5th SASTech
Iran | Mashhad
May 12 - 17 | 2011
5th Symposium on Advances in Science & Technology

A Survey of Wormhole Attack and Countermeasures against that in Wireless Ad-hoc Networks

Ahmad Heidari and Islamic Azad University-
Khosroshahr Branch + a.heidari@live.com
Paper Reference Number: 17
Name of the Presenter: Ahmad Heidari

Abstract

Wormhole attack is a Routing-Disruption Attack in ad hoc networks, those malicious nodes in these networks can bear wormhole attacks to make up a false scenario on neighbor discovery relations among mobile nodes. The attackers endanger the safety of ad hoc routing protocols with making a direct link, referred to as a *wormhole tunnel*, between malicious nodes. After building a wormhole tunnel, one attacker receives and copies packets from its neighbors, and forwards them to the other colluding attacker through the wormhole tunnel. However they need special hardware to support such communication.

This article reviews wormhole attack on ad hoc networks and discusses approaches for preventing wormhole attack in these networks.

Keywords: Wormhole Attack, Detection, Prevention, Avoidance

1. Introduction

Wireless ad hoc networks chiefly develop in unfriendly environments, where network nodes operate as continuum. In addition, the mobile devices use a radio channel to send and receive information. *Malicious nodes* (eavesdropper nodes) can bear both *Passive* and *Active* attacks against these networks. In passive attacks a malicious node only eavesdrop on packet contents, while in active attacks it may duplicate, drop or modify legal packets [5]. A typical example of active attacks is famous as a wormhole attack. In which, a malicious node entraps packets from one position in the network, and tunnels them to another malicious node at a far off point. The wormhole attack can affect network routing and position-based wireless systems [6].

The wormhole attack [1], [3], [4] is one of the most active attacks against wireless ad hoc networks. To set up a wormhole attack, attackers make a direct link, with name a wormhole tunnel, between malicious nodes. Wormhole tunnels can be set up via a wired link or a high quality wireless out-of-band link. Once a wormhole is set upped, malicious nodes can use it for traffic analysis or to make a Denial-of-Service (DoS) attack by dropping certain data or control packets. Inasmuch a wormhole attack can be run without compromising any node or the integrity and authenticity of the communication, the success of the attack is independent of the power of the cryptographic method that defends the network communications [7]. Therefore, a wormhole attack is executed with few resources and is difficult to detect.

As we said, in a wormhole, attackers are directly linked to each other, so they can communicate quickly. However they need special hardware to support such communication. Furthermore, the attackers can establish the attack without disclose their personalities [6]. Most routing protocols like AODV and DSR are vulnerable against this attack.
To make secure protocols in ad-hoc networks, we need to understand security attributes. Security is applied with the mixture of processes which are used to ensure *confidentiality*, *authentication*, *integrity*, *availability*, *access control*, and *non-repudiation* [8]. In these networks *Confidentiality* should be acquired by preventing the unauthorized nodes to access data. *Authentication* should be used to ensure the personality of source as well as neighbor nodes to prevent a node from accessing unauthorized resources and confidential information as well as to stop it from interfering operations of other nodes. *Integrity* helps to prevent malicious nodes from altering data and resending it (e.g. wormhole attack). Also, if a node sends a message, that node cannot deny that the message was sent by it which is called *Non Repudiation* [8]. In wormhole attack, attackers want to violations confidentiality, authenticity and Integrity of the network.

Figure 1 shows a basic wormhole attack. Suppose that node *A* and *B* are not neighbors and that an attacker can transmit packets at nodes *X* and *Y*, respectively, two nodes that it controls. The attacker can make *A* and *B* believe they are neighbors by transmitting packets received from *X* to node *Y*, and reverse. Thus, in a wormhole attack, an attacker forwards packets through a high quality out-of-band link and transmit those packets to another position in the network. Since the attacker replays packets received by *X* at node *Y*, and vice versa, if it would normally take several hops for a packet to traverse from a Position near *X* to a position near *Y*, packets transmitted near *X* traveling through the wormhole will arrive at *Y* before packets traveling through multiple hops in the network. The attacker can make *A* and *B* believe they are neighbors by forwarding routing messages, and then selectively drop data messages to disrupt communications between *A* and *B*.

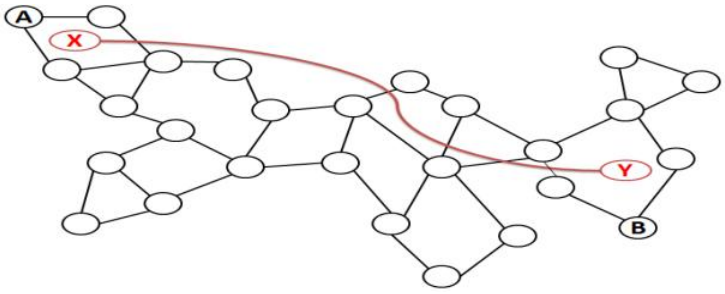

Fig 1: Wormhole attack. The adversary controls nodes *X* and *Y* and connects them through a low-latency link.

Many of the security problems in wireless ad hoc networks faced routing protocols are similar to those faced by wired networks [9]. Wormhole attack is a Routing-Disruption attack in ad hoc networks. Several approaches have been developed to defend against wormhole attacks in mobile ad hoc networks. The existing methods against the wormhole attack can be divided into *Proactive* and *Reactive* countermeasures [2]. In sec. II we will introduce proactive countermeasure methods and in sec. III we will introduce reactive countermeasure methods.

2. Proactive countermeasures against wormhole attack

Proactive methods attempt to prevent wormhole formation, typically through specialized hardware used to achieve accurate time synchronization or time measurement, or to transmit maximum power in a particular direction [2]. Among proactive methods, timing-based solutions attempt to restrict the maximum distance between two neighbors by computing the packet travel time. There are many methods that presented as proactive countermeasures. All presented methods in [1], [3], [4], use proactive countermeasure. Now here we compose some of them in more detail.

2.1. Preventing Wormhole Attack Approaches

Packet Leash in [1], [10] and [11] is a mechanism to detect and defend against wormhole attacks. A leash is any information increased to packets in order to limit the distance that the packet is allowed to transmit. A leash is affiliated with each hop. Thus, each packet for transmission needs a new leash. Two types of leashes are considered, namely geographical leashes and temporal leashes [1]. A geographical leash is deliberated to limit the distance between the transmitter and the receiver of a packet. In geographic leashes, each node should know its own location and when wants to transmit a packet adds its own location and packet transmitting time (needs loose time synchronization among the nodes in the network) in the packet. Receiver node uses this location and time information to compute if the packet has moved more than the permissible distance and if so the packet is dropped. Frame I calculates an upper bound for distance between sender and receiver. In transmitting a packet, the sender node includes in the packet its own location, ps, and the the time at which it received the packet, tr. If the clocks of the sender and receiver are synchronized to within ± time at which it sent the packet, ts; and in recipient, the receiver node compares these values to its own location, pr, and Δ, and v is a maximum speed of any node, then the recipient can compute an upper bound on the distance between the sender and itself with d_{sr} [1].

$$d_{sr} \leq \|p_s - p_r\| + 2v.(t_r - t_s + \Delta) + \delta \quad (1)$$

A temporal leash supplies an upper bound on the lifetime of a packet. As a result, the packet can only travel a limited distance. A receiver of the packet can use these leashes to check if the packet has traveled farther than the leash allows and if so can drop the packet. With temporal leashes, each node transmitting a packet includes the time at which the packet was sent. The receiving node notes the time at which the packet was received and uses this to infer if the packet has traveled too far. In an alternate formulation, a packet can contain the expiration time after which a receiver should not accept the packet. The transmitter node decides on this expiration time as an offset from the time of transmission. Note that in both these cases, geographical leashes and temporal leashes, the receiver needs to authenticate the information about the location and time included by a transmitter in the packet. This authentication can be achieved by a mechanism such as a digital signature.

L.Hu et al [3] also proposed a method to reduce the impact of wormhole attack in wireless networks. In this approach, authors use the directional antennae. The approach here is based on the use of packet arrival direction to detect that packets are arriving from the suitable neighbors. This information about the direction of packet arrival is expected to arrive to exact information about the set of neighbors of a node and be prepared with using directional antennas. Malicious nodes in wormhole attacks can be detected from another node with direction antennas information. To clarify this theory considers Figure 2. We show the

directional antenna with 6 zones obviously for each node and assumed every node have knowledge of the zone from where a packet is received. Due to this, the main theory used to determine reliable neighbors in network. For example consider nodes A, B, C, D, and E as shown in this Figure. Assume that B wants to transmit a Hello message. Node C is node B's neighborhood. Therefore node C replies back to B informing node B of the zone from which node B's hello message was received. If node B receives this reply in the opposite zone to what zone C reports, then node C can possibly be an authentic neighbor. Thus, in this case node C replies back to node B that the hello message was received in zone 1 of node C. This reply is received by node B in its zone 4, which is the zone opposite to zone 1. Thus, B can infer that node C is an authentic neighbor. Every node can repeat this and form the list of authentic neighbors. Any message that does not emanate from an authentic neighbor is rejected.

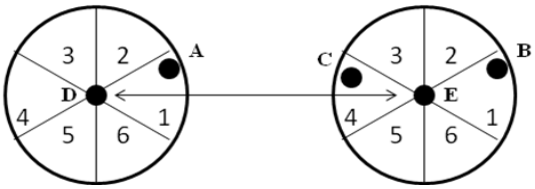

Fig 2: Detecting wormholes using directional antennae [3].

This method is not enough to detect all wormholes, albeit it does detect some of them. Because of that, this method authors modified the basic idea that nodes verifies receiving packets to destination that nodes requires cooperate with their neighbors by having other. In this case, after the messages of the basic protocol, the verifier is asked to confirm the zones from which the messages were received by the verifier. However, this approach needs completely organized directional antennae [3].

In ***SECTOR*** [4], each node can estimate the distance to another node by sending a challenge bit and receiving its instant response. SECTOR, is set of protocols for the secure verification of the time of encounters between nodes. Authors have built these protocols on well-established cryptographic techniques, including hash chains and Merkle hash trees. Authors have also shown how to adapt the protocols to the specific requirements of a given application. Authors have explained that the overhead is very reasonable and have assessed the robustness with respect to attackers of different degrees of strength. SECTOR applied to several problems, including prevention of wormhole attacks, securing routing protocols based on last encounters, as well as cheating detection by means of topology tracking. SECTOR is the first to address the problem of securing topology and encounter tracking; the only exception is the prevention of the wormhole attack, which was previously investigated by other researchers. For preventing wormhole attack, this method doesn't make any assumptions about clock synchronization between nodes, nor do any assume that the nodes are equipped with any positioning devices. To detect wormhole attacks, in this method, MAD protocol is use. This protocol applies the same principle as packet leashes, with the difference that it measures the distance at a single node, unlike with packet leashes where the distance is measured by calculating the difference in time or location at both nodes. MAD has another important advantage over packet leashes: that each node can perform distance bounding without having to trust another party, which is not the case in packet leashes, where two nodes detecting wormholes have to trust the exchanged information (time or location). Another way our mechanisms can help to detect wormholes in wireless networks is through topology and

encounter tracking with GTE mechanisms. If a base station or a node collects network topology information, it can also identify wormhole links by comparing the obtained encounter information [4].

TrueLink [13] is a practical countermeasure to the wormhole attack that presented as an extension to the IEEE 802.11 MAC layer. TrueLink enables a node to verify the adjacency of an apparent neighbor, using a combination of timing and authentication. This method is meant to be used together with a secure routing protocol. Authentication is an essential component of such protocols, and TrueLink can use any such mechanism for its own authentication needs.
TrueLink performs link verification between two nodes i and j in two phases: the *rendezvous phase*, and the *authentication phase*. In the rendezvous phase, i and j exchange nonces α_j and β_i, where the subscript indicates the node that generated the nonce (i.e., randomly generated numbers) via a single RTS-CTS-DATA-ACK exchange. This exchange proves the adjacency of the responding node through the use of strict timing constraints; only a direct neighbor is able to respond in time. In the authentication phase, i and j each sign and transmit the message (α_j, β_i), mutually authenticating themselves as the originator of their respective nonce. The timing constraints of the rendezvous phase make TrueLink immune to capture and replay style wormhole attacks, and strictly limit the range of attacks based on bit-by-bit or "cut-through" forwarding. TrueLink combines many attractive features, which make it a good candidate for practical deployment:

- *Deploy ability with minimal requirements:* TrueLink does not rely on precise clock synchronization, GPS coordinates, overhearing, or geometric or statistical methods.
- *Backwards compatibility with IEEE 802.11*: TrueLink can be implemented using standard IEEE 802.11 hardware with a minor, backwards compatible, firmware update.
- *Compatible with most authentication methods:* TrueLink can be used equally well with asymmetric, symmetric, hash based or other authentication mechanisms.
- *Widely applicable:* TrueLink is independent of the routing protocol used, and improves the security of both proactive and reactive routing protocols.

Lazos et al [7] propose a 'graph-theoretical' method for characterizing the wormhole attack and derives the necessary and sufficient conditions for any candidate solution to prevent wormholes. This theory, proposes a *Local Broadcast Key* (LBK) based for secure an ad-hoc network from wormhole attacks. In doing so, authors show that LBK solution satisfies the necessary graph theoretic condition. Unlike proposed method in [1], this approach does not require time synchronization, or highly accurate clocks, and only a small fraction of nodes need to know their location. This approach has low overhead in computation and communication.
This method is based on the use of Location (Aware 'Guard' Nodes (LAGNs)). Authors use 'local broadcast keys' (keys valid only between one-hop neighbors with name LBK) to defy wormhole attackers: a message encrypted with a local key at one end of the network cannot be decrypted at another end. Lazos proposes to use hashed messages from LAGNs to detect wormholes during the key establishment. A node can detect certain inconsistencies in messages from different LAGNs if a wormhole is present. Without a wormhole, a node should not be able to hear two LAGNs that are far from each other, and should not be able to hear the same message from one guard twice.

M.Khabbazian et al [2] we propose a proactive countermeasure based on timing analysis. Timing analysis techniques are based on the fact that a packet can travel at most at the speed of light. Therefore, a node can estimate its distance to a sender by multiplying Packet Travel Time (*PTT*) by the light speed (*c*). This method requires the nodes to have tightly synchronized clocks. Moreover, the sender needs to know the precise sending time which may not be possible in.

Using this scheme, each node can validate vicinity of all its neighbors in two rounds of communication. In the first round, each node sends a *signed* Hello message containing its ID and a nonce, and records the time at which the message is fully sent. It follows that after the first round, each node has a list of all its potential neighbors. In the second round, each node signs and sends a *follow-up* packet. The follow-up packet includes the time at which the node's Hello message was sent (in the first round), the list of all the ID's in the received Hello messages together with their corresponding nonces and the times at which they were received. Nonces are used to prevent malicious nodes to masquerade a legitimate node. Note that neither Hello messages nor follow-up packets are times tamped with their transmission time. Therefore, the nodes do not require computing a signature while having to timestamp the packet with its transmission time. After the second round, each node has a list of all its 2-hop neighbors. Therefore, it can employ the Maheshwari's algorithm [14] to further check the existence of a wormhole. Maheshwari's algorithm uses local neighborhood information to find a forbidden structure. The algorithm is based on the fact that inside a fixed region it is not possible to pack too many nodes without having edges between them.

Method	*Requirements*	*Commentary*
Packet leashes, geographical [1]	GPS coordinates of every node; Loosely synchronized clocks (ms)	Strong; have restrictions of GPS technology
Packet leashes, temporal[1]	Tightly synchronized clocks (ns)	required high time synchronization level
SECTOR [4]	GPS coordinates; Loosely Synchronized clocks (ms)	Module For Single Bit Communication
Directional Antenna [3]	All nodes use omnidirectional antennas	Directional Antennas (special hardware)
TrueLink [13]	Loosely synchronized clocks(ms); minor changes in IEEE 802.11-capable hardware's	Any special thing
Proposed method in [2]	Loosely synchronized clocks (ms)	Strong, using GPS technology

Table 1. Summary of wormhole prevention methods.

2.2. Comparison of Preventing Approaches

Among proactive methods, timing-based solutions attempt to restrict the maximum distance between two neighbors by computing the Packet Travel Time (PTT) [2]. In the proposed method in [1], each sender stamps the packet with the time at which it is sent. The receiver can then compute *PTT* by comparing the time stamp with the time at which it receives the packer. In [4], *PTT* is computed through a series of fast one-bit exchanges. This method

requires fast switching between the receiver and sender. In [13], the authors propose a similar asynchronous method that does not need fast switching and requires only minor changes in IEEE 802.11-capable hardware's. Proposed method in [7], utilizes a combination of location information and cryptography to prevent the wormhole attack. In [2], the nodes do not need to have synchronized clocks, and are not required to predict the sending time or to be capable of fast switching between the receiver and sender. Moreover, the nodes do not need to communicate with all their neighbors' one-to- one. Table 1 shows these proactive methods requirements and some Commentary.

3. Reactive countermeasures against wormhole attack

Reactive methods, on the other hand, don't need specialized hardware and time synchronization or time measurement, or to transmit maximum power in a particular direction.

3.1. Avoiding Wormhole Attack Approaches

EDWA [15] is one of the reactive and end-to-end countermeasures against wormhole attack in wireless ad hoc networks. A simple comparison method based on the estimated shortest path and the actual shortest path is used to determine whether there is a wormhole attack for each received route. Based on its own measured position and the receiver's position, the sender estimates the shortest path in terms of hop count. The sender also retrieves the hop count value from the received ROUTE REPLY packet and compares it with the estimated value. This method denotes the estimated hop count of the shortest path as h_e and the value from the ROUTE REPLY packet as h_r. If the received hop count value is smaller than the estimation, that is $h_r < \alpha.h_e$, the sender predicts a wormhole attack and will mark the corresponding route. Since h_e is the estimated shortest path between the source and the destination, the source node is expecting that all legitimate routes will be at least as long as α times the estimation. α is a parameter adjustable to the network. In our simulation we use $\alpha = 1$. If some shortest routes have smaller hop count than the estimated value, it is with high probability that the route has gone through a wormhole as a wormhole tends to bring nodes that are far away to be neighbors. Once a wormhole attack is detected, the source node launches wormhole TRACING procedure to identify the two end points of the wormhole and the result is broadcast into the network to warn other nodes. Finally, based on the wormhole detection and identification the source could select shortest route from a set of legitimate routes [15].

In [16], authors' have proposed a layered clustering approach where intrusion detection has been done in a cluster based mode to guard over of wormhole attacks. This method is used for detecting whether a node is joining in a wormhole attack. From security point of view, this will also reduce the risk of a cluster head being compromised. The entire network in this method is separated in clusters as in figure 3. The clusters may be overlapped or disjoint. Each cluster has its own cluster head and a number of nodes designated as member nodes. Member nodes pass on the information only to the cluster head. The cluster-head is responsible for passing on the aggregate information to all its members. The cluster head is elected dynamically and maintains the routing information.

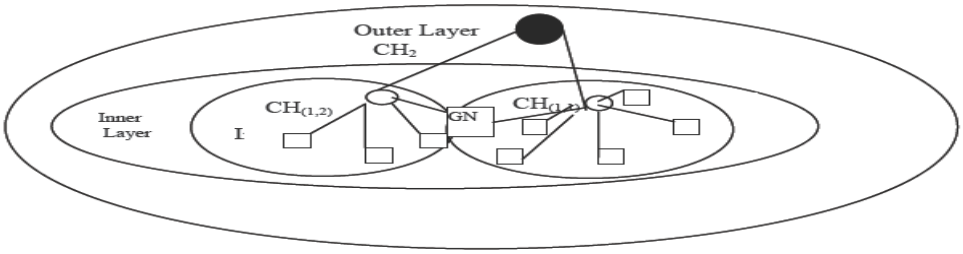

Fig 3. The Layered structure [16]

When a node in the i^{th} cluster of layer 1 suspect wormhole attack within the cluster, it informs the cluster head of i^{th} cluster at layer 1, which is denoted as CH (1,i). CH(1,i) informs cluster head at layer 2 (CH_2), about the malicious node. CH_2 broadcast this information to all cluster heads at layer 1. The cluster heads at layer 1 inform their respective cluster members.

We proposed another reactive approach for detecting, securing and avoiding wormhole attack in [17]. In this method we define cluster head nodes while a node wants connect more than two nodes. Each cluster head are connected with other cluster heads with one or more hops, and in each cluster head's routing table, moreover the distance until his cluster members, distances between neighbors cluster head's written. Malicious nodes are nodes that make virtual tunnel between each other that we call wormhole. In this paper w also used WADP[1] packet (consist wormhole route information): When a node suspect one route to be in wormhole tunnel, sends a WADP packet to his nearest cluster head and his routing table members nodes. For detecting and avoiding this kind of attack In this approach we divided attacker goals in wormhole attack in three main parts:

A. Attacker's wants to read or modify transition packets between sender and recipient: for defending this case of attack when a node wants to send a packet, at first all routes until destination will be found with broadcasting ROUTE REQUEST and ROUTE REPLY packets. After that, a private key will send to destination, from a route that is bigger than the shortest route then we initialize to send packets. We also add one *flag* bit with name *R/W*[2] to all packets that we send. This R/W flag bit has this characteristic that when a node wants modify packet, the data of this bit will be clear. Therefore recipient will be announcing of eavesdropping. And will send a WADP packet to his cluster head node and that cluster head will broadcast that packet to all neighbor cluster heads. And in parallel cluster heads send that packet for his cluster members. Each node that receive WADP packet updates his routing table by dropping wormhole route from his table. Finally that route information will dropped from all nodes routing tables. Therefore with this technique, attackers cannot read or write any of packets.

B. Attacker's wants to drop transition packets between sender and recipient: we consider that dropping packet is because of two main reasons: a) maybe the physical or wireless link between nodes are disconnected. In this case if sender, don't receive ack packet from receiver after a specified time slice, will send WADP packet for his cluster head node. b) Malicious nodes drop all packets or some of them and make them on irregular sequence. In this case if the receiver, revives packets on irregular sequence, will send a WADP packet to

[1] Wormhole Attack Detection Packet
[2] Read/Write Flag Bit

his cluster head. In that two manners ‘a’ and ‘b’, after cluster head receives WADP packet, will broadcast that packet to all neighbor cluster heads. And in parallel cluster heads send that packet for his cluster members. Each node that receive WADP packet updates his routing table by dropping wormhole route from his table. Finally that route information will dropped from all nodes routing tables. Therefore with this technique, if attacker drops some or all packet, or if the route disconnect, another nodes on the network will detect that, and will avoid sending packet from that route.

C. Sometimes malicious nodes records one packet at one end point and relayed to the other end and re-broadcasted into the network. Furthermore, the attackers can mount the attack without revealing their identities [1]. This kind of attack is because of that the senders IP is valid and known’s for all nodes on the network and they don’t suspect him. Attackers can make traffic and lose bandwidth with sending one packet more and more in the network. For detecting this kind of attack, receiver can periodically check header file that one packet don’t send more than one time for receiver. And for avoiding that, receiver will send WADP packet to his cluster head to announce other nodes, that route is unsecure and must remove from all routing table.

3.2. Comparison of Avoiding Approaches

Proposed method in EDWA [15] is an end-to-end method that with using TRACING procedure to identify the two end points of the wormhole and the result of that is broadcast into the network to warn other nodes. Finally, based on the wormhole detection and identification the source could select a shortest route from a set of legitimate routes. In [16] authors’ improved a cluster base approach that with using loosely synchronized clocks (ms) can only detect attack. Our method in [17] can effectively detect and avoid wormhole by using R/W bit and WADP packet and not any Synchronization and geographical devices. Table 2 comparisons these three methods in more details.

Method	*Geographical Device*	*Clock Synchronization*	*Other Special Requirements*	*usage*
EDWA [15]	Yes	No	TRACING procedure	Detect & Identify
Proposed method in [16]	No	Loosely synchronized clocks (ms)	No	Only Detecting
Our Method in [17]	No	No	R/W Flag Bit & WADP Packet	Detect, Secure & Avoid

Table 2. Summary of wormhole avoidance methods.

References

[1] Hu. Y. C., Perrig. A. & Johnson. D. B. (2003). *Wormhole Attacks in Wireless Networks.* in Proc. INFOCOM, Vol. 3, pp. 1976-1987.

[2] Khabbazian.M, Mercier. H & Bhargava. V.K. (2009). *Severity Analysis and Countermeasure for the Wormhole Attack in Wireless Ad Hoc Networks*. IEEE TRANSACTIONS on Wireless Communications, VOL 8, NO. 2.
[3] Hu. L. & Evans D., (2004). *Using directional antennas to prevent wormhole attacks.* in Proc. Network and Distributed System Security Symposium, Vol. 1.
[4] Capkun. S., Buttyan. L. & Hubaux. J. P., (2003). *SECTOR: secure tracking of node encounters in multi-hop wireless networks.* in Proc. First ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 21-32.
[5] Kassi.R.E, Chehab A., & Dway Z. (2005). *DAWWSEN: A Defense Mechanism against Wormhole Attacks in Wireless Sensor Networks*. in proceeding of the second International conference on innovations in information Technology (ITT' 05), UAE.
[6] Park. T., & Shin. K. (2004). *LISP: A Lightweight Security Protocol for Wireless Sensor Networks.* In proceedings of ACM transaction on Embedded Computing systems.
[7] Lazos. L., Poovendran. R., Meadows. C., Syverson. P. & Chang. L. W. (2005) "Preventing wormhole attacks on wireless ad hoc networks: a graph theoretic approach," in Proc. WCNC, pp. 1193-1199.
[8] Win. K.S. (2008). *Analysis of Detecting Wormhole Attack in Wireless Networks*. World Academy of Science, Engineering and Technology 48, pp. 422-428.
[9] Awerbuch. B., Holmer. D., Nita-Rotaru. C. & Rubens. H. (2002). *An on demand secures routing protocol resilient to byzantine failures.* ACM Workshop on Wireless Security (WiSe).
[10] Hu. Y.-C., Perrig. A. & Johnson. D. B. (2006).*Wormhole Attacks in Wireless Networks.* Selected Areas of Communications, IEEE Journal on, vol. 24, numb. 2, pp. 370- 380.
[11] Hu. Y., Perrig. A. & Johnson. D. (2004). *Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks.*, in Proc. INFOCOM ,Vol. 3, pp. 1976-1987.
[12] Sun. K., Ning. P., Wang. C., Liu. A. & Zhou. Y. (2006). *TinySeRSync: secure and resilient time synchronization in wireless sensor networks.* In Proc. 13th ACM Conference on Computer and Communications Security,.
[13] Eriksson. J., Krishnamurthy. S. V. & Faloutsos. M. (2006). *Truelink: a practical countermeasure to the wormhole attack in wireless networks*. In Proc. IEEE International Conference on Network Protocols, Vol. 10, pp. 75-84.
[14] Maheshwari. R., Gao. J. & Das. S. R. (2007). *Detecting wormhole attacks in wireless networks using connectivity information.* in Proc. INFOCOM, pp. 107-115.
[15] Wang, Wong. (2007). *EDWA: End-to-end detection of wormhole attack in wireless Ad hoc networks.* International Journal of Information and Computer Security (IJICS), under revision.
[16] Roy. B., &Chaki, (2009). *A NEW CLUSTER-BASED WORMHOLE INTRUSION DETECTION ALGORITHM FOR MOBILE AD HOC NETWORKS*. International Journal of Network Security & Its Applications (IJNSA), Vol 1, pp. 44-52.
[17] Ghanbarzadeh.Y, Heidari.A. (in proc 2011). *Wormhole Attack in Wireless Ad-hoc Networks.* International Conference on Information and Computer Applications ICICA, Dubai, UAE.