Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

Determining and Avoiding Wormhole Attack in MANET

Gulzar Ahmad Wani[1], Dr Sanjay Jamwal[2]
[1,2]*Department of Computer Science, BGSB University, Rajouri,,*

Abstract—In Mobile Adhoc network is accountable for path establishment from source to destination using multi-hop routing. It uses wireless medium i.e., radio signal for transmission. In MANET each node acts as a router and end node. i.e., it receives the data packet and then processes it and forwards it to another node along a path. MANET is vulnerable to different security attacks because of open and dynamic nature with a minute security measures. Wormhole attack is a tunneling attack and is one of the server attacks among all security attacks which involve two or more malicious nodes that are on either side of tunnel. Attacker attracts data packet from neighbors and transmits via tunnel and passes it to another attacker on other side. The wormhole attack is the most strongest and is difficult to detect. In this proposed paper, we did a change in AODV protocol that detects and avoids wormhole attack in MANET and make MANET secure for transmission.

Keywords—MANET, Wormhole Attack, AODV, Maximum hop-count.

I. INTRODUCTION

Wireless communication is one of the most vibrant areas in the communication field today. Wireless communication is the process of sending information from sender to receiver without use of any physical medium i.e., cables, wires. The distance between two communicating parties may be small (in meters for instance television remote control) and very far away (in thousands kilometers for instance radio communication). The well-known devices used in wireless communication are GPS system, cordless telephone and mobiles etc.The radio wave, ultrasonic, electromagnetic induction are the modes of wireless communication. Wireless communication is suitable for such environment where it is infeasible or impractical to lay down the wires.

One of the most demanding wireless networks is wireless Adhoc network which is also known as IBSS Independent Basic Service Set. It is network where connecting links between devices are wireless and term Adhoc means that each mobile device is doing both jobs i.e., one receiving the packet and then forwarding that packet to other mobile nodes. Based on mobile device connectivity, the selection of mobile node that forwards the data is done dynamically [1] .The Adhoc network is categorized into different types based on its applications [2].

1. Mobile Adhoc network
2. Vehicular Adhoc network
3. Smart phone Adhoc network
4. Internet based mobile Adhoc network (iMANET)
5. Military and tactical MANET

1.1. Mobile Adhoc Network (MANET)

6. It is continues self-configuring, infrastructure less and dynamic topology of mobile nodes connected without wires.

1.2. Vehicular Adhoc Network

It is the blind of Adhoc network that allows communications among vehicles and roadside equipments like traffic signals. It allows traffic to operate in a intelligent manure by using artificial intelligence.

1.3 Smart Phone Adhoc Network:

It is the network that makes maximum use of preexisting hardware (like Bluetooth, WiFi) in market available smart phones to make Peer-to-Peer network without depending upon cellular carrier network, wireless access points or traditional network infrastructure.

1.4. Internet Based Mobile Adhoc Network

Here mobile nodes and internet gateway are connected by means of Adhoc network. e.g., CloudRelay.

1.5. Military and Tactical MANET: It is Communication between devices that are used by defense organizations. Here emphasis is on security range.

In MANET [3] mobile nodes have restricted geographical range and sending message to the node that is not in transmission range can be sent through broadcast mechanism. The broadcast mechanism is used by the router for delivery the message to destinations that is not in the sender's range. The router uses routing protocols for accomplishing the broadcast mechanism. To manage connectivity of very large number of mobile devices that are provide with limited resources like bandwidth, energy and batter backup constraint, is the job of routing protocols. The main obstacle that routing protocols faces are nodes dynamic location i.e., node changes location frequently. The various routing protocols that are used in routing protocols are DSDV(Destination Sequenced Distance Vector) [4], OSPF (Open Shortest Path First)[5], DSR (Dynamic Source Routing)[6], AODV (Adhoc On-Demand Distance Vector)[7].The main goal of these protocols was to route the packet efficiently, due to which these routing protocols lacks the security measures. There are various security threats to MANET that can create harm to our network like black hole, gray hole, eavesdropping and wormhole attack [8].

Security in mobile ad-hoc network is the current important issue of network. The Services of network like confidentiality and integrity of data is attained by facing and solving the security issue of MANET. The dynamic topology and open nature makes the wireless network (especially Mobile Ad-hoc network) more vulnerable to security threats. The various loopholes that threatens the security of wireless network that consists of sink/black hole, MAC spoofing, Denial-of-Service attack , Network injection, worm hole, Man-in-the-middle attacks, Sybil attack and etc.

In wormhole attack two far away distinct nodes are connected with high speed tunnel also called wormhole tunnel (Figure 1). The node at one end of tunnel attracts packets from the neighbor node by giving offers like lower hop-count; than the normal routes, and passes these packets via tunnel to other end. Where another attacker node delivers into the destination address. Data passing via tunnel may result various data theft attacks like- black hole, gray hole and denial of services (DoS). The rest of paper is categorized into different sections where section II describes related work of wormhole detection, section III provides proposed work and section IV and V provide simulation and conclusion respectively.

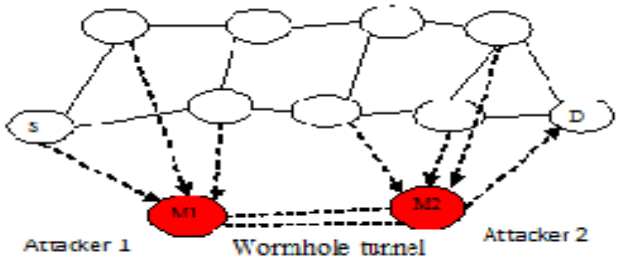

Figure 1. Wormhole attack in MANET

II. LITERATURE REVIEW

The basic method to detect and prevent wormhole attack is a leash method .A packet leash means adding some extra information to sending packet. Packet leashes method proposes two methods:

Geographical method

Each node in the network knows its current position with the help of Global Positioning System (GPS) and are having loosely synchronized clock. During geographical leashes, a node appends its current location (Ls) and sent time of a packet (Ts) before sending the packet [12].

The receiving node receives the packet and use its own location (Lr) and time it receives the packet(Tr) to determine the distance of packet it travelled, provided that

Maximum possible node velocity V
Clock synchronization error Δ
Possible GPS distance error σ
Distance between sender and receiver dsr
$dsr < \| Ls - Lr \| + 2v | Tr - Ts + \Delta | + \sigma$

This distance is used to determine whether data packets travel through wormhole link or not.

Temporal Leashes

In this type of leashes [1230], nodes in the network do not require the GPS but nodes must have tight clock synchronization. The sender node appends time of transmission Ts in the leash field of packet and receiving node uses its reception time Tr of packet for verification. The sender node calculates the expiration time Te for the packet after which packet should be not accepted and adds this information also to the leash field of packet. The expiration time Te is calculated as below

$$Te = Ts + (L / C) + \Delta$$

Where Ts time of transmission,C is the speed of light, Δis maximum clock synchronization error, and L is the maximum distance that packet can travel.

The receiver node uses speed of light as transmission propagation speed and its local time to find the distance up to the sender node or to find the distance travelled by the packet. Hence receiver node are capable to find whether the packet comes through the wormhole link or not.

L.Hu and D. Evans [9] analyses the wormhole attack and proposed an approach where mobile nodes are outfitted with directional antennas. For the need of communication with each other, nodes use some specialized sector of directional antennas. A relation between the nodes is set if direction of signal between node pair matches. This method is inexpensive and makes best utilization of MANET resources like energy and bandwidth. The only one problem with this approach is that if the attacker puts himself tactically in MANET

Katrin Hoper et.al [10] suggested a protocol that is performing its operation without use of any additional hardware like clock synchronization and directional antennas. In this method routes are discovered first then detection of wormhole takes place by using Hound Packet (uses hop-count as metrics). This approach is very much efficient in detection of large tunnel attacks. This approach is also physical medium independent.

The author [11] proposed a mechanism for detecting wormhole infected path based on determining the Round Trip time (RTT) between two nodes in the network during route discovery phase. The main idea of this approach depends on the fact that the transmission time between the legitimate nodes is lower than the illegitimate nodes. This approach has proven good performance as compared to the rest of techniques and also it does not require any hardware. Although it has minute overhead.

III. PROPOSED WORK

In proposed paper, we provide a method that avoids selection of wormhole infected path from source to destination by making a little change in AODV routing protocol. Normally AODV chooses the best path for transmission of packet from source to destination based on shortest hop-count and less traffic. A minute change in AODV routing protocol is made to provide wormhole free path by using that information from neighbor nodes.The main purpose of proposed technique to find a wormhole free path selected by AODV routing protocol.

Some Assumptions are:

Ni = Any Random node.

NbJ=neighbor node of Ni

T(NbJ)= total no of neighbor node of Ni

GHC = Greatest Hop-Count

HR=Hop-count from reply

The decision of taking whether route is wormhole infected or not is based on hop –count between node to its next-to-next node in alternate paths. If the hop-count between the node to its next-to-next node is greater than Greatest hop-Count (GHC) then its stated route is having wormhole attack as shown in Figure 2. The Greatest Hop-count is calculated with the help of hop-count and neighbor node information. Every node in the network finds the routes with largest number of hops over the entire possible routes between it and it's next to next node. Consider average of highest hop-count of the node as GHC as shown in Figure 3

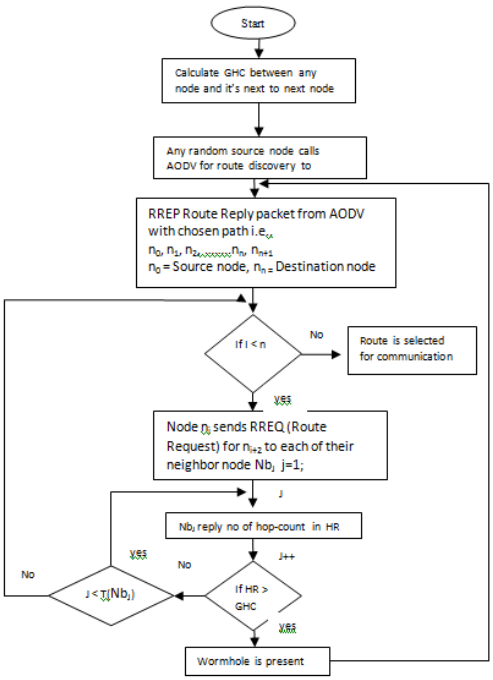

Figure 2. Technique for Wormhole Detection

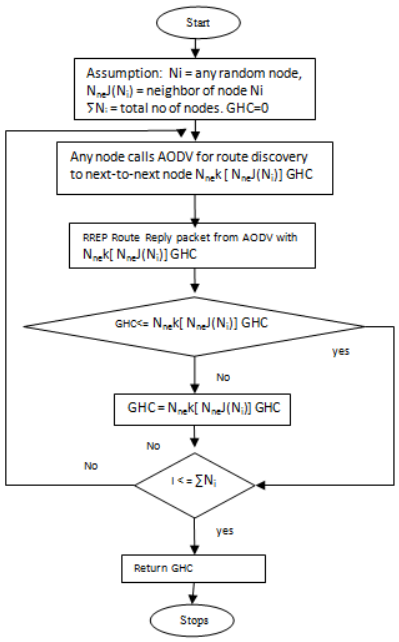

Figure 3: Greatest Hop-count Calculation

IV. EXPERIMENTAL ANALYSIS

For simulation purpose, we used NS2 simulator for Simulation and simulated different scenarios with having different node density e.g., 140, 160, 180 and 200 with keeping all parameters same.

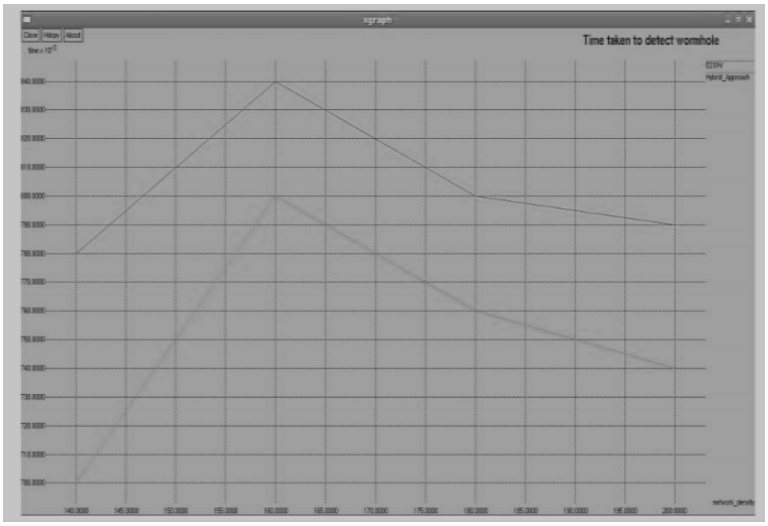

Figure 4. Duration of time taken for wormhole detection

Figure 4 shows the rate of wormhole detection depends on the node's density and Greatest Hop-count is considered as key on which wormhole detection depends on.

Wormhole attack occur's between any node and its next-to-next node. Duration of time taken for detection of wormhole attack in proposed technique is very mush less as compared other techniques. Its takes only 550 mili seconds of time in proposed technique where as in other technique it takes 790 and more mili seconds.

Other techniques use extra energy for locating the location information i.e., 1 joule of energy is used for collection location details. This 1 Joule of is energy is saved in proposed technique.

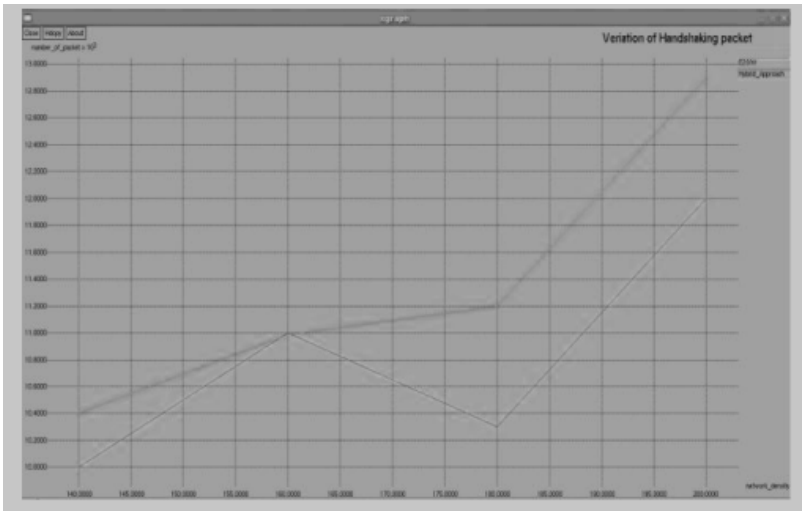

Figure 5. Comparison between proposed technique and E2SIW over handshaking

Figure 5 shows that proposed technique uses number of control packets for wormhole detection as compared to AODV. The above figure shows the detection technique works well but

having some overhead and increases packet overhead . but the main benefit is that when added with existing AODV protocol works well.

V. CONCLUSION

In this paper, the proposed technique detects and avoids the wormhole attack in mobile Adhoc network without using any extra hardware device like antenna, GPS system or Clock synchronization. This technique uses n hop-count for detection purpose. The performance and reliability of network depends on the node density and power consumption of the node.

In future to detect and avoid the wormhole attack in more efficiently for larger number of control packet and large density of nodes in the network

VI. REFERENCES

[1]. Ozan,k.Tonguy, Gianluigi Ferrari, John Wiley& Sons.ed.Adhoc Wireless Network: A communication Theoretic perspective,2006.

[2]. Tomas Krag and Sebastian Büettrich (2004-01-24). "Wireless Mesh Networking". O'Reilly Wireless Dev Center. Retrieved 2009-01-20.

[3]. P.Michiardi and R. Molva, "CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc network", In Proc. 6th IFIP Commun and Multimedia Security Conf. ,Sept.2002.

[4]. S.Marti et al., ''Multigatting Routing Misbehaviour in Mobile Adhoc Networks", Proc . 6th Ann. ACM int'l Conf. Mobile Computing and Networking ACM Press, 2000,pp 255-265.

[5]. S. Buchegger and J-Y. le Boudee, "Performance analysis of the CONFIDANT Protocol", In Proc. 3rd ACM Intl, Symp., On Mobile Adhoc Networking and Computing, Jun 2002.

[6]. P.G Argyroudis and D.O' Mahony," Secure Routing for mobile ad hoc networks", IEEE communication Survey and Tutorials, third quarter 2005, vol. 7, no3,2005,258. Authorized licensed use limited to : University of Allahabad. Downoaded on July 30,2010 from IEEE Xplore, Restrictions apply.

[7]. R.Mavropodi, P. Kotzanikolaou, and C. Douligeris, "Performance analysis of Secure Multipath Routing Protocols for Mobile Adhoc Networks, WWIC 2005, LNCS 3510, pp, 269-278, 2005.

[8]. Khabbazian, M.Mercier, H.; Bhargava, V.K Severity Analysis and Countermeasures for the Wormhole Attack in Wireless Network. IEEE Trans. Wireless Commun 2009, 8, 736-745.

[9]. L.Hu and D. Evans, "Using Directional Antenna to prevent Wormhole Attack ", in Network and Distributed System Security Symposium (NDSS), 2004.

[10]. Katrin Hoeper, Guang Gong, "pre-Authentication and Authentication models in Adhoc Network", Signal and Communication techonology, pp. 65-82, 2007.

[11]. Phuong Van et al. "TTM: An Effiecient Mechanism to Detect Wormhole Attack in Wireless Adhoc Networks".

[12]. Dabas , Poonam and Prateek Thakral. " A Novel Technique for the Prevention of Wormhole Attack", International Journal 3, no.6, 2013.

