Journal of Novel Applied Sciences
Available online at www.jnasci.org
©2014 JNAS Journal-2014-3-12/1386-1391
ISSN 2322-5149 ©2014 JNAS

SECURITY IN MOBILE AD HOC NETWORKS

Mohammad Reza Pourmir

Computer Engineering Department, Faculty of Engineering, Zabol University, Zabol, Iran

***Corresponding author*:** Mohammad Reza Pourmir

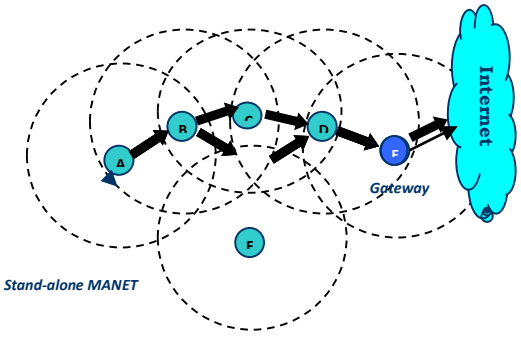
ABSTRACT: Security has become a primary concern in order to provide protected communication between mobile nodes in a hostile environment. Unlike the wire line networks, the unique characteristics of mobile ad hoc networks pose a number of nontrivial challenges to security design, such as open peer-to-peer network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology. These challenges clearly make a case for building multifence security solutions that achieve both broad protection and desirable network performance. In this article we focus on the fundamental security problem of protecting the data transmitting between two nodes in a MANET that is from *wormhole attacks* and find the solution related to this problem. We also identify the security issues related to this problem, various protocols (SRP) used in securing MANETs and overview of ongoing research in securing MANETs.

***Keywords*:** Security, Mobile, Ad Hoc, Network.

INTRODUCTION

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.



After one of the nodes is configured as a gateway, the entire network is connected to an external network like Internet

Presentation output:

- Mobile ad hoc networks-Overview.
- Challenges in Securing MANETS.
- Ongoing Research in securing MANETS.
- Conclusion.

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.

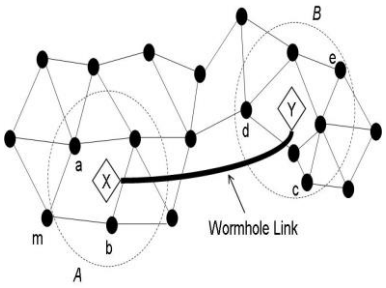
Wormhole attack:

Overview

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.

Wormhole Attack:

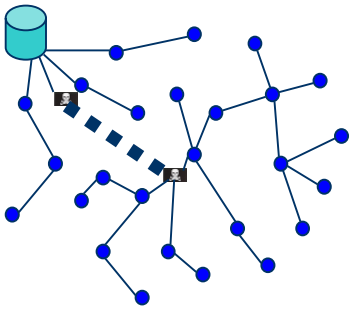
For launching a wormhole attack, an adversary connects two distant points in the network using a direct low-latency communication link called as the wormhole link. The wormhole link can be established by a variety of means, e.g., by using a Ethernet cable, a long-range wireless transmission, or an optical 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.



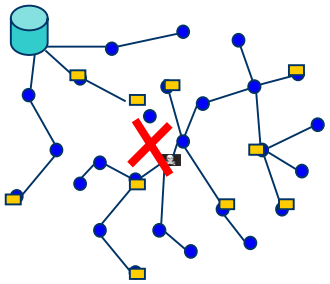
An example is shown in the above figure. Here X and Y are the two end-points of the wormhole link (called as wormholes). X replays in its neighborhood (in area A) everything that Y hears in its own neighborhood (area B) and vice versa. The net effect of such an attack is that all the nodes in area A 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.

***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.

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) -□

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.

Time-of-flight

Another set of wormhole prevention techniques is similar to temporal packet leashes in [6], is based on the time of flight of individual packets. One possible way to prevent wormholes, as used by Capkun et al is to measure round-trip travel time of a message and its acknowledgement, estimate the distance between the nodes based on this travel time, and determines whether the calculated distance is within the maximum possible communication range. The basis of all these approaches is the following. The Round Trip Travel Time (RTT) □□of a message in a wireless medium can, theoretically, be related to the distance *d* between nodes, assuming that the wireless signal travels with a speed of light *c*:

d=□□*c/2 (2) □=2d/c (3)

The neighbor status of nodes is verified if *d* is within the radio transmission range *R*: *R > d* (*d* within transmission range) R >□□*c/2 (4) □□<2*R/c* (5) In essence, the use of RTT eliminates the need for tight clock synchronization required in temporal leashes: a node only uses its own clock to measure time. When a de-facto standard of wireless

ad hoc networks 802.11 Medium Access Control (MAC) protocol is used, such calculations are downright impossible. 802.11 imposes a short wait time of 10□s (SIFS) between the reception of a packet and sending of 802.11 acknowledgement. When 802.11 is used, transmission range *R* is generally about 300 meters. The speed of light *c* is 3×10–8 *m/s*. Then, from equation 4: □□= 2d/c = 600m/3 ×10–8 m/s = 0.000002s = 2 × 10-6 = 2□s (6)

Therefore, the RTT is an order of magnitude smaller than the delay required by the protocol. We could, of course, account for this processing time by modifying formula 4 in the following manner:

□

□□=2d/c+S (7)

Where S is SIFS (Short Inter frame Space). However, note that wormhole attackers are not limited by the rules of the network, and could send their packets without 802.11-imposed delay. Approaches based on RTT that one node sends a packet to another; the answer should arrive very shortly, ideally within the amount of time a wireless signal would travel between the nodes. If there is a wormhole attacker involved, packets end up traveling farther, and thus can not be returned within a short time.

Specialized techniques

A wide variety of wormhole attack mitigation techniques have been proposed for specific kinds of networks: sensor networks, static networks, or networks where nodes use directional antennas. In this section, we describe and discuss such techniques, commenting on their usability and the possibility of their use in general mobile MANETs. Hu and vans propose a solution to wormhole attacks for ad hoc networks in which all nodes are equipped with directional antennas. In this technique nodes use specific 'sectors' of their antennas to communicate with each other. Each couple of nodes has to examine the direction of received signals from its neighbor. Hence, the neighbor relation is set only if the directions of both pairs match. This extra bit of information makes wormhole discovery and introduces substantial.

Inconsistencies in the network, and can easily be detected. Wang and Bhargava introduce an approach in which network visualization is used for discovery of wormhole attacks in stationary sensor networks. In their approach, each sensor estimates the distance to its neighbors using the received signal strength. 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 wormholes 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.

Lazos et al proposed a 'graph-theoretical' approach to wormhole attack prevention based on the use of Location-Aware 'Guard' Nodes (LAGNs). Lazos uses 'local broadcast keys' - keys valid only between one-hop neighbours - to defy wormhole attackers: a message encrypted with a local key at one end of the network can not be decrypted at another end. Lazos proposes to use hashed messages from LAGNs to detect wormholes during the key establishment. A node can detect certain inconsistencies in messages from different LAGNs if a wormhole is present. Without a wormhole, a node should not be able to hear two LAGNs that are far from each other, and should not be able to hear the same message from one guard twice. Khalil et al propose a protocol for wormhole attack discovery in static networks they call LiteWorp. In LiteWorp, once deployed, nodes obtain full two-hop routing information from their neighbours. While in a standard ad hoc routing protocol nodes usually keep track of their neighbours are, in LiteWorp they also know who the neighbours' neighbours are, - they can take advantage of two-hop, rather than one-hop, neighbor information. This information can be exploited to detect wormhole attacks. Also, nodes observe their neighbours' behavior to determine whether data packets are Being properly forwarder by the neighbor. Song et al proposes a wormhole discovery mechanism based on statistical analysis of multipath routing. Song Observes that a link created by a wormhole is very attractive in routing sense, and will be selected and requested with unnaturally high frequency as it only uses routing data already available to a node. These factors allow for easy integration of this method into intrusion detection systems only to routing protocols.

Ongoing Research in Securing MANETs:

Secure remote password protocol

Overview

The SRP protocol has a number of desirable properties: it allows a user to authenticate himself to a server, it is resistant to dictionary attacks mounted by an eavesdropper, and it does not require a trusted third party. It effectively conveys a zero-knowledge password proof from the user to the server. Only one password can be guessed at per attempt in revision 6 of the protocol. One of the interesting properties of the protocol is that even if one or two of the cryptographic primitives it uses are attacked, it is still secure. The SRP protocol has been revised several times, and is currently at revision six. The SRP protocol creates a large private key shared between the two parties in a manner similar to Diffie-Hellman, and then verifies to both parties that the two keys are identical and that both sides have the

user's password. In cases where encrypted communications as well as authentication are required, the SRP protocol is more securing than the alternative SSH protocol and faster than using Diffie-Hellman with signed messages. It is also independent of third parties, unlike Kerberos. The SRP protocol, version 3 is described in RFC 2945. SRP version 6 is also used for strong password authentication in SSL/TLS and other standards such as EAP and SAML, and is being standardized in IEEE P1363 and ISO/IEC 11770-4.

The Secure Routing Protocol (SRP) is designed as an extension compatible with a variety of existing reactive routing protocols. SRP combats attacks that disrupt the route discovery process and guarantees the acquisition of correct topological information. ARIADNE (A Secure Routing Protocol based on DSR) guarantees that the target node of a route discovery process can authenticate the initiator. The initiator can in turn authenticate each intermediate node on the path to the destination present in the RREP messages. No intermediate node can remove a previous node in node list in the RREQ or RREP messages. ARAN secure routing protocol (conceived as an on-demand routing protocol) that detects and protects against malicious actions carried out by third parties and peers in the ad hoc environment. It introduces authentication, message integrity and non-repudiation as part of a minimal security policy for the ad hoc environment. Consists of a preliminary certification process, a mandatory end-to-end authentication stage and an optional second stage that provides secure shortest paths.

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.

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.

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.

REFERENCES

Alfred Menezes A, Oorschot PV and Vanstone S. 2001. "Handbook of Applied Cryptography," CRC Press, October 1996 – 5th reprinting.

Asokan N and Ginzboorg P. 2000. "Key Agreement in Ad Hoc Networks," Computer Communications 23 (17): 1627-1637.

IEEE Std. 802.11, "Wireless LAN Media Access Control (MAC) and Physical Layer (PHY) Specifications," 1999.

Johnson DB. 2001. "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks," Internet Draft, IETF MANET Working Group, March 2nd.

Krawczyk H, Bellare M and Canetti R. 1997. "HMAC: Keyed-Hashing for Message Authentication," RFC 2104.

Lamport L, Shostak R and Pease M. 1982. "The Byzantine Generals Problem," ACM Trans. Program. Languages, Vol. 4, no. 3, pp. 382-401.

Stajano F and Anderson R. 1999. "The Resurrecting Duckling: Security Issues for Ad Hoc Wireless Networks," Security Protocols, 7th International Workshop, LNCS, Springer-Verlag.

Zhou L and Haas ZJ. 1999. "Securing Ad Hoc Networks," IEEE Network Magazine, vol. 13, no.6.