International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 3, Issue 10, October 2014 **ISSN 2319 - 4847**

Wormhole Attack Detection Technique in Mobile Ad Hoc Networks

[1]NEHA KULKARNI , [2]VINOD S. WADNE

[1]Department of Computer Engineering
Imperial College Of Engineering And Research, Wagholi, Pune

[2]Department of Computer Engineering
Imperial College Of Engineering And Research, Wagholi, Pune

ABSTRACT

MANET (Mobile Ad-hoc Network) refers to a multi-hop packet based wireless network composed of a set of mobile nodes that can communicate and move at the same time , without using any kind of fixed wired infrastructure . MANET'S are actually self organizing and adaptive networks that can be formed and deformed on-the-fly without the need of any centralized administration. It generally works by broadcasting the information and used air as medium. It's broadcasting nature and transmission medium also help attacker to disrupt network. Many type of attack can be done on such Mobile Ad Hoc Network. Our approach for wormhole detection enables the receiver to detect wormhole nodes using unobservable routing .We proposed an efficient method to identify the wormhole nodes exists in the routing path and rediscover new routes from the source node to target node . By applying an improved hop count based detection checking its one hop neighbors from its neighbor table. Once the wormhole nodes are detected then remove the wormhole entries from its neighbor table.

Keywords: – Wormhole; Malicious : DOS

1.INTRODUCTION

The MANETs work without a centralized administration where the nodes communicate with each other on the basis of mutual trust. This characteristic makes MANETs more vulnerable to be exploited by an attacker inside the network. Wireless links also make the MANETs more susceptible to attacks, which makes it easier for the attacker to go inside the network and get access to the ongoing communication. Mobile nodes present within the range of wireless link can overhear and even participate in the network. Security in Mobile Ad-hoc Networks (MANETs) is the most important concern to achieve its basic functionality without errors. The availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANETs often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battlefield situation for the MANETs against the security threats because of infrastructure less nature. MANETs must have a secure way for transmission and communication and this is a quite challenging and vital issue as there are increasing threats of attack on the Mobile Networks. In order to provide secure communication and transmission, the engineers must understand different types of attacks and their effects on the MANETs. Wormhole attack, Black hole attack, Sybil attack, Flooding attack, Routing table overflow attack, Denial of Service (DoS), Selfish node misbehaving, Impersonation attack are the kind of attacks that MANETs can suffer from. MANETs are more open to these kinds of attacks because communication is based on mutual trust between the nodes, there is no central point for network management, no authorization facility, vigorously changing topology and limited resources.

2 .WORMHOLE ATTACK

Wormhole attack is a network attack layer. 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 the destination node thus bypassing information from source node to destination node and disrupting proper routing. In figure 2.7 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.

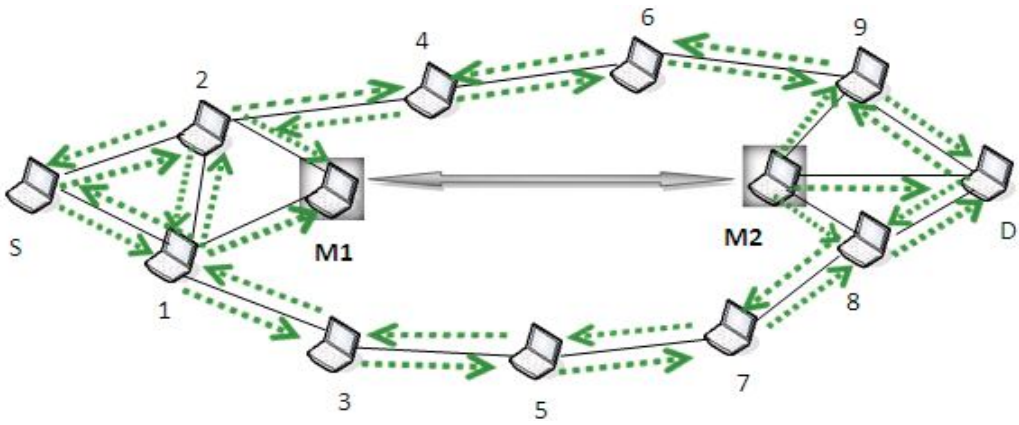
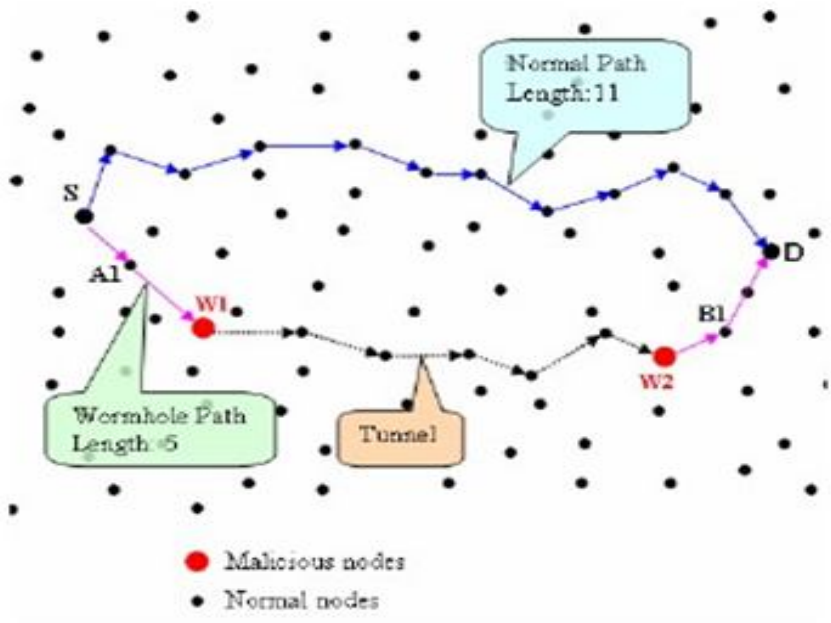


Figure 2.7: wormhole attack

Wormhole Attack and Classification Before discussing wormhole attack, first we try to understand types of attacks in Mobile Ad-hoc Networks. There are several ways to classify wormhole attacks. Here we divide wormhole attacks into 2 categories: hidden attacks & exposed attacks, depending on whether wormhole nodes put their identity into packets' headers when tunneling & replaying packets .



2.1Hidden Attacks

Before a node forwards a packet, it must update the packet by putting their identity (MAC address) into the packet's header to allow receivers know where the packet directly comes from. However, in hidden attacks, wormhole nodes do not update packets' headers as they should so other nodes do not realize the existence of them. a packet P sent by node S is overheard by node W1. W1 transmits that packet to node W2 which in turn replay the packet into the network. Because W1 & W2 do not change the packet header so D seems to get the packet directly from S. In this way, D& S are neighbors although they are out of radio range from each other (fake neighbors). General speaking, in hidden attacks nodes within W1's vicinity are "fake neighbors" of nodes within W2's vicinity and vice versa. In this kind of attack, a path from S to D via wormhole link will be:

$$S \rightarrow A1 \rightarrow B1 \rightarrow D$$

In the viewpoint of legitimate nodes, there is no existence of W1 & W2 in the path (hidden).

2.2.Exposed Attacks

In exposed attacks, wormhole nodes do not modify the content of packets but they include their identities in the packet header as legitimate nodes do. Therefore, other nodes are aware of wormhole nodes' existence but they do not know wormhole nodes are malicious. In case of exposed attacks, the path from S to D via wormhole will be:

$$S \rightarrow A1 \rightarrow W1 \rightarrow W2 \rightarrow B1 \rightarrow D$$

2.2.2 In hidden attacks, there are many fake neighbors created by wormhole link but there's no fake neighbor except (W1, W2) in this case. This difference leads to differences in detection mechanisms. Some mechanisms which can do well in detecting hidden attacks cannot detect exposed attacks and vice versa.

3.VARIOUS WORMHOLE DETECTION METHODS

Some work has been done to detect wormhole in Ad Hoc networks. Most of them based on the fact that transmission time between two wormhole nodes or between two fake neighbors is much longer than that between two real neighbors which are close together. Because two wormhole nodes (or two fake neighbors) are far from each other and packets sent between two wormhole nodes maybe go through several intermediate nodes so it takes a longer time to transmit a packet between two wormhole nodes (or two fake neighbors) than between two real neighbors which are close together. By detecting this difference, we can identify wormhole attacks.

3.1 Packet Leashes

One of the first proposals for detecting wormhole is packet leashes [3][4]. Every time a node, say A, sends a packet to another node, say B, A has to put a time stamp (sending time) (temporal packet leashes) or the location of A and sending time (geographical packet leashes) into the packet. Based on this information, B can estimate the distance between A & B. If the estimated distance is longer than the possible radio range, B will reject the communication with A. These two mechanisms require tightly synchronized clocks (temporal packet leashes) or special hardware for location (geographical packet leashes) which is expensive to use widely. Therefore, we can say these two mechanisms are impractical with current technology.

3.2 RTT

Round Trip Time (RTT) between two nodes [5]. A node, say A, calculates the RTT with another node, say B, by sending a message to node B requiring an immediate reply from B. The RTT between A and B is the time between A's sending the request message and receiving the reply message from B. In this mechanism each node (called N) will calculate the RTT between N and all N's neighbors. Because the RTT between two fake neighbors is higher than that between two real neighbors so by comparing these RTTs between A and A's neighbors, node A can identify which neighbors are fake neighbors and which neighbors are real neighbors. This mechanism do not require any special hardware and easy to implement but it cannot detect exposed attacks because no fake neighbor is created in exposed attacks.

3.3 Delphi

Another mechanism called Delphi (Delay Per Hop Indicator), proposed by Hon Sun Chiu and King-Shan Lui [6], is able to detect both hidden and exposed wormhole attacks. In this mechanism, they try to find every available disjoint path between a sender and a receiver. Then, they calculate delay time & length of each path, computing Delay per Hop value (average delay time per hop along each path). Delay per Hop values of paths are used to identify wormhole: the path containing wormhole link will have greater Delay Per Hop value. This mechanism can detect both kind of wormhole but they cannot pinpoint the wormhole location. Moreover, because lengths of paths are changed by every node (including wormhole nodes) so wormhole nodes could change the path length in a certain way to make them unable to be detected.

3.4 Sector

In multi-hop wireless networks, keeping track of node en- counters is a crucial function, to which the research community has devoted very little attention so far. This function can be used for the detection of wormhole attacks, to se- cure routing protocols based on the history of encounters, and for the detection of cheating attempts (e.g., in charging mechanisms).SECTOR can be used to prevent wormhole attacks [8, 9] in ad hoc networks, without requiring any clock synchronization or location information; it is therefore a valid alternative to the other solutions already proposed to this problem. SECTOR can also help to secure routing protocols in mobile ad hoc networks, which are based on the history of encounters; we illustrate this with FRESH [10], the last- encounter protocol that enables an efficient route discovery for large- scale ad hoc networks.

3.4 Neighbor Number Test

There are several other approaches which do not use transmission time to detect wormhole. In [10], the author proposed two statistical approaches to detect wormhole attack in Wireless Ad Hoc Networks. The first one called Neighbor Number Test bases on a simple assumption that a wormhole will increase the number of neighbors of the nodes (fake neighbors) in its radius. The base station will get neighborhood information from all sensor nodes, computes the hypothetical distribution of the number of neighbors and uses statistical test to decide if there is a wormhole or not. The second one called All Distance Test detects wormhole by computing the distribution of the length of the shortest paths between all pairs of nodes. In these two algorithms, most of the workload is done in the base station to save sensor nodes' resources. However, one of the major drawbacks is that they cannot pinpoint the location of wormhole which is necessary for a successful defense.

3.5 True Link

True Link developed by Jakob Eriksson in 2006 is a wormhole detection technique [11] that depends on time based mechanisms. True Link verifies whether there is a direct link for a node to its adjacent neighbor. Wormhole detection using True Link involves 2 phases namely rendezvous and validation. The first phase is performed with firm timing factors in which nonce exchange between two nodes takes place. In the second phase, both the nodes authenticate each other to prove that they are the originator of corresponding nonce. The major disadvantage is that True Link works

only on IEEE 802.11 devices that are backward compatible with a firmware update. A round trip time (RTT) approach is emerged to overcome the problems in using additional hardware. The RTT is the time taken for a source node to send RREQ and receive RREP from destination. A node must calculate the RTT between itself and its neighboring nodes. The malicious nodes have higher RTT value than other nodes. In this way, the source can identify its genuine and misbehaving neighbors. This detection technique is efficient only in the case of hidden attacks.

4.7) Secure Neighbor Discovery & monitor based system: This is provided by Issa Khalil in 2008 [12] which uses local observation schemes to prevent malevolent nodes in the vicinity. The position of each node in the network is traced by central authority and it is capable of even isolating the malicious nodes globally. The detection rate of this method decreases as the network mobility increases.

3.6 TTM

TM –Transmission Time Mechanism [12, 13] to detect wormhole in Wireless Ad Hoc Networks using AODV routing protocol by calculating & comparing the Round Trip Time between every two successive nodes along that route during route setup protocol. TTM is able to detect both hidden & exposed wormhole attacks, locating the wormhole, requiring no special hardware. The performance of TTM is also evaluated by simulation using network simulator The simulation shows that the mechanism can detect wormhole attack with 100% accuracy when the wormhole length is large enough. Some future work also needs to be done to extend our mechanism to work in other routing protocols such as DSDV and DSR. Comparative analysis of various wormhole detection techniques

Detection Technique	Advantages	Disadvantages
Packet Leashes	Can find Pinpoint location of wormhole	Can't Detect Exposed attacks Required special Hardware for location
RTT (Round Trip Time)	Don't required any Hardware Easy to implement	Can't detect Exposed Attacks
DelPHI (Delay Per Hop Indicator)	Can detect Exposed attacks as well as Hidden attacks	Can't Pinpoint the wormhole location
SECTOR	No need to Time Synchronization	Can't find pinpoint location
Neighbor number Test	Can detect Hidden attacks No special Hardware required	Can't detect Exposed attacks
Truelink: A Time based Mechanism	Can detect Hidden attacks More efficient	Works only on IEEE 802.11 Devices Can't detect Exposed attacks
Secure Neighbor Discovery and Monitor based Approach	Central Authority It is capable of even isolating the malicious nodes globally	The Detection rate of this method decreases as the network mobility increases
Transmission Time Mechanism(TTM)	Can find Hidden as well as Exposed attacks Can find Pin point lacation of wormhole No special hardware required	Wormhole detection rate is high only when wormhole length is more than 6 (hop)

REFERENCES

[1] C.Siva Ram Murthy and B. S. Manoj. "Ad hoc wireless networks: Architecture and Protocols",PrenticeHall Publishers, May 2004, ISBN 013147023X.
[2] P.V.Jani, "Security within Ad-Hoc Networks", Position Paper, PAMPAS Workshop, Sept. 16/17 2002.
[3] K. Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of Technology" Sweden, 22nd March 2007.
[4] Mishra Amitabh, Nadkarni Ketan M., and Ilyas Mohammad. "Security in wireless Ad-hoc networks, the handbook of Ad hoc wireless network". Chapter 30: CRC PRESS Publisher, 2003.
[5] Roy, D.B., Chaki, R & Chaki, N. "A New Cluster-Based Wormhole Intrusion detection. Algorithm for Mobile Ad Hoc Networks", International Journal of Network Security and its Applications (IJNSA), (2009).
[6] C.E.Perkins and E.M.Royer, "Ad-hoc On Demand Distance Vector Routing," Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applictions, pp.90-100, Feb, 1999.
[7] C.M barushimana, A.Shahrabi, "Comparative Study of Reactive and Proactive Routing Protocols Performance in Mobile Ad-Hoc Networks," Workshop on Advance Information Networking and Application, Vol. 2, pp. 679-684, May, 2003.
[8] http://www.faqs.org/rfcs/rfc3561.html
[9] M.Abolhasan, T.Wysocki, E.Dutkiewicz, "A Review of Routing Protocols for Mobile Ad-hoc Networks," Telecommunication and Information Research Institute University of Wollongong, Australia, June, 2003.
[10] http://www.netmeister.org/misc/zrp/zrp.html
[11] G. A. Pegueno and J. R. Rivera, "Extension to MAC 802.11 for Performance Improvement in MANETs", Karlstads University, Sweden, December 2006.
[12] S. Lu, L. Li, K.Y. Lam, L. Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack.", International Conference on Computational Intelligence and Security, 2009.
[13] C.Wei, L.Xiang, B.yuebin and G.Xiaopeng, "A New Solution for Resisting Gray Hole Attack in Mobile Ad-Hoc Networks", Second International Conference on Communications and Networking in china, pp.366-370, Aug, 2007.
[14] Zhu, C. Lee, M.J.Saadawi, T., "RTT-Based Optimal Waiting time for Best Route Selection in Ad-Hoc Routing Protocols", IEEE Military Communications Conference, Vol. 2, pp. 1054-1059, Oct, 2003.
[15] M.T.Refaei, V.Srivastava, L.Dasilva, M.Eltoweissy, "A Reputation-Based Mechanism for IsolatingSelfish nodes in Ad-Hoc Networks," Second Annual International Conference on Mobile and Ubiquitous Systems, Networking and Services, pp.3-11, July, 2005.

[16][16] F.Stanjano, R.Anderson, "The Resurrecting Duckling: Security Issues for Ubiquitous Computing," Vol.35, pp. 22-26, Apr, 2002.
[17][17] H.L.Nguyen,U.T.Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad-Hoc Networks," International Conference on Networking, Systems, Mobile Communications and Learning Technologies, Apr,2006.
[18][18] Y.-C. Hu, A. Perrig, D. B. Johnson; "Packet leashes: a defense against wormhole attacks in wireless networks"; INFOCOM 2003, Twenty-Second Annual Joint Conference of the IEEE Computer and Communication Societies, Vol. 3, pp. 1976-1986, 2003.
[19][19] S.Capkun, L. Buttyan, J.-P. Hubaux; "SECTOR: Secure Tracking of Node Encounters in Multi-Hop Wireless Networks"; Proc. of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks; 2003.

AUTHOR

Mr. Vinod S Wadne received the B.E and M.E. degrees in computer Engineering. And working As Assistant professor In Department of Computer Science and Engineering at Imperial College Of Engineering And Research, Wagholi, Pune. He has 11 year teaching Experience. His areas of interest in research are Wireless Communication & Wireless Networks.

Neha kulkarni received the B.E. degree in computer Engineering from RGPV university and pursuing master of technology in computer science & engineering from Imperial College Of Engineering And Research, Wagholi, Pune .and Working as Assistant professor In Department of Computer Science and Engineering at SGSITS college. she has 5 years experience. Her areas of interest in research are Wireless Networks and soft computing.