A Secure Mobile IP Registration Protocol

Cheng-Ying Yang[1] and Cheng-Yeh Shiu[2]
(Corresponding author: Cheng-Ying Yang)

Department of Computer Science and Information Engineering, National Formosa University[1],
64 Wen-Hwa Road, Hu-Wei, Yun-Lin, Taiwan 63208, R.O.C. (Email: cyang@cyut.edu.tw)
Department of Information Management, Chaoyang University of Technology[2],
168 Gifeng E. Rd., Wufeng Taichung County, Taiwan, R.O.C.

(Received Feb. 20, 2005; revised and accepted March 17, 2005)

Abstract

The wireless network develop is support mobility within the Internet at presently. The mobile Internet use Mobile IP technologies in the wireless Internet. This paper is concerned with the security aspect of the registration protocol in Mobile IP. In this paper we publish a new method use the secure-key combine minimal public-key besides produce the communication session key in mobile node registration protocol. The all communication message are encrypt in our propose method. An easy and fast authentication method for establishing a mobile node's identity that can also prevent replay, TCP spicing and guessing attack is proposed.

Keywords: Authentication, mobile IP, registration, security

1 Introduction

Mobile voice communications have become very popular in recent years and the focal point of industry attention from the first cellular phone system to the current wireless LAN [8, 9]. The speed of wireless communications has continually increased. More service providers are delivering wireless services to the public. For example, the traditional computer connection to a network involves a system of hard wire connections to the network equipment. Today, computers can be connected to network equipment with a wireless interface, eliminating the need for a hardwire network system. The wireless interface and wireless equipment are becoming the technology of the future [5, 12, 29].

Mobile communications have already developed up to now. Traditional mobile communications are just the part of the cellular phone system (GSM). Because of new technological developments and cellular phone techniques (i.e., GPRS, WCDMA, etc.) for wireless communications have become available (i.e., PDA). There are numerous articles that discuss cellular phone and wireless network advances [18, 19]. Some savants have proposed an Internet infrastructure for cellular CDMA networks using Mobile IP in Figure 1 [27].

Mobile communications deliver all messages using radio waves. Therefore anyone can easily receive and intercept these messages. For this reason, communications security is extraordinarily important services. In generally, these communication services must satisfy the following security requirements [31]:

- *Confidentiality:* The confidentiality is to insure that all transmitted data over a public network could not be eavesdropped by an illegal user.
- *Integrity:* The equipment integrity to insure that the all data formats for senders and receivers are compatible.
- *Authentication:* Prior to data delivery, both parties must be able to authenticate one another's identity.
- *Non-repudiation:* Prevents receivers of data services from denying receiving such services or the service provider from denying service to authorized users.

The current Internet Protocol does not support mobile service. The Internet Engineering Task Force (IETF) has been authorized to develop an Internet Standard "Mobile IP" designed to support node mobility within the Internet [24]. There are certain specifications identified by the Request For Comments (RFC) document [1, 2, 3, 22, 23].

The different between Mobile IP and IP protocol is its operating on a subnet. The Mobile IP protocol permits Mobile Node (MN) move to other subnets and still correspond with other nodes. All Mobile Nodes (MN) have a home address in their Home Network. The MN obtains a temp address (Care-of-Address, COA) when a mobile node is in another network (Foreign Network). The home agent employs COA to identify the MN site. When a corresponding node sends data to the MN, the MN's home agent will get the data and forward it to the MN [24].

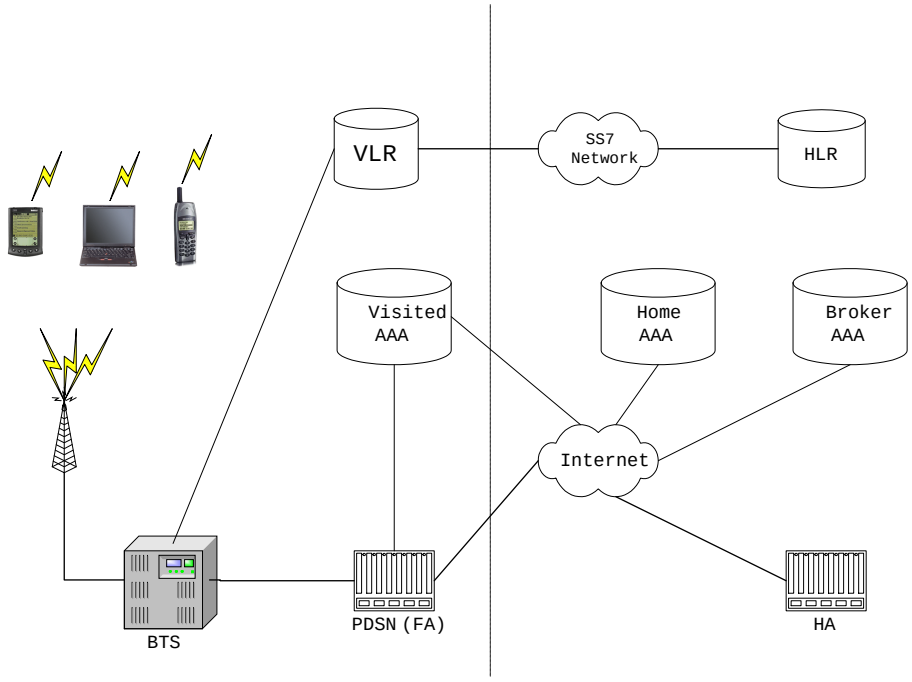


Figure 1: Mobile environment architecture

In a simplification of the Mobile IP protocol, the MN leaves its home network to go into a foreign network. The MN obtains a COA through a foreign agent, and via the foreign agent, notifies the home agent to update the home address with the COA. The home agent transmits packages outside the communication node to the MN's foreign agent. The foreign agent then passes these packages to the MN. There are some articles that discus the tunnel protocol used in this process [7, 21, 28]. In this study, we discuss Mobile IP security and focus on user authentication and deliver secure communications [11, 13, 16, 18, 19, 20, 27]. The safety of cellular phones has been discussed [4, 6, 15, 17]. Cellular phone systems are different from the Mobile IP system, in that the cellular phone system security function cannot completely imitate mobile IP.

User authentication in any communications system is very important. Providing communications security in Mobile IP service is no exception. When a mobile node gives correspond with another node, the package data will travel through the Internet [10, 19, 26, 27]. To prevent the communication contents of this package from being intercepted, tampered with, counterfeited or destroyed over the Internet, transmitted data must be encrypted [25, 30, 31, 32].

1.1 Objectives

There are three goals of this study as follows.

- to discuss the characteristics and requirements for the Mobile IP environment;
- to discuss practical and secure points of the existing methods;
- to propose a new secure communication protocol involving methods to improve the existing methods for the Mobile IP environment;

We will briefly discuss the requirements of the mobile IP services before developing the new secure communication techniques.

User Authentication

In general, a server must confirm the personal identity of a user before providing service. The user login process can determine if this user is a legal user of the system. If the person log on is verified as a legal user, the system offers the service. The Mobile IP user authentication protocol is different from the general user service authentication protocol. Three of identification levels are required in mobile Internet IP; the mobile node must authenticate with the foreign agent, the foreign agent with the home agent and the mobile node with the home agent. Users must be verified at all three authentication levels in order to receive service. The mobile node identity authentication process prevents illegal users from using the replay attack to acquire system services.

Confidentiality and Integrity

Both of the mobile and foreign agents are communicate through wireless wave and Internet. The wireless data is easy to intercept and steal. The Internet is an

open network. Data deliver through the Internet can be easily intercepted or falsified. Therefore, insuring the confidentiality and integrity of communications data are very important in a Mobile IP environment.

Locate Anonymous

An anonymous location is important requirement in a mobile communication system. This requirement is generality provided in a cell-phone system. This requirement provide mobile user with communications with other nodes, but the correspondent nodes cannot determine the senders' location. This requirement was previously not provided in Mobile IP services.

A simple and secure mobile IP user authentication and secure communication schemes have the following requirements:

1) The current mobile IP communication architecture must not change.
2) The mobile node hardware is simple and does not require complicated calculations.
3) The system must not increase the number of times that communication data must be exchange.
4) All communication data must be encrypted to insure communication confidentiality.
5) Provide the corresponding location of anonymous users in a Mobile IP environment.

In this research, we focused on security for mobile IP services shown in Figure 2.

2 Our Scheme

There are three steps in our scheme: mobile node registration, mobile node authentication, and tunneling. We introduce these steps in the following sub-sections.

2.1 Mobile Node Registration in the Mobile IP System

When a mobile node is added to the Mobile IP system, the home agent will allocate the new mobile node a permanent identity address (home address), secret key and a nonce. This data is consigned to the mobile user on a secure channel. After the user registration step, the mobile user stores a message $(MN_{HM}, S_{MN-HA}, nonce)$ in privacy. The home agent stores a message $(MN_{HM}, S_{MN-HA}, nonce)$ for each mobile node. Here, S_{MN-HA} denotes a secret key shared by mobile node and home agent.

2.2 Mobile Node Authentication Method in Mobile IP System

When a mobile node wants to communicate with a correspondent node, the mobile node must be authenticated. The mobile node authentication protocol is shown in Figure 3.

The proposed protocol proceeds as follows:

- S1. $Agent \rightarrow MN$: M_1
  where $M_1 = Advertisement, FA_{id}, MN_{COA}, N_{FA}$
  The first time the foreign agent will send an advertisement message flag with FA address FA_{id}, mobile node's care of address MN_{COA} and random a nonce N_{FA} to the mobile node.
- S2. $MN \rightarrow FA$: $HAid$, MN_{HM}, MN_{COA}, N_{FA}, $S_{MN-HA} < M_2 >$ where $M_2 = Request$, FA_{id}, HA_{id}, MN_{HM}, MN_{COA}, N_{HA}, N_{MN}, N_{FA}
  When the mobile user receives the agent advertisement. The mobile node will issue a registration request with the actual address MN_{HM}, HA address HA_{id}, HA's nonce N_{HA}, FA address FA_{id}, mobile user's care of address MN_{COA}, FA's nonce N_{FA} and random a nonce N_{MN}, uses the secret key S_{MN-HA} to encrypt message with HA address HA_{id}, mobile user's actual address MN_{HM}, mobile user's care of address MN_{COA}, with the FA's nonce N_{FA} sent to FA.
- S3. $FA \rightarrow HA$: M_3 where $M_3 = K_{HA}\{K_{FA}^{-1} << S_{MN-HA}\{M_2\}, MN_{HM} >>\}$, $S_{MN-HA}\{M_2\}$, HA_{id}, $Cert_{FA}$
  When FA receives the message, it will validate N_{FA}. If the nonce is lawful, the FA will use HA's public key encryption message $S_{MN-HA}\{M_2\}$ and MN_{HM} after digital signature of message $S_{MN-HA}\{M_2\}$ and MN_{HM} generated using FA's private key. Finally, the message is sent to HA with FA address HA_{id} and FA's certificate. If the nonce isn't lawful, FA will ignore the registration message and return an error message to the mobile node.
- S4. $HA \rightarrow FA$: M_4 where $M_4 = K_{FA}\{K_{HA}^{-1} << M_5, S_{sk}, N_{FA}, MN_{COA} >>$, M_5, S_{sk}, N_{FA}, $MN_{COA}\}$, FA_{id}, $Cert_{HA}$ and $M_5 = S_{sk}\{Reply, Result, FA_{id}, HA_{id}, MN_{HM}, N'_{HA}\}$, $S_{MN-HA}\{S_{sk}, S'_{MN-HA}, N'_{MN}\}$
  1) HA receives the authentication message. The first time it checks if the FA's certification $Cert_{FA}$ is lawful, and uses its private key and FA's public key to decrypt and verify the message integrity and validity. If the message integrity and validity are lawful, it will proof the message contents, otherwise it will abort the registration request and return an error message to FA. The follow steps are HA proof the message method. First, the HA use the mobile node address MN_{HM} find the common secure key to decrypt message M_2. Second, the HA compares messages M_1 and M_2. If the contexts have unity, the nonce N_{MN} is validated in the database with the received message and the care of address MN_{COA} corresponding to the mobile

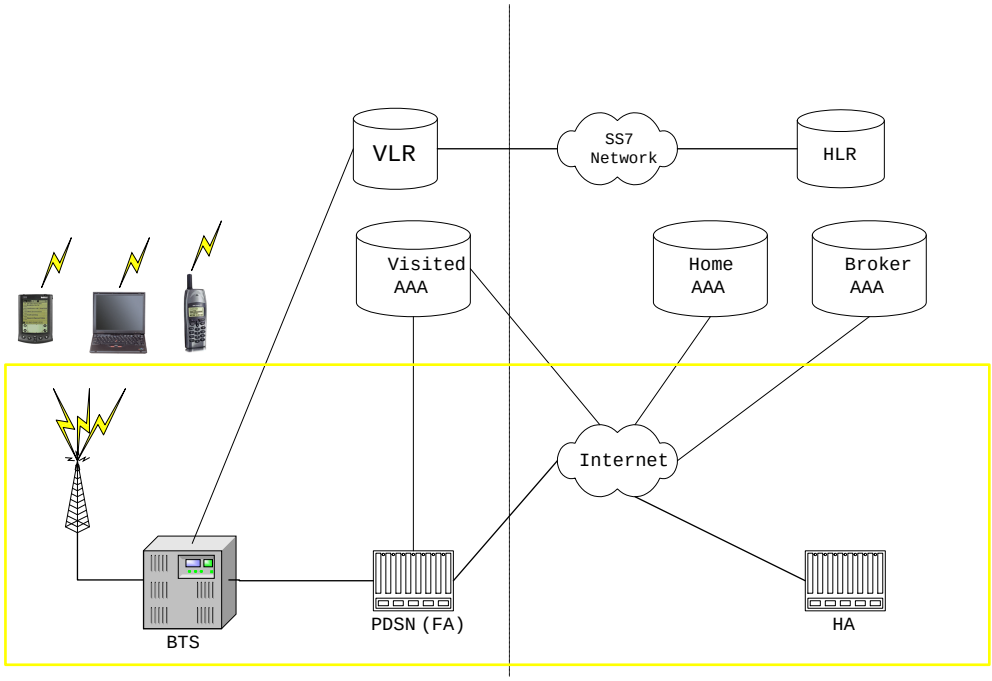


Figure 2: Research scope in this article

node is saved after the message is effective. If HA verify the message have any error, HA will return an error message to the FA and abort the registration procedure.

2) If the authentication messages are lawful, the HA produces a new random nonce N'_{HA}, new secure key S'_{MN-HA} (session key), temp secure key S_{sk} (temp key) and save in database. HA response Reply, Result, FA_{id}, HA_{id}, MN_{HM}, N'_{HA} use the session key encryption and response S_{sk}, S'_{MN-HA}, N_{MN} use old secure key S_{MN-HA} encryption. The HA sends message M_5, temp key S_{sk}, nonce N_{FA} and mobile node care of address MN_{COA} and use the HA private key to generate the message's digital signature and use FA's public key encryption to send to FA with FA's address FA_{id} and HA's certificate.

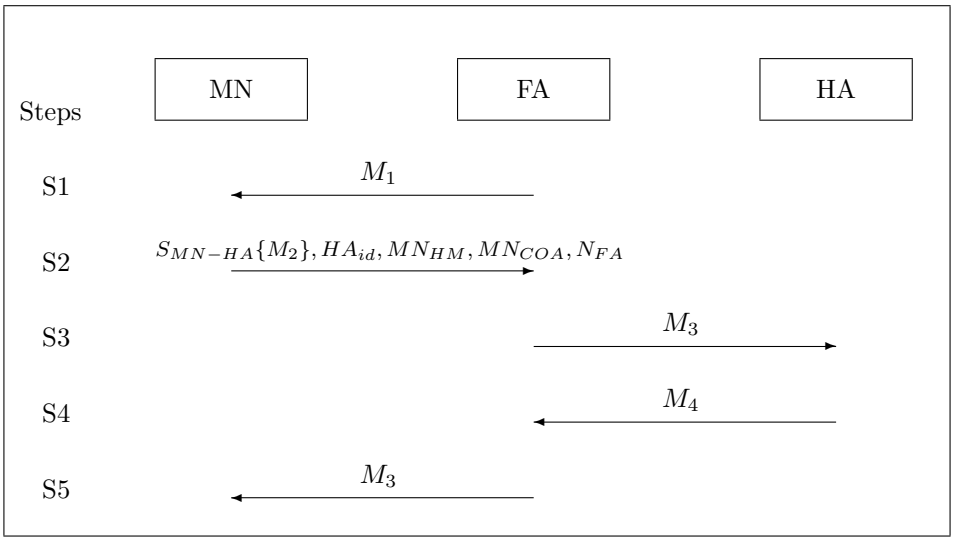
- S5. $FA \rightarrow MN$: M_5 where $M_5 = S_{sk}\{Reply, Result, FA_{id}, HA_{id}, MN_{HM}, N'_{HA}\}, S_{MN-HA}\{S_{sk}, S'_{MN-HA}, N'_{MN}\}$
When FA receives the message, it uses its' private key to decrypt the message. It then uses HA's public key to decrypt and verify the message's integrity and validity with HA's certificate. Afterward, FA will check N_{FA} unity with it send's nonce N_{FA} after foregoing proof. If the nonce is lawful, FA uses the temporary secure key S_{sk} to the decrypt message and check the registration result. If the register result is successful; the FA will send M_5 to the corresponding mobile node. After the test and verification, the FA will deliver the message with mobile node's encrypted message using the common temp secure key (temp key).

- S6. MN
When the mobile node receives the message, it uses the secret key S_{MN-HA} decrypt the new secure key (session key) S'_{MN-HA} and temp secure key (temp key) S_{sk} with the mobile node's nonce N_{MN}. If the received nonce is equal to the previously sent nonce, the mobile user uses the temporary secure key S_{sk} to decrypt the registration result. If the authentication succeeds, the mobile user saves the new nonce N'_{HA} and new secure key (session key) S'_{MN-HA} and the temp secure key (temp key) S_{sk}. In the next communication the mobile node will use the new secure key S'_{MN-HA} communicate with HA and use the temporary secure key to communicate with the FA. Finally, the mobile node uses the new nonce N'_{HA} for next registration authentication.

The mobile node uses the tunneling technique to receive data after the registration authentication. Our proposed method only changes the message length. The other operation actions and the number of communications are not changed.

2.3 Security Analysis

Advertisement message include a nonce N_{FA}, it can prevent the replay attack. The HA and FA use public key system, and provider the non-negation requirement. The identity authentication nonce N_{MN} and the encrypt key



$M_1 = Advertisement, FA_{id}, MN_{COA}, N_{FA}$

$M_2 = Request, FA_{id}, HA_{id}, MN_{HM}, MN_{COA}, H_{HA}, N_{MN}, F_{FA}$

$M_3 = K_{HA}\{K_{FA}^{-1} << S_{MN-HA}\{M_2\}, MN_{HM} >>, S_{MN-HA}\{M_2\}, MN_{HM}\}, HA_{id}, Cert_{FA}$

$M_4 = K_{FA}\{K_{HA}^{-1} << M_5, S_{sk}, N_{FA}, MN_{COA} >>, M_5, S_{sk}, N_{FA}, MN_{COA}\}, FA_{id}, Cert_{HA}$

$M_5 = S_{sk}\{Reply, Result, FA_{id}, MN_{HM}, N'_{HA}\}, S_{MH-HA}\{S_{sk'}, S'_{MN-HA}, N_{MN}\}$

Figure 3: The proposed registration protocol

S_{MN-HA} between the HA and MN can only be used one time. This protocol prevents the guess and replay attack. The temporary secure key (temp key) can only be used on one location after the registration procedure between the FA and MN. This provides the data confidentiality between the FA and MN over the air. Only the sender or receiver can decrypt the data in our proposed method. Deliver data are encrypt in our method, it can provider data confidentiality and prevent TCP splicing attack.

3 Comparisons

In this new protocol, the mobile terminal computing power and communication data security are considered. The data is communicated in the wireless environment between the FA and MN. Exposing wireless communication data in the air is very dangerous. We Therefore use a temporary secure key (temp key) S_{sk} to encrypt the communications data and the temporary secure key distributed by the HA. Only the FA and MN can read the data in the wireless environment. The power usage in the mobile node is kept to a minimum to prevent communication data leaks in the wireless environment. The FA and HA communicate through the Internet environment. Our proposed method uses encryption technique provides data confidentiality and corresponding location anonymity.

3.1 Comparisons with Other Schemes

Our method endeavor only secure key systems for mobile node. The functions analysis is shown in Table 1. The secure key systems use a few computations and power consumption for mobile node. It can increase the use time of the mobile node battery.

When data deliver through Internet and wireless environment is dangerous. So, the data confidentiality is very important. The data confidentiality is analyzed in Table 2. Our method is provider batter confidentiality that others methods.

The identity authentication nonce N_{MN} and the encrypt key S_{MN-HA} between the HA and MN can only be used one time. This protocol prevents the guess attack. The temporary secure key (temp key) can only be used on one location after the registration procedure between the FA and MN. This provides the data confidentiality between the FA and MN over the air. Only the sender or receiver can decrypt the data in our proposed method. The attack prevent analysis show in Table 3. Our method can prevent the attacks and provider data confidentiality.

Our method provide the mobile node locate anonymous. The characteristic is vary important in mobile environment, but previously research are not provider the function in Mobile IP environment. Our encrypt session key is random independent by HA. It can reduce incur the old key conjecture attack. There is provide non-repudiation between FA and HA in our method. The cryptanalysis is show in Table 4.

Table 1: Functions analysis

	MN-FA	FA-HA	MN-HA
Traditional method	None	None	Secure key + MAC
Jacob's method	Digital signature	Digital signature	Digital signature + Secure key
Suf & Lam's method	Session key	Digital signature	Secure key
Hor & Hsi's method	None	Digital signature	Session key
Our method	Temp key	Digital signature + Public key	Session key

3.2 Advantages

There are some advantages in our design framework:

1) The mobile node hardware requirements are simple: Only a secure key is needed to encrypt the communication data between the MN and the correspondent node. The mobile node does not use a public key system or complex computations, so the mobile node does not increase the overhead.

2) Prevent replay attack:
Our method uses the nonce in each step to verify each message. The reply message has message pairs, which prevents the replay attack.

3) The guess and TCP splicing attack are prevented:
Our method uses the session key to encrypt all communications data between a correspondent pair. The encrypted communications data and encryption key prevents the guess and TCP splicing attack.

4) Our method use cryptology techniques to encrypt identity related data of the mobile node. The identity data could not be exposed in the Internet environment. The correspondent node can connect with the mobile node, but cannot know the mobile node location.

5) provide non-repudiation:
The FA and HA use a public-key cryptosystem. No common session key needs to be saved for each correspondent node and a digital signature is used to verify each data delivery. The correspondents cannot repudiate one another. Only one mobile node can have the correct authentication data. If it passes through the authentication procedure, it cannot repudiate the resource.

Our method have the foregoing advantages, but it have some shortcoming, too. Our method deliver data is more than previously methods in communication process. Otherwise, the security carefully can't equally system simplify. So when request high security grade, our method is better than previously methods.

Table 2: Data confidentiality analysis

	MN-FA	FA-HA	MN-HA
Traditional method	No	No	Yes
Jacob's method	No	No	Yes
Suf & Lam's method	Yes	No	Yes
Hor & Hsi's method	No	No	Yes
Our method	Yes	Yes	Yes

4 Conclusions

The user authentication is an important research in many applications. Some applications need to authenticate a legal user before providing services. The user authentication scheme prevents an illegal user to access resources. In this research, we have proposed the user authentication schemes for mobile node in Mobile IP services.

The mobile wireless technique is becoming more mature. Nowadays, Internet can transit over to wireless mobility. Since, traditional Internet protocols cannot be used with mobile systems, mobile IP follows a logical train of thought in development. Mobile IP may incur the replay or TCP spicing attack during the registration process.

Sufatrio and Lam proposed a minimal public key based framework to prevent the replay attack. Horng and Hsieh proposed a session key based framework to prevent the TCP spicing attack but the framework must be executed using complex computations [14]. These methods are not adequate for the Mobile IP Internet.

Mobile communications systems identify the location of the anonymous correspondent. Therefore, we propose a new method to provide greater protection. This method uses a session key to encrypt all communications data during the communications process. The mobile node is not required to make complex computation and requires only minimal hardware and software in our method. Our proposed method can provide secure communications in Mobile IP environment.

References

[1] R. Atkinson, "RFC 1825- Security architecture for the Internet protocol," *IETF RFC*, pp. 1–27, Aug. 1995.

Table 3: Attack prevent analysis

	Reply Attack	TCP Splicing Attack	Guess Attack
Traditional method	No	No	No
Jacob's method	Yes	Yes	No
Suf & Lam's method	Yes	No	No
Hor & Hsi's method	Yes	Yes	Yes
Our method	Yes	Yes	Yes

Table 4: Cryptanalysis

	Locate Anonymous	Session Key Independent	FA-HA Non-repudiation
Traditional method	No	No	No
Jacob's method	No	No	Yes
Suf & Lam's method	No	Yes	Yes
Hor & Hsi's method	No	No	Yes
Our method	Yes	Yes	Yes

[2] R. Atkinson, "RFC 1826- IP authentication header," *IETF RFC*, pp. 1–16, Aug. 1995.

[3] R. Atkinson, "RFC 1827- IP Encapsulating Security Payload (ESP)," *IETF RFC*, pp. 1–27, Aug. 1995.

[4] M. J. Beller, L. F. Chang, and Y. Yacobi, "Privacy and authentication on a portable communications system," *IEEE Journal on Selected Areas in Communications*, vol. 11, pp. 821–829, Aug. 1993.

[5] P. Bhagwat, C. E. Perkins, and S. Tripathi, "Network layer mobility: an architect and surcey," *IEEE personal Communication*, pp. 54–64, Jun. 1996.

[6] C. Boyd and A. Mathuria, "Key establishment protocols for secure mobile communications: a selective Survey," *in Proceeding of Information Security and Privacy: Third Australasian Conference, ACISP'98*, Jul. 1998.

[7] G. Cho and L. F. Marshall, "An efficient location and routing scheme for mobile computing environments," *IEEE Journal on Selected Areas in Communications*, vol. 13, pp. 868–879, Jun. 1995.

[8] C. Déchaux and R. Scheller, "What are GSM and DCS," *Electrical Communication*, pp. 118–127, 2nd Quarter 1993.

[9] ETSI. "Digital European cordless telecommunications common interface part 7: security features,". Tech. Rep. Version 5.03, European Telecommunications Standards Institute, ETSI, May 1991.

[10] A. Giovanardi and G. Mazzini, "Transparent mobile IP: an approach and implementation," in *Procedings of IEEE Globecom'97*, pp. 1861–4865, 1997.

[11] A. Giovanardi and G. Mazzini, "Optimization routing and security features for transparent mobile IP," in *IEEE Global Telecommunications Conference*, vol. 2, pp. 880–885, 1998.

[12] A. Hac and L. Guo, "Mobile host protocols for the Internet," in *IEEE 50th Vehicular Technology Conference (VTC 1999)*, vol. 5, pp. 2790 –2794, 1999.

[13] B. Harris and R. Hunt, "TCP/IP security threats and attack methods," *Computer Communication*, pp. 885–897, 1999.

[14] J. S. Hsieh and G. B. Horng, "Mobile IP of registration protocol security discuss," in *Proceedings of 2000 workshop on Internet and Distributed Systems*, pp. 306–315, May 2000.

[15] M. S. Hwang, J. K. Wey, and W. P. Yang, "A new service for digital mobile communications," in *IEEE APCCAS'94*, Taipei, Dec. 1994.

[16] A. Inoue, M. Ishiyama, A. Fukumoto, and T. Okamoto, "Secure mobile IP using IP security primitives," in *Sixth IEEE Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*, pp. 235 –241, 1997.

[17] C. H. Lee, M. S. Hwang, and W. P. Yang, "Enhanced privacy and authentication for the global system for mobile communications," *Wireless Networks 5*, pp. 231–243, July 1999.

[18] A. Lo, W. Seah, and E. Schreude, "An efficient DECT-Mobile IP interworking for mobile computing," in *Proceedings of IEEE 51th Vehicular Technology Conference (VTC 2000)*, vol. 1, pp. 274 –278, 2000.

[19] P. J. McCann and T. Hiller, "An Internet infrastructure for cellular CDMA networks using mobile IP," *IEEE Personal Communications*, vol. 7 4, pp. 26–32, Aug. 2000.

[20] R. Molva, D. Samfat, and G. Tsudik, "Authentication of mobile users," *IEEE Network, Special Issue on Mobile Communications*, vol. 8, pp. 26–32, 1994.

[21] A. Myles, D. B. Johnson, and C. E. Perkins, "A mobile host protocol supporting route optimization and

authentication," *IEEE Journal on Selected Areas in Communications*, vol. 13 5, pp. 839 –849, Jun. 1995.
[22] C. E. Perkins, "RFC 2002- IP mobility support," *IETF RFC*, pp. 1–97, Oct. 1996.
[23] C. E. Perkins, "RFC 2003- IP encapsulation within IP," *IETF RFC*, pp. 1–18, Oct. 1996.
[24] C. E. Perkins, "Mobile IP," *IEEE Communication Magazine*, pp. 84–99, May 1997.
[25] C. E. Perkins, *Mobile IP design principles and practices*. Addison Wesley, Oct. 1997.
[26] C. E. Perkins, "Mobile IP networking through Mobile IP," *IEEE Internet Computing*, vol. 2, pp. 58–69, 1998.
[27] C. E. Perkins, "Mobile IP joins forces with AAA," *IEEE Personal Communications*, vol. 7, no. 4, pp. 59–61, Aug. 2000.
[28] C. E. Perkins and K. Y. Wang, "Optimized smooth handoffs in mobile IP," in *Proceedings of IEEE International Symposium on Computers and Communications*, pp. 340 –346, 1999.
[29] T. F. La Porta, L. Salgarelli, and G. T. Foster, "Mobile IP and wide area wireless data," in *Wireless Communications and Networking Conference*, vol. 3, pp. 1528–1532, 1999.
[30] R. L. Rivest, "The MD5 message-digest algorithm," *IETF RFC 1321*, Apr. 1992.
[31] B. Schneier, *Applied cryptography (second edition)*. John Wiley and Sons, 1996.
[32] William Stallings, "*Cryptography and network security: Principles and Practie*," 1996.

Cheng-Ying Yang was born in Taipei on October 13, 1964. He received the M.S. degree in Electronic Engineering from Monmouth University, New Jersey, in 1991, and Ph.D. degree from the University of Toledo, Ohio, in 1999. He is a member of IEEE Satellite & Space Communication Society. Currently, he is employed as an Assistant Professor at National Formosa University, Taiwan. His research interests are performance analysis of digital communication systems, error control coding, signal processing and computer security.

Cheng-Yeh Shiu received the M.S. in Information Management from Chaoyang University of Technology, Taichung, Taiwan, Republic of China, in 2003. His current research interests include cryptography, information security, and network security. Now, he work about GSM/GPRS/UMTS core network related item in taiwanmobile LTD.