Journal of Theoretical and Applied Information Technology
10th September 2015. Vol.79. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A REVIEW ON WORMHOLE ATTACKS IN MANET

MEHDI ENSHAEI[1], DR. ZURINA BT HANAPI[2]

Faculty of Computer Science and Information Technology, UPM
E-mail: [1]mehdi.enshaei@gmail.com, [2]zurinamh@upm.edu.my

ABSTRACT

Mobile Ad-hoc Network (MANET) refers to a multi-hop packet based wireless network consist of number of mobile nodes which be able to communicate and move simultaneously, without using any fixed infrastructure. MANET'S are self organizing networks that can be formed and deformed on the fly. A number of different attacks have been discovered that can be launched against MANETs. Wormhole attack is one such attack that has been recently discovered. Wormhole attack is a very severe and challenging attack because of the fact that it can be launched against any protocol and also due to its ability to be effective in case of encrypted traffic. Enormous amount of work has been done towards the mitigation of wormhole attack and its counter measure. In this paper we have summarize the efforts previously done, our aim here is to provide the researchers a platform where they can find a complete reference to all past work done in regards to the wormhole attack. In the review paper we try to know all the detection techniques and use appropriate one or modify previous related works to have better defense mechanism against wormhole attacks.
Keywords: *Mobile Ad hoc Network, Wormhole Attack, Wormhole Detection Techniques.*

1. INTRODUCTION

Structure of MANET is consists of movable and autonomous nodes which does not have central infrastructure to manage their role. These types of networks are very operative to have communication by nodes which are out of area of wireless transmission coverage. MANETs are use in many fields, which require to have wide range of coverage, usage areas example such as environmental control [1], tactical area such as military battlefields [2], education area such as university campus [3], home and enterprise networking such as meeting rooms and conferences. Figure 1 show, the nodes are moving by using air as a medium to transfer and communicate with the other devices, and this is the cause of serious security problems compared to wired network.

However it has some weaknesses such as nodes have to stay in range of communication due to limited radio signal range. Signals can block or absorbed after hitting to some objects. Mobile nodes have limited life of battery, if the node communication and transmission is continued for long time it reduced the life of battery and node cannot perform the duties and after a while going inactive in the network. This work is done to know information about wormhole attacks and the techniques to detect and prevent the wormholes in the network. We review many previous related works and wants to find who we can have a good defense mechanism to detect wormholes. We need to achieve better security in the network against the wormhole attacks to improve wormhole detection rate, as well as achieve greater throughput and less average delay.

2. FEATURES OF MANETS

The unique characteristic of MANET opened new opportunities with some challenges. By this approach, a study is being conducted on MANET. Below are attribute of MANETs:

Figure 1: Typical MANET

Self-organizing Wireless Node: In MANET, every single mobile node behaves autonomously, which allows it to operate like a host or a router. Thus, each work is completed through the agreement of both sides and acceptance among the nodes, and every node can be functional in both (occasionally may work as both router and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

as host). So usually in MANET, endpoints and switches are not detectable [4],[5].

Distributed Operation: For the central control of the network operations, the control and management of the network is distributed among the terminals. The involved nodes should collaborate with each other and behave the same as a relay when required to carry out responsibilities like security and routing [6], [7].

Multi-hop Routing: Routing algorithms in ad hoc is divided into single-hop and multi hop, as a result of divers' link layer routing protocols and attributes. Based on the structure and its implementation, multi-hop MANET is complex compared to a single hop due to the cost of less applicability and functionality. Once data packets are sent from source and reaches the target located outside the broadcast area, the packets need to send over individual or multiple intermediary nodes [8] [9].

Dynamic Topology: Due to having movable nodes, network topology can be changed from time to time and the connection between the terminals might be different at any time. MANET is supposed to adopt some conditions such as propagation and traffic plus the mobility models based on the nodes in the mobile network. In this type of network the mobile nodes seek to launch a routing between each other and make themselves a movement network in the process [10] [11].

Light-weight Terminal: In most situations, the mobile nodes in MANET have less Central Processing Unit (CPU) processing ability, limited memory size, and not enough battery life. These kinds of devices have to adopt better mechanisms and algorithms that employ some functions such as computing and communicating [12], [13].

Other aspects of MANETs was reviewed in our previous work [14].

3. RELATED WORKS

Within of past few years wormhole detection and prevention is an interesting area of research. The important task is to find the existence of wormhole. This section contains the summary of different techniques present in the literature for the detection of wormhole attacks.

A cluster based wormhole attack avoidance technique introduced by [15]. The concept of hierarchical clustering with a novel hierarchical 32-bit node addressing scheme is used for avoiding the attacking path during the route discovery phase of the DSR protocol, which is considered as the under lying routing protocol. Pinpoint the location of the wormhole nodes in the case of exposed attack is also given by using this method.

In paper [16] a more efficient Routing Protocol named Wormhole attack Detection Protocol using Time Stamp with Security Packet. W-TSP allows to the receiver to check whether there are any malicious nodes sitting along its paths from sender to receiver and try launching wormhole attacks. We obtain the average delay time and total hop count details of paths between the sender and the receiver and use this information to indicate that wormhole attack is subjected in this selected path among. The advantages of W-TSP are that it does not require any special hardware and clock synchronization.

The study by [17] evaluated the performance of AODV and DSR routing protocol under the scenario of a wormhole attack and without a wormhole attack. The performance parameters taken into consideration included average end to end delay, throughput, and packet delivery ratio (PDR).

A study by [18] proposed a clustering and digital signature based approach for avoidance and prevention of wormhole attacks. The algorithm needs some nodes to perform specialized functions also, e.g. some nodes are supposed to be Cluster Heads and some are assumed to be Gateway nodes. The model built assumes transmission through on Cluster heads and Gateway nodes and dropping traffic arising from any other model. The algorithm seems good only for avoidance of wormhole link, it cannot identify the attackers nor perform any mitigation any of the identified nodes.

Path Tracing algorithm to detect and prevent wormhole attack offered by [19]. This PT algorithm runs on each node in a path during the Ad hoc On-Demand Distance Vector (AODV) route discovery process. It calculates per-hop distance based on the Round Trip Time (RTT)

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

value and wormhole link using frequency appearance count. The corresponding node detects the wormhole if per-hop distance exceeds the maximum threshold range. They use MASK, a special type of public key cryptosystem to achieve anonymous communication in MANET.

Path Tracing (PT) algorithm offered by [20] to discover the wormhole attacks in MANET. PT computes the distance travelled per-hop by calculating RTT and speed of light. The distance is used to identify the abnormal routes. A normal distance is stored in the routing table which will be used as a threshold value for newly created paths. The network is such that it has loose clock synchronization. Per-hop distance is calculated by the source is also sent in the packet header. Each node in the path which receives the packet has to compare its calculated distance with the value that is present in the packet header. As a final check they test the number of appearances if there is a suspicious route in the routing table.

Modirkhazeni et al. [21] proposed neighbor discovery technique for handling wormhole attack. They look for data from unauthorized nodes/neighbors. It is assumed that nodes are static and number of nodes is fixed and every node identifies its authorized neighbors in initial stage and later rejects data from all nodes which are not authorized neighbors. The technique is quite effective in cases where we have static and fixed number of nodes. But it is not flexible in case where one need mobility and has no scalability.

The study by [22], introduced a protocol called Multi-path Hop-count Analysis (MHA), it is based on hop-count analysis to avoid the wormhole attack. Presumed that, too high or low of hop count is not fit well for the network. The novelty of the hop-count analysis in detecting wormholes, may be considered other similar works was issued before such as; [23].

In the method introduced by [24], the aim is detection of suspicious link and confirm them in the two steps; first, HELLO packet transmitted to all node located in transmission range. After HELLO request is received, node stores the senders address and delay time until next HELLO packet reached. For piggyback reply, the node adds the source recorded address and value of delay time. When destination node received the HELLO reply, the packet is checked and waits for information related to any outstanding requests. If there is no information available, then it treats as any other control packets.

MOBIWORP introduced by[25]. It is a neighbor monitoring based protocol in which nodes monitor the activities performed by their neighbors. Local monitoring is done by nodes, there is a central authority (CA) which is responsible for global monitoring and converge feedback is provided by the guard nodes. CA is likewise responsible for handshake and key exchange with mobile nodes. Each mobile node has a key shared with the CA. Every node keeps a list of its two hop neighbors. MOBIWORP is highly dependent upon neighbor communication and requires extra processing.

Most of previous related works are using different techniques to detect and prevent wormholes, these techniques are; neighbor discovery/verification based, time to live based, round trip time based, packet leashes based, clock based, and hardware based. Literature review reveals that none of the solutions proposed in the literature is perfect. In fact every solution takes only one dimension of the wormhole attack detection process for example if one solution doesn't need extra hardware it may require tight time synchronization which is itself a tough ask. On the other hand if a solution doesn't
need extra hardware and time synchronization both, it cannot detect both types of wormhole attacks (Hidden + exposed).

4. WORMHOLE ATTACKS

It is a severe attack in ad hoc networks where two malicious nodes form a virtual channel among them [19], [26]. Attackers pass the packet through virtual channel and replay them into the network. It can be launched even if the network communication uses cryptographic techniques. Wormhole may exists at bit level (the reply is done bit by bit even earlier than the whole packet arrived), same as cut through routing by [27] or at physical layer [28], [26].

In fact, nodes around the wormhole antenna realize that they can transmit packets with other wireless nodes located next to the other antenna and consider them as immediate neighbors. Lunching wormhole attack can be done easily. It is not depend on Medium Access Control (MAC)

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

layer protocol and cryptography techniques are not enough to prevent it, as wormhole attackers do not create separate packets, but simply replay packets that already exist on the network by passing all cryptographic checks [29], [30]. It is due to the wormhole attacker no needs to break into wireless nodes or realize the mechanism of communication used by the network.

The packets can be transmitted over the wormhole link and reach to destination without any changes or dropping of any packets, the existence of wormhole is not harmful, and even have benefit by enhance the network connectivity and makes a shorter path to transfer packets between sender and receiver otherwise far off area. If the distance of tunnel is longer than transmission range, nodes near the wormhole antenna look for faster and shorter reliable paths by using the wormhole tunnel. Wireless networks running any dissimilarities of shortest path routing will find out this kind of paths and finally use them to broadcast data.

Wormhole attack turn off and on the signal replayed by the adversary and it completely changes the network connectivity and then suddenly creates or destroys many of shortest paths in the network and upset most of routing protocols. Wormhole can get the RREQ packet through the tunnel and then play a denial of service attack by ignoring to broadcast any packets in on-demand routing protocols.

In routing protocols which discover neighbors, the attacker can do frequent neighbor and path changes, it makes nodes consume the energy and wastes communication bandwidth. When the wormhole node is exist, it replay the scheme, mostly wormhole used to obtain network traffic, then spoof the packets, drop packets, or act as man in the middle attacks. In this way, when the traffic gathered, it helps to break encryption and security mechanisms of the network. Impact of wormhole attack is measured in terms of number of pairs whose shortest paths are affected.

Wormhole attacks have more impact, when two antennas are placed far apart, because of more paths and more traffic in the network; as a result, more damages are done to the transmitted packets by the wormhole link. In Figure 2 two red nodes N1 and N2 are wormhole and the dotted line connects two nodes is a long wormhole link. The blue nodes are normal nodes and they consist more hops to transmit packets to destination.

When the attack happens, nodes located in area A consider nodes in area B as neighbors and vice versa. Overall, to messing up with the routing protocols, by using wormholes, adversary able to break any protocol relies on geographic proximity [31]. At the same time, every single one of localization algorithms which employ network connectivity would fail by the alteration of the network topology based on wormhole links.

It can be the main impact of wormhole, due to its position which can be exploited as a useful function in numerous application as well as protocols. On the other hand, out of band location systems like Global Positioning System (GPS) cannot be accessible or unusable because of the environment [32] [33].

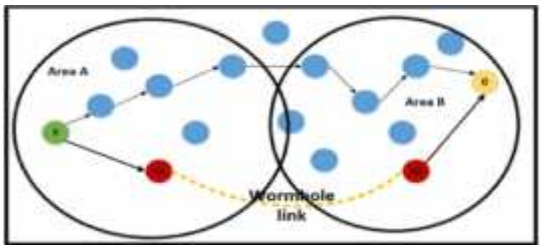

Figure2: Demonstration of Wormhole Attack

5. CLASSIFICATION OF WORMHOLES

The Wormholes can be broadly divided into two different types: exposed and hidden wormholes. During hidden attacks, wormhole attacker nodes do not update packets headers as they should, so other nodes do not realize the existence of them, as referring to Figure 3, a packet sent by source node is overheard by wormhole node M1, node M1 transmits that packet to second wormhole node M2 which in turn replays the packet into the communication network. In this way it seems D and S are neighbors although they are out of radio range. In this kind of attack, a path from S to D via wormhole attacker link will be:

$$S \rightarrow A \rightarrow B \rightarrow D$$

During exposed attacks, wormhole nodes do not make any alteration in the content of packets instead they include their identities in the packet header to be considered as trustworthy nodes.

Journal of Theoretical and Applied Information Technology
10th September 2015. Vol.79. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Therefore, other nodes are aware of the wormhole node existence but they do not know wormhole nodes are attacker. In scenario if the attack is revealed (Figure 3), the path from S to D via wormhole will be:

$$S \rightarrow A \rightarrow M1 \rightarrow M2 \rightarrow B \rightarrow D$$

Other classifications of wormholes are; wormhole based on launched types and based on visibility of wormhole.

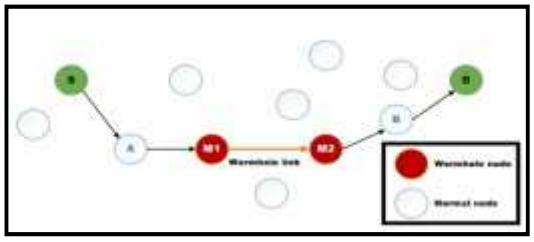

Figure 3: Hidden and Exposed Wormhole

5.1. Based on Launch Type: First we review the wormhole attack based on launch type, where it can be launched by five ways:

Wormhole Using Encapsulation: In between two nodes, a tunnel is generated, through this path the RREQ messages were received to node A (Figure 4) then it receives the RREQ messages and transmits them to the other nodes till they reach to the sink node. In wormhole attacks based on encapsulation, numerous internal nodes present among two malevolent nodes. Since received data packets do not increase the actual hop count during the traversal through wormhole link. At one wormhole edge point the data packets are received and then forwarded via the wormhole link [34], [24]. At the other end of wormhole, the data packets are received and broadcasted to its neighbors.

In Figure 4, source node (S) and sink node (SI) want to determine the lesser path among themselves when the network is threatened by two malicious nodes M1and M2. While the sender node broadcast a RREQ message, M1 node receives the RREQ and receives the data packet forwarded to M2 by the wormhole link located among both malicious nodes M1 and M2. The data packet received by node M2 is retransmitted. As mentioned earlier, the hop count does not increase when the transmission is carried out between M1 and M2.

Simultaneously, a duplicated RREQ transmits as a source to sink through path contains nodes A, B, and C. At this time, two routes are available starting from S to sink; first route has four hops size long starts from node S, continue to nodes "A,B,C" then reach to the sink node, another route consist three hops away again start from node S, and then pass through two malicious nodes M1, and M2, and reach the sink. In this case, the sink selects to transmit from the second path due to shortest path.

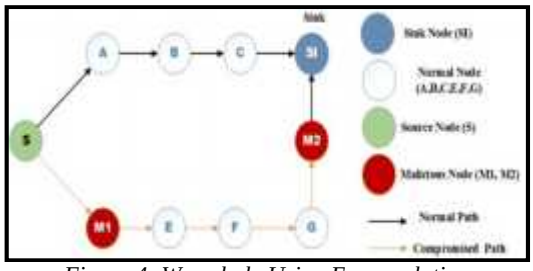

Figure 4: Wormhole Using Encapsulation

Out of Band Wormhole Channel/ High-quality: RREQ packets are transmitted between a straight wired links. An alternate is to use a link with long range directional wireless. In this model, the wormhole attack is launched and possess a single hop, high quality, and out of band link among the malicious nodes [35], [36]. This type of attack needs specialized hardware capability. Figure 5 demonstrates two malicious nodes connected by out of band channel connecting themselves. Let us assume that source node forward a RREQ to sink node and sink node gets two RREQs: starts from source node, continue to both malicious nodes M1 and M2 at the end reach to sink node, and another route again starts from source node and continue to pass three nodes A, B, and C and reach to destination; the earliest route has shorter path as well as faster due to use wormhole tunnel, and hence the sink node chooses the traversal.

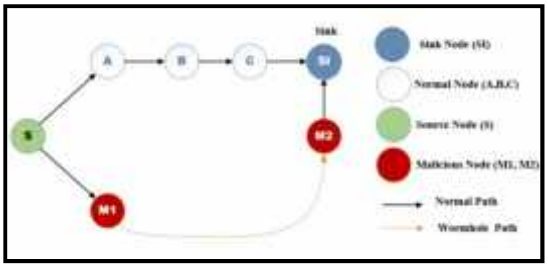

Figure5: Wormhole Attack Using Out of Band Channel

Wormhole with High Power Transmission:

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

RREQ packet is received by the node, later the node transmits the packet at high level of power. When node receives the high power broadcasts, it rebroadcasts the RREQ packet to reach to the destination node [37], [38].

In the network, only one malicious node exists, this node has capability of high power transmission. Malicious node is able to communicate from a far distance with all genuine nodes. When the RREQ packet received by the malicious node, it transmits by the request at high power level. When each node receives RREQ packet, transmits the RREQ to the neighbor nodes until reach to destination. RREQ is able to relieved when every one of nodes are correctly calculate the collected signal strength.

Wormhole Using Packet Relay: Nodes transmit the packets among two distinct nodes to compromise genuine nodes as attacker nodes are neighbors. In this model, an attacker transmits data packets of two faraway nodes to persuade nodes which attackers are legal neighbors. As shown in Figure 6, when having some cooperated malicious nodes, nodes can be victims of the attack due to they are multiple hops away from each other [5], [39]. Node A and node B are two non-neighboring nodes with a malicious neighbor node M1. Figure 6a node M1 can relay packets between nodes A and B to make them believe that they are neighbors. As shown in Figure 6b if there are several cooperating malicious nodes, nodes that are multiple hops away from each other can be victims of this attack.

Wormhole Using Protocol Deviations: When the RREQ message is transmitted all other nodes naturally back off for a random amount of time earlier than transmitting reduce MAC layer collision, on the other hand, nodes in this type of attack do not back off to let RREQ message arrive to destination. The routing protocols which based on the shortest delay rather than the smallest hop count is at risk of wormhole attacks which use the protocol distortion. Table 1 shows the summary and comparison between wormhole attacks models from attacker perspective.

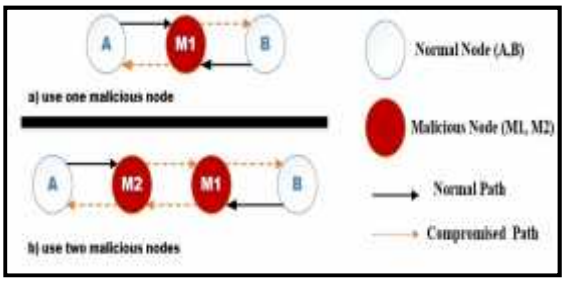

Figure 6: Wormhole Attack Using Packet Relay

5.2. Depend on Visibility of Attacker

The classification of such attacks will facilitate the design of detection methods. According to whether the attackers are visible on the route, we classify the wormholes into three types [40]:

5.2.1 Open Wormhole Attack: The attackers include themselves in the RREQ packet header following the route discovery procedure. Other nodes are aware that the malicious nodes lie on the path but they would think that the malicious nodes are direct neighbors. In the following figures M1 and M2 to represent the malicious nodes, S and D represent the good nodes as source and destination, and A, B, etc. as the good nodes on the route. In Figure 7, the malicious nodes M1 and M2 perform a wormhole attack tunneling the traffic sent by the source S to the destination D.

5.2.2 Half Open Wormhole Attack: One side of wormhole does not modify the packet and only another side modifies the packet, following the route discovery procedure. In Figure 8, the beacons of the compromised node M1 are tunneled towards the external malicious node M2 and the beacons of the M2 neighbors are tunneled back towards M1.

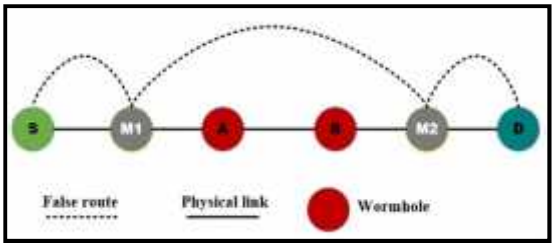

Figure7: Open Wormhole Attack

5.2.3 Closed Wormhole Attack: The attacker's are not modifying the content of the packet, even in a route discovery packet. Instead, they simply tunnel the packet from one side of wormhole to another side and it rebroadcasts the packet. In Figure 9, the neighbor discovery beacons are

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

tunneled between M1 and M2 without adding any self information. Thus, S and D believe that they are neighbors. The malicious nodes are external agents such as simple transceivers that can stay invisible for S and D.

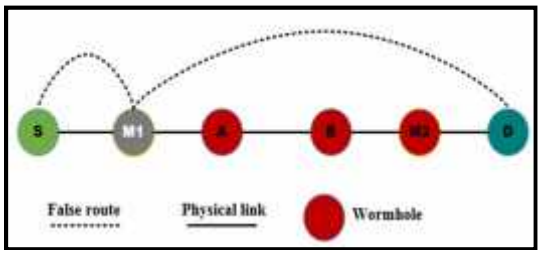

Figure 8: Half Open Wormhole Attack

6. THREATS OF WORMHOLE ATTACK

Wormhole is a serious threat to the network and has the ability to cause:

Alterations in Network and Base Station Deceptions: due to the identity deception, attacker may interfere with nodes and cause damage, drop or misdirect messages, create traffic collision or jam the communication channel [41].

Results in Routing Information Corruption: a wormhole attack is a collaborative attack because there are more than one attacker involved. It is a network layer attack because it occurs at the network layer and disrupts routing information [42].

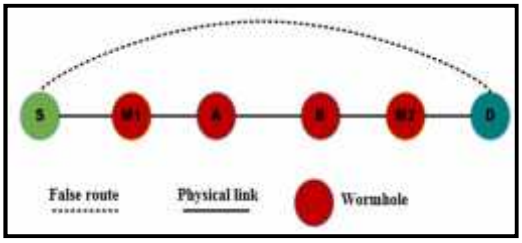

Figure 9: Closed Wormhole Attack

Can be Launched Upon any of the Current Routing Protocols: wormhole is not depend on routing protocol type and can be lunch in any of routing protocols e.g. DSR, AODV etc [43].

Can Penetrate Wrong Route/Topology Information Into the Network, Thereby, defeating the purpose of routing algorithms [18].

Can Launch Number of Other Attacks: The type of wormhole attack that allows the attackers to launch a number of other attacks such as black hole, grey hole, DOS, and sinkhole [44].

The summary of wormhole attacks are available in Table 1 at the end of the paper.

7. EFFECTS OF WORMHOLE ATTACK

Results of wormhole success can be very devastating. There are a lot of effects mentioned in the literature that can happen due to wormhole presence in the network.

I. The effects are; gain unauthorized access, disrupt routing, launch DoS, launch the grey-hole, black-hole attacks, and launch cryptanalysis attacks.

Gain Unauthorized Access: In the scenario of an internal attack where the malicious node within the network gains unauthorized access and impersonates as if it is a genuine node. Moreover, it can analyze the traffic in the network in between other nodes and may also take part in other activities within the network [45], [46].

Disrupt Routing: In a routing disruption attack, the attacker attempts to cause legitimate data packets to be routed in nonfunctional ways [47] [48].

Launch DoS: Currently, MANET's use IEEE 802.11 medium access control (MAC) protocol as the link layer protocol. The studies it was known that the IEEE 802.11 MAC is vulnerable or prone to DoS attacks which makes use of its binary exponential back-off scheme. As it is known that a successful transmission leads to a smaller contention window. Therefore, a node which is constantly transmitting has the capability to capture the channel conveniently at all times causing other nodes in the network to back off endlessly [49], [50].

Launch the Grey-hole, Black-hole Attacks: The wormhole attack is a great threat to network routing protocols in ad hoc networks. As the tunneled distances are usually greater in length compared to wireless transmission which are often limited to the range of a single hop. So the source can choose the path which includes the attack nodes. There are different types of attacks which can be attempted by the attack nodes, like the black hole attacks (by dropping all data

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

packets) and grey hole attacks (by selectively dropping packets) [51].

Launch Cryptanalysis Attacks: In the scenario of the network traffic is routed through the wormhole even once, it given the capability to the attacker to gain full management control over the traffic. After this it will begin its malicious actions which can be various. For instance, selection dropping data packets which pushes the network throughput to lower down or to store critical information regarding the traffic and later exploit it to perform cryptanalysis attacks [52].

II. At the end genuine paths cannot be found: due to use the wormhole link the nodes cannot detect and use genuine paths [53].

III. Some nodes might get isolated from whole network and will not be able to communicate at all [54].

8. IMPACTS OF WORMHOLE ATTACK

Once a successful wormhole attack is launched there are certain symptoms that can be observed in the network. The following are some of the symptoms mentioned in the literature.

Abrupt Decreases in Hops: When the wormhole attack is lunched and creates the link and attracts the packets to transfer so it cause of decrease in hops due to use long distance channel instead of using many hops. [55], [56].

Abrupt Increase in Path Delays: Some of the paths may not follow the advertised false-link, yet they may use some nodes involved in the wormhole attack. This will lead to an increase in hop delay due to wormhole traffic and subsequently an increase in end-to-end delay on the path [57].

Longer Propagation Delays: MANET is vulnerable to malicious attacks due to the high bit error rates, longer propagation delays, and low bandwidth, when the packet wants to transmit by wormhole, it may receive the packet and because of delay to transmit the packet [58].

Decrease in Network Utilization: when the packets are transfer through the wormhole link it cause of decrease network utilization due to use wormhole tunnel as transmission channel and the other routes are free. [59].

***One Link Getting Higher Usage Ratio Than Others*:** In the routing process, the wormhole link participates in more number than the normal link. A link can be checked whether it participates in the routing very often [30]. The wormhole link is participating to transmit the packets and as this link is shortest and able to transmit the packets faster so it has higher usage.

Reception of Data From a Far Apart Node: Wormhole attackers can make far apart nodes believe they are immediate neighbors, and force all communications between affected nodes to go through them [18].

9. Best Detection Method

After doing research and read the proposed work previously issued, we found that, major points of an ideal wormhole solution are;

***A) Minimal Change to Existing Implementations by*;**

• **Use already available information:** Check the previous information and find how the previous methods solve the problem and if able to combine the previous method or part of the method with the current work to improve the method [60].

• **Minimize use of extra information:** Look for a new method which is not proposed yet and create a new detection method [61].

***B) Protocol Independence*:** A solution that can detect wormhole independent of the protocol type [62].

***C) No Extra Hardware*:** A solution without dependency to any additional hardware [20] [63].

***D) No Time Synchronization*:** A solution that will not require tightly synchronized clocks [63] [64].

***E) Intelligent Nodes*:** Mobile nodes with the ability to detect/mitigate wormhole by themselves [65] [66].

***F) Detect all Types of Wormholes*:** Need to detect both types of wormhole attacks (e.g. hidden and exposed) [67] [66].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

***G) Avoid/prevent, Detect and Mitigate*:** Most of the solutions, avoid detect or mitigate. Most of them do not take into account all the three dimensions. In the first line of action we need to prevent wormholes i.e. do not allow them to occur at all (Avoid). Then we need to detect it; in case a wormhole was already present in the network (detect). And when wormhole found we need to eliminate the attackers i.e. we need to detect the attackers also and neutralize the effects of wormhole attack (mitigate) [68] [20].

10. CONTRIBUTION

This research deals with detection of wormhole attack in MANETs. Authors are look for make improvement of wormhole detection rate and improve QoS factors such as Packet delivery Ratio, Packet Overhead, Average delay and throughput to come with better defence mechanism against wormhole attacks. Authors currently evaluate a proposed work and find the lack of that algorithm. Then doing some improvement that related works by the adding some more steps. Authors are proposing a defence mechanism to detect both types of wormholes attack in MANET and in four different scenarios with different density in terms of number of nodes. First authors study and analysis the results of their proposed algorithm when hidden wormhole attack exists in network, then study exposed wormhole attack in network. After that study and analysis the existence of both wormholes in network, and not existents of wormhole attack in network. Authors are evaluating many previous related works and come with new idea, by combining two methods and new defence mechanism.

11. CONCLUSION

MANETs are applicable in different scenarios, but the development of the hardware infrastructure and the networking software, especially the security protection, is not meeting the demand. The results from the previous methods demonstrate that an appropriate MANET routing protocol should have the following qualities like, being reactive, anonymous and stateless. For Wormhole attack, number of methods presents that is usable in the network. All of these methods have their own positive and negative points. It is very important to analyze carefully the effect of wormhole attack to control the risks of it. It would also be helpful to propose a novel and stronger wormhole attack countermeasure. For the exposed wormhole problem we can detect it by using Routing Table and neighbor verifications. And for the hidden type of wormhole attack we can use a combination of Received Signal Strength Indicator (RSSI) and the Round Trip Time (RTT). We know that obtaining a complete solution will add some costs, what we will be doing in future is to asses these costs and compare with our solution to existing solutions. In fact every solution takes only one dimension of the wormhole attack detection process for example if one solution doesn't need extra hardware it may needs tight time synchronization which is itself a tough ask. On the other hand if a solution doesn't need both; extra hardware and time synchronization, it can detect both types of wormhole attacks (hidden and exposed). In future we are going to develop and design effective defense mechanism to detect and prevent other types of attacks simultaneously.

ACKNOWLEDGMENT

The authors would like to thank the Faculty of Computer Science and Information Technology (CSIT), University Putra Malaysia (UPM) for supporting this research. This research is part of Master by research and funded under Fundamental Research Grant Scheme (FRGS) number FRGS-08-02-13-1364FR.

REFERENCE

[1] 1. Nakamura, M., A. Sakurai, and J. Nakamura, *Autonomic Wireless Sensor/Actuator Networks for Tracking Environment Control Behaviors.* International Journal of Computer Information Systems and Industrial Management Applications, 2009. **1**: p. 125-132.

[2] 2. Amanowicz, M., et al. *A trust-based information assurance mechanism for military mobile ad-hoc networks*. in *Microwaves, Radar, and Wireless Communication (MIKON), 2014 20th International Conference on*. 2014. IEEE.

[3] 3. Pal, S., et al. *M-learning in university campus scenario-Design and implementation issues*. in *Industrial Technology (ICIT), 2013 IEEE International Conference on*. 2013. IEEE.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[4] 4. Smys, S. and G. Josemin Bala, *Efficient self-organized backbone formation in mobile ad hoc networks (MANETs).* Computers & Electrical Engineering, 2012. **38**(3): p. 522-532.
[5] 5. Sharma, P. and A. Trivedi. *An approach to defend against wormhole attack in ad hoc network using digital signature*. in *Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on*. 2011. IEEE.
[6] 6. Zhao, J. and K.E. Nygard. *A Two-Phase Security Algorithm for Hierarchical Sensor Networks*. in *FUTURE COMPUTING 2011, The Third International Conference on Future Computational Technologies and Applications*. 2011.
[7] 7. Bindra, H.S., S.K. Maakar, and A. Sangal, *Performance evaluation of two reactive routing protocols of MANET using group mobility model.* International Journal of Computer Science, 2010. **7**(3): p. 38-43.
[8] 8. Dong, H., et al., *Multi-Hop Routing Optimization Method Based on Improved Ant Algorithm for Vehicle to Roadside Network.* Journal of Bionic Engineering, 2014. **11**(3): p. 490-496.
[9] 9. Kaur, H., R. Vohra, and R.S. Sawhney, *Multi Hop Routing in Wireless Mobile Networks using Ant Colony Optimization.* 2013.
[10] 10. Upadhyay, S. and B.K. Chaurasia, *Detecting and Avoiding Wormhole Attack in MANET Using Statistical Analysis Approach*, in *Advances in Computer Science and Information Technology. Networks and Communications*. 2012, Springer. p. 402-408.
[11] 11. Yamini, K. and T. Arivoli. *Improved location-free topology control protocol in MANET*. in *Automation, Computing, Communication, Control and Compressed Sensing (iMac4s), 2013 International Multi-Conference on*. 2013. IEEE.
[12] 12. Wang, B., X. Chen, and W. Chang, *A light-weight trust-based QoS routing algorithm for ad hoc networks.* Pervasive and Mobile Computing, 2013.
[13] 13. Sudarsan, M.S., M. Vinodhini, and D.S. Karthik, *Enhancing Key Management In Intrusion Detection System For Manets.* International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 2012. **1**(8): p. pp: 219-222.
[14] 14. Enshaei, M., Z.M. Hanapi, and M. Othman, *Vulnerability and Routing Protocols.* 2014.
[15] 15. Banerjee, S. and K. Majumder, *WORMHOLE ATTACK MITIGATION IN MANET: A CLUSTER BASED AVOIDANCE TECHNIQUE.* International Journal of Computer Networks & Communications, 2014. **6**(1).
[16] 16. Rawat, C., *Wormhole Attack Detection Protocol using Time Stamp with Security Packet.* International Journal of Computer Science and Information Technologies, 2014. **5**(1): p. 621-626.
[17] 17. Ahuja, R., A.B. Ahuja, and P. Ahuja. *Performance evaluation and comparison of AODV and DSR routing protocols in MANETs under wormhole attack*. in *Image Information Processing (ICIIP), 2013 IEEE Second International Conference on*. 2013. IEEE.
[18] 18. Malhotra, A., D. Bhardwaj, and A. Garg. *Wormhole attack prevention using clustering and digital signatures in reactive routing*. in *Networking, Sensing and Control (ICNSC), 2012 9th IEEE International Conference on*. 2012. IEEE.
[19] 19. Anitha, P. and M. Sivaganesh, *Detection and Prevention of Wormhole Attack in MANETS using Path Tracing.* International Journal of communications and networking systems, 2012. **1**(2).
[20] 20. Sakthivel, T. and R. Chandrasekaran, *Detection and prevention of wormhole attacks in MANETs using path tracing approach.* European Journal of Scientific Research, 2012. **76**(2): p. 240-252.
[21] 21. Modirkhazeni, A., et al., *Mitigation of Wormhole Attack in Wireless Sensor Networks*, in *Trustworthy Ubiquitous Computing*. 2012, Springer. p. 109-147.
[22] 22. Jen, S.-M., C.-S. Laih, and W.-C. Kuo, *A hop-count analysis scheme for avoiding wormhole attacks in MANET.* Sensors, 2009. **9**(6): p. 5022-5039.
[23] 23. Djenouri, D., et al. *On securing manet routing protocol against control packet dropping*. in *Pervasive Services, IEEE International Conference on*. 2007. IEEE.
[24] 24. Naït-Abdesselam, F., *Detecting and avoiding wormhole attacks in wireless ad hoc networks.* Communications Magazine, IEEE, 2008. **46**(4): p. 127-133.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[25] 25. Khalil, I., S. Bagchi, and N.B. Shroff, *MOBIWORP: Mitigation of the wormhole attack in mobile multihop wireless networks.* Ad Hoc Networks, 2008. **6**(3): p. 344-362.
[26] 26. Eriksson, J., S.V. Krishnamurthy, and M. Faloutsos. *Truelink: A practical countermeasure to the wormhole attack in wireless networks.* in *Network Protocols, 2006. ICNP'06. Proceedings of the 2006 14th IEEE International Conference on*. 2006. IEEE.
[27] 27. Wang, P., et al., *A Comprehensive Comparison between Virtual Cut-through and Wormhole Routers for Cache Coherent Network On-chips.* IEICE Electronics Express, 2014. **11**(14).
[28] 28. Danev, B., D. Zanetti, and S. Capkun, *On physical-layer identification of wireless devices.* ACM Computing Surveys (CSUR), 2012. **45**(1): p. 6.
[29] 29. Tellez, F. and J. Ortiz, *Behaviour of Elliptic Curve Cryptosystems for the Wormhole Intrusion in Manet: A Survey and Analysis.* IJCSNS International Journal of Computer Science and Network Security, 2011. **11**(9): p. 1-12.
[30] 30. Keer, S. and A. Suryavanshi. *To prevent wormhole attacks using wireless protocol in MANET.* in *Computer and Communication Technology (ICCCT), 2010 International Conference on*. 2010. IEEE.
[31] 31. Zhang, W., et al., *Security issues in wireless mesh networks*, in *Wireless Mesh Networks*. 2007, Springer. p. 309-330.
[32] 32. Dhurandher, S.K., et al. *E2siw: An energy efficient scheme immune to wormhole attacks in wireless ad hoc networks.* in *Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on*. 2012. IEEE.
[33] 33. Keerthi, T.D.S. and P. Venkataram. *Locating the attacker of wormhole attack by using the honeypot.* in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on*. 2012. IEEE.
[34] 34. Veríssimo, P.E., *Travelling through wormholes: a new look at distributed systems models.* ACM SIGACT News, 2006. **37**(1): p. 66-81.
[35] 35. Hong, L., et al. *Grey theory based reputation system for secure neighbor discovery in wireless ad hoc networks.* in *Future Computer and Communication (ICFCC), 2010 2nd International Conference on*. 2010. IEEE.
[36] 36. Alshamrani, A.S. *PTT: packet travel time algorithm in mobile ad hoc networks.* in *Advanced Information Networking and Applications (WAINA), 2011 IEEE Workshops of International Conference on*. 2011. IEEE.
[37] 37. Buch, D.H. and D. Jinwala, *Prevention of wormhole attack in wireless sensor network.* arXiv preprint arXiv:1110.1928, 2011.
[38] 38. Hai, T.H., E.N. Huh, and M. Jo, *A lightweight intrusion detection framework for wireless sensor networks.* Wireless Communications and mobile computing, 2010. **10**(4): p. 559-572.
[39] 39. Nouri, M. and S.A. Aghdam. *Collaborative techniques for detecting wormhole attack in MANETs.* in *Research and Innovation in Information Systems (ICRIIS), 2011 International Conference on*. 2011. IEEE.
[40] 40. Marianne Azer, S.E.-K.M.E.-S., *A Full Image of the Wormhole Attacks.* 2009.
[41] 41. Meghdadi, M., S. Ozdemir, and I. Güler, *A Survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Networks.* IETE Technical Review (Medknow Publications & Media Pvt. Ltd.), 2011. **28**(2).
[42] 42. Maheshwari, R., J. Gao, and S.R. Das. *Detecting wormhole attacks in wireless networks using connectivity information.* in *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*. 2007. IEEE.
[43] 43. Shamaei, S. and A. Movaghar, *A Two-Phase Wormhole Attack Detection Scheme in MANETs.* The ISC International Journal of Information Security, 2015. **6**(2).
[44] 44. Modirkhazeni, A., S. Aghamahmoodi, and N. Niknejad. *Distributed approach to mitigate wormhole attack in wireless sensor networks.* in *Networked Computing (INC), 2011 The 7th International Conference on*. 2011. IEEE.
[45] 45. Satheeshkumar, M.B. and M.R. Kalaivani, *Privacy Protection Against Wormhole Attacks In Manet.* traffic, 2014. **2**(1).
[46] 46. Goyal, P., V. Parmar, and R. Rishi, *Manet: Vulnerabilities, challenges, attacks, application.* IJCEM International Journal of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Computational Engineering & Management, 2011. **11**(2011): p. 32-37.

[47] 47. Maan, F., Y. Abbas, and N. Mazhar. *Vulnerability assessment of AODV and SAODV routing protocols against network routing attacks and performance comparisons*. in *Wireless Advanced (WiAd), 2011*. 2011. IEEE.

[48] 48. Nagrath, P. and B. Gupta. *Wormhole attacks in wireless adhoc networks and their counter measurements: A survey*. in *Electronics Computer Technology (ICECT), 2011 3rd International Conference on*. 2011. IEEE.

[49] 49. Jhaveri, R.H., S.J. Patel, and D.C. Jinwala. *DoS attacks in mobile ad hoc networks: A survey*. in *Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on*. 2012. IEEE.

[50] 50. Hu, Y.-C., A. Perrig, and D.B. Johnson, *Wormhole attacks in wireless networks.* Selected Areas in Communications, IEEE Journal on, 2006. **24**(2): p. 370-380.

[51] 51. Reddy, K.G. and P.S. Thilagam, *Taxonomy of Network Layer Attacks in Wireless Mesh Network*, in *Advances in Computer Science, Engineering & Applications*. 2012, Springer. p. 927-935.

[52] 52. Alcaraz, C. and J. Lopez, *A security analysis for wireless sensor mesh networks in highly critical systems.* Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on, 2010. **40**(4): p. 419-428.

[53] 53. Reddy, K.G. and P.S. Thilagam, *Intrusion detection technique for wormhole and following jellyfish and byzantine attacks in wireless mesh network*, in *Advanced Computing, Networking and Security*. 2012, Springer. p. 631-637.

[54] 54. Lu, X., D. Dong, and X. Liao. *WormPlanar: Topological Planarization Based Wormhole Detection in Wireless Networks*. in *Parallel Processing (ICPP), 2013 42nd International Conference on*. 2013. IEEE.

[55] 55. Khainwar, R.S., A. Jain, and J.P. Tyagi, *Elimination of Wormhole Attacker node in MANET using performance evaluation multipath algorithm.* Network and Complex Systems, 2013. **3**(7): p. 22-29.

[56] 56. Niranjan, P., et al., *Detection of wormhole attack using Hop count and Time delay analysis.* International Journal of Scientific and Research Publications, 2012. **2**(4): p. 1.

[57] 57. Anita, E.M., V. Vasudevan, and A. Ashwini. *A certificate-based scheme to defend against worm hole attacks in multicast routing protocols for MANETs*. in *Communication Control and Computing Technologies (ICCCCT), 2010 IEEE International Conference on*. 2010. IEEE.

[58] 58. Seo, J. and G. Lee, *An effective wormhole attack defence method for a smart meter mesh network in an intelligent power grid.* International Journal of Advanced Robotic Systems, 2012. **9**.

[59] 59. Yang, B., et al. *Message Scheduling on a Wormhole-Switched Linear Client-Server Network*. in *ISCA PDCS*. 2006.

[60] 60. Vijayalakshmi, S. and S. Albert Rabara, *Weeding Wormhole Attack in MANET Multicast Routing Using Two Novel Techniques-LP3 and NAWA2*. 2011.

[61] 61. Jain, S., T. Ta, and J.S. Baras. *Wormhole detection using channel characteristics*. in *Communications (ICC), 2012 IEEE International Conference on*. 2012. IEEE.

[62] 62. Sadeghi, M. and S. Yahya. *Analysis of Wormhole attack on MANETs using different MANET routing protocols*. in *Ubiquitous and Future Networks (ICUFN), 2012 Fourth International Conference on*. 2012. IEEE.

[63] 63. Venkataraman, R., et al., *A graphtheoretic algorithm for detection of multiple wormhole attacks in mobile ad hoc networks.* International Journal of Recent Trends in Engineering (IJRTE), 2009. **1**(2): p. 220-222.

[64] 64. Upadhyay, S. and A. Bajpai, *Avoiding Wormhole attack in MANET using statistical analysis approach.* International Journal on Cryptography And Information Security, 2012. **2**(1).

[65] 65. Hazra, S. and S. Setua, *Trusted Routing in AODV Protocol Against Wormhole Attack*, in *Future Information Technology, Application, and Service*. 2012, Springer. p. 259-269.

[66] 66. Zhang, T., J. He, and Y. Zhang, *Secure DV-Hop Localization against Wormhole Attacks in Wireless Sensor Networks*, in *Soft Computing in Information Communication Technology*. 2012, Springer. p. 33-38.

[67] 67. Hu, Y.-C., A. Perrig, and D.B. Johnson. *Packet leashes: a defense against wormhole*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

attacks in wireless networks. in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*. 2003. IEEE.

[68] 68. Khan, Z.A. and M.H. Islam. *Wormhole attack: A new detection technique*. in *Emerging Technologies (ICET), 2012 International Conference on*. 2012. IEEE.

[69] 69. Khalil, I., S. Bagchi, and N.B. Shroff. *LITEWORP: a lightweight countermeasure for the wormhole attack in multihop wireless networks*. in *Dependable Systems and Networks, 2005. DSN 2005. Proceedings. International Conference on*. 2005. IEEE.

[70] 70. Van Tran, P., et al. *Ttm: An efficient mechanism to detect wormhole attacks in wireless ad-hoc networks*. in *Consumer Communications and Networking Conference, 2007. CCNC 2007. 4th IEEE*. 2007.

[71] 71. Farooq, N., I. Zahoor, and S. Mandal, *Recovering from In-Band Wormhole Based Denial of Service in Wireless Sensor Networks.* 2014.

[72] 72. Khabbazian, M., H. Mercier, and V.K. Bhargava, *Severity analysis and countermeasure for the wormhole attack in wireless ad hoc networks.* Wireless Communications, IEEE Transactions on, 2009. **8**(2): p. 736-745.

[73] 73. Roy, D.B., R. Chaki, and N. Chaki, *A new cluster-based wormhole intrusion detection algorithm for mobile ad-hoc networks.* arXiv preprint arXiv:1004.0587, 2010.

[74] 74. Khurana, S. and N. Gupta. *FEEPVR: First End-to-End protocol to Secure Ad hoc Networks with variable ranges against Wormhole Attacks*. in *Emerging Security Information, Systems and Technologies, 2008. SECURWARE'08. Second International Conference on*. 2008. IEEE.

[75] 75. Khalil, I., S. Bagchi, and N.B. Shroff, *Liteworp: Detection and isolation of the wormhole attack in static multihop wireless networks.* Computer networks, 2007. **51**(13): p. 3750-3772.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1: Summary Of Wormhole Attacks

Wormhole types	Encapsulation	Out of Band	High Power	Packet Relay	Protocol Deviations
Attack mode launching method	Node encapsulates the route request and transmits it to colluding node which de-capsulate it and RREQ forwards [69], [24].	Nodes send RREQs between them by using a long range directional wireless link or a direct wired link [26], [70].	A node gets a RREQ then transmits at high power level, any node which hears that rebroadcasts it towards the destination [71], [72].	Nodes relay packets between two distant nodes to convince they are neighbors [73], [74].	Nodes do not back off to let the request packet, it forwards arrive first at destination [75].
Advantages	1- there is a smaller probability of RREQ being discarded than other RREQs which are repeatedly received by intermediate nodes 2- RREQ packet arriving to destination, does not keep middle nodes as hops, and then it appears to have passed through minimum number of hops.	1- Control packet arrives faster since there is no processing from middle nodes 2- It has less probability of being discarded than other RREQs which are repeatedly received by intermediate nodes 3- Control packets arriving at destination, middle nodes not use as hops, and then it appears to have passed through minimum number of hops.	1- Control packets arrive faster 2- It has less probability of being discarded than other RREQs which are repeatedly received by intermediate nodes 3- Control packet arriving to destination, middle nodes not use as hops, and then it appears to have passed through minimum number of hops. 4- no need for colluding nodes, and any node could do the job	1- Two nodes think they are neighbors although they are not, and every RREQ to be sent to neighbors will arrive to relay nodes invisibility. 2- Control packet seems to arrive using minimum number of hops	1- Control packet arrives faster
Disadvantages	1- Resources and time consumption in packet encapsulation and decapsulation	This type of attack is different to lunch than the previous one because of needs specialized hardware capability. 2- Also the time difference in control packets arrival could be very remarkable.	1- Needs high power 2- Also speed difference could be noticed	1- Relaying nodes spend resources for processing RREQ packets and hiding their IDs	1- Dose not necessarily provide the minimum number of hops, it is not reliable if collisions happen to give minimum speed

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Wormhole types	Encapsulation	Out of Band	High Power	Packet Relay	Protocol Deviations
Suitable case	Large number of intermediate nodes, need to avoid intermediate processing	Small network size which speed difference would not be remarkable	A network with very middle nodes between source to destination with wide network range	Victim nodes need at least two hops away.	Network with the number of nodes have big difference from small saving
Faced Challenges	1- Sends encapsulation packet to the proper colluding node, while having a predetermined path 2- if any intermediate node check the contents of the sent packet	1- Needs of special hardware and arrangements for out of band channels	1- not only enough energy needs to have, also power adjustments needed to make the transmitted RREQ go to some suitable neighboring nodes, else RREQ could go out of range of network	1- Insert malicious nodes at proper positions 2- Hide malicious names which does not appear on RREQ packet 3- choice of optimum number of relaying nodes depends on victim's distance 4-Communicat-ion between relaying nodes	1- Collision occur between transmissions of malicious nodes
Possible solutions	1- For the predetermined path to be established, colluding nodes could send RREQ packets to establish paths. 2- For the second challenge of node checking packets, complex attacks will solve it	Add special hardware and arrangements for out of band channels	Sends a RREQ with different power levels, malicious node will have a primary network. Then use the communication ranges, and number of hops to adjust its power according to the location of destination	Start to having large number of relaying nodes and then minimize them to get optimum performance with small number of malicious nodes and traffic conquer. Different relaying nodes distribution should also be tried with optimum number	A priority round robin schema for malicious nodes packets could be used