International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:2, No:10, 2008

Wormhole Attack Detection in Wireless Sensor Networks

Zaw Tun and Aung Htein Maw

Abstract**—**The nature of wireless ad hoc and sensor networks make them very attractive to attackers. One of the most popular and serious attacks in wireless ad hoc networks is wormhole attack 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) and neighbor numbers based wormhole detection mechanism. The consideration of proposed mechanism is the RTT between two successive nodes and those nodes' neighbor number which is needed to compare those values of other successive nodes. The identification of wormhole attacks is based on the two faces. The first consideration is that the transmission time between two wormhole attack affected nodes is considerable higher than that between two normal neighbor nodes. The second detection mechanism is based on the fact that by introducing new links into the network, the adversary increases the number of neighbors of the nodes within its radius. This system does not require any specific hardware, has good performance and little overhead and also does not consume extra energy. The proposed system is designed in ad hoc on-demand distance vector (AODV) routing protocol and analysis and simulations of the proposed system are performed in network simulator (ns-2).

Keywords**—**AODV, Wormhole attacks, Wireless ad hoc and sensor networks

I. 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 because this attack does not inject abnormal volumes of traffic into the network. In this work, a specific type of emerging security threat knows as the wormhole attack is investigated.

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 the more attention in the detection and defending against wormhole attack is required.

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. This paper proposed a method of detection based on the transmission time and neighbor number of nodes to detect and locate wormhole attacks on the Ad hoc On-demand Distance Vector (AODV) routing protocol. This technique detects wormhole attack during the route setup procedure by the calculating of transmission time between each two successive nodes along the established route and the number of neighbor of the nodes. It is assumed that there are two clues for determination of worm attacks. The first assumption is that transmission time between two wormhole nodes is considerably higher than that between two legitimate successive nodes. The next assumption is that a wormhole that creates many new edges may increase the number of neighbors of the affected nodes. The presented system does not need any specific hardware to detect wormhole and the computational overhead is only little and no need of extra energy to detect the attack.

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 discusses the proposed detection mechanism. Finally, a conclusion is drawn in Section 5.

II. 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 replays 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

Zaw Tun. Author is presently doing his PhD on security issue in wireless and ad hoc networks at the University of Computer Studies, Yangon Myanmar; e-mail: zawtun78@ gmail.com).

Aung Htein Maw. Author is presently doing his PhD on energy efficient routing in wireless and ad hoc networks at the University of Computer Studies, Yangon Myanmar; e-mail: ahmaw73@ gmail.com).

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. This attack can be launched without having access to any cryptographic keys or compromising any legitimate node in the network. The wormhole attack is 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 attack 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.

III. Solution to Wormhole Attacks

In the wormhole attack, 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. This section briefly discusses their efforts.

A technique called 'packet leashes' [7] prevents packets from traveling farther than radio transmission range. The wormhole attack 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. When a node sends a packet to the destination, the sending packet includes the time which it sent the packet and the receiving node compares this value to the time which it received the packet. The drawback of this is that they need 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. Location information and loosely synchronized clocks are used together to verify the neighbor relation. 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 their system is 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 nodes' location 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, which knows the relative orientation of the neighbor with respect to itself. This extra bit 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 from verified neighbors. But it has the drawback that the need of the directional antenna is 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. With 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. Lazes 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 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, there may be a malicious node. In simple, a sensor cannot hear two guards that are more than 2R apart. Their system's weak 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 the majority of these techniques rely on specialized hardware. Network visualization technique presented in [15] for a dense sensor network 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 network's physical topology, to which a wormhole, in certain scenarios, introduces impossibilities. The detection of wormhole attacks that does not need any special hardware and additional information is proposed in this paper. The proposed detection mechanism is only based on the RTT of route request and reply message and the neighbor numbers of the suspected nodes. This detection mechanism is explained in detail in the next section.

IV. Proposed Detection Mechanism

In this section the proposed wormhole detection mechanism is discussed in detail. This mechanism does not need any special hardware or synchronized clocks because it only considers its local clock to calculate the RTT.

A. The System Model and Assumptions

Before the mechanism is described in detail, a system assumption of it is briefly discussed. In this work, the network is assumed to be 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). All nodes are uniquely identified.

To make the detection, it is based on the RTT of the message between successive nodes and their neighbor numbers. The consideration in here is that the adversary increases the number of neighbors of the nodes within the radius, shortens the path and increases the RTT value between successive nodes. This proposed mechanism consists of three phases. The first phase is to construct neighbor list for each node and the second phase is to find the route between sources to destination node. After that it finds the location of wormhole link to make any necessary action.

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 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.

B. Phase 1: Neighbor List Construction

In this first phase, each node broadcast the neighbor request (NREQ) message. The NREQ receiving node responds to the neighbor reply (NREP) message. The requesting node constructs the neighbor lists based on the received of NREP messages and counts its neighbor number (*nn*). After that the source node starts the route construction phase.

C. Phase 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 forwards the RREQ message and saves

T_{REQ} of its sending time. When the RREQ message reaches the destination node, it sends 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}. The assumption is based on the RTT of the route request and reply. The RTT can be calculated as

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

All intermediate nodes save this information and then send it also to the source node. The calculation of RTT is explained in detail in section 5.5.

D. Phase 3: Wormhole Attack Detection

In this phase, the source node calculates the RTT of all intermediate nodes and also it and destination. It calculates the RTT of successive nodes and compares the value to check whether the wormhole attack can be there or not. If there is no attack, the values of them are nearly the same. If the RTT value is higher than other successive nodes, it can be suspected as wormhole attack between this link.

The next detection mechanism is based on the fact that by introducing new links into the network graph, the adversary increases the number of neighbors of the nodes within its radius. So it needs to check the *nn* of these two nodes which find in section 4.2. Equation (2) is adopted form [5] to estimate average number of neighbors d. It is approximated as

$$d = (N-1)\,\pi\, r^2 / A \quad (2)$$

where A is the area of the region, N is the number of nodes in that region and r is the common transmission radius. For example, if the RTT value between A to B is considerably greater than for other links, it needs to check the value of nn for A and B. If also the nn value for A and B is higher than the average neighbor number d, there is a suspect that a wormhole link is between nodes A and B. In this way the mechanism can pinpoint the location of the wormhole attack.

E. Calculation of RTT

In this subsection, the detailed calculation of the RTT is discussed. The value of RTT is considered the time difference between a node receives RREP from a destination to it send RREQ to the destination. During route setup procedure, the time of sending RREQ and receiving RREP is described in Figure 1. In this case, 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:

$$RTT_{A,B} = RTT_A - RTT_B \quad (3)$$

Where RTT_A is the RTT between node A and the destination, 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 $T(S)_{REQ}$, $T(A)_{REQ}$, $T(B)_{REQ}$, $T(D)_{REQ}$ is the time the node S, A, B, D forward RREQ and $T(S)_{REP}$, $T(A)_{REP}$, $T(B)_{REP}$, $T(D)_{REP}$ is the time the node S, A, B, D forward REP.

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

$$RTT_S = T(S)_{REP} - T(S)_{REQ}$$
$$RTT_A = T(A)_{REP} - T(A)_{REQ}$$
$$RTT_B = T(B)_{REP} - T(B)_{REQ} \quad \textbf{(1)}$$
$$RTT_D = T(D)_{REP} - T(D)_{REQ}$$

And the RTT values between two successive nodes along the path will be calculated based on equation (3):

$$RTT_{S,A} = RTT_S - RTT_A$$
$$RTT_{A,B} = RTT_A - RTT_B$$
$$RTT_{B,D} = RTT_B - RTT_D$$

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 and suspected that there may be a wormhole link between these two nodes.

Figure1 shows the route setup procedure in AODV, the time of sending RREQ and receiving RREP in each node along the route.

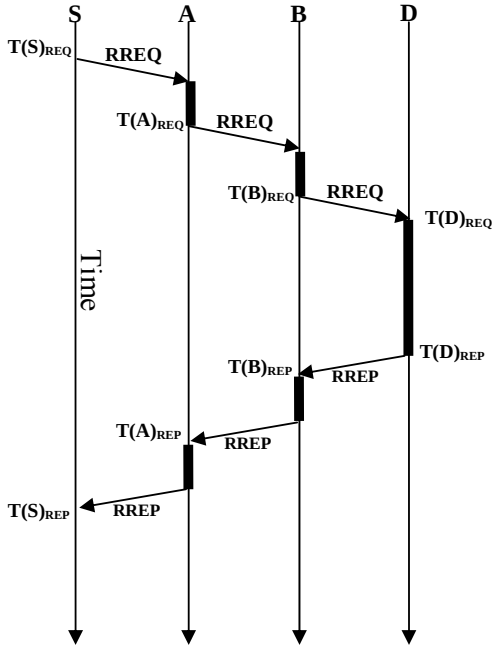

Fig. 1. Time for RREQ forward and RREP accept

F. Evaluation

In this section, the performance of the proposed mechanism is evaluated using network simulator (ns2). In this experiment, the network includes 50 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. The CBR connection with 4 packets per second are created and the size of the packet is 512 bytes. In the simulation, two wormhole nodes are created

randomly into the network and establish a tunnel between them using encapsulation.

Here it is needed to decide the two values, nn and RTT, as threshold values. In the first value, when the nn is larger two times than the average neighbor number, it may lead to increase in false negative and when nn lower than 1.5 times of the average neighbor number, it is raised to false positive value. So the threshold value of nn is defined 1.6, and the test result shows an acceptable range of false positive and negative as shown in Figure 2. The next threshold value to consider is RTT and it is proportional to false negative rate. To get the acceptable rate of false positive and negative, the simulation is made 1000 times and get the value of 50 ms as in Figure 3, which is minimizes both false positive and false negative rate. The rate of detection also depends on the length of the wormhole, because the more the wormhole length, the longer the transmission time between two fake neighbors and the easier to detect. In this case, the detection rate is 100 % when the length of wormhole is greater or equal 5 as in Figure 4.

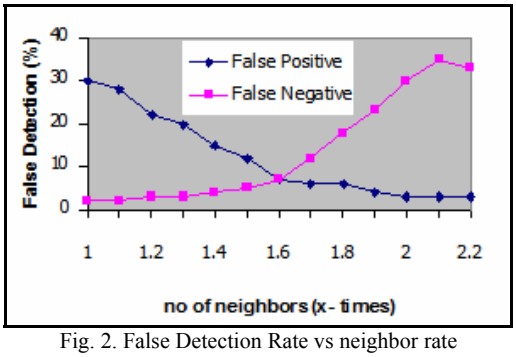

Fig. 2. False Detection Rate vs neighbor rate

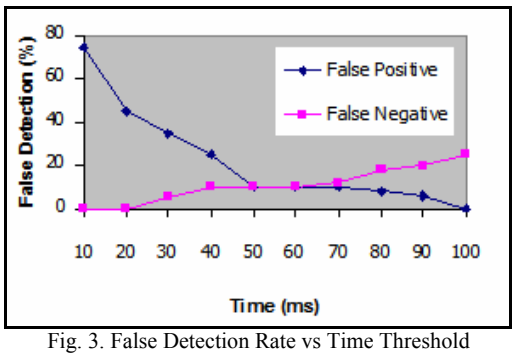

Fig. 3. False Detection Rate vs Time Threshold

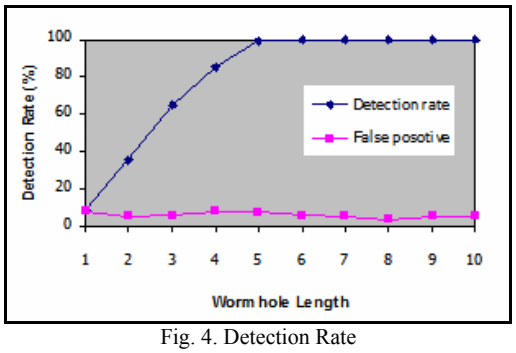

Fig. 4. Detection Rate

Memory overhead: Each node needs to store a neighbor list. It is assumed that the identity of a node is 2 bytes and the size of the neighbor list is $d = (N-1)\ \pi\ r^2\ /A$ entries, so the neighbor list requires 20 more bytes for the storage of them. To calculate RTT, each node needs n*(4+4) bytes memory, where n is the maximum number of RREQ come to the node at the same time and this value depends on the topology and traffic of network. In this case, n is set 4 and so each node needs 32 bytes of memory to run the mechanism.

Bandwidth overhead: The bandwidth overhead incurred after deployment of a node for neighbor discovery and in the case of wormhole detection. In each route request in AODV, every node forward RREQ once and RREP is forwarded by nodes along the established route, the size of RREQ is 32 bytes and its RREP is 20. But, the simulation needs the value of RTT to add in the established route path, the size of RTT is 4 byte values. The overhead is calculated as (size of RREQ * number of node) + (size of RREP * length of established route). In the simulation, 50 nodes and 1000m × 1000m space is used so the average established route path is 4.57438. So before using the mechanism the overhead is 1691.4876 and after using the mechanism is 1775.1874095. This is therefore a negligible fraction of the total bandwidth over the lifetime of the network because this overhead happens only when a new route is requested.

Energy consumption: In terms of energy consumption, the detection mechanism uses no more energy than before using it, so the life time of the network is the same as before and after the use of this mechanism. The simulation time is 1000 s and so it is enough to 100 J per node to efficient network life time.

V. Conclusion

In this paper, a survey on the wormhole attacks detection methods is made and found that to detect and prevent this attack mainly depends on the precise determination of the neighboring information. Most of the detection methods are considered the neighbor case of the node. The countermeasures for the wormhole attack can be implemented at different layers. For example, directional antennas are used at the media access layer to defend against wormhole attacks, and packet leashes are used at a network layer.

Since current wormhole detection methods are imperfect, a sensor node will have a lot of false neighbors under large-scale wormhole attacks. Having many false neighbors often causes trouble for many protocols. Some more efforts are needed to make the accurate neighbor discovery protocols in the detection and isolation of wormhole attacks. So the new mechanism to defend the wormhole attack based on the RTT of the route message and number of neighbor nodes is proposed. The first consideration is the RTT between two successive nodes and in normal case all of the RTT between two successive nodes are nearly the same and the next fact is wormhole nodes may increase its number of neighbors. The significant feature of the propose mechanism is that it does not need any specific hardware to detect the wormhole attacks. This mechanism does not require more energy than normal and can extend to other routing protocols than current AODV protocols.

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 proceeding of the Australian Telecommunication 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.