Exploration of Wormhole Attack with its Detection and Prevention Techniques in Wireless Ad-hoc Networks

Bintu Kadhiwala
Computer Engineering Department
Sarvajanik College of Engineering and Technology
Surat, India

Harsh Shah
Computer Engineering Department
Sarvajanik College of Engineering and Technology
Surat, India

ABSTRACT
Security emerges as a central requirementas mobile ad hoc network applications are deployed. In this paper, we introduce the wormhole attack, a severe attack in ad hoc networks that is particularly challenging to defend against. Wormhole attacks enable an attacker with limited resources and no cryptographic material to wreak havoc on wireless networks. It is possible even if the attacker has not compromised any hosts and even if all communication provides authenticity and confidentiality.Wormhole attacks can form a serious threat in wireless networks.

INDEXTERMS
Ad Hoc network, Wormhole attack, malicious node

1. INTRODUCTION
With the rapid development of mobile technologies however, the use of networks is not limited through earthbound cables anymore. Combining peer-to-peer techniques with the opportunities that mobility offers, so called Ad Hoc networks have become an important field of research in recent years. These networks are especially attractive for scenarios where it is infeasible orexpensive to deploy significant networking infrastructure[1].

An Ad Hoc network is defined as "an autonomous system of routers and associated hosts connected by wireless links, the unions of which form an arbitrary graph. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet operating as a hybrid fixed/ad hoc network." [2]

It is a collection of communication devices (nodes) which communicate with each other through wireless medium without the aid of centralized or fixed infrastructure. The nodes in ad hoc networks can be stationary or mobile, the latter being the most common situation. The absence of the centralized infrastructure implies that the responsibility of the nodes is equal. Therefore, participating nodes in the network need to cooperate in order to establish routes and to forward packets for other nodes.

Figure-1 depicts a simple ad hoc network of three nodes A, B and C. The layout shows that B relays messages between A and C. The dependence on B is because mobile nodes have power constraints and as a result, their transmission ranges are short.

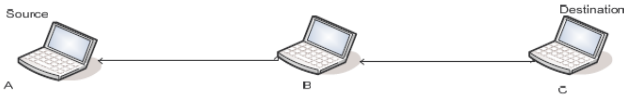


Fig. 1. **Three nodes Ad Hoc Network**

The remainder of the paper isorganized as follows. In Section 2, we have described the wormhole attack. Then, how the wormhole attack can be launched in the wireless network is explained in Section 3. In Section 4, various prevention methods against the wormhole attack are discussed.

2. WORMHOLE ATTACK
A severe security attack, called the wormhole attack, has recently been introduced in the context ofad-hoc networks [3], [4], [5].The wormhole attack is an attack in which attacker records packets (or bits) at one location in the network, tunnels them to another location, using either in-band (tunneling) or out-of-band communication and retransmits them there into the network[6].In a wormhole attack, a malicious node uses a path outside the network to route messages to another compromised node at some other location in the network. This is illustrated in the figure-2.

Thus, it can give nodes that are in the neighborhood of the attackers the impression that links exist between them andother nodes that are in reality faroutside of transmissionrange

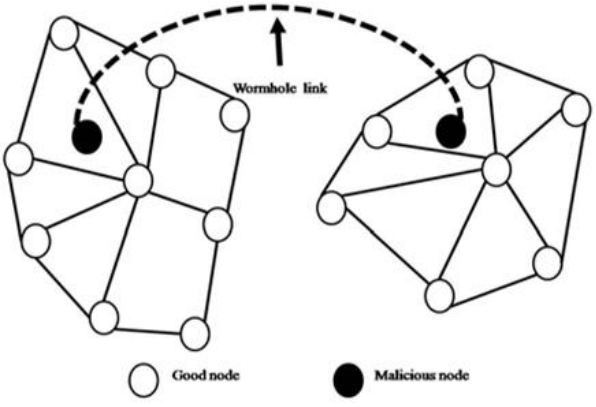


Fig. 2. **The Wormhole Attack[7]**

and thus creating the illusion of a link, attackers may be able to manipulate nodes to send more traffic through them; this traffic may then be dropped, modified or recorded.[8].

Due to the nature of wireless transmission, the attacker can create a wormhole even for packets not addressed to itself, since it can overhear them in wireless transmission and tunnel them to the colluding attacker at the opposite end of the wormhole.According to whether the attackers are visible on the route, the classification of the wormholes can be into three types:[9]Closed Wormhole Attack, Half open Wormhole Attack, and Open Wormhole Attack.

In closed wormhole attack, the attackers do not modify the content of the packet, even the packet in a route discovery packet. Instead, they simply tunnel the packet form one side of wormhole to another side and it rebroadcasts the packet.

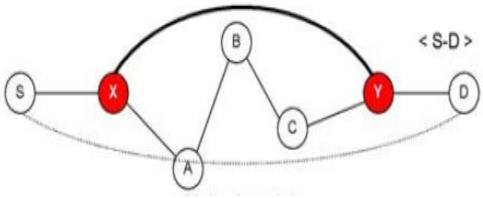


Fig. 3. **Closed wormhole[10]**

In half open wormhole attack, one side of wormhole does not modify the packet and only another side modifies the packet, following the route discovery procedure.

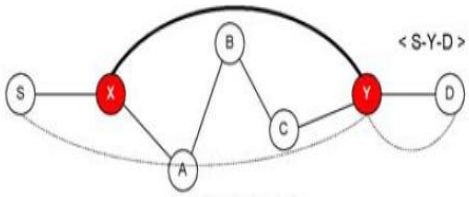


Fig. 4. **Half open wormhole[10]**

In open wormhole attack, theattackers include themselves in the RREQ packet headerfollowing the route discovery procedure. Other nodes areaware that the malicious nodes lie on the path but they wouldthink that the malicious nodes are direct neighbors.

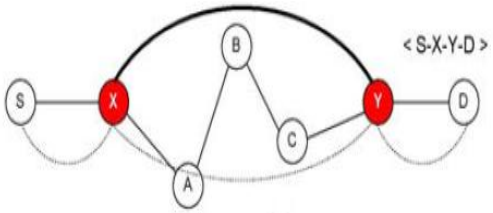


Fig. 5. **Open wormhole[10]**

3. HOW WORMHOLE ATTACK CAN BE LAUNCHED?

The tunnel can be established in many different ways. Wormhole modes differ in the level of sophistication needed by the adversary. The wormhole attack can be launched with the following modes: [11]

A. Packet encapsulation

In this mode, nodes A and B try to discover the shortest path between them, in the presence of the two malicious nodesX and Y. Node A broadcasts a route request (REQ), X gets the REQ and encapsulates it in a packet destined to Y through the path that exists between X and Y (U-V-W-Z). Node Y demarshalls the packet, and rebroadcasts itagain, which reaches B.

Due to the packet encapsulation, the hop count does not increase during thetraversal through U-V-W-Z. Concurrently, the REQ travels from A to B through C-D-E. Node B now has tworoutes, the first is four hops long (A-C-D-E-B), and the second is apparently three hops long (A-X-Y-B). Node B will choose the second route since it appears to be the shortest while in reality it is seven hops long.So X and Y succeed in involving themselves in the route between A and B. Any routing protocol that uses the metric ofshortest path to choose the best route is vulnerable to this mode of wormhole attack.

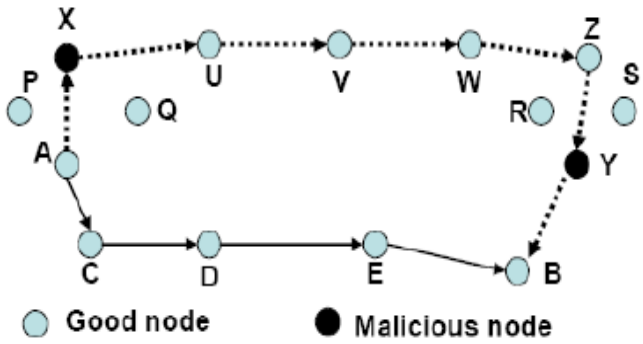


Fig. 6. **Wormhole through Packet Encapsulation[11]**

This mode of the wormhole attack is easy to launch since the two ends of the wormhole do not need to have any cryptographic information, nor do they need any special capabilities, such as a high speed wire line link or a high power source.

B. Out-of-band channel

In this, Node A is sending a route request to node B,nodes X and Y are malicious having an out-of-band channel between them.Node X tunnels the route request to Y,which is a legitimate neighbor of B.Node Y broadcasts the packet to its neighbors, including B. Node B gets tworoute requests A-X-Y-B and A-C-D-E-F-B. The first route is both shorter and faster than the second, and is thuschosen by B. This results into a wormhole being established between X and Y on the route between A and B.

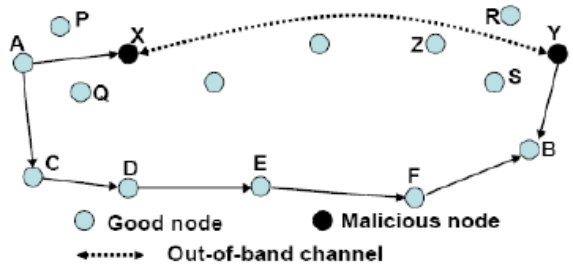


Fig. 7. **Wormhole Attack through out of band channel[11]**

C. High power transmission

In this mode, when a single malicious node gets a route request, it broadcasts the request at a high powerlevel, a capability which is not available to other nodes in the network. Any node that hears the high-powerbroadcast, rebroadcasts it towards the destination. By this method, the malicious node increases its chance to be inthe routes established between the source and the destination even without the participation of a colluding node. A simple method to mitigate this attack is possible if each node can accurately measure the received signal strengthand has models for signal propagation with distance. In that case, a node can independently determine if thetransmission it receives is at a higher than allowable power level. However, this technique is approximate at bestand dependent on environmental conditions.

D. Packet relay

Wormhole using PacketRelay is another mode of the wormhole attack in which amalicious node relays packets between two distant nodes toconvince them that they are neighbors. It can be launchedby even one malicious node. Cooperation by a greaternumber of malicious nodes serves to expand the neighborlist of a victim node to several hops.

It is carried out by anintruder node X located within transmission range oflegitimate nodes A and B, where A and B are not themselveswithin transmission range of each other. Intruder node X merely tunnels control traffic between A and B and viceversa, without the modification presumed by the routingprotocol e.g. without stating its address as the source in thepackets header so that X is virtually invisible. This results inan extraneous inexistent A - B link which in fact is controlledby X, as shown in figure-8 below.

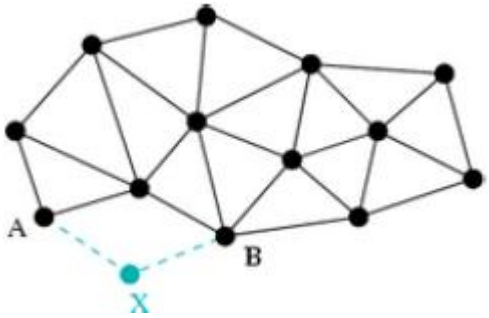


Fig. 8. Wormhole created by node X[7]

Node X can afterwards droptunneled packets or break this link at will. Thus, an extraneous A -B link can be artificially created by an intruder node X bywormholing control messages between A and B. Two intrudernodes X and X′, connected by a wireless or wired privatemedium, can also collude to create a longer wormhole which is more harmful, as shown in figure-9 below.

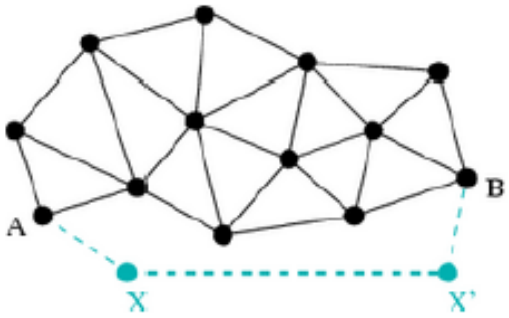


Fig. 9. A longer wormhole created by two colluding nodes[7]

4. WORMHOLE PREVENTION METHODS

The solution to wormhole attack can be characterized into Location and Time Based Solutionsand Neighbor Based Solutions. Packet Leashes and End to End detection are the location and time based solutionswhereas Lightworp – a light weight countermeasure is the neighbor based solution.

A. Packet Leash

Wormholes are hard to detect because the path that is used to pass on information is usually not part of the actual network. The general mechanism for detecting and, thus defending against wormhole attacks is “packet leash”[6].

“A leash is any information that is added to a packet designed to restrict the packet’s maximum allowed transmission distance.”

Leashes are designed to protect against wormholes over a single wireless transmission; when packets are sent over multiple hops, each transmission requires the use of a new leash.Leashes prevent wormhole attacks by letting the receiver of a packet determine if a packet has traveled further than the leash allows.

There are basically two types of leashes –Geographical Leash and Temporal Leash

In Geographical Leashes, each packet is stamped,upon transmission, with the current geographical location ofthe sending node, and signed by the sender. The receiver ofthe packet compares the location of the sender to its ownlocation, and is thus able to determine whether the senderis close enough to be a neighbor. It requires accurate and verifiable location information[8].

In Temporal Leashes, all nodes have tightly synchronized clocks. The sender stamps the packet with the current time, and signs it for later authentication. The receiver compares the time in the packet with its local clock. If the difference exceeds some small value, determined by the maximum transmission range of the radio in use, the packet is discarded. It requires extremely tight global clock synchronization, making it infeasible for many applications[8].

B. End to End Detection Method

This method has three phases, namely: Wormhole DETECTION, Wormhole TRACING and Select legitimate route for data communication.[12]

In Wormhole DETECTION, source node estimates minimum hop count between itself and destination. In some routing protocols of wireless ad hoc networks, the source node first initiates a routing discovery by broadcasting a ROUTE REQUEST packet. All intermediate nodes continue broadcasting the ROUTE REQUEST upon receiving it until the ROUTE REQUEST reaches the destination or some nodes that have a

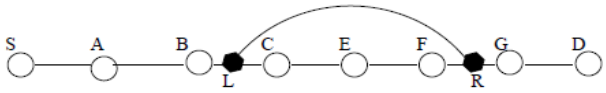
route to the destination. Then a ROUTE REPLY will be unicasted back to the source along a pre-cached path or according to the path in the packet header.

But here the routing protocol is modified such that it is resilience to wormhole attack. As specified in the above, the sender initiates a route discovery by broadcasting a ROUTE REQUEST packet into the network. The sender sets the flag such that only the receiver can respond the ROUTE REQUEST packet. Once the ROUTE REQUEST packet reaches the receiver, the receiver responds with a ROUTE REPLY with its current position. The sender authenticates the received ROUTE REPLY from the receiver. Then it retrieves the receiver's position from the packet.

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. We denote the estimated hop count of the shortest path as he and the value from the ROUTE REPLY packet as hr. If the received hop count value is smaller than the estimation, sender predicts a wormhole attack and will mark the corresponding route.

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.

To further identify the two end points of the wormhole the source starts wormhole TRACING procedure. Once a wormhole is detected by the sender, the sender temporarily enables the path with wormhole and sends out a TRACING packet to the receiver. This TRACING packet is forwarded by each intermediate node through the route with wormhole. When a node in the route receives the TRACING packet, it acknowledges the source node with its current position by replying a TRACING-RESPONSE packet. The source will then estimate shortest path to each intermediate node and identify the two end points of the wormhole in a small area.



S–	A	B	G	D
Received route length (hop count)	1	2	3	4
Estimated route length (hop count)	1	2	6	7

S–A–B–C–E–F–G–D: the shortest path from S to D without wormhole
S–A–B–G–D: the shortest path received from route reply packet
L, R: the two end points of the wormhole which is connected through other connection

Fig. 10. **An example of wormhole tracing [12]**

The above figure-10 depicts a shortest path from S to D. The first row of the table denotes the received path S-A-B-G-D. The second row records the corresponding hop count to each intermediate node and the destination. Then estimated values are shown in the third row. A peak increase can be observed at node G, and then the source asserts that the wormhole lies between node G and its previous hop B.

In Select legitimate route for data communication, the source selects a shortest path from all received paths. However, the shortest path is not always the first reply that the source obtained from the destination. Thus, the source could not determine whether there are wormhole attack based on the first received ROUTE REPLY. In addition, in case a wormhole is detected, the source has to wait to make its decision until a wormhole has been traced and identified. Based on that, we allow the source to wait for a certain time T before selecting a route for its data communication.

If the route has the property that the received hop count is greater than equal to estimated hop count, then the sender will select the shortest route from the set of legitimate routes for data communication.

C. LITEWORP: A Lightweight Countermeasure

LITEWORP uses secure two-hop neighbor discovery and localmonitoring of control traffic to detect nodes involved in the wormhole attack[11].It provides a countermeasuretechnique that isolates the malicious nodes from the network thereby removing their ability to cause futuredamage. It does this by two steps: Building neighbor list andLocal monitoring.

In Building neighbor list step, as soon as a node, say A, is deployed in the field, it does a one-hop broadcast of aHELLO message. Any node, say B, that hears the message, sends back an authenticated reply to A, using theshared key. Node A accepts all the replies that arrive within a timeout. For each reply, A verifies the authenticityof the reply and adds the responder to its neighbor list RA. Then A does a one-hop broadcast of a messagecontaining the list RA. This broadcast is authenticated individually by the shared key with each member in RA.

When B hears the broadcast, it verifies the authenticity of RA, and stores RA if correctly verified. Hence, at the end of this neighbor discovery process, each node has a list of its direct neighbors and the neighbors of each one of its direct neighbors.

This requires a larger memory than simply keeping a list of first hop and second hop neighbors. This process is performed only once in the lifetime of a node. Henceforth, a node will not accept a packet from a node that is not a neighbor nor forward to a node that is not a neighbor. Also, second hop neighbor information is used to determine if a packet is legitimate or not. If a node C receives a packet forwarded by B purporting to come from A in the previous hop, C discards the packet if A is not a second hop neighbor. After building its first and second hop neighbor list, node A activates local monitoring.

In Local Monitoring step, a collaborative detection strategy for wormholes is used, where a node monitors the traffic going in and out of its neighbors. For a node, say α, to be able to watch a node say, β, following two conditions are required:

- Each packet forwarder must explicitly announce the immediate source of the packet it is forwarding, i.e., thenode from which it receives the packet, and
- α must be a neighbor of both β and the previous hop from β, say ζ. If the second condition is satisfied, we call a guard node for the link from ζ to β.

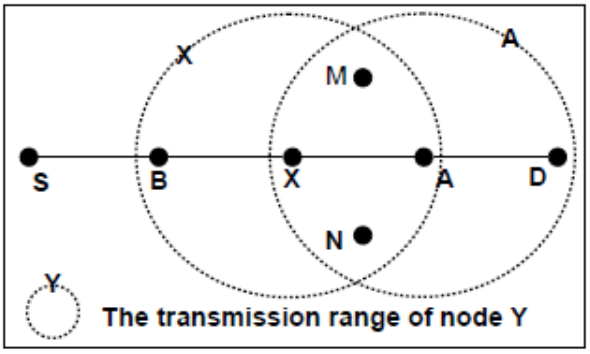


Fig. 11. **X, M, and N are guards of the link from X to A[11]**

This implies that α is the guard node for its entire outgoing links. For example, in figure-11, nodes M, N, and X are the guard nodes of the link from X to A. Information from each packet sent from X to A is saved in a watch buffer at each guard. The information includes the packet identification and type, the packet source, the packet destination, the packet's immediate sender (X), and the packet's immediate receiver (A). The guards expect that A will forward the packet towards the ultimate destination, unless A is itself the destination. Each entry in the watch buffer is time stamped with a time threshold, by which A must forward the packet. Each packet forwarded by A with Xas a previous hop is checked for the corresponding information in the watch buffer.

A malicious counter (MalC(i,j)) is maintained at eachguard node, i, for a node, j, at the receiving end of eachlink that i is monitoring. MalC(i,j) is incremented forany malicious activity of j that is detected by i. Theincrement to MalC depends on the nature of themalicious activity detected.

When MalC(a,A) crosses a threshold, Ct , a revokes A from its neighbor list, and sends to each neighbor of A, say D, an authenticated alert message indicating A is a suspected malicious node.When D gets enough alert messages, γ , about A, it isolates A by marking A's status as revoked in the neighbor list. After isolation, D does not accept or send any packet to a revoked node.this isolation is performed locally within the neighbors of the malicious node.This makes the response process quick and lightweight, and has the desired effect of removing the malicious nodes from the network.

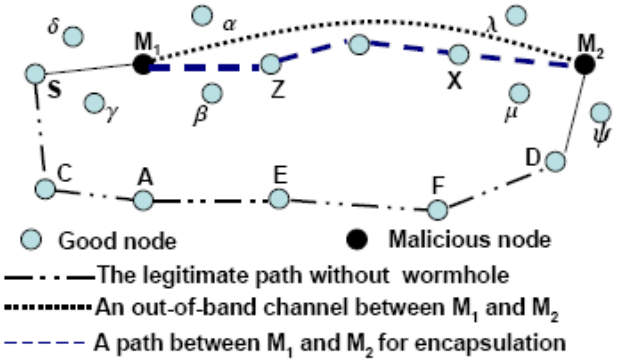


Fig. 12. **Wormhole detection for out-of-band and packet encapsulation modes [11]**

Consider the scenario in the figure-12 in which M1 and M2 are two malicious nodes wishing to establish a wormhole between the two nodes S and D. When M1 hears the REQ packet from S, it directs the packet to M2. Node M2 rebroadcasts the REQ packet after appending the identity of the previous hop from which it got the REQ. Node M2 has two choices for the previous hop -- either to append the identity of M1, or append the identity of one of M2's neighbors, say X. In the first choice all the neighbors of M2 will reject the REQ because they all know, from the stored data structure of the two-hop neighbors, that M1 is not a neighbor to M2. In the second case, all the guards of the link from X to M2 will detect M2 as fabricating the route request since they do not have the information for the corresponding packet from X in their watch buffer.

In both cases, M2 is detected, and the guards increment the MalC of M2. In addition, the REP packet may also be used for detection of M1 and M2. When D gets the REQ, it generates a route reply packet, REP, and sends it backM2. The guards of the link from D to M2overhear the REP and save an entry in their watchbuffers.

Node M2 sends the route reply back to M1 using the out-of-band channel or packet encapsulation. After t timeunits, the timers in the watch buffers of the guards run out, and thus the guards detect M2 as droppingthe REP packet and increment the MalC of M2. However if M2 is smarter, it can forward another copy of the REPthrough the regular slower route. In this case, MalC of M2 is not incremented. When M1 gets the REP from M2, M1forwards it back to S after appending the identity of the previous hop. As before, M1 has two choices — either toappend the identity of M2, or append the identity of one of M1's neighbors, say Z. In the first choice, node S rejectsthe REP because it knows that M2 is not a neighbor to M1. Also, all the neighbors of M1 know that M2 is not aneighbor to M1. In the second case, all the guards of the link from Z to M1 detect M1 as forging the REP since theydon't have the corresponding entry from Z in their watch buffers.

5. CONCLUSION

From this paper, it is clear that how wormhole attack can be used to make a severe threat in wireless ad hoc network. As now a days security is one of the main concern, such an attack is not desirable. It's true that wormhole will not be harmful to the ad hoc network if attacker performs tunneling honestly and reliably. But we know that no attacker is "honest".

Thus, there are so many methods as we have explained can be used to defend against the wormhole attack. All the methods have its own advantages and disadvantages and hence we can use those methods that are suitable to our system.

REFERENCES

[1] I. Khalil, S. Bagchi, and N. B. Shroff. "Liteworp : A lightweight countermeasure for the wormhole attack in multihop wireless networks". In DSN, pages 612–621, 2005.

[2] IRTF RRG Ad hoc Network Scaling Research Subgroup, http://w3.antd.nist.gov/wctg/manet/adhoclinks.html

[3] C. Karlof and D. Wagner, "Secure Routing in Sensor Networks: Attacks and Countermeasures," at the 1st IEEE International Workshop on Sensor Network Protocols and Applications, May, 2003.

[4] Y. C. Hu, A. Perrig, and D.B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM), pp. 1976-1986, 2003.

[5] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole attacks," in Network and Distributed System Security Symposium, 2004.

[6] Yih-Chun Hu, Adrian Perrig and David B. Johnson "Wormhole Attacks in Wireless Networks", IEEE Journal On Selected Areas In Communications, Vol. 24, No. 2, February 2006.

[7] Marianne Azer, Sherif El-Kassas and Magdy El-Soudani, "A Full Image of the Wormhole Attacks Towards Introducing Complex Wormhole Attacks in wireless Ad Hoc Networks", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 1, No. 1, May 2009.

[8] Jakob Eriksson, Srikanth V. Krishnamurthy, Michalis Faloutsos, "TrueLink: A Practical Countermeasure to the Wormhole Attack in Wireless Networks", University of California, Riverside

[9] W. Wang, B. Bhargava, Y. Lu, and X. Wu, "Defending Against Wormhole Attacks in Mobile Ad Hoc Networks", Wiley Journal on Wireless Communications and Mobile Computing, vol. 5, pp. 1-21, 2005.

[10] K. Lee, H. Jeon, and D. Kim, "Wormhole Detection Method based on Location in Wireless Ad-Hoc Networks," in *New Technologies,Mobility and Security*: Springer Netherlands, 2007, pp. 361-37

[11] K. Issa, B. Saurabh, and B. S. Ness, "LiteWorp: Detection and Isolation of the Wormhole Attack in Static Multihop Wireless Networks", The International Journal of Computer and Telecommunications Networking vol. 51, pp. 3750-3772, 2007.

[12] Xia Wang, JohnnyWong, "An End-to-end Detection of Wormhole Attack in Wireless Ad-hoc Networks", Department of Computer Science, Iowa State University, Ames, Iowa 50011.