PAPER *IEICE/IEEE Joint Special Issue on Assurance Systems and Networks*

Secure Wireless Network with Movable Base Stations*

Yi LU[†a)], **Bharat BHARGAVA**[†], **Weichao WANG**[†], **Yuhui ZHONG**[†],
and* Xiaoxin WU**[†], ***Nonmembers

SUMMARY Security, flexibility, and scalability are critical to the success of wireless communications. Wireless networks with movable base stations combine the advantages of mobile ad hoc networks and wireless LAN to achieve these goals. Hierarchical mobile wireless network (HMWN) is proposed for supporting movable base stations. In such a system, mobile hosts are organized into hierarchical groups. The group agents serve as a distributed trust entity. A secure packet forwarding algorithm and an authentication and key exchange protocol are developed to protect the network infrastructure. A roaming support mechanism and the associated mutual authentication protocol are proposed to secure the foreign group and the mobile host when it roams within the network. The computation overhead of secure packet forwarding and roaming support algorithms is studied via experiments. The results demonstrate that these two security mechanisms only require, respectively, less than 2% and 0.2% to 5% CPU time in a low-end 700 MHz PC.

key words: *wireless network, movable base station, secure communication, mobility*

1. Introduction

1.1 Wireless Network with Movable Base Stations

Wireless communication technology is significant in networking infrastructure. Mobile ad hoc networks and wireless LAN are two typical packet-switching wireless networks**.

A mobile ad hoc network consists of mobile hosts that communicate with each other over multi-hop wireless links in a collaborative way [1]. There is no fixed infrastructure or stationary base station to coordinate communications. These characteristics provide users with maximum flexibility, at the cost of limitations on scalability. The scalability problem is analytically studied in [2]. The result shows that even the most scalable routing protocol introduces a total overhead of $O(N^{1.5})$, where N is the number of hosts. The experimental study also shows that the increase of the number of hosts is the dominant cause for performance degradation [3].

In a wireless LAN, stationary sites (i.e., base stations) provide high-speed network connections for mobile hosts. For instance, IEEE 802.11a supports up to 54 Mbit/s communication capacity [4]. The fixed infrastructure makes it easy to manage the network, to enforce security policies, and to extend the system. It, however, limits the deployment of the network in environments where wireless access to a wired backbone is either inefficient or impossible. For tactical military networks, the fixed base stations are attractive targets, therefore, highly vulnerable.

Most limitations of wireless LAN, such as inflexibility and vulnerability, can be eliminated by letting base stations move. We deviate from the conventional wireless networks and propose *wireless network with movable base stations* (WNMBS). WNMBS is comprised of mobile hosts and *movable base stations*. The movable base stations typically are mounted on vehicles such as tanks and trucks and form a mobile backbone. They have more resources than mobile hosts in terms of memory, computation capability, transmission power, energy supply, etc. Neighboring base stations use wireless links to communicate. Because all base stations and mobile hosts are moving, the location of a node is not determinable by its network address. The traditional network architecture and routing protocols for wireless LAN are not suitable in this circumstance. We develop *hierarchical mobile wireless network* (HMWN) to support WNMBS. The details of HMWN, including the network maintenance mechanism, the routing protocol, and control overhead, are presented in [5].

1.2 Security Issues in WNMBS

Achieving security in a wireless network is challenging because of:

- The use of wireless channels that are susceptible to link attacks;

Manuscript received March 23, 2003.
Manuscript revised May 19, 2003.

[†]The authors are with the Center for Education and Research in Information Assurance and Security, Department of Computer Sciences, Purdue University, West Lafayette, IN 47907, U.S.A.

a) E-mail: yilu@cs.purdue.edu

*This research is supported by CERIAS security center, NSF grants IIS-0209059 and ANI-0219110, and CISCO URP.

**Sensor network is a new class of wireless networks that has become an attractive research area. A sensor network is essentially an ad hoc network that consists of a large number of tiny disposable and low-power devices. These devices are immobile, or have low mobility as compared with hosts in mobile ad hoc networks.

- Roaming in a hostile environment with relatively poor physical protection that makes a mobile host vulnerable;
- Dynamic network topology and memberships.

Secure protocols have been proposed for protecting a single wireless link, such as the one integrated with IEEE 802.11 [6]. Zhou and Haas [7], Awerbuch et al. [8], and Zapata and Asokan [9] investigate the use of cryptography to secure ad hoc routing protocols. These research efforts require mobile hosts to be able to identify each other based on some priori knowledge. The following mechanisms are usually used for identification. They have deficiencies when being applied to wireless networks.

- All hosts share a secret key so that everyone can prove its membership by showing the knowledge of this secret key. This scheme is relatively insecure. If one host is compromised, the whole system is compromised.
- Every host knows the public keys of all other hosts so that it can identify a host by using public-key cryptography. This scheme is not scalable. It requires all hosts to be known before the network is set up. If a host wants to change its public/private key pair, it has to inform all others in the system.
- There exists a centralized trusted entity, such as a key distribution center (KDC) or a trusted third party (TTP), which knows the public key of every host. Two hosts can use some authentication protocol, such as Yahalom, DASS, Woo-Lam, etc. [10], to authenticate each other. In this scheme, the centralized entity is the bottleneck of a system that will decrease the effectiveness of security solutions. It is prone to DoS attack and may become the single point of failure.

In a WNMBS, the mobile backbone (i.e., base stations) is typically maintained by system administrators (e.g., service providers) and provides network services to mobile users. The base stations, with appropriate security enhancements, form naturally a distributed trusted entity that is capable of balancing service load and tolerating site failures. To utilize movable base stations as a distributed trusted entity, research questions, such as how to organize base stations, how to distribute keys, and how to authenticate mobile hosts, need investigation.

We present mechanisms integrated with HMWN to secure WNMBS. The protection of network infrastructure, authentication and key distribution, and secure roaming support are addressed. The rest of the paper is organized as follows. Section 2 introduces HMWN. An example and four basic operations are presented. Secure packet forwarding mechanism that protects the network infrastructure is proposed in Sect. 3. Section 4 presents the authentication protocol. Section 5 discusses the secure roaming support. The computation overhead of the security mechanisms is numerically investigated in Sect. 6. Section 7 concludes the paper.

2. Hierarchical Mobile Wireless Network

2.1 Overview

To support WNMBS, we propose *hierarchical mobile wireless networks* (HMWN). In a HMWN, mobile hosts are partitioned into groups. Each group can be viewed as an ad hoc network. It consists of some members and a group agent that may be a member of another group. The group agent is the representative of a group. The agent-member relationship forms a hierarchy. A group agent (i.e., a movable base station) acts as a gateway that connects these two groups. Mobile hosts belonging to the same group rely on multi-hop routing to communicate with each other. Communication with a host outside the group is accomplished by the segmented membership-based group routing (SMGR) protocol presented in [5].

Figure 1 is the planform of a HMWN system. Every small square represents a mobile host and the dark ones are group agents. A solid line between two mobile hosts represents a wireless link. The dashed circles represent groups. Figure 2 shows a hierarchical representation of the network. The root group (level 0 group) only contains three members {A, B, C}, where A is the agent. There are two level 1 groups, {B, D, E} and {C, F, G}. B and C are group agents, respectively. D, E, F, and G are agents for level 2 groups.

A HMWN may be a heterogeneous wireless network, in which each group is an autonomous system. For instance, in Fig. 2, the level 1 and level 2 groups may be IEEE 802.11b wireless networks while the level 0 group is a satellite network. Based on various security requirements and available system resources, individual groups may enforce different security policies, such as encryption/decryption algorithm, key length, whether roaming is allowed, etc.

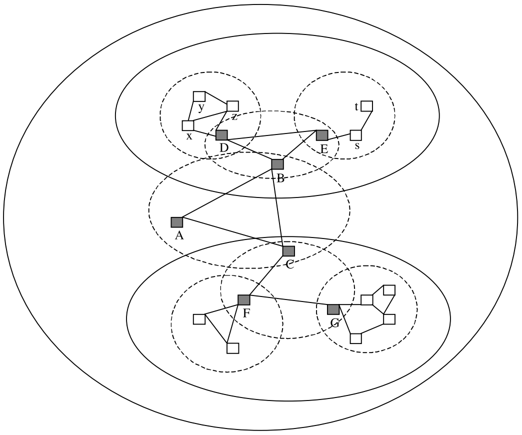


Fig. 1 Hierarchical mobile wireless network.

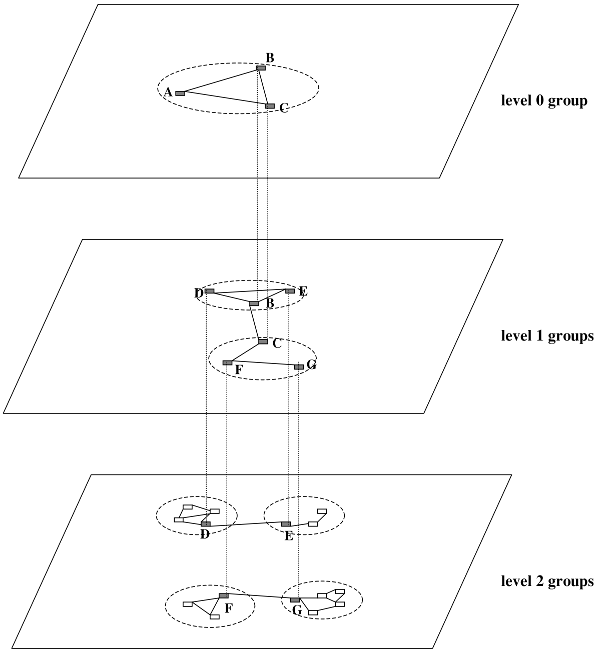


Fig. 2 Hierarchy of groups.

2.2 Basic Operations

The following definitions are used in the rest of this paper.

- Home group (HG) is where the mobile host registers its static membership. Its group agent is called home group agent (HGA).
- Foreign group (FG) is a group other than the HG. Its group agent is foreign group agent (FGA).
- Current group (CG) is the group where the mobile host is currently attached. The corresponding group agent is current group agent (CGA).

Four basic operations are defined for setting up and maintaining a HMWN system.

1) Grouping is the operation used to set up the static membership in a HMWN system. It assigns HG for every mobile host and is only performed at the bootstrapping phase. "Grouping" is accomplished in two steps. The first is to organize mobile hosts into groups (i.e., assign HG for each mobile host). The second is to determine group agents (HGA). The criteria for "Grouping" include the movement of a mobile host, the organization to which it belongs, the wireless MAC protocol that it supports, and the capacity of a mobile host. This operation can be done in two ways. In a WNMBS, only base stations can be chosen as group agents.

1. Mobile hosts may autonomously organize themselves into groups and supergroups in a distributed fashion. It is also suitable for self-organizing ad hoc networks, in which mobile hosts have no prior knowledge about the network.
2. A trusted authority may take charge of the operation. Every mobile host reports its information to the authority. The authority employs some global optimization algorithm to establish the hierarchy and distributes the result to all participated hosts.

Unlike "Grouping" that only determines the static membership, the operations of "Registration," "Leaving," and "Migration" maintain the dynamic membership and topology of the network (e.g., CG for a mobile host).

2) Registration is the operation that a mobile host must complete before it can connect to the network. Registration takes place between a mobile host MH and its HGA. One-hop registration is recommended to reduce the possibility of denial-of-service and man-in-the-middle attacks.

If connectivity rather than security is preferred, remote registration (i.e., MH registers itself to the HGA via intermediate hosts) will be allowed.

3) Migration operation is initiated by a mobile host that decides to leave its current group and join a foreign group. It occurs when a host MH realizes that the CGA is no longer reachable. MH starts this operation by sending out a "Migration" request. Foreign agents that are in the neighborhood reply this request based the security policy that determines whether or not providing migration support, MAC protocol compatibility and capacity. MH chooses the FGA whose reply comes first, set it to be the CGA, and invokes the hand-off procedure. Every agent that replies the request will start a timer. When the timer expires, the agent will cancel the operation.

In the remaining of this paper, we also refer "Registration" as "join a group," and "Migration" as "roaming."

4) Leaving operation is completed by group agents. It may be triggered by two events.

- When a mobile host MH decides to leave the network, it sends a "leave group" message to its CGA.
- When the agent finds out that the route to a mobile host MH is broken, it starts a Leaving Timer. If a route to MH cannot be reestablished or a "Migration" message has not been received before the timer expires, the agent starts the "Leaving" operation.

After the CGA of MH updates the membership information, it will forward the "leave group" message to its own CGA.

2.3 Security Objective and Assumptions

We focus on protecting the network infrastructure against both passive and active attacks, such as insertion, modification or replay of control messages, and traffic analysis. Although it is important to protect end-to-end data communications from unauthorized access, we do not address this problem due to space limit. As long as the network infrastructure is available and secure, the two ends of a communication can always set up a symmetric secret key by using some key-exchange algorithm such as Diffie-Hellman or COMSET [10]. The data packets can be encrypted by using the secret key to ensure confidentiality and integrity.

The objective is achieved by deploying secure packet forwarding and authentication protocols that are presented in the following sections. These security mechanisms are based upon the following assumptions:

- The wireless communication is robust with respect to attacks against the physical layer. These layers are well protected by lower-layer mechanisms, such as anti-jamming techniques [11], [12].
- The underlying cryptography primitives, such as digital signature and encryption, are practically secure (i.e., they are unbreakable with current computation power).
- All base stations know each other's public key (For instance, if each group has 50 members, a 5000-node networks requires about 100 base stations to maintain about 150 public keys, instead of 5000 nodes, most of which are resource-poor mobile hosts, to maintain 5000 public keys.).

3. Protection of Network Infrastructure

Unlike a wired network where the infrastructure is protected by physically securing the cables, the infrastructure of a wireless network is protected by ensuring that every mobile host has correct knowledge about the current network topology and the memberships. A mobile host obtains this knowledge by securely exchanging control information, such as neighbors, routes, etc., with other trustworthy hosts. An adversary should not be able to eavesdrop, insert, or modify the information. It is guaranteed by using unforgeable encryptions.

In addition to routing and control messages, packet headers need to be encrypted. Although encryption hides the content of a message, the packet header that contains the source, the destination, and the next hop will expose the relationships among the involved hosts. This is a reason why eavesdropping technology such as Carnivore is useful even in the presence of unbreakable communication [13]. Preferred targets can be identified in this way and attacks can be concentrated on the nerve centers. Encrypting packet headers will effectively obfuscate relationships among hosts.

3.1 Packet Forwarding Algorithm

We assume that each mobile host in a HMWN system has a public/private key pair and group members know the public key of the group agent. Each group agent maintains a potential member list (defined by "Grouping" operation), which contains the public keys of mobile hosts that might be a member of that group.

Algorithm 1 Secure packet forwarding.

```
Part I: sending a packet P:

X uses K to encrypt the header
if P is a routing or control packet
    it uses K to encrypt the body of P
X transmits encrypted packet P

Part II: receiving a packet P:

X decrypts and checks the header
if X itself is the destination and P is a control packet
    it decrypts the body
else
    X makes any necessary modifications to the header
    if X is a group agent AND P is sent from one group to another
        it encrypts the header with the destination group's key K'
        if P is a routing or control packet
            it decrypts the body with K and re-encrypts it with K'
    else
        X encrypts the header with K
    X forwards P to the next hop
```

We propose the secure packet forwarding algorithm for the protection of the network infrastructure. To use a symmetric cipher, each group has a group-shared secret key. This key is maintained and distributed by the group agent. It is renewed periodically, when a mobile host joins or leaves the group, or at the time a compromised host is discovered.

When a mobile host X registers to a group, it authenticates itself with the group agent and gets the group shared key K by invoking the protocol presented in Sect. 4. X uses K to communicate with other group members confidentially. A group agent may know two groups' shared keys.

The pseudo-code in Algorithm 1 shows how X handles (sends, receives, and forwards) packets after joining the group. This algorithm integrates with the routing protocol to realize secure packet forwarding.

Encrypting and checking headers when sending, receiving, or forwarding packets serve the following purposes.

1. The correctly encrypted header testifies that a packet is sent by a member of the group. Adversaries cannot produce such a header because they do not know the secret key. It prevents the network from being flooded with false control and data packets generated by malicious hosts.
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 host X, he can tell that X is within the radio range of the sender and initiates attacks against X.

4. Authentication and Key Exchange

The capability of a mobile host to authenticate itself and obtain the group-shared key is the basis of secure packet forwarding. In this section, we discuss the authentication and key exchange protocol.

4.1 Notations and Protocol

We introduce the following notations.

- X, Y: mobile hosts
- G: group agent
- gid: group ID
- R: request. It could be a request for joining a group or a request for secure roaming support.
- T: time stamp
- K: shared secret key
- K_X: public key of host X
- M: message
- E_X(M): encrypting message M with host 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 host that knows X's public key can verify that M is signed by X
- V_X(M): verifying message M with X's public key
- E_K(M): encrypting message M with secret key K
- D_K(M): decrypting message M with secret key K

Protocol 1 illustrates the process invoked by the "Registration" operation when host X joins a group whose ID is "gid." This protocol does not use a time stamp to guarantee the freshness of the request because a mobile host only registers once in the network. The agent can tell if the request is new by examining the membership information it maintains.

The correctness of Protocol 1 can be proven by adopting the logic of authentication [14].

4.2 Security Discussion

A security protocol should be robust against malicious attacks. Protocol 1 is immunized to the "man-in-the-middle" attack. An adversary can not modify the request or response because of the use of asymmetric cryptography. The "replay" attack will not work either since this protocol is invoked only once for each mobile host. Both X and G are capable of telling whether the request is brand new with respect to X.

Protocol 1 Authentication and key exchange.

1.	X→G:	<gid, X, R, S_X(gid, X, R)>
2.	G:	V_X(gid, X, R)
3.	G→X:	<gid, G, X, R, E_X(gid, G, X, R, K, S_G(gid, G, X, R, K))>
4.	X:	V_G(gid, G, X, R, K)
5.	X→G:	<X, G, E_K(X, G, R)>

The most severe threat to Protocol 1 is that an attacker could use it to initiate denial-of-service (DoS) attacks against group agents. Because the mobile host does not know the shared key and can not encrypt the packet header at this time, an attacker can discover the identity of a group agent and locate its position by eavesdropping these requests and analyzing the packet headers. This threat may be avoided by encrypting the packet header of the request with the agent's public key and the packet header of the response with the mobile host's public key. An attacker could not distinguish the authentication protocol packets with other control or data packets. Furthermore, the movement of a group agent makes it complicated for an attacker to launch continuous DoS attacks.

5. Secure Roaming Support

A mobile network allows mobile hosts to roam within the network. In wired environments, Mobile IP is the most widely used protocol to support roaming. Mobile IP is not an ideal solution for HMWN, because (1) it establishes a "tunnel" between the home agent and foreign agent, which consumes wireless bandwidth; (2) it does not support "group roaming" (i.e., a whole group moves from one place to another). The essence of roaming support is relocating a mobile host. SMGR protocol naturally supports roaming as it dynamically locates the destination when forwarding a packet.

In case secure packet forwarding is required by the foreign group, the mobile host must authenticate itself to the foreign group agent and obtain the shared key before it can communicate with other hosts in the foreign group. This process is called secure roaming.

5.1 Secure Roaming Support Algorithm

The pseudo-code in Algorithm 2 shows the sketch of the secure roaming support algorithm. This algorithm is a part of the "Migration" operation. Its purpose is to verify the identity of the mobile host and distribute the shared key safely. Other issues related to "Migration" are discussed in [5], including when to initiates the operation, how to choose a foreign group to join, how to update membership, and how to maintain routing table.

5.2 Mutual Authentication between a Mobile Host and a FGA

Mutual authentication is required by secure roaming support algorithm to protect the foreign group as well as the mobile host. Protocol 2 shows the procedure of

Algorithm 2 Secure roaming support.

Mobile host:

```
if homeless
  broadcasts a "join a group temporarily" request
  if a response from a FGA is received
    invokes the authentication process with that agent
    if authenticated
      changes the group ID and the shared key along with the CG and CGA
```

Group agent:

```
if a "join temporarily" request is received
  if the security policy allows hosting
    sends a response to the mobile host
    invokes the authentication process
    if authentication succeeds
      issues a new shared key
      distributes the new key to the current group members
      sends the group information (gid, key) to the mobile host
```

Protocol 2 Mutual authentication.

1.	X→FGA:	<X, FGA, HGA, R, T, S_X(X, FGA, HGA, R, T)>
2.	FGA→HGA:	<X, FGA, HGA, R, T, S_X(X, FGA, HGA, R, T)>
3.	HGA→FGA:	<S_{HGA}(X, K_X, R, T), S_{HGA}(FGA, K_{FGA}, R, T)>
4.	FGA→X:	<S_{HGA}(FGA, K_{FGA}, R, T), E_X(FGA, X, R, T, K, S_{FGA}(FGA, X, R, T, K))>
5.	X→FGA:	<X, FGA, T, E_K(X, FGA, T)>

mutual authentication. We only present message exchanges. The verifications at X, HGA, and FGA are omitted without losing the essence of the protocol.

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. The fourth step ensures that only X can get K. X must verify that K is generated by FGA using FGA's public key. Because roaming support may be required by the same mobile host multiple times, a time stamp is associated with each request to demonstrate its freshness. The use of time stamp may avoid the "replay" attack. It requires a loose synchronization among all mobile hosts.

5.3 Fault-Tolerant Authentication

In a WNMBS, group agents are also moving. When Protocol 2 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 HGAs are no longer available. To make HMWN networks survivable from such kind of unavailability, a fault-tolerant authentication scheme is proposed in [15].

In a HMWN system. A group agent itself may be a member of another group and has its own HGA, unless it's the root of the hierarchy. We define mobile host X's Intention Agent (IA) as follows:

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

For example, in Fig. 1, agents A and B are IAs of mobile host x. In the proposed fault-tolerant scheme, not only its HGA, but also all its IAs know the public key of a mobile host. A mobile host also knows all its IAs' public keys. Each IA has a priority based on several factors [16]. When Protocol 2 fails due to the unavailability of the HGA, the mobile host will choose the IA with the highest priority and retry the authentication protocol until it is authenticated or no IA is available. With this improvement, a mobile host at level n can tolerate n agent failures.

6. Computation Overhead

The majority of computation overhead introduced by the security mechanisms comes from two sources: the secure packet forwarding and the secure roaming support. We numerically investigate the overhead by conducting a series of real-world experiments and simulations.

The test-bed is a PC running Linux kernel 2.4.2. It has an Intel Celeron 700 MHz CPU, 128 M memory, and a 10 G hard disk. Currently, even a low-end notebook computer has better configuration than the test-bed machine in terms of computation power.

The cryptography implementations used in the experimental study are provided by the GNU Crypto package. The testing programs are written in Java and compiled using JDK 1.3.1.

6.1 Overhead of Secure Packet Forwarding

The computation overhead of secure packet forwarding is determined by the transmission rate, the length of packet header, the length of packets, and the encryption/decryption speeds. We take the IEEE 802.11b standard as an example, which supports up to 11 Mbps wireless bandwidth, to estimate the overhead. Suppose only the IP header is encrypted (i.e., the length of packet header is 20 bytes). Based on the study of IP packet length distribution [17], we let the length of a packet be 420 bytes, the mean of IP packet length obtained from more than 200 million packets.

Four block ciphers are studied. They are DES (Data Encryption Standard), Triple-DES, Twofish and Rijndael. Table 1 shows the results obtained from processing 1,000,000 blocks. The encryption/decryption speeds (column 2 and 3 in Table 1) are obtained by using the GNU CipherSpeed tool.

The results demonstrate that secure packet forwarding is quite feasible in wireless networks as the appropriate cipher only uses about 1.6% of a mobile host's CPU time.

6.2 Overhead of Secure Roaming Support

The computation overhead of secure roaming support is introduced by the mutual authentication protocol. The time consumed by different cryptography operations using the RSA algorithm are shown in Table 2. They are obtained by operating 1,000 64-byte blocks with different keys whose length is 1024 bits. The computation time in one roaming request can be estimated as follows according to Protocol 2.

Table 1 Encryption/decryption speed of some block ciphers.

Cipher	Encryption Speed (KB/s)	Decryption Speed (KB/s)	CPU Usage
DES	4035	4061	3%
Triple-DES	1338	1323	9.8%
Twofish	1284	1277	10%
Rijndael	8185	8134	1.6%

Mobile host: one signing, one asymmetric decryption, two verifying, and one symmetric encryption (whose computation time can be ignored) operations are required. The computation time is about 90 ms.

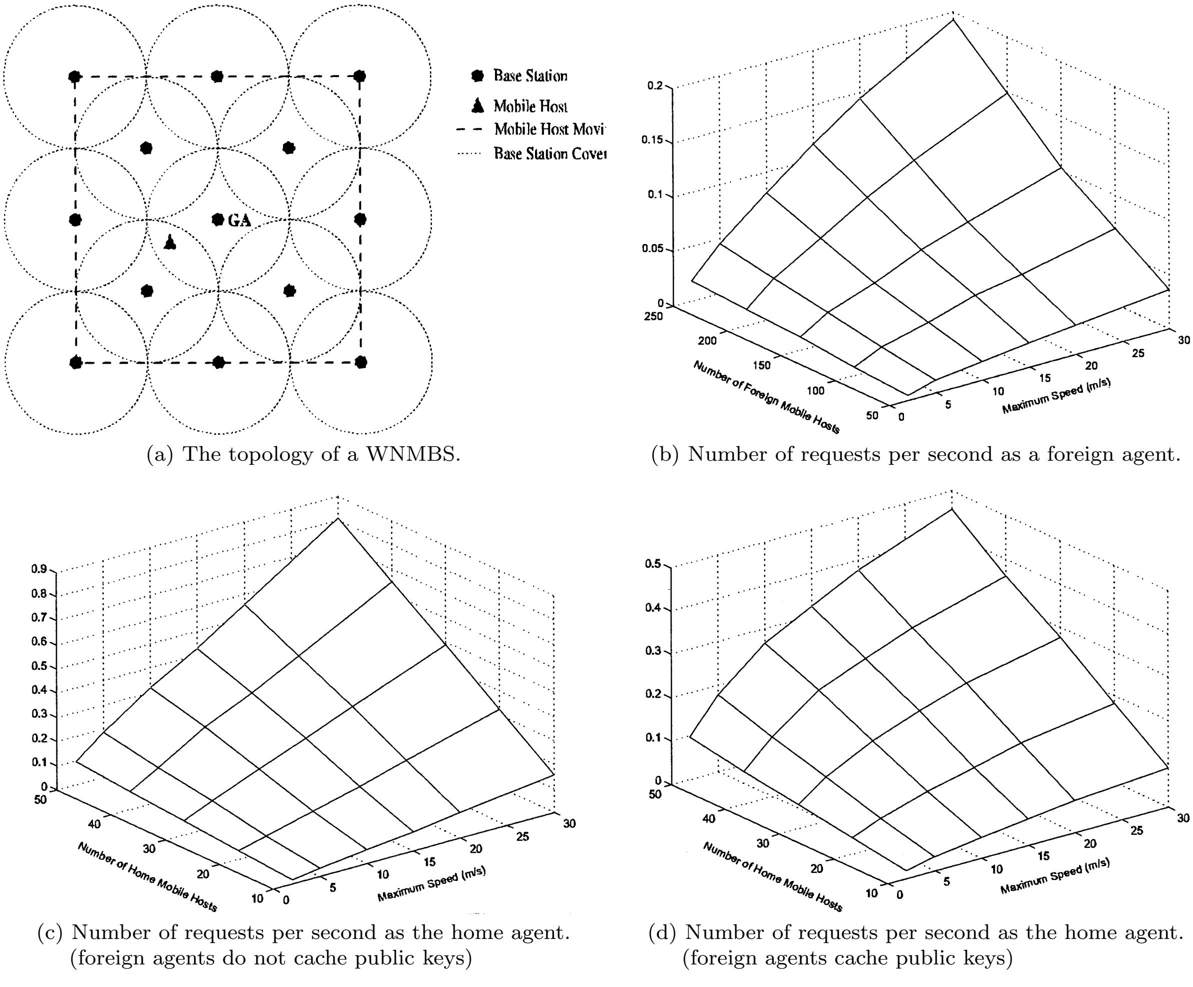
Foreign agent: one verifying, one asymmetric encryption, and one signing operations are required. The computation time is about 50 ms.

Home agent: one verifying and two signing operations are required. The computation time is about 90 ms.

Since roaming is caused by the relative motion between a mobile host and its group agent, for demonstration

Table 2 Speed of RSA.

Operation	Signing	Verifying	Encryption	Decryption
Time (ms)	40.73	2.38	2.29	40.66



(a) The topology of a WNMBS.

(b) Number of requests per second as a foreign agent.

(c) Number of requests per second as the home agent. (foreign agents do not cache public keys)

(d) Number of requests per second as the home agent. (foreign agents cache public keys)

Fig. 3 Frequency of roaming requests.

purpose, only hosts are moving in the simulations. Figure 3(a) shows the topology of a typical WNMBS. Mobile hosts move in a square area that is fully covered by 13 base stations. The movement is determined by the random way-point mobility [3] model. The pause time is 0 second. The maximum speed ranges from 2 m/s, the jogging speed of a person, to 30 m/s, the speed of a running vehicle. The radius of every circle is 250 m. Each simulation runs for 5000 seconds.

For a mobile host, the mean interval between two consecutive requests is 416.38 and 56.49 seconds, respectively, when the maximum speed is 2 m/s and 30 m/s.

The rest experiments study the requests related to the group agent GA.

Figure 3(b) shows the frequency of requests as a function of the number of foreign hosts in the area and their maximum speed, when GA acts as a foreign agent. For 50 foreign hosts, the number of requests per second increases from 0.005 to 0.04 with the maximum speed increasing from 2 m/s to 30 m/s. Even with 250 foreign hosts and 30 m/s maximum speed, there are less than 0.2 requests per second. In this set of experiments, the computation overhead on GA of being a foreign agent is always less than 1% CPU time.

The overhead on GA of being the home agent is determined by the number of hosts whose home agent is GA and their mobility. Figure 3(c) shows the frequency of requests as a function of the number of home hosts in the area and the maximum speed. For 50 home hosts and 30 m/s maximum speed, the frequency is as high as 0.8 requests per second, because the home agent is involved in every roaming request. In this case, the computation overhead is about 7.2% CPU time.

The number of requests can be reduced if foreign agents cache the public key of a mobile host for a period of time. Figure 3(d) shows the results of the experiments in which foreign agents cache public keys for 200 seconds. The highest frequency is 0.45 requests per second, about a half of that in the previous experiment. The corresponding computation overhead is about 4% CPU time. The total computation overhead on GA ranges from 0.2% to 5% CPU time in the experimental study depending on the number of hosts and their mobility.

7. Conclusion

This paper presents security mechanisms for HMWN to support wireless networks with movable base stations. In a HMWN system, mobile hosts form hierarchical groups. The base stations (group agents) serve as a distributed trusted entity. We propose a secure packet forwarding algorithm to protect the network infrastructure. A protocol is developed to authenticate a mobile host and distribute the group-shared key. An algorithm is designed to support mobile hosts roaming within the network. To secure both the foreign group and the mobile host, they mutually authenticate each other with the help from the home group agent. Experimental study justifies the feasibility of the proposed security mechanisms. The computation overhead of secure packet forwarding is less than 2% CPU time, and that of secure roaming support ranges from 0.2% to 5% CPU time depending on the number of hosts and their motion.

References

[1] “IETF MANET working group,” http://www.ietf.org/html.charters/manet-charter.html

[2] C. Santiváñez, B. McDonald, I. Stavrakakis, and R. Ramanathan, “On the scalability of ad hoc routing protocols,” Proc. INFOCOM 2002, vol.3, pp.1688–1697, 2002.

[3] Y. Lu, W. Wang, Y. Zhong, and B. Bhargava, “Study of distance vector routing protocols for mobile ad hoc networks,” Proc. IEEE Int. Conf. Pervasive Comput. Commun. (PerCom 2003), pp.187–194, Texas, March 2003.

[4] IEEE Std 802.11a-1999, supplement to IEEE Std 802.11-1999.

[5] Y. Lu, W. Wang, and B. Bhargava, “Hierarchical structure for supporting movable base stations in wireless networks,” Proc. Int. Conf. Telecommun. (ICT 2003), pp.729–736, Papeete, French Polynesia, Feb. 2003.

[6] S. Park, A. Ganz, and Z. Ganz, “Security protocol for IEEE 802.11 wireless local area network,” Mobile Netw. Appl., vol.3, no.3, pp.237–246, Sept. 1998.

[7] L. Zhou and Z.J. Haas, “Securing ad hoc networks,” IEEE Netw. Mag., vol.13, no.6, pp.24–30, Dec. 1999.

[8] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, “An on-demand secure routing protocol resilient to byzantine failures,” Proc. Workshop on Wireless Security (WiSe’02), pp.21–30, Atlanta, Sept. 2002.

[9] M.G. Zapata and N. Asokan, “Securing ad hoc routing protocols,” Proc. Workshop on Wireless Security (WiSe’02), pp.1–10, Atlanta, Sept. 2002.

[10] B. Schneier, Applied Cryptography Second Edition: Protocols, Algorithms, and Source Code in C, John Wiley & Sons, 1996.

[11] J. Chuprun, C. Bergstrom, and A. Guzek, “Advanced interference rejection and anti-jam methods for low power mobile battlefield communications,” Proc. IEEE Military Commun. Conf. (MILCOM 97), vol.2, pp.841–846, 1997.

[12] W. Myrick, J. Goldstein, and M. Zoltowski, “Low complexity anti-jam space-time processing for gps,” Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP’01), vol.4, pp.2233–2236, 2001.

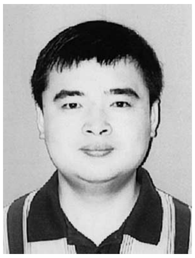
[13] B.K.C.S. Florian Buchholz and T.E. Daniels, “Packet tracker final report,” CERIAS TR 2000-23, pp.1–31, 2000.

[14] M. Burrows, M. Abadi, and R. Needham, “A logic of authentication,” ACM Trans. Comput. Syst., vol.8, no.1, pp.18–36, Feb. 1990.

[15] B. Bhargava, S. Kamisetty, and S. Madria, “Fault tolerant authentication and group key management in mobile computing,” Proc. Int. Conf. Internet Computing (IC, 2000), pp.176–185, June 2000.

[16] D. McClure and B. Bhargava, “On assigning priorities of keying parameters in a secure mobile network,” Dept. CS, Purdue University, Tech. Rep., pp.1–6, 2001.

[17] “Packet length distributions,” http://www.caida.org/analysis/AIX/plen_hist/



Yi Lu graduated from University of Science and Technology of China in 1996 with a B.S. degree in Computer Science. He got his M.S. degree in Computer Science from Institute of Software, Chinese Academy of Sciences in 1999. Since fall 1999, he has been a Ph.D. student in the department of computer sciences at Purdue University with Professor Bharat Bhargava as his advisor. He is a member of IEEE and ACM. His research interests include wireless network security, heterogeneous wireless networks, routing and congestion control protocols for ad hoc networks, and trust modelling for peer-to-peer applications.

Bharat Bhargava received his B.E. degree from Indiana Institute of Science and M.S. and Ph.D. degrees in EE from Purdue University. He is a professor of computer sciences at Purdue University. Bhargava is conducting research in security issues in mobile and ad hoc networks. This involves host authentication and key management, secure routing and dealing with malicious hosts, adaptability to attacks, and experimental studies. Related research is in formalizing evidence, trust, and fraud. He has proposed schemes to identify vulnerabilities in systems and networks, and assess threats to large organizations. He has developed techniques to avoid threats that can lead to operational failures. These ideas and scientific principles are being applied to the building of peer-to-peer systems, cellular assisted mobile ad hoc networks, and to the monitoring of QoS-enabled network domains. Bhargava received Outstanding Instructor Awards, from the Purdue chapter of the ACM in 1996 and 1998. His name is included in Purdue's book of great teachers. Bhargava is a Fellow of the Institute of Electrical and Electronics Engineers and of the Institute of Electronics and Telecommunication Engineers. He has been awarded the charter Gold Core Member distinction by the IEEE Computer Society for his distinguished service. In 1999 he received IEEE Technical Achievement award for a major impact of his decade long contributions to foundations of adaptability in communication and distributed systems.

Weichao Wang is a student member of IEEE. He joined the RAID Lab in the Department of Computer Sciences, Purdue University in 2000 and he is a Ph.D. student there now. His research interests focus on mobile, ad hoc networks, especially on the routing procedure, security vulnerability, intrusion detection and intruder identification. His other interests include high performance routing in TCP/IP, network security, and computer architecture.

Yuhui Zhong received her B.S. degree from Beijing Normal University of China in 1996 and M.S. degree from Institute of Software, Chinese Academy of Sciences in 1999. She was enrolled in the department of computer sciences at Purdue University as a Ph.D. student in 2000. Her research interests include trust modelling and evaluation, fraud formalization, trusted routing protocols for ad hoc networks, and trusted cooperation in peer-to-peer environments.

Xiaoxin Wu received his B.E. degree from Beijing University of Posts and Telecommunications in 1990 and the Ph.D. degree from University of California, Davis in 2001. After that he joined Arraycomm Inc. as a protocol research engineer. Since 2002, he has been working as a postdoctoral researcher in Department of Computer Sciences, Purdue University. His major research interests include routing, security, quality of service (QoS), and resource allocation in ad hoc network, cellular network, and integrated wireless networks. He served as technical program committee member for VTC2003 in symposium of Integrated Heterogeneous Wireless Networks.