Round Trip Time based Wormhole Attacks Detection

Zaw Tun and Ni Lar Thein
University of Computer Studies, Yangon
zawtun78 @gmail.com, nilarthein@gmail.com

Abstract

The nature of wireless ad hoc and sensor networks make them very attractive to attackers. One of the most popular and serious attack in wireless ad hoc networks is wormhole attacks and most proposed protocols to defend against this attack used positioning devices, synchronized clocks, or directional antennas This paper analyzes the nature of wormhole attack and existing methods of defending mechanism and then proposes round trip time (RTT) based wormhole detection mechanism. The consideration of the detection mechanism is the RTT between two successive nodes to compare other successive. Wormhole is identified based on the fact that transmission time between two fake neighbors created by wormhole is considerably higher than that of each other. The propose system does not require any specific hardware, has good performance and little overhead.

1. Introduction

Ad hoc and sensor networks are emerging as a promising platform for a variety of application areas in both military and civilian domains. However, the open nature of the wireless communication channels, the lack of infrastructure, the fast deployment practices, and the hostile environments where they may be deployed, make them vulnerable to a wide range of security attacks. Among these attacks wormhole attack is hard to detect for it is not inject abnormal volumes of traffic into the network. In this work we investigate a specific type of emerging security threat knows as the wormhole attack.

Wormhole attacks can cause severe damage to the route discovery mechanism used in many routing protocols. In a wormhole attack, the malicious nodes will tunnel the eavesdropped packets to a remote position in the network and retransmit them to generate fake neighbor connections, thus spoiling the routing protocols and weakening some security enhancements. The simulation results in [6] have shown that when there are more than two wormholes in the network, more than 50% of the data packets will be attracted to the fake neighbor connections and get discarded. So we need more attention in the detection and defending against wormhole attack.

Some work has been done to detect wormhole attacks in wireless ad hoc networks [2,6,7,8,9,11,14] but they do not efficiently eliminate wormhole from the networks. In this paper, we proposed a method of detection based on the transmission time to detect and locate wormhole attacks on the Ad hoc On-demand Distance Vector (AODV) routing protocol. Our technique detects wormhole attack during route setup procedure by calculating the transmission time between each two successive nodes along the established route. Our assumption is that transmission time between two wormhole nodes is considerably higher than that between two legitimate successive nodes. Our system does not need any specific hardware to detect wormhole and the computational overhead is only little and it can also pinpoints the wormhole attacks.

The remaining sections of the paper are structured as follows: Section 2 describes the wormhole attacks in detail. Section 3 studies the detection and countermeasure of wormhole attacks, Section 4 discuss the propose detection mechanism. Finally, we draw conclusions in Section 5.

2. Wormhole Attacks

In the wormhole attack [6,7], a malicious node tunnels messages received in one part of the network over a low latency link and replay them in a different part. 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. The tunnel can be established in many different ways, such as through an out-of band hidden channel (e.g., a wired link), packet encapsulation, or high powered transmission. The tunnel creates the illusion that the two end points are very close to each other, by making tunneled packets arrive either sooner or with lesser number of hops compared to the packets sent over normal routes. This allows an attacker to subvert the correct operation of the routing protocol, by controlling numerous routes in the network. Later, he can use this to perform traffic analysis or selectively drop data traffic. The wormhole attack mainly consists in network layer attacks when the attack is classified according to network protocol stacks. A.A. Pirzada and C.McDonald [10] analyzed the creation of the wormhole and poses three ways:

1) Tunneling the packets above the network layer

2) Long Range tunnel using high power transmitters

3) Tunnel creation via wired infrastructure

Wormhole facilitates a number of attacks against key establishment and routing protocols [7,8]. Once the wormhole attackers have control of a link, they can do a number of things to actively disrupt the network. The wormhole attack can affect network routing, data aggregation and clustering protocols, and location-based wireless security systems. Finally, it is worth nothing that the wormhole attack can be launched even without having access to any cryptographic keys or compromising any legitimate node in the network. The wormhole attacks are particularly dangerous against many ad hoc network routing protocols in which the nodes that hear a packet transmission directly from some node consider themselves to be in range of (and thus a neighbor of) that node. The wormhole attacks cannot be defeated by cryptographical measures as wormhole attackers do not create separate packets- they simply replay packets already existing on the network, which pass all cryptographic checks. So it needs to defend wormhole attacks effectively.

3. Solution to wormhole attacks

In the wormhole attacks, an attacker receives packets at one point in the network, tunnels them to another point in the network, and then replays them into the network from that point. To defend against wormhole attacks, some efforts have been put into hardware design and signal processing techniques. If data bits are transferred in some special modulating method known only to the neighbor nodes, they are resistant to closed wormholes. Another potential solution is to integrate the prevention methods into intrusion detection systems. However, it is difficult to isolate the attacker with a software-only approach, since the packets sent by the wormhole are identical to the packets sent by legitimate nodes. Virtually all generalized secure extensions proposed for currently popular routing protocols do not alleviate wormhole attacks. However, since wormhole attacks are such a severe thread to ad hoc network security, several researchers have worked on preventing or detecting wormhole attacks specially. In this section, we briefly discuss their efforts.

First, we discuss a technique called ‘packet leashes’[7], which prevents packets from traveling farther than radio transmission range. The wormhole attacks can be detected by an unalterable and independent physical metric, such as time delay or geographical location. It overcomes wormhole attacks by restricting the maximum distance of transmission, using either tight time synchronization or location information. *Temporal leash* is to ensure that the packet has an upper bound on its lifetime. The sending a packet includes the time which it sent the packet and the receiving node compares this value to the time which it received the packet. Location information and loosely synchronized clocks are used together to verify the neighbor relation. The drawback of this is that they need to highly synchronized clocks. *Geographical leash* is to ensure that the recipient of the packet is within a certain distance form the sender. The sending packet includes the sending node location and its sending time. When they reach the receiving node, the receiving node computes the upper bound on the distance between the sender and its own. The drawback of this scheme is that, each node must know its own

location and all nodes must have loosely synchronized clocks. Because clock synchronization is resource demanding, and, thus, packet leashes have limited applicability in wireless sensor networks.

Wang [16] proposes an approach inspired by packet leashes, but based on end-to-end location information, rather hop-by-hop leashes in [7]. Similar to geographic packet leashes, Wang's method requires each node to have access to up-to-date GPS information, and relies on loosely synchronized clocks. In Wang's approach, each node appends its location and time to a packet it is forwarding, and secures this information with an authentication code. The packet's destination node then verifies the nodes' coordinates (i.e. verifies that reported coordinates are within the communication range) and speeds. A minor disadvantage of this approach is that the end node is left to do all verification. Just like geographical packet leashes proposed by Hu, this approach should work fine where GPS coordinates are appropriate.

Another set of wormhole prevention techniques, somewhat similar to temporal packet leashes, is based on the time of flight of individual packets. Wormhole attacks are possible because an attacker can make two far-apart nodes see themselves as neighbors. Capkun et al [3] propose a method called SECTOR which use specialized hardware that enables fast sending of one-bit challenge messages without CPU involvement, as to minimize all possible processing delays. SECTOR uses a distance-bounding algorithm to determine the distance between two communicating nodes. It can be used to prevent wormhole attacks in MANET without requiring any clock synchronization or location information. To prevent wormhole is to measure round trip travel time of a message and its acknowledgement, estimate the distance between the nodes based on this travel time, and determine whether the calculated distance is within the maximum possible communication range. To verify distance between the nodes, each node sends a one-bit challenge to the nodes it 'encounters', and wait for a response. A receiving node immediately sends a single-bit reply.

In [6], Hu and Evans propose a solution to wormhole attacks for ad hoc networks in which all nodes are equipped with directional antennas. When directional antennas are used, nodes use specific 'sectors' of their antennas to communicate with each other. Therefore, a node receiving a message from its neighbor has some information about the location of that neighbor, -it knows the relative orientation of the neighbor with respect to itself. This extra bit if information makes wormhole discovery much easier than in networks with exclusively omni-directional antennas. This approach does not require either location information or clock synchronization, and is more efficient with energy. They use directional antenna and consider the packet arrival direction to defend the attacks. They use the neighbor verification methods and verified neighbors are really neighbors and only accept messages form verified neighbors. But it has the drawback that the need of the directional antenna impossible for sensor networks.

Wang et al. [15] present a method for graphically visualizing the occurrence of wormholes in static sensor networks by reconstructing the layout of the sensors using multidimensional scaling. MDS-VOW [15] uses multidimensional scaling to reconstruct the network and detects the attack by visualizing the anomaly introduced by the wormhole, based on the distance of neighbors to a central server. In their approach, each sensor estimates the distance to its neighbors using the received signal strength. During the initial sensor deployment, all sensors send this distance information to the central controller, which calculates the network's physical topology based on individual sensor distance measurements. Whit no wormhole present, the network topology should be more or less flat, while a wormhole would be seen as a 'string' pulling different ends of the network together. Wang's approach has several aspects that may limit its applicability to general ad hoc networks. This method requires a central controller, and thus not readily suitable for decentralized networks.

L. Lazos et al. [9] describe another scheme to prevent the wormhole attacks on wireless ad hoc networks based on the use of Location-Aware 'Guard' Nodes (LAGNs). They inherit the guard node to detect the message flow between nodes. A node can detect a wormhole

attack during the fractional key distribution using single guard property and communication range constraints property. They consider that a node receives an identical message more than once because of a malicious entity replays the message or of the multipath effects. Their main consideration is the communication range. If any two guards within the area where guards heard to nodes are located and the area where guard hears at the origin point of the attack are located have a distance larger than double of radius(R) range. In simple, a sensor cannot hear two guards that are more than 2R apart. Their week is that the guard nodes are required to know their location. Lazos's method is elegant. However, it seems more suitable for dense stationary sensor networks.

N. Song et al. [13] proposed another detection technique for detection of the wormhole attacks called a simple scheme based on statistical analysis (SAM). They mainly consider the relative frequency of each link appears in the set of all obtained routes. They calculate the difference between the most frequently appeared link and the second most frequently appeared link in the set of all obtained routes. The maximum relative frequency and the difference are much higher under wormhole attack than that in normal system. The two values are together to determine whether the routing protocol is under wormhole attack. The malicious node can be identified by the attack link which has the highest relative frequency. Song's method requires neither special hardware nor any changes to existing routing protocols. In fact, it does not even require aggregation of any special information, as it only uses routing data already available to a node. These factors allow for easy integration of this method into intrusion detection systems.

Possible solutions to wormhole attacks proposed by different researchers are discussed in this section. Several researchers use distance-bounding techniques to detect network packets that travel distance beyond radio range, thus preventing packets that have gone through the wormhole from being accepted. However majority of these techniques rely on specialized hardware. Network visualization technique presented in [15] for dense sensor networks does not require special hardware, and appears to be very interesting. In this technique, each node reports its perceived distance to its neighbours to a centralized controller. Based on the data collected from network nodes, the controller calculates the estimation of netowrk's physicl topology, to which a wormhole, in certain scenarios, introduces impossibilities. We propose the detection of wormhole attacks that does not need any special hardware and additional information. Our detection mechanism is only based on the RTT of route request and reply message. This detection mechanism is explained detail in the next section.

4. Proposed Detection Mechanism

In this section we present our wormhole detection mechanism. Our mechanism does not need any special hardware or synchronized clocks because we only consider its local clock to calculate the RTT.

4.1. The System Model and Assumptions

Before we describe the mechanism, we briefly discuss our system assumptions. In this work, we assume the network are homogeneous (all network nodes contain the same hardware and software configuration), symmetric (node A can only communicate with node B if and only if B can communicate with A), and static (network nodes do not move after deployment). The radio transceivers of all members of the network operate under the same configuration throughout the lifetime of the network. All nodes are uniquely identified.

Our detection is based on the RTT of the message between nodes. Our consideration is that the adversary may longer the RTT value between successive nodes.

Upon initial deployment, the wireless network engages in a neighborhood discovery process. This gives each node's information about which sensor nodes it can communicate with directly. Next, the sensor network executes a routing protocol so that senders are able to send messages to their desired destination. For this particular application, requirements determine the functionality expected of the underlying routing protocol. Since nodes both send and receive messages, the protocol must provide nodes with

routing information so that nodes can send messages specifically to other nodes.

4.2. Route Finding

At that phase, the source node is responsible to construct the hierarchical routing tree to other nodes in the sensor field. The node sends the route request (RREQ) message to the neighbor node and save the time of its RREQ sending T_{REQ}. The intermediate node also forward the RREQ message and save T_{REQ} of its sending time. When the RREQ message reach to the destination node, it reply route reply message (RREP) with the reserved path. When the intermediate node receives the RREP message, it saves the time of receiving of RREP T_{REP}. Our assumption is based on the RTT of the route request and reply. The RTT can be calculated as

$$\mathbf{RTT} = \boldsymbol{T_{REP}}\text{-}\boldsymbol{T_{REQ}} \quad (1)$$

All intermediate nodes save this information and then send it also to the base station. The calculation of RTT is explained detail in section 4.4.

4.3. Wormhole Attacks Detection

When the source node gets the RREP, it triggers the detecting process to check if the established route is valid or not. The source node will calculate RTTs between every two successive nodes along the path based on RTT values. As we know, a considerably higher RTT value between two successive nodes than others will indicate a wormhole link between those two nodes. The question is how much higher the RTT is considered a wormhole link. As in some other proposals, we used a threshold to make the decision. The threshold can be determined based on our simulation with appropriate parameters and it will be discussed detail in section 4.5.

4.4. Calculation of RTT

In this subsection, we describe the detail calculation of the RTT. Our consideration of RTT is the time between a node send RREQ to the destination and receive RREP from that. So the case of synchronized clock is not need as they only consider their own local clock only. In this case, we assume that every node will save the time they forward RREQ and the time they receive RREP from the destination to calculate the RTT. Given all RTT values between nodes in the route and the destination, RTT between two successive nodes, say A and B, can be calculated as follows:

$$\mathbf{RTT_{A,B} = RTT_A - RTT_B} \quad (2)$$

Where RTT_A is the RTT between node A and the destination, and RTT_B is the RTT between node B and the destination.

For example, the route from source (S) to destination (D) pass through node A, and B so which routing path includes:

$S \rightarrow A \rightarrow B \rightarrow D$

whereas $T(S)_{REQ}$, $T(A)_{REQ}$, $T(B)_{REQ}$ is the time the node S, A, B forward RREQ and $T(S)_{REP}$, $T(A)_{REP}$, $T(B)_{REP}$ is the time the node S, A, B forward REP.

Then the RTT between S, A, B and D will be calculated based on equation (1) as followed:

$RTT_S = T(S)_{REP} - T(S)_{REQ}$

$RTT_A = T(A)_{REP} - T(A)_{REQ}$

$RTT_B = T(B)_{REP} - T(B)_{REQ}$

$RTT_D = T(D)_{REP} - T(D)_{REQ}$

And the RTT values between two successive nodes along the path will be calculated based on equation (2):

$RTT_{S,A} = RTT_S - RTT_A$

$RTT_{A,B} = RTT_A - RTT_B$

$RTT_{B,D} = RTT_B - RTT_D$

Under normal circumstances, $RTT_{S,A}$, $RTT_{A,B}$, $RTT_{B,D}$ are similar value in range. If there is a wormhole line between two nodes, the RTT value may considerably higher than other successive RTT values. So we can easily consider that there may be a wormhole link between these two nodes.

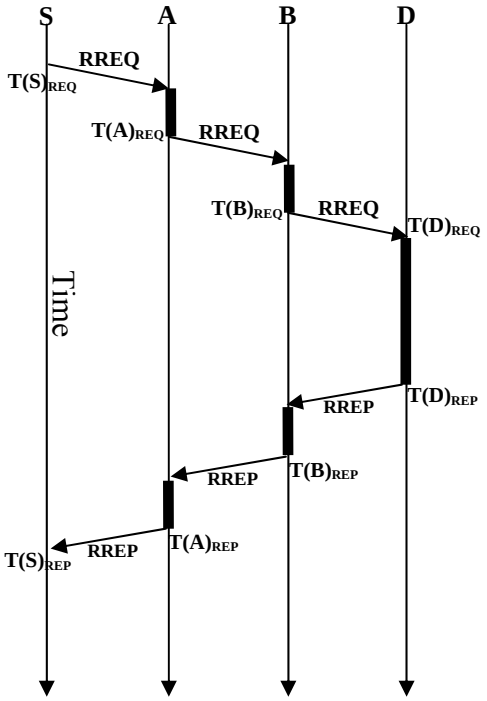

Figure 1. Time for RREQ forward and RREP accept

4.5. Evaluation

In this section, we evaluate the performance of our proposed mechanism using network simulator (ns2). In our experiments, the network includes 50,100,150 and 200 nodes deployed randomly in a 1000 meters 1000 meters field and the transmission range is defined 250 meters. There is no movement of nodes and the background traffic is generated randomly by a random generator provided by ns2. We create CBR connection with 4 packets per second and the size of the packet is 512 bytes. In our simulation, we create two wormhole nodes randomly into the network and establish a tunnel between them using encapsulation.

In here, we need to decide the value RTT, as threshold value. The value RTT is proportional to false negative rate. To get the acceptable rate of false positive and negative, we try the simulations 1000 times and get the acceptable value of 50 ms as in Figure 2, which is minimize both false positive and false negative rate.

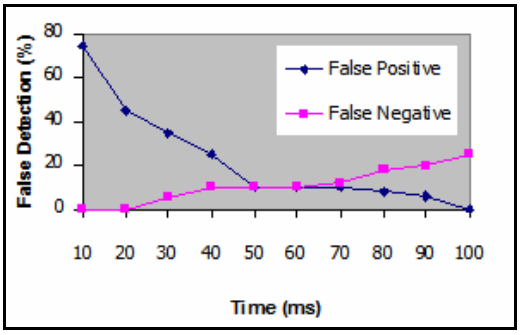

Figure 2. False Detection Rate vs Time Threshold

The following metrics are chosen to evaluate the system performance.

4.5.1 Detection Rate. The detection rate shows the actual performance of the detection in our system. The detection rate is proportional to the wormhole length. This is easy to understand because the more the wormhole length, the longer the transmission time between two fake neighbors and the easier to detect. The detection rate is 100% when the wormhole length is more than or equal to 5 hops as in Figure 3.

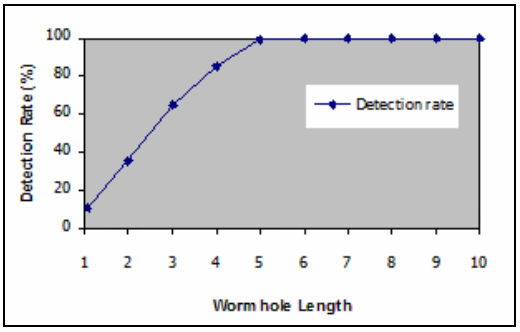

Figure 3. Detection Rate

4.5.2 Packet delivery ratio. The packet delivery ratio in this simulation is defined as the ratio between the number of packet sent by constant bit rate sources (CBR, "application layer") and the number of received packets by the CBR sink at the destination.

$$\text{Packet Delivery Ratio} = \frac{\Sigma \text{CBR packets Received by CBR sinks}}{\Sigma \text{CBR packets sent by CBR source}} \times 100\ \%$$

It describes percentage of the packets which reach the destination.

To evaluate this value, we collect all the CBR packets sent by the source node along the simulation time and also the CBR packets received by the destination node. When we make the simulation 1000 time with the value changing of nodes 50, 100, 150, and 200 also the simulation time between 50s, 100s, up to 1000 s, the packet delivery ratio can be found as in Figure 4.

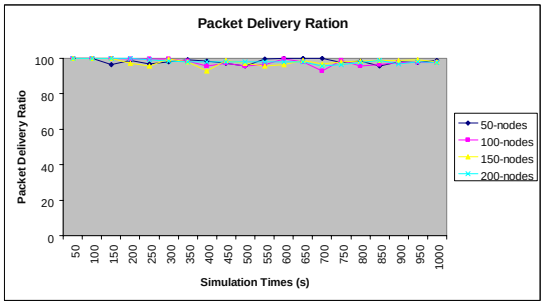

Figure 4. Packet Delivery Ratio

So these values show that our detection mechanism doesn't disrupt the normal packet delivery function.

4.5.3 Routing Overhead. The sum of all transmissions of routing packets sent during the simulation. For packets transmitted over multiple hops, each transmission over one hop, counts as one transmission.

$$\text{Routing Overhead} = \frac{\Sigma\text{Transmission of Routing Packets}}{\Sigma\text{Transmission of Data Packets}} \times 100\ \%$$

Routing overhead is important to compare the stability of the routing protocols, the adoption to low-bandwidth environments and its efficiency in relation to node battery power (in that sending more routing packets consume more power). Sending more routing packets also increases the probability of packet collision and can delay data packets in the queues.

To evaluate the routing overhead of the proposed system, we make the placement of 50 nodes, 100 nodes, 150 nodes and 200 nodes within the 1000m 1000m space and then run these with the simulation time of 50s to 1000s with the interval of 50ms. At that time we found that our system overhead is lesser when we make the more simulation time because we note that the overhead happens only when a new route is requested.

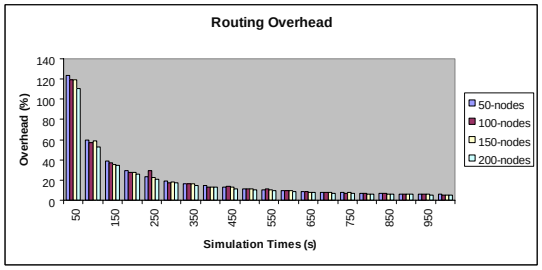

Figure 5. Routing Overhead

5. Conclusion

Wormhole attacks are significant problems that need to be addressed in wireless network security. This attack can be conducted without requiring any cryptographic breaks. An attacker who conducts a successful wormhole attack is in a position to disrupt routing, deny service to large segments of a network and use selective forwarding to temper with network application. The proposed detection mechanism is based on the round trip time (RTT) between two successive nodes and our consideration is that the attacks lead to the considerable longer RTT value than actual neighbor. We demonstrate our detection system under different node placement in a region and different simulation time using a NS-2 simulator. The simulation results show that our system has acceptable range of performance and applicability. However our system does not mean to a perfect solution to wormhole attacks because it can be only applied AODV based routing protocol.

References

[1] I.F. Akylidiz, W.Su, Y. Sankarubramaniam, E. Cayiric, "A Survey on Sensor Networks", *IEEE Computer Magazine*. August 2002. pp.102-114.

[2] L. Buttyán, L. Dóra, I. Vajda, "Statistical Wormhole Detection in Sensor Networks", *Second European Workshop on Security and Privacy in Ad Hoc and Sensor Networks (ESAS*

2005), Visegrád, Hungary, July 13-14, 2005,pp. 128-141

[3] S. Capkun, L. Buttyan, and J. Hubaux, "SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks", *In Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks, 2003*.

[4] C. Karlof and D. Wanger, "Secure Routing in Sensor Networks: Attacks and Counter-measures", *In Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications*, Anchorage, AK, May, 2003, pp.113-127.

[5] J. C. Hou and N. Li, "Topology Construction and Maintenance in Wireless Sensor Networks", *Book Chapter of Handbook of Sensor Networks: Algorithms and Architectures*, John Wiley & Sons, Inc. 2005

[6] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks", *In Proceedings of the IEEE Symposium on Network and Distributed System Security (NDSS)*, 2004.

[7] Y. Hu, A. Perring, and D.B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks", *In Proceedings of 22nd Annual Conference of the IEEE Computer and Commu-nication Societies*, Vol.3, April 2003. pp.1976-1986.

[8] I. Khalil, S. Bagchi, and N.B. Shroff, "LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks", *In proceeding of International Conference on Dependable Systems and Networks (DSN 2005)*, Yokohama, Japan.

[9] L. Lazos, R. Poovendran, C. Meadows, P. Syverson, L.W. Chang, "Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach", *In Proceedings of Wireless Communictions and Networking Conference, 2005.IEEE*. March 2005. pp.1193-1199.

[10] A. A. Pirzada, and C. McDonald, "Circumventing Sinkholes and Wormholes in Wireless Sensor Networks", *International Work-shop on Wireless Ad Hoc networks, 2005(5)*:pp. 132-150.

[11] L. Qian, N. Song, and X. Li, "Detecting and locating wormhole attacks in Wireless Ad Hoc Networks through statistical analysis of multi-path", *IEEE Wireless Communications and Networking Conference - WCNC 2005*.

[12] W. Sharif and C. Leckie, "New Variants of Wormhole Attacks for Sensor Networks", *In the roceeding of the Austrialian Telecom-munication Networks and Applications Conference*, Melbourne Austrila, December 2006, pp.288-292.

[13] N. Song, L. Qian, and X. Li, "Wormhole Attacks Detections in Wireless Ad Hoc Networks: A Statistical Analysis Approach", *In Proceeding of the 19th International Parallel and Distributed Processing Symposium (IPDPS'05)*

[14] C.-Y. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, and K. N. Levitt, "A specification-based intrusion detection system for AODV", *In ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'03)*

[15] W. Wang and B. Bhargava, "Visualization of Wormholes in Sensor Networks", *In Proceedings of the ACM workshop on Wireless security (Wise'04)*, 2004. pp. 51-60.

[16] W. Wang, B. Bhargava, Y. Lu and X. Wu, "Defending Against Wormhole Attacks in Mobile Ad Hoc Networks", *Wireless Communication and Mobile Computing*, Volume 6, Issue:4, June 2006, pp.483-503