Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 14 Issue 1 Version 1.0 Year 2014
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

A Survey: Detection and Prevention of Wormhole Attack in Wireless Sensor Networks

By Akanksha Gupta & Anuj K. Gupta
RIMT College of Engineering & Technology, India

Abstract- Wireless Sensor Networks refers to a multi-hop packet based network that contains a set of mobile sensor nodes. Every node is free to travel separately on any route and can modify its links to other nodes. Therefore, the network is self organizing and adaptive networks which repeatedly changes its topology. The relations among nodes are restricted to their communication range, and teamwork with intermediate nodes is necessary for nodes to forward the packets to other sensor nodes beyond their communication range. The network's broadcasting character and transmission medium help the attacker to interrupt network. An attacker can transform the routing protocol and interrupt the network operations through mechanisms such as selective forwarding, packet drops, and data fabrication. One of the serious routing-disruption attacks is Wormhole Attack. The main emphasis of this paper is to study wormhole attack, its detection method and the different techniques to prevent the network from these attack.

Keywords: *wormhole attack, classification, detection mechanism, wsn, security, routing protocols*

GJCST-E Classification : *C.2.1*

Strictly as per the compliance and regulations of:

A Survey: Detection and Prevention of Wormhole Attack in Wireless Sensor Networks

Akanksha Gupta [α] & Anuj K. Gupta [σ]

Abstract- Wireless Sensor Networks refers to a multi-hop packet based network that contains a set of mobile sensor nodes. Every node is free to travel separately on any route and can modify its links to other nodes. Therefore, the network is self organizing and adaptive networks which repeatedly changes its topology. The relations among nodes are restricted to their communication range, and teamwork with intermediate nodes is necessary for nodes to forward the packets to other sensor nodes beyond their communication range. The network's broadcasting character and transmission medium help the attacker to interrupt network. An attacker can transform the routing protocol and interrupt the network operations through mechanisms such as selective forwarding, packet drops, and data fabrication. One of the serious routing-disruption attacks is Wormhole Attack. The main emphasis of this paper is to study wormhole attack, its detection method and the different techniques to prevent the network from these attack.

Keywords: wormhole attack, classification, detection mechanism, wsn, security, routing protocols.

I. Introduction

In Wireless Sensor Networks, the nodes use the open air medium to communicate with each other, in doing so they face sensitive security problems as compared to the wired networks. One such dangerous problem is wormhole attack. In this attack, two distant malicious nodes can plan together using either wired connection or directional antenna, to give an feeling that they are only one hop away. Wormhole attack can be executed in hidden or in sharing mode. Wormholes can either be used to examine the traffic throughout the network or to crash packets selectively or totally to affect the flow of information. The security mechanisms that are used for wired systems such as authentication and encryption are useless under hidden mode of wormhole attack because the nodes do not modify their headers but only forward these packets. But the attack in participating mode is more complicated, because if it once launched, it is difficult to detect.

WSN faces some challenges which are as follows:

1. Power Consumption – conservation of power is necessary and detection of some power saving routing protocol.
2. Multicast Routing – scheming of multicast routing protocol for a frequently changing WSN surroundings
3. Internetworking – Communication among wired system and WSN while maintaining synchronization.

II. Security Goals Designed for Wireless Sensor Networks

Security goals for WSN can be categorized as primary and secondary goals [35]. Some of the primary goals are Data Confidentiality, Data Authentication, Data Availability and Data Integrity and secondary goals are Data Freshness, Secure Localization, Self- Organization and Time Synchronization. The primary goals are also known as standard security goals.

Primary goals are as follows:

a) Data Confidentiality

Confidentiality is the capability to hide messages from a passive attacker such that every message communicated using the sensor network remains confidential. It is the most important concern in network security. A sensor node should not expose its data to its neighbors.

b) Data Authentication

Authentication ensures the consistency of the message by identifying its foundation. Attackers in sensor networks can not only responsible for the alteration of packets but can also insert additional fake packets [34]. Basically data authentication is used for the verification of the identity of the senders and receivers. Symmetric or Asymmetric mechanisms are used for data authentication in which sending and receiving nodes share secret keys. Because of wireless medium and unattended nature of sensor networks, it is very demanding to ensure authentication.

c) Data Integrity

Data integrity in wireless networks is desired to ensure the consistency of data and to verify that a message has not been altered, tampered with or changed. Though the system has secrecy measures, but still there is a possibility of alterations. The integrity of the system will be in dilemma when:

- A wicked node present in the network adds false data.
- Due to wireless channel unstable conditions can cause harm or loss of data [33].

Author α: RIMT College of Engineering & Technology, Mandi Gobindgarh, Fatehgarh Sahib, Punjab, India.
e-mail: gupta.akanksha75@gmail.com
Author σ: Head of the Department (Computer Science and Engineering), RIMT College of Engineering & Technology, Mandi Gobindgarh, Fatehgarh Sahib, Punjab, India.
e-mail: anujgupta@rimt.ac.in

d) Data Availability

Availability ensures whether the resources are free to be used by a node and whether the network is existing for the messages for communication. However, failure of the base station or cluster leader's availability will eventually threaten the entire sensor network. Thus data availability has a main importance for maintaining an operational network.

Secondary goals are as follows:

e) Data Freshness

Even though confidentiality and data integrity are guaranteed, there is also a need to make sure the freshness of each message. Basically, data freshness [33] ensures that the data is new and no old data have been replayed. To resolve this trouble related counter will be added into the packet to guarantee data freshness.

f) Self-Organization

A wireless sensor network is a usually an ad hoc network, in which every sensor node is independent and flexible such that each nodes is self-organizing and self-healing to different situations. No permanent infrastructure is present in a wireless sensor network for network management. This natural feature challenges the wireless sensor network security. So if self-organization is absent in a sensor network, then the harm that results from an attack or from the risky environment may be disturbing.

g) Time Synchronization

Most of wireless sensor network applications are based on some type of time synchronization. Moreover, sensors tries to calculate the end-to-end delay of a packet as it travels from source to destination sensor or node. A shared sensor network can require group synchronization [33] for purpose of tracking applications.

h) Secure Localization

The effectiveness of a sensor network is based on its ability to locate each sensor node in the network correctly and automatically. Now a days, sensor networks designed to locate faulty nodes which will require the accurate location information. An attacker can easily operate all the non protected location information by exposing the replaying signals and false signal strengths etc.

III. Wormhole Attacks

Wormhole attack contains two nodes that are connected to one another with the a medium that is not offered to normal nodes, due to which the nodes can communicate with one another over a range in which normal nodes cannot. These two colluding nodes are operated such that they shown like a neighbors to all the other nodes. In [Figure 1], suppose node-1 wants to send any data to node-25 through the network, so node-1 broadcasts the route request. Let node-Xs and node-Xd are the two colluder nodes in the locality of source node and destination node. Now Xs along with other nodes in the network gets the route request from source node, it replays the same request to Xd, Xd receives the request and de-capsulate it and rebroadcasts it to its neighborhood. After receiving the route request through Xd the destination node-25 will think that they are direct neighbors to source node-1, and it will reply to that route request. Xd will then capture that reply and using the same process it will send it to Xs; which further send to node-1. Thus node-1 and node-25 will believe that they are 2- hop neighbors. And complete communication will pass through Xs and Xd. This is one type of wormhole attack; many more number of variants are defined in the literature [3], [4], [5].

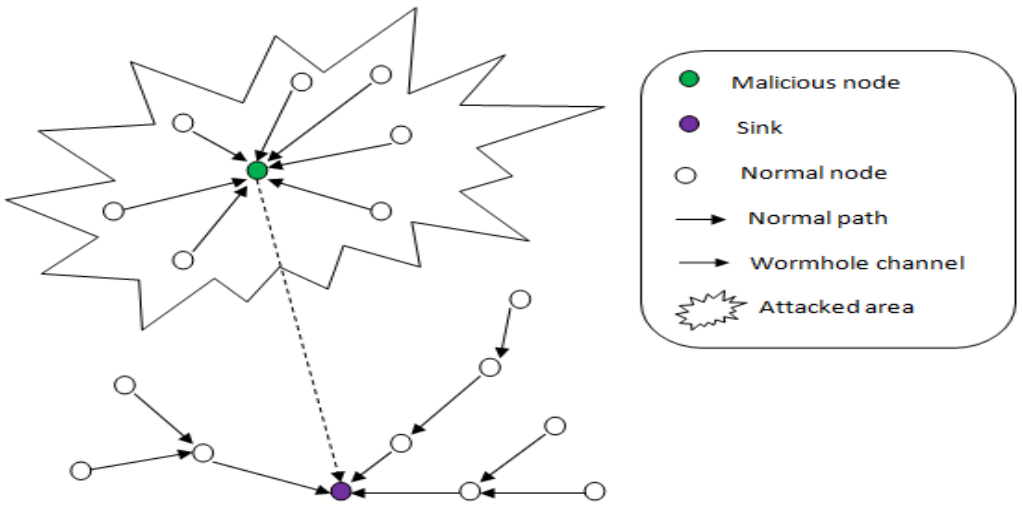


Figure 1

IV. Classification of Wormhole Attacks

In [6], [7], [8]; Wormhole attacks can be classified on the basis of:

1) Its Implementation
2) The medium used
3) The attackers
4) The location of victim nodes.

a) Classification based upon Implementation

This is the most important classification; which depends upon the behavior the attack is launched.

i. *Using Encapsulation*

In this manner, there are some nodes are occupied along the path (these nodes may or may not be conscious of wormhole) between xs and xd. The packet gets encapsulated at xs and travels through the path in encapsulated form to avoid the increase in the hop count. In this case the attackers are not directly connected to one another rather make the other nodes believe that they are directly connected. These packets are transmitted between xs and xd using a virtual tunnel. Once this attack is successfully launched, then all the paths will contain a link that will contain of link between xs and xd.

ii. *Using Out-Of-Band Channel*

These colluder nodes get connected directly through a out of band channel having high bandwidth. The channel can be obtained by a wired connection or using a wireless connections. The requirement of extra hardware made it difficult to launch, but provides a simplicity because it will not require any encapsulation/de-capsulation while the colluders are directly connected.

iii. *Using High Power Transmission*

This type of wormhole particularly launched from two colluder nodes that facilitates high power transmission potential.

iv. *Via Protocol Deviations*

In this case the attackers generate the wormhole by not following the protocol set of laws e.g. Some protocols suppose the nodes to wait for a while before retransmitting but the attackers keeps on broadcasting and do not obey this rule and thus trying to reach first at the destination and thus avoiding any future genuine requests to reach destination. If the future requests arrive at destination, they will be dropped, since a request passing through the colluder has previously been received.

b) Classification based upon Medium Used

On the basis of medium used, wormhole attacks can be classified as in-band and out-of-band wormhole attacks.

i. *In-Band Wormhole*

Same medium will be used by the attackers for creating link between them e.g. protocol deviations, packet relay and, encapsulation.

ii. *Out-Of-Band Wormhole*

Like normal network nodes attackers do not use the same medium, e.g. High Transmission Mode and Out-Of-Band Channel.

c) Classification based upon Attackers

i. *Self-Sufficient*

Here colluder nodes present themselves as normal nodes and thus all paths passes through them e.g. using high power transmission or out-of-band channel.

ii. *Extended Wormhole*

The colluder nodes extends the attacks beyond themselves to normal nodes and are unseen by themselves e.g. packet relay or encapsulation.

d) Classification based upon location of Victim nodes

i. *Simplex*

The victim node is present inside the range of only one attacker.

ii. *Duplex*

The victim node is present inside the range of both the attackers.

V. Literature Review

A significant amount of work have been prepared for the detection of wormhole attacks and the attackers. The work ranges from suggestion of extra and exclusive hardware to minor modifications in the system protocols and suggestion of smart ways of avoiding or detecting the wormholes. However some can need extra hardware and other require extra processing and battery life. This section shows a small review of the approaches proposed till date.

Hu et al. [16] proposed the method in 2003 based upon geographical and temporal packet leaches. In this method to avoid the wormhole, the geographical location or temporal location is used to bound the distance travelled by the packet. This approach is restricted by condition of GPS technology or the time synchronization. Lazos et al. [17] proposed a method in 2005 where a few nodes are mandatory to be equipped by GPS locators and directional antennas. This procedure uses “local broadcast keys” for safe communication between one another.

Tran et al. and Phuong et al. proposed TTM (Transmission Time based Mechanism) in 2007, where every node in the pathway work together and attack is identified through route setup stage by calculating transmission time among two nodes. Venkataraman et al. in 2009 proposed a graph theoretic mechanism for

the finding of wormhole attacks, which is right for proactive protocols.

Chen et al. [18] proposed a secure localization approach in 2010 based on the inconsistent set based resistant localization. Graaf et al. [19] proposed a dispersed detection approach based upon ranges of nodes for the detection of wormhole attacks. A Vani et al. [20] proposed a solution in 2011 that combines the decision anomaly, neighbor list count and hop count methods for AODV protocol. This procedure depends upon hierarchical processing of nodes and their respective neighbors. They used the hop count information available in the routing table of the nodes which needs that we need to store two copies of routing table of every node so as to maintain the track of earlier hop counts.

VI. Routing Protocols and Wormhole Attack

Various routing protocols are existing for WSN. Some of the often used routing protocols are considered in this section and the risk of wormhole attacks to such protocols is described. These routing protocols are classified into two types: proactive / table-driven protocols and reactive / demand-driven protocols [1]. AODV, DSR and Ariadne are reactive routing protocols and OLSR, DSDV and SEAD are proactive routing protocols.

a) OLSR (Optimized Link State Routing)

It is a proactive routing protocol in which information of the topologies get exchanged periodically. Hello messages are transmit to determine single hop neighbors. To allocate signaling traffic, flooding system is use. In this system each node forwards flooded message that was not forwarded by them earlier. The topology messages contains all the information about link states that are sent to all other nodes. With the help of this information, partial topology graph are obtained by every node after calculating the shortest path using symmetric relations. Now this system is open to wormhole attack [9] – [11]. Isolated nodes can send hello and topology manage messages are available at its colluding nodes to its personal neighbors for broadcasting fake information into the system. This will create two distant nodes to mistakenly believe themselves as neighbors, that leads to the failure of routing protocol.

b) DSDV (Destination Sequenced Distance Vector)

It is a proactive routing protocol, in which all the metric, destination routes, sequence number generated by the destination node and next hop to each destination are maintained in a table [1], [2]. Every node in the network acts as a router and the table gets updated periodically by exchange of messages among neighboring routers. This protocol is open to wormhole attack [9]. By using a tunnel, the colluding nodes surpass message between two distant nodes, suppose X and Y which will results X and Y to consider themselves as neighbors and they will publicize a hop count of one among each other. As a result of this false information, if the alternative route has hop count more than one then all other authenticated nodes will aim to send the messages through X to destination Y.

c) DSR (Dynamic Source Routing)

It is a reactive routing protocol because it discovers the required routes only after it has packets to transmit to the destination. It wants source route maintenance because during the utilization of the route, it is necessary to check the operation of the path and to report the sender regarding the errors [2]. It is at risk to wormhole attack and denial of service attack at the destination [9]. This protocol ensures forwarding of just the first RREQ that it will received and will reject all other RREQ packets for the same route. This RREQ packet contains the intermediate nodes and the hop count information. The route then established is used to send data packets. As wormhole attack ensures a fast channel for forwarding messages, so as compared to other paths RREQ packet through them will arrived at destination faster. This will result in only the wormhole path to be discovered as the route to destination. The wormhole attacker discards the data packets totally or partially that results in denial of service attack at the destination.

d) SEAD (Secure Ad-hoc Distance Vector)

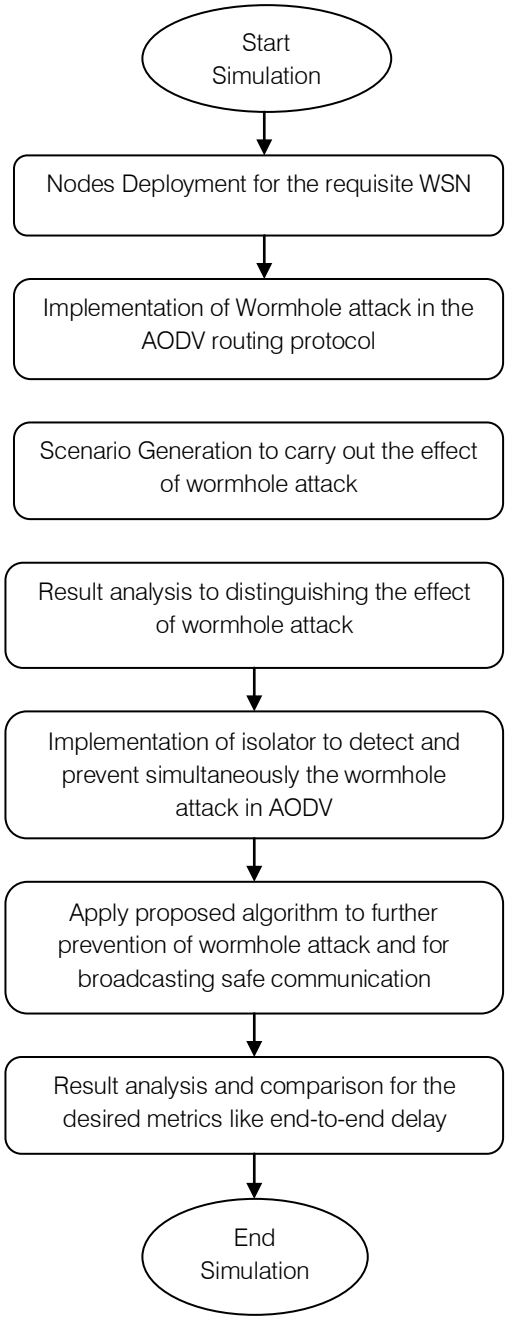
This protocol depends upon on one-way hash chains rather than asymmetric cryptograph and protects the network from uncoordinated attacks and DoS attacks. Several nodes have the ability to authenticate all other elements of the chain. This requires authenticating the metric of the routing table and the sequence number. The receiver should also verify the sender [2]. Thus, an enemy is not able to send routing message without compromising a node, as it does not give authentication code to its neighbors [12]. Although SEAD effectively handles replay attack, it is incapable to handle the wormhole attack [13] by a malicious node that are replaying the message from an unauthenticated node as a repeater.

e) AODV (Ad-hoc On-demand Distance Vector)

It is an on-demand routing protocol which broadcasts RREQ messages to its immediate neighbors for sending messages to final destination and in turn these neighbors rebroadcast them to their neighbors. This whole process continues unless until the RREQ message reaches the destination. On getting the initial RREQ message from the source, the destination node sends a RREP to the source node through the same reverse path [1], [15]. All the in-between nodes also put forward route entries in their respective table. The

neighboring nodes forward route error message to all its neighbors after detecting fault in any link to a node. This will again start a route discovery procedure to change the broken link. This AODV routing protocol is also at risk to wormhole attack [9].

As wormhole attack ensures a fast channel for forwarding messages, so as compared to other paths RREQ packet through them will arrived at destination faster. In this protocol, the destination rejects all the later on RREQ packets received, yet they are from authenticated node. Hence the destination chooses the fake path through wormhole for RREP [1].



The Prevention of Wormhole attack in AODV using WSN

f) Ariadne (A Secure On-Demand Routing Protocol for Ad-hoc Networks)

This protocol depends on symmetric cryptography and ensures that the source can authenticate each intermediate node in the route and the destination node authenticates the source. All intermediate node can eliminate or insert nodes in the list of nodes of the route request. It uses the key management protocol known as TESLA that focuses on the clock synchronization to authenticate routing

messages. TESLA uses per-hop hashing method [2]. An authentication done at each node does not only depends upon the information contained in the RREQ packet but also depends the authentication code of the preceding node. Ariadne protocol is free from over-flooding of RREQ attack because the attacker is prevented from replaying the message due to the network-wide shared secret key. It is necessary for each node to insert authentication code to every RREQ packet that it forwards. Then the source can be able to authenticate the origin of all individual data field in the RREP packet [14]. It is protected from rushing attack wormhole and attack [13] while successful route distortion requires RREQ to be tailored cautiously.

VII. Detection and Avoidance of Wormhole Attacks

From past few years the main area of research is the detection of wormhole attack. The most important task is to discover the occurrence of wormhole in the system [12], [24] – [31].

Detection of wormhole on the basis of the Hello control messages [26]. With the use of OLSR specifications, the percentage of HELLO Message Timing Intervals (HMTIs) which lies in a range enclosed by the amount of jitter. A range $R = [T - \delta, T + \delta]$ have been defined. If HMTI is in the range R, then it will considered to be valid; otherwise it is said to be out-of-protocol. A second check is made every time when the HMTI packet behavior is doubtful. On other side, a badly performing node would get coupled with it a comparatively large number of repeat packets, that would not be the case by an attacking node. In this way, the false positive alarms problem gets negotiated.

A new protocol known as Multi-path Hop-count Analysis (MHA) is proposed on the basis of hop-count analysis to stay away from wormhole attack [24]. It is supposed that very low or very high hop-count is not good for the network. The uniqueness of the hop-count analysis for detecting wormholes nodes is yet uncertain.

Wormholes nodes are detected by assuming that wormhole attacks have longer packet latency as compared to the normal wireless propagation latency in a single hop [10]. As the route during wormhole seems to be shorter, various new multi-hop routes be also channeled in the direction of the wormhole that leads to the longer queuing delays. The links having delays are considered to be doubtful links, as the delay might also takes place due to congestion as well as intra-nodal processing. The OLSR protocol is used for routing. This approach aims to sense the suspicious link and authenticate them in a two step process that is described below.

In first step, Hello packets has been sent to all the nodes that are within its transmission range. As soon as the receiver receives the Hello message, then it records the address of the sender and the time delay Δ left until it will be programmed to send its next Hello message. The node attaches the address of the sender and their respective values of time delay Δ that has recorded for piggybacked reply. When Hello reply is received by a node, then it checks for the information related to any of its outstanding requests. But if no such information is there, then it will suppose it as any other control packet. Otherwise, node checks the arrival time of Hello reply message to notice whether it is arrived within its scheduled timeout interval by considering the time delay Δ that occur at the receiver side. If the arrival time is within its timeout interval then link between itself and node is taken to be safe, otherwise doubtful and communication to that node is terminated by the sender until the verification process gets over.

In second step, a probing packet is sent to all the suspected nodes (that are detected in the previous step) by the sender.

If a suitable acknowledgement is received from any node X within its scheduled timeout interval then node X is considered to be safe. Otherwise the occurrence of wormhole is proved.

Both delay per hop indication (DelPHI) and hop count are monitored for wormhole detection [22]. The basic assumption is that the delay that packet experience in standard conditions for propagation of one hop will become too high under wormhole attack as the actual path between the nodes is shorter than the advertised path. This proposed methodology for wormhole detection is a two-step process.

The first phase has the route path information, gained from a set of disjoint paths from sender to receiver. Every sender will consist of a timestamp on a unique DREQ packet and send it to receiver after signing it. After receiving the packet for first time every node will adds its node ID then increase the hop count by 1 and rejects the packet next time onwards. After receiving each disjoint path the receiver send the DREP packets. This process is carried out for three times and the hop count and smallest delay information will be chosen for wormhole detection.

In second phase, the time difference between the packet it had sent to its neighbor and the reply received by it known as round trip time (RTT) is calculated. Delay per hop value (DPH) is evaluated as RTT/2h, where h stands for hop count to the particular neighbor. Under ordinary circumstances, a smaller h also have smaller RTT. However, smaller hop count will have larger RTT under wormhole attack. But one DPH value for node X exceed the consecutive one by several threshold, then path from node X to every another paths with DPH values greater than it is considered as under wormhole attack.

Similar propositions are made in SaW [29] and DaW [30]. In SaW, AODV protocol was used and in

DaW, DSR routing protocol was used. In these papers, security models have been planned and used to detect interruption. To detect the attacks, it will use statistical methods. If any link is identified to be doubtful, then existing information is used to detect the presence of a wormhole. In trusted model, nodes monitor their neighbors on the basis of packet drop pattern but not on the basis of number of drops. Other algorithm has been proposed in [30] to detect the presence of wormhole into system. In this algorithm, the source waits for RREP after sending the RREQ. The source receives a lot of RREP from different routes. By using the below expression we can find out the link with very high frequency:

$$Fi = pi / P, \text{ for all } Li$$
$$Fmax = max\ (Fi),$$

where r is the set of all obtained routes, *Li* is the ith link, pi is the number of times that *Li* appears in *r,* P is the total number of links in *r*, and *Fi* is the relative frequency that *Li* appears in *r*. If *Fmax* > *Fthreshold,* then check the information present in RREP of that route. The node will be malicious if the value of correlation coefficient for packets dropped is greater than the pre-set threshold value t, then it will inform the operator otherwise continue with routing process.

According to [29] and [30], the regular link frequency analysis may lead to fake detection of wormhole attacks. Though, these recognize the performance of a wormhole as they record the total number of packet drops rather than the pattern of drop.

The wormhole attack can be detected using multipath routing [27]. When a source node wants a new route, it will broadcast the RREQ into the network and wait for responses. Then the in-between node will forward only the first RREQ packet. After receiving the first RREQ the destination will wait for a while to gather all the obtained routes. A new scheme known as Statistical Analysis of Multi-path (SAM) is projected in [27]. SAM uses *Pmax* (i.e. maximum probability of relative frequency of a link to occur in the set of all obtained routes from one route discovery) and Ø (i.e. difference between the most frequently appeared link and the second most frequently appeared links in the set of all obtained routes from one route discovery), which will be higher in the presence of wormhole attack. Relative Frequency is calculated using probability mass function (PMF) which is more for a network that is under wormhole attack as compared to a normal network. The performance of Dynamic Source Routing (DSR) and On-demand multipath routing (MR) protocol are compared under wormhole attack.

A cluster based counter-measure known as WHIDS [28] is proposed for the wormhole attack. By using MATLAB simulation results the effectiveness of WHIDS are revealed for detecting wormhole attack. This method, yet not been experienced in existence of multiple wormhole attacks.

Vu et al. proposed the technique to detect the existence of wormhole node using two phases [31] as in [10] and [22]. The first phase contains of two methods: In first method, the computation of round-trip-time (RTT) among the source and all of its immediate neighbors is measured. In second method, source identifies its one-hop and two-hop neighbors to form its neighbor set. If it is originated that the destination is not the neighbor of source node then the link between them will be taken as suspicion. After detecting the doubtful links, the next phase is used to verify the presence of wormholes for exchange of messages by using the RTS / CTS mechanism.

Table 1 represents multi-aspect comparison among eight different wormhole detection techniques. Significant aspects like false alarm detection, the node mobility along with QoS parameters are considered for each detection technique. This qualitative study have been supported by quantitative one also for several algorithms using the network simulator tool.

Table 1 : Summary about the detection methods for wormhole attack.

Method	Mobility	QoS Parameter	Synchronization	False detection
WORMEROS [31]	Topological change is not considered	Not considered	Time synchronization not required. RTT between source node and destination node is considered	Both false positive and false negative alarms are considered
HMTIs [26]	Handled weakly. Topologically robust, short range worm-hole can be detected	Jitter and delay	Not required. Since PSD profiling is done locally	Used PSD to detect false positive alarm
Farid et al. [10]	Not considered	Packet processing time, queue	Some time delay added to detect suspicious links	Not handled
DelPHI [22]	Not considered	Delay	Not required	Not handled

SAM [27]	Cluster and uniform topology considered	Not considered	Not considered	Not handled
SaW [29]	Not considered	Not considered	Not considered	Failed to detect
DaW [30]	Not considered	Delay parameter	Not considered	Failed to detect
WAP [23]	Maximum transmission distance is calculated	Delay per hop	Only the source node is synchronized	Not handled

References Références Referencias

1. 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, 2008.
2. D. Vivian, E.A.P. Alchieri, "Evaluation of QoS Metrics in Ad Hoc Networks with the use of Secure Routing Protocols", In Network Operations and Management Symposium, 2006.
3. Meghdadi M, Ozdemir S," A Survey of Wormhole-based Attacks and their Counter measures in Wireless Sensor Networks", IETE Tech Rev 2011.
4. S.Vijayalakshmi and S.Albert Rabara "Weeding Wormhole Attack in MANET Multicast Routing Using Two Novel Techniques - LP3 and NAWA2", International Journal of Computer Applications, February 2011.
5. Jhaveri, R.H.; S.J.; Jinwala, D.C.; "DoS Attacks in Mobile Ad Hoc Networks: A Survey," Advanced Computing & Communication Technologies (ACCT), 2012.
6. V. Mahajan, M. Natu "Analysis of wormhole intrusion attacks in MANETS", In IEEE Military Communications Conference (MILCOM), 2008.
7. H.S. Chiu and K. Lui. "Wormhole Detection Mechanism for Ad Hoc Wireless Networks". In Proceedings of International Symposium on Wireless Pervasive Computing, 2006.
8. R. Maulik, N. Chaki. "A Comprehensive Review on Wormhole Attacks in MANET". In 9th International Conference on Computer Information Systems and Industrial Management Applications, 2010.
9. Yih-Chun Hu, Adrian Perrig. "Packet leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks". In 22nd Annual Joint Conference of the IEEE Computer and Communications Societies, 2003.
10. F. Nait-Abdesselam, B. Bensaou. "Detecting and Avoiding Wormhole Attacks in Wireless Ad hoc Networks", IEEE Communications Magazine, 2008.
11. John S. Baras, George Theodorakopoulos. "Intrusion Detection System Resiliency to Byzantine Attacks: The Case Study of Wormholes in OLSR". In IEEE Military Communications Conference, 2007.
12. Y.-C. Hu, A. Perrig, D.B. Johnson. "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks". In Proceedings of Fourth IEEE Workshop on Mobile Computing Systems and Applications, 2002.
13. Kamanshis Biswas, Md. Liakat Ali. "Security Threats in Mobile Ad Hoc Network". Paper submitted to the Department of Interaction and System Design, School of Engineering at Blekinge Institute of Technology, 2007.
14. Y.-C. Hu, D.B. Johnson. "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", Wireless Networks, 11(1-2), 2005.
15. Bounpadith Kannhavong, Hidehisa Nakayama, Abbas Jamalipour. "A Survey of Routing Attacks in Mobile Ad Hoc Networks", IEEE Wireless Communication, 2007.
16. Hu, Y.-C.; Perrig, A.; Johnson, D.B.; "Packet leashes: a defense against wormhole attacks in wireless networks,". Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies , April 2003.
17. Lazos, L.; Poovendran, R.; Syverson, P.; Chang, L.W.; , "Preventing wormhole attacks on wireless ad hoc networks: a graph theoretic approach," Wireless Communications and Networking Conference, March 2005.
18. Honglong Chen , Wei Lou , Zhi Wang, A secure localization approach against wormhole attacks using distance consistency, EURASIP Journal on Wireless Communications and Networking, April 2010.
19. R. Graaf, I. Hegazy, J. Horton. "Detection of wormhole attacks in wireless sensor networks," Springer book chapter Ad Hoc Networks, 2010.
20. A.Vani, D. Sreenivasa Rao, "A Simple Algorithm for Detection and Removal of Wormhole Attacks for Secure Routing In Ad Hoc Wireless Networks", International Journal on Computer Science and Engineering (IJCSE), June 2011.
21. V. Mahajan, M. Natu. "Analysis of wormhole intrusion attacks in MANETS". In IEEE Military Communications Conference, 2008.
22. H.S. Chiu and K. Lui. "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks". In Proceedings of International Symposium on Wireless Pervasive Computing, 2006.
23. S. Choi, D. Kim, J. Jung. "WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks". In International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing, 2008.

24. Shang-Ming Jen, Chi-Sung Laih. "A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET", 2009.
25. D. Djenouri, O. Mahmoudi, M. Merabti, "On Securing MANET Routing Protocol Against Control Packet Dropping". In IEEE International Conference on Pervasive Services, 2007.
26. M.A. Gorlatova, P.C. Mason, L. Lamont, R. Liscano, "Detecting Wormhole Attacks in Mobile Ad Hoc Networks through Protocol Breaking and Packet Timing Analysis". In IEEE Military Communications Conference, 2006.
27. 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, 2005.
28. D.B. Roy, R. Chaki, N. Chaki. "A New Cluster-based Wormhole Intrusion Detection Algorithm for Mobile Ad-hoc Networks", 2009.
29. M.S. Sankaran, 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.
30. Khin Sandar Win. "Analysis of Detecting Wormhole Attack in Wireless Networks", World Academy of Science, Engineering and Technology, 2008.
31. 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 Conference on Wireless Algorithms Systems and Applications, 2008.
32. R. Maulik, N. Chaki. "A Comprehensive Review on Wormhole Attacks in MANET". In Proceedings of 9th International Conference on Computer Information Systems and Industrial Management Applications, 2010.
33. Ian F. Akykildiz, Yogesh Sankarasubramaniam and Erdal Cayirci, "A Survey on Sensor Networks", IEEE Communication Magazine, 2002.
34. Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Communication Surveys Tutorials, 2006.
35. John Paul Walters, Zhengqiang Liang, Vipin Chaudhary, "Wireless Sensor Network Security: A Survey", Security in Distributed, Grid and Pervasive Computing Yang Xiao, 2006.