Volume 6, Issue 5, May 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Tunnel Communication for Wormhole Attack and Response

S. Usha Devi
Research Scholar, Dept. of Computer Science,
Tamil University, Thanjavur, Tamilnadu, India

A. Senthil Kumar
Asst. Professor, Dept. of Computer Science,
Tamil University, Thanjavur, Tamilnadu, India

Abstract: The wormhole attack is possible even if the attacker has not compromised any hosts, and even if all communication provides authenticity and confidentiality. In the wormhole attack, attacker records packets at one location in the network, tunnels them to another location, and retransmits them there into the network. Most existing countermeasures either require specialized hardware devices or make strong assumptions on the network in order to capture the specific symptom induced by wormholes. Using analytical and simulation results, we show that a strategic placement of the wormhole all communications across the network. Sensor nodes, when deployed to form Wireless sensor network operating under control of central authority Base station are capable of exhibiting interesting applications due to their ability to be deployed ubiquitously in hostile & pervasive environments. But due to same reason security is becoming a major concern for these networks. Wireless sensor networks are vulnerable against various types of external and internal attacks being limited by computation resources, smaller memory capacity, limited battery life, processing power & lack of tamper resistant packaging.

Keywords: Basic attack, Request, Response

I. INTRODUCTION

Applications are emerging and widespread adoption is on the horizon. Most previous ad hoc networking research has focused on problems such as routing and communication, assuming a trusted environment. However, many applications run in untrusted environments and require secure communication and routing. In particular, several important applications for such networks come from military and defence arenas. Use of wireless medium and inherent collaborative nature of the network protocols make such network vulnerable to various forms of attacks. In this paper our focus is on a particularly devastating form of attack, called wormhole attack. Here, the adversary connects two distant points in the network using a direct low-latency link called the wormhole link. The wormhole tunnel gives two distant nodes are close to each other. The wormhole can attract and bypass a large amount of network traffic, and thus the attacker can collect and manipulate network traffic.

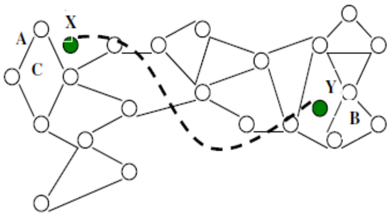
II. WORMHOLE ATTACKS

In this section, we introduce the notion of a packet leash as a general mechanism for detecting and, thus defending against wormhole attacks. A leash is any information that is added to a packet designed to restrict the packet's maximum allowed transmission distance. Leashes are designed to protect against wormholes over a single wireless transmission; when packets are sent over multiple hops, each transmission requires the use of a new leash. We distinguish between geographical leashes and temporal leashes.

After the attacker attracts a lot of data traffic through the wormhole, it can disrupt the data flow by selectively dropping or modifying data packets, generating unnecessary routing activities by turning off the wormhole link periodically, etc. propose MobiWorp to complement LiteWorp with the assistance of some location-aware mobile node. Some approaches observe the symptom of graph mismatch under special assumptions of network graph models. Present a graph-based framework to tackle wormholes. Their approach assumes the existence of guard nodes with extraordinary communication range.

III. BACKGROUND AND SIGNIFICANCE OF WORMHOLE ATTACK

Scarcity of various resources makes wireless sensor network vulnerable to several kinds of security attacks. Attacker possessing sufficiently large amount of memory space, power supply, processing abilities and capacity for high power radio transmission, results in generation of several malicious attacks in the network. Wormhole attack is a type of Denial of Service attack that misleads routing operations even without the knowledge of the encryptions methods unlike



Wormhole Attack

The above protocol has the drawback that message authentication is delayed; the receiver must wait for the key before it can authenticate the packet. We observe that we can remove the authentication delay in an environment in which the nodes are tightly time synchronized. In fact, the sender can even disclose the key in the same packet that carries the corresponding message authentication code.

3.1. Security Analysis

The geographic leashes are used, nodes also detect tunnelling across obstacles such as mountains that are otherwise impenetrable by radio. Our technique does not use location information and is able to detect attacks that are launched even before the network is set up, that may influence localization. We expect that our technique is particularly useful for sensor networks as the existing techniques are quite limited there. Also, connectivity is not expected to change frequently in sensor networks, making our connectivity-based approach quite practical.

Knowledge of the wireless communication model between the nodes helps our detection algorithm. This is because a communication model can help define what substructures observed in the connectivity graph could be forbidden. However, our approach is still applicable when the communication model is unknown. In this case we need to run an extra search procedure to determine a critical parameter for the detection algorithm. This parameter will be made clear later in this section. We first develop our wormhole detection algorithm, starting from the unit disk graph model and then general known or unknown communication models, and finally discuss how to automatically remove links created by wormhole once a wormhole is detected.

IV. DISTRIBUTION AND GENERAL COMMUNICATION MODEL

Consideration of node distribution is important in the performance of our algorithm. The packing number the maximum number of independent common of two independent nodes, is the theoretical worst case bound for an arbitrary distribution. If the sensors are deployed with a known distribution, then the forbidden parameter we use in the forbidden substructure can be much smaller than the theoretical worst case. An ideal wormhole detection method should require as little preknowledge assumptions about the network as possible. The only preknowledge that we will assume is the fact that the network is deployed on a continuous geometric surface, where each node locally communicates with neighboring ones.

4.1. Wormhole Problem location:

A similar approach is used in, where each node can estimate the distance to another node by sending a challenge bit and receiving its instant respond. In, a small fraction of network nodes called guards have access to location information for example using GPS and are assigned specific network operations. Directional antennas can also be used to mitigate the wormhole attack. All of the above methods require specialized hardware to achieve accurate time synchronization or time measuring, or to transmit maximum power in a particular direction. give a formal definition of the wormhole problem based on the UDG communication graph model in Euclidean space. According to their definition, a communication link is a wormhole link if the distance between its two endpoints exceeds the regular communication range. Their definition naturally binds the wormhole features with external geometric environments, and thus neglects the inherent topological impacts introduced by wormholes.

4.2. Wormhole using Protocol Distortion

In this mode of wormhole attack, single malicious node tries to attract network traffic by distorting the routing protocol. This mode does not affect the network routing much and hence is harmless. Also it is known as “rushing attack” in the literature.

Once a forbidden structure is discovered, it is usually expected that user should manually intervene and remove the wormhole links. Here, we devise a simple approach that can be used to isolate all links possibly affected by wormhole without manual intervention. We outline the approach for the 1-hop detection case for UDGs. It can be easily extended for other cases. After a successful 1-hop detection in UDGs, we have two non-neighbouring nodes *a, b* with 3 common independent neighbours *c, d* and *e*. one possible placement of these nodes to form the forbidden substructure, such that *a* and *b* are placed in one region.

The develop principles in continuous domain, assuming continuous deployment of nodes over the geometric surface with one-to-one mapping to the points on the surface. In the continuous setting, a legitimate network is a 2-manifold surface without singular points and of genus 0, which is hemitropic to the plane area with a certain number of boundaries. We refer to the surface of the legitimate network as original surface. A wormhole link is a continuous line segment with extremely short length that connects two points on the surface.

V. ROUTE ATTACK DISCOVERY

In the route discovery phase, the source and the destination nodes typically use flooding in order to discover a path between each other. In our proposed protocol, we assume that some techniques such as digital signature verification and buffer reservation are used to protect the nodes from being congested by a flooding attack. We also assume that the network links are bidirectional as it is required by many wireless Medium Access Control protocols.

In the first step of the route discovery phase, the source node S generates a

VI. ROUTE REQUEST

Packet signs it using its private key and broadcasts it to its neighbours, bedfast, Sags, Carts. The RREQ packet consists of a packet identifier which includes some information such as packet type. The RREQ packet also includes a request identifier, the destination IP address, a nonce, the source signature and the source certificate note that the source IP address is included in the certificate. Both NS and RI are incremented monotonically, but NS is increased for each routing packet while RI may remain the same for several route discovery attempts. When an intermediate node receives an unprocessed RREQ packet, it first compares the nonce NS to the last nonce received from S, validates the source signature and then rebroadcasts the verified packet.

This step should be carried out as quickly as possible since its only goal is to inform the destination that the source node intends to communicate with it. Consequently, this step requires no hop count or extra authentication.

When the destination node D receives the first legitimate RREQ from S, it initiates the second step by broadcasting a

6.1. Route Response:

Packet note that a broadcast is required in order to guarantee that the RREP packet reaches the source node. The RREP packet requires a hop count and a hop count hash chain if the shortest path is desired. As in the first step, the first intermediate node A rebroadcasts a received RREP packet if the packet is verified. Before rebroadcasting the packet, A sets up a reverse path to D, adds a number HIPA to the RREP packet and signs the packet. The next intermediate node B validates the packet, sets up a reverse path to D, removes A's certificate and signature, adds its number HIPB and then signs it.

The subsequent intermediate nodes along the path behave like B. As in the ARAN protocol, intermediate nodes' signatures are used to ensure that only nodes with valid cryptographic keys can participate in the routing. The number HIPX is obtained by taking the first byte of Hash, where Hash is a hash function. As it will be explained later, these short numbers are added to the RREP packet by intermediate nodes to prevent a new attack.

VII. CONCLUSIONS

To detect and defend against the wormhole attack, we introduced packet leashes, which may be either geographic or temporal leashes, to restrict the maximum transmission distance of a packet. Finally, to implement temporal leashes, we presented the design and performance analysis of a novel, efficient protocol, called TIK, which also provides instant authentication of received packets. The algorithm is simple, localized, and is universal to node distributions and communication models. Our simulation results have confirmed a near perfect detection performance whenever the network is connected with a high enough probability, for common connectivity and node distribution models.

REFERENCES

[1] N. Abramson, "The ALOHA system—another alternative for computer communications," in *Proc. Fall 1970 AFIPS Comput. Conf.*, Nov. 1970, pp. 281–285.

[2] Specification sheet for ORiNOCO world PC card, Agere Systems Inc. Available: ftp://ftp.orinocowireless.com/pub/docs/ORINOCO/BROCHURES/US/World%20PC%20Card%20US.pdf

[3] ARC releases blueForm, a comprehensive solution for bluetooth systems on a chip, ARC International. Available: http://www.arccores.com/newsevents/PR/6-04-01-2.htm

[4] J. Eriksson, S. Krishnamurthy, and M. Faloutsos, "Truelink: A practical countermeasure to the wormhole attack," in ICNP, 2006.

[5] L. M. Ni and P. K. McKinley, "A survey of wormhole routing techniques in direct networks," Computer, vol. 26, no. 2, pp. 62–76, 1993.

[6] A. Scaglione and Y. W. Hong, "Opportunistic large arrays: Cooperative transmission in wireless multihop ad hoc networks to reach far distances," Transactions on Signal Processing, vol. 51, no. 8, 2003

[7] J. Eriksson, S. V. Krishnamurthy, and M. Faloutsos, "Truelink: A practical countermeasure to the wormhole attack in wireless networks," in Proc. ICNP, 2006, pp. 75–84.

[8] R. Poovendran and L. Lazos, "A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks," Wireless Netw., vol. 13, pp. 27–59, 2007.

[9] R. Maheshwari, J. Gao, and S. R. Das, "Detecting wormhole attacks in wireless networks using connectivity information," in Proc. INFOCOM, 2007, pp. 107–115.

[10] A. Papoulis, Probability and Statistics. Prentice Hall, 1990.