Survey on Wormhole Attack Detection Techniques in Mobile Ad-hoc Network

Dipika Baid
Department of Computer Science and Engineering, SMIT, Sikkim, India

Kriti Dugar
Department of Computer Science and Engineering, SMIT, Sikkim, India

Pratima Sarkar
Assistant Professor
Department of Computer Science and Engineering, SMIT, Sikkim India

ABSTRACT

Mobile Ad-hoc Network (MANET) exposes itself to wide range of security attacks due to its broadcast nature and lack of central authority, wormhole attack is one of devastating attack that can easily be launched by attacker without the knowledge of the network of compromising any legitimate nodes or cryptographic mechanisms.Here a malicious node can drop, delay, tunneling or replay the packets depending nature of the attack.As malicious nodes in wormhole attack hide their original identity and they do not compromise any node so detection of this attack is difficult.In this paper several detection techniques of wormhole attack in a MANET are discussed that uses on demand AODV or DSR routing protocol. The result shows comparison between different wormhole attack detection techniques.

General Terms

MANET, AODV, DSR

Keywords

Mobile Ad-hoc Network (MANET), Wormhole attack, Malicious node.

1. INTRODUCTION

A MANET [2] [4] is a self-configuring network of mobile nodes.It has no central authority which can supervise the individual nodes in the network operating in the network. In MANET all the nodes has capability of forwards packets from one node to another node because each node acts a router. Therefore selection of robust, effective, adaptive and suitable routing protocol is important. MANET is a type of Wireless Ad-hoc network that works on Link Layer ad hoc network. MANETs composed of a self-forming, peer-to-peer, self-healing network.There are different types of routing protocols exist like Proactive Protocols, Reactive Protocols and Hybrid Protocols. The aim of different routing protocols is to minimize delay but to maximize network throughput, network lifetime and energy efficiency.

Security is the main issue in MANET due to its dynamic nature.A particularly severe security attack known as Wormhole attack [2] has been introduced in the context of MANET.Wormhole attacks are of different types like All Pass, All Drop, Threshold, Replay, Tunneling and Propagation Delay [3].In wormhole attack malicious node gives false reply packet to the source node for creating illusion that it has less hop count to reach the destination node. After receiving packets from source node, it performs various activities like received packets from the source node either drop them or delay them or tunnels them in other malicious node and replays them locally. In these types of attack one most important type is Tunneling .The tunnel can be created in many different ways, such as through an out-of-band hidden channel (e.g., a direct wired link or a long-range directional wireless link), packet encapsulation, or high powered transmission [6]. This tunnel create an illusion that two end point of the tunnel are very close to each other which makes the tunneled packet arrive either sooner or with lesser number of hops as compared to the packets transmitted over normal routing. A wormhole tunnel can actually be useful if used for forwarding all the packets. However, in its malicious incarnation, it is used by attacking nodes to subvert the correct operation of ad-hoc network routing protocols. The two malicious end points of the tunnel may use it to pass routing traffic to attract routes through them.

Consider the scenario depicted in Figure 1. Node S is sending a route request RREQ for destination node D. M1 and M2 are malicious nodes having a channel between them. Node M1 tunnels the route request to *M2*, which is a legitimate neighbor of destination node D. On receiving RREQ packet node M2 broadcasts the packet to its neighbors. RREQ packet reached to the destination node in two different paths first is *S-M1-M2-D* and second is *S-C-E-F-B-D*. The first route is shorter and faster than the second route. Thus RREP packets forwarded to the M2 node. Another situation may occur where malicious nodes gives false RREP to the source node and if path to the destination node does not exists then drop the packet.

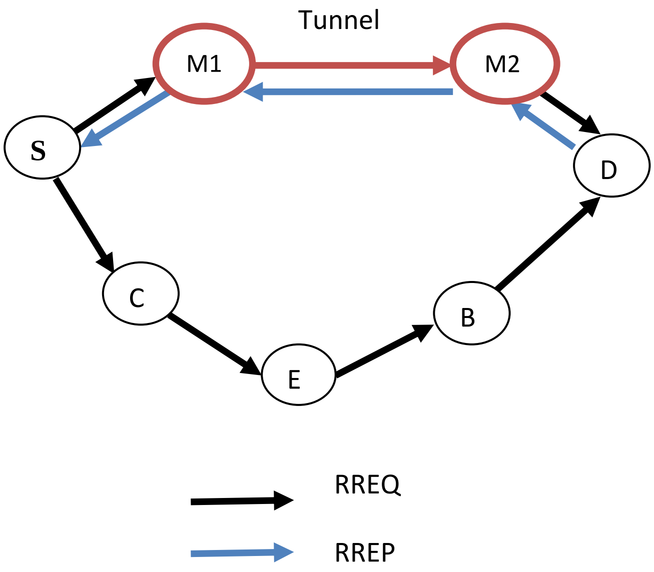

Figure 1: Wormhole Attack

2. WORMHOLE DETECTION TECHNQUES

2.1. Packet leashes

Packet leashes [10] are a general mechanism to detect and defend against wormhole attack.It is mainly of two types: Geographical leashes and Temporal leashes.

2.1.1.Geographical leashes

In this, each node knows its exact location and every node has loosely synchronized clock. At the sender site, before sending any packet every node attaches its current location and the transmission time along with the packet. On the other end, at the receiver site the receiver calculates the distance to the sender and the time it took the packet to traverse the path. Now, the receiver can use this distance to know whether received packet passed through the wormhole or not.

2.1.2.Temporal leashes

But in case of temporal leashes, every node has tightly synchronized clock such that maximum distance between two node's clocks is Δ.The value of the parameter should be known by all other nodes in the network.Every node in the network calculates the expiration time in the packet header. After calculating the expiration time, the destination node compares it with its own arrival time to know whether there is wormhole attack exists or not.The disadvantage of temporal leashes is that time synchronization can be less loose compare to geographical leashes.

2.2 SECTOR (Secure Tracking of Node Encounters in multi-hop wireless network)

This wormhole detection technique [7] doesnot uses any location information or clock synchronization as in case of packet leashes.It uses a mutual authentication with distance bounding(MAD) protocol for estimating the distance between two nodes or users.This technique use special hardware called transceiver for challenge request-response and accurate time measurements. The transceiver accepts a single bit as input,carryout 2 bit XOR process over it and broadcast it.The disadvantage of using this technique is that it doesnot nullifies the capacity of the compromised nodes from launching attacks in future.

2.3 DELPHI (Delay Per Hop Indication)

This technique [1] doesnot need any hardware or clock synchronization as in case of SECTOR or packet leashes.It uses delay and hopcount information to detect wormhole attack (by evaluating the delay per hop to serve as indicator).This technique is mainly divided into two phases.In the first phase the delay is calculated and hop information is obtained.And in the second phase the sender uses the information obtained in the former phase to know whether wormhole attack exists or not.

2.4 LITEWORP

LITEWORP [6] is a lightweight countermeasure for detection of wormhole attack.It does not require any specialized hardware such as directional antennas or finegranularity clocks neither does it require any time synchronization between the nodes in the network and is particularly suitable for resource constrained multi-hop wireless network. This paper uses local monitoring system for detection of different types of wormhole attack. Different types of attack it considers such as out-of-band and packet encapsulation wormholes, packet relay wormhole and protocol deviation wormhole. For detecting all the attacks in the first phase, creates information structure for each node and builds neighbor list. After that it applies local monitoring system for identifying traffic going in and out of its neighbors. By using Response and Isolation Algorithm and data received from local monitoring it detects different types of wormhole attack. Disadvantage of this technique is that it has low storage and it incurs negligible bandwidth overhead. While having this disadvantage it has the advantage that no specialized hardware is required that make it ideally suited to resource constrained wireless networks.

2.5 MOBIWORP

It [5] is mitigation of wormhole attack in mobile multi-hop wireless network. Mitigation involves detection of the attack, diagnosis of the adversary nodes, and nullifying their capability for further damage. A primitive is provided that mitigate the wormhole attack in mobile ad-hoc network such that primitive prevents a node from claiming to exist at more than one position in the network. A protocol is developed called MOBIWORP that can detect and diagnose wormhole attack in mobile network. In proposed solution central Authority (CA) given to trusted node and each node share key with the CA. Here local monitoring is used for black listing the malicious node in the network. For blacklisting any node continuous monitoring of the network traffic is required. Each node has memory for maintaining black list so that malicious node cannot be a neighbor of any node. This technique is called localization of malicious node.

It enforces a global isolation of the malicious node from the whole network .It does not choose guard nodes based on their location, which eliminates the causes of loss in detection coverage or false detection. It does not provide computationally tractable ways of accumulating suspicion information from multiple guard nodes. It alleviates the drawbacks such as accuracy, resource requirements, and applicability to ad hoc and sensor networks and efficiently mitigates the wormhole attack immobile networks

2.6. Path Tracing Approach

This detection technique [9] is performed with at the time of route discovery to reduce overhead.In this technique we calculate per hop distance based on RTT value and store it in packet header after that the next set nodes in the path will compute the per hop distance and compare it with prior per hop distance.If this hop distance exceed the max threshold range then the wormhole tunnel is identified and frequent appearance of the in the path is counted.And if that count exceeds the max frequent appearance count then the wormhole attack is confirmed.Once the wormhole attack is detected the corresponding nodesinform the other entire node about the wormhole and as a result wormhole nodes are isolated from the network.

3. COMPARISON BETWEEN DIFFERENT WORMHOLE DETECTION TECHNIQUES

Table1. Comparison Table

Methods	Localization Information	Checking the Authentication	Hop Count Analysis	Mobility factor	Requirement	Limitations
GEOGRAPHICAL LEASHES	Yes	RSA	No	Maximum transmission of packet to be restricted	Loosely Synchronize clock	Global Positioning System (GPS) technology
TEMPORAL LEASHES	Yes	TIK Protocol on TESLA	No	Maximum transmission of packet to be restricted	Tightly Synchronize clock	Global Positioning System (GPS) technology
SECTOR	No	MAD	No	Not required	Tranciever	It doesnot nullify the occurrence of wormhole attack.
DELPHI	No	No	Yes	Not required	None	Unable to find the exact location of the attack
LITEWORP	No	No	No	Not required	Guards for local monitoring	Low storage and incurs negligible bandwidth overhead.
MOBIWORP	No	No	No	Not required	Central Authority	Detection rate decreases as the network mobility increases.
PATH TRACING	No	No	Yes	Not required	None	Time consuming

4. CONCLUSION

In this paper various wormhole detection techniques are discussed.Along with the explanation of this technique a qualitative comparison of all wormhole detection technique has been done in Table 1.All detection techniques have their own merits and demerits.But there areno detection techniques which detect wormhole attack perfectly. Based on the existing approaches Path Tracing Approach will be helpful to detect wormhole attack in the network.

In the near future, we are analyzing performance of Wormhole attack with respect to different parameters. We will try to propose better solution for Wormhole attack detection techniques and try to improve the performance of the network after detection of malicious node.

5. ACKNOWLEDGMENTS

Our thanks go to the experts who have contributed to the development of this paper.

6. REFERENCES

[1] Chiu, HS: Wong Lui, KS, 2006 "DELPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Network" 1st International Symposium on Wireless Pervasive Computing.

[2] C. Siva Ram Murthy, B. S. Manoj, 2004 "Ad Hoc Wireless Networks", Pearson Education, Inc.

[3] Urmeet Kaur and Amanpreet Kaur "Performance Analysis of AODV for WormholeAttack Using Different Mobility Models", International Conference on Communication, Computing & Systems (ICCCS–2014), pp, 67-72.

[4] ImrichChlamtac, Macro Conti and Jennifer J.N. Liu, 2003 "Mobile Ad Hoc Networking: Imperatives and Challenges" Ad Hoc Networks, Volume 1, Issue 1 , pp, 13-64.

[5] Issakhalil, Saurabh Bagchi, and Ness B. Shroff, 2008 "MOBIWORP: Mitigation of the Wormhole Attack Multihop Wireless Network" Ad hoc Networks, Volume 6, Issue 3, pp, 344-362.

[6] Issakhalil, Saurabh Bagchi, and Ness B. Shroff, 2005 "LITEWORP: A Liteweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks" IEEE International Conference on Dependable Systems and Networks, pp, 612-621.

[7] Moutushi Singh, Rupayan Das, 2012 "A Survey of Different Techniques for Detection of Wormhole Attack in Wireless Sensor Network" International Journal of Scientific & Engineering Research Volume 3, ISSN 2229-5518.

[8] Srdjan Capkun, Levente Buttyan and Jean-Pierre Hubaux, 2003 "SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks" SASN'03 Proceedings of 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, pp, 21-32.

[9] T. Sakthivel, R. M. Chandrasekaran, 2012 "Detection and Prevention of Wormhole Attack in MANETs using Path Tracing Approach", European Journal of Scientific Research, Volume 76, pp, 240-252.

[10] Yih-Chun Hu, Adrian Perrig, David B. Johnson, 2003 "Packet Leashes: A Defense against Wormhole Attack in Wireless Network", Twenty-Second Annual Joint Conference of IEEE Computer and Communications, Volume 3, pp, 1976-1986.