Network and Complex Systems
ISSN 2224-610X (Paper) ISSN 2225-0603 (Online)
Vol.5, No.9, 2015

Detection of Hidden Wormhole Attack in Wireless Sensor Networks using Neighborhood and Connectivity Information

Mr. Manish M Patel
Research Scholar, Computer Engineering,Gujarat Technological University,Ahmedabad, Gujarat, INDIA

Dr. Akshai Aggarwal
Vice Chancellor, Gujarat Technological University, Ahmedabad, Gujarat, INDIA

Abstract
Wireless sensor networks (WSNs) have inspired many applications such as military applications, environmental monitoring and other fields. WSN has emergence in various fields, so security is very important issue for sensor networks. Security comes from attacks. Due to the wireless and distributed nature anyone can connect with the network. Among all possible attacks, wormholes are very hard to detect because they can cause damage to the network without knowing the *protocols* used in the network. It is a powerful attack that can be conducted without requiring any cryptographic breaks. Wormholes are hard to detect because they use a private, out-of-band channel invisible to the underlying sensor network. In this paper we have proposed a wormhole detection protocol based on neighborhood and connectivity information. Performance analysis shows that our proposed approach can effectively detect wormhole attack with less storage cost.
Keywords: Wireless sensor network, wormhole, out-of-band, security, neighborhood.

1. Introduction

Wireless sensor network consists of hundreds or thousands of tiny sensor nodes. The sensor nodes can sense, process and communicate with their neighbor nodes [1]. The low power sensor nodes can collectively monitor a particular area [2]. One sensor node sends data to the next node and finally data reaches to the base station. A base station can be a powerful data processing center. Sensor nodes can be used for continuous sensing, event detection and event identification. The application of wireless sensor networks includes military, environment, health, home, commercial, space exploration, chemical processing and disaster relief etc [3, 4].

Security is very crucial factor for sensor network that deserves great attention. Wireless sensor networks are vulnerable to malicious attacks due to their fundamental characteristic such as open medium, dynamic topology and resource constraints [5, 6]. WSNs could be attacked at all levels. The survey by Karlof and Wagner [7] classifies a number of attacks that prove devastating to many fundamental WSN routing protocols. Major attacks on sensor networks include blackhole, selective forwarding, Sybil, wormhole, jamming etc. Among all the attacks wormhole attack is very dangerous.

In a wormhole attack, two malicious nodes are connected by a high-speed tunnel and they both are far away from each other [8-11]. One malicious node records the packets in one area, forward to another malicious node and the second malicious node replay the packets in the different location. This generates a false scenario that the original sender is in the neighborhood of the remote location. The tunneling procedure forms a wormhole. This might be harmful if the data within the packet is altered to contain different information than the original. Due to the fast transmission path between the two ends of the wormhole, the tunneled packets can propagate faster than those through a normal multi-hop route. Wormholes fake a route that is shorter than the original one within the network; this can confuse routing mechanisms which rely on the knowledge about distance between nodes.

In this paper, we present a wormhole detection mechanism based on neighborhood and connectivity information in wireless sensor networks. It uses a secure pre-distribution pair-wise key management protocol. Our proposed protocol consists of three phases: In the first phase, every node builds its one hop neighborhood table. In the second phase, the neighbor table is exchanged to forms two hop neighborhood list. Third phase includes the wormhole detection procedure. The proposed protocol is applicable to resource constraints wireless sensor networks. It does not require any hardware such as time synchronized clock or directional antenna.

The rest of the paper is organized as follows. Section 2 presents significance of wormhole and wormhole attack taxonomy, whereas in Section 3, we discuss various existing methods to detect wormhole attack. Section 4 provides detail description of our proposed approach. Cost analysis and simulation results are discussed in Section 5. Finally, concluding remarks are made in Section 6.

2. Wormhole Attack Description

2.1 Significance of Wormhole Attack

A shortcut delivered by a malicious node will harm the normal network operations. The data packets received by one malicious node are transferred to another malicious node which is located far away. This transmission is

done through an out-of-band high speed channel. Such a simple operation can severely affect the localization and routing procedures.

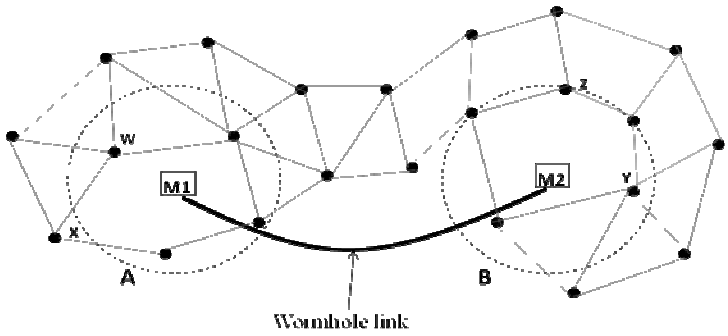

Fig. 2.1 Wormhole Attack

As shown in fig. 2.1, two malicious nodes M1 and M2 makes a tunnel. Node M1 attracts traffic from one area and passes it to node M2 in other area. The malicious nodes and the link between them are hidden from the genuine nodes. They do not hold any valid network Ids. To launch the attack, there is no need to compromise the network node. Using tunneling an attacker can creates a false scenario. In the presence of wormhole, target tracking applications can be easily confused. The localization algorithms based on connectivity are also affected by wormhole attack. Detection of wormhole attack is hard because the malicious entities make it "invisible" to the upper layers [12, 13]. Wormhole attack can be launched at the bit level or at the physical layer [14]. After establishing wormhole, the attackers can perform various types of attacks, such as the black hole attacks or selective forwarding attacks.

2.2 Wormhole Attack Taxonomy

Wormhole attacks can be launched using several different techniques [15, 16] mentioned as follow:

2.2.1 Wormhole using Encapsulation

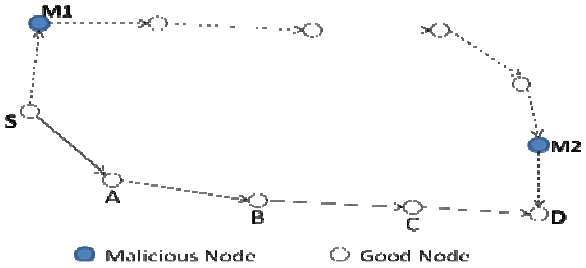

Fig.2.2 Wormhole through packet encapsulation

In between two malicious nodes, the actual hop counts do not increase. As shown in fig. 2.2, source node S try to discover the shortest path to the destination node D. Node S broadcasts a route request (RREQ), malicious node M_1 gets the RREQ and encapsulates it in a packet routed to M_2. Malicious node M2 replies it to destination node D. Because the packet is encapsulated, the actual hop count does not increase between malicious node M_1 and malicious node M_2. The RREQ also travels from source node S to destination node D through A – B – C. Destination D has two routes, one is four hops long (S-A-B-C-D), and the another is three hops long (S-M_1-M_2-D). In reality the second route is seven hops long, but it appears the shortest route, so destination node D will selects the second route.

2.2.2 Wormhole using Out-of-Band Channel

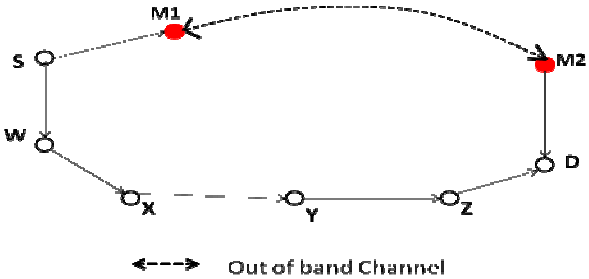

Fig.2.3 Wormhole through out-of-band channel

Two malicious nodes create high bandwidth out of band tunnel to launch the wormhole attack. The tunnel can be establish through wired or wireless link. As shown in fig. 2.3, nodes M1 and M2 are malicious nodes and having an out of band channel between them. Source node S is sending a route request to destination

node D. Node M1 tunnels the route request to M2 and M2 broadcasts it to destination node D. Destination node D receives two route request packets – S-M1-M2-D and S-W-X-Y-Z-D. The first route is faster and shorter than the second, so the destination node D chooses the first route.

2.2.3 Wormhole with High Power Transmission

A route request packet received by a malicious node having high power transmission capability is broadcasted from a long distance. When the node hears the broadcast request with high power, it rebroadcasts it to the destination. In this way, the chances of malicious node increases to be in the path establishment between source and destination.

2.2.4 Wormhole using Packet Relay

One malicious node relays packets between two far away nodes to convince them that they are neighbors. As shown in fig. 2.4, node S and D are not neighbor nodes. They are connected through a malicious node M1. Malicious node M1 relays packets between node S and node D so both nodes believe that they are neighbors.

Fig. 2.4 Attack using packet relay with one malicious node.

3. Related Work

Wormhole attack detection has been a hot research topic during the last decade and lots of schemes have been proposed. Most of the existing schemes proposed in the literature require additional hardware or software or calculation of round trip time.

3.1 Distance-bounding/Consistency-based Approaches

In [12, 13] author has proposed packet leash approach. In geographical leash, when a node sends a packet, it adds its transmission time and its location. After receiving the packet, the receiving node computes the distance to the sender. Temporal leash approach requires tight clock synchronization. The transmission distance of a packet is calculated as the product of signal propagation time and the speed of light. In [17] the author has proposed secure localization method using received signal strength indicator. Challenge-response delay measurement technique is proposed in [18]. Using the measured times, the sender and receiver node estimate an upper bound on their distance. Timing based measurement approach is presented in [19] to validate the neighbors. In the ranging based approach [20] every node calculates its distance from all of its neighbors for link verification. In [21] using hop counting technique local map will be computed and if the diameter of the computed local map will be larger than the physical one, it indicates the presence of the wormhole. The approaches presented in [22, 23, 24] are all based on round trip time.

3.2 Secure Neighbor Discovery Approaches

In [25] every node sends reports wait for an acknowledgement. If node does not receive the ACK message, the next node is wormhole node. The ACK messages must be transmitted via different path than the original report is sent on and transmitted between nodes separated by two hops. In [26] using statistical analysis of multipath routing and based on the percentage of ACKs received, the destination will verify the presence of the wormhole attack. In [27] every node is equipped with a special hardware: directional antenna. Directional antenna is used to get approximate direction based on received signals. In [28], the observer nodes monitor traffic in the sensor network and generate digital evidences. It tries to detect the nodes that are not forwarding the datagram.

3.3 Connectivity-based Approaches

In [29] to detect wormhole attack the network connectivity is examined. The malicious node can not cooperate with the local connectivity test or it report incorrect connectivity information. In [30] if the size of the maximal independent set is equal or larger than forbidden parameter, node x identifies that there is a wormhole attack in the network. Due to the wormhole, the one hop neighbors of a node will increase and the node degree is used to detect wormhole [31]. In [32] the idea behind neighbor number test is that the number of neighbors of the malicious node is increased by creating fake links and the idea behind all distance tests is that due to the wormhole the path becomes shorter in the network. In [33] the wormhole is located by finding the fundamental topology deviations and tracing the sources. For visualization based approach [34], if there is a presence of wormhole, the shape of the network layout will have some bent or distorted features. By visualizing the graph, the wormhole attack is detected. In [35] the idea is to find alternate shortest path between sender and receiver and count the no. of hops to detect the wormhole attack.

3.4 Localization-based Approaches

The author has presented a graph theoretic framework for modeling wormhole links in [36].The mobile beacon moves in the networks to communicate with the static beacons [37]. For a request message, if mobile beacon receives a reply message from a static beacon more than once then it can determine there is a wormhole attack in its transmission range. In [38] the author has proposed the concept of location based keys that can act as efficient countermeasures against wormhole attack. In [39], communication keys to prevent wormhole attacks are efficiently distributed to sensor nodes. Sensor nodes located beyond the communication ranges do not share a communication key. The scheme presented in [41] is an improvement over the scheme presented in [40] by utilizing antenna rotations and multiple transmit power levels.

4. Proposed Method

4.1 System Model and Assumptions

Wireless sensor network consists of n sensor nodes. In wireless sensor network, two sensor nodes are considered neighbors if the distance between them is within the transmission range r. We assume that the sensor nodes are static. The sensor nodes uses broadcast communication primitive. When sensor nodes are deployed, all nodes are legitimate nodes and no malicious nodes are present. Initially during some interval there are no malicious nodes present in the network and nodes safely found their neighbor information.

Once deployed immediately the nodes form their neighborhood table. We assume that the ranges (wormhole radius) of receiving and the sending of both wormhole transceivers are the same. Proposed scheme requires a pre-distribution pair-wise key management protocol as in [42].

4.2 Adversary Model

We assume that a malicious entity can launch many kinds of wormhole attacks. It is able to launch high-speed low-latency tunnel. One malicious node records packets at one location and replays them to second malicious node at the location which is far away through out of band tunnel. The malicious node drop packets without forwarding them to the next node. In such situation, base station is not able to receive any information from the target area. The malicious entity can also modify the data packets.

4.3 Defense Algorithm

Proposed protocol consists of three phases: In the first phase, every node builds its one hop neighborhood table. In the second phase, the neighbor table is exchanged to forms two hop neighborhood list. Third phase includes the wormhole detection procedure.

(1) Build one-hop neighborhood list.

After deployment, each node sends a hello message to its neighbors. The node who receives the hello message sends reply back. A shared key is used to authenticate this reply. After verifying the authenticity, the sender node adds the receiving node to its neighbor list. Every node performs the same procedure to build one hop neighborhood list.

(2) Build two-hop neighborhood list.

To build two hop neighbor lists, each node exchanges its neighbor list to its neighbors. Every node broadcast message that contains its own neighbor list. It is authenticated individually by the shared key. When receiving node hears the broadcast request, it first verifies the authenticity of neighbor list of sender node and stores it if verified correctly. At last, each node has a table of its neighbor list and its neighbors' neighbor list.

(3) Wormhole detection procedure.

At some point of time, node x overhears packets from some new nodes, say node y. Node y is a suspected node. The neighbor list consists of two parts: trusted and suspected. Node y is added into suspected part. There might be a wormhole attack or not. For every suspected node added in the neighbor list, the following steps are performed:

Step 1: Node x verifies that whether node x and node y share any one hop common neighbor. Two fake neighbor nodes can not share a common one hop neighbor node. Two genuine neighbor nodes generally share a common one hop neighbor node among them. If found then go to step (4), otherwise go to the next step.

Step 2: Node x verifies that any neighbors of x is directly connected to any neighbors of node y. Node x visits all its neighbor's neighbor table to verify that if any of y's neighbors is present. If found then go to step (4), otherwise go to the next step.

Step 3: Node x tells its trusted neighbors to find the shortest path to suspected node y which can not be direct and it avoids the one hop neighbors of node x. It does not include the path from node x to y. If the reported path length is less than predefined threshold, then go to next step otherwise go to step (6).

Step 4: Delete node y from suspicious entry and add it to the list of trusted entry. The link x->y is declared as safe link. No wormhole attack presence in the network.

Step 5: Stop.

Step 6: The link x->y is declared as fake link and wormhole attack is detected.
Step 7: Stop the communication with two far away located nodes.
Step 8: Stop.
The algorithm for detection procedure is as follow:
Result: To identify whether new node is genuine neighbor or not.
Input: x and y, where y is a suspected neighbor of node x and 2-hop neighbor information of node x.
Output: The link x->y is declared as safe link or fake link.

```
BOOL Detection(x, y, Suspects(x))
Begin
    For each node yi in Suspected_Part(x) do
        if ( Nx ∩ Ny ≠ Φ )
          then
            return FALSE;
            Add y to the list of trusted neighbors;
        end
        if (2hop-Nx ∩ Ny ≠ Φ)
          then
            return FALSE;
            Add y to the list of trusted neighbors;
        end
            for each y Ɛ Suspected_Part
                  every xi Ɛ Nx, xi finds routes from  xi  to suspected node y where Nx is not subset  of the route
                  and the path from xi to y is not direct;
               every xi Ɛ Nx, xi sends  | Rxi-y| to x.
       if any |Rxi-y| <=threshold
          then
         return FALSE;
         Add y to the list of trusted neighbors;
       end;
return TRUE;
Remove y from the list of neighbors;
end;
end;
```

5. Performance Analysis and Simulation Results

5.1 Storage Cost Analysis

The average number of neighbors is represented by N_A. The total number of nodes is represented by N_T. The size of ID is represented by S_{ID}. The key size is represented by S_K. To store the neighbor list the storage cost required is $S_{ID}N_A$. To store a shared key with its neighbors the storage cost required is S_KN_A. To store the neighbors' neighbor list the storage cost required is $S_{ID}N_AN_A$. Therefore, the total storage cost for each node is $\{S_{ID}N_A + S_KN_A + S_{ID}N_AN_A\}$. If S_{ID} is 4 bytes, S_K is 8 bytes, and N_A is 10, then the storage cost for each node is 520 bytes. The sensor node has 4 kB of RAM and 512 kB of flash memory in wireless sensor network [43]. Proposed approach is suitable for wireless sensor network because it uses very less memory. The total storage cost in the network is $\{S_{ID} * N_A + S_K * N_A + S_{ID} * N_A * N_A\} * N_T$.

5.2 Simulation Results

For simulation we have used NS2. Packet delivery ratio and throughput both decrease after creating the attack. After applying proposed algorithm, it is nearer to its original value. The detection rate is the ratio of the number of attacked links detected to the total number of attacked links. The detection rate increases as the tunnel length increases. The proposed algorithm has 95% detection accuracy. The threshold value used is 3. False positive are totally reduced. False negative occurs when wormhole launched for short distance.

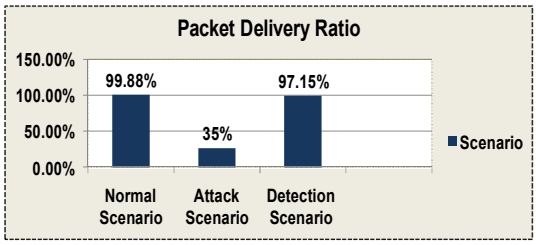

Fig. 5.1 Packet Delivery Ratio

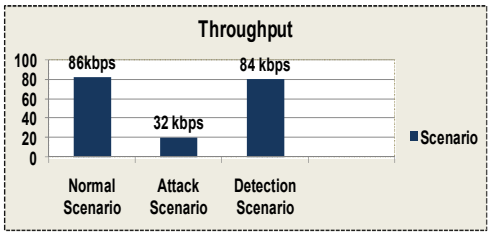

Fig. 5.2 Throughput

6. Conclusion

Wormhole attack is very dangerous to wireless sensor networks. Detecting it is very hard because it disturbs routing without any cryptographic break. Our proposed method can effectively detect wormhole attack in wireless sensor networks. Performance analysis shows that it has good storage cost and it is applicable to resource constrained wireless sensor networks. In future we will develop wormhole detection method for dynamic sensor networks.

References

[1] K. Romer and F. Mattern; "The design space of wireless sensor networks," IEEE Wireless Communications, vol. 11, no. 6, pp. 54–61, Dec. 2004.
[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci; "A Survey on Sensor Networks," IEEE Communications Magazine, Vol. 40, No. 8, 2002, pp. 102-114.
[3] S. Capkun, and J.P. Hubaux; "Secure positioning of wireless devices with application to sensor networks," 24th Annual Joint Conference of the IEEE Computer and Communications Societies, IEEE INFOCOM 2005, vol. 3, pp. 1917-1928.
[4] S. Hadim and S.N. Mohamed; "Middleware challenges and approaches for wireless sensor networks," IEEE Distributed Systems, vol. 7, no. 3, pp. 1-23, Mar. 2006.
[5] Wang,Yong, Attebury, Garhan and Ramamurthy, Byrav; "A Survey of security issues in wireless sensor networks" IEEE Communications Surveys and Tutorials, 2006.
[6] Chen, Xiangqian, et al.; "Sensor network security: A survey" IEEE Communications surveys & tutorials, vol. 11, pp. 52-73, 2009.
[7] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," Journal of Ad Hoc Networks, vol. 1, no. 2-3, pp.293–315, 2003.
[8] R. Shokri, M. Poturalski, G. Ravot, P. Papadimitratos, and J. P. Hubaux,"A practical secure neighbor verification protocol for wireless sensor networks," in WiSec '09: Proceedings of the second ACM conference on Wireless network security, NY, USA: ACM, 2009, pp. 193–200.
[9] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in ACM Workshop on Wireless Security (WiSe 2003), September 2003.
[10] Poturalski, Marcin, Papadimitratos, Panos and Hubaux; "Jean-Pierre.Secure neighbor discovery in wireless networks: formal investigation of possibility" ACM symposium on Information, computer and communications security, NY, USA: ACM, 2008.
[11] Azer, Marianne A, Sherif M and Magdy S; "An innovative approach for wormhole attack detection and prevention in wireless sensor networks" IEEE International conference on Networking, Sensing and Control (ICNSC), 2010, pp. 366 - 371.
[12] Y. C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," IEEE Computer and Communications Societies, IEEE, vol. 3, pp. 1976–1986, 2003.
[13] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Wormhole attacks in wireless networks." IEEE Journal on Selected Areas in Communications , vol. 24, no. 2, pp. 370–380, 2006.
[14] J. Eriksson, S. Krishnamurthy, and M. Faloutsos, "Truelink: A practical countermeasure to the wormhole attack," in ICNP, pp. 75-84, 2006.
[15] S. Han, E. Chang, L. Gao, and T. Dillon. "Taxonomy of attacks on wireless sensor networks," Proceeding of the First European Conference on Computer Network Defense School of Computing, pp. 97−105, Dec. 2005.
[16] Sanzgiri, Kimaya, et al, "A secure routing protocol for ad hoc networks" Proceedings of the 10th IEEE International Conference on Network Protocols, pp. 78 – 87, 2002.
[17] Honglong Chen,Wei Lou, Xice Sun and ZhiWang; "A Secure localization approach against wormhole attacks using distance consistency" EURASIP Journal on Wireless Communications and Networking, Volume 2010, 11 pages.

[18] S. Capkun, L. Buttyan and J.P. Hubaux, "SECTOR: Secure tracking of node encounters in multi-hop wireless networks" Proceedings of the 1st ACM workshop on Security of ad-hoc and sensor networks (SASN 03), pp. 21-32, Oct. 2003.
[19] Majid Khabbazian, Hugues Mercier and Vijay K. Bhargava, "Severity Analysis and Countermeasure for the Wormhole Attack in Wireless Ad Hoc Networks" IEEE Transactions on Wireless Communications, Vol. 8, and Issue: 2, 2009, pp. 736-745.
[20] Reza Shokri, Marcin Poturalski, "A Practical Secure Neighbor Verification Protocol for Wireless Sensor Networks" ACM, WiSec'09, March 16-18, 2009, Zurich, Switzerland.
[21] Yurong Xu, Yi Ouyang, Zhengyi Le, James Ford, Fillia Makedon, "Analysis of Range-Free Anchor-Free Localization in a WSN under Wormhole Attack" ACM, MSWiM'07,October 22-26, 2007, Chaina, Greece.
[22] Prasannajit B, Venkatesh, Anupama S, Vindhykumari K, Subhashini S R, Vinitha G; "An Approach towards detection of wormhole attack in sensor networks" First IEEE International Conference on Integrated Intelligent Computing, 2010.
[23] Zhibin Zhao, Bo Wei, Xiaomei Dong, Lan Yao, Fuxiang Gao; **"**Detecting wormhole attacks in wireless sensor networks with statistical analysis" International Conference on Information Engineering(ICIE), 2010, pp. 251-254.
[24] Shams Qazi, Raad Raad, Yi Mu, Willy Susilo; "Securing DSR against wormhole attacks in multirate ad hoc networks" Journal of Network and Computer Applications, pp 582-593, 2013.
[25] Hyeon Myeong Choi, Su Man Nam, Tae Ho Cho, "A Secure routing method for detecting false reports and wormhole attacks in wireless sensor networks" Scientific Research on Wireless Sensor Network, March 2013, vol. 5,pp. 33-40.
[26] Lijun Qian, Ning Song, Xiangfang Li; "Detection of wormhole attacks in multi-path routed wireless ad hoc networks: A statistical analysis approach" Journal of Network and Computer Applications, 2005.
[27] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks" in Network and Distributed System Security Symposium (NDSS), pp. 131–141, 2004.
[28] Bayrem Triki, Slim Rekhis, and Noureddine Boudriga, "Digital investigation of wormhole attacks in wireless sensor networks" *Eighth IEEE International Symposium on Network Computing and Applications,* pp. 179-186, 2009.
[29] Xiaomeng Ban, Rik Sarkar, Jie Gao, "Local Connectivity Tests to Identify Wormholes in Wireless Networks" ACM, MobiHoc'11, May 16-20, 2011, Paris, France.
[30] Ritesh Maheshwari, Jie Gao and Samir R Das; "Detecting wormhole attacks in wireless networks using connectivity information" IEEE INFOCOM, 2007.
[31] Y.-T. Hou, C.-M. Chen, and B. Jeng; "Distributed detection of wormholes and critical links in wireless sensor networks," in Proc. of IIHMSP, 2007.
[32] Levente Buttyan, Laszlo Dora, and Istvan Vajda; "Statistical wormhole detection in sensor networks" SAS 2005, Springer, pp. 128–141.
[33] Dong D, Liu Y, yang Li X, Liao X, Li M; "Topological detection on wormholes in wireless ad hoc and sensor networks" 17th IEEE International Conference on Network Protocols, 2009, pp. 314-323.
[34] W. Wang and B. Bhargava; "Visualization of wormholes in sensor networks" WiSe'04, Proceeding of the 2004 ACM workshop on Wireless Security, ACM Press, pp. 51-60, 2004.
[35] Thaier Hayajneh, Prashant Krishnamurthy, David Tipper, "DeWorm: A Simple Protocol to Detect Wormhole Attacks in Wireless Ad hoc Networks" Third International Conference on Network and System Security, 2009, NSS'09, Pages: 73-80.
[36] Radha Poovendran, Loukas Lazos; "A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks" Springer, Wireless Netw (2007) 13:27–59.
[37] Honglong Chen, Wendong Chen, Zhibo Wang, Yanjun Li, "Mobile Beacon Based Wormhole Attackers Detection and Positioning in Wireless Sensor Networks" International Journal on Distributed Sensor Networks, Vol. 2014, 10 pages.
[38] Yanchao Zhang, Wei Liu, Wenjing Lou, Yuguang Fang, "Location-Based Compromise – Tolerant Security Mechanisms for Wireless Sensor Networks" IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, February 2006.
[39] Issa Khalil, Saurabh Bagchi, Ness B. Shroff, "MOBIWORP: Mitigation of the wormhole attack in mobile multihop wireless networks" Elsevier, Journal of Ad Hoc Networks 6 (2008), 344-362.
[40] L. Lazos and R. Poovendran, "SeRLoc: Robust Localization for Wireless Sensor Networks," ACM Transactions on Sensor Networks, pp. 73–100, 2005.
[41] L. Lazos and R. Poovendran, "HiRLoc: High-Resolution Robust Localization for Wireless Sensor Networks," IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 233–246, 2006.
[42] D. Liu and P Ning, "Establishing Pair-wise Keys in Distributed Sensor Networks," in Proceedings of the 10th ACM conference on Computer and communication security (CCS'03), Washington D.C., USA October 27-

30, 2003.
[43] C. Karlof, N. Sastry, D. Wagner, TinySec: a link layer security architecture for wireless sensor networks, in: Proceedings of the Second ACM Conference on Embedded Networked Sensor Systems (SenSys 2004), Baltimore, Maryland, 2004.