Impact Factor (SJIF): 4.542

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 4, Issue 4, April-2017

A Survey on Wormhole Attack in MANET

Jaydeep Pandya[1], Prof. Virendra Barot[2]
Sardar Vallabhbhai Institute of Technology, Vasad, Gujarat, India

Abstract – *MANET is a plethora of security. In MANET each node act as a router so trust among nodes in the network is important. Now a days Trust based secure routing protocol gained lots of researchers globally. In this paper a survey on wormhole attack in MANET Network Layer with its classification and few detection schemes are presented. Wormhole attack is all about fake a route so in compare to other attacks like blackhole it is difficult to launch and detect.*

Keywords – *MANETs: Wormhole, Security Attacks, Trust.*

I. INTRODUCTION

Wireless networks divided into two parts: 1. Infrastructure Based Network and 2. Infrastructure less Networks (Mobile Ad-hoc Networks). MANET is an autonomous system of mobile devices like laptops, smart phones, sensors etc. In MANET there is no centralized administration as it present, so all devices can't send message directly to the receiver. Each mobile node operates not only as a host but also acts as a router. Routing algorithm in MANET will guide each node how they can communicate each other in efficient manner. The main objective of routing protocol is to establish optimal path from source node to destination node in network. Generally MANET routing protocols broadly classified into two major categories: Proactive and Reactive.

Proactive Routing Protocols, as the name tells it will continuously (after some fix amount of time) identify the topology of the network by exchanging neighbor node information among the network nodes.

Reactive Routing Protocol, as the name states these protocols are called only when transmission is required. They are based on some sort of query-reply dialog, also known as On Demand Routing Protocol.

Hybrid protocols are the combinations of reactive and proactive protocols and takes advantages of both routing protocols and as a result, routes are found quickly in the routing zone.

The outstanding paper is organized as follows. Section II Taxonomy of wormhole attack. Section III Literature Survey of wormhole detection and prevention schemes. Section IV Conclusion and Future work.

II. TAXONOMY OF WORMHOLE ATTACK

In this section explain, the taxonomy of wormhole attack. In general wormhole attack is all about fake a route. Two or more malicious nodes are creates a virtual path which appears shorter than the original one. The attacking node captures packet from one end and tunnel it to the colluding node.

1. Packet Encapsulation [5-11]: In packet encapsulation mode malicious node captures the packet from legitimate source/intermediate node and encapsulates its header of the original packet, after that it forwards encapsulated packets towards another malicious node. This encapsulation prevents other/intermediate legitimate nodes from increasing actual hop counts. On receiving the encapsulated packet malicious node will convert into original form and broadcast it locally to the destination. After RREP by the receiver, during the actual data transmission attacker may drop all or some specific packets (based on size); perform man-in-the-middle attack. It is also known as in-band channel.

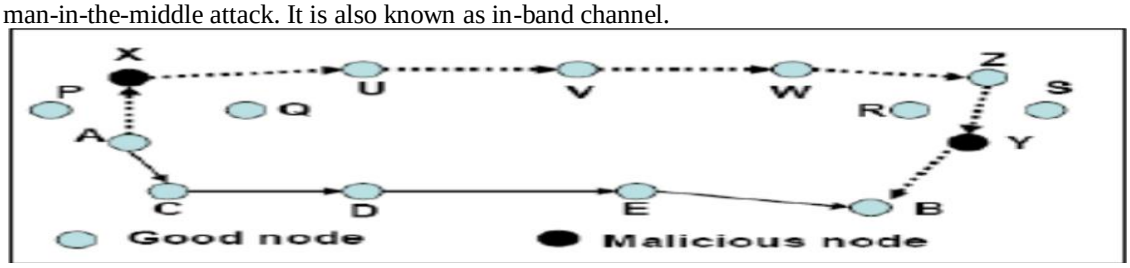

Figure 1. Packet Encapsulation

2. Out of band channel [5-11]: Out of band channel can be achieved by using a long-range directional wireless link or a direct wired link which is hidden from network. This mode of attack is more difficult to launch than the in-band/encapsulation, since it needs specialized hardware capability. Both malicious node can easily communicate with each other via this link and perform wormhole attack.

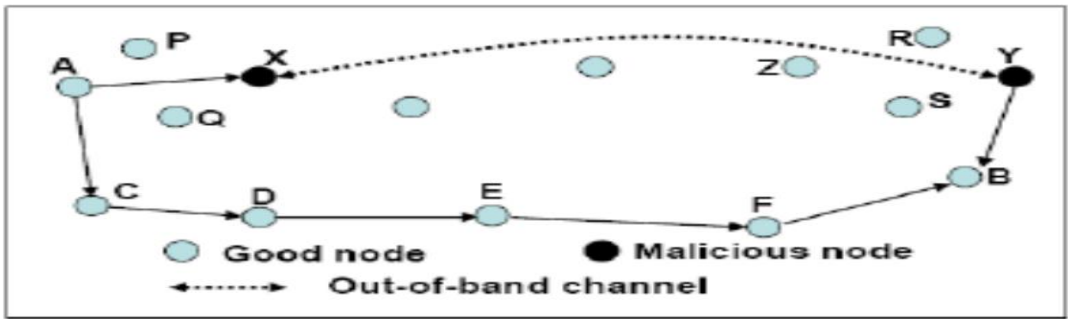

Figure2. Out of Band channel

3. High Power Transmission [5-11]: High power transmission, whenever a single malicious (wormhole) node gets a RREQ during route request, it will broadcasts the request at a high power level. Due to high-power rebroadcasts towards the destination wormhole node increases its chance to get involve in route. But this kind of attack easily gets detected as they have high transmission power than the rest nodes in the network.

4. Protocol Deviation [5-11]: Wormhole node can perform this attack in three ways: open wormhole attack, half open wormhole attack and close wormhole attack.

a. Open wormhole attack: In this type of wormhole attack, the attackers are actively taking part into the network and include themselves in the RREQ packet header. Other nodes in the network are aware that the node exists in the network but not as malicious nodes.

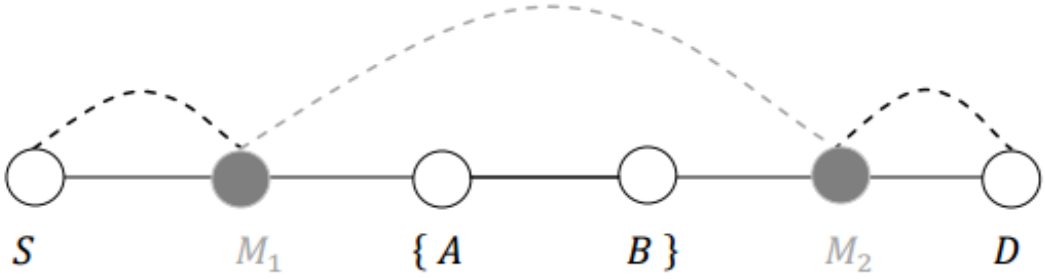

Figure 3. Open wormhole attack

b. Half Open wormhole attack: In this type of wormhole attack, one of the wormhole nodes does not modify the packet and only another end modifies the packet, following the route discovery procedure as shown in below figure. So only one node include itself in RREQ process where another one is in hidden from the network.

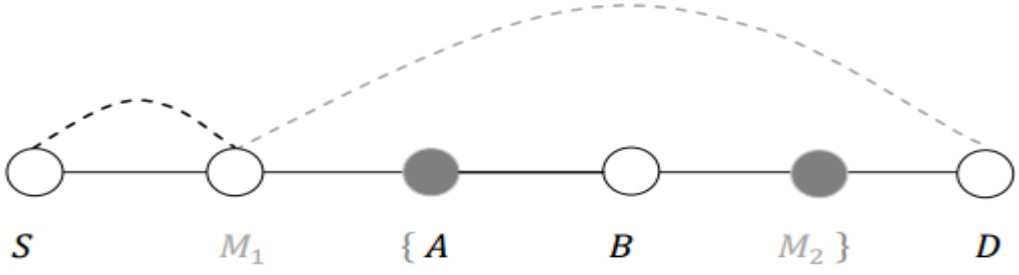

Figure 3. Half Open wormhole attack

c. Close wormhole attack: In this type, the attacker does not alter the RREP packet. They simply tunnel the packet form one end of wormhole to another end. At the second end malicious node will rebroadcasts packet locally.

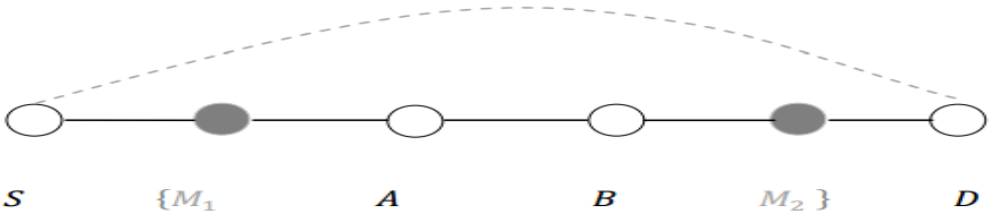

Figure 4. Close wormhole attack

III. LITERATURE SURVEY

1. **Packet Leashes:** A Defense against Wormhole Attacks in Wireless Networks: In 2003 packet leash method proposed by Yih-Chun Hu. This method used for defends against the wormhole attack. The packet leashes can be implemented two ways: a. geographic leash and b. temporal leash [12].

   A. **geographical leashes**: all nodes should have knowledge of its own location in the network and insecure synchronized clock. It is used for to identify that the sender node is within suitable distance or not. Whenever a sender sends RREQ packets, it includes its own recent location and transmission time in header. Based on this information receiver can easily predict the neighbor relation (by calculating the distance between itself and source). Geographical leashes are more advantageous than temporal leashes as they do not require a tightly synchronized clock. It has the limitations of GPS technology.

   Advantages: Used when tight clock synchronization not needed.
   Disadvantages: Limitation of GPS technology. Increase Computation and network overhead.

   B. **Temporal leashes**: all nodes are tightly synchronized clock. They calculate the expiration time of each packet by using light's velocity and append this expiration time in the packet's header. The maximum difference between any two nodes' clocks is bounded by Δ, and this value should be known to all the nodes. Destination compares its own arrival time and expiration time in the packet to detect the wormhole attack. If a packet receiving time exceed the expiration time, the packet is discarded.

   Advantage: Do not rely on GPS information, highly efficient when client used TIK.
   Disadvantages: All nodes require tight synchronization.

2. **Preventing replay attacks for secure routing in ad hoc networks:** Round Trip Time (RTT) mechanism is proposed by Jane Zhen and Sampalli in 2003. The RTT is the time that difference between the Route Request (RREQ) messages sending time from sender node to Route Reply (RREP) message receiving time from destination node. Sender will calculate the RTT between sender and all its neighbors. Because the RTT between two virtual neighbors is definitely higher than between two real neighbors. Sender can easily recognize both the virtual and real neighbors in the network. The main advantage of this mechanism is there is no need to obtain any special hardware. In this mechanism, each node calculates the RTT between itself and all its neighbors. However it cannot detect exposed attacks because fake neighbors are created in exposed attacks [13].

3. **DelPHI- Wormhole Detection Mechanism for Ad Hoc Wireless Networks**: The Delay per Hop Indicator (DelPHI) proposed by Hon Sun Chiu and King-Shan Lui in 2006. This method used for to detect both hidden and exposed wormhole attacks. In DelPHI, delay per hop (the delay time and length of each route are calculated and the average delay time per hop along each route) is computed. Based on this value nodes can predict about wormhole nodes. The route containing a wormhole link will have a greater Delay per Hop (DPH) value than the ideal one. It fails to detect the exact location of a wormhole, because the lengths of the routes are changed by every node, including wormhole nodes, wormhole nodes can change the route length in a certain manner so that they cannot be detected [14].

   Advantages: Synchronization doesn't need.
   Disadvantages: QoS is low because of delay is there.

4. **Securing MANET against Wormhole Attack using Neighbor Node Analysis**: In neighbor node approach analyses the entire neighbor node for the purpose of authentication, so that secure transmission can be occur over the wireless network. Sender will transmits RREQ packet using neighbor's public key so only legitimate neighbor able to decrypt it otherwise that node marked as bad node and removed from the

network, so exposed wormhole nodes can easily identified. This method is use request and response mechanism. Node will send a request to its all neighbor nodes. The node will maintain a table which store a reply time. If reply time is not accurate there is a harmful node in the current network. The response time of RREP message is compare to the response time of actual message sent. If response time of actual message is greater than the response time of RREP + threshold value than we can say that wormhole link is present in the route. Comparison of this process is repeated till the destination reached [15].

Advantages: Through put is increase Also Provide better efficiency.

Disadvantages: Not use for large network.

5. **WHOP- Wormhole Attack Detection Protocol using Hound Packet**: WHOP (Wormhole Attack Detection Protocol using Hound Packet), which is proposed by Saurabh Gupta, Subrat Kar and S Dharmaraja in 2011 based on AODV. In WHOP, a hound packet will be send after the route has been exposed using AODV routing protocol, the hound packet will be processed by every node except nodes who were involved in route from source to destination during path set up. WHOP contains other three column address of node processing bit (PB) and count to reach next hop (CRNH). CRNH represents the hop difference between neighbors of one hop separated node; its value will be increment by one after each node in processing bit of the packet [16].

Advantages: Doesn't require any hardware support and clock synchronization. It is used to avoid/detect both types of wormhole attack in-band and out of band.

Disadvantages: Network overhead is increase.

6. **WAP- Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks**:

a. Neighbor Node Monitoring during RREQ: During RREQ each node will monitor their neighbour node behavior. Neighbor table contain a RREQ sequence number, neighbor node ID, sending time and receiving time of the RREQ and count. By using this table information, nodes in the network monitor the activities of their neighbors and check for malicious behavior of the neighbors.

b. Wormhole Prevention Timer: The WPT is wormhole prevention timer will consider the maximum amount of time required for a packet to travels from a node to a neighbor node and back to the node. So if WPT is too small; the legitimate nodes can be excluded and on the other hand, if it is too large, it is difficult to detect wormhole attacks.

i. If the nodes are fixed like sensor node, the WPT is
WPT = (2 * Transmission Range) / Propagation speed of packet

ii. If the nodes have a mobility with an average velocity of Vn,
WPT = (2 * Transmission Range * Vn) / Propagation speed of packet

iii. When network are formed in the mobile environment, the WPT of nodes is given by
$WPT = (2 * \text{Transmission Range} * Vn) / (\text{Propagation speed of packet})^2$

c. Wormhole Route Detection: During RREP on receiving it from neighbor nodes, when a wormhole node sends a RREP to indicate that a colluding node is its neighbor, normal neighbor nodes of the wormhole node examine whether they have corresponding RREQ packet previously received from the node in their table. As show in in below figure a source node S broadcasts RREQ at time Ta, and then receives a RREP at time Tb; the source node can calculate the time delay per hop in the route by using hop count field in the RREP. The formula is given by

Delay per hop = (Tb – Ta) / Hop Count

Delay per hop <= WPT

Table 1: Comparison of Wormhole detection Prevention schemes

Title	**Author, Publisher and Year**	**Description**	**Outcome/ Future Scope**
Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks	Yih-Chun Hu, Adrian Perrig, David B. Johnson [16] - *IEEE* (2003)	1. Temporal Leashes: All modes must need strongly synchronized clock. It is based on off- the -shelf hardware. 2. It requires GPS hardware. In this method when one node send a packet to another node then it add its own location ps and time on which it sends a packet ts. The receiver compare the value of sending packet with its own location pr and time at which it receives packet tr.	Network overhead is increase.
Preventing Replay Attacks for Secure Routing in Ad Hoc Networks	J. Zhen and S. Srinivas [17] ADHOC-NOW (2013)	This paper presents a Round Trip time method to detect and prevent wormhole attack. Only sender node required for timings so not required to sync clock.	Exposed wormhole nodes not detected.
DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks	Hon Sun Chiu and King-Shan Lui [18] IEEE(2006)	It is based on the calculation of delay per hop value. Under normal condition, the delay a packet experiences in propagates one hop should be comparable along each hop path. While in wormhole attack, the delay for propagating across fake neighbors are high as there are many hops between them. It works for both In-Band and Out of –Band mode.	QoS is low because of delay is there.
Securing MANET against Wormhole Attack using Neighbor Node Analysis	Sweety Goyal, Harish Rohil [19] IJCA (2013)	In this method the entire neighbor node for the purpose of authentication, so that secure transmission can be occur over the wireless network. This method is use request and response mechanism. If response time of actual message is greater than the response time of RREP + threshold value than we can say that wormhole link is present in the route.	Better efficiency and throughput increase but not used for large networks.
WHOP: Wormhole Attack Detection Protocol using Hound Packet	Saurabh Gupta, Subrat Kar, S Dharmaraja [20] IEEE (2011)	WHOP is based on AODV. In WHOP, a hound packet will be send after the route has been exposed using AODV routing; this will processed by intermediate nodes. WHOP contains other three column address of node processing bit (PB) and count to reach next hop (CRNH). CRNH represents the hop difference between neighbors of one hop separated node; its value will be increment by each node for the first node entry whose processing bit is zero in the packet.	Detect both in-band and out-of-band but overhead is increases.
WAP: Wormhole Attack Prevention Algorithm in MANET	Sun Choi, Doo-young Kim, Do-hyeon Lee, [21] IEEE (2008)	During path search monitor nodes in promiscuous mode overhear and generate suspected wormhole node counter with WPT. During RREP it compare per hop distance with WPT.	Detect both hidden and exposed wormhole; but some time due to congestion generate false alert.

III. CONCLUSION

In this paper detail classification of wormhole attack and various existing method for detection and prevention of wormhole attack presented with future work. In MANET security and trust among network is important thing. There are several methods exists and efficient method available, but still trust based detection and prevention method can be carried of further research to overcome many drawbacks in the existing system.

REFERENCES

[1] Ruchia A.Kale, Prof. Dr. S. R. Gupta, "AN OVERVIEW OF MANET AD HOC NETWORK", International Journal of Computer Science and Applications - Apr 2013.

[2] David Airehrour, Jairo Gutierrez, Sayan Kumar Ray, "GradeTrust: A Secure Trust Based Routing Protocol for MANETs" IEEE – 2015

[3] Edna Elizabeth, Radha S, Priyadarshini S, Jayasree S, Naga Swathi "SRT-Secure Routing using Trust Levels in MANETs " EuroJournals Publishing, Inc. Vol.75 No.3 (2012), pp. 409-422

[4] J. Godwin Ponsam, Dr. R.Srinivasan, "A Survey on MANET Security Challenges, Attacks and its Countermeasures", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) - Volume 3, Issue 1, January – February 2014

[5] Mohit Jain, Himanshu Kandwal, "A Survey on Complex Wormhole Attack in Wireless Ad Hoc Networks" IEEE – 2009

[6] Saurabh Upadhyay, Brijesh Kumar Chaurasia, "Impact of Wormhole Attacks on MANETs", International Journal of Computer Science & Emerging Technologies - Volume 2, Issue 1, February 2011

[7] Akansha Shrivastava, Rajni Dubey, "Wormhole Attack in Mobile Ad-hoc Network: A Survey", International Journal of Security and Its Applications - Vol.9, No.7 (2015), pp.293-298

[8] MEHDI ENSHAEI, DR. ZURINA BT HANAPI, "A REVIEW ON WORMHOLE ATTACKS IN MANET", Journal of Theoretical and Applied Information Technology - 10th September 2015. Vol.79. No.1

[9] Marianne Azer, Sherif El-Kassas, Magdy El-Soudani, "A Full Image of the Wormhole Attacks Towards Introducing Complex Wormhole Attacks in wireless Ad Hoc Networks" - International Journal of Computer Science and Information Security, Vol. 1, No. 1, May 2009

[10] Felipe Téllez, Jorge Ortiz, "Behavior of Elliptic Curve Elliptic Curve Elliptic Curve Cryptosystems for the Wormhole Intrusion in MANET: A Survey and Analysis" - IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.9, September 2011

[11] Priya Maidamwar, Nekita Chavhan, "A SURVEY ON SECURITY ISSUES TO DETECT WORMHOLE ATTACK IN WIRELESS SENSOR NETWORK" - International Journal on AdHoc Networking Systems (IJANS) Vol. 2, No. 4, Oct 2012

[12] Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks" - IEEE 2003

[13] J. Zhen and S. Srinivas, "Preventing Replay Attacks for Secure Routing in Ad Hoc Networks," ADHOC-NOW 2003, Montreal, Canada, Oct 8-10, 2003, pp. 140-150.

[14] Hon Sun Chiu and King-Shan Lui, "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks - IEEE 2006.

[15] Sweety Goyal, Harish Rohil, "Securing MANET against Wormhole Attack using Neighbor Node Analysis" - International Journal of Computer Applications - Volume 81. No 18, November 2013

[16] Saurabh Gupta, Subrat Kar, S Dharmaraja, "WHOP: Wormhole Attack Detection Protocol using Hound Packet" - IEEE 2011

[17] Sun Choi, Doo-young Kim, Do-hyeon Lee, Jae-il Jung, "WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks" - IEEE 2008

[18] Juhi Biswas, Ajay Gupta, Dayashankar Singh, "WADP: A Wormhole Attack Detection And prevention Technique in MANET using Modified AODV routing Protocol" - IEEE 2014