International Journal of Contemporary Technology and Management
Volume V , Issue XII , December 2016 ISSN (Online) 2278-8034

A survey on wormhole attack avoidance in mobile ad hoc network

Nitika Chaure
nitikachaure7@gmail.com
Computer Scince Department, Jagadguru Dattatray College Of Technology, Indore (India) R. G. P. V. Bhopal , M.P India

Khushboo Sawant (Ass.Pro.)
SawantKhshboo@gmail.comJagadguru Dattatrya College Of Technology,Indore (India)

Abstract–**mobile ad hoc network (MANET) is a rapidly growing network technology. In this technology the network is dynamic and usage the dynamic topology development for communication. Due to its dynamic nature of communication the routers are key component of technology. The routing techniques are responsible for route creation and their maintenance. Therefore most of security threads are deployed using the routing protocols. In this presented work a well-known security attack namely wormhole attack is investigated. Thus different approaches of wormhole attack detection and prevention is studied finally a new technique for securing the network by avoiding the attackers is prepared. The proposed technique and their working process are reported in this paper.**

Keywords:MANET, wormhole attack, solution development, security analysis, proposal

I. INTRODUCTION

With development of new technologies in the field of wireless communication, especially in wireless ad-hoc networks, mobile ad-hoc networks (MANET) have become an important research area nowadays. MANET is widely used in militarily monitoring, heath care, conference room, disaster relief, battle field communication and it is also useful also where infrastructure network deployment is either difficult or costly [1]. Wireless communication faces several security risks. An attacker can easily inject bogus packets impersonating another sender. In wireless ad hoc networks, nodes compromise to forward packets for each other to communicate beyond their transmission range. Security is a major concern for protected communication between mobile nodes in a hostile environment. In hostile environments adversaries can bunch active and passive attacks against intercept able routing in embed in routing message and data packets [2]. An ad-hoc network is a collection of wireless mobile hosts forming a temporary network without the assistance of any stand-alone infrastructure or centralized administration. Mobile Ad-hoc networks are self-organizing and self-configuring multi-hop wireless networks. Each node in mobile ad hoc networks is fit out with a wireless transmitter and receiver, which permits it to communicate with other nodes in its radio communication range. Nodes usually share the similar physical media; they transmit and get signals at the same frequency band, and follow the same hopping sequence or spreading code

Therefore the proposed work is dedicated to find the solution for mobile ad hoc network based attacks. During investigation a number of different routing attacks are establish persons are much regularly deploy in network and hard to recover. Thus the wormhole attack is selected for investigation and solution development. The wormhole attack in most of the situations is deployed by more than one attacker in network. These attackers are connected through the high speed data buses and attract the network traffic. The attracted traffic can causes the network performance losses or the congestion in network. This section provides the basic overview of the proposed work about the mobile ad hoc network and their security investigation.

In this proposed study the security in MANET investigation is primary aim, additionally to improve the security and trust in network a new technique development is the second key aim of the work. Therefore the following works are included in the proposed work.

a. **Study of various Security Schemes over MANETs Environment:** In order to find an optimum technique, various recently developed techniques are investigated and collected for study in this phase. Additionally an adoptable method is required to identify by which the security becomes more feasible for MANET.
b. **Investigation of Different Routing Attacks based on their Deployment Situation:** In this phase the different kinds of routing based attacks are studied additionally a detailed study on the Packet drop attack is also summarized
c. **Implementation of Proposed Work:** In this stage, key issues based on the Wormhole are addressed and their solution is prepared. Finally prepared solution is implemented with the help of NS - 2 simulation environments.
d. **Performance Analysis of the Proposed Secure Technique:** In this segment the performance estimation of the proposed security technique is

demonstrated, in addition of that with the similar network performance parameters proportional study is also listed.

In this section the core objective of the proposed work and the overview of the proposed work is described. In these listed objectives this paper provides the study on first two objectives additionally required security technique is also given in this paper.

II. BACKGROUND

This section provides the basic overview of the mobile ad-hoc network and their different area of applications. In addition of those different kinds of topology support is also provided in this section.

A. Wireless Network

Wireless network is a network set up by using radio signal frequency to communicate among computers and other network devices. Sometimes it's also referred to as Wi-Fi network or WLAN. This Wireless network is a network set up by using radio signal frequency to communicate among computers and other network devices. Sometimes it's also referred to as Wi-Fi network or WLAN [4].

Networking a large number of wireless devices in ad hoc mode will facilitate a wealth of applications not feasible under the conventional base station-to-network node communication model. The absence of infrastructure and the low-cost, on demand deployment makes ad hoc networks ideal candidate solutions for civilian applications such as disaster relief and emergency rescue operations, patient monitoring, and environmental control, as well as military applications such as target identification and tracking, and surveillance networks. On the other hand, an infrastructure less network has to rely on the collaboration among network nodes in implementing most, if not all, network operations. Moreover, due to limited resources of the wireless devices, algorithms and protocols are designed and implemented to allow distributed collaborative communication and computing involving multiple nodes. For example, two nodes that are not within the direct communication range will have to rely on intermediate nodes to exchange messages, thus forming multichip networks [5].

If you already have wired Ethernet network at home, you can attach a wireless access point to existing network router and have wireless access at home. Wireless router or access points should be installed in a way that maximizes coverage as well as throughput. The coverage provided is generally referred to as the coverage cell. Large areas usually require more than one access point in order to have adequate coverage. You can also add access point to your existing wireless router to improve coverage [4].

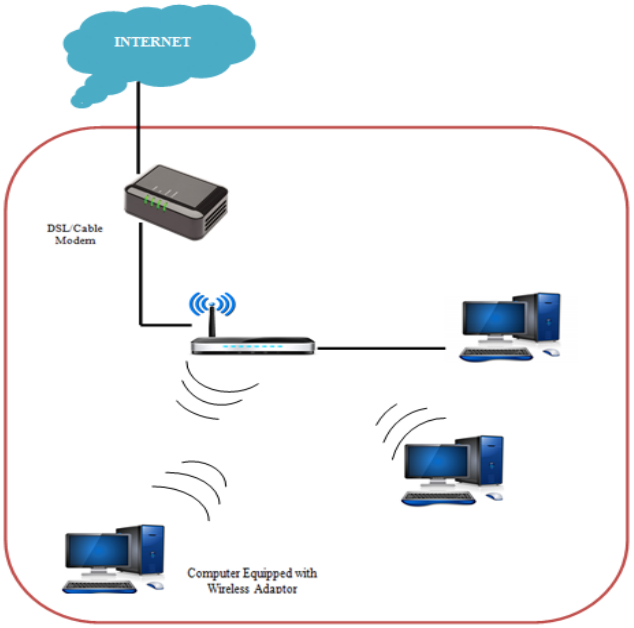

Figure1: wireless Network [4]

Advantages

- Mobile users are provided with access to real-time information even when they are away from their home or office.
- Setting up a wireless system is easy and fast and it eliminates the need for pulling out the cables through walls and ceilings.
- Network can be extended to places which cannot be wired.
- Wireless networks offer more flexibility and adapt easily to changes in the configuration of the network.

Disadvantages

- Interference due to weather, other radio frequency devices, or obstructions like walls.
- The total Throughput is affected when multiple connections exists

B. Mobile Ad hoc Networks: MANETs

Fast expansion of wireless communication technology and the broad usage of mobile communication tools, wireless ad hoc networks are getting more and more consideration. Nowadays, wireless ad hoc networks are not only used in military, but also been applied to civilian application, including home area networks, mobile communication networks, and so on. Wireless ad hoc networks are envisioned to be one of the most important parts of future Internet. However, in civilian wireless ad hoc networks, nodes often belong to different parties who have their own interests and always want to maximize their own benefits. Such selfish behavior can hurt

the robustness and availability of wireless ad hoc networks. Here solution concepts from microeconomics and game theory to study important incentive problems in wireless ad hoc networks, including spectrum allocation and routing. Here objective is to achieve a series of cooperation-incentive mechanisms with high availability, low cost, and high adaptability, through the following four closely related studies: game-theoretic problem modeling, impossibility analyzing, strong incentive mechanism designing, and systematic evaluation methodology is developing.

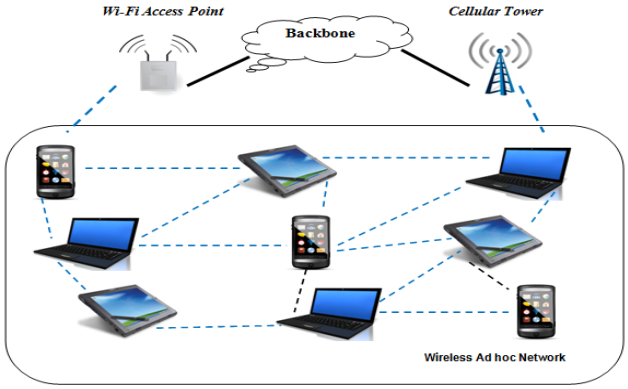

Figure 2: Wireless Ad hoc Network [6]

Mobile ad hoc network is a new technology. That is basically invented for those conditions where the management of huge infrastructure and maintenance is costly, such as battle ground. MANET (Mobile ad hoc network) is defined by its own characteristics; it is self-organizing, mobile communication manner where topologies are dynamically created. Due to the ad hoc nature of the network infrastructure and mobility it is still an area of new research and development. Due to mobility of wireless communication two major issues are found in such kind of network i.e. performance and security [7].

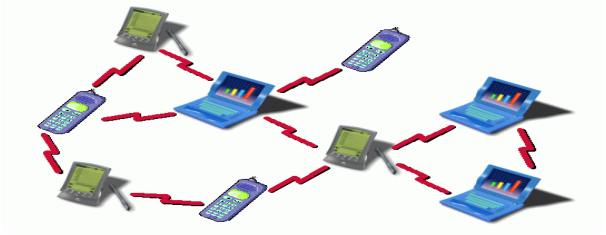

Figure 3: Mobile Ad Hoc Networks [8]

The above characteristics of MANET attract researchers in domain of MANET, but some key issues and challenges are also available which limit the performance and security of MANET. A MANET environment has to overcome certain issues of limitation and inefficiency. It contains [9]:

- **The Wireless Link Characteristics are Time-Varying in Nature**: There are some transmission impediments like vanishing, path loss, blockage and interference that add to the susceptible behaviour of wireless channels. The nature of the network depends upon the infrastructure that the network holds at that time.
- **A Limited Range of Wireless Transmission** – The limited radio band results in reduced data rates compared to the wireless networks. Hence the optimal usage of bandwidth is necessary by keeping low overhead as possible.
- **Packet Losses due to Errors in Transmission** – MANETs experience higher packet loss due to factors such as hidden terminals that results in collisions, wireless channel issues (high BER), interference, and frequent breakage in paths caused by mobility of nodes, improved collisions due to the presence of hidden terminals and unidirectional links.
- **Route Changes due to Mobility-** The dynamic nature of network topology results in frequent path breaks.
- **Frequent Network Partitions-** The random movement of nodes often leads to the partition of the set of connections. This mainly affects the intermediate nodes.

III. LITERATURE SURVEY

The given section introduces the different techniques and methods that are recently developed for optimizing the solutions for effective wormhole detection and prevention. These techniques are helps to develop an effective methodology for wormhole prevention.

Wireless Mesh Networks (WMNs) has become an emerging technology in recent days due to its easy deployment and low setup cost. In WMN, Routing protocols play an important role and these are susceptible to various kinds of internal attacks. One such attack that has severe impact on a WMN is a wormhole attack. A Wormhole is a low-latency link between two parts of the network through which an attacker tunnels network messages from one point to another point. In this paper, we specifically focus on wormhole attack launched by colluding nodes referred to as Byzantine wormhole attack. Unfortunately, most of the existing wormhole defense mechanisms are either centralized, or rely on additional hardware. The major challenge in detecting a byzantine wormhole link is the inability to distinguish nodes involved in the attack process, as they form the legitimate part of network. Being legitimate part of the network, they can bypass all security mechanisms and timing constraints imposed by the network. In this paper, ***P Subhash et al [9]*** propose a mechanism to prevent byzantine wormhole attack in WMNs. The proposed mechanism relies on digital signatures and prevents formation of wormholes during route discovery process and it is designed for an on-demand hop-by-hop routing protocol like HWMP (Hybrid Wireless Mesh Protocol-the default routing protocol for WMN). This is simplistic and also applicable to source routing protocols like DSR. This is a

software based solution and does not require additional (or) specialized hardware.

In this paper ***S. Capkun et al [10]*** present SECTOR, a set of mechanisms for the secure verification of the time of encounters between nodes in multi-hop wireless networks. This information can be used notably to prevent wormhole attacks (without requiring any clock synchronization), to secure routing protocols based on last encounters (with only loose clock synchronization), and to control the topology of the network. SECTOR is based primarily on distance-bounding techniques, on one-way hash chains and on Merkle hash trees. We analyze the communication, computation and storage complexity of the proposed mechanisms and we show that, due to their ef- ficiency and simplicity, they are compliant with the limited resources of most mobile devices.

Wormhole attacks enable an attacker with limited resources and no cryptographic material to wreak havoc on wireless networks. To date, no general defenses against wormhole attacks have been proposed. This paper presents an analysis of wormhole attacks and proposes a countermeasure using directional antennas. ***L. Hu et al [11]*** present a cooperative protocol whereby nodes share directional information to prevent wormhole endpoints from masquerading as false neighbors. This defense greatly diminishes the threat of wormhole attacks and requires no location information or clock synchronization.

The lack of centralized infrastructure in ad hoc network makes it vulnerable to various attacks. MANET routing disrupts if participating node do not perform its intended function and start performing malicious activity. A specific attack called Wormholes attack enables an attacker to record packets at one location in the network, tunnels them to another location, and retransmits them into the network. In this paper, ***S. Gupta et al [12]*** present a protocol for detecting wormhole attacks without use of any special hardware such as directional antenna and precise synchronized clock and the protocol is also independent of physical medium of wireless network. After the route discovery, source node initiates wormhole detection process in the established path which counts hop difference between the neighbours of the one hop away nodes in the route. The destination node detects the wormhole if the hop difference between neighbours of the nodes exceeds the acceptable level. This simulation results shows that the WHOP is quite excellent in detecting wormhole of large tunnel lengths.

Wireless Mesh Networks (WMNs) are widely used in many areas, such as industrial, commercial and public-safety environments. However, due to the open nature of wireless communication, it is relatively easy for an adversary to launch serious wormhole attack which can't be even prevented by cryptographic protocols. To enhance the efficiency and facility of wormhole detection, ***Huaiyu Wen[13]*** here propose a high efficiency wormhole detection algorithm based on 2-hop neighbor in WMNs, which is called Wormhole Detection based on Neighbor's Neighbor scheme (WDNN). Then a simple Random Walk Route scheme (RWR) is proposed to prevent routes from wormholes, which attract traffic of the routing protocols based on least cost. In WDNN, through enlarging the transmission range of the 2-hop neighbor, the faked network topology resulted by wormholes can be detected without using extra hardware or clock synchronization. In RWR, the route is chosen without using the low latency link which is created by wormholes. Security analysis shows that the wormhole attacks can be detected and also be prevented using our schemes efficiently. And our simulation results also indicate that our schemes can obtain a 100% wormhole detection rate and prevent routes from being attacked by the adversary against traditional routing protocols.

IV. PROPOSED WORK

The Mobile Ad hoc Network is one of the most popular networks in the different application oriented network technologies. The mobile ad hoc network having the various essential properties by which the various applications are getting the advantages of these properties. The network is a kind of distributed network technology by which the network information is not handled with the centralized control. Due to their wireless properties that are supports the mobility, in other words the network can be accessible from anywhere therefore the participating devices can move one place to another in random nature. But due to limited radio range network nodes are communicating with the help of intermediate nodes. These intermediate nodes are relaying the information by one to other in multi-hop manner. Due to this the responsibility on the routing algorithms are increases.

In this context the malicious user can also join the network and capture the sensitive information transmitted towards the base stations. Therefore in this presented work the security analysis against the wormhole attack is performed and the two phase solution for the malicious node discovery and prevention is suggested. In this methodology the network analyze the network user behavior and change on the basic behavior is estimated. By using this the list of suspected nodes are prepared and then after the suspect nodes are monitored continuously for finding the exact malicious node in network.

This section provides the basic details of the proposed solution for wormhole attack in the next section the detailed protocol design is presented by which the wormhole attacker is detected and prevented in Mobile ad hoc network.

A. Problem Identification

Due to study there are various models and IDS systems are found for detection and prevention of wormhole attack. Basically wormhole attack is performed using the routers and by more than one attackers in network. These attackers are advertise self for providing the efficient and less hop route to the target machine, and diverting the network traffic in

different directions. The main issues of this attack are summarized as:

- Complex in detection
- Nodes are acting as the normal node therefore identification of malicious nodes are complex.
- Due to mobility the nodes are not properly located in the network, during detection phases.

B. Methodology

The proposed technique needs to develop a method by which the routing algorithm self-detect and prevent the wormhole attack in network. Therefore the proposed technique needs to incorporate the following solution.

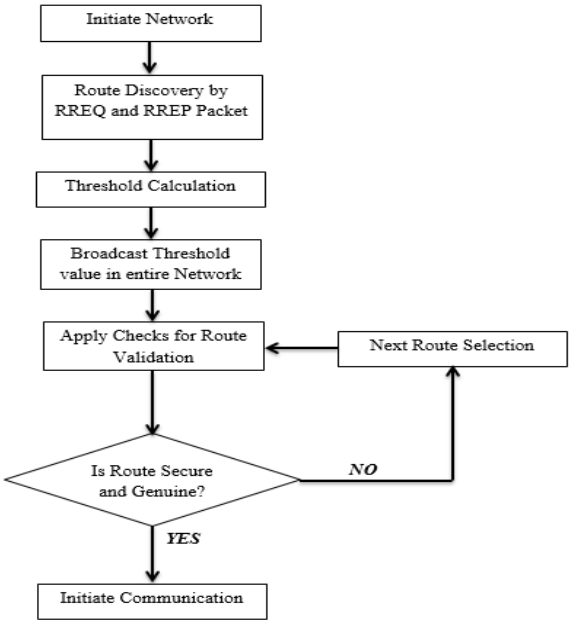

Figure 4 Flow diagram of Proposed Work

Existing detection technique based on 3 steps named Route redundancy, route aggregation and round trip time (RTT). Due to multiple RREQ & RREP there are extra overhead or load on the nodes of the routes. To overcome this load we proposed a scheme that minimizes routing overhead from the network. In this presented work a wormhole infected route is distinguished by comparing the RTT values of individual hop count, in addition of that in order to minimize the overhead in the system a load aware secure routing strategy is suggested in the proposed work.

V. CONCLUSION

In this presented paper the security issues in MANET is investigated. Therefore the first the MANET and their basic technology is discussed and then the recently contributed techniques and methods are studied. After concluding them, using the traditional techniques a new methodology for wormhole attack detection and prevention is developed and designed. In near future this approach is implemented using the suitable simulation technology and their performance is reported.

REFERENCE

[1] L. Zhou and Z. J. Haas, "Securing ad hoc networks," IEEE Network, vol. 13, no. 6, pp. 24– 30, 1999.
[2] PriyankaGoyal and SahilBatra, "A Literature Review of Security Attack in Mobile Ad-hoc Networks", International Journal of Computer Applications (IJCA), Volume 9 Number 12, November 2010.
[3] "What is Wireless Network", online available at: http://www.home-network help.com/wireless-network.html
[4] "How Wireless Networks Work", online available at: http://www.webopedia.com/DidYouKnow/Computer_Science/wireless_networks_explained.asp
[5] Fan Wu, "Economic Incentive Mechanisms for Wireless Ad Hoc Networks Principal Investigator", Natural Science Foundation of China (NSFC), 2012.
[6] Mario Gerla, Ling-Jyh Chen, Yeng-Zhong Lee, Biao Zhou, Jiwei Chen, Guang Yang, Shirshanka Das, "Dealing with node mobility in ad hoc wireless network", Computer Science Department, UCLA, Los Angeles, CA 90095, USA
[7] "Ad Hoc Networks", ARC Communications Research Network, available online: http://www.acorn.net.au/telecoms/adhocnetworks/adhocnetworks.html
[8] ImrichChlamtac, Marco Conti, Jennifer J.-N. Liu, "Mobile ad hoc networking: imperatives and challenges", Ad Hoc Networks 1 (2003) 13–64.
[9] P Subhash and S Ramachandram, "Preventing Wormholes in Multi-hop Wireless Mesh Networks", Third International Conference on Advanced Computing & Communication Technologies, pp. 293-300, 2013.
[10] S. Capkun, L. Buttyan and J.P., Hubaux, "SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks", In Proceedings of 1st ACM Workshop on Security of Ad hoc and Sensor Networks (ACM SANS), pp. 21-32, New York, USA, 2003.
[11] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks," In Network and Distributed System Security Symposium (NDSS), San Diego California, USA, 5-6 February, 2004.
[12] S. Gupta and S. Dharmaraja, "WHOP: Wormhole Attack Detection Protocol using Hound Packet", In International Conference of Innovations in Information Technology, PP. 226 – 231, 2011.
[13] Huaiyu Wen, and GuangchunLuo, "Wormhole Attacks Detection and Prevention Based on 2-Hop Neighbor in Wireless Mesh Networks", Journal of Information & Computational, PP. 4461–4476, September 20, 2013.