An Efficient Authentication Scheme between MANET and WLAN Based on Mobile IPv6

Ching-Wen Chen[1], Ming-Chin Chuang[1] and Chwei-Shyong Tsai[2]
(Corresponding author: Ching-Wen Chen)

Department of Computer Science and Information Engineering, Chaoyang University of Technology[1],
168 Jifong E. Rd., Wufong Township Taichung County, Taiwan 41349, R.O.C. (Email: chingwen@mail.cyut.edu.tw)
Department of Management Information Systems, National Chung Hsing University[2],
250 Kuo Kuang Rd., Taichung, Taiwan 402, R.O.C.

(Received Feb. 15, 2005; revised and accepted March 10, 2005)

Abstract

One of the major challenges for a wireless network design is the efficient authentication scheme. A mobile node (MN) attached to a WLAN and then moved into an area where the radio signal coverage from the access point (AP) does not exist. The mobile node may reconfigure itself into ad hoc mode and connect to this network. Before the mobile node using the resource, it must be verified whether legally or not. But in Mobile IP protocol, every mobile node must perform the home registration to register with HA every second. If the foreign network is far from the home network, the authentication time delay will be long. To reduce the time delay of authentication and home registration, we provide an efficient registration scheme. We use local authentication to achieve efficiency, and use Mobile IPv6 to support the mobility.

Keywords: Authentication, mobile Ad hoc network, mobile IPv6, wireless local area network

1 Introduction

In recent years, the wireless network has become more and more popular due to low cost and high bandwidth capacities. The Internet Engineering Task Force (IETF) Mobile IP working group has proposed the Mobile IP to support that a mobile node can roam around different foreign domain and keep a session connected.

Wireless networks can be broadly classified into two types. The infrastructure network such as hub, bridge, router, and another is without any infrastructure such as Mobile Ad Hoc Network (MANET). In this paper, we used hybrid network architecture to integrate infrastructure network and MANET, and discuss how to support Mobile IPv6 in such environment.

WLANs offer mobile nodes to access the services of Internet. If a mobile node moves into an area where the radio signal off an access point, it may reconfigure itself into ad hoc mode and use multi-hop mechanism to connect the Internet by MANET's gateway. Before the mobile node using the resource, it must be authenticated validly by HAAA. If the foreign network is far away from the home network, the authentication time will be longer. In this paper, we provide a local mutual authentication scheme, which can decrease the authentication time when the mobile node roams to WLAN or MANET.

The rest of the paper is organized as follows. In Section 2, some backgrounds of mobile IPv6 are introduced. In Section 3, the proposed authentication scheme between WLAN and MANET. In Section 4, we show the security of our scheme. In Section 5, we present the performance analysis and some comparisons with other schemes. In Section 6, we make conclusion.

2 Background

2.1 Mobile IPv6

In recent years, the mobile devices are in widespread use. The Internet Engineering Task Force Mobile IP working group has proposed the Mobile IP to support that a mobile node can roam around a foreign domain. In Mobile IPv6 [6, 7], a mobile node has a home address and a home agent in its home subnet. Unlike the Mobile IPv4, the Mobile IPv6 architecture without any foreign agent (FA) in the visit network. The mobile node should register its new care-of-address to HA using binding update mechanism. When the mobile node changes its current address, it will send a binding update packet to any CN directly. The CN can renew its binding cache after receiving the binding update packet. Then, data packets can be sent to the MN by using its care-of-address without forwarding by the HA.

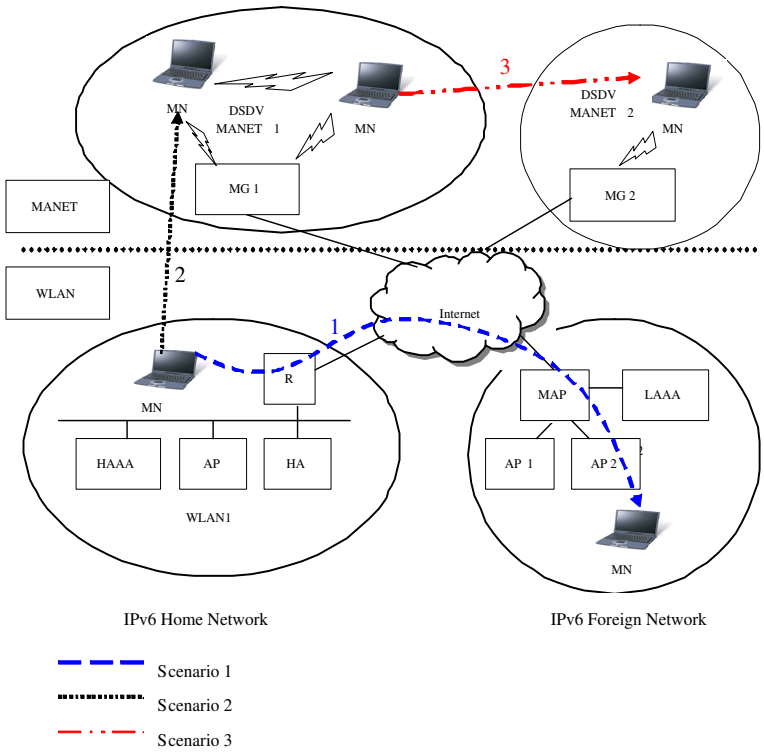


Figure 1: Network architecture and mobility scenarios

2.2 Use Mobile IPv6 Joins with AAA in WLAN

To integrate heterogeneous networks, IP as the common network layer protocol is essential. Each mobile node is assigned a permanent IP address in the same way, and this IP address is known as the mobile node's home address. When mobile node roams to the visit network, it receives the advertisement messages including the address of the subnet prefix. The mobile node may generate a new care-of-address using address auto-configuration. Then, the mobile node changes its current address, and sends the binding update to its correspondent node and home agent.

The AAA protocol means authentication, authorization, and accounting protocol. The IETF has proposed the AAA protocol to solve the authentication, authorization, and accounting problems when it suffers the request of MN from heterogeneous network roaming. So the AAA server surely will be an important supporter in the future. The characteristics of AAA are mentioned as follows:

- Authentication: The purpose of authentication is to confirm the mobile node validity.
- Authorization: In the issue of authentication, resource management is closely related to many aspects. When user authentication successes, it is necessary to make out the limits of user's authority.
- Accounting: It collects information on resource usage for the purpose of trend analysis, auditing, billing, or cost allocation.

In the Mobile IP combined with AAA architecture, besides the original component in the Mobile IP. There are some new components such as HAAA and LAAA. The HAAA server is responsible for authentication, authorization, and accounting for mobile nodes in the home domain. The LAAA server is responsible for authentication, authorization, and accounting for roaming mobile nodes. When a mobile node roams around a foreign domain, it needs to use resources within the foreign domain. Mobile node provides some authentication information before the resources can be allowed to proceed accessing. The local AAA server receives the requests in the foreign domain, and the LAAA will check the MN's authentication information However, the LAAA itself may not have enough information to verify the mobile node. Therefore, the LAAA has to send the authentication information of MN back to the MN's home network and wait for the reply. The verification of the MN's authentication information can be completed with the help of the MN's HAAA. Whenever the MN moves to a new foreign agent, the new LAAA has to repeat this procedure.

2.3 Use Mobile IPv6 in MANET

Address allocation to mobile node is a critical problem in mobile ad hoc networks. In this paper, we used IPv6 stateless address auto-configuration protocol. Because the MANET is built without any network infrastructure,

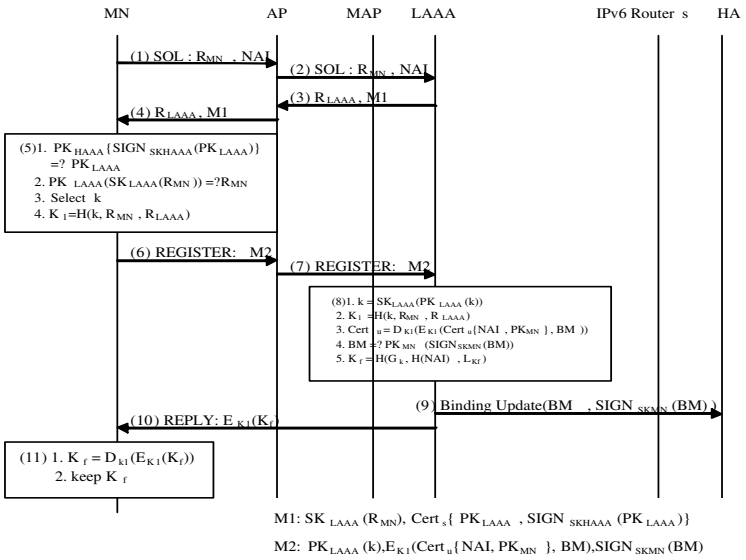


Figure 2: First roaming at a foreign network

each mobile node in the MANET must get the address by itself. Then, it will start the duplicate address detection (DAD) mechanism to avoid the address collision.

The ad hoc networks are self-organized and non-infrastructure network. There is no Certificate Authority (CA) in the MANET. So the authentication in the MANET is a difficult work. Therefore, some researchers proposed the Pretty Good Privacy (PGP) mechanism and threshold cryptography [9] to share the key. Then, some schemes are used the cluster-based [2, 3, 10, 14] to manage the mobile node by cluster head. The cluster head plays an important role such as CA and responsible to authenticate the mobile node within cluster.

2.4 Hierarchies of Mobile IPv6

The main goal of Hierarchical mobility management for Mobile IPv6 is to reduce the amount of signaling between the mobile node, its correspondent nodes and its HA. The traditional Mobile IP allows the mobile node to move around any foreign network. However, the mobile node often moves around different access points in the same domain. MN must send the binding update with its HA frequently which result in too much bandwidth consumption and the authentication time will become higher. So the hierarchical mobility management scheme [5, 11, 13, 16] is proposed in the foreign network. Hierarchical mobile IPv6 [4] utilizes a new code called Mobility Anchor Point (MAP).

In the hierarchical architecture, MN needs to find a Mobile Anchor point (MAP) when it first arrives at a visit domain. During a home registration procedure, HA records the regional care-of-address (RCoA) on the MAP's domain. Then, micro handoff happens when MN moves locally to another network within MAP network. In micro-mobility, MN only needs to changes its link care-of-address (LCoA), but not sending the blinding update to HA and CN.

3 Proposed Scheme

In traditional Mobile IP, one of the technical challenges is that HA and FA has no security association. This restriction about authentication between home network and foreign network results in authentication time delay become long. Therefore, we proposed a novel authentication scheme which can provide the local authentication without returning the MN's home network for authentication.

3.1 Network Architecture

As illustrated in Figure 1, our network architecture is a hybrid network, which is composed of WLANs and MANETs [8, 15]. WLAN building infrastructure with 802.11b technology, but access points signal in WLAN have limited coverage. For this reason multi-hop ad hoc routing protocols are considered to provide ways to extend the range of access points. In this paper, we assume a gateway in the MANET which can connect to Internet. There are some attendants such as HA, HAAA, IPv6 routers, access points, and gateway router.

The responsibility of HA in the WLAN is to record the mobile node information, and verify the mobile node whether it is legal or not. HAAA has the responsibility in terms of authentication, authorization, and accounting. The IPv6 routers support forwarding packets to destinations. A gateway is used for connecting to the Internet. In this paper, the MANET's gateway played an important role which can authenticate the mobile node in the

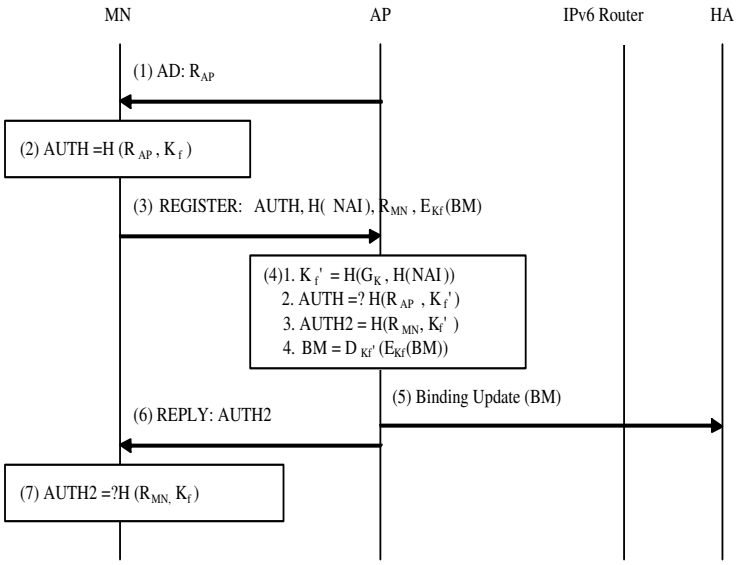


Figure 3: Fast re-authentication at the same foreign network

MANET. The access points in the foreign domain can authenticate the mobile node when the mobile node roams around this domain again.

Each mobile node has an IPv6 address corresponding to its home subnet as its identifier in the Internet. Once the mobile node roams into a foreign subnet, it receives the advertisement and generates its care-of-address (CoA) using the IPv6 auto-configuration mechanism. The new CoA reflects the mobile node's current location. The foreign domain could be either a WLAN or a MANET. Within the MANET, the packets are routed based on the table-driven [12] protocol, whereas in the remainder of the network the packet routing follows the Mobile IPv6 routing scheme.

3.2 Authentication Procedures

In this subsection, there are three scenarios where a node moves into a WLAN from WLAN, a node moves into an MANET from WLAN, and a node moves into an MANET from MANET. The notations are used in our proposal are listed in Table 1.

3.2.1 First Scenario: $WLAN_1 \rightarrow WLAN_2$

When a mobile node roams to the foreign $WLAN_2$ from home $WLAN_1$.

- Initial Step between $WLAN_1$ and $WLAN_2$:
  The mobile node has a certificate which is signed by HAAA. The certificate of mobile node includes the public key of MN, and network access identifier of MN. If the HAAA and LAAA have the roaming agreement, the LAAA will get a certificate which is signed by HAAA. The certificate of LAAA includes the public key of LAAA, and the public key of LAAA is signed by HAAA's private key.

Table 1: Notations

PK_A:	A's public key
SK_A:	A's secret key
$SIGN_{SKA}$:	Signature by A's private key
DSDV:	Destination sequence distance vector
AP:	Access point
MAP:	Mobile anchor point
MN:	Mobile node
MG:	MANET's gateway
GK:	Group key of a MANET or WLAN.
NAI:	An unique network access identifier
BM:	Binding update message
$Cert_A$:	A's certificate
R_A:	random number issued by A
L_{Kf}:	Lifetime of K_f

- First Roaming at a Foreign Network:
  Within the wireless network, a mobile node can often roam around foreign domain, where it expects to access real-time network services and resources at any time and anywhere. Thus the mobile node provides some information to be verified by LAAA. As Figure 2 illustrates, a mobile node not only be authenticated with LAAA but also LAAA be authenticated with mobile node, too. The processes go through as follows:

  1) $MN \rightarrow AP$: Solicitation.
  The solicitation includes random number R_{MN} and its network access identifier.

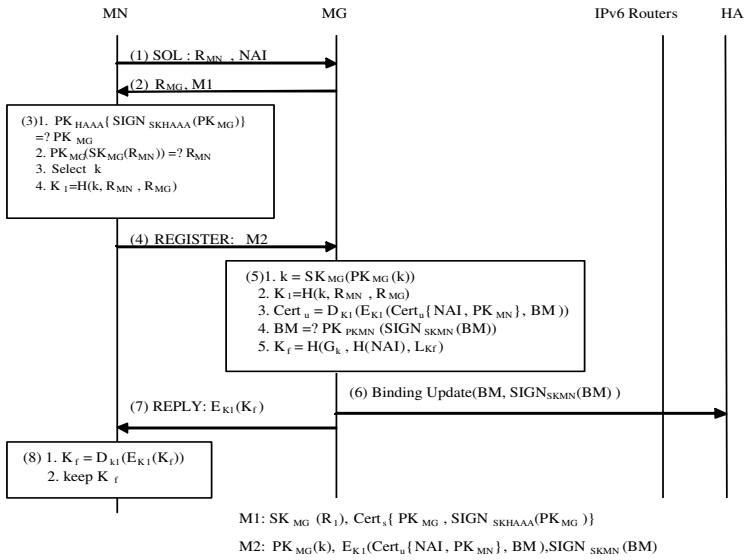


Figure 4: First roaming at a MANET

2) $AP \rightarrow LAAA$: AP forwards the message of (1) to LAAA.

3) $LAAA \rightarrow AP$: LAAA sends R_{LAAA} and $M1$ to AP.
According to the NAI of MN, LAAA can find the corresponding certificate $Cert_s$ and it sends message $M1$ and random number to AP. Where $M1 = SK_{LAAA}(R_{MN})$ and $Certs\{PK_{LAAA}, SIGN_{SKHAAA}(PK_{LAAA})\}$. If LAAA can not find the corresponding certificate, the security association will be built according to MN's NAI.

4) $AP \rightarrow MN$: AP forwards the message R_{LAAA} and $M1$ to MN.
The message includes a random number R_{LAAA} and message $M1 = SK_{LAAA}(R_{MN})$, $Certs\{PK_{LAAA}, SIGN_{SKHAAA}(PK_{LAAA})\}$.

5) MN: Authenticate the LAAA:
MN checks the following equation: $PK_{HAAA}\{SIGN_{SKHAAA}(PK_{LAAA})\} \stackrel{?}{=} PK_{LAAA}$ and uses PK_{LAAA} to get the R_{MN}. If hold, it means the LAAA has the roaming agreement with HAAA. Then, MN selects the k and computes the $K1$ as $K1 = H(k, R_{MN}, R_{LAAA})$.

6) $MN \rightarrow LAAA$: Registration request
The Registration request includes $PK_{LAAA}(k)$, $E_{K1}(Cert_u\{NAI, PK_{MN}\}, BM)$, and $SIGN_{SKMN}(BM)$.

7) $AP \rightarrow LAAA$: AP forwards the message of (6) to LAAA.

8) LAAA: Authenticate the MN.
LAAA uses its private key to get the k and computes the $K1$. LAAA used the $K1$ to get the MN's registration information. Then, LAAA uses the MN's public key to get the binding update message. Finally, LAAA computes the $K_f = H(GK, H(NAI), L_{Kf})$.

9) $LAAA \rightarrow HA$: Binding update.
LAAA use public key of HA to encrypt the binding update message and send to HA.

10) $LAAA \rightarrow MN$: Registration reply.
LAAA uses $K1$ to encrypt the K_f and sends registration reply message to MN.

11) MN: MN gets the K_f and keeps it.

- Micro-mobility within the Same Foreign Network:
When the mobile node micro-moves within the same foreign network where it needs to be verified again. In our scheme, the AP can provide a fast re-authentication scheme. The procedure is shown in Figure 3 and the flow demonstrated as follows:

1) $AP \rightarrow MN$: Advertisement
The advertisement includes random number R_{AP}.

2) MN: generate AUTH
MN computes an authentication factor AUTH as $H(R_{AP}, K_f)$.

3) $MN \rightarrow AP$: Register request
Register request includes $AUTH$, $H(NAI)$, R_{MN}, and $E_{Kf}(BM)$

4) AP: Authenticate the MN
When the AP receives the MN's register request, it will authenticate the MN. First, the AP will check the L_{Kf}. Second, the AP computes the $K_{f\prime} = H(GK, H(NAI), L_{Kf})$. Then, the AP checks the following equation: $AUTH \stackrel{?}{=} H(R_{AP}, K_{f\prime})$. If it equals, it means the MN's authentication is valid. Then, the AP

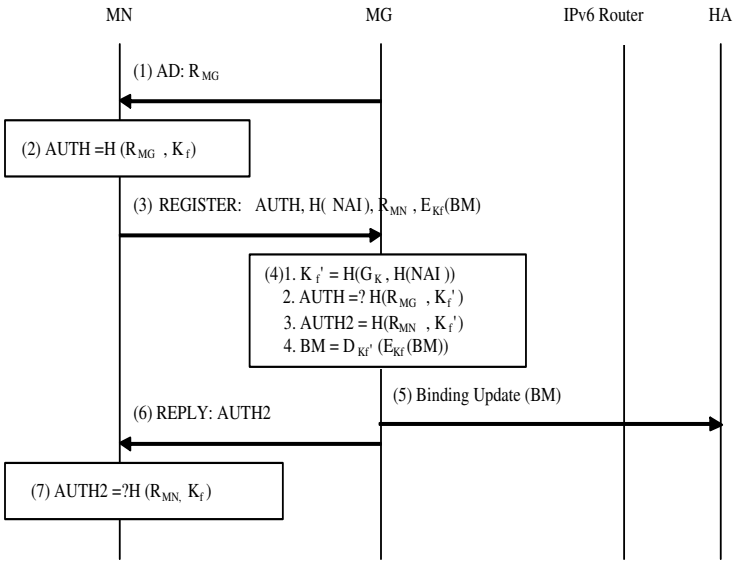


Figure 5: Fast re-authentication at the same MANET

generates an authentication factor $AUTH2 = H(R_{MN}, K_{f\prime})$. Then AP uses $K_{f\prime}$ to get the binding update message.

5) $AP \rightarrow LAAA$: AP sends binding update message to LAAA.

6) $AP \rightarrow MN$: Register reply
The register reply includes the $AUTH2$.

7) MN: Authenticate the AP
When the MN receives the AP's register reply, it will authenticate the AP. The MN checks the following equation: $AUTH2 \stackrel{?}{=} H(R_{MN}, K_f)$. If it holds, it means the reply is trustworthy. Otherwise, the MN will ignore this message.

Our scheme provides the mutual authentication for MN and AP. And localized authentication is efficient to decrease the time of authentication delay.

3.2.2 Second Scenario: $WLAN \rightarrow MANET$

- Initial Step between WLAN and MANET
The mobile node has a certificate which is signed by HAAA. The certificate of mobile node includes the public key of MN, and network access identifier of MN. If the HAAA and MANET's gateway have the roaming agreement, the MANET's gateway will get a certificate which is signed by HAAA. The certificate of LAAA includes the public key of MANET's gateway, and the public key of MANET's gateway is signed by HAAA's private key.

- First Roaming at a MANET
Mobile node roams into the MANET, where it expects to access network services and resources rapidly at any time and anywhere. Thus the mobile node provides some information to be verified by MG. As Figure 4 illustrates, a mobile node can be authenticated with MG.

- Fast re-authentication at the Same MANET
When the mobile node roams into the same MANET again, it needs to be verified again. In our scheme, the gateway can prove fast authentication. The procedures were shown in Figure 5. When the MN receives the MG's register reply, it will authenticate the MG. Then, the MN checks the following equation. $AUTH2 \stackrel{?}{=} H(R_{MN}, K_f)$. If the equation holds, it means the reply is trustworthy. Otherwise, the MN will ignore this message. Our scheme provides the mutual authentication for MN and MG. And localized authentication is efficient to decrease the authentication time delay.

3.2.3 Third Scenario: $MANET_1 \rightarrow MANET_2$

- Initial Step between $MANET_1$ and $MANET_2$
The mobile node has a certificate which is signed by MG_1. The certificate of mobile node includes the public key of MN, and network access identifier of MN. If the MG_1 and MG_2 have the roaming agreement, the MG_2 will get a certificate which is signed by MG_1 The certificate of MG_2 includes the public key of MG_2, and the public key of MG_2 is signed by private key of MG_1.

- First Roaming at a Foreign MANET
Within the mobile ad hoc network, a mobile node may roam around another MANET. It can access network services and resources only after being authenticated. Thus the mobile node provides some information to be verified by MANET's gateway. Because the MANET is a non-infrastructure network,

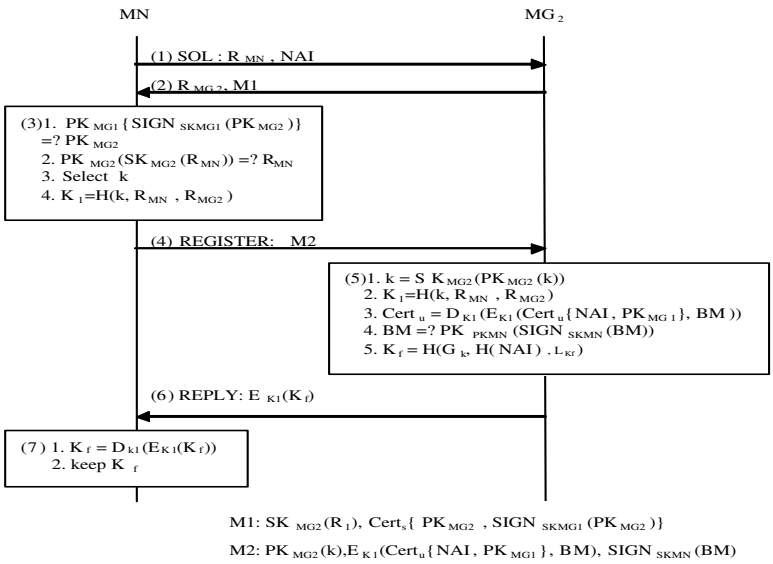


Figure 6: First roaming at a MANET

there is no agent to record the location of MN. So the MN could not send the binding update. As Figure 6 illustrates, a mobile node authenticates with MG_2.

- Fast re-authentication at the same MANET
  When the mobile node roams around the same MANET, it needs to be verified again. In our scheme, the MG_2 can provide a fast authentication scheme. The procedures were shown in Figure 7. When the MN receives the MG_2's registration reply, it will authenticate the MG_2. The MN then checks the following equation: $AUTH2 \stackrel{?}{=} H(R_{MN}, K_f)$. If MN holds, it means the reply is trustworthy. Otherwise, the MN will ignore this message. Our scheme provides the mutual authentication for MN and MG_2. And localized authentication is efficient to decrease the authentication time delay.

4 Security Analysis

In this section, we will demonstrate some security properties. And we will analyze the security of our scheme.

Property 1: One-way hash function.
The one-way hash function H, we know x, and we can easy to compute the $H(x) = y$. But we know the y, it is very difficultly to compute the $H^{-1}(y) = x$. And the hash function is hard to find the $x' \neq x$ such that $H(x') = H(x)$.

Property 2: Public-key cryptosystem.
There are several public key cryptosystem algorithms, including RSA, ElGamal, and Elliptic Curve cryptography. These algorithms relay on the mathematical problems that are easy to perform but difficult to do in reverse. In this paper, MN uses the public key of AAA server to encrypt the authentication message, and send the message to AAA server. Because public key of AAA server can only be decrypted which use private key of AAA server, another users can not decrypt the message.

4.1 Mutual Authentication

When a mobile node roams to a foreign domain, it must be authenticated by the LAAA or MANET's gateway in the foreign domain. However, some proposals schemes don't provide the mutual authentication. In our scheme, we achieve mutual authentication for LAAA (MG) and MN.

- First situation: MN first roams at foreign domain.
  1) MN receives $SIGN_{SKHAAA}(PK_{LAAA})$ from AP's message. Then, MN uses HAAA's public key to get PK_{LAAA}, and uses PK_{LAAA} to get the R_{MN}. If MN can not decrypt the R_{MN} or R_{MN} is not the same as the one MN selected before, the LAAA is not trustworthy. Otherwise, the LAAA is trustworthy.
  2) LAAA receives $PK_{LAAA}(k)$, $E_{K1}(Cert_u\{NAI, PK_{MN}\}, BM)$, and $SIGN_{SKMN}(BM)$. First, LAAA uses its private key to get k. Second, LAAA computes the $K1$. Third, LAAA uses $K1$ to decrypt the MN's certificate. If the $K1$ is unable to decrypt the certificate, the MN is distrust.
- Second situation: MN roams at the same foreign network.
  1) AP receives MN's registration message. The registration message could be $AUTH$, $H(NAI)$,

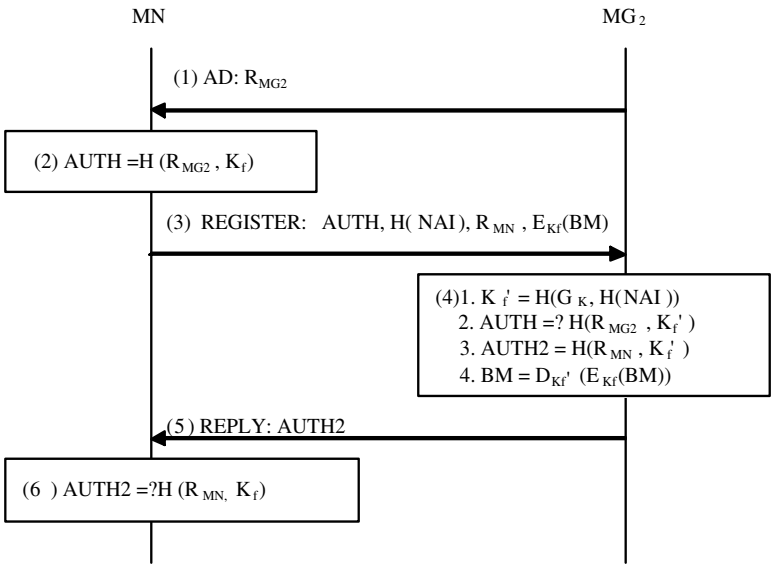


Figure 7: Fast re-authentication at the same MANET

R_{MN}, $E_{Kf}(BM)$. The AP computes the $K_{f\prime}$ as $H(GK, H(NAI), L_{Kf})$ and then the AP checks the following equation: $AUTH \stackrel{?}{=} H(R_{AP}, K_{f\prime})$. If it equals, the MN's authentication is valid.

2) MN receives the register's reply message and it computes the AUTH2. The MN then checks the following equation: $AUTH2 \stackrel{?}{=} H(R_{MN}, K_f)$. If the equation equals, the AP is trustworthy. On the contrary, the AP is distrust.

4.2 Replay Attack

In the authentication procedure, an attacker may try to raise the replay attack. The random numbers are employed in our scheme, and it can successfully avoid the replay attack.

5 Comparisons

When an MN roams to the foreign network, it must perform authentication and home registration. When it changes frequently its point of attachment to other APs, it will cause longer delay, consume more bandwidth, and further suffer packet loss. Therefore, we used the hierarchical mobility management schemes to solve such a problem of MN's frequent handoff, and proposed the local authentication to reduce the authentication delay. Table 2 shows the comparisons with other Mobile IP schemes.

6 Conclusions

In this paper, we provide an efficient local authentication scheme that can reduce the overhead of HA and save the authentication time between MANET and WLAN. In our scheme can not only realize the mutual authentication between a visit network and a roaming user which can be performed locally without the contact with user's home network, but also can resist the replay attack. As proved, our scheme is more efficient and securer than the traditional Mobile IPv6 scheme.

Acknowledgment

This work is supported by the National Science Council of the Republic of China under grants NSC93-2213-E-005-033.

References

[1] C. Castelluccia, "HMIPv6: A hierarchical mobile IPv6 proposal," *ACM SIGMOBILE Mobile Computing and Communications*, vol. 4, no. 1, pp. 48–59, Jan. 2000.

[2] T. C. Chiang and Y. M. Huang, "Group keys and the multicast security in ad hoc networks," in *IEEE International Conference on Parallel Processing Workshops,* pp.385-390, Oct. 2003.

[3] X. Du, Y. Wang, J. Ge, and Y. Wang, "A group key establishment scheme for ad hoc networks," in *IEEE International Conference on Advanced Information Networking and Applicationsm,* pp. 518-520, March 2003.

[4] S. Glass, T. Hiller, S. Jacobs, C. Perkins. "Mobile IP authentication, authorization, and accounting requirements," *RFC 2977*, Oct. 2000.

[5] E. Gustafsson, A. Jonsson, and C. Perkins, "Mobile IP regional registration," http://www.ietf.org/internet-drafts/draft-ietf-mobileip-regtunnel-04.txt, Mar 2001, Work in Progress, 2001.

Table 2: Comparisons

	Byung-Gil et al. [9]	Traditional MIPv6	Chung and Chae [1]	Our scheme
Authentication time	Long	Long	Long	Short
Mutual authentication	No	No	No	Yes
Impact resulting from home network failure	Max	Max	Max	Min
Replay attack	No	Yes	No	No
Fast authentication	No	No	No	Yes
Overhead of HA	Heavy	Heavy	Heavy	Light

[6] D. B. Johnson and C. Perkins, "Mobility Support in IPv6," http://www.ietf.org/internet-drafts/ draft-ietf-mobileip-ipv6-15.txt, July 2001

[7] R. Koodli, "Fast handovers for mobile IPv6," http://www.ietf.org/internet-drafts/draft-ietf-mipshop-fast- mipv6-02.txt, Jan 2004.

[8] L. Lamont, M. Wang, L. Villasenor, T. Randhawa, and S. Hardy, "Integrating WLANs & MANETs to the IPv6 based Internet," in *IEEE International Conference on Communications,* vol. 2, pp. 1090-1095, May 2003.

[9] B. G. Lee, H. G. Kim, S. W. Sohn, and K. H. Park, "Concatenated wireless roaming security association and authentication protocol using ID-based cryptography," in *IEEE International Conference on Vehicular Technology,* vol. 3, pp. 1507-1511, April 2003.

[10] X. Y. Li, Y. Wang, and O. Frieder, "Efficient hybrid key agreement protocol for wireless ad hoc networks," in *IEEE International Conference on Computer Communications and Networks,* pp. 404-409, Oct. 2002.

[11] M. Long, C. H. Wu, and J. D. Irwin, "Localized authentication for wireless LAN internetwork roaming," in *IEEE Wireless Communications and Networking Conference*, vol. 1, pp. 264-267, March 2004.

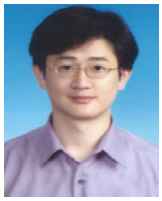
[12] C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing for mobile computers," *Computer Commmunications,* vol. 17, no. 10, pp.234-244, Oct. 1994.

[13] C. E. Perkins, "Mobile-IP local registration with hierarchical foreign agents," *Internet Draft*, Feb. 1996.

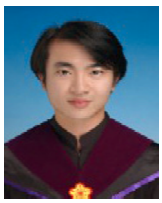
[14] L. Venkatraman and D. P. Agrawal, "A novel authentication scheme for ad hoc networks," in *IEEE International Conference on Wireless Communications and Networking Conference,* vol.3, pp. 1268-1273, Sep. 2000.

[15] R. Wakikawa, J. T. Malinen, C. E. Perkins, A. Nilsson, and Antti J. Tuominen, "Global connectivity for IPv6 mobile ad hoc networks," http://www.ietf.org/internet-drafts/draft-wakikawa-manet-globalv6-02.txt, Nov 2002.

[16] J. Zao, S. Kent, J. Gahmb, G. Troxel, M. Condell, P. Helinek, N. Yuan, and I. Castineyra, "A public-key based secure mobile IP," *Wireless Networks*, vol. 5, pp. 373-390, 1999.



Ching-Wen Chen received the M.S. degree in Department of Computer Science from National Tsing Hwa University, Taiwan, 1995 and the Ph.D. degree in computer science and information engineering at National Chiao Tung University, Taiwan, 2002. He joined the faculty of the department of information and communication engineering, Chaoyang University of Technology, Taiwan, as an Assistant Professor in 2002. His research interests include computer architecture, interconnection network, parallel processing, embedded system and Ad-Hoc network.



Ming-Chin Chuang received the B.S. degree in department of computer information science from Aletheia University, Taiwan, in 2003. At present, He studies in the department of computer science, Chaoyang University of Technology, Taiwan. His research interests include mobile IP, network security, and Ad-Hoc network.

Chwei-Shyong Tsai was born in Changhua, Taiwan, Republic of China, on September 3, 1962. He received the B.S. degree in Applied Mathematics in 1984 from National Chung Hsing University, Taichung, Taiwan. He received the M.S. degree in Computer Science and Electronic Engineering in 1986 from National Center University, Chungli, Taiwan. He received the Ph.D. degree in Computer Science and Information Engineering in 2002 from National Chung Cheng University, Chiayi, Taiwan. From August 2002, he was an associate professor of the Department of Information Management at National Taichung Institute of Technology, Taichung, Taiwan.

Since August 2004, he has been an associate professor of the Department of Management Information Systems at National Chung Hsing University, Taichung, Taiwan. His research interests include image watermarking, image authentication, information hiding, bio-information and computer networks.