Wormhole Attacks and Countermeasures in Wireless Sensor Networks : A Survey

Manish Patel[1], Akshai Aggarwal[2], Nirbhay Chaubey[3]
Computer Engineering Department, Gujarat Technological University, Ahmedabad, Gujarat, INDIA
[1] it43manish@gmail.com
[2] akshai.aggarwal@gmail.com
[3] nirbhay@ieee.org

Abstract—**Wireless sensor networks can be deployed in inhospitable terrains or in hostile environments to provide continuous monitoring and processing capabilities. Due to the wireless and distributed nature, security is very crucial issue in wireless sensor network. Security comes from attacks. Detecting wormhole attack is very hard compared to other attacks because it uses private, out-of-band channel to launch the attack. To launch this type of attack, attacker does not require any cryptographic breaks. Wormhole attack represents one forms of Denial of Service attack. It is a gateway of many more attacks. This paper focuses on the various wormhole detection techniques, the open research areas and future research directions.**

Keywords: Wireless sensor network, security, distributed, wormhole, out-of-band.

I. Introduction

Wireless sensor network consists of large number of sensor nodes. Each sensor node consists of processor, analog to digital converter, transceiver and battery. Sensor nodes are densely deployed. They use broadcast communication primitive. Sensor nodes rely on wireless channels for transmitting and receiving data from other nodes [1, 2]. Sink node is the data aggregation point. Wireless sensor networks that are capable of observing the environment, processing data and making decisions based on these observations [3-6]. These networks are important for a number of applications such as coordinated target detection and localization, surveillance and environment monitoring.

Providing security services in sensor networks turns out to be a very challenging task. First, sensor nodes usually have very limited resources such as storage, bandwidth, computation and energy. It is often undesirable to implement expensive algorithms on sensor nodes. Second, sensor nodes are usually deployed in unattended environment. An attacker can easily capture and compromise a few sensor nodes without being noticed. When sensor nodes are compromised, the attacker can learn all the secrets stored on them and launch a variety of attacks [7-12]. Thus any security mechanism for sensor networks has to be resilient to compromised sensor nodes. Third, most sensor applications are based on local computation and communication, while adversaries are usually much more powerful and resourceful than sensor nodes.

Wireless sensor networks are vulnerable to many attacks, but among all the attacks wormhole attack is very dangerous. Two malicious nodes are located far away and create a high speed tunnel [13-15]. At one ends of the tunnel, one malicious node receives the traffic and forwards it to the end of the tunnel to the other malicious node. It is also possible that packet is altered that contains different information. The packets pass through the tunnel can propagate faster compared to the normal path. To launch the attack, attacker does not require knowing the protocols used in the network or the services offered in the network.

The rest of the paper is organized as follows. In section 2 we have discussed the significance of wormhole. Section 3 provides wormhole attack taxonomy. In section 4, we have discussed existing detection techniques. Section 5 presents the open research areas. Finally, conclusion is presented in section 6.

II. Significance of Wormhole Attack

In this paper, we discuss very dangerous attack, known as the wormhole attack. It is easy to deploy but difficult to detect.

A. Motivation

Security is very crucial for sensor network because of their fundamental characteristics. Security comes from attacks. If no attacks are there, there is no need for security. A typical threat called wormhole attack is very dangerous for WSNs. One malicious node records packets from one end of the network and tunnels them to another malicious node located in different area of the network and disturbs the whole routing process [16-18]. Research related to wormhole attack in wireless sensor network has received much interest recently. Survey papers presented recently on the countermeasures of wormhole attack have discussed merits and demerits of some existing techniques. But it lacks the recent techniques and the detailed analysis of all existing techniques for wireless sensor networks. This motivates us to present a survey of all existing wormhole attack detection

DOI: 10.21817/ijet/2017/v9i2/170902126

techniques for WSNs. We have presented the advantages and limitations of all the methods. This paper can assist the researchers to develop a new effective detection scheme.

B. Description of Wormhole Attack

One malicious node records the packets from one area, tunnels them to another malicious node which is located far away in another area and disturbs the routing process.

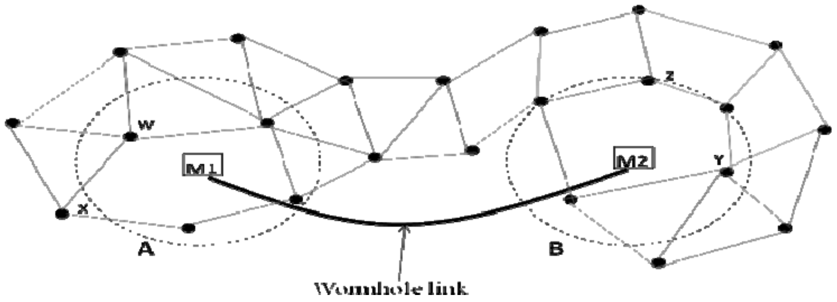

Fig. 1 Wormhole Attack

The functionality of wormhole attack is shown in fig. 1. Two Malicious nodes M1 and M2 create a tunnel. Two nodes M1, M2 and the link are hidden. Genuine network nodes are not aware about them. Attacker does not require any cryptographic break. Wormhole can leads to many more attacks such as denial of service, black hole or selective forwarding attacks.

C. Wormhole Threat against Routing Protocols

1) Periodic Protocols: In distance vector routing algorithm [19], the routing table of a node contains the distance from the node itself to other nodes. Periodically every node sends its entire routing table to its neighbors. As per the entries in the neighbor's routing table, the node updates its routing table. As shown in fig. 2, when node S_9 broadcasts its routing table, S_2 hears it via tunnel and updates its routing table that S_9 is one hop away and $\{S_8, S_{10}, S_{11}, S_{12}, S_{13}\}$ all are two hops away.

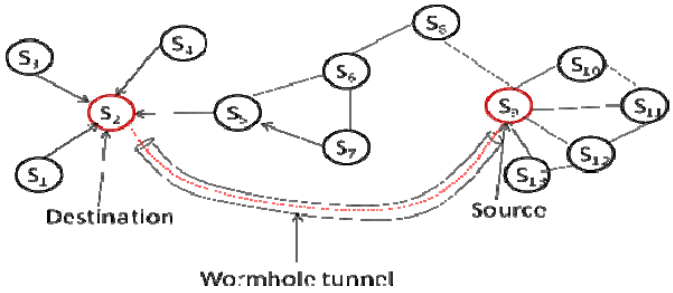

Fig. 2 Wormhole attack against distance vector routing protocol

2) On-Demand Protocol: The mechanism to discover the route in DSR [20] and AODV [21] protocols is an example of on demand protocols. As shown in fig. 3, node S_9 wants to establish a path to node S_2. So S_9 broadcasts route request (RREQ) packet to all neighboring nodes. The node that receives the RREQ packet, forward it to the next node and it reaches to the destination. When destination node receives the first RREQ, it sends route reply (RREP) message on the same path to the source node. In this way, a path is establishes between source and destination node. If an attacker mounts a wormhole tunnel between source node S_9 and destination node S_2, the tunnel establishes a path of one hop route.

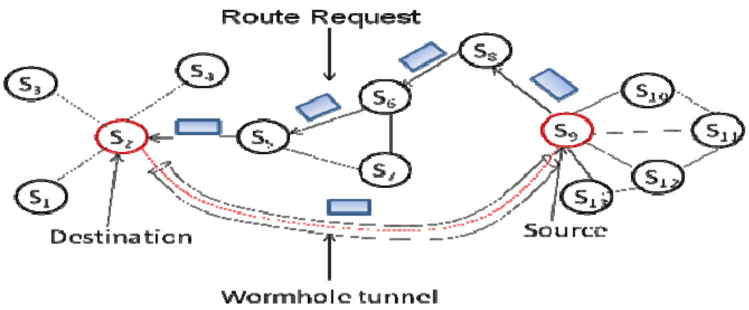

Fig. 3 Wormhole attack against on demand routing protocol

D. Variants of Wormhole Attacks

In wireless sensor network, following attacks are related to wormhole attacks.

1) Spoofing: The malicious node takes the identity of another node in the network and traffic is directed towards the malicious node. It is similar to hidden wormhole attacks.

2)Selective Forwarding: In order to reduce the probability of detection, the malicious node can mount an intelligent attack, called selective forwarding attack, in which it selectively drops the data packets.

3) Sinkhole: A malicious node attracts network traffic by advertising itself as having the shortest path to the base station. It can be achieved by using a wormhole tunnel. One malicious node attracts traffic from one location and diverts it to the other malicious node through tunnel.

III. Wormhole Attack Taxonomy

The wormhole attack can be launched in two different modes [22]: The hidden mode and the participation mode. In the first mode, the attackers remain hidden from the legitimate nodes. They do not use their identities in communication. They capture messages at one end of the wormhole and reply them at the other end. In this way, they can make a "tunnel" between two nodes that are actually far away from each other. To launch the wormhole attack, the attackers require no cryptographic keys. In the second mode, the attackers can launch a more powerful attack by using valid cryptographic keys. The malicious nodes do not create tunnel. In between two malicious nodes, the actual hop count does not increase and the packets will be delivered with smaller no. of hops. Wormhole attacks can be launched using encapsulation based technique or by creating out-of-band tunnel [23, 24] mentioned as follow:

A. *Wormhole using Encapsulation*

As shown in fig. 4, source node S broadcasts a packet. The packet is received by node A and also malicious node M1. In between malicious nodes M1 and M2, the actual hop count does not increase. The path that includes the malicious nodes has shorter hop count compared to the original path. The original path consists of path S-A-B-C-D.

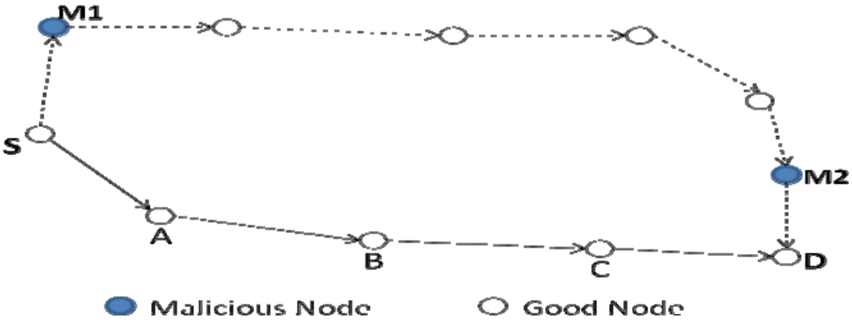

Fig.4 Wormhole through packet encapsulation

B. Wormhole using Out-of-Band Channel

As shown in fig. 5, two malicious nodes M1 and M2 are connected through high speed tunnel. Node M1 records packets from source node S and tunnel it to node M2. Node M2 replies it to destination node D. The original path is S-W-X-Y-Z-D. The tunnel is out-of-band high speed channel.

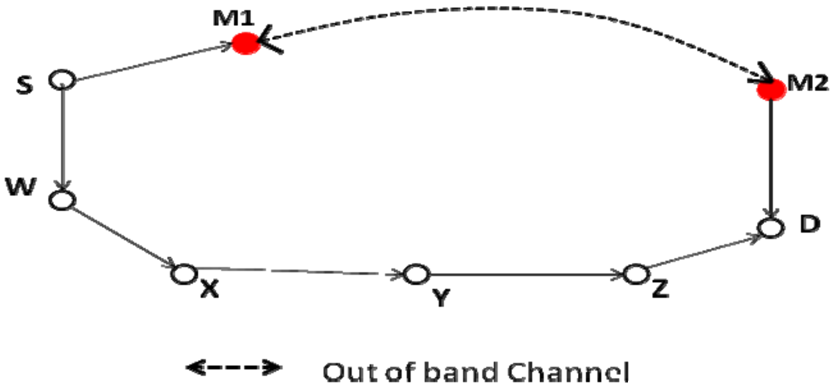

Fig. 5 Wormhole through out-of-band channel

IV. Wormhole Attack Detection Mechanism

Wormhole attack detection has been a hot research topic during the last decade and lots of schemes have been proposed. We categorize existing schemes in the literature that could be used to find wormhole links, analyze their properties and comment on their practicality.

A. Distance-bounding/Consistency-based Approaches

1) Geographical Packet Leashes Approach: Author has proposed geographical leash approach for wormhole attack detection [16, 17]. A leash is any information that is added to a packet designed to restrict the packet's maximum allowed transmission distance. Every node knows its own location. When a node sends a packet, it appends two things to the header: the transmission time and the sender's location. After receiving the packet, the receiving node computes the distance to the sender. It also computes the time taken by the packet to traverse the path. The distance information is used to identify whether the packet has passed through tunnel or not.

Advantages: (1) It can be used in conjunction with a radio propagation model, thus allowing them to detect tunnels through obstacles. (2) It does not require the tight time synchronization. *Limitations:* Broadcast authentication mechanism results in increased network overhead. Location information may require more bits to represent, further increasing the network overhead.

2) Temporal Packet Leash Approach: Location information of nodes is not needed in temporal packet leash approach [16, 17]. It requires tight clock synchronization in the order of nanoseconds. An authenticated timestamp is added to the header, before the node sends a packet. The node, who receives the packet, compares this timestamp with the receiving time. The transmission distance of a packet is calculated as the product of signal propagation time and the speed of light. A wormhole is present if the estimated distance is too large. *Advantages:* It is highly efficient.

Limitations: It may not detect physical layer wormholes.

3) Distance Consistency Approach: In [25] the author has proposed a distance-consistency-based secure localization method to detect wormhole attacks. Three different types of nodes locators, sensors, and attackers are deployed in the network. The sensors use the Received Signal Strength Indicator (RSSI) method to measure the distances to their neighboring locators. A sensor node is under a duplex wormhole attack if it receives the location request message from itself. The sensor identifies the valid locators using different identification approaches. The Maximum Likelihood Estimation (MLE) method is used by the sensor nodes to estimate their locations. *Advantages:* (1) It can distinguish the duplex and simplex wormhole attack. (2) It has good performance even when the malicious locators are more than the normal ones. *Limitations:* It assumes that the transmission range of all nodes is same.

4) Using Rank Information: The author has proposed wormhole detection approach for RPL (Routing Protocol for Low-Power and Lossy Networks) in [26]. For measuring the distance the rank value is used. The rank value is used to represent the position of a node. The root node has the rank value of zero. The rank value of any node is the number of hops to the root plus one. As the node moves away from the root, the rank value is increased. If unreasonable rank values are found to estimate the distance to root node then malicious nodes are detected. Once malicious nodes are found, they are stored in a black list. *Advantages:* The computing process is not complex. No additional hardware is required. *Limitations:* Attacker can make fake messages to evade detection. Confidentiality is also an important parameter for consideration.

5) Challenge-Response Delay Measurement: In [27] author has presented SECure Tracking Of node encounteRs (SECTOR). It is based on distance bounding techniques and one way hash chains. Using Mutual Authentication with Distance Bounding protocol, the nodes calculate their mutual distance at the time of encounter. Both nodes measure the distance to the other node at the same time. The protocol consists of bit exchanges between the nodes. Node X sends bit α_i to node Y (considered as a challenge). Node Y sends bit β_i to node X immediately after it received α_i (considered as a response). Node X measures time between sending α_i and receiving β_i and node Y measures the times between sending β_i and receiving $\alpha_{i+1.}$ Using this measured times, node X and Y calculate an upper bound on their distance. A symmetric key is shared by each pair of nodes. The shared key is established between two nodes before running the distance bound protocol. Using this key, message authentication code will be generated. This code is used to prove the authentic of the messages exchanged. *Advantages:* Location information or clock synchronization is not needed. *Limitations:* Using multiple hash chains, as the number of nodes increase the storage requirement also increases linearly.

6) Timing-based Measurement Approach: Timing based measurement approach for wormhole attack detection is proposed in [28]. During two rounds of communication, each node can validate its neighbors. During the first step, every node sends a signed Hello message and records a time. This message contains its ID and a nonce. After the first step, each node has a list of its neighbors. In the second step, every node signs and sends a follow-up packet which includes the sending and receiving time of the node's Hello message and the list of all the ID's. For example, node X receives Y's Hello message. After receiving a follow-up packet from Y, node X checks its nonce and verifies Y's signature. If $((t_{X,Y} – t_X) – (t_Y – t_{Y,X}) *C) /2 \leq T_{max}$, then it accept Y as its neighbor, where t_A is the time recorded by node A when it has send the Hello message, $t_{A,B}$ is the time recorded by A when it receives B's Hello and T_{max} represents the maximum transmission range. The term ($t_{X,Y}$ – t_X) is the time to get the response. Node X subtracts (t_Y – $t_{Y,X}$), the delay at node Y, from ($t_{X,Y}$ – t_X). At the end of second step, each node has a list of its 2-hop neighbors. *Advantages:* (1) It does not require synchronized clocks. (2) One-to-one communication with the neighbors is not required. *Limitations:* It is assumed that when any node sent or received a packet, it is able to record time.

7) Ranging-based Secure Neighbor Discovery Approach: Ranging-based secure neighbor discovery protocol for WSNs is proposed in [29]. Each node estimates its distance to the other nodes it can communicate with through a single hop. Sensor nodes exchange information about their estimates. A series of tests is conducted by each node for detecting topology distortions created by tunneling. The protocol is divided into three phases: The first phase is ranging. In this phase, every node calculates its distance from all of its neighbors. By broadcasting an ultra-sound message, ranging is done simultaneously for all neighbors. An acknowledgement message secures the synchronization. In the second phase the neighbor table is exchanged. The node shares its neighbor table with each of its neighbors. The calculated distance during the ranging phase is included in the table. The third phase is link verification. The neighbor table is verified through a number of security tests. *Advantages:* The chance of creating a tunnel by the adversary is very negligible. *Limitations:* Each node requires a microsecond precision clock, a radio-frequency interface and a sound interface.

8) Range-Free Anchor-Free Localization Approach: In [30] the author has discussed range free (not using distance measurement) and anchor free (no reference nodes with known physical coordinates) localization in a wireless sensor network. The algorithm consists of three parts: The first part introduces the measurement or probe procedure. In the second part, a local map will be computed by each node for its neighbors. The third part introduces detection procedure. The diameter feature is used to determine whether there is a wormhole attack or not. Because of the presence of the wormhole, the diameter of the computed local map will be larger than the physical one. If $d > (1 + \lambda)\ 1.4\ R$ then there is a wormhole attack in the network, where d is the diameter of a local map, λ is a constant parameter in between 0 and 1. Once the wormhole attack is detected a special message will flood out to freeze neighboring nodes. Upon receiving this message, the bootstrap node will restart the localization procedure and other nodes clean the stored hop-coordinates. *Advantages:* It has a low false toleration rate and a low false detection rate. *Limitations:* Threshold and λ should be decided automatically to improve the detection method.

9) Geographic Wormhole Detection in Wireless Sensor Networks: In [31], the authors have presented wormhole detection approach for geographic routing protocol. For detecting malicious nodes efficiently, the authors have proposed a new pair wise key pre-distribution protocol. The public and private keys are generated through one-way hash function. The neighborhood table is periodically updated by receiving the beacon packets from the neighbors. When the destination node receives the packet, it calculates the distance between source and destination and counts the number of hops from source to destination. If wormhole is detected then source sends a request to destination to send packet again to another path. *Advantages:* It does not require network synchronization, additional hardware, special guard nodes or any assumptions. It is able to detect all wormhole attacks. *Limitations:* Each sensor node requires a pair of public and private keys to communicate with the other nodes.

10) Statistical Analysis & Time Constraint-based Approach: The proposed detection algorithm in [32] is based on statistical analysis (SA) and time constraint (TC). After collecting the routing information, the sink node initiates statistical analysis to identify the suspicious links. The link which is attractive in terms of traffic is defines as a suspicious link. Let L_{xy} is a suspicious link. For validation node x sends a probe message to node y. Node y makes a reply when it receives the message. The sensor node compares the round trip time with the standard time delay T and decide whether it is genuine neighbor or not. *Advantages:* It does not require any extra hardware or strict clock synchronization. *Limitations:* In some cases, the round trip time may be longer due to processing or queuing delay at any intermediate node without the presence of a tunnel.

11) Delay per Hop Indication Detection Mechanism: In [33] the main focus is to measure the delay and hop count information of different paths from sender to the receiver. After collecting the information, detection is performed at sender. High delay per hop value indicates path suffers from wormhole attack. Smaller value of delay per hop indicates legitimate path. *Advantages:* (1) It does not require any position information and clock synchronization. (2) It provides higher power efficiency because the mobile nodes do not required any special hardware. *Limitations:* The detection mechanism does not work well when all the paths are tunneled. This is because of the detection algorithm is based on difference of delay per hop values between normal paths and tunneled path.

12) RTT-based Approach in Multirate Ad hoc Networks: Proposed protocol in [34] is based on round trip time based mechanism. The source node calculates the round trip time of all the neighboring nodes involved in the route. Processing time (PT) and transmission time (TT) for route request (RREQ) and route reply (RREP) packets are calculated. Round trip time is calculated as, $RTT = TT_{Ni} + PT_{Ni} + PD$. Actual round trip time is compared with expected round trip time. If $|A(RTT\ N_iN_{i+1}) - E(RTTN_iN_{i+1})| <= |\mu|$ then no wormhole attack is detected between N_i and $N_{i+1.}$ *Advantages:* (1) It covers the multi rate transmission problem. (2) It does not need any special hardware. (3) It does not need any complex calculations. *Limitations:* (1) Some additional memory is required to store the round trip time. (2) To find RTT, processing time is required to perform the calculation.

13) Wormhole Resistant Hybrid Technique: Proposed algorithm in [35] takes advantages of both watchdog and Delphi methods to detect wormhole attack. To find the probability of wormhole presence, it calculates packet loss and time delay probability of the established path. Ranking and color is assigned as per the behavior of the node. During the route discovery phase of AODV, time delay probability per hop is calculated and using this time delay probability for the complete path is calculated. Then packet loss probability per hop is calculated and using this packet loss probability for the complete path is calculated. These two values are used to decide whether the path is wormhole free or not. *Advantages:* (1) It does not require any additional hardware and high computational. (2) It can defend against almost all categories of wormhole attacks. (3) It has good detection accuracy.

B. Secure Neighbor Discovery Approaches

1) ACK Message Transmission Approach: The author has proposed an acknowledgement (ACK) message transmission approach for wormhole attack detection in WSNs [36]. It consists of three parts: Initialization, En-route filtering and wormhole attack detection. In the initialization part, each node sends hello messages to identify their neighbor nodes. In the second phase, each intermediate forwarding node drops the false reports and sends drop messages to the next node. In the third phase, 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. The TTL (time to live) is the maximum number of hops required to transmit the ACK messages. If the ACK message is not delivered to the previous node within the TTL limit, then there is a presence of wormhole attack. *Advantages:* It reduces both false alarms and energy consumption. *Limitations:* (1) If TTL limit was not set, then ACK messages would float throughout the network. It will consume the energy of nodes. (2) If the TTL value is too large then the ACK send by Y may be delivered to node X even though the data are transmitted via a wormhole. (3) If the TTL value is too small, it may not be delivered to node X even though the data are not sent via wormhole.

2) Statistical Analysis of Multipath (SAM) Approach: In [37] the statistical analysis of multipath routing has been considered. If any anomalous pattern is found during statistical analysis of the routes, the destination node will send some probe packets including some dummy data packets to the source node along the suspected route. Probe packets are identified by the source node and will send acknowledgement (ACKs) through the same route. Based on the percentage of ACKs received, the destination will verify the presence of the wormhole attack. After confirming the presence of attacker, it is isolated from the network by informing all its neighbors. *Advantages:* (1) Overhead required is very limited. The required route information is collected by route discovery. Only the destination node needs to run SAM. (2) It works well under different network topologies and node transmission range. *Limitations:* (1) The nodes are assumed to have low mobility. (2) If an adversary node behaves normally during routing, SAM cannot detect it.

3) Detection using SeRWA : Secure Routing protocol against a Wormhole Attack (SeRWA) for WSNs is proposed in [38]. By sending hello message, each node builds its neighbor list which may include neighbors connected through tunnel. The neighbor lists are exchanged by the neighboring nodes. The base station broadcasts a routing beacon for initial route discovery process. Each node records the neighboring node as its parent by accepting the first routing beacon and it rebroadcast the updated routing beacon. The process recursively continues. Each node sends a packet will monitor its parent and if the parent node drops or tampers the packet, it indicates that parent node is connected by a tunnel. Both of these nodes and their neighbors will reconstruct their neighbor lists by avoiding the remote neighbors. After detecting the wormhole, the base station sends a new routing beacon for route discovery to avoid wormhole attack. *Advantages:* (1) It does not require any special hardware. (2) Only private key cryptography is used that is suitable for WSNs. (3) False positives are very less. *Limitations:* (1) The sensor nodes are static (not movable). (2) It is assumed that the sensor nodes uses reliable channel.

4) Using Directional Antenna: In [39], every node is equipped with a special hardware: directional antenna. Directional antenna is used to get approximate direction based on received signals. The author has presented three protocols: directional neighbor discovery, verified neighbor discovery and strict neighbor discovery. The first protocol does not require any cooperation between nodes. It cannot prevent many wormhole attacks. The second protocol share information among neighboring nodes to prevent wormhole attacks. The attacker controls only two endpoints and the victim nodes are at least two hops distant. The third protocol prevents wormhole attacks even when the victim nodes are nearby. *Advantages:* It not only provides security, but efficient use of energy and bandwidth. While reducing the threat of wormhole, the network connectivity loss is minimum. *Limitations:* Each node requires additional hardware that is directional antenna.

5) Digital Investigation-based Approach: As presented in [40], an observation network that is virtually separate WSN is forms through observer nodes and base stations. The observers and the BS uses different frequency band than the sensor nodes. An observed network is built using high capacity sensor nodes. 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. The activity of observers is unnoticeable by sensor nodes. *Advantages:* All forms of wormhole attacks are detected because whole network is covered. *Limitations:* There are many chances of false positive such as (1) if some damage occurs with the node, the observer node may find it as malicious; (2) if the battery depletion occurs then the node can no longer send the data and might be detected as malicious; (3) the unobserved routing path may be detected as a tunnel.

C. Connectivity-based Approaches

1) Detection Using Local Connectivity Tests: In [41], to detect wormhole attack the network connectivity is examined. The author has proposed [α, β] ring connectivity test. The test starts with smaller values of α, β. For those nodes found to be suspicious, it performs some more tests with larger values. The attacker node reports incorrect connectivity information. The algorithm measures the hop distance between the wormholes connected nodes. The different sizes neighborhood is considered to check whether it will fall into multiple connected components. Once the malicious nodes are detected, the links that connect the nodes are removed. *Advantages:* (1) The algorithm is scalable to large network size. (2) It handles multiple wormhole attacks. (3) The cost for communication is low. The detection is accurate. *Limitations:* It has slightly more false alarms.

2) Detection-based on Forbidden Substructures: In the algorithm presented in [42] each node search a forbidden structure in its neighborhood. The forbidden parameter (f_k) is based on node distribution and communication model. Each node *x* finds its *2k*-hop neighbor list $N_{2k}(x)$. Node *x* finds the set of common *k*-hop neighbors with *y* and the maximal independent set of the sub-graph on common vertices with *y*. If the size of the maximal independent set is equal or larger than forbidden parameter (f_k), node *x* identifies that there is a wormhole attack in the network. *Advantages:* (1) It does not require any hardware or node's location information. (2) It has 100% detection accuracy and no false alarms. *Limitations:* For low density network, detection probability does decrease.

3) Detection-based on Neighbor Number Test & All Distances Test: Sensor nodes send their neighborhood details to the base station. After obtaining the received neighborhood details, the base station performs two detection mechanisms [43]: Neighbor Number Test (NNT) and All Distances Test (ADT). The idea behind NNT is that the number of neighbors of the malicious node is increased within its radius by creating fake links. The base station computes both the expected histogram of the neighbor numbers and the histogram of the real neighbor numbers in the graph and compares these two with the χ^2–test. If the calculated χ^2 number is larger than a predefined threshold value, then a wormhole attack is detected. Similarly, the χ^2–number is calculated for ADT. The idea behind ADT is that due to the wormhole the path becomes shorter in the network. *Advantages:* (1) No additional hardware is required. (2) If the radius of the wormhole is small, the ADT performs better than the NNT. (3) Both have very low false alarms. *Limitations:* The proposed approach detects the wormhole attack, but it does not pinpoint its location.

4) Detection-based on Topology Deviations: Based on the impacts on topology, the wormhole is classified into different categories [44]. The wormhole is located by finding the fundamental topology deviations and tracing the sources. Four types of wormholes have been presented, Class I, Class II, Class III and Class IV. For the first category wormhole, both the endpoints are located inside the surface. For the second category wormhole, one endpoint is located inside the surface and the other end point is on the boundary of the surface. For the third category wormhole, both the endpoints are on two different boundaries. For the fourth category wormhole, both the endpoints are on the same boundary. A finite combination of these is considered as a complex wormhole attack. By using homology and homotopy, how to characterize the global properties of wormholes from local information is discussed. Wormholes are located by detecting non-separating pairs. *Advantages:* It is based on network connectivity information and does not require any special hardware devices. *Limitations:* It cannot detect a candidate loop formed by a fourth category wormhole attack and any other topological approach.

5) Multi-Dimensional Scaling Visualization based Approach: In [45] the author has presented multi-dimensional scaling visualization based approach to detect wormhole attack in wireless sensor networks. To estimate the distance to its neighbors, sensor nodes use received signal strength. After receiving the distance information from all sensor nodes, the base station computes the network's physical topology. The network topology should be approximately flat if there is no wormhole in the network. 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. All sensor nodes are informed about the fake connections. *Advantages:* It does not require any special hardware. *Limitations:* In the experiments, the sensors are deployed on a flat plane. In the real environments, more complex conditions need to be considered.

6) MDS Based Detection Using Local Topology: In [46], the main focus is on abnormal structure created by wormhole attacks. After collecting neighborhood information using local connectivity information, an estimation distance matrix is created. Each node reconstructs the neighborhood sub graph using multidimensional scaling. If the distortion factor of the node exceeds than the threshold then the node is suspected as a wormhole. Finally the suspected nodes are filtered out using refinement process. *Advantages:* (1) The algorithm is applicable in practical wireless sensor network due to its extremely low overhead. (2) It produces very few false positives. (3) It does not require any additional hardware devices. *Limitations:* When both ends of two wormholes are very close to each other, nodes would be filtered during the refinement process and the proposed approach fails to detect the wormhole.

7) Passive and Real-Time Wormhole Detection Scheme: The approach presented in [47] is based on the observation that due to the wormhole attack, the path length reduces significantly. When any node A marks packet P, it registers its own source ID, hop and sequence number. When node A receives the next packet, it first search into its cache, found that sequence number is consistent, hop count and source ID are same then it will not mark the packet but only updates the hop and sequence number. All nodes mark the packet as per neighborhood proximity rule. If all nodes have mark the packet, then sink will receives the packet with empty mark ID field. If there is a presence of wormhole attack, then it will be filled. Sink node passively collects the network path information and performs detection. Based on marking information, the sink node reconstructs the topological diagram. For the marked packet, the parsing module will check the message authentication code. If it is modified then the parsing module generates an attacking report. *Advantages:* (1) Network overhead and computation is minimal. By adding the packet marking scheme, it modifies packet forwarding pattern. Detection and localization of wormhole is done only at the sink node, not on the resource constrained sensor nodes. (2) It is a real time approach and quickly finds the attackers. *Limitations:* It is probabilistic method. If the attackers attract less traffic, attack may not be detected.

8) Unit Disk Graph Model-based Approach: Most of the methods in the literature initiate wormhole detection after observing packet loss. The algorithm proposed in [48] finds those route requests that traverse through a wormhole and do not allow such routes to be established. The nodes monitor the two hop sub path on a received route request. A route request that traverses through a wormhole can be detected at the neighbors of a wormhole. The path is considered without tunnel if for each sub-path of length 2R (R is the transmission range of a node) there exists an alternate sub-path of maximum length 4R. Every node keeps a neighborhood relation in their two hop range. The node compares the two hop address present in route request packet with the existing routing entries. If there is a match found then it is updated with better metric. If there is no match found, then node compares it with three and four hop address. A new entry is created if any comparisons do not match.

Advantages: (1) Both hidden and byzantine wormholes are prevented. (2) It does not require any extra hardware or any computational cryptographic mechanisms.

Limitations: (1) Minimum average node degree required is 3. For a node degree of 3, the percentage of false positives is high. (2) For a lower density values, the amount of false positives is high.

D. Radio Fingerprinting Approach

In [49] the author has proposed radio fingerprinting approach to detect wormhole attack in wireless sensor networks. The reference fingerprints of all the genuine nodes are known by the central authority. The keys of all genuine nodes are known by the central authority to verify the integrity of the message.

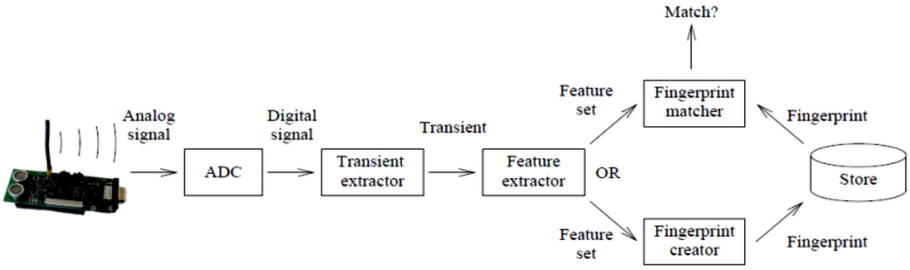

Fig. 6 Radio Fingerprinting Process

As shown in fig. 6, the fingerprinting device receives the radio signal and it is converted to its digital form. The signal transients are located. The extracted features forms a fingerprint and that can be used for device identification.

Advantages: A receiver can identify origins of messages even if contents of the message and device IDs are hidden.

Limitations: (1) The assumption that the fingerprinting device is able to separate the signals from the different nodes will not always true. (2) The signal characteristics will be altered if the malicious node transmits a weak jamming signal.

E. Localization-based Approaches

1) Graph Theoretic Framework Approach: The author has presented a graph theoretic framework for modeling wormhole links [50]. Only a subset of nodes that is location aware is referred to as guards and they can help other nodes to establish neighbor relation. A wormhole attack is present in the network if there exists at least one edge e (x, y) such that e (x, y) = 1 for || x – y || > r, where r represents the communication range. A communication graph should be constructed to prevent the wormhole in which no link longer than r exists. To prevent wormhole, the author has proposed a cryptographic mechanism based on local broadcast keys. When the location of all the nodes is known then a centralized method for establishing local broadcast keys is used. A decentralized mechanism for local broadcast keys establishment successfully defends against wormhole.

Advantages: (1) It does not need any time synchronization. (2) It is computationally efficient because it is based on symmetric cryptography. (3) It has a small communication overhead because each node needs to broadcast only a small number of messages.

Limitations: Guard nodes are assigned special network operations.

2) Mobile Beacon-based Detection: The detection scheme presented in [51] is based on mobile beacon. It accurately localizes the attackers and eliminates them out of the network. If the communication properties are violated between mobile and static beacon then it finds the intersection point of the chords' perpendicular bisector. The malicious node can be localized as the center of its communication disk. The mobile beacon moves in the networks to communicate with the static beacons. When the mobile beacon stops, a request message is broadcasted to its neighboring static beacons. When the static beacons receive the message, they will reply with its ID and coordinate. 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. Otherwise it calculates the Euclidean distance between itself and each of them. If the distance is larger than the communication range, then wormhole attack is detected. Simulation results show that it can obtain high detection probability.

Advantage: It has high detection probability and accuracy for localizing the attackers.

Limitations: The basic positioning scheme is energy consuming.

3) Location-Based Compromise-Tolerant Security Approach: In [52] the author has proposed the concept of location based keys. In this method, each node has a private key bound to both its ID and location. A node to node neighborhood authentication protocol that is based on location based keys is proposed. Location based keys can act as efficient countermeasures against wormhole attack. Each node accepts another node as a genuine neighbor if that node is within its communication range and it has the corresponding location based keys. Authentication process is denied from the nodes that are not physically within the communication range, so wormhole attack can be prevented.

Advantages: It has low computation and communication overhead. It requires low memory.

Limitations: (1) It is assumed that sink node is trustworthy and unassailable. (2) Range based localization requires a group of mobile robots having GPS capabilities.

4) Secure Localization and Key Distribution Approach: In [53], communication keys to prevent wormhole attacks are efficiently distributed to sensor nodes. As per the distance bounding rule, two sensor nodes can share a communication key only if they are physical neighbors. Sensor nodes located beyond the communication ranges do not share a communication key. If any node receives a message via wormhole link from a distance node, it cannot process it and the message will be dropped because the node does not have a shared key to decrypt it. While determining the communication key set, priorities are given to the communication keys shared by close neighbors. The chances of shared communication keys between two nodes located far away are very less. So the number of wormhole links is very less.

Advantages: (1) It is practical, low cost and requires minimal human interaction during the deployment. (2) It is scalable for large scale WSN deployments.

Limitations: It is assumed that master node will not be compromised by any attack.

5 Secure Range-independent Localization Approach (SeRLoc): Secure Range-independent Localization scheme (*SeRLoc*) is proposed in [54]. Each sensor node calculates their location based on beacon information transmitted by the locators. It is distributed and range independent localization scheme. Each locator transmits different beacons. If sector uniqueness property and transmission range violation property are satisfied, then wormhole attack is detected. For this purpose directional antenna is used. If the sensor hears two messages authenticated with the same hash value or it hear two locators more than 2R apart, then wormhole attack is detected, where R is the communication range of a node.

Advantages: It gives higher accuracy and requiring fewer reference points with lower communication cost.

Limitations: (1) It is unable to detect wormhole attacks when anchor nodes are compromised, especially nodes located near the end of a wormhole. (2) It does not distinguish the duplex and simplex wormhole attack.

6) High-resolution Range-independent Localization Approach (HiRLoc): High-resolution range-independent localization approach (HiRLoc) is proposed in [55]. It is an improvement over the scheme presented in [54] by utilizing antenna rotations and multiple transmit power levels. To increase the localization accuracy, it provides more information. Sensors calculate their location based on the intersection of the areas covered by the beacons which is transmitted by multiple reference points. All sensors can determine their location with high resolution without increasing the number of reference points. Range measurements are not required to estimate the sensors' location.

Advantages: (1) The communication cost is lower because fewer locators are required to get the desired localization accuracy. (2) The robust location computation is possible in the presence of security threats.

Limitations: If any malicious entity selectively jams transmissions of locators, then it is able to displace sensors. It is vulnerable to jamming attack.

V. Future Research Direction

Existing wormhole detection methods are imperfect. Under a large scale wormhole attack, a sensor node will have a lot of false neighbors. Many false neighbors lead to disturbance in routing. Some more efforts are needed in this direction to find the accurate neighbor and preventing the wormhole attacks. Majority of the wormhole detection techniques require additional hardware and it increases the cost of a sensor node. The software based solutions have some special assumptions. Another research direction is to propose a secure routing protocol against wormhole attacks in multi rate transmission approach without assuming data rates between links. Most of the distance-bounding and time-based techniques assume that time or distance data used for attack detection cannot be altered. Unauthorized nodes can change these data. So these techniques must be supported by cryptographic authentication techniques. Another good research area is the integration of trust-based systems with time or distance-bounding attack detection techniques. If malicious nodes alter the time or distance data then trust module is used to detect it.

In a dynamic wireless sensor networks, two genuine nodes that were far away can become one hop neighbors. In such situation base station identify the presence of a wormhole attack. Differentiating such genuine nodes from the malicious nodes is a challenging task. The scenario becomes very complicated when multiple attackers attack simultaneously on the sensor nodes. Detection and localization of multiple wormhole attack is another research area.

VI. Conclusion

In this paper we have reviewed the state-of-the-art schemes for detection of tunneling also called wormhole attack. Existing schemes are good for detecting and preventing wormhole attacks, but they also have drawbacks. After developing many prevention techniques wireless sensor network is still vulnerable to wormhole attack. The literature study indicates that there are still a lot of challenges in wormhole attack detection problem and also becomes accepted by the resource constrained sensor node. Finally, by analyzing advantages and limitations of the existing techniques, we have discussed the open research challenges in the wormhole detection area.

References

[1] 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.

[2] S. Tilak, N.B. Abu –Ghazaleh and W.B. Heinzelman, "A taxonomy of wireless micro-Sensor network models," ACM Mobile Computing and Communications Review, vol. 6, no. 2, 2002

[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] K. Romer and F. Mattern; "The design space of wireless sensor networks," IEEE Wireless Communications, vol. 11, no. 6, pp. 54–61, Dec. 2004.

[5] 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.

[6] Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal; "Wireless sensor network survey," Journal of Computer Networks Elsevier, pp.2292-2330, April-2008.

[7] Qiuwei Yang, Xiaogang Zhu, Hongjuan Fu, Xiqiang Che; "Survey of Security Technologies on Wireless Sensor Networks," Journal of Sensors, volume 2015, Article ID 842392, 9 pages.

[8] Murat Dener; "Security Analysis in Wireless Sensor Networks," International Journal of Distributed Sensor Networks, volume 2014, Article ID 303501, 9 pages

[9] Sergio Saponara, Agusti Solanas, Gildas Avoine and Bruno Neri; "Privacy and Security in Wireless Sensor networks: Protocols, Algorithms and Efficient Architectures," Journal of Computer Networks and Communications, volume 2013, Article ID 528750, 3 pages.

[10] Wang,Yong, Attebury, Garhan and Ramamurthy, Byrav; "A Survey of security issues in wireless sensor networks" IEEE Communications Surveys and Tutorials, 2006.

[11] Chen, Xiangqian, et al.; "Sensor network security: A survey" IEEE Communications surveys & tutorials, vol. 11, pp. 52-73, 2009.

[12] 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.

[13] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in ACM Workshop on Wireless Security (WiSe 2003), September 2003.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] J. Eriksson, S. Krishnamurthy, and M. Faloutsos, "Truelink: A practical countermeasure to the wormhole attack," in ICNP, pp. 75-84, 2006.

[19] Yang Xiao, Xuemin Shen and Ding Zhu Du, "Wireless Network Security" Signal and Communication Technology, Springer, 2007, ISBN: 978-0-387-28040-0.

[20] D.B. Johnson, D.A. Maltz and J. Broch, "The dynamic source routing protocol for multihop wireless ad hoc networks", in: Ad Hoc Networking, (Addison-Wesley, 2001), ch. 5, pp. 139–172.

[21] C.E. Perkins and E.M. Royer; "Ad-hoc on-demand distance vector routing" Proceedings of WMCSA (Feb. 1999) pp. 90–100.

[22] Khabbazian, Mercier, Bhargava; "Wormhole attacks in wireless Adhoc networks: Analysis and Countermeasures" Global Telecommunications Conference, 2006, IEEE GLOBECOM'06

[23] 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.

[24] 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.

[25] 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.

[26] Gu-Hsin Lai; "Detection of wormhole attacks on IPv6 mobility-based wireless sensor network" EURASIP Journal on Wireless Communications and Networking 2016

[27] 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.

[28] 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.

[29] Reza Shokri, Marcin Poturalski, "A Practical Secure Neighbor Verification Protocol for Wireless Sensor Networks" ACM, WiSec'09, March 16-18, 2009, Zurich, Switzerland.

[30] 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.

[31] Mehdi Sookhak, Adnan Akhundzada, Alireza Sookhak, Mohammadreza Eslaminejad, Abdullah Gani, Muhammad Khurram Khan, Xiong Li, Xiaomin Wang; "Geographic Wormhole Detection in Wireless Sensor Networks" Journal of PLOS ONE, January 20, 2015, DOI: 10.1371/journal.pone.0115324

[32] 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.

[33] Hon Sun Chiu, King –Shan Lui; "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks" 1st IEEE International Symposium on Wireless Pervasive Computing, 2006

[34] 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.

[35] Rupinder Singh, Jatinder Singh, and Ravinder Singh; "WRHT: A Hybrid Technique for Detection of Wormhole Attack in Wireless Sensor Networks" Journal of Mobile Information Systems, Hindawi Publishing Corporation, Volume 2016, Article ID 8354930, 13 pages

[36] 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.

[37] 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.

[38] Sanjay Madria, Jian Yin; "SeRWA : A secure routing protocol against wormhole attacks in sensor networks" Journal of Ad Hoc Networks, September 2008.

[39] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks" in Network and Distributed System Security Symposium (NDSS), pp. 131–141, 2004.

[40] 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.

[41] Xiaomeng Ban, Rik Sarkar, Jie Gao, "Local Connectivity Tests to Identify Wormholes in Wireless Networks" ACM, MobiHoc'11, May 16-20, 2011, Paris, France.

[42] Ritesh Maheshwari, Jie Gao and Samir R Das; "Detecting wormhole attacks in wireless networks using connectivity information" IEEE INFOCOM, 2007.

[43] Levente Buttyan, Laszlo Dora, and Istvan Vajda; "Statistical wormhole detection in sensor networks" SAS 2005, Springer, pp. 128–141.

[44] 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.

[45] 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.

[46] Xiaopei Lu, Dezun Dong and Xiangke Liao; "MDS-Based Wormhole Detection using Local Topology in Wireless Sensor networks" International Journal of Distributed Sensor networks, Volume 2012, Article ID 145702, 9 pages.

[47] Li Lu, Muhammad Jawad Hussain, Guoxing Luo, Zhigang Han; "Pworm: passive and Real-Time Wormhole Detection Scheme for WSNs" International Journal of Distributed Sensor networks, Volume 2015, Article ID 356382, 16 pages

[48] Rakesh Matam, Somanath Tripathy, "WRSR: wormhole-resistant secure routing for wireless mesh networks" Springer, EURASIP Journal on Wireless Communications and Networking 2013.

[49] K.B. Rasmussen and S. Capkun; "Implications of radio fingerprinting on the security of sensor networks" Third International Conference on Security and Privacy in Communication Networks and the Workshops, pp. 331-340, Sep. 2007.

[50] 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.

[51] 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.

[52] 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.

[53] 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.

[54] L. Lazos and R. Poovendran, "SeRLoc: Robust Localization for Wireless Sensor Networks," ACM Transactions on Sensor Networks, pp. 73–100, 2005.

[55] 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.