論文2003-40TC-4-3

차세대 이동통신 네트워크의 Virtual Home Environment 구조에 적용 가능한 3자간 상호 인증 프로토콜

(Extended 3-Party Mutual Authentication Protocols for the Virtual Home Environment in Next Generation Mobile Networks)

鄭 鍾 民 *, 李 九 淵 **, 李 庸 ***

(Jong-Min Jeong, Goo-Yeon Lee, and Yong Lee)

요 약

개인 서비스 환경의 이동성과 전역 로밍을 위해 제안된 VHE(virtual home environment) 구조에서 가입자는 홈 망에서와 동일한 서비스를 방문 망에서도 제공받을 수 있게 된다. 가입자에게 서비스 이동성을 제공하기 위해서는 홈 망에 보관되어 있는 사용자 데이터와 서비스 로직이 방문 망으로 전달되어야 한다. 이 경우 사용자 프로파일과 서비스 로직은 보안에 민감한 정보를 포함하고 있으므로 통신의 신뢰성을 유지하기 위해서 모든 엔티티 사이의 상호 인증 절차가 요구된다. 이를 위해 본 논문에서 3G/4G 망의 VHE에 적용 가능한 3자간의 상호 인증 절차를 제안하고 분석한다.

Abstract

In the virtual home environment (VHE), which was proposed to offer global roaming and personal service environment portability, user's profiles and service logics are conveyed from home network to visited network to provide services at the visited network. Because user's profiles and service logics may contain confidential information, some procedures for mutual authentication among entities for offering confidence are needed. For these issues, we propose and analyze three 3-party mutual authentication protocols adaptable to the VHE in 3G ; password based mutual authentication protocol, mutual authentication protocol with CHAP and key exchange and mutual authentication protocol with trusted third party.

Keywords : Mutual authentication, VHE, CHAP, 3G, AC, KDCI. INTRODUCTION

* 正會員, 江原大學校 컴퓨터情報通信工學科
(Dept. of Information and Telecommunications Kangwon National University)
** 正會員, 江原大學校 電氣電子情報通信工學部
(Dept. of Information and Telecommunications Kangwon National University)
*** 正會員, 韓國情報保護振興員 電子署名引證管理센터
(Korea Certification Authority Central Korea Information Security Agency)
※ This research was supported by the 2003 Sabbatical Research Program of Kangwo National University and BK21 project of Kangwon National University
接受日字:2002年10月25日, 수정완료일:2003年3月18日

Ⅰ. INTRODUCTION

The VHE, which was defined for personal service environment portability and global roaming service among different networks in 1999, has been an essential technology together with the intelligent network (IN) and the open service architecture (OSA) in 3G mobile networks. The VHE is a network capability that enables users visiting 3G networks to receive the same services offered to them at their home networks (HN)[1]. To realize the VHE, it has been raised considerations of not only an architectural design for networks but also a way to protect subscribers' profiles. To do this, authentications for each entity are indispensable. That is, from the standpoint of HN, it needs to identify whether the visited network (VN) that requests subscriber's profiles is really serving its user now.

Moreover, from the standpoint of users, it is required to confirm whether the VN has information really received from the subscriber's HN.

Until now, several implementation scenarios, which focused on control and logic elements of service about VHE, have been proposed. However researches for protection of subscribers' profiles and mutual authentications have not been performed yet.

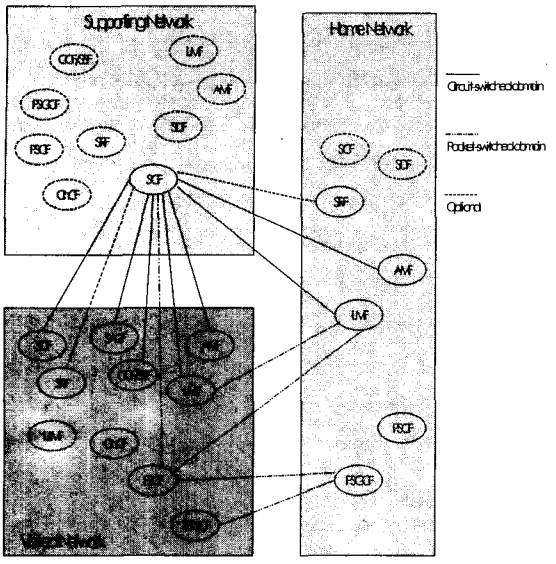
Accordingly, in this paper, we propose three mutual authentication protocols to protect profiles and to verify entities. We also analyze the security intensity of the protocols. Moreover, because it is essential to work together with the existing VHE scenarios, we investigate the feasibility of integration of the proposed protocols with the VHE scenarios of ITU-T Recommendation Q.1711.

Ⅱ. RELATED WORKS

There are two ways of descriptions for the VHE scenarios within Q.1711. One is the direct home command (DHC) and the other is the relay service control (RSC). DHC scenario relies on the service control function (SCF) and service switching function (SSF) interface and calls for invocation of service logic to query instruction/information to the SCF of supporting network (SN). RSC scenario relies on the SCF-SCF interface and calls for invocation of service logic via the SCF of HN or SCF of VN to query instruction/information to the SCF of SN.

Besides, M. Torabi suggested 5 scenarios by role assignments and locations of service control in HN and VN; shadow home service, relay home service/relay service control (RSC), shared service control, direct home command and actual home service[3].

- **Shadow Home Service** : Service profiles, data, service logic and some necessary information needed to serve a visiting user are temporarily shadowed /downloaded from the subscriber's HN to the VN where the service process is done.
- **Relay Home Service/Relay Service Control** : The queries of SSF of VN for instruction and information are relayed through SCF of the VN to SCF of HN. The responses of the SCF of the HN are reversely relayed back to the SSF of the VN. That is, this scenario calls for capability of the SCF of the VN for relaying queries.
- **Shared Service Control** : This scenario is a variation of the relay scenario. In this scenario, service logics are prearranged and shared by HN and VN. The user service is co-processed by HN and VN through the operation of joint service control point (JSCP).
- **Direct Home Command** : To control transaction, queries are directly transferred to SCF of HN. In this scenario, SCF of VN does not perform any relaying or downloading/shadowing of the user service profiles and service logics.
- **Actual Home Service** : In this scenario, an "end-to-end signaling association" is established between the mobile terminal's call control agent function and HN to support both call and service. That is, HN acts as a proxy agent for the subscriber to manage VN.



AMF : Authentication management function
CCF : Call control function
CnCF : Connection control function
LMF : Location management function
PSCF : Packet service control function
PSGCF : Packet service gateway control function
SACF : Service access control function
SCF : Service control function
SDF : Service data function
SRF : Specialized resource function
SSF : Service switching function
UIMF : User identification module function

그림 1. 서포팅 네트워크 개념이 포함된 3G 네트워크 구조
Fig. 1. 3G network architecture

In another research of M.Torabi, the case that some services of VN are not registered at subscriber's profiles is considered. In the case, a concept of supporting network (SN) is introduced and located in the midway between VN and HN. And he proposed an extended RSC scenario[4]. <Figure 1> shows the 3G network architecture adding a concept of SN.

Finally, Harmann explained a way to provide an agent-based service based on the adaptive profile manager and the virtual address book for the VHE[5].

Ⅲ. PROPOSED PROTOCOLS

In this paper, we propose 3 protocols about mutual authentication among VN, HN and MS (mobile station) in the VHE. In the three protocols, we consider authentication and confidentiality separately. For the confidentiality between HN and VN, public key algorithm is used.

However, in the case of MS, we do not use it because of the possible limitation of computing power. According to authentication methods, we present 3 protocols. The first protocol is the password based mutual authentication protocol. In this protocol, each network has to maintain password tables of other networks. When an authentication is requested, the transferred password is compared with the one in the password tables. The second protocol is the mutual authentication protocol with key exchange and CHAP (challenge handshake authentication protocol). In this protocol, a session key is shared by a key exchange protocol between two networks that want to authenticate each other. After that, mutual authentication is completed using CHAP. The third protocol is the mutual authentication protocol with trusted third party. In this protocol, each entity totally relies on a trusted third party to authenticate the others.

M1: MS -> VN : $\{MS\_ID, VN\_ID, n1\}K_{MS/HN}$, MS_TID, HN_AID
M2: VN -> HN : $\{\{MS\_ID, VN\_ID, n1\}K_{MS/HN}, VN\_Pass, VN\_ID, MS\_ID, n2\}K_{HN}+$
M3: HN -> VN : $\{HN\_ID, HN\_Pass, n3\}K_{VN}+$

-- HN/VN mutual authentication is complete --

M4: HN -> VN : $\{MS\_ID, \{MS\_Pass, n4\}K_{MS/HN}, n5, \{VN\_ID, MS\_ID, n4\}K_{MS/HN}\}K_{VN}+$
M5: VN -> MS : $\{VN\_ID, MS\_ID, n4\}K_{MS/HN}$
M6: MS -> VN : $\{MS\_Pass, n4\}K_{MS/HN}$

-- MS/VN mutual authentication is complete

MS_ID : Identification of a mobile station
n1, n2, n3, n4, n5 : Nonces, used for time limit
MS_TID : Temporary ID of MS
VN_Pass : Password of VN
MS_Pass : Password of MS
VN_ID : Identification of visited network
HN_ID : Identification of home network
HN_AID : Alias of HN
HN_Pass : Password of HN

그림 2. 패스워드 기반의 상호 인증 프로토콜
Fig. 2. Password based mutual authentication protocol.

M1: MS -> VN : {MS_ID, VN_ID, n1}$K_{MS/HN}$, MS_TID, HN_AID
M2: VN -> HN : {{MS_ID, VN_ID, n1}$K_{MS/HN}$, VN_ID, MS_ID, n2, COUNT1}K_{HN}+
M3: HN -> VN : {pubValue$_{HN}$, HN_ID, n3}K_{VN}+
M4: VN -> HN : {pubValue$_{VN}$, VN_ID, n4}K_{HN}+
M5: HN -> VN : {Rand1, n3} $K_{VN/HN}$
M6: VN -> HN : {{Rand1, COUNT2}$K_{VN/HN}$

-- HN/VN mutual authentication and key exchange is complete --

M7: HN -> VN : {{MS_ID, Rand2, $K_{MS/VN}$, n4}$K_{MS/HN}$, VN_ID, $K_{MS/VN}$, Rand2, n5}$K_{VN/HN}$
M8: VN -> MS : {MS_ID, Rand2, $K_{MS/VN}$, n4}$K_{MS/HN}$

-- MS/VN mutual authentication will be executed with CHAP --

pubValue$_{HN}$: HN's public value used for key exchange. It is equal to $\alpha^{X_{HN}} \bmod q$ in Diffie-Hellman key exchange algorithm. (X_{HN} is HN's random private value. α and q are global public value)

pubValue$_{VN}$: VN's public value used for key exchange. It is equal to $\alpha^{X_{VN}} \bmod q$ in Diffie-Hellman key exchange algorithm. (X_{VN} is VN's random private value)

Rand1, Rand2 : Random challengers

COUNT1, COUNT2 : Sequential integer values

그림 3. CHAP와 교환방식 기반의 상호 인증 프로토콜
Fig. 3. Mutual authentication protocol with CHAP and key exchange.

1. Password Based Mutual Authentication Protocol

<Figure 2> shows the procedure of password based mutual authentication protocol. We denote a public key of entity X by K_X+, a private secret key of entity X by K_X-, a shared secret key between entities X and Y by $K_{X/Y}$ and a message M encrypted with a key K by {M}K. In the protocol, we assume that the shared secret key between MS and HN is already established. At message 1(M1), $K_{MS/HN}$ which is a shared secure key between MS and HN and was generated at the subscription time of MS to HN is used for HN to identify MS. MS_TID is a temporary identification of MS and is pre-assigned by VN at the registration time of MS to VN. HN_AID is an alias of HN. All networks maintain alias tables about other network's identifications, so VN can match HN_AID with its real HN. M2 and M3 show that VN and HN send their passwords encrypted and authentications of each other are made using the passwords.

At M4, HN sends to VN the password of MS ({MS_Pass, n4}$K_{MS/HN}$), VN_ID and MS_ID ({VN_ID, MS_ID, n4}$K_{MS/HN}$) encrypted with the shared secret key between MS and HN. After storing the {MS_Pass, n4}$K_{MS/HN}$, VN forwards the {VN_ID, MS_ID, n4}$K_{MS/HN}$ to MS at M5. Then MS extracts n4 and generates {MS_Pass, n4}$K_{MS/HN}$ with its password and sends the message to VN at M6. Finally, VN which received M6 compares it with the {MS_Pass, n4}$K_{MS/HN}$ stored at M4 and then authenticates MS. Also because only VN which was authenticated by HN can transfer M5, MS can also authenticate VN by decrypting the message.

2. Mutual Authentication Protocol with CHAP and Key Exchange

<Figure 3> shows the mutual authentication protocol with CHAP and key exchange. The functions of M1 and M2 are similar to the M1 and M2 of the password based mutual authentication protocol. COUNT fields in M2 and M6 are for preventing retransmission attacks. The value of COUNT2 correlates with the value of COUNT1. COUNT2 field in M6 is used for HN to confirm that the entity which sent M6 is the VN which sent M2. At M3 and M4, a key exchange protocol (in the <figure 3>, Diffie-Hellman (DH) key exchange protocol is given as an example) is executed. At M3, HN selects a random number X_{HN} and calculates pubValue$_{HN}$ with the random number. Then HN encrypts the value with the public key of VN and sends it to VN. At M4, VN selects a random number X_{VN} and calculated pubValue$_{VN}$ with the random number. Then VN encrypts the value with the public key of HN and sends it to HN. After M3 and M4, HN and VN can get their shared secret key calculated from the *PubValues*. In the case of DH key exchange protocol as in the <figure 3>, the shared secret is calculated by

$$\begin{aligned} K_{VN/HN} &= (pubValue_{VN})^{X_{HN}} \bmod q \\ &= (\alpha^{X_{VN}} \bmod q)^{X_{HN}} \bmod q \\ &= (\alpha^{X_{VN}})^{X_{HN}} \bmod q \\ &= (\alpha^{X_{HN}})^{X_{VN}} \bmod q \\ &= (pubValue_{HN})^{X_{VN}} \bmod q \end{aligned}$$

M1: MS -> VN : {MS_ID, VN_ID, n1}$K_{MS\cdot HN}$, MS_TID, HN_AID

Case with AC

$M2_{AC}$: VN -> HN : {{MS_ID, VN_ID, n1}$K_{MS\cdot HN}$, {VN_ID}$K_{AC\cdot VN}$, MS_ID, VN_ID, n2, AC_ID}K_{HN}+

$M3_{AC}$: HN -> AC : {AC_ID, VN_ID, {VN_ID}$K_{AC\cdot VN}$, HN_ID,n3}$K_{AC\cdot HN}$

$M4_{AC}$: AC -> HN : {AC_ID, VN_Token, {AC_ID, HN_Token}$K_{AC\cdot VN}$, n4}$K_{AC\cdot HN}$

$M5_{AC}$: HN -> VN : {{AC_ID, HN_Token}$K_{AC\cdot VN}$, MS_Token, {MS_ID, VN_Token}$K_{MS\cdot HN}$, VN_ID, n5}K_{VN}+

-- HN/VN mutual authentication is complete --

Case with KDC

$M2_{KDC}$: VN -> HN : {{MS_ID, VN_ID, n1}$K_{MS\cdot HN}$, {VN_ID}$K_{KDC\cdot VN}$, MS_ID, VN_ID, n2, KDC_ID}K_{HN}+

$M3_{KDC}$: HN -> KDC : {KDC_ID, VN_ID, {VN_ID}$K_{KDC\cdot VN}$, HN_ID,n3}$K_{KDC\cdot HN}$

$M4_{KDC}$: KDC -> HN : {KDC_ID, $K_{VN\cdot HN}$,{KDC_ID, $K_{VN\cdot HN}$}$K_{KDC\cdot VN}$, n4}$K_{KDC\cdot HN}$

$M5_{KDC}$: HN -> VN : {{KDC_ID, $K_{VN\cdot HN}$}$K_{KDC\cdot VN}$, MS_Token, {MS_ID, n6, VN_Token}$K_{MS\cdot HN}$, VN_ID, n5}K_{VN}+

-- HN/VN mutual authentication is complete --

M6. VN -> MS : {MS_ID, n6, VN_Token}$K_{MS\cdot HN}$

-- MS/VN mutual authentication is complete --

AC_ID : Identification of authentication center

KDC_ID : Identification of key distribution center

HN_Token : Indicator that HN is authenticated by trusted third party

VN_Token : Indicator that VN is authenticated by trusted third party or HN

MS_Token : Indicator that MS is authenticated by HN

그림 4. 신뢰기관을 이용한 상호 인증 프로토콜
Fig. 4. Mutual authentication protocol with trusted third party.

At M7 and M8, HN generates a session key, $K_{MS/VN}$ which is supposed to be used as a shared secret key between VN and MS and distributes the key to VN and MS. After M7 and M8, MS and VN will execute CHAP similar to M5 and M6. Through the CHAP, the shared secret key ($K_{MS/VN}$) is confirmed and mutual authentication between HN and VN will be completed. At M7 and M8, Rand2 is a challenger for CHAP between MS and VN. Generally, challengers are generated by one of two entities which want authentication and normally are exposed to the others. However, in this protocol HN generates Rand2 and sends it encrypted for protecting it from exposure. After M8, MS and VN execute CHAP with the Rand2 for mutual authentication between MS and VN.

3. Mutual Authentication Protocol with Trusted Third Party

<Figure 4> shows the mutual authentication protocol with trusted third party. We consider two cases for authentication between VN and HN. One is to totally rely on authentication center (AC). We call it 'case with AC'. The other is to use a session key that is acquired from key distribution center (KDC). We call it 'case with

KDC'. Therefore <figure 4> is divided into two parts according to the cases. In the protocol, authentication between HN and VN are carried out through the trusted third party first. Then the authentication between VN and MS is executed using the token which HN issues. In the protocol, we also assume that each network and AC/KDC share their own shared secret key.

The function of M1 is similar to the M1 of the password based mutual authentication protocol and mutual authentication protocol with CHAP and key exchange protocol. At M2 and M3, VN and HN request authentication from AC ($M2_{AC}$ and $M3_{AC}$) or distribution of session key from KDC ($M2_{KDC}$ and $M3_{KDC}$). The trusted third party can authenticate HN and VN by the shared secret keys. At M4, AC sends authentication indicators (tokens) to HN ($M4_{AC}$) or KDC sends a session key to HN ($M4_{KDC}$). At M5, HN forwards the authentication indicator (HN_token) to VN ($M5_{AC}$) or the session key to VN ($M5_{KDC}$). M5 also includes another tokens (VN_token, MS_token) encrypted with the shared secret key KMS/HN for authentication between VN and MS. After M5, VN authenticates MS by identifying MS_token. At M6, VN sends the authentication indicator (VN_Token) encrypted with KMS/HN which is received from HN to MS. After decrypting the authentication indicator, MS completes the mutual authentication between MS and VN.

Ⅳ. ANALYSIS OF PROPOSED PROTOCOLS

1. Analysis of Operation Structure

For convenience, we call the password based mutual authentication the first protocol, call mutual authentication protocol with CHAP and key exchange the second protocol and call the mutual authentication protocol with trusted third party the third protocol. In the first protocol, all networks must maintain other networks' password tables. When networks are generated or removed, it is necessary to process registrations or withdrawals of passwords of the networks. Also the boundary of responsibility of networks to preserve password tables must be defined. In the second protocol, key exchange protocol should be predefined among networks. Therefore, it should be considered which secure key exchange algorithms are selected and how long the exchanged session keys are used before updating them.

In the third protocol, an authorized third party authenticates entities. Therefore, all networks are relieved of a load of maintaining password tables and exchange of session keys. Of course, the responsibilities are imposed on the third party. Therefore, bottleneck may occur. Also it is required to define message procedures between networks and the trusted third party and the scope of authority of the trusted third party. In that each network and AC/KDC shares a secret key, the two cases show resemblance. However, in the "case with AC", authentication totally depends on AC and after authentication, secure communications between HN and VN can continue using public key encryption algorithms if there is not any additional session key exchange procedure. On the other hand, in the "case with KDC", after receiving the session key from KDC, the networks must execute challenge-response procedure for the proof of possession of the session key and secure communication between HN and VN can be achieved using symmetric encryption algorithms with the session key.

2. Security Analysis

(1) *Authentication* : In the three protocols described in this paper, HN can authenticate MS by decrypting M1 encrypted with KMS/HN successfully. In the second protocol, if key exchange is securely executed by key exchange protocol, we can assert that mutual authentication between HN and VN is accomplished. In the third protocol, As long as shared secret keys between networks and trusted third party are not exposed, secure mutual authentication among entities can be possible.

We consider the mutual authentication between MS and VN. In the first protocol, since authentication messages are encrypted with $K_{MS/HN}$ and K_{VN^+}, only intended MS and VN can decrypt them, which results in mutual authentication between MS and VN. At the second and the third protocols, HN which was mutually authenticated with VN sends the session key or token encrypted. Only intended MS and VN can begin mutual authentication by decrypting them.

(2) *Entity Privacy* : Using MS_TID and HN_AID at M1, actual identifications of MS and HN does not appear in the messages transmitted at air interface, which is a good prevention against traffic analysis attack. Also, all the messages between HN and VN are encrypted with their shared secret key or public keys. This means that entity privacy is guaranteed.

(3) *Prevention against Retransmission* : Nonces within most messages include time related information. Therefore, they are used to check the term of validity of the messages. In some messages, sequential COUNT value fields are used. Initially an entity locally stores $COUNT_x$ value and sends it. When the entity receives a message including $COUNT_y$ value as a response, it compares it to the stored $COUNT_x$ value. Then the entity can check whether the received message is not retransmitted and normally continuous.

(4) *Disguise Prevention* : VN_ID encrypted with $K_{MS/HN}$ at M2 is used for HN which is mutually authenticated with VN to ascertain that the VN is

currently really serving the MS. Because VN cannot generate or modify the {MS_ID, VN_ID, n1}$K_{MS/HN}$, HN can confirm, after decrypting this information, that the VN which requests authentication has authority. After receiving M5 in the first protocol, M8 in the second protocol and M6 in the third protocol, MS can make sure, by decrypting the massages encrypted with the key $K_{MS/HN}$, that the messages from VN are originated from its HN. This means that disguise prevention is provided.

3. Integration with VHE Scenarios

The VHE scenarios in Q.1711 focused on the operational structures between HN and VN from the viewpoint of MS. However, 3 party mutual authentication protocols we propose in this paper are designed considering the positions of all the entities. Therefore there may be some disagreements when integrating the proposed protocols with the VHE scenarios in Q.1711. However if we concentrate on the standpoint of MS, the proposed protocols can be integrated with the VHE scenarios. In the first protocol, since HN sends the password of MS to VN for authentication of the MS, it is the same structure as M. Torabi's shadow home service. However, when we compare it with the VHE scenarios within Q.1711, it can be combined with RSC scenario since some processing of SCF of VN is required. In the second protocol, because it uses AMF (authentication management function) function via SCF of VN for processing $\{K_{MS/VN}\}K_{MS/HN}$ received from HN, it can be applied to the RSC scenario. In the third protocol, MS uses the token received from HN for authentication of VN. Even if it is transferred via VN, it could be said that it is directly acquired from HN. Therefore it can be applied to the DHC scenario.

V. CONCLUSION

In this paper, we dealt with the mutual authentication protocols that are inevitably required among entities in the VHE. Currently, studies of VHE focus on elements of service logic and locations of service control. However, in order to realize personal service portability, subscribers' confidence in security of VHE services is necessary.

For these issues, we proposed three mutual authentication protocols among HN, VN and MS in this paper; the password based mutual authentication protocol, the mutual authentication protocol with CHAP and key exchange and the mutual authentication protocol with trusted third party. We also did security analysis of the proposed protocols and discussed adaptability of the protocols to the VHE scenarios in Q.1711. The study in this paper will be a motive for researches on VHE to expand to the area of personal information protection with the technical functions and procedural scenarios.

REFERENCE

[1] "3rd Generation Partnership Project: The Virtual Home Environment (3G TS22.121 Ver 3.1.0)", 3GPP Technical Spec., 1999.

[2] "Network functional model for IMT2000", ITU-T Recommendation Q.1711, Mach 1999.

[3] M. Torabi, Rolfe E.Buhrke, "Third Generation Mobile Telecommunications and Virtual Home Environment", Bell Lab Tech. Journal, 1998.

[4] M. Torabi, "A Shift in the Mobile Network Service Provisioning Paradigm", Bell Lab Tech. Journal, 2000.

[5] J. Hartmann, C. Gorg, P. Farjami, "Agent Technology for the UMTS VHE Concept", ACM/IEEE MobiCom'98, Workshop on Wireless Mobile Multimedia, Dallas, United States, October 1998.

[6] R. Joos, A. Tripathi, "Mutual Authentication in Wireless Network", Technical Report, Department of Computer Science, University of Minnesota, June 4, 1997.

[7] C. Boyd, D. G. Park, "Public Key Protocols for

Wireless Communications", Proceedings of ICISC; 98, pp. 47~57, 1998.

[8] A. Aziz, W. Diffie, "Privacy and Authentication for Wireless Local Area Network", IEEE Personal Communications, Vol. 1, pp. 25~31, 1994.

[9] Y. Mu, V. Varadhrarajan, "On the Design of Security Protocols for Mobile Communications", ACISP'96 Conference, Pringer-Verlang, pp. 134~146, 1996.

[10] "3rd Generation Partnership Project : General Report on the Design, Specification and Evaluation of 3GPP Standard Confidentiality and Integrity Algorithms", 3GPP Technical Spec., 2000.

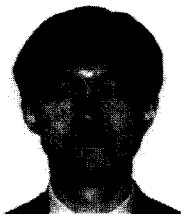
저 자 소 개

鄭 鍾 民(正會員)

1998년 : 강원대학교 정보통신공학과(학사). 2000년 : 강원대학교 컴퓨터정보통신공학과(석사). 2000년~현재 : 강원대학교 컴퓨터정보통신공학과 박사과정.

李 庸(正會員)

1997년 : 연세대학교 컴퓨터과학과(석사). 2001년 : 연세대학교 컴퓨터과학과(박사). 1993년~1994년 : 디지콤 정보통신 연구소 연구원. 2001년~현재 : 한국정보보호진흥원 전자서명인증관리센터 선임연구원.



李 九 淵(正會員)

1988년 : KAIST 전기및전자공학과(석사). 1993년 : KAIST 전기및전자공학과(박사). 1993년~1996년 : 디지콤정보통신연구소. 1996년 : 삼성전자. 1997년~현재 : 강원대학교 전기 및 전자공학부 부교수.