CERIAS Tech Report 2001-56

AN ARCHITECTURE FOR SECURE WIRELESS NETWORKING

by Yi Lu, Bharat Bhargava, Mohamed Hefeeda

Center for Education and Research in
Information Assurance and Security,
Purdue University, West Lafayette, IN 47907

An Architecture for Secure Wireless Networking*

Yi Lu Bharat Bhargava Mohamed Hefeeda
Center of Education and Research in Information Assurance and Security
and
Department of Computer Science
Purdue University
West Lafayette, IN, U.S.A.
{yilu, bb, mhefeeda}@cs.purdue.edu

Abstract

As wireless networks are rapidly deployed, the security of wireless environments will be mandatory. Considering the inherent security limitations of Ad Hoc networks, we propose a new architecture: Hierarchical Hybrid networks for secure wireless networking. In such a network, wireless nodes are organized into groups. We present a secure communication scheme to defend against link attacks. Secure mobility support for mobile hosts roaming among groups is also discussed. Mutual authentication is used to protect both foreign groups and mobile hosts. We propose a fault-tolerant authentication scheme to make systems survivable from agent failures. These security schemes take into account the characteristics of wireless networks.

1. Introduction

Ad Hoc wireless networks provide users with maximum flexibility. In an Ad Hoc network, there is no fixed infrastructure such as base stations or mobile switching centers. Nodes of an ad-hoc network are mobile hosts with similar transmission power and computation capabilities. Mobile hosts that are within each other's radio range communicate directly through wireless links. Otherwise, they communicate through multi-hop routing (intermediate mobile hosts forward packets as internal routers). Ad Hoc networks play important roles in environments where wireless access to a wired backbone is either inefficient or impossible. Its applications include national security operations, rescue missions, and military communications.

Although most applications are highly sensitive, Ad Hoc networks lack security. Achieving security in an Ad Hoc network is challenging because of the following reasons: the use of wireless links, which are susceptible to link attacks; roaming of mobile hosts in a hostile environment with relatively poor physical protection; the frequent changes in network topologies and memberships [7].

Many researchers are working on the security of wireless networks. Secure protocols have been proposed for IEEE 802.11 PCF (Point Coordination Function) [9]. Secure routing algorithms are being studied to defend against both external and internal malicious attacks [7]. We think the lack of security is an inherent weakness of Ad Hoc networks. To provide flexible connectivity, an Ad Hoc network is set up and maintained dynamically based on the geographical information of mobile hosts. The consequence is that *any* two nodes in a network can set up a wireless link between them if they are physically close enough. If secure communication is required, a mobile host must have the ability to identify any node before establishing a link with it. The following mechanisms are usually used for identification, but all of them have deficiencies in Ad Hoc networks.

- All nodes in a system share a secret key so that a node can prove its membership by showing the knowledge of this secret key. This scheme is relatively insecure. If one node is compromised, the whole system is compromised.
- Every node knows the public keys of all other nodes so that it can prove the identity of a node by using public-key cryptography. This requires that all nodes to be known before the network is set up. If a node wants to change its public/private key pair, it has to inform all other nodes in the system. This scheme is not scalable.
- There is a trusted entity called *Certificate Authority (CA)*, which knows the public key of every node. All nodes know the CA's public key. Two nodes can use some authentication protocol, such as Yahalom, DASS, Woo-Lam, etc.[3], to identify each other without prior knowledge of each other's public key.

*This research is supported by CERIAS, NSF grants CCR-9901712 and CCR-0001788, and DARPA grant F3361501C1902. This paper is published in IEEE workshop on "Reliable and Secure Application in Mobile Environment", New Orleans, Oct. 2001.

In this scheme, CA is the bottleneck of a system. If CA is compromised, the whole system is compromised.

- Utilizing distributed CA to remove the bottleneck and applying threshold cryptography to defend against comprised nodes [7]. This is an active research area. Some research questions, such as how to distribute CA, how to duplicate keys, and how to maintain keys' consistency, are still open.

The objective of our research is to build a secure and survivable wireless network. We realize that the Ad Hoc architecture of wireless networks is the main barrier to security. We designed a new architecture for secure wireless networking.

The rest of the paper is organized as follows. Section 2 introduces the proposed architecture. Section 3 presents schemes for secure communication. Secure mobility support is discussed in section 4, along with the authentication protocol and the fault-tolerant authentication scheme. A prototype and on-going experiments are presented in section 5. Section 6 summaries the paper.

2. Hierarchical hybrid networks

In a previous work, we proposed the Hierarchical Hybrid (HH) architecture as an infrastructure for wireless networking [10]. The HH architecture provides more security for the wireless environments, as we describe in the following sections.

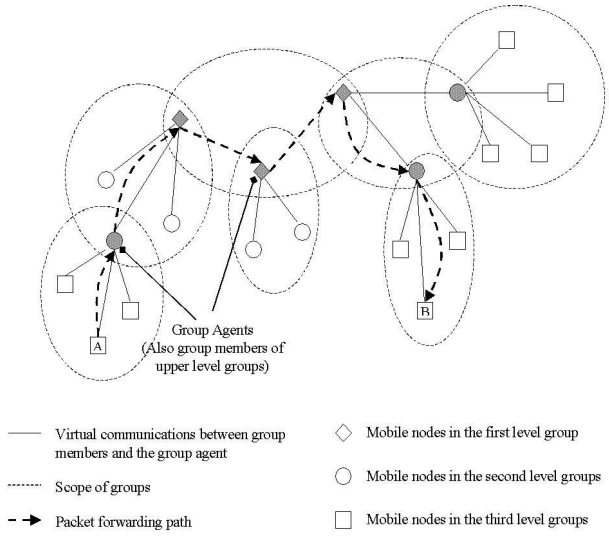

Figure 1. Hierarchical Hybrid (HH) network

In a HH network, all mobile nodes are partitioned into groups. Each group has a *group agent* and some *group members*. A group agent itself can be a group member of a higher level group. If we conceive the links between the group agent and the other members in the same group, the network looks like a forest as shown in Figure 1. Mobile nodes in the same dotted circle are considered in the same group. The group agents are distinguished by the dark color. The shape of a mobile node indicates the level of the group to which it belongs.

Two mobile nodes that belong to the same group may communicate directly via wireless link if they are within each other's radio range. Otherwise, other group members (including the group agent) in the same group act as internal routers to forward packets for them. Packets sent to a mobile node in another group must go through the group agent. Hence, group agents can enforce security policies on incoming/outgoing packets. Figure 1 also shows how a packet is sent from a mobile node A to another mobile node B.

3. Secure communications in HH networks

There are many kinds of link attacks to a network system, especially a wireless network system, such as eavesdropping, impersonating, and message distortion. Eavesdropping may enable an adversary to access secret information. Impersonating may give an adversary specific privileges that are supposed to be granted to others. Message distortion may cause the whole system to behave abnormally, even crash. Many protocols have been developed to defend against link attacks. The essential idea is to apply authentication and encryption.

Wireless networks are more vulnerable to link attacks than wired networks. The characteristics of wireless networks must be considered when designing a secure communication scheme.

3.1. Characteristics of wireless networks

The following characteristics of wireless networks are pertinent to the design of security protocols.

Use of wireless medium: Radio channels are open in the air. Everyone can send messages to or receive messages from a channel. Cryptographic techniques shall be applied to ensure that sensitive information is never disclosed to unauthorized entities. Security schemes must also provide some mechanisms to identify senders.

Weak power supplies: Since nodes in wireless networks are usually powered by lightweight batteries, reducing power consumption is an important consideration. Thus, security schemes shall use less complex computations.

Limited bandwidth: The limited ISM frequency band allocated by the FCC and the requirement to use spread spectrum communication limit the data rate. For example, in IEEE 802.11 standard, the data rate is up to 2 Mbps. This characteristic requires security schemes to minimize the number of messages exchanged over the wireless medium.

These characteristics are taken into account in the proposed security schemes.

3.2. Secure communications among group members

Secure communication is significant in a network system. It prevents sensitive information from unauthorized access. Currently proposed security mechanisms employ symmetric (private key) systems and/or asymmetric (public key) systems. The proposed security scheme utilizes both symmetric and asymmetric cryptographic techniques. It consists of two parts. The first part is for authentication and key distribution and the second part is for secure message forwarding.

In a HH network, each group has a unique ID and all members of a group share the same secret key (a private key in a symmetric system). This secret key is maintained by the group agent. Whenever a new member joins the group, it authenticates itself to the group agent and gets the secret key. To improve security, a group agent shall update the secret key periodically. Two mobile hosts in the same group use the secret key to establish a secure link and encrypt/decrypt messages exchanged between them. An adversary may capture the traffic among a group; however, it cannot know the information without the knowledge of the secret key.

Each node in a HH network has a public/private key pair. Every group member knows the public key of the group agent. Each group agent maintains a potential member list, which contains the public keys of mobile nodes that might be a member of that group.

We present a number of notations used in the remaining part of the paper.

- X, Y: mobile nodes,
- G: group agent,
- gid: group ID,
- K: secret key,
- K_X: public key of node X,
- M: message,
- $E_X(M)$: encrypting message M with node X's public key so that only X can read M,
- $S_X(M)$: signing message M with X's private key so that every node that knows X's public key can verify that M is signed by X,
- $E_K(M)$: encrypting message M with secret key K,
- $D_K(M)$: decrypting message M with secret key K.

The following authentication and key distribution protocol is invoked when node X joins a group whose ID is "gid".

Step 1 (X→G): X generates a "join group" request R, it signs the request and broadcasts a message containing: $\langle gid, X, R, S_X(gid, X, R)\rangle$.
Step 2 (G): If G receives $\langle gid, X, R, S_X(gid, X, R)\rangle$ and it is the agent of group "gid", it checks the potential member list to make sure that X is a member of the group. Then, it uses X's public key to verify that the request is actually initiated by X.
Step 3 (G→X): G sends a message containing: $\langle gid, G, X, E_X(gid, G, X, K, S_G(gid, G, X, K))\rangle$ to X.
Step 4 (X): X uses its private key to decrypt the message and get the secret key K; it will verify G's signature with G's public key to make sure that K is actually sent by G.

This protocol is immunized to the "replay" attack. Although an adversary can capture the signed request initiated by X in step 1 and later impersonates X by broadcasting the same request, it cannot get the secret key K in step 4 because it does not know X's private key.

In the above protocol, each group agent has to maintain a potential member list for authentication purpose. It is neither efficient nor expendable. The potential member list could be unnecessarily large although there might be only a few members in a group. When the structure of the network changes, for example, a node may no longer be a member of a certain group, the potential member list must be changed in advance. However, the protocol can be improved by applying certificates.

We assume there is a certificate authority (CA) within or outside the wireless system. For example, if the wireless network is a military system, the CA could be the commander in chief. The CA can issue certificates that have the following format:

$S_{CA}(gid, X, \text{public key of } X, \text{expiration date})$.

The above statement signed by the CA states that X *can* join the group whose ID is "gid" before the expiration date. All nodes know the public key of the CA so that everyone can verify the statement.

The first two steps of the proposed protocol thus will be modified as follows.

Step 1 (X→G): X broadcasts a "join group" request with the certificate $\langle gid, X, S_{CA}(gid, X, \text{public key of } X, \text{expiration date})\rangle$.
Step 2 (G): If G receives the request and it is the agent of the group "gid", it verifies the signature of the CA and checks the group ID and the expiration date of the certificate, then it gets the public key of X from the certificate.

A comparison between the proposed protocol and other wireless security schemes is summarized in Table 1.

Once X gets K, it uses it to set up secure communications with other group members. The pseudo-

code in Algorithm 1 shows how X handles (sends, receives, and forwards) packets after joining the group.

Table 1. Comparison with other wireless security schemes

	Proposed Protocol	PCF Security Protocol [9]	Aziz and Diffie [1]
# of expensive computations	3[1]	3	4
Authentication in first phase	YES[2]	YES	NO
Privacy of Nonce	N/A	YES	NO

Sending a packet *P*:

X uses K to encrypt the header and the body of P before sending it.

Receiving a packet *P*:

X decrypts and checks the header.
IF *X is the destination*
THEN *it decrypts the body.*
ELSE
X makes any necessary modifications to the header and
IF *X is a group agent* AND *P is sent from one group to another*
THEN *X encrypts the header with the destination group's key K' and decrypts the body with K then encrypts it again with K'.*
ELSE
X encrypts the header again with K.
X forwards P to the next hop.

Algorithm 1. Secure communication

In addition to the body of a packet, the header is encrypted when the packet is being forwarded. Although encrypting headers introduces a little overhead, it provides protection to systems in two ways.

1. The correctly encrypted header testifies that the packet is sent by a member of the group. Adversaries cannot produce such a header because they do not know the secret key.
2. The encrypted header ensures that routing and location information, which is valuable to attackers, will not be disclosed. For example, if an adversary captures a packet and knows the next hop is node X, he can tell that X is within the radio range of the sender.

[1] The signature used in step 1 can be computed in advance.
[2] The first phase consists of step 1 and 2.

In a HH network, a group usually consists of about 10 members. If a mobile host is compromised, only members of the same group will suffer, the rest of the system is still secure. Additionally, a new secret key can be reissued quickly to eliminate to the effects caused by the compromised member.

3.3. Secure communications between two hosts

The above scheme for secure communications only guarantees that intruders outside the group are not able to access information exchanged among group members. However, there is no secret to the members in the same group. We do not prefer to set up secure communications between any two hosts due to the following considerations.

Cost: Before setting up a secure communication, two hosts must authenticate each other. Private-key based authentication techniques are not suitable in this case, because the two hosts may not be in the same group (share the secret key). Public-key cryptographic techniques are proved very slow. Therefore, the cost is high.

Necessity: Although some communications require a high level of security, most of them are not sensitive to group members. For instance, routing information packets should be visible to all group members.

If two hosts need to establish secure communication, Deffie-Helmman [3] protocol can be used to generate the secret key. Moreover, if both hosts hold a certificate discussed in section 3.2, a random-nonce based mutual challenge-response protocol can be employed to exchange the secret key.

4. Secure mobility support

A mobile system allows mobile nodes to roam within the network, and nodes' roaming is transparent to the upper level protocols such as TCP. Mobile IP [5] is the most widely used protocol to achieve network mobility in wired environments. When a mobile host travels to a foreign subnet of the system, it will be assigned a "care of address", which is its temporary IP address in this subnet, by the foreign agent. Then a "tunnel" will be set up between its Home Agent and the "care of address". All the IP packets destined to the mobile host are captured by the home agent and transmitted to the "care of address". Mobile IP provides some sort of security to protect both the home and the foreign subnets. It requires the mobile host to authenticate itself to the home agent before the tunnel can be set. However, Mobile IP is not an ideal solution for wireless networks, because the tunnel will consume unnecessary bandwidth. It is a big issue in wireless networks since bandwidth is so limited.

In Ad Hoc networks, dynamic routing algorithms are used to provide mobility support, such as Destination-

Sequenced Distance-Vector (DSDV) routing [4], zone routing [11], etc. When a dynamic routing algorithm is used, the location of a mobile host must be identified before a connection can be established. The routing algorithm shall be able to update the routing paths correspondingly when a mobile host moves to a new point of the system, so that the packets destined to this host can be delivered correctly. If security is desired, routing algorithms need to authenticate mobile nodes before updating routing paths. It is infeasible in wireless environments because authentication requires expensive computations and routing paths are updated frequently.

Our approach for supporting mobility in HH networks is a combination of these two schemes.

We use the following notations in the mobility support protocol.

Home Group (HG): Each mobile host has a HG, the group of which the mobile host is a permanent member.

Foreign Group (FG): A FG to a mobile host X is a group that is not X's HG.

Home Group Agent (HGA): The group agent of the HG.

Foreign Group Agent (FGA): The group agent of a FG.

Current Group (CG): CG is the group through which the mobile host connects to the system currently. It is either the HG or a FG of the mobile host.

Current Group Agent (CGA): The agent of the CG.

When the connection (not necessarily a direct connection) between a mobile host and its CGA is no longer available, it is considered as homeless. Because a mobile host cannot set up a secure link with nodes in other groups, mobility support must be provided to keep the host connected with the system. We propose a secure mobility support scheme for mobile hosts roaming around.

4.1. Mobility support algorithm

The following pseudo-code shows the sketch of the secure mobility support algorithm.

Mobile host:

IF *homeless*
  THEN *broadcast a "join a group temporarily" request.*
    IF *a response from a FGA is received*
      THEN *invoke the authentication process with that agent.*
        IF *authenticated*
          THEN *change the group ID and the shared key along with the CG and CGA.*

Group agent:

IF *a "join temporarily" request is received*
  THEN IF *the security policy allows hosting*
    THEN *send a response to the mobile host.*
      invoke the authentication process.
      IF *authentication succeeds*
        THEN *issue a new shared key and distribute it to the current group members.*
          Send the group information (gid, key) to the mobile host.

Algorithm 2. Mobility support

Because HH networks use dynamic routing algorithms, there is no need to set up a "tunnel" between the HGA and the mobile host. The routing algorithm will identify the new location of the mobile host and change the corresponding routing paths.

4.2. Authentication protocol

Mutual authentication is the key to ensure security in the above mobility support algorithm. We propose a mutual authentication protocol for a mobile host and a FGA with the aid of the HGA. We assume that all the group agents know each other's public keys. A timestamp T is used to guarantee the freshness of the request.

Step 1 (X→FGA): X generates a request R and a fresh timestamp T and sends $<X, FGA, HGA, R, T, S_X(X, FGA, HGA, R, T)>$ to FGA;
Step 2 (FGA→HGA): FGA gets HGA address from the request and forwards $<X, FGA, HGA, R, T, S_X(X, FGA, HGA, R, T)>$ to HGA;
Step 3 (HGA→FGA): HGA checks if X is a valid member, then sends $S_{HGA}(X, K_X, T)$ and $S_{HGA}(FGA, K_{FGA}, T)$ to FGA;
Step 4 (FGA→X): FGA sends $S_{HGA}(FGA, K_{FGA}, T)$ and $E_X(FGA, X, T, K, S_{FGA}(FGA, X, T, K)$ to X;

Through this protocol, X and FGA can get each other's public key, which is signed by the HGA. FGA can verify that the request is initiated by X by using X's public key. The fourth step ensures that only X can get K. X must verify that K is generated by FGA by using FGA's public key.

4.3. Fault-tolerant authentication

In a HH network, group agents are also moving. When the above authentication process is taking place, the HGA of X may be temporarily or permanently unavailable because of movement or failure. In this case, X's request for the temporary membership in the foreign group will be denied. Mobile hosts will be detached from the system if their HGA is no longer available. To make HH

networks survivable from such kind of unavailability, we proposed a fault-tolerant authentication scheme [1].

Mobile nodes are organized in a multi-level hierarchy in a HH network. A group agent itself may be a member of a higher level group and has its own HGA, unless it's the root of the hierarchy. We define mobile node X's *Intention Agent* (IA) in a recursive way:

Mobile node Y is X's IA if and only if Y is the HGA of X' HGA or Y is the HGA of one of X's IAs.

In the proposed fault-tolerant scheme, not only its HGA, but also all its IAs know the public key of a mobile node. A mobile node also knows all its IAs' public keys. Each IA has a priority based on several factors [6]. When the above authentication protocol fails due to the unavailability of the HGA, the mobile node will choose the IA with the highest priority and retry the authentication protocol until it is authenticated or no IA is available.

5. Prototype and experiments

We have implemented a prototype of HH networks using **ns2** (Network Simulator) [8]. We are conducting a series of experiments to study this type of wireless networks. Our agenda includes the following:

- Experiments to compare the throughput of HH networks and the corresponding Ad Hoc networks with the number of mobile nodes as the input parameter.
- Experiments to study how long it will take to set up a secure link and how long the link exists. We take the number of mobile nodes and the moving speed as input parameters.
- Experiments to study the fault-tolerant authentication scheme. We will evaluate the number of messages exchanged in the authentication process, the time it takes to authenticate a mobile node. We take the number of levels in the hierarchy and the probability that an agent is unavailable as input parameters.

6. Conclusion

In this paper, we present a new architecture *Hierarchical Hybrid networks* for secure wireless networking. We discuss the characteristics of wireless networks and their impact on the design of security protocols. Security schemes are proposed to protect communications among group members from various link attacks and support mobile hosts to roam around the system. These security schemes utilize encryption/decryption and public-key based authentication techniques. In the secure mobility support scheme, a mobile host will be detached from the system if its HGA fails. We introduce a fault-tolerant authentication scheme to make the system survivable from agent failures.

7. Reference

[1] A. Aziz and W. Diffie, Privacy and Authentication for Wireless Local Area Networks. In *IEEE Personal Communications, First Quarter*, 1994, pp 25-31.

[2] B. Bhargava, S. Kamisetty, and S. Madria, Fault-tolerant Authentication in Mobile Computing. In *Proc. of Intl. Conf. on Internet Computing (IC'2000)*, Jun. 2000, pp 176-185.

[3] B. Schneier, *Applied Cryptography*, John Wiley & Sons, Inc. 1996.

[4] C. E. Perkins and P. Bhagwat, Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers. In *Proc. of the SIGCOMM'94 Conf. on Communications Architectures, Protocols and Applications*, Aug. 1994, pp 234-244.

[5] C. Perkins, IP mobility support. *RFC 2002*, Oct. 1996.

[6] D. McClure and B. Bhargava, On Assigning Priorities of Keying Parameters in a Secure Mobile Network. Tech Report, CS department, Purdue University, 2001.

[7] L. Zhou and Z. J. Haas, Securing Ad Hoc Networks. In *IEEE Network Magazine, Vol. 13, No. 6*, Dec. 1999.

[8] Network Simulator: http://www.isi.edu/nsnam/ns/.

[9] S. H. Park, A. Ganz, and Z. Ganz, Security protocol for IEEE 802.11 wireless local area network. In *Mobile Network Application, Vol. 3, No. 3*, Sep. 1998, pp 237-246.

[10] Y. Lu and B. Bhargava, Achieving Flexibility and Scalability: A New Architecture for Wireless Network. In *Proc. of Intl. Conf. on Internet Computing (IC'2001)*, Jun. 2001, pp 1105-1111.

[11] Z. J. Haas and M.Perlman, The performance of query control schemes for zone routing protocol. In *SIGCOMM'98*, Jun. 1998.