A Framework for Integrated Internet and Ad hoc Network Security

Bin Xie and Anup Kumar
Computer Science and Computer Engineering,
University of Louisville, Louisville, KY, USA, 40292
b0xie001@louisville.com and ak@louisville.edu

Abstract

Extending mobile IP to ad hoc networks with the foreign agent (FA) acting as the bridge between the wired network and ad hoc networks can provide the global Internet connectivity for ad hoc hosts. The existing research in the area of the integrated wired and ad hoc network is carried out in a non-adversarial setting. This paper proposes an effective solution to solve the security related problems encountered in these integrated networks. The proposed approach uses the modified minimal public based authentication protocol not only for mobility binding at the home agent (HA) but also for access control and route discovery. This security protocol also excludes malicious nodes from performing the ad hoc network routing. This paper focuses on preventing ad hoc hosts from the attacks of anti-integrity, anti-confidentiality, anti-authentication and duplication.

1. Introduction

The mobile ad hoc network can be used to extend the coverage of not only the cellular networks, but also of the high frequency wireless LANs. For example, the scheme discussed in [1] provides the global Internet connectivity for the ad hoc networks to support ubiquitous communications. The Internet connectivity and the ad hoc networks are susceptible to attacks due to wireless links, energy constraints, and difficulty to self-configure because of the mobility. In this paper, we have studied the security threats that can arise on the integrated Internet and ad hoc network. Our proposal consists of the following three parts: i) extending mobile IP security mechanism over to ad hoc network; ii) certificate and key management with the help of foreign agent (FA) and home agent (HA), iii) development of secure routing protocol for FA discovery and ad hoc routing.

The rest of this paper is organized as follows. Section 2 briefly describes the related works about ad hoc and mobile IP security. Section 3 represents the global connectivity for ad hoc networks and then discusses different types of possible attacks in the integrated network. Section 4 proposes a security mechanism of mobile IP to enhance the trustworthiness of ad hoc hosts. Then section 4 addresses how to enforce security rules both on FA discovery and on ad hoc route by the way of certificates. Section 5 analyzes the effectiveness of the proposed security approach on the Internet connectivity as well as the ad hoc networks. Concluding remarks are discussed in section 6.

2. Related works

The policies of the security of ad hoc networks and mobile IP are normally studied separately in the existing literature and have never been considered before in an integrated environment. We review some existing security schemes for ad hoc protocols and mobile IP.

Since the ad hoc routing protocols are based on a benign environment, those protocols may suffer from security attacks in an adversarial environment. Some of the ad hoc security protocols include Secure Efficient Distance Vector Routing protocol (SEAD) [3], The Secure Routing Protocol (SRP) [4], ARIADNE [5], ARAN [6]. However, these ad hoc security protocols are based on standalone mobile ad-hoc networks. There are no apriori trust relationships between ad hoc hosts. In a standalone ad hoc network, it is difficult to consistently identify a host with a unique identifier because it is easy for ad hoc host to change its identity. Moreover, it is difficult to prevent selfish behavior of an ad hoc host.

Although the base mobile IP protocol [8] defines an authentication extension (AE) to support authentication at registration (secret-key based authentication), there are some deficiencies in this authentication process. Since the protocol [8] only requires authentication between home agent (HA) and mobile node (MN), network may be attacked unless an overall authentication is enforced between the FA and HA and between the FA and MN. Enforcing the overall authentication requires heavy secret-key management to support large number of users since it is necessary for MN to have a separate secret-key for every HA and FA. *Minimal public based authentication* [9] provides a strong and scalable authentication strategy. The protocol also uses secret key cryptography in order to minimize the requirement of computing power, as well as the administration cost imposed on MN. In addition, the protocol given in [9] provides the scalability and non-repudiation that seem likely to be demanded by various settings. The key idea of the protocol in [9] is to let the HA act as a public-key authentication agent for MN by sharing security association between the HA and MN or FA. MN performs all cryptographic operations using its secret key.

This paper investigates the security for combined mobile IP and mobile ad hoc networks. The paper also

0-7803-8623-X/04/$20.00 ©2004 IEEE

proposes the establishment of trust relationships for MNs through FA authentication.

3. Integrated Internet and ad hoc networks

3.1. Connectivity for the integrated network

Figure 1 illustrates an example of the integrated Internet and ad hoc network. The inside area of dash circle represents the coverage of FA. The left side of figure is the wired network that consists of HA, correspondent node (CN), and FA connected by the Internet. The FA acts additionally as the bridge between the ad hoc and wired network as necessary. The right side is the ad hoc network using ad hoc routing protocol for multi-hop communication. In Figure 1, since the MNs 1 and 3 are located in the coverage of FA, the two nodes can act as gateways for other ad hoc hosts in ad hoc network to provide connectivity to the Internet. There are two types of communications possible in Figure 1: i) between MN 5 and CN; ii) between the MNs 6 and 8.

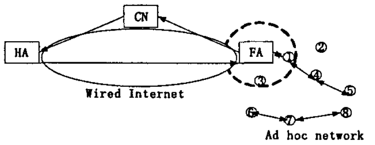


Figure 1. Integrated ad hoc network

Figure 2 illustrates an instance of the integrated ad hoc and wired network. In Figure 2, the dotted lines represent the wireless connections. The M1, M2, and M3 are three malicious ad hoc nodes. In Figure 2, MNs 1, 5 and M1 can reach FA directly. If the communicating source and target MNs are both in the ad hoc network (in Figure 2, *S* and *D*). Then this type of communication is called Intra-MANET (Mobile Ad hoc Network) communication. On the other hand, if one of the communicating hosts is on the ad hoc network (in Figure 2, e.g., *D*) and the destination is outside the ad hoc network (in Figure 2, e.g., *CN*), this communication is referred as Internet-MANET. In the Internet-MANET communication, a connection could be compromised by attacks on the Internet connectivity and attacks on the ad hoc routing protocols. The two groups cannot be neatly separated in this framework because the attacks on the ad hoc routing protocols may also disrupt the Internet connectivity.

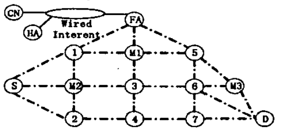


Figure 2: An example of an adversarial integrated network. (M: malicious host, S: source Node, D: destination Node.)

3.2. Security requirements

An integrated Internet and ad hoc network can be subjected to many types of attacks. The goal of the proposed security scheme is to provide protection not only from Internet intrudes but also from malicious nodes (M1, M2, and M3) in ad hoc network. A few of those possibilities are mentioned in this section. A bogus registration is an example of active attack in which an attacker does a registration with a bogus care-of-address by masquerading itself as some one else. By advertising fraudulent beacons, an attacker might be able to entice MN to register with the attacker as if MN has reached HA or FA. Furthermore, the attacker can capture sensitive personal or network data for the purpose of accessing network. This type of attack is difficult for an attacker to implement because the attacker must have detailed information about the agent. Another type of attack for the same purpose is when an attacker records the valuable messages transmitted while MN accesses and registers with FA via a receiver and antenna that is compatible with the agent. After entering the network, the malicious node pretends to be a trustable node to ruin network operation. In general, attacks on Internet connectivity are caused by malicious nodes that modify, drop or generate messages related to mobile IP such as *Advertisement*, *Registration Request* or *Reply* to disrupt the global Internet connectivity.

Most of the ad hoc routing protocols are based on the two underlying assumptions: there's no reachable fixed infrastructure in ad hoc network; all nodes in the ad hoc network are trustworthy during the process of route discovery. In the trustable environment, each participating node cooperates honestly during the process of route discovery. In practice, however the routing protocols are susceptible to a wide variety attacks in adversarial environment. Almost all possible attack methods on the traditional ad hoc network also exist in the integrated wired and ad hoc networks. Whatever the attacks are, the attackers will exhibit their actions in the form of refusing to participate fully and correctly in routing protocol according to the principles of *integrity, authentication, confidentiality, and cooperation.* The detailed information about attacks can be found in [3, 4, 5 and 6].

4. Proposal for securing global connectivity

This section develops a secure connectivity framework for integrated ad hoc and wired network. The protocol provides security to mobile IP communication as well as ad hoc routing. The proposed approach for securing global connectivity between ad hoc network and Internet has the following properties:

1. Mobile IP security follows the security strategy of the *minimal public based authentication protocol* with certain extensions. HA acts as the authentication server.
2. Only after being registered with FA and certified by FA, a MN can be trusted by other MNs so that the MN can participate in ad hoc routing protocol.
3. MN's home address, its ad hoc address and its certificate are bound for identifying an ad hoc host. Therefore, the trustable relationship between ad hoc nodes is enhanced.

4. The proposed approach also uses the cryptographic certificates, which are also used in a single hop 802.11 and Authenticated Routing for Ad hoc Network (ARAN) [6], to make ad hoc routing secure.

The security protocol for integrated wired and ad hoc network includes two parts: i) the global security of mobile IP, ii) the security of ad hoc network. In order to communicate with other nodes in ad hoc network or wired network, the following operations take place in the integrated network:

1. FA advertisement and discovery: FA advertises and MN finds a route to FA.
2. MN's registration with FA and HA: MN follows the *minimal public based authentication protocol* to register with FA and HA.
3. Binding MN's mobile IP home address and its ad hoc ID: MN's Home address, its ad hoc identifier and its certificate are bound for tracking the history of the MN activity.
4. FA issues a certificate to the registered MN for ad hoc routing and broadcasts it to all the ad hoc hosts in the network.
5. MN creates its local data structure of certificates for verifications during ad hoc network routing.

The sequence diagram in Figure 3 illustrates the basic process of security implementation in the integrated wired and ad hoc network. The example assumes that it is the first time MN_A is communicating in ad hoc network. Other ad hoc hosts are already successfully registered with FA and are certified by FA. To find a path from MN_A to FA, MN_A initiates the FA discovery by issuing a message *R_Request*. FA replies the MN_A with *R_Reply*. Then MN_A sends a message *Solicitation* to FA for requesting an *Advertisement* with a COA (care of address) from FA. After receiving advertisement, the MN_A registers with HA via FA. If the registration is successful, then FA issues MN_A a certificate and also sends other MN's certificates. FA also sends other MNs the MN_A's certificate. Therefore, MN_A can initiate a route discovery for searching other mobile host, such as MN_X in ad hoc network or CN in wired network. In the following sections, each step is discussed in detail.

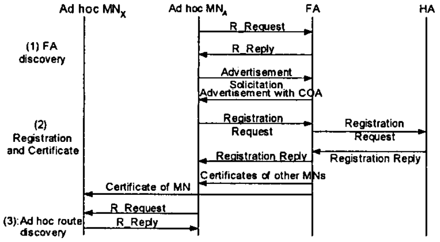


Figure 3: An example of routing security

4.1. Global security of mobile IP

The proposed approach for securing global route uses the *minimal public based authentication protocol* with the extension of using registration as means to control access in the ad hoc network. Before MN gains its successful mobile IP registration and a certificate from FA, it cannot participate in ad hoc routing protocol. After MN registers with FA successfully, FA creates and discloses MN's certificate to other ad hoc mobile hosts, meanwhile FA is responsible for updating MNs' certificates periodically or at the request of MN. Each ad hoc host has a local table to record recently received packet information, e.g., packet source address (MN_{HM}), nonce (N_{MN}), and time (t). Each node shares a secret key with it's HA for the calculation and validation of MAC (Message Authentication Code). Certification Authority, HA, and FA have a pair of public and private keys separately. Tables 1 and 2 list the notations and messages used for the development of the proposed protocol.

Table 1. Notations used for the proposed protocol.

M, N	Concatenation of two messages M and N in the order specified
MN_{HM}	MN home address
HA_{id}, FA_{id}	HA and FA IP address as its ID
N_X	Nonce issued by X, e.g. HA, MN.
<M>K	MAC value of message *M* under key K
CA	Certification authority
K_X, K^{-1}_X	Public and private key of X
$[M]\,K^{-1}_X$	Digital signature of message *M* generated using private key of MN *X*
$Cert_X$	Certificate of X
T_{MN}	Issuing time of MN's certificate
T	Current estimated time
MN_{COA}	MN's care-of-address
$S_{MN\text{-}HA}$	Shared secret key between MN and HA
MN_{HMx}, MN_{IPx}	Home's address, and care-of-address of Mobile Node *X*
E_{MN}	Certificate expiring time of MN
MN_X	Mobile node *X*

Table 2. Messages for the proposed protocol.

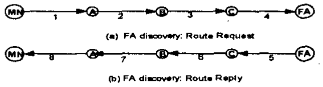
Request	A bit pattern indicating a registration request
Reply	A bit pattern indicating a registration reply
Reśult	A value indicating the result of registration
R_Request	A packet indicating a route request
R_Reply	A packet indicating a route reply
R_Error	A packet indicating a routing error
Advertisement	A bit pattern indicating an advertisement

4.1.1. FA advertisement and FA discovery

FA advertises periodically to MNs, *(AA1):* M_1, $[M_1]$ K^{-1}_{FA} $Cert_{FA}$; where M_1 is *Advertisement*, FA_{id} and MN_{COA}. While receiving an advertisement from FA, MN decrypts the advertisement by using FA's public key, and compares the FA's address and sequence number with those of previously received advertisements in its local table. MN discards the duplicate advertisements. If it is a fresh advertisement, MN records FA certificate, IP address, and sequence number to avoid duplication. The records are also used for tracking FA advertisement history. Then MN rebroadcasts the original advertisement on its interface for other neighboring ad hoc hosts.

Before FA discovery, MN establishes public-private keys with FA (K_{MN}, K^{-1}_{MN}) using key setup protocol, e.g., *Diffie-Hellman* key exchange [7]. Since the *Diffie-Hellman* key exchange allows two entities to exchange keys on an unsecured communication path, therefore during key setup, MN doesn't take care of the route to FA. Although after key exchange, MN still can not authenticate FA, it does not matter because if FA is a forged one, a registration reply message will indicate it. If MN has never registered with the FA, but MN wishes to have the knowledge of route to FA, MN issues a route discovery with a destination address of FA_Address (224.0.0.11); this address is the mobile agent multicasts group address. Otherwise, if MN has registered with the FA, the MN could start its route discovery according to the steps in 4.2.3 (ad hoc route discovery). *R_Request* packet in the proposed approach is named for route request and *R_Reply* is named for route reply. The process of MN to discover FA includes two stages as shown in Figure 4: FA discovery request and FA discovery reply.

The MN's request for FA discovery has the following steps. MN initiates *R_Request* with FA_Address that is signed with its private key. When any neighbor *A* of MN receives *R_Request*, the neighbor *A* checks if it has already seen the request and whether the packet has a valid timestamp and then discards the duplicated or invalid request. Knowing that the destination is FA, the neighbor *A* cannot verify MN' signature because FA still has not disclosed the MN's public key with a certificate. Therefore the neighbor *A* leaves the job of verification of MN's signature to FA. The neighbor *A* rebroadcasts the FA discovery request after appending its address and signing the packet. All intermediate nodes, e.g., *A*, *B*, and *C*, must be registered nodes. Aside from above steps, each intermediate node except for MN's neighbors, e.g., node *B* and *C*, but no *A*, must validate the signature of its preceding node with the public key of preceding node, which is disclosed by FA and stored by each MN in its local certificate data structure. Each intermediate node except for MN's neighbors, e.g., node *B* and *C*, but not *A*, removes the signature of preceding node before its rebroadcast. In the end, FA receives the route discovery packet. The following steps in Figure 4 show the above processes.



(a) FA discovery: Route Request

(b) FA discovery: Route Reply

Figure 4. Steps of FA discovery

1. *MN* broadcasts route request:

$[R\_Request, MN_{HM}, FA\_Address, N_{MN}, t]\ K^{-1}_{MN}$

2. *A* receives *R_Request* from *MN:*

$[[R\_Request, MN_{HM}, FA\_Address, N_{MN}, t]\ K^{-1}_{MN}, MN_{IPa}]\ K^{-1}_{IPa}$

3. *B* receives *R_Request* from *A:*

$[[R\_Request, MN_{HM}, FA\_Address, N_{MN}, t]\ K^{-1}_{MN}, MN_{IPa}, MN_{IPb}]\ K^{-1}_{IPb}$

4. *C* receives *R_Request* from *B:*

$[[R\_Request, MN_{HM}, FA\_Address, N_{MN}, t]\ K^{-1}_{MN}, MN_{IPa}, MN_{IPb}, MN_{IPc}]\ K^{-1}_{IPc}$

When the FA receives the route discovery packet from node *C* as shown in Figure 4, the FA validates *C*'s signature as well as MN's signature using their public keys. If FA receives several valid discovery packets from the same MN, FA chooses a route with optimal metrics, for instance, minimal multi-hops. FA initiates *R_Reply* packet by using FA's address with a new nonce for next request message. FA returns the *R_Reply* to MN with the reverse path from MN to FA. Before *R_Reply* arrives to MN's neighbor, each intermediate node validates the signature of the preceding node and prevents duplication by comparing nonce and timestamp with its local table. Then each intermediate node rebroadcasts the *R_Reply* after removing the signature of preceding node and signing with its own private key. When *R_Reply* reaches the MN's neighbor *A*, *A* validates the signature of preceding node, and then rebroadcasts the packet to MN without signing on it. The detailed message exchange based on Figure 4 is shown below.

1. *FA* receives *R_Request* from *C*:

$[R\_Reply, MN_{HM}, MN_{IPa}, MN_{IPb}, MN_{IPc}, FA_{id}, N_{FA}, t]\ K^{-1}_{FA}$

2. *C* receives the R_Reply form *FA*:

$[[R\_Reply, MN_{HM}, MN_{IPa}, MN_{IPb}, MN_{IPc}, FA_{id}, N_{FA}, t]\ K^{-1}_{FA},]\ K^{-1}_{IPc}$

3. *B* receives the R_Reply form *C*:

$[[R\_Reply, MN_{HM}, MN_{IPa}, MN_{IPb}, MN_{IPc}, FA_{id}, N_{FA}, t]\ K^{-1}_{FA},]\ K^{-1}_{IPb}$

4. *A* receives the *R_Reply* form *B*:

$[R\_Reply, MN_{HM}, MN_{IPa}, MN_{IPb}, MN_{IPc}, FA_{id}, N_{FA}, t]\ K^{-1}_{FA}$

When MN receives *R_Reply* from the neighbor *A*, MN validates the signature of FA. Node *A* does not sign *R_Reply*. It doesn't matter because if any malicious node provides falsified route information, MN can detect the falsification by checking the signature of FA. MN extracts the route from MN to FA from the *R_Reply*. In the above example, $[MN_{HM}, MN_{IPa}, MN_{IPb}, MN_{IPc}, FA_{id}]$ is the route.

After the MN receives a route reply from FA, it can then use the route to send an Agent Solicitation message to

FA. Upon receiving Agent Solicitation message, the FA returns an Agent Advertisement back to the MN with COA. MN selects one of the advertised COA to register with FA.

4.1.2. MN registration with FA and HA

All nodes must register with FA and obtain a certificate from FA before participating in ad hoc routing protocol. After registration, the MN with AODV and other on-demand ad hoc routing protocol maintains its registration only when the global connectivity is required. But all nodes must keep a fresh certificate with FA. To update its certificate before expiration, the MN does not need to register with FA again. The policy of registration in this proposal uses the *minimal public based authentication protocol*, in which HA serves as authentication server. The scheme assumes that a public key infrastructure (PKI) exists for use by HA and FA. Each MN performs cryptographic operation using secret-key ($S_{MN\text{-}HA}$) just like in secret-key based authentication. Each MN and it's HA share a security association to create MAC (Message Authentication Code) for registration request and reply. The basic process of registration is as follows. MN starts a registration request as (R1). The registration request message is signed by MN with the secret key ($S_{MN\text{-}HA}$). Then the registration request is sent to HA via FA appending FA's nonce (R2). HA verifies MN and FA (R3). Then HA returns the registration result back to FA (R4). FA validates the HA (R5). Therefore, FA returns the registration result to MN (R6). Once MN receives a successful reply from HA (R7), it is guaranteed that FA's certificate is valid. The *Minimal public based authentication protocol* [9] operates as follows:

(R1): MN -> FA: M_2, $< M_2 > S_{MN\text{-}HA}$. Where M_2=Registration Request, FA_{id}, HA_{id}, MN_{HM}, MN_{COA}, N_{MN}, N_{HA}, {Message in AA1}

(R2): FA->HA: {Message in R1}, N_{FA}

(R3): HA: (upon receipt of R2):
Validate $< M_2> S_{MN\text{-}HA}$ using $S_{MN\text{-}HA}$
Check whether FA_{id} in AA1 = FA_{id} in M_2
Validate $Cert_{FA}$ based on existing PKI at HA
Validate $[M_1]\, K^{-1}{}_{FA}$ using authenticated K_{FA}
Continue with the steps in [8] (Perkins, Mobile IP support)

(R4): HA->FA: M_3, $[M_3]\, K^{-1}{}_{HA}$, $Cert_{HA}$,
Where $M_3 = M_4$, N_{FA};
M_4= Reply, Result, FA_{id}, HA_{id}, MN_{HM}, N'_{HA}, N_{MN}, $<M_4> S_{MN\text{-}HA}$

(R5): FA: (upon receipt of R4)
Validate N_{FA}
Validate $Cert_{HA}$ based on existing PKI at FA
Validate $[M_3]\, K^{-1}{}_{HA}$ using authenticated K_{HA}
Log this message as the history trace of MN
Continue with the steps in [8] (Perkins, Mobile IP support)

(R6): HA->MN: M_4

(R7): MN (upon receipt of R6):
Validate $< M_4> S_{MN\text{-}HA}$ using $S_{MN\text{-}HA}$
Continue with the steps in [8] (Perkins, Mobile IP support)

FA authenticates MN via HA. MN also authenticates FA at HA by using secret-key ($S_{MN\text{-}HA}$). Therefore if FA is a forged one, message M_4 indicates an error. It is difficult for malicious node to forge HA due to sharing of secret-key ($S_{MN\text{-}HA}$) between MN and HA.

4.2. Global security of Ad hoc Network

4.2.1. Data Structure of Certificates

In general, if a node registers with FA successfully, it is assumed that the node is trusted. Therefore, after the successful registration of a MN, FA is responsible for issuing a certificate for the MN, and updating certificate list at every other node in ad hoc network. Each node maintains a data structure of certificates to keep those issued certificates, which includes home address of the mobile node, public key of the mobile node, issuing and expiring time of the certificate, as MN_{HM}, K_{MN}, T_{MN}, *and* E_{MN} respectively. For example, (R8) and (R9) are two certificate messages for distributing certificates after MN has registered with FA successfully.

(R8): FA->MN: *Certificate*: $[\{MN_{IP}, K_{MN}, T_{MN}, E_{MN}\}, \{MN_{IPa}, K_{IPa}, T_{IPa}, E_{IPa}\}, \{MN_{IPb}, K_{IPb}, T_{IPb}, E_{IPb}\} \ldots \{MN_{IPn}, K_{IPn}, T_{IPn}, E_{IPn}\}]\, K^{-1}{}_{FA}$

(R9): FA->Other Registered Node: *Certificate*, $<MN_{IP}, K_{MN}, T_{MN}, E_{MN}> K^{-1}{}_{FA}$

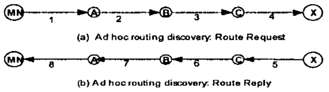
On receiving an ad hoc route discovery message (except for FA discovery) from a neighbor, MN extracts the neighbor's IP address. Then MN tries to find a valid match in the local data structure of certificates by using the extracted IP address. After a match is found, MN checks the signature of the route message by using the neighbor's public key. If the signature is matched, it shows that the neighbor is a certificated node. Otherwise the neighbor with its IP address is invalid, and the received packet must be discarded during the processing of ad hoc route discovery.

4.2.2. Binding mobile IP with ad hoc ID

Depending on ad hoc network protocols, ad hoc networks may use different addressing solutions; AODV, DSR, and TORA use Node ID; HSR has a hierarchical address solution. ZLHS uses <zone id + node id> as the MN's ad hoc address. A detailed survey of the ad hoc protocols can be found in the paper [2]. The ad hoc network with global connectivity must bind the ad hoc hosts' home addresses with their identifiers in ad hoc network. In the registration step (R5), FA records message M_3. This binding and recording make it possible to track the MN's history so that the bad credit MN can be excluded from the ad hoc networks. To do so, we may either have a correlation between the ad hoc host's ad hoc address and its home address or use directly home address as its ad hoc address. The following discussion uses the ad host's home address as its identity in ad hoc network for route discovery.

4.2.2. Ad hoc route discovery

In order to discover a route to a target node in the ad hoc network, a MN follows the steps outlined in Figure 5. If it is the first time for MN to discover the target node as shown in Figure 5, a MN creates a pseudo-random number as a nonce. The target node will return a new nonce for the next route request. Both intermediate nodes and the target node check the local data to prevent duplicates. Each intermediate node or the destination node validates whether the neighbor, from which the packet is received, is a trusted node by validating its certificate and the signature. The validation uses the association between the IP address of the neighbor and its certificate. If in the local table the T_{MN} and E_{MN} of the neighbor are invalid or expired, the received packet will be discarded. Each intermediate node records its reverse route, from which the packet is received, and then signs with its private key before sending a packet out. The ad hoc route discovery has two stages: route request and route reply. Figure 5 illustrates the route discovery with AODV routing protocol. In Figure 5, *A*, *B*, and *C* are intermediate nodes, and *X* is the destination node. Firstly, MN broadcasts *RREQ* marked as *R_Request* with its signature. The *R_Request* includes IP addresses of source and destination node, a nonce, and issue time. The signature of MN to non-mutable fields (MN_{IP}, MN_{IPx}, N_{MN}, *and t)* protects the integrity of non-mutable items of *R_Request*. The signature of intermediate node is to protect mutable field, such as *hop_cnt*, from being modified by a malicious node. After receiving the route discovery at the destination node, the destination node checks the request and replies with *R_Repy*.



(a) Ad hoc routing discovery: Route Request

(b) Ad hoc routing discovery: Route Reply

Figure 5. An example of steps of ad hoc discovery

1) *MN* broadcasts

$[R\_Request, MN_{IP}, MN_{IPx}, N_{MN}, t]\, K^{-1}{}_{MN}$

2) *A* receives *R_Request* from *MN*

$[[R\_Request, MN_{IP}, MN_{IPx}, N_{MN}, t]\, K^{-1}{}_{MN}, hop\_cnt]\, K^{-1}{}_{IPa}$

3) *B* receives *R_Request* from *A*

$[[R\_Request, MN_{IP}, MN_{IPx}, N_{MN}, t]\, K^{-1}{}_{MN}, hop\_cnt]\, K^{-1}{}_{IPb}$

4) *C* receives *R_Request* from *B*

$[[R\_Request, MN_{IP}, MN_{IPx}, N_{MN}, t]\, K^{-1}{}_{MN}, hop\_cnt]\, K^{-1}{}_{IPc}$

5) Target node *X* receives *R_Request* from *C*

$[R\_Reply, MN_{IP}, MN_{IPx}, N_x, t, hop\_cnt]\, K^{-1}{}_{IPx}$

6) *C* receives *R_Reply* from target node *X*

$[[R\_Reply, MN_{IP}, MN_{IPx}, N_x, t, hop\_cnt]\, K^{-1}{}_{IPx}]\, K^{-1}{}_{IPc}$

7) *B* receives *R_Reply* from target node *C*

$[[R\_Reply, MN_{IP}, MN_{IPx}, N_x, t, hop\_cnt]\, K^{-1}{}_{IPx}]\, K^{-1}{}_{IPb}$

8) *A* receives *R_Reply* from *B*

$[[R\_Reply, MN_{IP}, MN_{IPx}, N_x, t, hop\_cnt]\, K^{-1}{}_{IPx}]\, K^{-1}{}_{IPa}$

5. Security analyses and performance

5.1. Security analyses of global connectivity

If a node counterfeits a registration by spoofing an address of a benign node or inventing a non-existent address, its registration will fail at HA while HA validates the secret key of the malicious node. Actually, by trusting HA for authentication, using the strategy of the *minimal public based authentication protocol* ensures that registration is legitimately created, either by FA or MN. It also ensures that the registration has not been modified in transit, and that no old registration message has been replayed. It achieves the goals of preventing the attacks with bogus registration requests; precluding the reply attacks from malicious nodes; obviating the attacks of advertising fraudulent beacons by a counterfeit agent; and averting the attacks using old registration messages by a malicious node. By sharing secret key between MN and HA to calculate MAC, registration messages are protected from being modified. Malicious node could not registers successfully with HA even if masquerading itself with bogus care-of-address because of the shared secret key. Without the other node's secret key, any malicious node could not generate any valid registration control message by spoofing other nodes.

The process of FA discovery establishes a path between FA and MN by using authenticated nodes. It avoids those unregistered malicious nodes to mislead route or drop registration related messages with the intention of hindering MN registration.

5.2. Security analysis of ad hoc networks

Authentication and access control: HA authenticates MN, and FA. FA issues certificates to each MN that is used for authentications of other ad hoc hosts. Before participating in ad hoc routing protocol, MN must register with FA to obtain a certificate from FA. From the view of MN, once a MN receives a successful registration reply from the HA, it is assured that the FA is valid. Meanwhile from the view of ad hoc network, if MN registers with FA successfully, the MN is a trustable host. Furthermore FA issues a certificate to the MN. Therefore, registration with FA plays three main roles here:

1. MN's registration with FA for mobility binding at HA.
2. FA is trusted by MN after FA is authenticated by HA by using a secret key ($S_{MN\text{-}HA}$).
3. Access control in ad hoc network to determine whether the MN can participate in ad hoc routing protocol, which enhances the trust relationships in the ad hoc network.

A node cannot generate a valid route discovery message by spoofing or inventing an IP address. In the process of route discovery, control messages created by a node must be signed and validated by a receiving node. Thus the route discovery prevents anti-authenticating attacks, such as *creating routing loop*, *fabrication* because no node can create and sign a packet in the name of a spoofed or invented node.

Identification: Without any centralized administrative, one of crucial problems in ad hoc network is that it is very easy for MNs to change their identities. It is because of the lack of consistent identities for ad hoc hosts that the histories of ad hoc hosts could not be tracked. But in the proposed approach, when global connectivity is requested, the ad hoc hosts' home address is bound with their identity in ad hoc network. This binding is unique because of the uniqueness of ad hoc host's home IP address. The binding is also associated with ad hoc host's secret key and certificate. Therefore, it becomes difficult for any ad hoc host to masquerade itself by spoofing or creating a valid address.

Non-duplication: Nonce and timestamp.make a route request or reply contain unique data, to battle against the attack of forwarding a duplicated message from a malicious node. The first route request message to a certain destination contains a nonce. A new nonce in the reply message indicates the next nonce in the next request. When an intermediate or target node receives routing control message, the node compares the nonce and originator of the received packet with corresponding data in the local table to avoid duplicate processing. If it has timestamp in the received packet, the received node also makes sure the timestamp is close enough to current estimated time. The time check of timestamp prevents duplication too.

Integrity: Packets in ad hoc network are signed using a private key at each node. Then the receiver verifies the signature and certificate of the sender. It fights again the attacks of anti-integrity, such as the attack of *modification.*

Cooperation: Just like any other ad hoc security protocol, although selfishness is difficult to know, the Internet connectivity provides the backbone for making some policies to encourage the cooperation in ad hoc network, such as setting high priority for global connectivity or giving extra credits for communication to co-operating nodes. In the traditional ad hoc network, because of the absence of a mechanism to identify nodes in ad hoc network, it is easy for selfish node to change its identity to get rid of its bad records, to elude monitoring from other nodes, and furthermore to escape from cooperation. In the proposed approach, the nodes in the ad hoc network with global connectivity can be related to its home address uniquely, to enforce a cooperating solution to solve the selfishness problem.

6..Conclusion

In any ad hoc network application, trustworthiness is a primary challenge that should be met in its open and distributed environment. The proposed approach provides the security for the internet connectivity and the ad hoc networks. Based on this access control mechanism, malicious nodes can be effectively excluded from ad hoc network so that the trust relationship between ad hoc nodes is enhanced for the security of route. Meanwhile it is difficult for malicious node to masquerade a benign FA. The protocol avoids those unregistered malicious nodes to mislead ad hoc routing discovery with the intention of hindering MN's registration. Also each mobile node maintains a fresh certificate table to enforce authentication and integrity in the processing of ad hoc routing to prevent the attacks by using unauthenticated, modified, fabricated or duplicated message.

10. References

[1] Yuan Sun Elizabeth M. Belding-Royer Charles E. Perkins, "Internet Connectivity for Ad Hoc Mobile Networks", International Journal of Wireless Information Networks special issue on Mobile Ad hoc Networks, 9(2), Apr. 2002.

[2] E.M.Royer and C-K Toh "A Review of Current Routing Protocols for \Ad-Hoc Mobile Wireless Networks," IEEE Personal Communication, 1999.

[3] Yih-Chun Hu, David B. Johnson, and Adrian Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks", Proceedings of the 4th IEEE Workshop on Mobile Computing Systems & Applications (WMCSA 2002), pp. 3-13, IEEE, Calicoon, NY, June 2002.

[4] P. Papadimitratos, Z.J. Haas, P. Samar, "The Secure Routing Protocol (SPR) for Ad Hoc Networks", draft-papadimitratos-secure-routing-protocol-00.txt 2002-12-11.

[5] Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Ariade: A Secure On Demand Routing Prottocol for Ad hoc Network", MobiCom 2002, Sept. 23-28, 2002, Atlanta, Georgia, USA.

[6] Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields, Elizabeth M. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Network", In Proceedings of 2002 IEEE International Conference on Network Protocols (ICNP). November 2002.

[7] Whitfield Diffie and Martin Hellman, "New directions in cryptography," IEEE Transaction on information Theory, Vol. IT-22, no. 6, pp. 644-654, Nov. 1976.

[8] C. E. Perkins, "IP Mobility Support for IPV4", Revised. IETF internet Draft, draft-ietf-mobile-rfc2002-bis-08.txt, Sept. 2001.

[9] Sufatrio & Kwok Yan Lam, "Mobile-IP Registration Protocol: A Security Attack and New Secure Minimal Public-key Based Authentication", Proceeding of the 1999 International Symposium on Parallel Architectures, Sept. 1999.