International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 12, 2017 ISSN: 2348-6600
Reference ID: IJCS-215 PAGE NO: 1342-1347
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

A STUDY ON VARIOUS WORMHOLE ATTACK DETECTION TECHNIQUES IN MANET

M. Devi[1], Dr. G. Kesavaraj[2],
[1]M.Phil Full Time Research Scholar, PG & Research Department of Computer Science,
[1]devimuthusamy995@gmail.com
[2]Head of the Department, PG & Research Department of Computer Science,
[2]kesavaraj2020@gmail.com
Vivekanandha College of Arts & Sciences for Women (Autonomous),
Tiruchengode, Namakkal, TamilNadu, India, - 637205.

ABSTRACT- A Mobile Ad-Hoc Network (MANET) is defined as an arrangement of wireless mobile nodes which creates a temporary network for the communication. MANET doesn't having any access point. Due to high availability of wireless devices infrastructure-less networks are using every day's life. MANET is suffering from both kinds of attacks, active and passive attacks at all the layers of network model. Wormhole attack is one the most severe attack on routing protocols in which two or more malicious nodes receive packets at one point of network and transmit them another location by wired or wireless tunnel. This attack can form a serious threat in wireless networks, especially against many wireless ad-hoc networks and location-based wireless security systems. There is several wormhole detection methods in the wireless ad-hoc networks which some of them are reviewed in this paper.

Keywords: AdhocNetworks, Manet Attacks, Wormhole Attack,Detection Methods.

I. INTRODUCTION

A wireless network is the any type of computer network that uses wireless data connections for connecting network nodes. Wireless communications networks are implemented by using radio communication channels. Infra-Structure Based and Infrastructure Less Are two types of Wireless network [1]. The main research problem is how to provide security protection to the network topology and the routing in a MANET. The major challenges includes dynamic topology, decentralized control, limited resources, and the lack of information dissemination control. Many Applications runs in untrusted environments which requires secure communication and routing such as, Military Arena, Provincial level, Personal Area Network, Bluetooth and Commercial Sector etc.There are some challenges of MANETs like Quality of Service (QoS), security, scalability, power control and performance measurement.
There are two different kind of attacks in MANET, External Attack: External attacks are

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 12, 2017 ISSN: 2348-6600
Reference ID: IJCS-215 PAGE NO: 1342-1347
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

Carried out by nodes that do not belong to the network. It causes congestion and sends false routing information. It also causes unavailability of services.

Internal Attack: Internal attacks occurred from the nodes that are part of the network. In this attack the malicious node gains unauthorized access and pretend as a genuine node. It can also analyze traffic between other nodes and may participate in other network activities [2]. wormhole attack, black hole attack, grey hole attack, flooding, replay attack, DoS (Denial of Service) attack, Man-in-middle attack and evas dropping attack[3]are different types of attacks form in MANET and create trouble in network topology which trouble upper layer Applications.

II. MANET CHALLENGES:

Limited Bandwidth: The bandwidth for wireless networks is generally low than that of wired networks in mobile ad-hoc. Due to this throughput is also low in this.

Dynamic Topology: Nodes are free to move arbitrarily in any direction so the topology of the network changes continuously.

Energy Constrained Operation:Nodes are portable devices in the network and which are dependents on batteries [7].

Security: Number of possible attack in wireless network in more than that of wired network. So, more security required in wireless network.

Quality of Service (QoS): Difficult to Provide constant QoS for different multimedia services in often changing environment.

III. WORMHOLE ATTACK

Figure 1 shows the working of wormhole attack. At one end of the tunnel, a malicious node captures a control packet and sends it to another collaborating node at the other end through a private channel, which rebroadcasts the packet locally. Communication between source and destination is selected through the private channel because of having better metrics e.g., less number of hops or less time, as compared to packets transmitted over other normal routes. There are mainly two phases which describes working of wormhole attack. In the first phase, the wormhole nodes involved themselves in several routes. In the last phase, these malicious nodes start exploiting the packets they receive. These nodes can confuse the protocols that depend upon location or geographic proximity of nodes, or the colluding nodes may forward data packets back and forth to each other in case of virtual tunnel so as to exhaust the battery of other intermediate nodes. Wormhole nodes can drop, modify, or send data to a third party for malicious purposes.

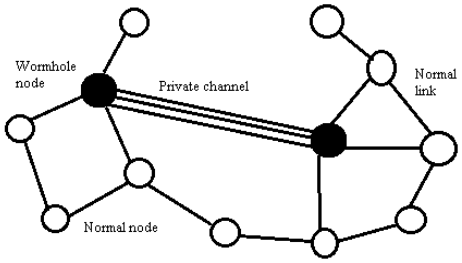

Fig. 1 Wormhole Attack

Tunnel in the wormhole attack can be established in many ways: in-band and out-of-band channel.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 12, 2017 ISSN: 2348-6600
Reference ID: IJCS-215 PAGE NO: 1342-1347
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

This creates illusion that two end points of tunnel are very close to each other. It can be used by malicious nodes to interrupt the correct operation of ad hoc routing protocols. They can then launch a variety of attacks against like selective dropping, replay attack, eavesdropping etc.

Classification Of Wormholes

The Wormholes can be broadly divided into twodifferent 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 2, a packet sent by source node is overheard by wormhole node M1, nodeM1 transmits that packet to second wormholenode M2 which in turn replays the packet intothe communication network. In this way it seems D and S are neighbors although they are out ofradio range. In this kind of attack, a path from Sto D via wormhole attacker link will be:

S → A → B → D

During exposed attacks, wormhole nodes do notmake any alteration in the content of packetsinstead they include their identities in the packetheader to be considered as trustworthy nodes.Therefore, other are aware of thewormhole node existence but they do not knowwormhole nodes are attacker. In scenario if theattack is revealed (Figure 2), the path from S to D via wormhole will be:

S → A → M1 → M2 → B → D

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

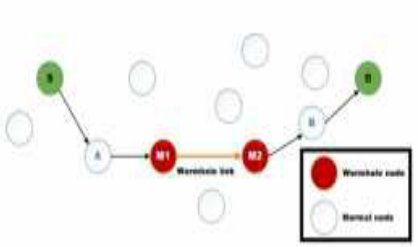

Fig. 2 Classification of Wormhole Attack

IV. WORMHOLE ATTACK DETECTION TECHNIQUES:

The capability of a node involved in wormhole attack can be measured by considering several metrics such as: Strength: Strength is the number of end-to-end paths attracted by false link advertisements sent by the attacker. The effectiveness of the wormhole attack is the number of traffic attracted by a wormhole [3]. The more is the number of traffic passing through the wormhole tunnel, the more effective is the wormhole attack.

Difference between the advertised path and the actual path length: If the advertised path has a path length of smaller number of hops as compared to that of actual path, this difference in the path length can be a useful metric to detect wormhole attack. The irregularity can be more easily observed if there is larger difference between the advertised path and the actual path.

Attraction: Attraction refers to the decrease in path length offered by wormhole. If the attraction is small then, the small improvements in normal path may reduce the strength of wormhole attack as the nodes may choose an alternative route that does not pass through the wormhole tunnel.

Robustness: Robustness refers to the ability of wormhole attack to persist its effect without

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 12, 2017 ISSN: 2348-6600
Reference ID: IJCS-215 PAGE NO: 1342-1347
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

significant decrease in its strength even in the presence of minor topology change.
Packet delivery ratio: The Packet delivery ratio metrics refers to the ratio of total number of packets delivered to the total number of packed sent.

Packet Leashes
Numerous methods were proposed using a packet leash technique for the detection of the wormhole attack. The packet leash is the method that defends against the wormhole attack. Whenever a sender sends the data packet, it includes its own recent location and transmission time Directional antenna detects the existence of wormhole nodes. In this method, directional information is shared between source and destination. The destination can detect the wormhole by comparing the received signal from the malicious nodes and directional information from the source. If the both the signals from the source and intermediate nodes are different, then the wormhole link is detected. [10]

Using Directional Antennas
This method used an special hardware called directional antenna at each mobile nodes antennas to defend against wormholes and maintain an directional scheme i.e. sender node sends packets in a given direction and receiver packet will get that packet from the opposite direction whole communication will performed only when the directions of both pairs match, the neighboring relation is confirmed .This approach work only when system has only two end points does not prevent multiple endpoint attacks. Directional errors are possible[10].

Geographic Distribution Technique
WGDD algorithm detects the wormhole attack based on the damage caused by them and the parameter used for wormhole detection is hop count. According to the hop count measured, it reconstructs the mapping details in each node and finally it exploits diameter feature to detect distortions caused by malicious nodes. WGDD algorithm is effective in finding the exact location of the wormholes.

True Link:Atimebased Mechanism [8]
True Link verifies whether there is a direct link for a node to its adjacent neighbor. Wormhole detection using True Link involves 2 phases namely rendezvous and validation. The first phase is performed with firm timing factors in which nonce exchange between two nodes takes place. Around trip time (RTT) approach is emerged to overcome the problems in using additional hardware. The RTT is the time taken for a source node to send RREQ and receive RREP from destination. A node must calculate the RTT between itself and its neighboring nodes. The malicious nodes have higher RTT value than other nodes. In this way, the source can identify its genuine and misbehaving neighbors. This detection technique is efficient only in the case of hidden attacks.

Neighbor Node Analysis Approach
Neighbor node analysis approach analyzes the neighboring nodes so as to check the authenticity of the nodes for secure transmission of data over the network. According to this approach a node

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 12, 2017 ISSN: 2348-6600
Reference ID: IJCS-215 PAGE NO: 1342-1347
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

will request to its neighboring nodes and perform a request and response mechanism. The node will maintain the table to track the timeout. If the reply time is not accurate there is an attack in the network. All the intermediate nodes are analyzed to detect the presence of wormhole attack using AODV protocol in MANET.
computational overhead. It needs no specialized hardware and has good performance.

V. CONCLUSION AND FUTURE WORK

The Mobile Ad Hoc network is greatly influenced by wormhole attack. These attacks degrade the network performance and menace to network security. In this paper various techniques are presented for detection of wormhole attacks .In future these approaches will help to efficiently remove the malicious nodes from the Mobile Ad Hoc networks .The techniques for detection have both advantage and disadvantage. These nodes are also responsible in elimination of nodes that are performing malicious activities in the network. Some networks need more security like whether forecasting and military area may increase the cost. From all above solutions we can find the efficient method to detect the wormhole attacks by equating all factors. Future work will include algorithm enhancements for improvement and consideration of internal attackers, with the help of various no of experiments and by using many number of scales and combination of this work with a localization protocol.

VI. REFERENCES

[1]. Anal Patel, Nimisha Patel, Rajan Patel "Defending Against Wormhole Attack in MANET", Fifth International Conference on Communication Systems and Network © 2015 IEEE, 2015

[2]. VikaskumarUpadhyay,RajeshShukla "An Assessment of Worm Hole attack over Mobile Ad-Hoc Network as serious threats", Int. J. Advanced Networking and Applications Vol No 05 January,2013

[3]. D. Helen, D. Arivazhagan "Applications, Advantages and Challenges of Ad Hoc Networks", Journal of Academia and Industrial Research (JAIR) Vol No 2, 8 January 2014

[4]. YashpalsinhGohil, SumeghaSakhreliya, SumitraMenaria "A Review On: Detection and Prevention of Wormhole Attacks in MANET", International Journal of Scientific and Research Publications, Vol No 3, February 2013

[5]. PriyankaGoyal, VintiParmar, Rahul Rishi "MANET: Vulnerabilities, Challenges, Attacks, Application", IJCEM International Journal of Computational Engineering & Management, Vol. No.11, January 2011

[6]. Gupta N., Khurana S., "SEEEP: Simple and Efficient End-to-End Protocol to Secure Ad hocNetworks Against Wormhole Attacks", Proceedings of the 4th International Conference on

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 12, 2017 ISSN: 2348-6600
Reference ID: IJCS-215 PAGE NO: 1342-1347
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

Wireless and Mobile Communications (ICWMC'08); Athens, Greece. 27 July–1 August 2008; Pp. 13–18."

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

[8]. Chiu H.S., Lui K.-S. "DelPHI: Wormhole Detection Mechanism for Ad hocWireless Networks.", Proceedings of the 1st International Symposium on Wireless Pervasive Computing; Phuket, Thailand. January 2006.Pp 16-18

[9]. Phuong Van Tran1, Le Xuan Hung1, Young-Koo Lee1, Sung, Young Lee1, and Heejo Lee2, "TTM: An Efficient Mechansim to Detect Wormhole Attacks in Wireless Ad-Hoc Networks."

[10]. Shang-Ming Jen , Chi-Sung Laih and Wen-Chung Kuo, "A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET", Sensors 2009.