An Assessment of Mobile Ad-Hoc Network Security Threads: A Wormhole Attack

Neha Sahu
Department of Computer Science and Engineering, Technocrats Institute of Technology,
Bhopal

Deepak Singh Tomar
Department of Computer Science and Engineering, Technocrats Institute of Technology,
Bhopal

Neelam Pathak
Department of Computer Science and Engineering, Technocrats Institute of Technology,
Bhopal

ABSTRACT

Mobile Ad hoc networks typically work in an open un-trusted environment with little physical security, and are vulnerable for different type of security attacks. one attack in ad hoc networks is the wormhole attack that has received a great deal of recent attention. In wormhole attack, an attacker captures the packets from one point in the network and tunnels them to a distant location where they are replayed, typically without modification. Thus the detection of wormhole is a very important in the network. For wormhole attack to have a best impact on the network, it must attract a large amount of network traffic which is done by giving a shortest route to destination in the network. Therefore, the routes going through the wormhole must be shorter than alternate routes through valid network nodes. .This paper uses demonstrate different existing worm hole deduction mechanism and discus problem in existing mechanism

Keywords

Mobile Ad hoc Network, Selfish, Malicious

1. INTRODUCTION

Mobile ad hoc network [3] is a self-configuring network that is formed automatically by a set of mobile nodes without the help of a fixed infrastructure or centralized management. Each node is prepared with a wireless transmitter and receiver, which allow it to communicate with other nodes in its range. In order for a node to forward a packet to a node that is out of its radio range, the support of other nodes in the network is needed; this is known as multi-hop communication. Therefore, each node must act as both a host and a router at the same time. The network topology normally changes due to the mobility of mobile nodes in the network.

MANET was initially developed for military purposes, as nodes are scattered across a battlefield and there is no infrastructure to help them form a network. MANETs have been increasing quickly and are gradually more being used in many applications, ranging from military to civilian and commercial uses, since setting up such networks can be done without the help of any infrastructure or interaction with a human. Some examples are search-and rescue missions, data collection, and virtual classrooms and conferences where laptops, PDA or other mobile devices share wireless medium and communicate to each other. As MANETs become widely used, the security issue has become one of the primary concerns. For example, most of the routing protocols proposed for MANETs assume that every node in the network is cooperative and not malicious. Therefore, only one compromised node can cause the failure of the entire network.

2. SECURITY ISSUES IN MOBILE AD HOC NETWORK

MANET is vulnerable to various types of attacks. Some attacks affect to general network, some affect to wireless network, and some are particular to MANETs. These security attacks can be classified according to different criteria, such as the domain of the attackers, or the techniques used in attacks. These security attacks in MANET and all other networks can be generally classified by the following criteria: passive or active, internal or external, different protocol layer, stealthy or non-stealthy, cryptography or non-cryptography related.

Passive vs. active attacks: The attacks in MANET can generally be classified into two major categories, namely passive attacks and active attacks. A passive attack obtains data exchanged in the network without disrupting the operation of the communications, while an active attack involves information interruption, modification, or fabrication, thereby disrupting the normal functionality of a MANET. Examples of passive attacks are eavesdropping, traffic analysis, and traffic monitoring. Examples of active attacks include jamming, impersonating, modification, denial of service (DoS), and message replay.

Internal vs. external attacks: The attacks can also be classified into external attacks and internal attacks, according the domain of the attacks. Nodes that do not belong to the domain of the network carry out external attacks. Internal attacks are from compromised nodes, which are actually part of the network. Internal attacks are more harmful when compared with outside attacks since the insider knows valuable and secret information, and possesses confidential access rights.

Eavesdropping: Eavesdropping is the intercepting and reading of messages and conversations by unintended receivers. The mobile hosts in mobile ad hoc networks share a wireless medium. The majorities of wireless communications use the RF spectrum and broadcast by nature. Signals broadcast over airwaves can be easily intercepted with receivers tuned to the proper frequency. Thus, messages transmitted can be overheard, and fake messages can be injected into network [15].

Interference and Jamming: Radio signals can be blocked or interfered with, which causes the message to be corrupted or lost. If the attacker has a powerful transmitter, a signal can be generated that will be strong enough to overwhelm the targeted signals and disrupt communications. The most common types of this form of signal jamming are random noise and pulse[15].

Black hole attack: The black hole attack has two properties. First, the node exploits the mobile ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is false, with the intention of intercepting packets. Second, the attacker consumes the intercepted packets without any forwarding.

Byzantine attack: A compromised intermediate node works alone, or a set of compromised intermediate nodes works in collusion and carry out attacks such as creating routing loops, forwarding packets through non-optimal paths, or selectively dropping packets, which results in disruption or degradation of the routing services [15].

Rushing attack: Two colluded attackers use the tunnel procedure to make a wormhole. If a fast transmission path exists between the two ends of the wormhole, the tunnelled packets can transmit faster than those through a normal multi-hop route. This forms the rushing attack. The rushing attack can act as an effective denial-of- service attack against all currently proposed on-demand MANET routing protocols.

Malicious code attacks: Malicious code, such as viruses, worms, spywares, and Trojan Horses, can attack both operating systems and user applications. These malicious programs usually spread themselves through the network and cause the computer system and networks to slow down or even damaged. In MANET, an attacker can produce similar attacks to the mobile system of the ad hoc network.

Denial of service: Denial of service (DoS) attacks could be launched from several layers. An attacker can employ signal jamming at the physical layer, which disrupts normal communications. At the link layer, malicious nodes can occupy channels through the capture effect, which takes advantage of the binary exponential scheme in MAC protocols and prevents other nodes from channel access. At the network layer, the routing process can be interrupted through routing control packet modification, selective dropping, table overflow, or poisoning. At the transport and application layers, SYN flooding, session hijacking, and malicious programs can cause DoS attacks.

Impersonation attacks: Impersonation attacks are launched by using other node’s identity, such as MAC or IP address. Impersonation attacks sometimes are the first step for most attacks, and are used to launch further, more sophisticated attacks.

Man-in-the-middle attacks: An attacker sits between the sender and the receiver and sniffs any information being sent between two ends. In some cases, the attacker may impersonate the sender to communicate with the receiver, or impersonate the receiver to reply to the sender.

Wormhole attacks: In a wormhole attack, two attacker nodes join together. One attacker node receives packets at one point and “tunnels" them to another attacker node via a private network connection, and then replays them into the network.

3. RELATED WORK

Marti et al. proposed two techniques that improve throughput in an ad hoc network in the presence of selfish and malicious nodes [1]. The watchdog method is used for each node to detect misbehaving nodes in the network. When a node sends a packet to next hop, it tries to overhear the packet forwarded by next hop. If it hears that the packet is forwarded by next hop and the packet matches the previous packet that it has sent itself, it considers the next hop node behaves well. Otherwise it considers the next hop node is misbehaving. The pathrater uses the knowledge about misbehaving nodes acquired from watchdog to pick the route that is most likely to be reliable. Each node maintains a trust rating for every other node. When watchdog detects a node is misbehaving, the trust rating of the node is updated in negative way. When a node wants to choose a safe route to send packets, pathrater calculates a path metric by averaging the node ratings in the path.

Marti et al. implemented the solutions on DSR protocol using ns2 as simulation environment. The simulation result shows the throughput of the network could be increased by up to 27% in a network where packet drop attack happens. However routing overhead is also increased by up to 24%.

In [2], authors study the impact of wormhole attacks on a real wireless mesh network testbed. Through theoretical analysis and comprehensive experiments, and find that when a path is under the control of wormhole links, standard deviation of RTT (stdev (RTT)) is a more efficient metric than per-hop RTT to identify wormhole attacks. Based on the observation, authors propose a neighbour-probe-acknowledge algorithm (NPA) to detect wormhole attacks by identifying the occurrence of large stdev(RTT). The evaluation results on testbed show that the proposed algorithm can achieve near 100% wormhole detection rate and zero false alarm rate both in light and heavy background traffic load scenarios. But, the parameters in NPA are static and not adaptive. So, in the future work on dynamic adjustment of algorithm parameters and routing algorithm that is resilient to wormhole attacks will be done. Furthermore, there will a possibility of adopt the observation to design a new routing protocol which can resilient to inside attacks without triggering the detection frequently to further decrease the overhead.

In [3] authors used the scheme called multihop count analysis (MHA) with verification of legitimate nodes in network through its digital signature. Destination on node analyses the number of hop count of every path and selects the best path for replying. For checking the authentication of selected path, proposed methodology used verification of digital signature of all sending node by receiving node. If there is no malicious node between the paths from source to destination, then source node creates a path for secure data transfer.

In [4] authors proposed E2SIW, a routing protocol immune to wormhole attacks. E2SIW uses a simple location information and alternate route finding techniques to detect and prevent wormhole attack in ad hoc networks. E2SIW has a high detection rate and less energy requirements compared to the De Worm protocol And also contributed in reducing the overhead associated with the control packets. Most of the work done so far in this topic assumes that the wormhole nodes are not capable of maliciously changing the data passing through them. But this may not always be the case. The design of the mitigation solutions keeping in mind that intelligent malicious nodes may exists is the need of the hour.

In [5] wormhole attack defence strategy of WSN based on neighbour nodes verification. Under this strategy, when each normal node received control packet, it will monitor the packet to determine whether it comes from its normal neighbour nodes to avoid Wormhole attack effectively. Modelling and simulation of WSN based on OMNeT++ shows that the AODV added neighbour nodes verification successfully implement effective defence.

A Defence against Wormhole Attacks in Wireless Networks: As mobile ad hoc network applications are structured, security appears as a central requirement. The author introduces the wormhole attack, a severe attack in ad hoc networks that is mostly challenging to defend against. The wormhole attack is possible even if the attacker has not compromised any hosts and even if all communication provides authenticity and confidentiality. Author presented the design and performance analysis of a novel, efficient protocol, called TIK, In particular, a node needs to perform only between 3 and 6 hash function evaluations per time interval to maintain up-to-date key information for itself, and roughly 30 hash functions for each received packet. When used in conjunction with precise timestamps and tight clock synchronization, TIK can prevent wormhole attacks that cause the signal to travel a distance longer than the nominal range of the radio [9]. And wireless MAN technology could be sufficiently time-synchronized using either GPS or LORAN-C radio signals.

4. WORM HOLE ATTACK

One of the serious threats in MANET is wormhole attack because it cannot be detected easily. As shows in figure 1 in wormhole attack two selfish nodes join together. One node receives packets at one point and “tunnels" them to another attacker node via a private network connection, and then replays them into the network. The wormhole puts the attacker nodes in a very powerful position compared to other nodes in the network. This type of attack prevents other routes instead of the wormhole from being discovered, and thus creates a permanent Denial-of-Service attack by dropping all the data, or selectively discarding or modifying certain packets as needed [14].

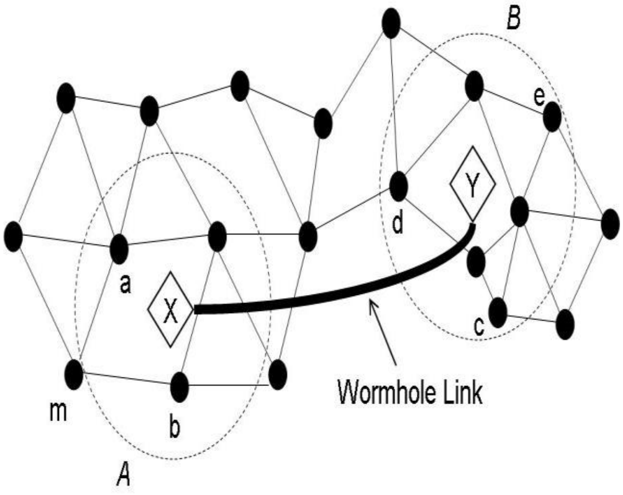

Figure 1: Worm Hole

Wormhole attacks are organized on the basis of visibility of selfish node in the route and classified into three types: closed, half open, and open. As show in figure 2 consider two nodes behave like worm hole stating point (WHS) and worm hole ending point (WHE), represent the malicious nodes and all other node entitle with NNi treated as good node . In closed wormhole attack tunnel start from source and hide both starter and end node of tunnel, as show in figure 2 because of closed worm hole source node analysis destination node as their neighbour node. Where as in open worm hole attack both the end point of tunnel are not hide form rest of network and make a part of route as shows in figure 3 but in half open worm hole one of end node of tunnel is hide from rest of network for route as show in figure 4 [15].

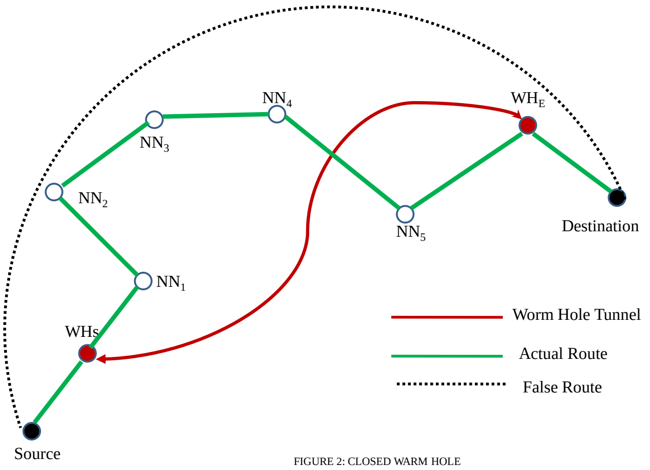

FIGURE 2: CLOSED WARM HOLE

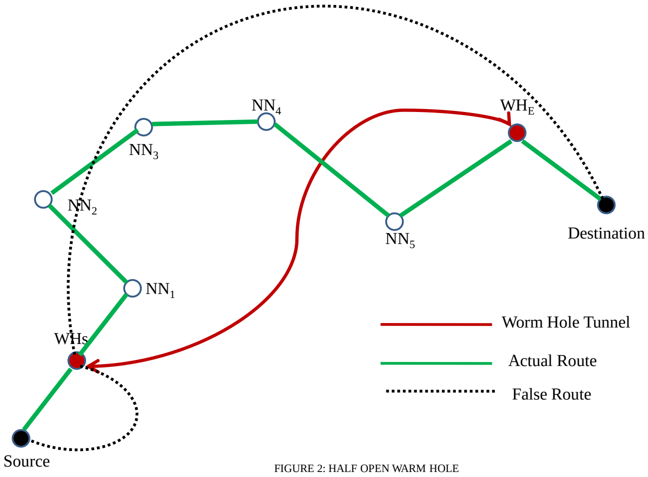

FIGURE 2: HALF OPEN WARM HOLE

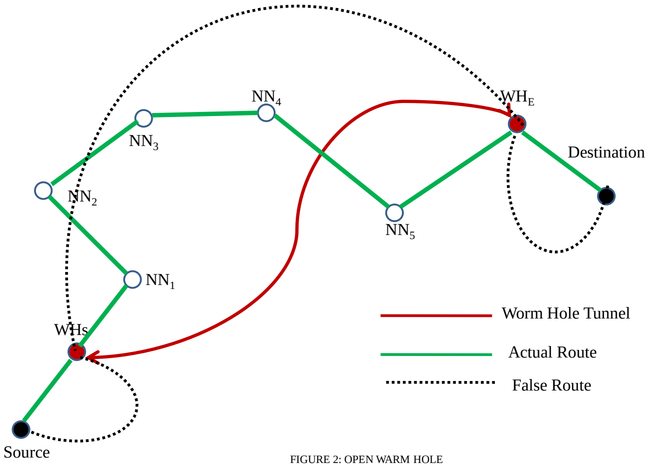

FIGURE 2: OPEN WARM HOLE

5. CONCLUSION AND FUTURE WORK

This paper presented and discussed various security attack and threats in MANETs. And explain selfish node behaviours along with wormhole attack. In future we plan to continue our work in field of secure routing over MANETs & present a wormhole detection and prevention technique in order to enhance the security of MANETs.

6. REFERENCES

[1] S. Marti et al. “Mitigating routing misbehavior in mobile ad hoc networks,” Proceedings of Sixth Annual IEEE/ACM Intl. Conference on Mobile Computing and Networking , April 2009,PP. 225-256.

[2] Jie Zhou1, Jiannong Cao, Jun Zhang1, Chisheng Zhang and Yao Yu, “Analysis and Countermeasure for Wormhole Attacks in Wireless Mesh Networks on a Real Test bed” in 26th IEEE International Conference on Advanced Information Networking and Applications,2012

[3] Pallavi Sharma, Prof. Aditya Trivedi “An Approach to Defend Against Wormhole Attack in Ad Hoc Network Using Digital Signature” in IEEE ,2011

[4] Sanjay Kumar Dhurandher and Isaac Woungang “E2SIW: An Energy Efficient Scheme Immune to Wormhole Attacks in Wireless Ad Hoc Networks” in 26th International Conference on Advanced Information Networking and Applications Workshops in IEEE,2012

[5] Jin Guo, Zhi-yong Lei “A Kind of Wormhole Attack Defense Strategy ofWSN Based on Neighbor Nodes Verification” in IEEE 2011 RFC 792, Internet Control Message Protocol

[6] D. Johnson , D. A. Maltz, and J. Broch. The Dynamic Source Routing Protocol for Mobile Ad hoc Networs (Internet-Draft). Mobile Ad-hoc Network (MANET) Working Group, IETF, October 1999

[7] M. Tamer Rafaei, Vivek Srivastav, Luiz DaSilva, ”A Reputation-based Mechanism for Isolating Selfish Nodes in Adhoc Networks,”Proceedings of the Second Annual Internatinal Conference on Mobileand Ubiquitous Systems:Networking and Services(MobiQuitous’05

[8] Katrin Hoeper, Guang Gong, “Pre-Authentication and Authentication Models in Ad Hoc Networks,” Signals and Communication Technology, pp. 65-82, 2007.

[9] Hu. Yih-Chun and A. Perrig, “A Survey of secure wireless ad hoc routing,” Security & Privacy, IEEE, vol. 2, pp. 28–39, 2004.

[10] Fei Shi, Jaejong Baek, Jooseok Song, Weijie Liu. “A novel scheme to prevent MAC layer misbehavior in IEEE 802.11 ad hoc networks,” Journal of Telecommunication Systems (JTS) - Springer, (DOI) 10.1007/s11235-011-9552-y, 2011.

[11] Khalil, S. Bagchi, and N. B. Shroff, LiteWorp: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks, in Proceedings of the 2005 IEEE International Conference on Dependable Systems and Networks (DSN 2005), Yokohama, Japan, June 28-July 1, 2005.

[12] Y. C. Hu, A. Perrig, and D. B. Johnson, Wormhole Attacks in Wireless Networks, IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp.370-380,2006.

[13] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, “Wormhole Attacks in Wireless Networks” citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.110.609

[14] W. Wang, B. Bhargava, Y. Lu, and X. Wu, “Defending against wormhole attacks in mobile ad hoc networks: Research articles,” Wireless Communication Mobile Computing, vol. 6, no. 4, pp. 483–503, 2006.