International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 4 Apr 2022, pp: 291-295 www.ijaem.net ISSN: 2395-5252

A Composite Wormhole Intrusion Detection in Mobile Ad-Hoc Network (MANET)

Suresh C
Assistant Professor, Department of Information Technology
Gojan School of Business and Technology, Redhills, Chennai

Submitted: 01-04-2022 Revised: 06-04-2022 Accepted: 11-04-2022

ABSTRACT
Mobile Ad-hoc Networks (MANET) are wireless networks that communicate without the use of fixed infrastructure. Wormhole attacks make MANETs insecure and vulnerable. Wormhole attacks are extremely difficult issues that record packets from one position of the network and tunnel them to another position in order to degrade the performance of the wireless network and disrupt the most common routing protocol. Nevertheless, existing approaches to wormhole attacks have been established, but they still require extra equipment, incur high delivery delays, or fail to provide high levels of security. In this article, a composite wormhole intrusion detection (CWID) algorithm is proposed that can detect both in-band wormholes via round trip time (RTT) based on hop count and packet delivery factor (PDR), as well as out-of-band wormholes via communication range between successive nodes in a more optimism way than existing methods. CWID saves time and energy by avoiding wormhole identification for all available nodes in the network. CWID is not dependent on any specialized hardware or middleware.. To improve the detection method, the suggested methodology made use of the Ad-hoc On-Demand Distance Vector (AODV) reactive or on demand routing protocol.

Index terms: Warmhole Attacks, MANET, AODV

I. INTRODUCTION

Wireless technology has brought about significant advancements in the field of internet. It has spawned a slew of new applications. A lot of work has been done in the domain of Mobile Ad hoc Networks (MANET) in recent years, which has made it so famous in the area of research work. MANET is a dynamic network with no infrastructure. It is made up of a collection of wireless mobile end devices and interaction between these nodes is done without the use of a central authority. MANET stands for Mobile adhoc Network also called a wireless adhoc network or adhoc wireless network that usually has a routable networking environment on top of a Link Layer ad hoc network.. They consist of a set of mobile nodes connected wirelessly in a self-configured, self-healing network without having a fixed infrastructure. MANET nodes are free to move randomly as the network topology changes frequently. Each node behaves as a router as they forward traffic to other specified nodes in the network. ANET may operate a standalone fashion or they can be part of larger internet. They form a highly dynamic autonomous topology with the presence of one or multiple different transceivers between nodes. The main challenge for the MANET is to equip each device to continuously maintain the information required to properly route traffic. MANETs consist of a peer-to-peer, self-forming, self-healing network MANET's circa 2000-2015 typically communicate at radio frequencies (30MHz-5GHz). This can be used in road safety, ranging from sensors for the environment, home, health, disaster rescue operations, air/land/navy defense, weapons, robots, etc.

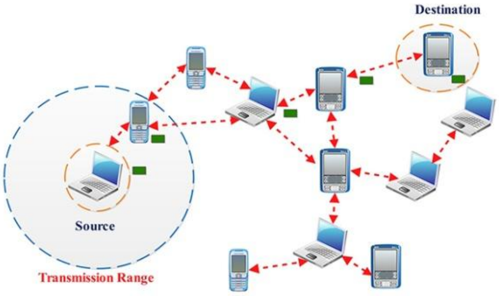

Fig 1: Mobile Ad hoc Network (MANET)

A mobile ad hoc network (MANET) is a self-organizing and self-configuring multi-hop wireless network in which the network structure changes dynamically. This is primarily due to node mobility. The nodes in the network not only serve as hosts, but also as routers, sending data from one node to the next. To communicate with the other nodes in the MANET, each node uses a wireless interface. These networks are completely distributed and can operate in any location without the assistance of any fixed infrastructure such as access points or base stations. The routing protocol's primary function is to find the shortest path between the sender and the receiver. If nodes are in direct range of each other, they can connect and communicate directly; however, if nodes are not in direct range of each other, they must use intermediate nodes to transfer their data packets. There are three main types of routing protocols in MANET: proactive, reactive, and hybrid. The participating node in a MANET has a limited transmission range. As a result, if two nodes are not within radio coverage of each other, they will be unable to communicate. As a result, the multi-hop scenario will be used, and the intermediate node will have to forward the packet to the next node until it reaches the destination. Because of the wireless transmission's spontaneous nature and characteristics, MANET is vulnerable to a variety of attacks and security threats, including wormhole attacks. As a result, it is critical to preserve the confidentiality of data transmission from device to device in a wireless network without jeopardizing data transmission integrity.

Wormhole attacks are difficult to detect and are one of the most serious security concerns to MANET. The wormhole attack occurs when an attacker establishes a communication link between two remote nodes by capturing a packet from one network site and sending it to an illegal network location. To create duplicate connections, deceive the legal path by modifying or dropping sent packets, resulting in a fictitious network structure as depicted in Fig.2. The assailants have a direct line of communication with one another. As a result, it can connect faster than legal nodes in order to carry out the assault. Packet encapsulation (in-band) can be used to create a tunnel by forwarding the packet through accessible legitimate nodes in the network. The out-of-band channel, which likewise sends packets over great distances and uses a separate external communication link between malicious nodes, is also used. The source node and destination node are separated in an out-of-band assault.

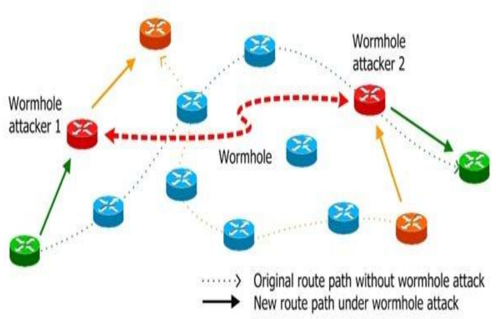
Wormhole attacker 1
Wormhole attacker 2
Wormhole
Original route path without wormhole attack
New route path under wormhole attack

Fig 2: Wormhole attack in MANET

However, because of the fictitious tunnel established, they appear to be adjacent and direct neighbors, reducing the hop count. In-band attacks, on the other hand, employ valid routes and do not raise the hop count during traversal. A wormhole attack does not need understanding of a security system, such as cryptographic techniques, public/private keys, and so on. As a result, even if the data is encrypted, it cannot be identified using cryptographic procedures. To achieve high wormhole attack detection accuracy, the proposed technique combines RTT based on hop count, PDF, and transmission range characteristics. The suggested approach was used to identify the threshold value in packet delivery ratio for both out-of-band and in-band wormhole attacks, and the K-Means clustering approach was utilized in this study to establish the threshold value. It is a commonly used approach in the field of data mining.

II. MOTIVATION

Wormhole attacks are one of the most serious attacks, and are considered a complex problem that can be initiated at the network layer of the OSI model. It consists of two malicious nodes involved in the routing path and the communication link between them. In Figure 2. Between the two nodes of the wormhole. The attacker receives data packets somewhere on the network, sends them to a remote location on the network, and then replicates them locally. Tunnels can be created in different ways, such as in scope and out of scope. The routing path between the source and the target is selected through the created tunnel, which is later used to exchange data packets between malicious nodes. Unauthorized access by malicious hosts may cause data packets to be discarded, delay important data packets, affect network performance or send them to other networks, and ultimately cause network interruption. Wormhole can be decomposed into four attack modes, namely packet encapsulation, high-performance transmission, packet retransmission and out-of-band transmission. The tunnel can be initiated through wired and wireless transmission or through an optical channel.

The packet could be forwarded via remote wormhole nodes with the aid of using growing an phantasm that they're near every different while in reality, they're not. Malicious nodes are prepared with better transmission energy and better bandwidth in evaluation to different valid nodes. Therefore, they are able to transmit packets over lengthy distances to create faux shortcuts, stopping the valid nodes to be determined with the aid of using its neighbours, growing wrong routing paths, after which inflicting community disruptions. This faux shortcut direction that is created with the aid of using wormhole node could be hired for packet change amongst themselves.

III. LITERATURE SURVEY

Sayan Majumder and Debika Bhattacharyya [5] proposed statistical methodology based on AD (Absolute Deviation) to avoid and prevent Wormhole attacks. It takes less time to identify a Wormhole assault with absolute deviation covariance and correlation than it does with a conventional one. Any additional circumstances, such as GPS, are not required in the suggested algorithms. Wormhole attackers construct a phony tunnel from point A to point B, which is a link with go. As a result, the time required to avoid and prevent Wormhole attacks must be calculated. Simulation using a MATLAB simulator for wormhole assault shows that absolute deviation approach outperforms AODV. The Absolute Deviation Correlation Coefficient is then used to measure the packet drop pattern for Wormholes. The major disadvantage of this paper is time complexity and required to calculate the correlation rate of each nodes.

Chiu and Lui [10] Propose a method for detecting wormholes known as delay per hop indication (DELPHI). DELPHI uses a multipath technique to compute the average latency per hop each and every route The sender calculates the average delay per hop for each recipient. a path As a result, wormhole nodes can be discovered if the path that leads to them is followed has higher delays and will not be used for data transmission a packet. They fail to give solution for round trip packet loss due to congestion.

Mohanapriya Marimuthu and Ilango Krishnamurthi [3] analyzed the weaknesses of optimal link state routing (OLSR), a proactive routing protocol, against a sort of denial-of-service (DOS) attack known as node isolation. Following an analysis of the attack, they offer the improved OLSR (EOLSR) protocol, which is a trust-based strategy for protecting OLSR nodes against the attack. Our method is capable of achieving finite results Detecting node isolation threats by determining if a node is advertising valid topological information or not by checking its Hello packets. The disadvantage is EOLSR protocol is not efficient and consumed more energy.

S. Qazi, R. Raad, Y. Mu, and W. Susilo [6] they showed that DelPHI fails to protect AODV in a multirate transmission environment because it ignores the wireless channel's changing bit rate nature and expects a constant bit rate, resulting in either erroneous or no detection of wormhole attacks. We next propose a DelPHI extension (M-DelPHI) that adapts the protocol to the multi rate 802.11 wireless channel. We recommend the following: 1. Neighbor monitoring, 2. Processing delay, and 3. Multi rate channel We present two test scenarios that show our expansion and mimic the new protocol in a variety of settings. Under the required test circumstances, M-DelPHI works extraordinarily well, with a wormhole detection rate of over 90% against incoming and out-of-band wormholes. The disadvantages of this paper is it uses only AODV to find the bit rate, they didn't use any specific algorithm to identify wormhole attack.

Lai [2] Propose a solution for preventing wormhole attacks in Low Power and Lossy Networks by using the standard routing protocol IPv6 (RPL). This method, on the other hand, restricts the maximum distance a packet can travel during transmission. To calculate the distance, the rank of a node determined by RPL is used. If inappropriate rank values are used in the suggested detection approach, malicious wormhole nodes are discovered. This paper fails to identify the time delay and time complexity is high.

Hu et al. [4] offer a packet-based wormhole attack detection technique. Both geographical and temporal constraints are considered in the suggested technique. The geographical relies on the packet's current location and transmission time. To determine if the packets are valid, the receiving node will compute the distance to the sender and the time it takes for the packet to travel the path. Temporal leashes are based on a synchronized clock but do not rely on GPS information. To prevent packets from travelling over long distances, the sending node will attach the transmission time and the expiry time with each transmitted packet, and the receiving node will utilise its own packet receipt time for verification.

Tamilarasi and Santhi [1] In MANET, a strategy for preventing wormhole attacks was proposed that involved recognizing the wormhole and choosing the optimum route. Using the Ad-hoc on demand Multipath Distance Vector (AOMDV) routing protocol, many paths termed K will be constructed between source and destination at first. The wormhole attacked path will then be identified by confirming the Detection Packet through the originating node and the destination's Feedback Packet (FP). After determining the wormhole attacked pathways, the source node uses the Particle Swarm Optimization (PSO) algorithm to choose the optimal path among the attacker free pathways and sends the data to the destination through that path. The disadvantage of this paper is time complexity is high.

Sankara and Murugaboopathi [7] identified wormhole assaults, a technique based on Quality of Service (QoS) was proposed for the whole network. To mitigate the wormhole attack in MANET, the modified secure AODV protocol (MSADOV) has been suggested, which leverages the packet forward ratio and round trip time. Furthermore, the suggested method can identify both active and passive assaults.

Jamali and Fotohi [8] Defending against wormhole attack (DAWA) is a strategy for preventing wormhole attacks that uses a fuzzy logic framework and an artificial immune system. Using fuzzy logic, the first phase will pick a high-performance path between the source and the destination. In the second phase, a denes strategy based on an artificial immune system (AIS) will be used to combat wormhole attacks.

IV. PROPOSED MODEL

In a mobile ad-hoc network, the suggested approach is based on Composite Wormhole Intrusion Detection (CWID). To avoid conducting wormhole verification on all accessible nodes, a next ratio threshold (NRT) has been established. The detection algorithm will then be used to merge the several detection techniques. The algorithm techniques that have been proposed include.

Step 1: As indicated in the algorithm 1, use a technique called next ratio threshold (NRT) to reduce the number of nodes that must be identified.

Step 2: Next, assess whether or not the neighboring nodes are inside the source's transmission range. If the source is out of range, categories it as an out-of-band wormhole attack.

Step 3: Use round trip time based on hop count and packet delivery ratio to calculate the in-band attack if neighboring nodes are within transmission range of the source.

Some assumptions about network and opponent capabilities in the proposed MANET design are discussed in this section.

Premise 1: When the distance between two nodes is within the transmission range, they are considered neighbors.

Premise 2: In the proposed model, the nodes all start at the same energy level and move in a random manner.

Premise 3: Malicious nodes are capable to launching a variety of wormhole assaults.

Algorithm: Next Ratio Threshold (NRT).

```
Start
foreach node ni in Q and its neighbor set Bi in S do
Let si = |Bi |(which is the neighbor number of ni);
foreach node njSi do
sj = |Bj| (which is the neighbor number of nj);
Set a =0;
a =a + sj;
To find the average neighbor number of ni's neighbors, Then si= a/s
To Find the ni's neighbor ratio NRTi = si
ifNRTi > NRT then
put ni to suspected nodes set A area;
end
End of Pseudocode.
```

The process of determining if every single node in the network was impacted by a wormhole or not is one of the most energy-intensive approaches as well as a source of increased latency for nodes in the network. In most cases, a wormhole does not target every node in a wireless network. Wormholes increase the number of neighbor nodes, resulting in erroneous RTT and increased network connection. As a result, a simple yet efficient strategy known as Next Ratio Threshold has been utilized (NRT). To avoid performing the wormhole detection on all nodes in MANET, it will check a node's neighbor number with all of its neighbors. The nodes will know who their neighbors are when the neighbor discovery operations are completed. The node then calculates the next or neighbor ratio, which is the ratio of its neighbor number to the average neighbor number (sNi) of all its neighbors. Following that, the neighbor ratio (NRTi) will be compared to the Next Ratio Threshold (NRT) to see if wormhole detection is required.

V. CONCLUSION AND FUTURE WORK

A composite wormhole intrusion detection (CWID) set of rules in MANET capable of stumble on varieties of wormhole assault, in-band wormhole the usage of spherical experience time and packet transport ratio that used K-Means clustering set of rules. While out-of-band wormhole makes use of transmission variety among successive nodes. CWID become proposed to decorate the wormhole assault detection for each kinds, in-band and out-of-band. Neighbors or next ratio threshold helped to decrease the electricity intake and postpone via lowering the wide variety of detection nodes. This set of rules is implemented at the AODV protocol to degree specific parameters for numerous wide variety of nodes with specific metrics. The simulation of the proposed set of rules consequences have actually proved that the proposed method has better performance, extra powerful and detection accuracy over in comparison algorithms in numerous metrics together with throughput, packet transport ratio, cease to cease postpone and eating electricity. CWID detection method guarantees that the wormhole assault is dealt with for each kinds in-band and out-of-band assault. However, the proposed set of rules in preferred outperformed different algorithms in a set of measured parameters.

In the destiny we are able to cognizance on the use of Ad-hoc community in a big length topological vicinity which supplied more edibility and extra correct detection overall performance in wi-fi networks. In addition, we are able to triumph over the ingesting electricity because of the confined electricity deliver of cell node. It is of the maximum significance to cognizance of take a look at on wormhole assault detection, because it allows us via searching out extra feasible strategies to counteract the assault in our destiny research.

REFERENCES

[1]. N. Tamilarasi and S. G. Santhi, ``Detection of wormhole attack and secure path selection in wireless sensor network,"Wireless Pers. Commun., vol. 114, pp. 329345, Sep. 2020.

[2]. G.-H. Lai, ``Detection of wormhole attacks on IPv6 mobility-based wirelesssensor network," EURASIP J. Wireless Commun. Netw., vol. 2016, no. 1, p. 274, Dec. 2016.

[3]. Mohanapriya Marimuthu and Ilango Krishnamurthi"Enhanced OLSR for Defense against DOS Attack in Ad Hoc Networks", JOURNAL OF COMMUNICATIONS AND NETWORKS, VOL. 15, NO. 1, FEBRUARY 2013.

[4]. Y.-C. Hu, A. Perrig, and D. B. Johnson, ``Wormhole attacks in wireless networks," IEEE J. Sel. Areas Commun., vol. 24, no. 2, pp. 370380, Feb. 2006, doi: 10.1109/JSAC.2005.861394.

[5]. S. Majumder and D. Bhattacharyya, ``Mitigating wormhole attack in MANET using absolute deviation statistical approach," in Proc. IEEE 8th Annu. Comput. Commun. Workshop Conf. (CCWC), Las Vegas, NV, USA, Jan. 2018, pp. 317-320.

[6]. S. Qazi, R. Raad, Y. Mu, and W. Susilo, ``Multirate DelPHI to secure multirate ad hoc networks against wormhole attacks," J. Inf. Secur. Appl., vol. 39, pp. 3140, Apr. 2018.

[7]. S. Sankara Narayanan and G. Murugaboopathi, ``Modied secure AODV protocol to prevent wormhole attack in MANET," Concurrency Com- put., Pract. Exper., vol. 32, no. 4, Feb. 2020, Art. no. e5017, doi:10.1002/cpe.5017

[8]. S. Jamali and R. Fotohi, ``DAWA: Defending against wormhole attack inbMANETs by using fuzzy logic and articial immune system," J. Super-comput., vol. 73, no. 12, pp. 51735196, Dec. 2017

[9]. H. Sun Chiu and K.-S. Lui, ``DelPHI:Wormhole detection mechanism for ad hoc wireless networks," in Proc. 1st Int. Symp. Wireless Pervas. Com- put., Phuket, Thailand, 2006, p. 6, doi: 10.1109/ISWPC.2006.1613586.

[10]. Amara korba, M. Nafaa, and S. Ghanemi, ``Analysis of security attacks in AODV," in Proc. Int. Conf. Multimedia Comput. Syst. (ICMCS), Marrakech, Morocco, 2014, pp. 752-756, doi: 10.1109/ICMCS. 2014.6911193.

[11]. R. Singh, J. Singh, and R. Singh, ``WRHT: A hybrid technique for detection of wormhole attack in wireless sensor networks," Mobile Inf. Syst., vol. 2016, Jan. 2016, Art. no. 8354930

[12]. D. Dong, M. Li, Y. Liu, X.-Y. Li, and X. Liao, ``Topological detection on wormholes in wireless ad hoc and sensor networks," IEEE/ACM Trans. Netw., vol. 19, no. 6, pp. 17871796, Dec. 2011, doi: 10.1109/TNET.2011.2163730.