Survey of wormhole attack in wireless sensor networks

Umashankar Ghugar, Jayaram Pradhan
Department of Computer Science, Berhampur University, Brahmapur, Odisha 760007, India

Article Info

Article history:

Received May 12, 2020
Revised Jul 2, 2020
Accepted Jul 29, 2020

Keywords:

IDS
MANET
Sensor node
Wormhole attacks
WSN

ABSTRACT

From the last decade, a wireless sensor network (WSN) has a very important role over the networks. The primary features of WSN include satellite communication, broadcast channel, hostile environment, medical system and data gathering. There are a lot of attacks available in WSN. In wormhole attack scenario is brutal from other attacks, which is smoothly resolved in networks but tough to observe. This survey paper is an experiment to observing threats and also focuses on some different method to identify the wormhole attacks.

Corresponding Author:

Umashankar Ghugar
Department of Computer Science
Berhampur University
Brahmapur, Odisha 760007, India
Email: ughugar@gmail.com

1. INTRODUCTION

Wireless sensor network (WSN) built a network, which is a spread, automatic governing network and it corresponding with several sensor nodes in specific environment. Nodes are observed by the natural conditions, such as humidity, compression, heat, wave and direction at different areas [1]. It is a tiny device which has a limited measurement resource. They are gradually arranged in a wireless sensor environment [2]. WSN are broadly utilized on different applications such as, area observing, defense surveillance, health care system, home affirmation and satellite communication.WSN suffers from various security issue because usually it is deployed in hazardous environment. Sensor node has some limitation such as limited lifetime, less computing capability and low memory space [3, 4]. Based on these limitations, they are arranged in noisy environment, it is highly affected and sensitive to several types of attacks [5]. Basically, sensor nodes are category by four sub-systems [6-13, 14]. Processor and memory, transceiver, sensor and battery. Here we have discussed the several types of attacks.Mainly attacks are classified by two parts. First part is the attack against security mechanism and another is routing mechanism. Numbers of attacks are listed as below but we are focuses on wormhole attack.

- Wormhole Attack
- Sybil Attack
- Blackhole Attack
- Hello flood Attack
- Sinkhole Attack
- Denial of Service

Thus, these survey papers basically focus on various approaches to detect wormhole attacks. In Section 2 discussed the intrusion detection system in WSN; In Section 3 discussed the wormhole attack in wireless sensor networks; In Section 4 discussed various detection approaches of the wormhole attack in wireless sensor networks with summary. Finally in Section 5, we have discussed the future research challenges and conclusion.

2. INTRUSION DETECTION SYSTEMS

An intrusion detection system (IDS) is used for observing the network diagnosis against nasty movements and informed to the base stations. Mainly it is divided by two types: misuse IDS and anomaly IDS. Misuse IDS In this system, the abnormal pattern is calculated and contrast with the previous data [5]. Signal's energy is used to detect the malicious node, where if the energy is collision with the actual positions then the message transmission is considered as doubtful [6]. Anomaly IDS- It is detected by protocol, where prevention method is used before the detection stage. Here protocols are activated on the data with respect to the network performance. When the data is satisfying the rule then it is called as normal node else malicious node. When the intruder is detected, then informs to the system [7, 8]. In routing ,various multipath routing technique is used for best redundancy path with high energy efficiency efficiency [9]. Watchdog technique is a detection technique, where each node can observers their neighboring nodes within the radio range [10].

3. WORMHOLE ATTACK

The wormhole attacks are most brutal in nature. Generally, more than two malicious nodes create a secrete route is called tunnel. Here the attackers are built a connection to each node, so that they can communicate at a high speed over the networks with other nodes. A wormhole attacks can be freely carried out across routing in the sensor networks. Routing protocols has no mechanism to prevent against it [11]. In other words, when the wormhole attacks occurs, it dropping all the packets and cause network interruption. Wormhole attack is also used in the form of merging of selective forward and Sybil attack [12]. In Figure 1, the data packet accepted Node D from Node A and vice versa.

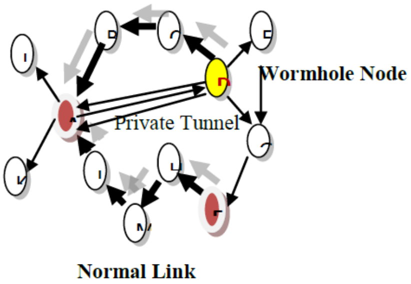

Figure 1. Wormhole attack in WSN

3.1. Types of wormhole attack

Here, we have categories the wormhole attack established on the several techniques. Numbers of nodes are participating for establishing the method for wormhole into following types [15].

- Using packet encapsulation: The number of data packet and node are encapsulated between two nasty nodes.
- Using out-of-band channel: Only single nasty node is occurring with the high speed of communication scope.
- Using packet relay: The nasty node gives replays to all data packets between the two communicated nodes. Finally, the duplicate node is created by nasty node.
- Using protocol distortion: Single nasty node is tries for cracking the attack, which is attack by the routing protocol.

3.2. Routing protocols for wormhole attack

Most of the routing protocols are used in WSN.The routing protocols are categories into: Proactive and Reactive [16]. AODV, Secure-AODV and DSR are proactive routing protocols where as DSDV, OLSR, OSPF are Reactive routing protocols.

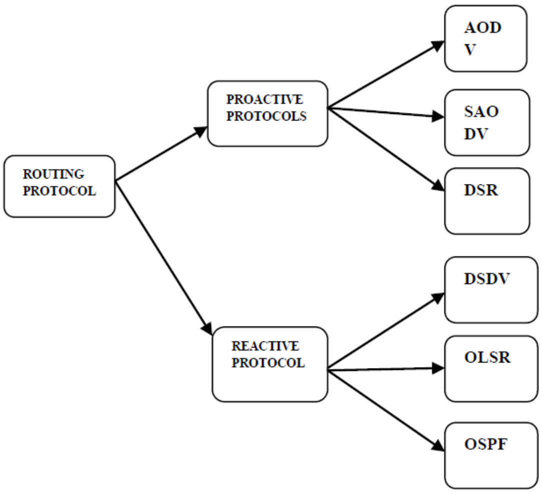

Figure 2. Routing Protocols

3.2.1 Aodv routing protocol

The AODV stand for ad-hoc on-demand distance vector. Its is a mostly used protocol and called as dynamic reactive routing protocol [17-18], that create a self route on call support. When a sender node sends a data packet to destination node, it must take the help of routing table. If the node gain recent paths then the data packet are forwarded to destination else it uses the route discovery process. In AODV protocol, two control message is used by route discovery process *i.e* route request (RREQ) and Route Reply (RREP). To obtain the recent path, RREQ and RREP control messages are used. When the route discovery process is over, than the data packet of source and destination node can be connected.

3.2.2 Saodv routing protocol

AODV protocol on extension leads to SAODV protocol [19]. This has a greater utility in the security to protect the route discovery mechanism. From desirable asymmetric cryptosystem, each node has a couple of signature key and it is ability to verify the assumption between given address and public key of the same node. So SAODV has the task of key management scheme [20].

3.2.3 Dynamic source routing protocol (DSR)

DSR protocol is use to update the cache memory of route by route discovery process. It updates the information about all links between the sender and receiver node. In order to transmit data, a well defined route is taken into account by the route discovery process for node. This motive is achieved by route discovery process and route maintenance process.

Route Discovery process: When a sender node forward a data to another node over network, it has to go through its route cache. In case of unavailability of routes between the receiver and sender than route is discarded and it broadcast RREP (Route Reply).When the receiver node or any intermediate node has received the fresh path from the sender node, then RREP (Route Reply) is generated[21].

Route Maintenance Process: With the initiation of data transmission process, it is the task of sender node to confirm that very next hop received both the data and transmit the route to receiver. In case sender didn’t get a confirmation message than it generates route error message. After that the hop again starts the route discovery process.

3.2.4 Destination sequenced distance vector routing protocol (DSDV)

As per the theory of Bellman algorithm, it is a table driven routing program. Here the authors describe the concept of routing loop problem using their algorithm. In this algorithm routing table store the sequence number. Basically the sequence number is used even number for the active network and odd number for inactivate network. When the routing information circulated among inactive node, at that time occurs more sending troubles [22].

3.2.5 Optimized link state routing protocol (OLSR)

It is a proactive routing protocol and used for IP routing [23].Basically it is compatibility with mobile ad hoc networks and ad hoc networks. To identify and set up the transmission link over network then it must used hello and control message of topology. In OLSR, each node is calculating the next hop destination using shortest forwarding path.

3.2.6 Open shortest path first

It is used to find the least –cost path from a source node to a destination node within a group of nodes. As shown in Figure 3, a group of routers using the same routing protocol for all introduced to an autonomous system (AS).Upon joining the AS, a node uses the hello protocol to discover neighboring nodes. Then it forms adjacencies with its new neighbors to exchange routing information [24] .Above all, it is faulty for every node on a network connect to all other node of the network. To prevent this situation, a node is considered as the destination node. It is considered to be neighboring node of each node over network and communicate the information between them.

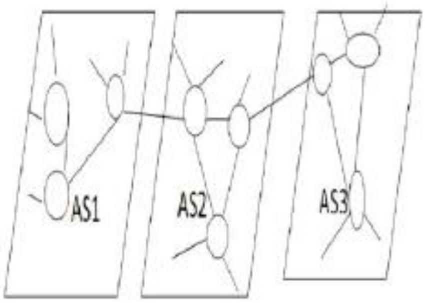

Figure 3. Connected autonomous system (ASS)

A backup node, which is always maintain update records for successful transaction so that if the primary designated node crash can be replaced immediately. At the time of regular process, each node repeatedly floods updated messages to neighboring nodes of every node. This message indicates its status and provides the cost for topological database. When flooding message are proved acknowledgement that means system is reliable. A node can check whether the incoming link is older or newer using sequence number. When the cost is change then it sends all these messages. Database Messages provide the sequence number for the entire channel, which is held by sender. When the value is comparing with the sender, then receiver can resolve the most current values. When a line is delivering then this message is fully used in the system as the result of this algorithm is that each pair of neighboring nodes detects the most recent data and new information is transmitted on this way [25, 26].

4. DETECTION APPROACHES OF THE WORMHOLE ATTACK

We have discussed the different technique of intrusion detection system for wormholes attack and categorized the different technique in ascending order from year 2013 to 2016. In [27], a wise solution is prescribed to eradicated wormhole attacks for ad-hoc network by providing directional antenna to the nodes. Node uses the definite regions of their antenna in establishing connection among them. Each pair of node has evaluated the direction of receiving the information from either. Hence relation between consecutive neighbors is established only if the direction of information flow of both the nodes is in arrangement with one another. This additional information enable wormhole discovery and introduces the network fluctuation. So that it can be smoothly spot. In [28], the authors' proposed a more simple tool known as "Packet leashes" accordance with the recognition of geographical and temporal leashes. The information provided to the packets that controls the transmission distance called Leach. The distance of sender and the receiver is specified by the geographical leash. When the receiving nodes accept the data packets, it calculates the distance and time of the transmission. The receiver analyze now on comparing this information can detect whether the packet has forwarded through wormhole attacks or not. Here the packet limitation is known by temporal leashes, which is determining the distance it can cover the most. In this technique the position of node is not that important rather than time factor plays an important role. It can access the time calculation and its comparison up to an order of nanosecond. On each packet, the sender mention an authorized time bar, which is compared by the receiver and the packet forwarding distance is simply given by the product of velocity of lights and transmission time. In case of a large time difference it indicates the presence of wormhole. In [29], the authors put forward a "graph theoretical" approach to prevent wormhole attacks. This concept is purely established on the "location aware guard node" (LAGNs).When the key establishment process is used for detecting wormhole attack and it also used the decoded message. If same message is heard from one guard or two LAGNs are heard from different far away LAGNs then wormhole is detected.

In [30], the authors proposed that wormhole attacks in stationary sensor network are investigated using network visualization. In this method, the signal strength determines the distance. Each sensor conveys all the gathered information to the main station. The controller computes the networks physical topology using sensor predicted distance. If a wormhole attack is present then it is seen that a string pulling the network terminals, if not then the topology is flat. In [31], the authors adopted lightweight countermeasure for wormhole attack called LITEWORP and this result has advantages of very quick detection of wormhole attacks and the loss of fraction of packets is very less. In [32], here the author's emphasis on the "round –trip travel time" (RTT) message, which provides the maximum times require for the transmission. When this time is multiplied with speed of lights it gives the distanced travelled. Now this distance is to be compared with the predicted distance. If there is a large difference then it threat wormhole attacks. In [33], the authors describe that, wormhole attacks in found in multipath routing. In case of new root requirements source excess by using route request (RREQ) in the network and then the response is waited. The intermediate node only pass away this route request (RREQ).On the same time the receiver will wait to get route after getting route request (RREQ).Statistical Analysis of Multi-path (SAM) is introduced, that use Pmax and .which are higher if wormhole attack is present.Pmax gives the probability of the routes out of all possible route and (theta) is the difference between top two frequently papered links. If a wormholes attack is more than PMF (probability mass function) then it gives high frequency. Here authors also analysis the multipath routing and DSR with fine comparisons.

In [34] a "hello control message" is used to detect wormhole attacks as consent with OLSR in particular. He used the aggregate of hello message time interval (HMTI) that lie within a jitter. A ranger= [T-α, T+∞] is coated. In range HMTI are considered valid or else it is out of set of rules. In case of unusual HMTI secondary checks are done. In addition to this an untrue positive alarm in negated in case of weak working node which has many packets but this is not the case of and attacking node. In [35], the authors implemented delay per hop indication (DelPHI) to detect wormhole attacks. It is also work on the same principle of comparison of path time distance and predicted distance. This process works in two phases, first is collection of route path by the receivers and senders include a DREQ packets similar to the concept of SAM and sign it before sending. On the getting the packet the receiver has to add its ID and 1 hop count is incremented. The minimum delay and hope count information are utilized for the minimum detection. In the second phase, "round –trip travel time" (RTT) is used to calculate the time difference between the total number of sent information and acknowledgement received. In this process the delay per hop value (DPH) is calculated as RTT/2h, where h is the hop count to the definite consecutive. In normal case tiny hops have tiny RTT where as in case of wormhole attack the tiny hops are giant RTT. If one delay per hop value (DPH) crosses the threshold value then all paths next to this treated as under wormholes attacks In [36], the authors used a unique technique of radio finger printing. It initiates with the radio signal receiving by the fingerprinting device and then the signal is converted to the digital form. The signal passing is positioned and its characteristics are described. A set of characters from fingerprints is later used for apparatus identification. In [37], the authors proposed a method, when a sender send a RREQ message to receiver, then it waits for the RREP. Out of the number of RREP received by the source, the RREP with highest frequency is compare with the predefined value. If the packet drop ratio is larger than packet sent ration then it implies that wormhole is present. In [38], the authors proposed that, two plot nodes are connected by tunnel such as they are neighbors.

The route request (RREQ) and topology control messages (TCM) are convey among these plot nodes through tunnels. By using the extra tunnel nodes, these nodes have the shortest path. After the link is establishing, the attacker select one another as multipoint relays (MRPs). As result few topologies control messages and data packets are leaked through the tunnel. As consequence false topology information is spread through the networks. In [39], the author's proposed a trust based model for detection in wireless sensor networks. In trust based system, each node has some values, which is called trust value. By using this trust values the source node is calculated the actual route to the destination. When the transmission occurs over network, in which number of packets drop ratio is high means trust value is less and wormhole attacks is present in the network. If the trust value is high means, all the packets which is received by the destination, it indicates that the trust value is high on the neighboring node of source node between the source to destination. In [40], the author's proposed a distributed intelligent agent-based system. Here the ambition is the use of generalized intrusion detection system (IDS) framework which is so lightweight that it can run on the sensors node and it identifies the wormhole attacks along with its attackers. When that attacker's node is found in the network, then it is informed with an indication message. After that each node makes their conclusion on the base of consecutive node repeat. In [41], it is assumed that behaviors of a node are control by its consecutive nodes. A node uses its neighbor node to send route request (RREQ) message to the destination node. If the sender didn't get route reply (RREP) message within predicted time, then sender conclude the presence of wormholes attack and enclose this route in the list of wormhole attacks list. A conjugative node that is managed by every node that consists of RREQ sequence number, Neighbors node ID, sending & receiving time of RREQ.The maximum time limit equal to WPT/2 is waited by the sender if RREQ is delayed more than thus it indicates the wormhole attacks and entirely it doesn't support DSR Routing protocol.

In [42], Al the sender's nodes wait for acknowledgment (ACK) message. If ACK message is not received then the next node is attack, which is wormhole attacks. ACK message should not retrace the path and sent between the separation by two hops. Now Time to Live (TTL) plays a great role since the path is different. If the ACK message is not received within TTL then wormhole attacks is detected. In [43], the authors used two step mechanism for the detecting the wormhole attacks. The first steps consist of two methods. In the first method, the node and his next node are identified by using round-trip-time (RTT) and in the second method their list is made and if the destination node is not in that list then it is doubt full in nature. In the second step mechanism, after detection of doubt full link the attack is concluded using RTS/CTS method. In [44], the authors used AODV and DSR routing protocol. Here also a Trust based security model is used for detecting intrusion. This model has been introduced to identify the attacks, which is called statically method. If any connection gets doubtful, then the trust value is calculated to determine the wormhole attacks. In the trust model, nodes monitored their neighbouring on the basis of packet drop pattern. If any node is found to be doubt then stock trust is identified by the node, whether the node is affected by wormhole attack or not. In [45], the authors proposed Digital investigation to detect wormhole attacks in WSNs. WSN are explained that add generation and protects flow of evidences about sensors node characteristics in the network. A group of detective nodes are spread over the networks to controls the topology and datagram passing by sensor nodes. Observation node and base station node jointly forms different WSN networks called observation network. Frequency bands are used to establish link between observers and the base station but this is not supported by sensors node. The detection sensitivity of sensor node is less than the observer. In [46], the authors proposed a 'conflicting-set' for each node is made to filtering the false measurement of distance but its biggest limitation was that, it works only where there is no packet loss but when attackers attacks then the Packet drops is certain to happen. So the system is under a wormhole attacks.

In [47], the authors proposed a model, which create a cluster using no of nodes in MANET. In this paper various data structure are explained and algorithm is also proposed. Here two layers are mention in the cluster, where one node is treated as cluster head among several nodes. When a node is affected by a wormhole attack in the layer1, then which informs to the cluster head of layer1.After that cluster head of layer1 will indicates the cluster head of layer2 about the abnormal node. So that cluster head of layer2 indicate the message to all the cluster head of layer1, then the cluster head of layer1 inform the messages to their respective node within their cluster. In [48], the authors proposed localization-based systems, which are vulnerable to wormhole attacks as they manipulate the localization method To prevent the wormhole attack, a 'distance-consistency-based secure location' scheme was implemented, This works on the detection, exact location and trapping of wormhole attacks In [49], the authors used techniques that identify the wormhole attacks. In the first way algorithm uses hop counting method, rebuilt local maps at every nodes and then a diameter features to identify by the problems due to wormhole attacks. The evaluated round trip times (RTT) between the consecutive nodes are used to compare in the second way. Its major advantages is not required additional hardware and consume less energy. In [50], the authors proposed that attackers may record the location of packets in WSN and send them to one more location and again transmit them in to the network. When it found the roots, the wormhole detection process is going on, which counts difference between the neighbour nodes to another node? If the difference is more than the destination node detect the wormholes. In [51], the authors proposed the statistical analysis to identify the wormhole attacks in WSN.The proposed algorithm is categories by three parts.i.e.

- Statistical analysis method, which is used for routing information for detecting the wormhole attacks.
- Determination of the vulnerable wormholes.
- Time constraints is used for validation in wormhole attacks.

It uses multi-path routing, time constraints and statistical analysis to verify the vulnerable connection. It doesn't need time synchronisation, directional antenna and GPS. In this method it can wormhole attacks with high quality of accuracy. In [52], the authors propose the security emerges as a centrally in MANET. The applications of MANET were deployed in various fields. Wormhole attack is a severe destructive in nature, which is smoothly resolved in networks but tough to observe. It is visible even if the intruder has not negotiated at any situation and rest of all communication gives security, novelty, authenticity and confidently. In [53], the author's presents different types of sensor nodes and many layer wise attacks must be present in the network. Wormhole attacks are used in this paper in attack model, which is smoothly resolved in networks but tough to observe. Here the authors proposed a method, which is used the Mint route protocol. In [54], the authors address the multiple –hop Mobile ad hoc networks, where each node acts as a host and router in the route. Author proposed a technique, which is identify the attacks without using synchronization requirements. The basic thing is to find another way from source to next hop and finally it calculates the no of hops for detecting wormholes attacks. In [55], it uses packet encapsulation technique. Here packets are encapsulated in AODV protocol. In this technique, less hop count is created and it is compared to other normal links. MLDW maintain a big structure, which is divided by 04 parts, *i.e:*

- Examination layer.
- Disclosure layer.
- Reorganization layer.
- Segregation layer.

Here the First 03 layers work as a Detector and last layer works as a Preventer for wormhole attacks in MANET using AODV protocol. In [56] ,the author's proposed a technique, which is gives secure data transmission using neighbour node analysis concept to identify the wormhole attacks in MANET. This technique analyze the neighbouring nodes .so that it checks the reliability of the nodes for data transmission on the network, According to this technique, a node send a request to its neighbour nodes and it maintain the request and response system. Here node maintains a table for tracing the time out. If a node doesn't get the reply time that means attacks occurs in the network. The entire node from source to destination is analyzed to detect the wormholes attack using AODV protocol in MANET. In [57], the authors propose a technique, which is liable to detect wormholes attacks in MANET using analysis of the misbehaving nodes concept. According to the authors, it concentrates on the detection of the abnormal nodes and prevention of the wormhole attacks. The route discovery process is used, which is a sender node want to data sending process with another node in the network, it has to go through its route cache. In case of unavailability of routes between the receiver and sender than route is discarded and it broadcast RREP. The RREP is generated, when the receiver node or any intermediate node has got the recent route to the receiver node. Another important is that DSR protocol is used to detect the nodes where the misbehaving nodes are simple discarded and not including into the routing table of DSR. In DSR, parameter is used for evaluating the network performance i.e jitter, throughput and delay. In [58], here the authors used a general mechanism, which is used without hardware. It explains the details about packet detection technique. That packet holds the information of localization and clock synchronization for detecting affected node in MANET. Detection Packet has four fields: total hop count, processing bit, count to reach next hop and timestamp .This fields are added to the header of detection packet. In [59], the authors proposed a normalized wormhole local intrusion detection algorithm, which is up gradation version of local intrusion detection routing security in MANET. In this technique an intermediate neighbor nodes are uses discovery mechanism process and packet drop calculator. Based on the isolation technique, at the time of transmission over the network, where each node received packet for the confirmed Wormhole nodes.

In [60], the authors proposed technique, which is based on Hash based compression function (HCF). It is basically used for secure hash function to calculate the value of hash field for route request (RREQ) passes over the networks. Here AODV routing protocol is used .As per the authors. Source node starts the route discovery process for searching the destination node. Then the source node compute the HCF and also compute the value of hash field with RREQ and it passes to his neighboring node. If the value of neighboring node is same to the value of destination node .At that situation the destination node receives the no of RREQ. Finally the destination node implement the HCF concept. Otherwise the others intermediate node between source to destination, they will implement HCF hash fields and passes to its next node. If the calculated hash value is compared to append hash value and gets the same result then the destination node send back RREP message to the source. Otherwise if calculate the hash value is not same with the append hash value then the destination node detects the RREQ and it treated as affected node by wormhole attackers.

In [61], the authors used a hybrid technique "wormhole resistant hybrid technique (WRHT)". It based on watchdog and Delhi Concept. It gives information about the packet drop and the delay per each hops and used for the full phase route process in wireless sensor network. Here the authors build up method which is used for wormhole detection in every sensor devices with low costs. WHRT is an extension version AODV routing protocol. The proposed method is to allow for calculating the wormhole presence probability (WPP) for a path in addition to hop count information in the source node over the sensor networks. During the route discovery process, per hop time delay probability (TDPH) and time delay probability (TDPP) is calculated for detecting wormhole attacks. In the next part of the WHRT, another parameter is calculated, which is called per hop packet loss probability (PLPP). The values of PLPP and TDPP are used for decision making ,whether a path P is affected by wormhole attacks or not. So that the routing protocol AODV is taking correct way for the transmission over the sensors networks. We presented several wormholes attacks in WSN.Finally, by evaluating the positive and negative aspects of all existing techniques, till date open research challenges studied are required for detection wormhole attacks. In Tables 1, the most important detection methods and requirements are elaborated in sequentially with respect to year.

Tables 1. The most important detection methods and requirements are elaborated in sequentially with respect to year

Researcher	Year	Method	Tools	Protocol	Requirements/Commentary
H. Lu, D. Evans [27]	2003	Directional Antenna	-	Directional neighbor discovery protocol	Directional antennas on each node with GPS
Y.C. Hu and D.B. Jhanson [28]	2003	Packet leashes and end-to-end	NS2	TIK protocol	GPS Coordinator and Loosely Synchronized clock.
L.lazos, R. Poovendram [29]	2004	Localization	-	-	Based on location aware ‘guard nodes’(LAGNs), not applicable to MANET
W. Wang and B. Bhargava [30]	2004	Network visualization	-	-	Centralized control, seems promising, works based on dense networks, mobility is not studied
Issa Khalil, Saurabh Bagchi, Ness B. Shroff [31]	2005	LITEWORP	NS2	Key management protocol	Applicable only in static networks,
A. Baruch, R. Curmola, C. Nita-Rotaru, D. Holmer, H. Rubens [32]	2005	Time of flight	NS2	ODSBR	Hardware enabling one-bit messages and immediate reply without CPU involvement
N. Song, L. Qian, X. Li. [33]	2005	Statistical Approaches	NS2	MR and DSR	Works only with multipath on demand protocol
H.S. Chiu and K. Lui [35]	2006	Delphi	NS2	AODV	Not considered
K.B. Rasmussen and S. Capkun, [36]	2007	Radio Fingerprinting	-	-	Fingerprinting Devices is needed.
Khin Sandar Win. [37]	2008	DAW	NS2	DSR, LF analysis	Delay Parameter
S. Choi, D. Kim, D. Lee, J. Jung [41]	2008	WAP	CBR	DSR	Maximum transmission distance is calculated
H. Vu, A. Kulkarni, K. Sarac, N. Mittal [43]	2008	WORMEROS	-	-	Time synchronization is required. Topological change is not considered
M.S. Sankaran, S. Poddar, P. Das, [44]	2009	SAW	-	AODV	Not considered
H. Chen, W. Lou, X. Sun, and Z. Wang [48]	2010	Secure localization	NS2		Conflicting the set-based resistance localization, Distributed detection system
Gupta S, Kar S, Dharmaraja [50]	2011	WHOP	NS2	WHOP, AODV	Not required any hard support and clock synchronization
C.P. vandana, A.F.S. Devraj [55]	2013	MLDW	NS2	AODV	Not required any specialized hard support and clock synchronization
R. singh, J, singh, Ravindar singh [61]	2016	WRHT	NS2	AODV	It based on the combination of two techniques, i.e. Watchdog and Delphi.

5. CONCLUSION

Wormhole attacks in WSNs are one of the brutal attacks that can be implemented easily in sensors networks. In this paper numbers of methodologies is discussed for detecting wormhole attack. However, it is not less information. Therefore we believe that the analysis on this paper is helping us for developing the new method to detect wormhole.

REFERENCES

[1] M. Tiwari, K. Veer Arya, R. Choudhari, K. Sidharth Choudhary. “Designing Intrusion Detection to Detect Black hole and Selective Forwarding Attack in WSN based on local Information.” *Fourth International Conference on Computer Sciences and Convergence Information Technology*” 2009.

[2] E. Nam Huh and T. Hong Hai. “Lightweight Intrusion Detection for Wireless Sensor Networks” iTech.2011.

[3] J. Du, J. Li, “A Study of Security Routing Protocol for Wireless Sensor Network.” *International Conference on Instrumentation, Measurement, Computer, Communication and Control*, 2011.

[4] F. Bao, I. Ray Chen, M. Jeong Chang, and J.-Hee Cho. “Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection.” *IEEE Transactions on Network and Service Management*, vol. 9, no. 2, pp. 169-183, June 2012.

[5] M. A. Rassam, M.A. Maarof and A. Zainal. “A Survey of Intrusion Detection Schemes in Wireless Sensor Networks.” American Journal of Applied Sciences, vol. 9, no. 10, pp. 1636-1652, January 2012.

[6] W. Ribeiro Pires J´unior, T. H. de Paula Figueiredo H. Chi Wong, A. A.F. Loureiro. “Malicious Node Detection in Wireless Sensor Networks.” Proceedings of the *18th International Parallel and Distributed Processing Symposium (IPDPS’04), IEEE*, 2004.

[7] V. K. Jatav, M. Tripathi, M S Gaur and V. Laxmi. “Wireless Sensor Networks: Attack Models and Detection.” *IACSIT Hong Kong Conferences IPCSIT, IACSIT Press*, Singapore, vol. 3, 2012.

A. Paula R. da Silva, M.H.T. Martins Bruno, P.S. Rocha, A. A.F. Loureiro, L. B. Ruiz, H. Chi Wong. “Decentralized intrusion detection in wireless sensor networks.” Proceedings of the *1st ACM International Workshop on Quality of Service and Security in Wireless and Mobile Networks*, 2005.

[8] G. Saravanan, P. R. Patil, M.R. Kumar. “Survey on Intrusion Detection System in Heterogeneous WSN Using Multipath Routing.” *IOSR Journal of Computer Engineering (IOSR-JCE)*, vol. 16, no. 2, pp. 26-31, 2014.

[9] U Ghugar, J Pradhan, M Biswal. “A Novel Intrusion Detection System for Detecting Black Hole Attacks in Wireless Sensor Network using AODV Protocol.” *IJCSN International Journal of Computer Science and Network*, vol. 5, no. 4, August 2016.

[10] Y. Sabri, N. El Kamoun. “GRPW-MuS-s: A Secure Enhanced Trust Aware Routing against Wormhole Attacks in Wireless Sensor Networks.” *Communications on Applied Electronics (CAE)*, pp. 2394–4714, 2016.

[11] Singh, M., Das, R. Sahoo. “A Survey of Different Techniques for Detection of Wormhole Attack in Wireless Sensor Network.” *International Journal of Scientific and Engineering Research*. vol. 3, no. 10, 2012.

A. Bharathidasan and V. A. S. Ponduru. “Sensor Networks: An Overview.” Technical Report, Dept. of Computer Science, University of California at Davis, 2002.

[12] M. Tubaishat and S. Madria. “Sensor networks: an overview.” *IEEE Potentials*, vol. 22, pp. 20-23, 2003.

[13] Priya Maidamwar and Nekita Chavhan. “A Survey on Security Issues to detect wormhole Attack in Wireless Sensor network.” *International Journal on Ad Hoc Networking Systems (IJANS)*, vol. 2, no. 4, October 2012.

[14] R.H. Khokhar, Md. A. Ngadi, S. Manda. “A Review of Current Routing Attacks in Mobile Ad Hoc Networks.” *International Journal of Computer Science and Security*, vol. 2, no. 3, pp. 18-29, 2008.

[15] Jali, Kamarularifin Abd, Jamalul-Lail Ab Manan Zaid Ahmad. “Mitigation of Black Hole Attacks for Aodv Routing Protocol.” International Journal of New Computer Architectures and Their Applications, vol. 1, pp. 336-343, 2011.

[16] Kumar, V. “Simulation and Comparison of AODV and DSR Routing Protocols in MANETs.” *Master Thesis*, 2009.

[17] S. Lu, L. Li, K. Lam and L. Jia. “SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack.” *2009 International Conference on Computational Intelligence and Security*, Beijing, pp. 421-425, 2009.

[18] Manel Guerrero Zapata,” Secure Ad hoc On-Demand Distance Vector Routing.” in *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 6, no. 3, pp. 106-107, June 2002.

[19] Chunhui Zhu, Myung J. Lee, Tarek Saadaw. “RTT-Based Optimal Waiting Time for Best Route Selection In Ad Hoc Routing Protocols.” *IEEE Military Communication Conference*, vol. 2, pp1054-1059, Oct 2003.

[20] K.U.R Khan, A.V. Reddy, R.U. Zaman, K.A Reddy, T.S Harsha. “An Efficient DSDV RoutingProtocol for WirelessMobile Ad Hoc Networks and its Performance Comparison.” *SecondUKSIM European Symposium on Computer Modeling and Simulation*, India, pp. 506-511, 2008.

[21] B Kannhavong, H Nakayama, Y Nemoto, N Kato. “A Survey of Routing Attacks In Mobile Ad Hoc Networks.” *IEEE Wireless Communication*, vol. 14, no. 5, October 2007.

[22] Abhishek Verma and Neha Bhardwaj. “A Review on Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) Routing Protocol.” *International Journal of Future Generation Communication and Networking.*vol. 9, pp. 161-170, 2016.

[23] https://en.wikipedia.org/wiki/Open_Shortest_Path_First.

[24] E Kaffashi, Ai Mousavi, H Rahvard. “A new attack on link-state database in open shortest path first routing protocol.” *Journal of Electrical and Electronic Engineering*, vol. 3, no. 2-1, pp. 39-45, 2015.

[25] L. Hu, D. Evans. “Using Directional Antennas to Prevent Wormhole Attacks.” 14 Proceedings of the 11th Network and Distributed System Security Symposium, pp. 2003.

[26] Y. C. Hu, A. Perrig, and D. B. Johnson. “Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks.” In Proc., *of IEEE -INFOCOM*, vol.3, pp. 1976-1986, 2003.

[27] Lazos, Loukas & Poovendran, Radha. “SeRLoc: Secure Range-Independent Localization for Wireless Sensor Networks.” *ACM Transactions on Sensor Networks*, vol. 1, pp. 21-30, 2004.

[28] [30] W. Wang, B. Bhargava. “Visualization of wormholes in sensor networks.” Proceedings of the *2004 ACM workshop on Wireless Security*, pp. 51-60, 2004.

[29] Khalil, Saurabh Bagchi and N. B. Shroff. “LITEWORP: a lightweight countermeasure for the wormhole attack in multihop wireless networks.” *2005 International Conference on Dependable Systems and Networks (DSN'05)*, Yokohama, Japan, pp. 612-621, 2005.

[30] B. Awerbuch, R. Curtmola, D. Holmer, H. Rubens and C. Nita-Rotaru. “On the Survivability of Routing Protocols in Ad Hoc Wireless Networks.” *First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05)*, Athens, pp. 327-338, 2005.

[31] N. Song, L. Qian, X. Li. “Wormhole Attacks Detection in Wireless Ad Hoc Networks: A Statistical Analysis Approach”. In Proceedings of the 19th IEEE *International Parallel and Distributed Processing Symposium*, pp. 8-15, 2005.

[32] M.A. Gorlatova, P.C. Mason, M. Wang, L. Lamont, R. Liscano. “Detecting Wormhole Attacks in Mobile Ad Hoc Networks through Protocol Breaking and Packet Timing Analysis.” In *IEEE Military Communications Conference*, pp. 1-7, 2006.

[33] H.S. Chiu and K. Lui. “DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks”. In *Proceedings of International Symposium on Wireless Pervasive Computing*, pp. 6-11, 2006.

[34] 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.

[35] Khin Sandar Win. “Analysis of Detecting Wormhole Attack in Wireless Networks”, World Academy of Science, Engineering and Technology, vol. 48, pp. 422-428, 2008.

[36] F. Nait-Abdesselam, B. Bensaou and T. Taleb. “Detecting and avoiding wormhole attacks in wireless ad hoc networks.” in IEEE Communications Magazine, vol. 46, no. 4, pp. 127-133, April 2008.

[37] S. Özdemir, M. Meghdadi, and Ý. Güler. “A time and trust-based wormhole detection algorithm for wireless sensor net- works.” (manuscript in Turkish), in 3rd Information Security and Cryptology.

[38] Krontiris, T. Giannetsos, and T. Dimitriou. “Lidea: A distributed lightweight intrusion detection architecture for sensor networks.” in *SECURECOMM ’08: Fourth International Conference on Security and Privacy for Communication Networks*, Istanbul, Turkey, September 22- 25 2008.

[39] S. Choi, D. Kim, D. Lee, J. Jung. “WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks.” In *International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing*, pp. 343-348, 2008.

[40] S Özdemir, M Meghdadi, Ý Güler. “Detection algorithm for wireless sensor networks” in 3rd Information Security and Cryptology Conference (ISC’08).

[41] H. Vu, A. Kulkarni, K. Sarac, N. Mittal. “WORMEROS: A New Framework for Defending against Wormhole Attacks on Wireless Ad Hoc Networks.” In *Proceedings of International Confernce on Wireless Algorithms Systems and Applications*, LNCS 5258, pp. 491-502, 2008.

[42] M.S. Sankaran, S. Poddar, P.S. Das, S. Selvakumar. “A Novel Security Model SaW: Security against Wormhole attack in Wireless Sensor Networks.” In Proceedings of International Conference on PDCN, 2009.

[43] B. Triki, S. Rekhis, and N. Boudriga. “Digital Investigation of Wormhole Attacks in Wireless SensorNetworks.” Eighth IEEE International Symposium on Network Computing and Applications, 2009.

[44] H. Chen, W. Lou, and Z. Wang. “Conflicting-set-based worm- hole attack resistant localization in wireless sensor networks." Book Chapter Lecture Notes in *Computer Science−Ubiquitous Intelligence and Computing*, vol. 5585/2009, pp. 296−309, 2009.

[45] D.Barman Roy, R. Chaki, N. Chaki,” A New Cluster-based Wormhole Intrusion Detection algorithm for Mobile Adhoc Networks”, *International Journal of Network Security & Its Applications (IJNSA),* vol 1, no 1, April 2009.

[46] H. Chen, W. Lou, X. Sun, and Z. Wang. “A secure localization approach against wormhole attacks using distance consistency.” *EURASIP Journal on Wireless Communication and Net- working- Special Issue on Wireless Network Algorithms, Systems and Applications*, vol. 1, pp.22−32, 2010.

[47] Prasannajit B, Venkatesh, Anupama S, Vindhykumari K, Subhashini S R, Vinitha G. “An approach towards Detection of Wormhole Attack in Sensor Networks.” *First International Conference on Integrated Intelligent Computing (ICIIC)*, pp.283-289, 2010.

[48] S. Gupta, S. Kar and S. Dharmaraja. “WHOP: Wormhole attack detection protocol using hound packet.” *2011 International Conference on Innovations in Information Technology*, Abu Dhabi, pp. 226-231, 2011.

[49] Z. Zhao, B. Wei, X. Dong, L. Yao and F. Gao. “Detecting Wormhole Attacks in Wireless Sensor Networks with Statistical Analysis.” 2010 *WASE International Conference on Information Engineering*, Beidaihe, Hebei, pp. 251-254, 2010.

[50] Bintu Kadhiwala and Harsh Shah. “Exploration of Wormhole Attack with its Detection and Prevention Techniques in Wireless Ad-hoc Networks.” *IJCA Proceedings on International Conference on Recent Trends in Information Technology and Computer Science 2012 ICRTITCS*, no. 9, pp. 1-6, February 2013.

[51] K. Patel, T. Manoranjitham. “Detection of wormhole attack in wireless sensor network.” *International Journal of Engineering Research & Technology (IJERT)*, 2013.

[52] D.S Kushwaha, A. Khare, J. L. Rana. “Improved Trustful Routing Protocol to Detect Wormhole Attack in MANET.” *International Journal of Computer Applications*, vol. 62, no. 7, pp. 21-25, January 2013.

[53] C.P. Vandana, A.F.S. Devraj. “MLDW-a Multilayered Detection mechanism for Wormhole attack in AODV based MANET.” *International Journal of Security, Privacy and Trust Management*, vol. 2, no. 3, pp. 29-41, June 2013.

[54] S. Goyal, H. Rohil, “Securing MANET against Wormhole Attack using Neighbor Node Analysis.” *International Journal of Computer Applications,* vol. 81, no. 18, pp. 44-48, November 2013.

[55] Y. Singh, A. Khatkar, P. Rani, “Wormhole Attack Avoidance Technique in Mobile Adhoc Networks”, Third International Conference on Advanced Computing & Communication Technologies, Rohtak, 6-7 April 2013.

[56] P. Nayak, A. Sahay, Y. Pandey. “Detection and Prevention of Wormhole Attacks in MANETs using Detection Packet.” *International Journal of Scientific & Engineering Research*, vol. 4, no. 6, June-2013.

[57] N. Choudhary, S. Agrawal. “Analysis of Worm-Hole Attack in MANET using AODV Routing Protocol.” *SSRG International Journal of Electronics and Communication Engineering (SSRG-IJECE)*, vol. 1, no. 10, Dec 2014.

A. Patel, N. Patel and R. Patel. “Defending against Wormhole Attack in MANET.” *2015 Fifth International Conference on Communication Systems and Network Technologies*, Gwalior, pp. 674-678, 2015.

[58] R. Singh, J, singh, Ravindar singh. “WHRT: A Hybrid Technique for Detecting of Wormhole Attack in Wireless Sensor Networks.” *Mobile Information Systems, Hindawi publishing Corpoartion*, vol. 2016, no. 13, pp. 1-13, 2013.