive sensor nodes along the established path. Wormhole is determined based on the fact that the transmission time between two fake neighbors created by wormhole is considerably higher than two actually real neighbors, which are within radio range of each other. Wormhole attacks interfere in the route setup before they cause any harm. TTM requires no special hardware. But as only delays are measured, two authenticated neighbors suffering link congestion is not taken into account and thus suffers from high false alarm rate [7].

Alam and Chan [12] developed mechanism called RTT-TC which is based on the topological comparison and round trip time measurement. In this method, a wormhole attack is suspected using RTT measurements and genuine neighbors are eliminated from the suspected list using topological comparison. In this method, a Neighbor List includes two segments: TRST and SUS i.e Trusted and Suspected respectively. Two nodes suspect a wormhole tunnel between them if the RTT between them is more than 3 times of their current RTTavg. If there is a wormhole tunnel, those two node‘s NodeID is inserted to their respective SUS lists. Wormhole detection method is provoked when a source node finds non empty SUS list. A node sends request packets to every node in the SUS part of its Neighbor List. In response, the recipients reply back with its TRST list to the source, which is compared with the TRST list of the source to detect whether a link is attacked by the wormhole. This mechanism has higher detection rate and does not need any clock synchronization but has high message overhead [7].

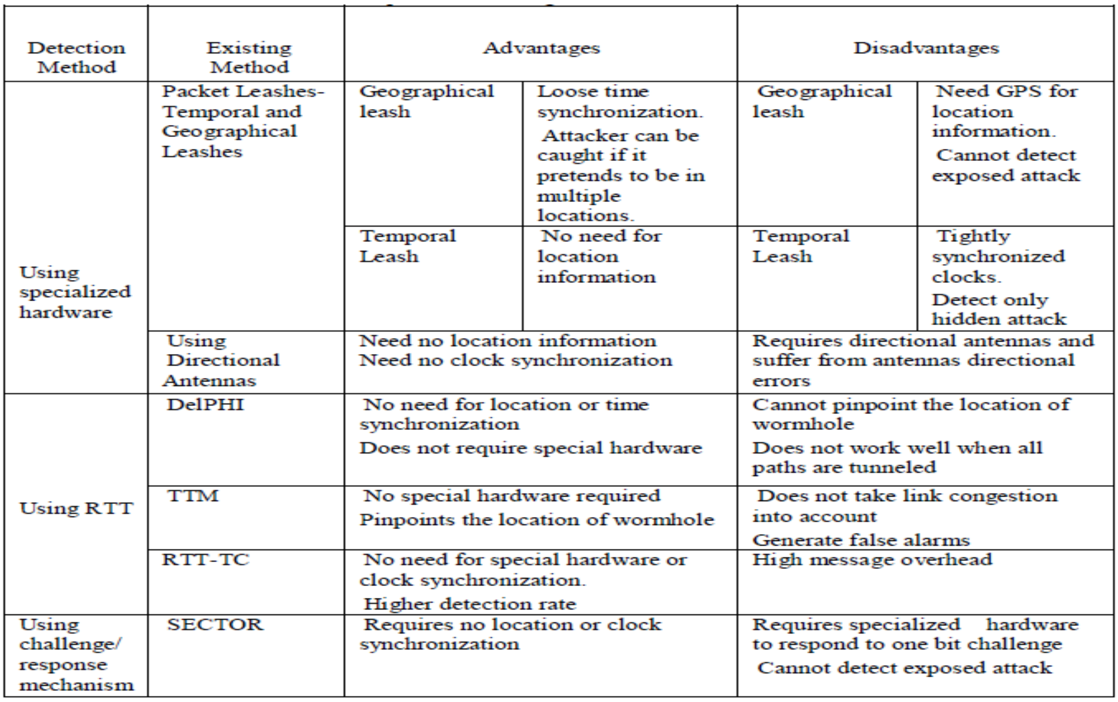
2.2.4 Based on Challenges/Response

Capkun et al. [14] proposed a protocol, called SECTOR, which relies on a special hardware. The main idea of the proposed protocol is the distance between two sensor nodes can be measured accurately based on the speed of data transmitted between them. The proposed protocol does not require any clock synchronization and location information by using (mutual authentication with distance bounding) MADB protocol. The MADB protocol enables the nodes to determine their mutual distance at the time of encounter. The notion of distance-bounding protocols was first introduced by Brands and Chaum [15]. They proposed a mechanism that enables a party to determine a practical upper-bound on its physical distance to another party. By measuring the time between sending out the challenges and receiving the responses, the first party can compute an upper-bound on the distance to the other party. Capkun et al. modified the distance bounding protocol proposed by Brands and Chaum. The protocol allows both parties to measure the distance to the other party simultaneously. At the same time, it is considered that each pair of parties share a symmetric key, that the nodes are established before running the distance-bounding protocol between them.

3 CONCLUSION

In this paper we have describe the wormhole attack with its different type in details. We have also discussed the various methods used to eliminate or at least minimize effect of this attack. In this type of attacks many solution have been suggested that can be used in network. All these solution have their own advantage and disadvantage. Disadvantage are in form of requirements (which can either be impractical, costly or else affecting other parameters of ad hoc network like mobility or decentralization) or their effect on overall performance (by increasing load on network).It’s very necessary to further investigate effect of this attack to contain the danger that this attack posses.

Table2: Summary and Comparison of existing wormhole detection mechanism



Detection Method	Existing Method	Advantages		Disadvantages	
Using specialized hardware	Packet Leashes-Temporal and Geographical Leashes	Geographical leash	Loose time synchronization. Attacker can be caught if it pretends to be in multiple locations.	Geographical leash	Need GPS for location information. Cannot detect exposed attack
		Temporal Leash	No need for location information	Temporal Leash	Tightly synchronized clocks. Detect only hidden attack
	Using Directional Antennas	Need no location information Need no clock synchronization		Requires directional antennas and suffer from antennas directional errors	
Using RTT	DelPHI	No need for location or time synchronization Does not require special hardware		Cannot pinpoint the location of wormhole Does not work well when all paths are tunneled	
	TTM	No special hardware required Pinpoints the location of wormhole		Does not take link congestion into account Generate false alarms	
	RTT-TC	No need for special hardware or clock synchronization. Higher detection rate		High message overhead	
Using challenge/ response mechanism	SECTOR	Requires no location or clock synchronization		Requires specialized hardware to respond to one bit challenge Cannot detect exposed attack	

4 REFERENCES

[1] http://en.wikipedia.org/wiki/Wireless_network.Wireless Network - Wikipedia, Retrieved March 4, 2015.

[2] Debnath Bhattacharyya, et al, “A Comparative Study of Wireless Sensor Networks and Their Routing Protocols”, In MDPI-2010, Basel, Switzerland, Nov. 2010.

[3] Priya Maidamwar and Nekita Chavhan,“ A Survey on Security Issues to Detect Wormhole Attack In Wireless Sensor Network”, In Proceeding of the International Journal on Ad-Hoc Networking Systems (IJANS) Vol. 2, No. 4, October 2012.

[4] Dr.G.Padmavathi and Mrs. D. Shanmugapriya, “A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks,” In Proceeding of the International Journal of Computer Science and Information Security (IJCSIS), Vol. 4, No. 1 & 2, 2009.

[5] Shaishav Shah and Aanchal Jain, “Techniques For Detection & Avoidance Of Wormhole Attack In Wireless Ad Hoc Networks”, In Proceeding of the International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 10, December- 2012.

[6] Ali M, et al, “Mitigation of Wormhole Attack in Wireless Sensor Networks”, In Proceeding of the Atlantis Press 2012.

[7] Majid M, et al, “A Survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Networks”, In Proceeding of the IETE Technical Review, April.2011.

[8] Maria Sebastian and Arun Raj Kumar P. “ A Novel Solution for Discriminating Wormhole Attacks in MANETs from Congested Traffic using RTT and

Transitory Buffer", In Proceeding of the I. J. Computer Network and Information Security, 2013.

[9] Yih-Chun Hu, Adrian Perrig, and David B. Johnson— "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks", In Proceedings of the IEEE Conference on Computer Communications (Infocom), 2003, p. 1976-1986.

[10] L.Hu and D. Evans. "Using directional antennas to prevent wormhole attacks," Proceedings of Network and Distributed System Security Symposium, pp. 131−41, Feb. 2004.

[11] Hon Sun Chiu and King-Shan Lui, "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks", International Symposium on Wireless Pervasive Computing (ISWPC), 2006.

[12] T Phuong Van Tran, Le Xuan Hung, Young-Koo Lee, Sungyoung Lee, and Heejo Lee," Transmission time-based mechanism to detect wormhole attack" ,In Proceedings of the IEEE Asia-Pacific Service Computing Conference, Dec. 11-14, 2007, p. 172-178.

[13] Mohammad Rafiqul Alam and King Sun Chan, "RTT-TC: A Topological Comparison Based Method to Detect Wormhole Attacks in MANET", 12th IEEE International Conference on Communication Technology, 2010, p. 991-994.

[14] S. Capkun, L. Buttyán, and J.P. Hubaux, "SECTOR: Secure tracking of node encounters in multi-hop wireless networks," Proceedings of the 1st ACM workshop on Security of ad-hoc and sensor networks (SASN 03), pp.21−32, Oct. 2003.

[15] S. Brands and D. Chaum, "Distance-bounding protocols," In Theory and Application of Cryptographic Techniques, pp. 344−59, 1993