ISSN (Online): 2230 - 8849
International Journal of Enterprise Computing and Business Systems (Online)
IJECBS India
IJECBS
Frequency: Bi-Annual
Specialized, Refereed and Indexed Journal in International Scientific and Corporate Databases
http://www.ijecbs.com
Vol. 2 Issue 2 July 2012

WORMHOLE DETECTION METHODS IN MANET

Ankita Gupta
Jayoti Vidyapeeth Women's University
Jaipur(Rajasthan). INDIA

Sanjay Prakash Ranga
HOD Computer Science Deptt,
Govt. Engineering College of Bikaner,
Bikaner(Rajasthan). INDIA

Abstract
Wormhole Attack is one of the most severe attacks on routing protocols in which two or more malicious nodes receive packets at one point of the network and transmit them to another location by a wired or wireless tunnel. This attack so powerful that the detection of it is difficult. This attack can form a serious threat in wireless networks, especially against many wireless ad-hoc networks and location-based wireless security systems. There are several wormhole detection methods in the wireless ad-hoc networks which some of them are reviewed in this paper. Finally, a qualitative comparison among all methods is provided.
Keywords— Ad-hoc Network, MANET attacks, Wormhole Attack, wireless security systems.

I. INTRODUCTION
In the recent years with technological advances in all science especially in Micro-Electro-Mechanical Systems (MEMS), sensor networks have gained worldwide attention among scientists. These kinds of sensors compared to traditional sensors, are smaller and have limited resources. Also, they are cheaper than prior sensors. The sensor nodes which deployed in the network have great abilities such as sense, measure, and gather information from the environment. After that, they can transmit all sensed nformation to the sink [1]. As it is illustrated in the Fig. 1, wireless ad-hoc networks can be classified into three sub networks.

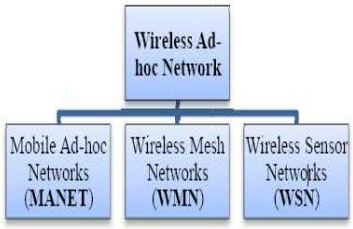

Fig. 1 : Classification of Wireless Ad-hoc networks

Mobile ad hoc networks (MANET) are the first categorization which are consist of some auto-configuring nodes that can move freely and utilize wireless equipment to communicate with each other. These kinds of network do not need a concentrate entity and are infrastructure-less [2]. The second part of this classification is wireless mesh network (WMN) in which each node that communicates with the other nodes via radio wave transmit its own data and also collaborates with the other nodes in order to relay their data. Finally, a wireless sensor network (WSN) mostly consists of a gateway or base station, which can communicate with other wireless sensors by a radio link. The collected data via the wireless sensor node, compressed, and transmitted to the gateway (sink) directly [3].
One of the major concerns in wireless ad-hoc networks is Security, due to the sensor nodes have been deployed in the rough environment. If there are no security features in sensor networks, the attackers can effect on various parts of them like preventing the event detection, spreading false alarms, draining the energy of the network, risk of failing the privacy, and confidentiality of information, and altering the traffic. On the other hand, according to the sensor nodes are faced to

ISSN (Online): 2230 - 8849
International Journal of Enterprise Computing and Business Systems (Online)
IJECBS India
Frequency: Bi-Annual
Specialized, Refereed and Indexed Journal in International Scientific and Corporate Databases
http://www.ijecbs.com
Vol. 2 Issue 2 July 2012

some restrictions such as limited memory, short lifetime and low power radios, almost complicated security algorithms are not suitable and pplicable for a long time in these networks. So, create a solution to provide a security for sensor networks is inevitable.[4]

The various holes that threaten the security of sensor networks are consist of sink/black hole, worm hole, Sybil attack and etc. They can form in sensor networks and create variations into the network topology which trouble the upper layer applications [3].In the selective forwarding attack, a malicious node firstly tries to be trusted by sender for next forwarding packet, and finally, intercepts a transmission by selecting an arbitrary packet or dropping it completely. Sinkhole attacks happen when the attacker can attract the large part of traffic to a region but if the attackers are able to forge the identities of the other nodes, the Sybil attack is occurred [4].

Among all attacks, the wormhole is more dangerous than the others; because this type of attack does not need to compromise a sensor in the network and it can create the other type of attack easily. On the other hand, using a cryptographic technic cannot prevent wormhole attack [5].

The remaining parts of this paper are arranged as follows. Section 2 gives a basic definition of Wormhole attack. Section 3 consists of reviewing on several wormhole detection methods. Section 4 depicts a qualitative comparison of wormhole detection methods that are discussed in the previous section. Finally, a conclusion is presented in Section 5.

II. WORMHOLE ATTACK

A wormhole is a type of attack that usually occurs by two malicious nodes via an out-of-band connection in which the first adversary receives or eavesdrop packets at one area and then tunnel them to the next adversary that is located in another point of the networks through a long-range directional wireless link or even by using direct wired link [6]. So, it can simply convince these two Separated nodes that they are neighbors by sending packets between the two of them. On the other hand, an adversary by using this attack could convince nodes that they are normally situated multiple hops from a base station that they are only one or two hops away. If an attacker is located near of sink or base station, it can interrupt
routing by making a well-placed wormhole completely [7].

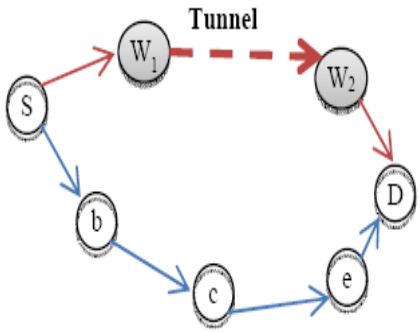

Fig. 2: The sample of Wormhole Attacks

For example, as it is shown in the figure 2, the source node (S) sends packets to destination through the normal path (S-b-c-e- D), but these packets also are eavesdropped by the first malicious node (W_1) and then tunneled to second malicious node (W_2). Finally, W_2 transmits them to the destination node (D) before they are arrived to D from the normal path. So, the rest of packets that follow the normal path will be dropped by destination.

The wormhole attacks are able to be created in wireless adhoc networks by using at least one of the following methods:

The first type of wormhole occurs when the malicious nodes are static. In this situation, at least one malicious node is located within the route from the source to the destination. This type of wormhole attack is named static wormhole.

Another type of this attack is mobile wormhole. In mobility pattern, malicious nodes are not deployed in the path to destination. So, one of this nodes will be located within the path by movement and overhearing the data packets and processing them for routing information [8]. The identification of dynamic wormhole is so difficult and it is not easy to design a method to prevent both of them at the same time. This type of attack maybe appeared in the other type in which an expert attacker can create their own virtual network until the new route

ISSN (Online): 2230 - 8849
International Journal of Enterprise Computing and Business Systems (Online)
IJECBS India
IJECBS
Frequency: Bi-Annual
Specialized, Refereed and Indexed Journal in International Scientific and Corporate Databases
http://www.ijecbs.com
Vol. 2 Issue 2 July 2012

created by the attacker contains the same number of hops as of original route.

III. OVERVIEW ON WORMHOLE DETECTION METHODS

One of the main classifications of wireless networks that are usually vulnerable against wormhole attack is wireless ad hoc network in which the malicious nodes prevent to discover any routes to destination except through the wormhole (Hu, Perrig, & Johnson, 2003). Therefore, in recent years, a wormhole attack attracts more consideration and some studies are performed on this issue.

Detection of wormholes is difficult because the packets are transmitted by the malicious nodes to a far location from the received point by utilizing just a single hop out-of-band channel. This channel cannot be listened to by the network. Also, when this attack combine with the other attacks like selective forwarding, it becomes more dangerous for security of the network. It is important to mention that wormhole can cause to create Sybil and sinkhole attack [6]. In the following some defense methods against wormhole attack are reviewed.

A. Geographical Leashes

A geographical leash [9] is a method that is implemented in 2003 by Hu to protect ad hoc network from wormhole attack. It is based on this feature that the receiver of the packet is located within a certain distance from the sender. In order to implement geographical leash in the ad hoc networks, firstly some requirements should be provided such as each node must know its own location (using GPS), all nodes must have loosely synchronized clocks and digital signature (RSA) in order to checking the authentication of the location and time of sender. When a packet is sent by a node, it inserts its own location (p_s) and the time that the packet is sent (t_s) in the header of packet. When the packet arrives to the next node, the location of the receptor (p_r) and the time of receive packet (t_r) is compared with the values of sender. As regards to the sender and receiver are used synchronized clocks, if the clocks of them are synchronized to within $\pm\Delta$, so, an upper bound distance between the sender and receiver (d_{sr}) is computable by receptor.

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

In which is light speed, t_s is the timestamp in the packet and _ is the maximum error that maybe occurred in finding location information.

B. Temporal Leashes

The next method that is designed to protect sensor networks against wormhole attack is called temporal leash [9] in which an expiration time is considered to each transmitted packet. According to this time restriction in temporal leash, a sender of packet should prevent broadcasting packet more than distance L ($L_{min} = \Delta_t.c$, where c is the propagation speed of light). Before a packet is sent at t_s by sender the packet expiration time is calculate ($t_e = t_s + L/c - \Delta_t$) and it is added to packet. So, when the packet received by the next node at its local time (t_r), this time is compared with the time of expire packet (t_e). Then, the packet is drop if $t_r > t_e$.One of the important requirements of this method is checking the authentication of nodes. According to the existence issue in HMAC and RSA authentication and the side effects of them like the number of keys, the TIK protocol is considered for temporal packet. TIK is constructed based on TESLA, using a symmetric cryptographic [9].

One of the important weak-point of this method is that it is important to mention TIK has some impractical assumptions. It relays on synchronized time between all nodes and there are no delay when the packet sending and receiving. These assumptions are weak points of packet leash method to detect wormhole [10].

C. Graph Theoretic Approach

L. Lazos [11] designed a model to characterize wormhole attack in ad hoc networks that called “a graph theoretic approach”. According to this method, to secure an ad hoc network from wormhole attacks a Local Broadcast Key (LBK) was considered and provided a distributed mechanism for establishing them in randomly deployed networks. To succeed these approach its need to use a GPS and special localization

ISSN (Online): 2230 - 8849
International Journal of Enterprise Computing and Business Systems (Online)
IJECBS India
IJECBS
Frequency: Bi-Annual
Specialized, Refereed and Indexed Journal in International Scientific and Corporate Databases
http://www.ijecbs.com
Vol. 2 Issue 2 July 2012

equipment. This method is not readily applicable to mobile networks.

D. Localized Encryption and Authentication Protocol (LEAP)

"Localized Encryption and Authentication Protocol (LEAP)" is a method which is suggested by Zhu [12]. This model is based on clustering and it requires defining 4 type key for each sensor node such as: an individual key shared with the base station, a pair wise key shared with another sensor node, a cluster key shared with multiple neighboring nodes, and a group key that is shared by all the nodes in the network. This method is implemented for static or immobile sensor networks.

E. Multipath Hop-count Analysis

According to the nature of wireless transmission, the security issues in MANET are more than wired environments. Among all possible attack on wireless sensor networks, one of the specific types is wormhole attack in which the attacker does not need to exploit any nodes in the network and it can be done by the route establishment process. MHA is a method based on hop-count analysis in order to avoid this attack in MANETs from the standpoint of users without any special environment assumptions. Recently a new model [10] is prepared by Jen which is called "Multipath Hop-count Analysis" to prevent wormhole attack for MANETs. The MHA method is contained the following steps: Firstly, the hop-count values of all routes are calculated. In the next step, a safe set of routes are chosen for data transmission.
Ultimately, the packet is transmitted to destination through the safe routes due to decreasing the rate of packet that is sent by wormhole. One of the features of this method is that it does not require any specific hardware to well-done. It utilizes control packets as in RFC3561 and tries to modify it. Therefore, it used the RREQ packet is used for route discovery and the RREP packet is used for route reply. Generally, the main idea of this method is that when the wormhole attacks happen, the number of hops will be smaller than normal situation. As a result of this rule, the wormhole attack is detected and by using multipath method, the packet is transferred from another path.

F. An End-to-end Detection of Wormhole Attack in Wireless Ad-hoc Networks

EDWA [13] is a method that is suggested to detect wormhole attack in DSR routing protocol based on hop-count scenario. There are some assumptions which should be considered in order to use this method such as all nodes have to find their geographical information by using Global Positioning System (GPS) and also, all network nodes record each other's authentic public keys (using TESLA for authentication). EDWA is consisted of following step which is explained sequentially.

1). Detecting a wormhole by using estimate shortest path
When the destination receives a Route Request packet, it prepares a Route Reply packet to broadcast it to sender. Once a packet reaches to source node, firstly, it authenticates this packet then it extracts the location of destination from the Route Reply packet. Finally, the source estimates the shortest path through goal in terms of hop count by using Euclidean distance estimation model. If the location of source node is l_s and the position of destination is l_d, the distance from source to destination and _ is the maximum relative error in location measurement is estimated based on Euclidean method as

$$d = \left\| l_d - l_s \right\| + \delta$$

Imagine that a node A is the neighbour of S which the shortest Euclidean distance to D crosses from it. So, this node (A) is selected for the next hop through the shortest path to the destination. If (x_a, y_a) is the coordinates of A, the distance between A and D is computed as

$$e_a = \sqrt{(x_a - d)^2 + y_i^2}$$

Finally, the distance is calculated as:

$$E(e_a) = d - r\int_{d+r}^{d-r} \left(1 - P_{E_a}(e_a)\right)^{N\pi r^2} de_a$$

Once the $E(e_a)$ is estimated, it is possible to compute the next hop after A easily. Finally the

ISSN (Online): 2230 - 8849
International Journal of Enterprise Computing and Business Systems (Online)
IJECBS India
IJECBS
Frequency: Bi-Annual
Specialized, Refereed and Indexed Journal in International Scientific and Corporate Databases
http://www.ijecbs.com
Vol. 2 Issue 2 July 2012

minimum number of hops through source to destination is determined.

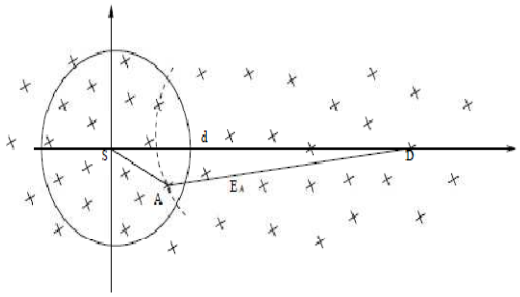

Fig. 3: Estimate the First Hop Distance

After that the source node compares the hop-count which is retrieved from Route Reply (h_r) with the number of hop within the shortest path to destination (h_e). The wormhole attack is occurred during this path if and only if $h_r < h_e$ [13].

2). Identifying the malicious nodes
In order to discoverer a malicious node and the tunnel between them in this method, a Tracking packet is sent through destination. When each one of intermediate nodes receives the packet, they transmit the Track-Response to the first node. Finally, the source will compute shortest path to each intermediate node to identify the two malicious nodes.
The last step is involved selecting a shortest path to destination from the trusted routes that will be performed when the malicious nodes are identified and eliminated from the path [13].

G. Detecting Wormhole Attack in OLSR

This method [14] contain three approaches such as detecting Suspicious Links, wormhole Verification and timeouts that they are explained in the following respectively.

1). Detecting Suspicious Links
The detection approach in this method is based on that the packet latency. One of the important side effects of wormhole attack on the network is increasing delay compared to normal wireless propagation latency on a single hop. In order to find suspicious links in OLSR protocol, it is needed to apply two new control packets $HELLO_{req}$ and $HELLO_{rep}$. A source node transmits one $HELLO_{req}$ message and set a time for expiry of this packet. When a node receives a$HELLO_{req}$, firstly save the address of sender then due to avoid overloading the network with too many HELLO answers, it holds the packet for Ni until it is scheduled for transmitting its next HELLO message. It is important to mention that the default transmission interval time for HELLO message is 2 seconds in OLSR and piggybacks the replies to this HELLO message ($HELLO_{rep}$).When a requester node receives a $HELLO_{rep}$, it checks an in arrival time of this packet in order to determine that whether it has arrived within its scheduled timeout interval or not. If the packet did not arrive within its scheduled timeout, the source node supposes this link as an untrusted link and not allows communicating with that node until the wormhole verification procedure archive to the end point.

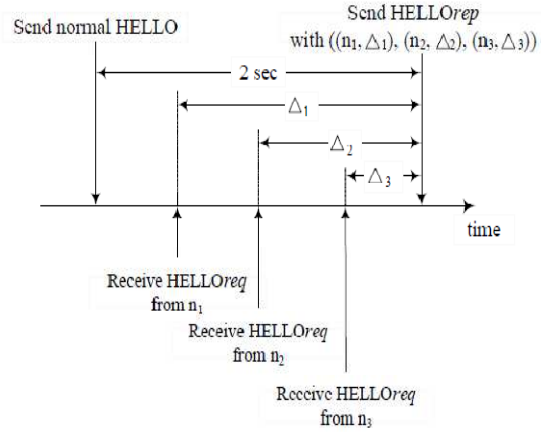

Fig. 4: $HELLO_{rep}$ aggregation

2). Wormhole Verification
The mechanism that is used to detect wormhole attack is similar to $HELLO_{req}$ and $HELLO_{rep}$ procedure in which the source node broadcasts another packet that is called Probe to all of its suspect nodes and it is waiting to receive ACK_{probe} from them. When the ACK_{probe} packet is arrived to the originator of Probe, the source node compares its evaluation from the reputation of the other end-point in the suspicious link with the evaluation of other nodes from its own reputation status. It is

ISSN (Online): 2230 - 8849
International Journal of Enterprise Computing and Business Systems (Online)
IJECBS India
Frequency: Bi-Annual
Specialized, Refereed and Indexed Journal in International Scientific and Corporate Databases
http://www.ijecbs.com
Vol. 2 Issue 2 July 2012

important to mention that the Suspicious link is not a trusted link if and only if the reputation of the remote node or the contents of the ACK_{probe} or both of them [14].

3). Timeouts
The value of timeout play a vital role in this scenario [14] in order to take a correct decision because if it is considered as a too small value, the trust node could be suspected wrongly but if it was so big, detection of a malicious nodes is hard. Timeout can be then calculated as follows:

$$\text{Timeouts} = \frac{2R}{V} + T_{Proc}$$

In which, the maximum transmission radio range of each node is shown with R and V is the light speed. T_{proc} is the approximation of the packet processing time and the queuing delays within nodes.

H. Defense Mechanism against Wormhole Attacks in Wireless Sensor Networks

DAWWSEN [15] is method that is designed to prevent wormhole attack in WSNs with constructing a hierarchical tree by base station - via transmitting a request packet due to find its children nodes - in which the base station is the root of tree, and the rest of sensor nodes are located in the intermediate or the leaf nodes of the tree. This method consists of three major components such as request packet, replay packet and hopcount. When the request packet is originated by the source node, the hop-count and IDs is determined by the source node then this packet is transmitted. Each intermediate node that receives this packet should not replay it immediately. So, this packet is entered in the waiting list based on its hop-count. Once a replay timer is expired, the replay packet is prepared and sent through source node. This packet includes these fields like: The id address of the generator the replay packet (ID_s), The id address of the source node that is equal to IDs request packet (ID_d), The number of hop-count, The number of replayed packets (Num_Rep), The acceptance flag (Recv_Accept). Upon the replay packet is received by any nodes, each node firstly runs a timer that is called accept timer and before this timer expire, it checks its replay wait-list that is contain the id address of sender, hop-count and number of reply (Num_reply). If an entry is discovered that its ID is similar to the ID of received packet, its num_reply field will be enhanced by one else a new entry will be created and insert to the list (Num_reply=1). When the timer expires, this node prepares a packet (accept packet) that is contained its id (IDs), destination id that is equal to IDs of replay wait-list, and the Num_reply field and then it sends this packet to each entry in its reply list. Once a node receives an accept packet, it checks its replay list to find an entry that its id is similar to the received packet id. If this node finds a related entry, its feature in the list should update (Num_reply = Num_Rep + 1) otherwise the wormhole attack is detected and the following steps should be performed:

1. The received accept packet should be deleted.
2. Add the ID of the sender of the accept packet should be inserted into its (Not Accepted Packets (NAP) list.
3. Update its replay wait-list by resetting all values to zero.
4. In last step, the node should wait for another request packet or it can send another reply that is similar to the second item in its request list.

As a consequence, based on this method a hierarchical 3- way handshake routing tree can be made easily in order to detect wormhole attack for a multi-hop wireless sensor networks [15].

I. Wormhole Geographic Distributed Detection

Another model to detect the wormhole attack dependent on the existence of disorder in the network due to this attack is called “Wormhole Geographic Distributed Detection” [16] which is designed in 2008 by Xu. In this model to detect wormhole attack is used hop-count technic Then, the local map is re-built finally; a method is utilized to identify the irregularity in the network which is named “diameter”. The main advantage of using a distributed wormhole detection algorithm is that the proposed algorithm can approximately detect the location of a wormhole.

ISSN (Online): 2230 - 8849
International Journal of Enterprise Computing and Business Systems (Online)
IJECBS India
IJECBS
Frequency: Bi-Annual
Specialized, Refereed and Indexed Journal in International Scientific and Corporate Databases
http://www.ijecbs.com
Vol. 2 Issue 2 July 2012

IV. SUMMARY OF WORMHOLE DETECTION METHODS

In the following Table I, there are all wormhole detection methods that are explained previously. Also, the requirements of each method are listed.

Table 1: Qualitative Comparison of Wormhole Detection Methods

Method	Localization Information	Checking the Authentication	Hop Count Analysis	Others
Geographical Leashes	Yes	RSA	N/A	Loosely Synchronized clocks
Temporal Leashes	Yes	TIK Protocol based on TESLA	N/A	Loosely Synchronized clocks
Graph Theoretic Approach	N/A	Local Broadcast Key (LBK)	N/A	N/A
LEAP	N/A	Four Type Keys	N/A	N/A
MHA	N/A	N/A	Yes	N/A
EDWA	Yes	TESLA	N/A	N/A
DWOLSR	N/A	N/A	N/A	Four Way Handshaking Messages
DAWWSEN	N/A	RC5	Yes	N/A
WGDD	Yes	N/A	Yes	Local Map

V. CONCLUSION

In this paper, we review the various detection mechanisms against wormhole attacks in wireless Ad-hoc networks. Along with the explanation of these methods, the weak points of these are also discussed and a qualitative comparison of these methods is summarized in Table 1.

REFERENCES

[1]. Yick, J., Mukherjee, B., & Ghosal, D. (2008). Wireless sensor network survey. (E. Ekici, Ed.) Computer Networks 52, 2292-2330.

[2]. Nguyen, D. Q., & Lamont, L. (2008). A Simple and EfficientDetection of Wormhole Attacks. IEEE Confrances NewTechnologies, Mobility and Security (pp. 1-5). NTMS '08.

[3]. Chris, T., & Steven, A. (10 2, 2004). Wireless Sensor Networks: Principles and Applications. Retrieved 18 2, 2011, from MicroStrain: microstrain.com/white/Wilson-chapter-22.pdf

[4]. Fonseca, R., & Merino, A. S. (2004). Receiver Based Forwarding: Improving the security of Geographic Routing in Wireless Sensor Networks. Berkeley: Berkeley University.

[5]. Loo, C., Ng, M., Leckie, C., & Palaniswami, M. (2006).Intrusion Detection for Routing Attacks in Sensor Networks. International Journal of Distributed Sensor Networks, 313–332.

[6]. Çayırcı, E., & Rong, C. (2009). Security in Wireless Ad Hoc and Sensor Networks. London: Wiley.

[7]. Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: attacks and countermeasures. Ad Hoc Networks , 293–315.

[8]. Poornima, E., & Bindhu, C. (2011). Prevention of WormholeAttacks in Geographic Routing Protocol.

ISSN (Online): 2230 - 8849
International Journal of Enterprise Computing and Business Systems (Online)
IJECBS India
IJECBS
Frequency: Bi-Annual
Specialized, Refereed and Indexed Journal in International Scientific and Corporate Databases
http://www.ijecbs.com
Vol. 2 Issue 2 July 2012

International Journal of Computer Network and Security (IJCNS), 42-50.
[9]. Hu, Y.-C., Perrig, A., & Johnson , D. (2006). Wormhole attacks in wireless networks. IEEE Journal on Selected Areas in Communications , 370-380.
[10]. Jen, S.-M., Laih, C.-S., & Kuo, W.-C. (2009). A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET. sensors, 5022-5039.
[11]. Lazos, L., Poovendran, R., Meadows, C., Syverson, P., & Chang, L. (2005). Preventing wormhole attacks on wireless ad hoc networks: a graph theoretic approach. Wireless Communications and Networking (pp. 1193 - 1199).
Washington: IEEE Conference.
[12]. Zhu, S., Setia, S., & Jajodia, S. (2003). LEAP: efficient security mechanisms for large-scale distributed sensor networks. Proceedings of the 10th ACM conference on Computer and communications security (pp. 62 - 72). New York: ACM.
[13]. Wang, X., & Wong, J. (2007). An End-to-end Detection of Wormhole Attack in Wireless Ad-hoc Networks. 31st Annual International Computer Software and Applications Conference, (p. 8). Washington, DC, USA: IEEE Computer Society.
[14]. Abdesselam, F., Bensaou, B., & Taleb, T. (2008). Detecting and Avoiding Wormhole Attacks in Wireless Ad Hoc Networks. Communications Magazine, IEEE , 127 - 133 .
[15]. Kaissi, R. E., Kayssi, A., Chehab, A., & Dawy, Z. (2005). DAWWSEN: A DEFENSE MECHANISM AGAINST WORMHOLE ATTACKS IN WIRELESS SENSOR NETWORKS. The Second International Conference on Innovations in Information Technology (p. 10). Dubai: IIT.
[16]. Xu, Y., Chen, G., Ford, J., & Makedon, F. (2007). Distributed Wormhole Attack Detection inWireless SensorNetwork.