Securing Mobile Networks From Wormhole Attacks

In a hostile environment of mobile ad-hoc networks, security has become a primary concern in order to provide protected communication with location privacy between nodes which pose a number of nontrivial challenges to security design.

In this paper we focus on the fundamental security problem of protecting the data transmission in a MANET that is from wormhole attacks and find the solution to this problem. To fix this problem we use directional antennas to secure the physical location privacy of the transmitters and its related expert proposals. We also identify the security issues related to this problem and an overview of ongoing research in securing MANETs.

MANET is a self-configuring network of mobile nodes connected by wireless links-the union of which forms an arbitrary topology. In recent years mobile ad hoc networks (MANETs) have received tremendous attention because of their self-configuration and self - maintenance capabilities. While research effort assumed a friendly and cooperative environment and focused on problems such as wireless channel access and multihop routing; security has become a primary concern in order to provide protected communication between nodes in a potentially hostile environment. Although security has long been an active research topic in networks, the unique characteristics of MANETs present a new set of nontrivial challenges include open network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology. Consequently, the existing security solutions or Wired networks do not directly apply to the MANET domain. The ultimate goal of the security solutions for MANETS is to provide security services such as authentication, confidentiality, integrity, anonymity, and availability to mobile users.

Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural or human-induced disasters, military conflicts, and emergency medical situations etc.Such a network may operate in a standalone fashion, or may be connected to a larger Internet. All these features have helped MANETS gain popularity in the last decade.

II. PRESENTATION OUTPUT

Mobile ad hoc networks-Overview.

Challenges in Securing MANETS.

Ongoing Research in securing MANETS.

Conclusion.

III. CHALLENGES IN SECURING MANETS

The salient features of ad hoc networks pose both challenges and opportunities in achieving these security goals

Use of wireless links renders in MANET susceptible to active impersonation, message reply and message distortion.

To achieve high survivability, ad hoc networks should have a distributed architecture with no central entities.

Due to dynamic nature of MANETS, and a priori trust relationship between the nodes cannot be derived. It is desirable for the security mechanisms to adopt on-the-fly to these changes. A MANET may consist of hundreds or even thousands of nodes. Security mechanisms should be scalable to such a large network.

Security in MANET is an essential component for basic network functions like packet forwarding and routing

Network operation can be easily jeopardized if countermeasures are not embedded into their design.

To secure an ad hoc network, the following attributes may be considered:

Availability

Confidentiality

Integrity

Authentication

Non-repudiation

Security exposures of ad hoc routing protocols are due to two different types of attacks:

Active attacks through which the misbehaving node has bare some energy costs in order to perform some harmful operation and

Passive attacks that mainly consist of lack of cooperation with the purpose of energy saving.

Nodes that perform active attacks with the aim of damaging other nodes by causing network outage are considered to the malicious.

Nodes that perform passive attacks with the aim of saving battery life for their own communications are considered to be selfish.

Selfish nodes can be severely degraded network performances and eventually partition in the network.

A. Overview on WARMHOLE ATTACKS

Wireless ad hoc and sensor networks have gained popularity in recent years for the ease of deployment due to their infrastructure-less nature. One obvious use of such networks is in hostile environments for communications, monitoring, sensing etc. But being a broadcast medium, wireless medium offers an innate advantage to any adversary who intends to spy in or disrupt the network. Wormhole attacks are one of most easy to deploy for such an adversary and can cause great damage to the network.

B. Wormhole Attacks

For launching a wormhole attack, an adversary connects twodistant points in the network using a direct low-latency communication link called as the wormhole link. The wormhole link can be established by a variety of means, e.g., by using a Ethernet cable, a long-range wireless transmission, or an optical link. Once the wormhole link is established, the adversary captures wireless transmissions on one end, sends them through the wormhole link and replays them at the other end.

An example is shown in the above figure. Here X and Y are the two end-points of the wormhole link (called as wormholes). X replays in its neighborhood (in area A) everything that Y hears in its own neighborhood (area B) and vice versa. The net effect of such an attack is that all the nodes in area A assume that nodes in area B are their neighbors and vice versa. This, as a result, affects routing and other connectivity based protocols in the network. Once the new routes are established and the traffic in the network starts using the X-Y shortcut, the wormhole nodes can start dropping packets and cause network disruption. They can also spy on the packets going through and use the large amount of collected information to break any network security. The wormhole attack will also affect connectivity-based localization algorithms and protocols based on localization, like geographic routing, will find many inconsistencies resulting in further network disruption.

In a wormhole attack a malicious node can record packets (or bits) at one location in the network and tunnel then to another location through a private network shared with a colluding malicious node .Most existing ad hoc routing protocols would be unable to find consistent routes to any destination. When an attacker forwards only routing control messages and not data packets, communication may be severely damaged.

Wormhole Attacks

Tunnel packets received in one place of the network and replay then in another place. The attacker can have no key material. All it requires is two transceivers and one high quality out-of-band channel.

Most packets will be routed to the wormhole. The wormhole can drop packets or more subtly, selectively forward packets to avoid detection.

IV. SOLUTIONS TO WORMHOLE ATTACKS AND COUNTERMEASUREMENTS:

In an ad hoc network, several researchers have worked on pretending and detecting wormhole attacks specifically. In section A we discuss a technique called 'packet leashes', which allows preventing packets from traveling farther than radio transmission range. In section B explain about wormhole prevention methods that rely on Round Trip message Time (RTT). Finally, in section C we discuss wormhole detection or prevention techniques suitable for only particular kinds of networks and in D discuss summary of wormhole discovery methods.

A. Packet leashes

Packet Leash is a mechanism to detect and defend against wormhole attacks. The mechanism proposes two types of leashes for this purpose: Geographic and Temporal. In Geographic Leashes, each node knows its precise position and all nodes have a loosely synchronized clock. Each node, before sending a packet, appends its current position and transmission time to it. The receiving node, on receipt of the packet, computes the distance to the sender and the time it took the packet to traverse the path. The receiver can use this distance anytime information to deduce whether the received packet passed through a wormhole or not. In Temporal Leashes, all nodes are required to maintain a tightly synchronized clock but do not rely on GPS information. When temporal leashes are used, the sending node append the time of transmission to each sent packet ts in a packet leash, and the receiving node uses its own packet reception time tr for verification. The sending node calculates an expiration time te after which a packet should not be accepted, and puts that information in the leash. To prevent a packet from traveling farther than distance L, the expiration time is set to:

$$te = ts + (L/C) - \Delta$$

Where c is the speed of light and is the maximum clock synchronization error. All sending nodes append the time of transmission to each sent packet. The receiver compares the time to its locally maintained time and assuming that the transmission propagation speed is equal to the speed of light, computes the distance to the sender. The receiver is thus able to detect, whether the packet has travelled on additional number of hops before reaching the receiver. Both types of leashes require that all

nodes can obtain an authenticated symmetric key of every other node in the network. These keys enable a receiver to authenticate the location and time

Information in a received packet.

In temporal leashes, when sending a packet, the sending node includes in the packet the time at which it sent the packet, ts ; when receiving a packet, the receiving node compares this value to the time at which it received the packet, tr. The receiver is thus able to detect if the packet traveled too far, based on the claimed transmission time and the speed of light. Alternatively, a temporal leash can be constructed by instead including in the packet an expiration time, after which the receiver should not accept the packet; based on the allowed maximum transmission distance and the speed of light, the sender sets this expiration time in the packet as an offset from the time at which it sends the packet. As with a geographical leash, a regular digital signature scheme or other authentication technique can be used to allow a receiver to authenticate a timestamp or expiration time in the received packet.

B. Proposals

1) Directional antenna concept

In a hostile environment, it is important for a transmitter to secure its physical location privacy because an adversary can detect the transmitter if the received power at its antennas is strong enough. We propose this solution to wormhole attacks for ad-hoc networks in which all nodes are equipped with directional antennas. When directional antennas are used, nodes use specific ‘sectors’ of their antennas to communicate with each other. Therefore, a node receiving a message from its neighbor has some information about the location of that neighbor, which knows the relative orientation of the neighbor with respect to itself. This extra bit information makes wormhole discovery much easier than in networks with exclusively omni-directional antennas. This approach does not require either location information or clock synchronization, and is more efficient with energy. They use directional antenna and consider the packet arrival direction to defend the attacks. They use the neighbor verification methods and verified neighbors are really neighbors and only accept messages from verified neighbors. But it has the drawback that the need of the directional antenna is impossible for sensor networks.

Typically, the assumption for ad hoc networks is that nodes are equipped with omni-directional antennas, which can transmit and receive signals in all horizontal directions. However, directional antennas can get antenna gain in the main lobe direction, transmitters can use directional antennas to transmit signals farther away than omni-directional antennas with the same transmit power, or transmit signals to a receiver while using less transmit power.

We model adversaries as passive. Adversaries in this model are assumed to be able to receive any transmitter's signals but are not able to modify these signals. If a set of adversaries detect a transmitter in a synchronous manner, they may be able to compute the transmitter's position with localization algorithms. It is dangerous to reveal the position information to adversaries, because adversaries may find the transmitter and catch it according to its position.

We can employ several directional antennas as relays to bypass a detection system. In Figure, node a, b and c are three network nodes and the black node is a detection system. Assume that node a wants to send data to node c. If node a transmits data to node c directly using directional antenna, as the detection system happens to lie in main lobe direction of node a, it can detect node a with 100% probability.

Using directional antennas to bypass a detection system

2)Related Expert Proposals

Wang et al. present a method for graphically visualizing the occurrence of wormholes in static sensor networks by reconstructing the layout of the sensors using multidimensional scaling. MDS-VOW uses multidimensional scaling to reconstruct the network and detects the attack by visualizing the anomaly introduced by the wormhole, based on the distance of neighbors to a central server. In their approach, each sensor estimates the distance to its neighbors using the received signal strength. During the initial sensor deployment, all sensors send this distance information to the central controller, which calculates the network's physical topology based on individual sensor distance measurements. With no wormhole present, the network topology should be more or less flat, while a wormhole would be seen as a 'string' pulling different ends of the network together. Wang's approach has several aspects that may limit its applicability to general ad hoc networks. This method requires a central controller, and thus not readily suitable for decentralized networks.

L. Lazes et al. describe another scheme to prevent the wormhole attacks on wireless ad hoc networks based on the use of Location-Aware 'Guard' Nodes (LAGNs). They inherit the guard node to detect the message flow between nodes. A node can detect a wormhole attack during the fractional key distribution using single guard property and communication range constraints property. They consider that a node receives an identical message more than once because a malicious entity replays the message or of the multipath effects. Their main consideration is the communication range. If any two guards within the area where guards heard to nodes are located and the area where guard hears at the origin point of the attack are located have a distance larger than double of radius(R) range, there may be a malicious node. In simple, a sensor cannot hear two guards that are more than 2R apart. Their system's weak is that the guard nodes are required to know their location. Lazos's method is elegant. However, it seems more suitable for dense stationary sensor networks.

N. Song et al. proposed another detection technique for detection of the wormhole attacks called a simple scheme based on statistical analysis (SAM). They mainly consider the relative frequency of each link appears in the set of all obtained routes. They calculate the difference between the most frequently appeared link and the second most frequently appeared link in the set of all obtained routes. The maximum relative frequency and the difference are much higher under wormhole attack than that in normal system. The two values are together to determine whether the routing protocol is under wormhole attack. The malicious node can be identified by the attack link which has the highest relative frequency. Song's method requires neither special hardware nor any changes to existing routing protocols. In fact, it does not even require aggregation of any special information, as it only uses routing data already available to a node. These factors allow for easy integration of this method into intrusion detection systems

V. ONGOING RESEARCH IN SECURING MANETS

A. Dealing With Selfish And Malicious Nodes

CONFIDANT (Cooperation OF Nodes, Fairness in dynamic ad hoc by means of combined monitoring and reporting and establishes routes by avoiding misbehaving nodes It is designed as an extension to a routing protocol such as DSR. Another approach is a Token based Cooperation Enforcement Scheme that requires each node of the ad hoc networks to hold a token in order to participate in the network operations. Tokens are granted to a node collaboratively by its neighboring based on the monitoring of the node's contribution to packet forwarding and routing operations. Upon expiration of the token, each node renews its token through a token renewal exchange with its neighbors.

B. Key Management and Node Authentication

A self-Organized Public-key Management scheme based on PGP has been proposed to support security of ad hoc networks routing protocols. Users issue certificate for each other based on their personal acquaintances. In authentication based on Polynomial Secret Sharing public-key certificate of each node is cooperatively generated by a set of neighbors.

- based on the behavior of the node as monitored by the neighbors

Using a group signature mechanism based on polynomial secret sharing, the secret digital signature key used to generate public-key certificate is distributed among several nodes.

VI. CONCLUSION

Security of ad hoc networks has recently gained momentum in the research community Due to the open nature of ad hoc networks and their inherent lack of infrastructure, security exposures can be an impediment to basic network operation Security solution for MANET has to cope with a challenging environment including scarce energy and computational resources and lack of persistent structure