Review of Various Wormhole Attack Detection Techniques for MANET

Sahil Sharma
Computer Science and engineering
Senior Security Analyst at Capgemini
National Institute of Technology, Hamirpur.

Abstract - The mobile ad hoc network is the self configuring type of network in which mobile nodes can join or leave the network when they want. Due to such dynamic nature of the network malicious nodes enter the network which triggers various types of security attacks. The wormhole attack is the active type of attack which increases delay in the network. The various schemes are proposed which detect and isolation malicious nodes from the network which are responsible to trigger wormhole attack. The Delphi is the most popular technique for the isolation of wormhole attack in MANET. The Delphi technique use static threshold value for the isolation of malicious nodes from the network which affect detection rate from the network. The various dynamic methods are proposed for the isolation of malicious nodes from the network.In this paper, various wormhole detection techniques are reviewed in terms of certain parameters

Keywords - MANET, Wormhole, Active Attack, Threshold Technique

I. INTRODUCTION

A MANET or Mobile Ad Hoc Network generally refers to an interconnected system of wireless devices. These devices or nodes establish communication with each other over wireless channels with limited bandwidth. All wireless nodes can perform the role of both sender as well as receiver (or router) in this network. A node can deliver messages to a destined destination node via some route while playing the role of a host or a sender. On the other hand, the same node can get messages from other network nodes, in the role of router. A node as a router is capable of sending the packet to the destination or subsequent receiver within the route. Every node can buffer packets in the anticipation of transferring, if essential. The nodes generally roam around randomly [1]. Due to this reason, an ad hoc network occurs between the nodes at a specific time period. This situation gives rise to a random network topology. It is possible to construct MANETs dynamically amidst any set of wireless users without the need of a permanent framework or set up. In contrast to the conventional manually constructed infrastructure based networks, a MANET can be used to serve lots of objectives. For instance, mobile ad hoc networks can offer mobile network offloading. The role of network offloading may be very important in conditions where the number of clients on a network reaches or goes beyond the network capacity, which causes delays and disrupts the networks service in one or other way. These networks can divert traffic temporarily from conventional network set-up to re-establish service for, or upsurge the number of, clients within a representative coverage area.These networks are also capable of providing communication and information distribution abilities in regions that do not have a temporary or permanent competent infrastructure for message sharing. Some of these areas include post-natural disasters regions, rural regions, areas with less no. of economic resources, or highly inaccessible regions, such as tunnels.

Security is one of the major concerns to mobile adhoc networking (MANET) as this network is way more susceptible to malicious activities as compared to a classic wired network [2]. At the outset, the use of wireless connections extracts the network vulnerable to intrusions in the range from passive eavesdropping to active intrusive. In contrast to wired networks, in which a malicious must gain physical access to the network wires or go through various defensive lines at firewalls and gateways before launching an attack, attacks on a wireless network can be launched from any direction by targeting any node. Disruptions may involve leak out of confidential information, message corruption, and node imitation. This indicates that a wireless ad-hoc network does not have a clear defensive measure, and all nodes must be ready for encountering a malicious in direct indirect manner. Secondly, mobile devices are independent units. These units can move autonomously [3]. This depicts that nodes with insufficient physical safety can be easily captured, contaminated, and hijacked. The intrusions launched by an adversary cause more damage to the network and cannot be detected easily as it is very hard to track down a specific mobile node in a big ad hoc network. Hence, it is essential to prepare mobile devices and the infrastructure for operating

in a non-peering trust mode. Thirdly, in a mobile computing environment, the making of decisions is sometimes localized. Also, some wireless network algorithmic approaches depend on the supportive contribution of all participating nodes and the set-up. The absence of centralized control depicts that the attackers can exploit this susceptibility for novelsorts of intrusions destined to interrupt the cooperative algorithms. Applications and amenities in a mobile wireless network can also be a weak link. The weakness of a MANET is targeted by a large number of intrusions. In MANET, The attacks can be generally classified into two main groups, called passive intrusions and active intrusions, in accordance to the purpose of the attack. In a passive attack, data is shared in the network without causing disruption in the process of the communications. An active attack, on the other hand, interrupts, modifies,or fabricates information, and disrupts the normal operation of a mobile ad hoc network. Instances of passive intrusions include eavesdropping, traffic analysis, and traffic monitoring. However, some popular examples of active attacks are jamming, impersonating, modification, denial of service (DoS), and message replay. The attacks can be further categorized into two classes of external and internal attacks, in accordance to the area of the intrusions. The attacks are sometimes also classified as outsider and insider attacks. External attacks are launched by nodes, unrelated to the area of the network. Internal attacks are launched by contaminated nodes, which are really part of the network [4]. As compared to the external attacks, Internal attacks are more serious as the insider knows about the valuable and secret information, and has advantaged access privileges. There are some security intrusions which make use of sneakiness, by which the adversaries attempt to conceal their activities from either an individual, observing the system or an IDS(Intrusion Detection System). However, it is not possible for some attacks such as DoS to be stealth. Wormhole attack is a very classy and understated routing attack. In this intrusion, an intruder does the recording of packets at one position in the network and channelizes them to some other position. The disruption in routing can occur during the tunnelling of routing control messages. This tunnel amida couple of conspiring attackers is known as a wormhole [5]. Wormhole attacks are a serious challenge to the routing protocols of a mobile ad hoc network. For example, a wormhole attack launched against an on-demand routing protocol including DSR or AODV can prevent the detection of any routes except through the wormhole.Wormhole attacks are frequently represented as attack events mutually performed by a couple of adversaries at different locations. Among these two adversaries, the first one transmits the routing message to the other via a clandestine tunnel. These two adversaries seem to be in the neighbourhood of each other in spite of the remoteness between them. Thus, there is a high possibility that the hop count passing through the malicious motes will be found shorter in comparison with the normal nodes for maximizing the chances of grabbing the route to transmit the data. Thus, the data packets which are passed through the malicious devices can be dropped or eavesdropped [6]. A packet encapsulated channel and out-of-band channel are utilized to characterize the secret tunnel within wormhole attacks. A packet encapsulated channel is also known as an in-band channel that means a malicious node places the received routing messages into the payload of a data packet and the regular nodes are deployed in which tunnel is established for the transmission to the other malicious node.

II. LITERATURE REVIEW

Sayan Majumder, et.al (2018) suggested an algorithm on AD of statistical approach for avoiding and preventing the Wormhole attack [7]. The covariance and correlation of suggested approach had consumed less time while detecting the Wormhole attack in comparison with the traditional approach. There was not any necessity of extra essential conditions in the suggested approach. The assailant generated a false tunnel between source and destination that was linked with a fine amount of frequency level. This led to make a forge idea that the origin path was close to the destination and it had consumed less time. However, more time was consumed by the original path. Thus, the computation of the time consumed while avoiding and preventing wormhole attack was required. A MATLAB simulator was employed to conduct the simulation. The simulation outcomes demonstrated that the suggested approach provided superior performance for wormhole attack as compared to AODV. Afterward, The ADCC was implemented to evaluate the packet drop pattern.

S Gayathri, et.al (2019) analyzed that there were nodes included in the MANETs whose communication was done with the dynamic request and also through the static table driven method [8]. There were many difficulties occurred in the field of network analysis due to the wormhole attacks in Mobile ad hoc networks. A high power transmission was executed to recognize the wormhole scenario. The energy model of ns2 simulator was utilized to perform the execution. The energy level of every node was recognized and the node of high transmission power was tracked using the Apktool simulator. The performance curves were evaluated in terms of throughput, node

energy for different encrypted values, PDR and E2ED.

Saurabh Sharma, et.al (2017) discussed that there were various security attacks occurred on the Mobile ad hoc networks as they had unique features [9]. One of the common problems occurred in the routing protocol of MANETs was wormholes. A novel routing protocol known as hop count model based EPPN was recommended. The current active route assisted in acquiring the hop count from source to destination. The incorporation of the hop count model was carried out into AODV protocol. Initially, the route was chosen depending upon the RREP. After that, the hop count was evaluated from between source to destination using the recommended model. At last, the process to detect the attack was initiated when the computed hop count was larger as compared to the received hop count within the route for getting out the suspicious motes.

Hossein As'adi, et.al (2018) described that the Mobile ad hoc networks were becoming susceptible to deal with several security attacks such as wormhole attack due to their features [10]. There were diverse techniques established in the last few years to detect, alleviate and prevent wormhole attacks in these networks. A novel decentralized method planned on the basis of statistical metrics was constructed to detect the wormholes in which a number of new neighbours were deployed together with various neighbours for each node as its parameters. There was least detection delay obtained from the presented technique and it had not generated any traffic overhead for routing algorithms having neighbour discovery technique. The reasonable processing power and memory utilization had also been provided by it. NS3 simulator was carried out to conduct the simulations. The outcomes obtained in simulation proved that the suggested technique performed effectively with respect to the accuracy of detection and false positive rate.

Shripriya Tripathi, et.al (2019) analysed that the MANET had susceptibility against a number of attacks like spoofing attack, wormhole attack etc. because it had changed rapidly and had self-organizing behaviour [11]. The repercussion of the wormhole attack was compared and analysed 2 common routing algorithms of reactive category named DSR and AODV for which the number of wormhole tunnels was maximized in this network. The simulation outcomes represented that this attack affected the Dynamic Source Routing. Thus, a routing protocol for DSR planned on the basis of trust was intended as a solution for preventing the routes from caching malicious motes.

Shaubham N. Ghormare, et.al (2018) presented an AODV routing algorithm to detect and prevent the wormhole attack within MANET based on the WiMAX [12]. The packet was kept on another location of the network and transmitted to another attacker mobile node which away from the tunnelling through the attacker mobile motes. The NS2 software was employed to conduct this research. First of all, the AODV routing algorithm was utilized to construct the WiMAX based MANET. Later on, the wormhole attack was launched and the established MANET was analyzed considering various performance metrics such as PDR etc.

Aditya Bhawsar, et.al (2020) intended a technique for detecting and preventing the wormhole attack from Mobile ad hoc Networks for which trust calculation based AODV protocol was carried out [13]. The best path was discovered for routing applying the multiple path selection in this technique. The testing of path was done for the wormhole attack because the node detected the data packet which was transmitted to destination from source node and selected the path from the multi-paths available and thus assisted in enhancing the packet delivery. The PDR of the intended technique was evaluated. The outcomes demonstrated that the PDR was enhanced by71.25% and the reduction of E2ED was found by 57.92ms for the network including 125 nodes.

Author	**Year**	**Description**	**Outcome**
Sayan Majumder, Debika Bhattacharyya	**2018**	Suggested an algorithm on AD of statistical approach for avoiding and preventing the Wormhole attack.	The simulation outcomes demonstrated that the suggested approach provided superior performance for wormhole attack as compared to AODV. Afterward, The ADCC was implemented to evaluate the packet drop pattern.

S Gayathri, R. Seetharaman, L.Harihara Subramanian, S. Premkumar, S. Viswanathan, S. Chandru	**2019**	Analysed that there were nodes included in the MANETs whose communication was done with the dynamic request and also through the static table driven method.	The energy level of every node was recognized and the node of high transmission power was tracked using Apktool simulator. The performance curves were evaluated in terms of throughput, node energy for different encrypted values, PDR and E2ED.
Saurabh Sharma, R. M. Sharma	**2017**	A novel routing protocol known as hop count model based EPPN was recommended in this work.	The Process to detect the attack was initiated when the computed hop count was larger as compared to the received hop count within the route for getting out the suspicious motes
Hossein As'adi, Alireza Keshavarz-Haddad, Ali Jamshidi	**2018**	A novel decentralized method planned on the basis of statistical metrics was constructed to detect the wormholes in which a number of new neighbours were deployed together with various neighbours for each node as its parameters.	The outcomes obtained in simulation proved that the suggested technique performed effectively with respect to the accuracy of detection and false positive rate.
Shripriya Tripathi	**2019**	Analysed that the MANET had susceptibility against a number of attacks like spoofing attack, wormhole attack etc. because it had changed rapidly and had self-organizing behaviour.	The simulation outcomes represented that this attack affected the Dynamic Source Routing. Thus, a routing protocol for DSR planned on the basis of trust was intended as a solution for preventing the routes from caching malicious motes.
Shaubham N. Ghormare, Swati Sorte, S.S. Dorle	**2018**	Presented an AODV routing algorithm to detect and prevent the wormhole attack within MANET based on the WiMAX,	The wormhole attack was launched and the established MANET was analysed considering various performance metrics such as PDR etc.
Aditya Bhawsar, Yogadhar Pandey, Upendra Singh	**2020**	Intended a technique for detecting and preventing the wormhole attack from Mobile ad hoc Networks for which trust calculation based AODV protocol was carried out.	The outcomes demonstrated that the PDR was enhanced by71.25% and the reduction of E2ED was found by 57.92ms for the network including 125 nodes.

III. CONCLUSION

In this work, it is concluded that wormhole attack is the active type of which affects network performance in terms of delay. The worm hole attack is triggered by the malicious node which creates a tunnel between the mobile nodes to increase delay. The Delphi method is further improved using the various parameters like processing time, queue size for the isolation of malicious nodes from the network. The further various other parameters can be added in the Delphi technique for the detection of malicious nodes from the network.he various schemes for the detection of malicious nodes are reviewed. It is analyzed that scheme which is based on threshold scheme gives maximum performance for the isolation of malicious nodes.

IV. REFERENCES

[1] Prabhleen Kaur, Sukhman, "An Overview on MANET- Advantages, Characteristics and Security Attacks", International Journal of Computer Applications, vol. 4, pp.6-9, 2016

[2] Meenakshi Yadav, Nisha Uparosiya, "Survey on MANET: Routing Protocols, Advantages, Problems and Security", International Journal of Innovative Computer Science & Engineering, vol.1, pp.12-17, 2014.

[3] Reshmi Maulik1 and NabenduChaki, "A Study on Wormhole Attacks in MANET", 2011, International Journal of Computer Information Systems and Industrial Management Applications, vol. 3, pp. 271-279

[4] Muhammad Imrana, Farrukh Aslam Khanb, Tauseef Jamala , Muhammad Hanif Durad, "Analysis of Detection Features for Wormhole Attacks in MANETs", 2015, International Workshop on Cyber Security and Digital Investigation

[5] Chaurasia, U.K., Singh, V., "MAODV: Modified wormhole detection AODV protocol", 2013, Sixth International Conference on Contemporary Computing (IC3), pp.239-243

[6] Subhashis Banerjeeand Koushik Majumder, "Wormhole Attack Mitigation In MANET: A Cluster Based Avoidance Technique", 2014, International Journal of Computer Networks & Communications (IJCNC) Vol.6, No.1

[7] Sayan Majumder, Debika Bhattacharyya, "Mitigating wormhole attack in MANET using absolute deviation statistical approach", 2018, IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)

[8] S Gayathri, R. Seetharaman, L.Harihara Subramanian, S. Premkumar, S. Viswanathan, S. Chandru, "Wormhole Attack Detection using Energy Model in MANETs", 2019, 2nd International Conference on Power and Embedded Drive Control (ICPEDC)

[9] Saurabh Sharma, R. M. Sharma, "EPPN: Extended Prime Product Number based wormhole DETECTION scheme for MANETs", 2017, 11th International Conference on Intelligent Systems and Control (ISCO)

[10] Hossein As'adi, Alireza Keshavarz-Haddad, Ali Jamshidi, "A New Statistical Method for Wormhole Attack Detection in MANETs", 2018, 15th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC)

[11] Shripriya Tripathi, "Performance Analysis of AODV and DSR Routing Protocols of MANET under Wormhole Attack and a Suggested Trust Based Routing Algorithm for DSR", 2019, IEEE International WIE Conference on Electrical and Computer Engineering (WIECON-ECE)

[12] Shaubham N. Ghormare, Swati Sorte, S.S. Dorle, "Detection and Prevention of Wormhole Attack in WiMAX Based Mobile Adhoc Network", 2018, Second International Conference on Electronics, Communication and Aerospace Technology (ICECA)

[13] Aditya Bhawsar, Yogadhar Pandey, Upendra Singh, "Detection and Prevention of Wormhole Attack using the Trust-based Routing System", 2020, International Conference on Electronics and Sustainable Communication Systems (ICESC)