A secure routing protocol for wireless ad hoc network

Vijay khata

M.E(I.T) Student,I.T Department,L.D College of engineering Ahmedabad,Gujarat,India.

ABSTRACT

Ad hoc networks have attractive applications in both military and disaster situations and also in commercial uses like sensor networks or conferencing. However the nature of ad hoc networks makes them vulnerable to attacks, especially in the routing protocols. In this we present an on demand secure routing protocol for ad hoc network based on distributed authentication mechanism. The protocol makes use of recommendation and trust evaluation to establish a true relationship between network entities and use feedback to adjust it. The protocol does not need support of trusted third party an can discover multiple threats against ad hoc routing protocols, specifically examining aodv(ad hoc on demand distance vector) and dsr(dynamic source routing). Our routing protocol is based on certificates and successfully defeats all identified attacks.

Keywords: *Trust table,distributed authentication model,routing protocol,ad hoc network*

1. INTRODUCTION

An ad hoc network is a set of wireless mobile nodes that form a dynamic autonomous network without the intevention of centralized access points or base stations. Ad hoc wireless networks assume no pre-employed infrastructure is available for routing packets end-to-end in network and instead rely on intermediary peers.securing ad-hoc routing packets exchanges because each user brings to network their mobile unit, without centralizes control of traditional network.in this paper we demonstrate exploits that are possible against ad hoc routing protocols defined various security environments and offer secure solutions with an authentication routing protocol. Our proposed protocol, authenticated routing for ad hoc networks, detects and protects against malicious actions by third parties and peers in one particular ad hoc environment.

ARAN introduces authentication, message integrity and non-repudiation to an ad hoc environment as part of minimal security policy.our evaluations show ARAN has minimal performance costs for increased security in terms of processing and networking overhead.

BACKGROUND

An ad hoc networks form, of mobile nodes join together and create network by agreeing to route messages for each other. There is no shared infrastructure in an ad hoc network, such as centralized routers or defined administrative policy.Fundamental difference between ad hoc network and standard ip networks necessitates the development of new security services.

ATTACKS TO AD HOC NETWORK ROUTING PROTOCOLS

Our main concern is those attacks, which are trying to improperly modify data, gain authentication, or gain authorization by inserting false packets or by modifying packets. The attacks analyzed here are general attacks to ad hoc network routing protocols, not to a specific routing protocol. Broadly speaking, attacks to routing protocols come mainly from two sources, external and internal . External attacks come from outside intruders who do not belong to the network. Internal attacks come from compromised nodes in the network.

EXTERNAL ATTACK

An outside intruder could attack a routing protocol in various ways. Specific threats include the following:

- Replay attack: An intruder could passively collect routing information, for example route request/reply. Later, the intruder could retransmit "obsolete" routing information. If obsolete information is accepted and disseminated, a node could make incorrect routing decision.

- Denial of Service (DoS): A malicious node could generate false routing messages and flood them into the network so that a portion of network resource is wasted by these junk messages and some CPU cycles and memory of nodes are taken up by the processing of them. Sometimes, DoS attacks are quite harmful. For example, an attacker can broadcast bogus route error messages about some links so that these links are thought to be down.

- Modification: Malicious nodes can modify fields of a routing message, like sequence number and hop counts of AODV, to cause redirection of network traffic. If integrity measures, e.g., Message Authentication Code, are used to protect the routing message, this attack will not succeed, but it is still a DoS attack.

- Masquerading: A malicious node can launch IP spoofing attack, impersonate other nodes, and disseminate false routing message so that the routing tables are not consis- tent

Internal Attacks

Internal attackers may control everything of the compromised nodes, even the private keys or shared secrets with other nodes. An internal attacker can launch all the attacks of an external attacker and it is more harmful. Even with security measures, the internal attackers can still pass authentication and generate correct Message Authentication Code for modified or fabricated routing updates. So internal attacks are difficult to detect and handle. When an internal attacker inhabits in a network, it has two choices during the route discovery process: launching attacks to destroy routinfrastructure,

Attack	AODV	DSR	ARAN
Remote redirection			
modif. of seq. numbers	Yes	No	No
modif. of hop counts	Yes	No	No
modif. of source routes	No	Yes	No
tunneling	Yes	Yes	Yes, but only to lengthen path
Spoofing	Yes	Yes	No
Fabrication			
fabr. of error messages	Yes	Yes	Yes, but non-repudiable
fabr. of source routes (cache poisoning)	No	Yes	No

Behaving as a benign node during route establishment and launching attacks during data packet delivery . So in either case the attacker does not want to be excluded from the routing protocol, otherwise it gains no benefit.

A Distributed authentication model

In our protocol, authentication among different nodes is done by a "Distributed Authentication Model", which is described in this section. In an ad hoc network, each node maintains a repository (Trust Table) of known entities. Each entity on the table is assigned a trust value depending on its reliability. The trust value metric is an important factor on the accuracy of the trust management system. At present there are no standards. We utilize a concrete trust value metric. The trust value of a node can be: -1(distrust), 0(ignorance), 1(minimal), 2(aver- age), 3(good), and 4(complete), where the number is the trust value and the word in "()" gives the meaning of the value. In our protocol, as long as an entity's trust value is ≥ 2, it is assigned a "yes", meaning "trustworthy", otherwise, it is assigned a "no", meaning "untrustworthy".

A SECURE ROUTING PROTOCOL

In this section we present our secure routing protocol for ad hoc networks. It is an on-demand routing protocol and satisfies the special features common to ad hoc networks: dynamically changing topology and low-power devices. We do not assume the existence of trusted servers, which may be infeasible for ad hoc networks. The protocol can discover multiple paths between two nodes. This is essential for an ad hoc network to be able to tolerate attacks induced path failures and provide robust packet delivery. Our protocol is designed for the following situations: military applications, e.g., battle field. Emergency situations. The sole assumption of the protocol is that at the beginning, all the nodes share a group key K and can be trusted. This is a reasonable assumption since all the members belong to same troop or team. Certainly it is possible that some nodes may be compromised later and become untrustworthy. Yet as analyzed in Section V, these attacks can be prevented or detected. Moreover, our protocol can keep out the attackers timely and proactively. We do not consider physical layer and link layer attacks in this paper, like jamming attacks. We also presume that there are no collaborating attacks.

Setup

Every node installs the Distributed Authentication Model. Each node creates a Trust Table. At the begining, all the nodes can be trusted and are assigned a trust value. An optimistic node might assign a larger trust value to other nodes, e.g., 4, while a conservative node may assign a smaller value, e.g., 3. This is the starting point of trust.

B. Neighbor Discovery and Key Establishment

Every node periodically broadcasts a Hello message. With this mechanism, a node can detect its new neighbors. When a new neighbor is found, a node invokes the Distributed Authentication Model to authenticate the neighbor and puts the neighbor in its Trust Table. Every node sets up a secret key with each trustworthy neighbor by using a two-party key establishment protocol.

Authenticated Routing for Ad hoc Networks

ARAN makes use of cryptographic certificates to offer routing security. Such certificates are already seeing deployment as part of one-hop 802.11 networks; this is the case on the UMass campus, where an 802.11 VPN is deployed and certificates are carried by nodes. ARAN consists of a preliminary certification process followed by a route instantiation process that guarantees end-to- end authentication. The protocol is simple compared to most non-secured ad hoc routing protocols. It should be noted that the exploits listed in Section 3 are primarily due to the optimization that have been introduced into ad hoc routing protocols for route computation and creation. Route discovery in ARAN is accomplished by a broadcast route discovery message from a source node which is replied

to unicast by the des- tination node, such that the routing messages are authenticated at each hop from source to destination, as well as on the reverse path from the destination to the source.

Certification ARAN requires the use of a trusted certificate server T, whose public key is known to all valid nodes. Keys are a priori generated and exchanged through an existing, perhaps out of band, relationship between T and each node. Before entering the ad hoc network, each node must request a certificate from T. Each node receives exactly one certificate after securely authenticating their identity to T. The methods for secure authentication to the certificate server are left to the developers. Details of how certificates are revoked are explained below in Section 5.4. A node A receives a certificate from T as follows: T! A:certA =[IPA;KA+ ;t; e ₵KT] The certificate contains the IP address of A, the public key of A, at which the certificate expires. Fig. 4 summarizes our notation. These variables are concatenated and signed by T. All nodes must maintain fresh certificates with the trusted server. Nodes use these certificates to authenticate themselves to other nodes during the exchange of routing messages.

Authenticated Route Discovery

The goal of end-to-end authentication is for the source to verify that the intended destination was reached. In this process, the source trusts the destination to chose the return path. Source node ,A, begins route instantiation to destination X by broadcasting to its neighbors a route discovery packet (RDP):A broadcast :[RDP;IPX;certA;NA;t₵KA].

The RDP includes a packet type identifier ("RDP"), the IP ad- dress of the destination (IPX), A's certificate , a nonce NA, and the current time t, all signed with A's private key. Each time A performs route discovery, it monotonically in- creases the nonce. The nonce and timestamp are used in con- junction with each other to allow for ease of nonce recycling. The nonce is made large enough that it will not need to be recycled within the probable clock skew between receivers. Other nodes then store the nonce they have last seen for a particular node along with its timestamp. If a nonce later re-appears in a valid packet that has a later timestamp, the nonce is assumed to have wrapped around, and is therefore accepted. Note that a hop count is not included with the message. When a node receives an RDP message, it sets up a reverse path back to the source by recording the neighbor from which it received the RDP. This is in anticipation of eventually receiving a reply message that it will need to forward back to the source. The receiving node usesA's public key, which it extracts from A's certificate, to validate the signature and verify that A's certificate has not expired. The receiving node also checks the (NA;IPA) tuple to verify that it has not already processed this RDP. Nodes do not forward messages for which they have al- ready seen the tuple, otherwise, the node signs the contents of the message, appends its own certificate, and forward broad- casts the message to each of its neighbors. The signature pre- vents spoofing attacks that may alter the route or form loops. Let B be a neighbor that has received from A the RDP broadcast, which it subsequently rebroadcasts. Broadcast :[[RDP;IPX;certA;NA;t₵KA₵KB;certB] Upon receiving the RDP,B's neighbor validates the signature with the given certificate .C then removes B's certificate and signature, records its predecessor, signs the contents of the message originally broadcast by A, appends its own certificate and forward broadcasts the message.C then rebroadcast the RDP .a time stampt of when the certificate was created.

SECURITY REQUIREMENTS OF AD HOC NETWORKS

A good secure routing algorithm prevents each of the exploit presented in Section 3; it must ensure that no node can prevent successful route discovery and maintenance between any other nodes other than by non-participation. In sum, all secure ad hoc routing protocols must satisfy the following requirements to ensure that path discovery from source to destination functions correctly in the presence of malicious adversaries: (1) Route signaling cannot be spoofed; (2) Fabricated routing messages cannot be injected into the network; (3) Routing messages cannot be altered in transit, except according to normal functionality of the routing protocol; (4) Routing loops cannot be formed through malicious action; (5) Routes cannot be redirected from the shortest path by malicious action. The above requirements comprise the security needs of an open environments. The following additional requirement dis- tinguishes a managed open environment: (6) Unauthorized nodes should be excluded from route computation and discovery. This requirement does not preclude the fact that authenticated peers may act maliciously as well. Additionally, we assume that the managed-open environment has the opportunity for pre-deployment or exchange of public keys, session keys, or certificates. We define a managed hostile environment to have requirements listed above as well as the following: (7) The network topology must not be exposed neither to adversaries nor to

authorized nodes by the routing messages. Exposure of the net- work topology may be an advantage for adversaries trying to destroy or capture nodes

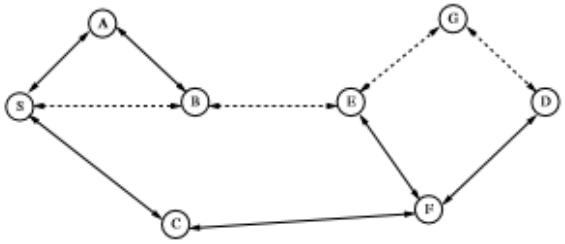

Fig. 1. An example ad hoc network. S-source node; D-destination node; A, B, C, E, F and G are intermediate nodes.

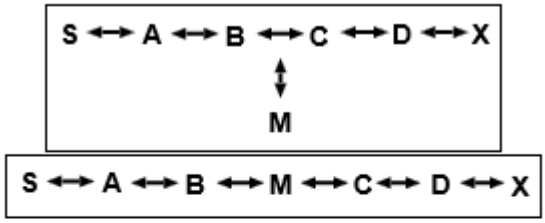

Figure 1. (A) A simple ad hoc network. (B) Another example ad hoc network.

CONCLUSION:-

In this paper, we proposed a secure routing protocol for ad hoc networks with a shared group key as the sole assumption .The key security measures in this protocol are distributed authentication and Message Authentication Code. We developed a Distributed Authentication Model, with which different nodes can authenticate each other. Integrity is ensured by Message Authentication Code, which is calculated by using the shared group key or pair-wise shared secret keys. A node establishes shared secret keys only with its trustworthy neighbors rather than all network nodes. The protocol can prevent or detect most of the attacks common to ad hoc routing protocols. The protocol is also able to exclude attackers timely and proactively. Moreover the protocol is capable of discovering multiple routes existed between two nodes and is also appropriate for dynamically changing network topology. Trust value system and trust evaluation functions are important components of the Distributed Authentication Model. Currently there are no standards. We plan to optimize them and improve their accuracy in our future work.

Our secure routing protocol can detect attacks, such as the modification of RREQ and the modification of sequence number. In our future work we will study the measures to take when these attacks are detected.

REFERNCES:-

(1)HUAIZHI LI,DEPARTMENT OF COMPUTER SCIENCE,PROCEEDINGS OF 39TH HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES IN 2006

(2)MUKESH SINGAL,DEPARTEMENT OF COMPUTER SCIENCE,PROCEEDINGS OF THE 39TH HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES 2006

(3)KIMAYA SANZGIRI,BRIDGET DAHILL,BRIAN NEILLEVINE,CLAY SHIELDS DEPARTMENT OF COMPUTER SCIENCE,UNIVERSITY OF MASSACHUSETTS,AMHERST.

BIBLOGRAPHY

Vijay khata got the Bachelor degree in computer science from MS UNIVERSITY and now pursuing M.E(I.T) from L.D College of Engineering,Ahmedabad.