DETECTING WORMHOLE ATTACK IN MOBILE AD-HOC NETWORKS

Mr. Chaudhari Vishvash R.[1], Mr. Vinitkumar Gupta[2]
[1]Computer Engineering Student, [2]Deptartment of Computer Engineering
Hasmukh Goswami College of Engineering
Ahmedabad, Gujarat, India.

Abstract: A Mobile Ad Hoc Network (MANET) is self-organizing, less infrastructure, multi-hop networks. In wireless network and distributed nature of MANETs poses a huge challenge to system designers. Mobile Ad hoc networks are by used very open to any person. Anyone with the proper knowledge of the network topology and hardware then protocols can connect to the network. They allow potential attackers to gain access to the network and carry out attacks on its participants with the purpose of Disrupt the network or stealing or altering information. A specific type of attack, the Wormhole attack does not require exploiting any nodes in the network and can interfere with the route establishment process. It does not require any cryptographic primitives. This attack targets specifically routing control packets, the nodes that are close to the attackers are shielded from any alternative routes with more than one or two hops to the remote location. All routes are thus directed to the wormhole established by the attackers.

Index Terms: MANET, Wormhole Attack, Detection Method. (Key words)

I. INTRODUCTION

In mobile ad hoc networks to Several Challenging Problems Continues to Attract Research projects. They include multicast routing; power Consumption, Quality of Service and security. It is also possible access to some hosts in a fixed infrastructure or infrastructure less, depending on the mobile ad hoc network available. Some cases where a Mobile ad hoc network can be used are government or business Person sharing data during a meeting, emergency disaster relief personnel coordinating efforts after all natural disaster such as an earthquake, or flooding, and military personnel relaying tactical and other types of information in a battlefield. MANETs are originally motivated by military applications such as border surveillance and battlefield monitoring. MANET can be used in many civilian applications, including all home automation, healthcare, traffic control and habitat/environment monitoring. Basic security services of MANET include authentication, confidentiality, integrity, non-repudiation and availability. Tunneling attack does not require exploiting any nodes in the network and can interfere with the route establishment process. By the versatile nature of their application domain, mobile ad hoc networks are very likely to be often deployed in hostile environments. Due to numerous constraints such as, infrastructure less, dynamic topology and lack of pre-established trust relationships between nodes, most of the routing protocols for mobile ad hoc networks are vulnerable to a number of disruptive attacks

II. GENERAL DESCRIPTION OF ATTACKS

Routing is a very important function in MANETS. It can also be easily misused, leading to several types of attack. Routing protocols in general are create colluding nodes from an illusion that two remote regions of colluding nodes create an illusion that two remote regions of a MANET are directly connected through nodes that appear to be neighbors but are actually distant from one another . These protocols are usually not designed with security in mind and often are very vulnerable to node misbehavior. This is particularly true for MANET routing protocols because they are designed for minimizing the level of overhead and for allowing every node to participate in the routing process. Making routing protocols efficient often increases the security risk of the protocol and allows a single node to significantly impact the operation of the protocol because of the lack of protocol redundancy. Below are some examples of attacks that can be launched against MANET routing protocols.

A. Black Hole Attack

In this attack, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. The attacker will then receive the traffic destined for other nodes and can then choose to drop the packets to perform a denial-of-service attack, or alternatively use its place on the route as the first step in a man-in-the-middle attack by redirecting the packets to nodes pretending to be the destination.

B. Spoofing

A node may attempt to take over the identity of another node. It then attempts to receive all the packets destined for the legitimate node, may advertise fake routes, and so on. This attack can be prevented simply by requiring each node to sign each routing message (assuming there is a key management infrastructure). Signing each message may increase the bandwidth overhead and the CPU utilization on each node.

C. Modifying Routing Packets in Transit

A node may modify a routing message sent by another node. Such modifications can be done with the intention of misleading other nodes. For example, sequence numbers in routing protocols such as AODV are used for indicating the freshness of routes. Nodes can launch attacks by modifying the sequence numbers so that recent route advertisements are ignored.

D.Ppacket Dropping

A node may advertise routes through it to many other nodes and may start dropping the received packets rather than forwarding them to the next hop based on the routes advertised. Another variation of this attack is when a node drops packets containing routing messages. These types of attacks are a specific case of the more general packet dropping attacks.

E. Selfish Nodes

Routing in MANET depends on the willingness of every node to participate in the routing process. In certain situations nodes may decide not to participate in the routing process. For example, nodes may do that in order to conserve battery power. If several nodes decide to do that then the MANET will break down and the network will become inoperable. Certain protocols have been proposed for encouraging nodes to participate in the routing process.

F. Wormhole Attack

In this attack adversaries can collude to transport routing and other packets out of band (using different channels). This will interfere with the operation of the routing protocols.

G. Rushing Attack

In this case, an adversary can rush some routing packets towards the destination, leading to problems with routing. Among all this attack, wormhole attack is very hard to detect because it does not require any cryptographic break. Without knowing any security material am attacker can launch the attack.

III. DEMOSTRATION OF A WORMHOLE ATTACK

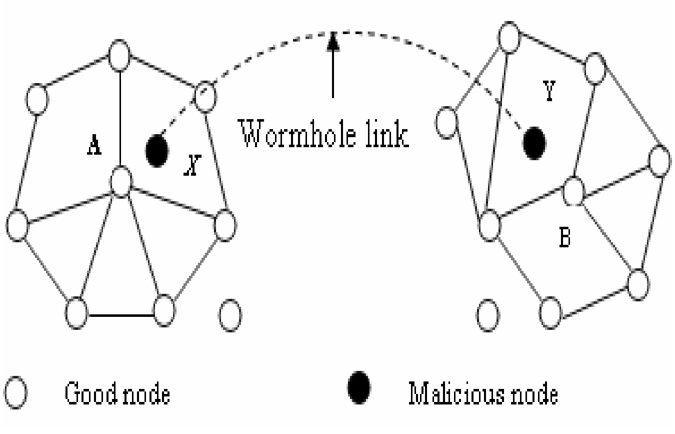

Fig.1 Demonstration of a wormhole attack.

A typical Tunneling attack requires two or more attackers - malicious nodes - who have better communication resources than regular sensor nodes. The attacker creates a low-latency link (i.e. high-bandwidth tunnel) between two or more attackers in the network. Attackers promote these tunnels as high-quality routes to the base station. Hence, neighboring sensor nodes adopt these tunnels into their communication paths, rendering their data under the scrutiny of the adversaries. Once the tunnel is established, the attacker collect data packets on one end of the tunnel, sends them using the tunnel (wired or wireless link) and replays them at the other end as shown in fig.1. Wormholes are hard to detect because the path that is used to pass on information is usually not a part of the actual network. Interestingly, a wormhole itself does not have to be harmful; for it usually lowers the time it takes for a package to reach its destination. But even this behavior could already damage the operation, since wormholes fake a route that is shorter than the original one within the network; this can confuse routing mechanisms which rely on the knowledge about distance between nodes.

.

IV. PROPOSED ALGORITHM

Step 1: Sender will create an information packet with information 1.Sender's current time 2. Next packer interval 3.Sender network address 4.Receiver network address 5. Sending time and Sender will encrypt this package using a randomly generated encryption key

Step 2: Sender will set its time clock as per next packet interval (i.e. after this time sender will generate new information packet) Sender will remember encryption key and time to send packet.

Step 3: on receiving packet, receiver will note time of receiving packet and will wait for time to receive key to decrypt.

Step 4 : after fix time (this time will be decide on network parameter and it should be enough time that before it ends any how receiver will receive information packet)

Sender will broadcast key to decrypt information packet.

Step 5: upon receiving key to decrypt receiver will decrypt information packet and synchronize its time with sender clocks.

Step 6: receiver will count network delay using sender's sending time – receiving time

Step 7: if this time is more than normal network delay it detects wormhole in network

Step 8: receiver will get time to receive next information packet. If receiver doesn't get packet in time (next packet interval + network delay timing) , it indicates there are some wormhole in the network who are performing DOS .

Step 9: To check first mechanism, called the Neighbor Number Test (NNT), detects the increase in the number of the neighbors, which is due to the new links created by the wormhole in the network.

Step 10: The second mechanism, called the All Distances Test (ADT), detects the decrease of the lengths of the shortest paths between all pairs which is due to the shortcut links created by the wormhole in the network.

Step 11: Both mechanisms assume that their neighbor list to the base station and it is the base station that runs the algorithms on the network graph that is reconstructed from the received neighborhood information.

A. Performance Analysis

Simulation Parameter

Simulator	NS-2
Protocol	DSR
Communication type	CBR
Number of nodes	25
Simulation area	500m*500m
Simulation time	500 s

Effects of wormhole attack Effect of wormhole attack in the network is that packet is not reached to the destination as shown in the fig we carried out the simulation using ns2.We used AODV protocol. In Fig. shown without wormhole attack packet reached to the destination. Varying throughput with time indicate that the packet reached to the destination but in the Fig shown with the wormhole attack there is constant line i.e zero throughput ,which indicate that no packet is reached to the destination because malicious node dropped all the received packet. So no packet is received at the destination.

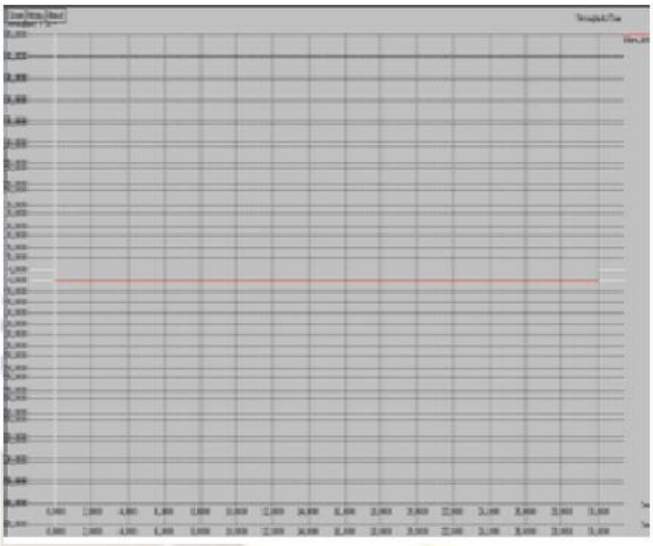

Fig. 2:Wormhole detection graph

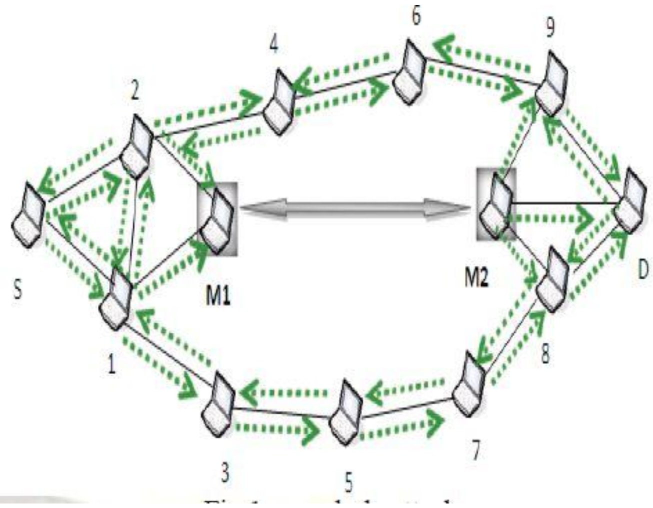

Fig. 3: Wormhole link

Wormhole attack is a network layer attack. In a typical wormhole attack at least two colluding nodes in the network are located at different places that are not in direct communication range of each other i.e. one near to the source node and another near to the destination node thus bypassing information from source node to destination node and disrupting proper routing. In Fig. 1, M1 and M2 are two colluding nodes. The malicious node M1 takes data near the source node then tunnels it to M2 placed near the destination node. Communication of data occurs via path having this low latency link all the times due to less number of hops.

V. CONCLUSION

Security is very crucial for MANET. In this work, we propose Improve Detection Method using Timestamp of sending packet and receiving packet. Using this routing scheme we will increase the delivery ratio and reduce the delivery latency. It gives better result compare to other methods of Detection and here we have to provide security if malicious node creates a tunnel then it will not alter the message and here we have to find the wormhole link is created or not

REFERENCES

[1] Lazos, L.; Poovendran, R.; Meadows, C.; Syverson, P.; Chang, L.W. Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach. In IEEE WCNC 2005, Seattle, WA, USA, 2005; pp. 1193–1199.

[2] Khalil, S. Bagchi, and N. B. Shroff. LITEWORP: A lightweight countermeasure for the wormhole attack in multihop wireless networks. In Dependable Systems and Networks (DSN), pages 612–621, Jun 2005

[3] Hu, Y.C.; Perrig, A.; Johnson, D.B. Wormhole Attacks in Wireless Networks. IEEE J. Sel. Area Comm. 2006, 24, 370–380

[4] L. Hu and D. Evans. Using directional antennas to prevent wormhole attacks. In Proceedings of the Network and Distributed System Security Symposium. 2004.

[5] Jen S.-M.; Laih C.-S.; Kuo W.-C. A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET.Sensors. 2009.

[6] Shalini Jain and Dr.Satbir Jain. Detection and prevention of wormhole attack in mobile adhoc networks. International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010.

[7] S. Özdemir, M. Meghdadi, and Ý. Güler. "A time and trust based wormhole detection algorithm for wireless sensor networks," (manuscript in Turkish), in 3rd Information Security and Cryptology Conference (ISC′08), pp. 139−4, 2008.

[8] Preeti Nagrath, Bhawna Gupta. Wormhole Attacks in Wireless Adhoc Networks and their Counter Measurements: A Survey. In IEEE WCNC 2011, Seattle, WA, USA, 2011; pp. 978-1-4244-8679-3/11

[9] Manikandan K.P. Satyaprasad R.; Rajasekhararao. Analysis and Diminution of Security Attacks on Mobile

Ad hoc Network. IJCA Speial Issue on MANETs, 2010.

[10] JenS.-M.; LaihC.-S.; KuoW.-C.A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET. Sensors. 2009.

[11] J. M. Kahn, R. H. Katz, and K. S. J. Pister, "Next century challenges: mobile networking for smart dust," in Proc. 5th Ann. Int. Conf. Mobile Compu.Netw,, Aug. 1999, pp. 271–278.

[12] Bulusu, N, J. Heidemann and D. Estrin. "GPS-less Low Cost Outdoor Localization for Very Small Devices." IEEE Personal Communications Magazine, October 2000. 23 October 2003.

[13] He, Tian, Chengdu Huang, Brain M. Blum, John A. Stankovic and Tarek Abdelzaher. "Range-Free Localization Schemes for Large Scale Sensor Networks." Mobicom 2003. 23 October 2003

[14] Y. Hu, D. Johnson, and A. Perrig. SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. IEEE Workshop on Mobile Computing Systems and Applications, June 2002.

[15] Y-C Hu and A. Perrig "A Survey of Secure Wireless Ad Hoc Routing", IEEE Sec. and Privacy, 2004

[16] K. Sanzgiri "A Secure Routing Protocol for Ad Hoc Networks", Proc. 2002 IEEE Int\'l. Conf. Network Protocols, 2002

[17] Y-C. Hu, A. Perrig and D. Johnson "Wormhole Attacks in Wireless Networks", IEEE JSAC, vol. 24, no. 2, 2006