Wireless Personal Communications **16:** 35–50, 2001.

Authentication of Mobile Users in Third Generation Mobile Systems [⋆]

ZHI-JIA TZENG and WEN-GUEY TZENG
Department of Computer and Information Science, National Chiao Tung University, Hsinchu, Taiwan 30050, ROC
E-mail: tzeng@cis.nctu.edu.tw

Abstract. The goal of the third-generation mobile systems is to provide worldwide operation, enhance service capabilities, and improve performance over the second-generation mobile systems. In this paper, we propose an authentication procedure for third-generation mobile systems. The authentication procedure is a protocol suite consisting of two subprotocols: a certificate-based authentication (CBA) protocol and a ticket-based authentication (TBA) protocol. Only two parties, MS and VLR, are involved in executing our protocol. Our authentication procedure uses both public- and secret-key cryptosystems. Our authentication procedure not only provides uniform authentication across domains, but also reduces computational costs in the process of repeated authentication. We provide firm proof of our procedure's correctness.

Keywords: IMT-2000, third-generation mobile systems, GSM, authentication protocol, mobile computing.

1. Introduction

Third-generation mobile systems are currently being developed in Europe and worldwide, and are referred to as UMTS (Universal Mobile Telecommunications Systems) and IMT-2000 (International Mobile Tele-communication 2000), respectively. UMTS is regarded as a member of the IMT-2000 family. The goal of third-generation mobile systems [7, 16] is to provide worldwide operation, enhance service capabilities, and improve performance. In the security aspect, it aims to minimize the drawbacks of the second-generation mobile systems, such as insufficiency of location privacy, long-distance real-time signaling, and pre-arrangements between service providers and network operators, etc. In general, third-generation mobile systems intend to integrate all services and functionality of second-generation systems, including audio, video, speech, data, multimedia, supplementary services, roaming, virtual home environment, billing, and security. It may actually be considered as a multi-function, multi-service digital system.

Security and privacy are important issues in mobile computing. In order to provide wireless access and roaming across network and national boundaries, strong security measures are required for radio and network interfaces. Therefore, IMT-2000 defines comprehensive security requirements [16]. The security requirements for IMT-2000, similar to that of the second-generation mobile systems, are authentication, privacy and anonymity, confidentiality, integrity, authorization, and access control. IMT-2000 focuses on minimizing long-distance real-time signaling and bilateral pre-arrangements between service providers and network operators for international roaming for a long period of time. Additionally, in con-

[⋆] This work was supported in part by NSC grant 89-2212-E-009-052, Taiwan, ROC.

trast to the second-generation mobile systems that use unilateral authentication based on secret key cryptosystems, IMT-2000 makes it possible to base authentication on digital signatures or public-key schemes. IMT-2000's security functions include UIMF (user identification management function), ACF (authentication control function), and ADF (authentication data function).

Second-generation mobile systems have some weaknesses [14, 20, 22, 23]. Take the GSM system as an example. The GSM system involves three parties: MS, VLR, and HLR. When VLR authenticates MS, VLR communicates with HLR to get the information for authenticating the MS. HLR usually sends a set of authentication information to VLR in order to reduce contacting frequency with HLR. Furthermore, authentication of the GSM system is only unilateral, i.e., only VLR authenticates MS. GSM does not have the feature of location privacy since it may disclose a user's identity over the radio channel in some situations, such as in the registration procedure.

Our results. In this work, we propose an authentication protocol suite for third-generation mobile systems. The main contributions of the protocol suite are:

- Remedy the drawbacks of security of the second-generation mobile systems. For example, our authentication procedure involves only two parties, the mobile station (MS) and the network operator. Thus, the protocol suite reduces traffic between hosts, i.e., VLR does not communicate with HLR when executing the authentication procedure. Thus, the protocol minimizes long-distance real-time signaling. Furthermore, our protocol suite has attractive security functions, including key exchange, mutual authentication, location privacy, anonymity, avoidance of clone, and perfect forward secrecy. We summarize them in Table 1.
- Use the concept of the ticket to improve performance and maintain good properties. Because it uses a symmetric cryptosystem to generate tickets, the TBA protocol has better performance than the CBA protocol. Furthermore, the TBA protocol is a two-party protocol, which keeps good security properties.
- Propose a hierarchical architecture to support long-time international roaming. The architecture allows MS to roam into another domain and reside there for a long period of time. Based on the architecture, the network operator does not communicate with MS's home for authentication even for international roaming. Similarly, it can minimize bilateral prearrangements between service providers and network operators since they only exchange their certificates.
- We prove correctness of our protocol suite using BAN-type logic [5].

If PKI (public-key infrastructure) is established, we can easily integrate personal public-key certificates into our authentication procedure. Since most people will have public-key certificates in the near future, our authentication procedure has significant use in electronic commerce.

Since our CBA protocol uses public-key certificates for authentication and key exchange, its computational cost is higher than that using symmetric-key systems. Due to technological advancement, high-computing power and long-life batteries are a reality. For example, Motorola SLE44CR80S [17] microprocessor verifies an RSA signature of 1024-bit modulo in only 168 ms. Public-key operations will not be a burden for MS. On the other hand, our authentication procedure adopts some measures to reduce computing costs. For example, for repeated authentication, when an MS remains at the same VLR, we use symmetric-key

Table 1. Security functions

	CBA protocol	TBA protocol	IRCBA (International Roaming) protocol
Security Functions	Mutual authentication Key exchange Privacy and anonymity Avoidance of clone Data privacy Perfect forward secrecy	Mutual authentication Privacy and anonymity Data privacy Key exchange	Mutual authentication Key exchange Privacy and anonymity Avoidance of clone Data privacy Perfect forward secrecy

systems and tickets, inspired by Kerberos, for authentication and key exchange between MS and VLR.

1.1. Related Work

Some wireless communication protocols use the secret-key cryptosystem for authentication, such as GSM [22, 23] and IS-41 [14, 20]. The authentication of these systems is only unilateral. Furthermore, the user's identity and location are not anonymous. Protocols in [3, 15] also use the secret-key cryptosystem for authentication, but provide more security functions, such as identity confidentiality and mutual authentication. The above protocols involve three parties. That is, their authentication procedures need a third trusted server, such as HLR or the old VLR.

Some protocols [2, 6, 8, 10–12, 18, 24, 25] use hybrid schemes of public-key and secret-key schemes. Brown [4] discusses techniques for using the public-key and secret-key cryptosystems to get privacy and authentication in personal communication systems. CDPD [8] uses the Diffie–Hellman scheme to generate a session key. One advantage of CDPD is that it has a mechanism to detect a clone. For efficiency, some protocols [6, 18, 24, 25] let one MS directly communicate with another MS. These protocols provide secure channels between mobile users. In [2], there are three proposed hybrid schemes, MSR, IMSR, and MSR+DH. These three schemes involve two parties only. In contrast to other schemes, MSR and IMSR send the secret information to the network end in order to verify a user's legality. This is very insecure because a malicious operator may clone the user.

There are some proposed certificate-based protocols for wireless authentication [1, 13, 17]. The main merit of certificate-based protocols is that the traffic between VLR and HLR is minimized. When roaming across domain becomes more frequent, this shall dramatically reduce the frequency of long-distance signaling across domains. However, we should be careful about the use of certificates in authentication. Incorrect use of certificates in protocols may result in security flaws. For example, the protocols in [17] use a user's certificate as secret information. It is possible to clone users in this case.

Finally, some articles [9, 19, 26] that list security requirements for mobile computing discuss how to protect user identity and location.

1.2. Preliminaries and Model

In the following, we discuss certificate, ticket, and communication models.

Certificate. A certificate defined in X.509 [27] contains the user's public key and other information and a signature of that information by CA (Certificate Authority). For example, the equations below are certificates.

$$\mathrm{Cert_{MS}} = \{\mathrm{ID_{MS}}, \mathrm{KU_{MS}}, \mathrm{Date_{MS}}, \mathrm{L_{MS}}, (\mathrm{ID_{MS}}, \mathrm{KU_{MS}}, \mathrm{Date_{MS}}, \mathrm{L_{MS}})_{\mathrm{KR_{HLR}}}\}\,,$$

$$\mathrm{Cert_{VLR}} = \{\mathrm{ID_{VLR}}, \mathrm{KU_{VLR}}, \mathrm{Date_{VLR}}, \mathrm{L_{VLR}}, (\mathrm{ID_{VLR}}, \mathrm{KU_{VLR}}, \mathrm{Date_{VLR}}, \mathrm{L_{VLR}})_{\mathrm{KR_{HLR}}}\}\,,$$

$$\mathrm{Cert_{HLR}} = \{\mathrm{ID_{HLR}}, \mathrm{KU_{HLR}}, \mathrm{Date_{HLR}}, \mathrm{L_{HLR}}, (\mathrm{ID_{HLR}}, \mathrm{KU_{HLR}}, \mathrm{Date_{HLR}}, \mathrm{L_{HLR}})_{\mathrm{KR_{TC}}}\}\,.$$

$\mathrm{Cert_{MS}}$ represents the certificate of MS, $\mathrm{Cert_{VLR}}$ represents the certificate of VLR, and $\mathrm{Cert_{HLR}}$ represents the certificate of HLR, in which $\mathrm{ID_x}$ means the identity of entity X, $\mathrm{KU_x}$ is the public key of entity X, $\mathrm{Date_x}$ is the issue date of the certificate to X, and $\mathrm{L_x}$ is the lifetime. These data are signed by HLR (TC) using its private key $\mathrm{KR_{HLR(TC)}}$. Therefore, we can view HLR (TC) as CA. Furthermore, we can view TC as the global CA and HLR as a local CA. The public key of HLR (TC), stored in both the SIM card and VLR, is used for authentication between MS and VLR.

Ticket. Ticket is a MAC (message authentication code) of {TID, Date, L, (TID, Date, L) $\mathrm{K_{VLR}}$}, where $\mathrm{K_{VLR}}$ is the secret key of VLR, TID is the temporary identity for MS, "Date" is the issue date of the ticket, and L is the lifetime of the ticket. Only the user owning the secret key can make a ticket and verify the validity of the ticket. Therefore, VLR should save the secret key K. Here, $(\cdot)_{\mathrm{K_x}}$ means a secret-key cryptosystem.

Model. The mobile system contains MS, BS (base station), MSC (mobile switch center), and a mobility database. BS is further divided into two components: the base station controller and the base transceiver station for GSM, or radio port control unit and radio port for PACS. GSM's MSC connected to BS is a special switch tailored for mobile applications. MSC communicates with mobility databases to track the location of MS. The mobility databases store information about MS. In GSM, there are two types of mobility database: Home Location Register (HLR) and Visitor Location Register (VLR). When MS subscribes to the service of a mobile system, HLR creates a record that contains MS's directory number, profile information, current location, and validation period, etc. When MS visits a mobile telephony system other than the home system, VLR records the temporal information for MS. In registration and handoff, VLR communicates with HLR. A simplified architecture is shown in Figure 1, in which MS directly communicates with VLR. HLR acts as the CA. VLR is responsible for authenticating MS.

2. The Authentication Protocol Suite

Our authentication protocol suite consists of two parts: The certificate-based authentication (CBA) protocol and the ticket-based authentication (TBA) protocol (shown in Figure 2). The CBA protocol is used in registration, handover, and when the ticket is invalid. If MS stays at the same cell and requests the service several times, we use the TBA protocol.

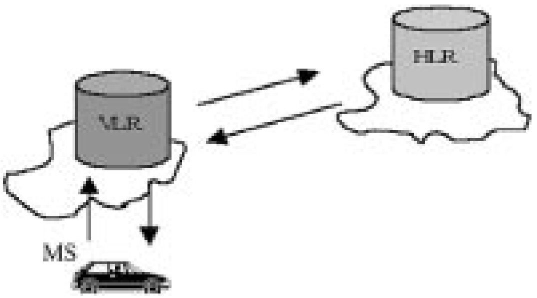

Figure 1. Authentication procedure in GSM.

2.1. The CBA Protocol

HLR issues the certificates Cert_{VLR} and Cert_{MS} to VLR and MS. MS stores the following data: Cert_{MS}, Cert_{HLR}, and KR_{MS}. VLR saves the following data: Cert_{VLR}, Cert_{HLR}, KR_{VLR}, and K_{VLR}. Our CBA protocol is described as follows.

1. Cert_Auth_Ask: Cert_{VLR}, R_1
2. Cert_Auth_Resp: $(\text{K}_s)_{\text{KU}_{\text{VLR}}}$, $(\text{Cert}_{\text{MS}}||(\text{R}_2||\text{R}_1)_{\text{KR}_{\text{MS}}})_{\text{K}_s}$
3. Cert_Auth_Ack: $(\text{Ticket}||(\text{R}_1||\text{R}_2)_{\text{KR}_{\text{VLR}}})_{\text{K}_s}$

(the session key: $\text{R}_1 \oplus \text{R}_2$)

- *Step 1:* When MS asks the service by the radio channel, VLR in which MS resides generates a Cert_Auth_Ask message, where R_1 is a random number. Then sends the message to MS. After receiving the message, MS should validate certificate Cert_{VLR} using the public key of HLR. If the certificate is valid, MS constructs a Cert_Auth_Resp message as follows. MS generates a temporal key K_s and a random number R_2, uses its private key KR_{MS} to sign $(\text{R}_2||\text{R}_1)$, the public key of VLR to encrypt K_s, and K_s to encrypt the message $(\text{Cert}_{\text{MS}}||(\text{R}_2||\text{R}_1)_{\text{KR}_{\text{MS}}})$, where "||" means concatenation. Then, MS sends Cert_Auth_Resp to VLR. In this step, MS remembers K_s, R_1, R_2, and Cert_{VLR}.
- *Step 2:* After receiving Cert_Auth_Resp from MS, VLR decrypts it to get K_s, Cert_{MS}, and $(\text{R}_2||\text{R}_1)_{\text{KR}_{\text{MS}}}$. Then, VLR verifies the validity of the certificate Cert_{MS} using the public key of HLR. If it is valid, MS uses its public key to recover $(\text{R}_2||\text{R}_1)$. Finally, VLR checks whether R_1 is the same as the one sent previously. If it is, MS convinces VLR that it is a legal subscriber. VLR saves R_2, constructs the Cert_Auth_Ack message as an acknowledgement, and generates the session key $\text{R}_1 \oplus \text{R}_2$. First, VLR generates a ticket for MS as follows. VLR generates TID, computes MAC $=$ (TID, Date, L)$_{\text{K}_{\text{VLR}}}$, signs $\text{R}_1||\text{R}_2$ using its private key, encrypts $(\text{Ticket}||(\text{R}_1||\text{R}_2)_{\text{KR}_{\text{VLR}}})$ using K_s as an acknowledgement, and sends it to MS.
- *Step 3:* After receiving Cert_Auth_Ack from VLR, MS opens the message to get the ticket and $(\text{R}_1||\text{R}_2)_{\text{KR}_{\text{VLR}}}$, recovers $(\text{R}_1||\text{R}_2)$ using the public key of VLR, and checks whether $(\text{R}_1||\text{R}_2)$ is correct. If it is correct, MS saves the ticket and generates the session key $\text{R}_1 \oplus \text{R}_2$. The ticket and the session key are then stored for later use in the repeated authentication protocol.

The protocol works as above, but if any error happens in any phase, the protocol fails and should restart from the first phase.

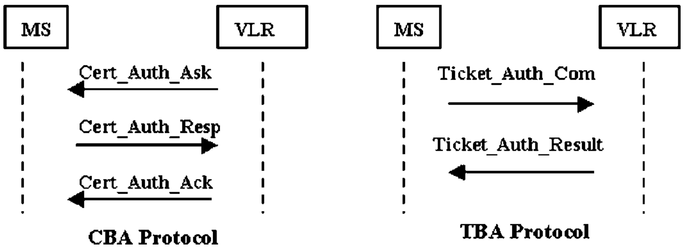

Figure 2. CBA and TBA protocol.

2.2. The TBA Protocol

In this protocol, we use the ticket in the authentication procedure. The TBA protocol is described as follows:

1. Ticket_Auth_Com: TID,$(\text{Ticket}||R_1)_{K_o}$
2. Ticket_Auth_Result: $(R_2||R_1)_{K_o}$

(the session key: $R_1 \oplus R_2$)

- *Step 1:* When MS calls another user or receives a call, it constructs a Ticket_Auth_Com message, where TID is a temporary identity, R_1 is a random number, and K_o is the old session key. Then, MS sends the challenge (command) to VLR. After receiving the challenge from MS, VLR gets K_o using its TID, decrypts the message to get the ticket, and verifies validity of the ticket. If it is valid, VLR believes that MS is a legal subscriber. VLR constructs a Ticket_Auth_Result as the response, where R_2 is a random number. Finally, VLR generates the new session key $R_1 \oplus R_2$. If the ticket is out of date, MS should run the CBA protocol to get the current ticket.
- *Step 2:* When receiving Ticket_Auth_Result from VLR, MS uses K_o to decrypt the message $(R_2||R_1)_{K_o}$ to get $(R_2||R_1)$. Then, MS verifies whether R_1 is correct. If it is, MS generates the new session key $R_1 \oplus R_2$. Otherwise, MS initiates another new authentication procedure.

In this protocol, we use the symmetric cryptosystem in authenticating MS. Therefore, the computational cost is lower and the efficiency is higher than that of the CBA protocol.

3. International Roaming

One of the goals of third-generation mobile communication systems is worldwide roaming. In this section, we demonstrate how our protocol authenticates a mobile user during international roaming. First, we describe the infrastructure of a worldwide telecommunication organization. Then, we enhance our protocol to support international roaming.

3.1. Infrastructure of Telecommunication Organization

The worldwide telecommunication organization is a hierarchical structure consisting of three levels (shown in Figure 3). The first level is the worldwide center of telecommunication, TC. When a telecommunication company wants to join the worldwide telecommunication organization, TC issues a certificate to the HLR of the telecommunication company. The second

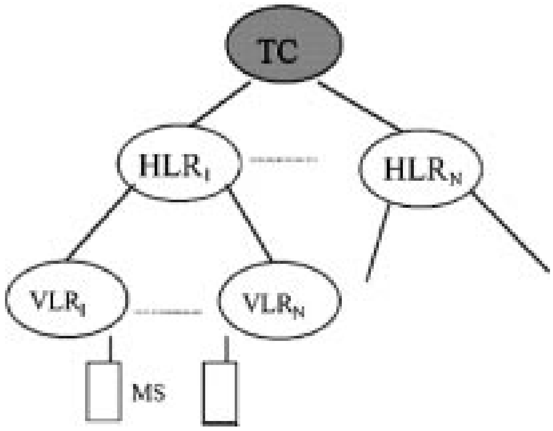

Figure 3. The infrastructure of telecommunication organization.

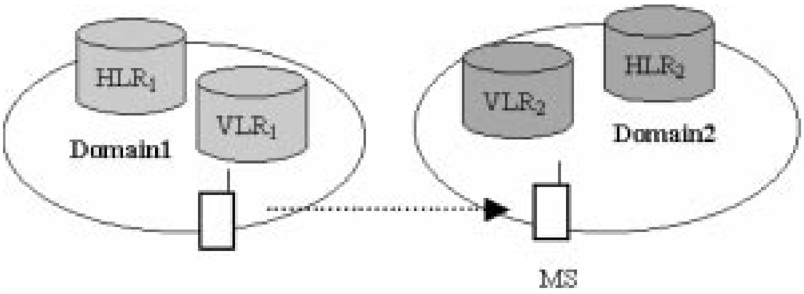

Figure 4. International roaming.

level is the local center, HLR. HLR is responsible for issuing a certificate to each of his VLRs. If a user asks for the service, HLR of the telecommunication company issues a SIM card with a certificate and other information to the user. The third level contains mobile stations and VLRs.

3.2. System Setup

When a mobile user asks for international roaming service, the telecommunication company sets up the related information in the SIM card of the user. The SIM card records three certificates: $\mathrm{Cert}_{\mathrm{MS}}$, $\mathrm{Cert}_{\mathrm{HLR}}$, and $\mathrm{Cert}_{\mathrm{TC}}$. For a telecommunication company that supports worldwide roaming, its VLRs record three certificates: $\mathrm{Cert}_{\mathrm{VLR}}$, $\mathrm{Cert}_{\mathrm{HLR}}$, and $\mathrm{Cert}_{\mathrm{TC}}$. Hence, the mobile user needs to record $\mathrm{Cert}_{\mathrm{TC}}$ for inter-domain roaming, while this is not necessary for intra-domain roaming.

3.3. The International Roaming Certificate-Based Authentication Protocol

The international roaming certificate-based authentication (IRCBA) protocol (shown in Figure 5) is compatible with the CBA protocol, but uses extra information. We assume that MS registers at domain D_1 with HLR_1 and roams into domain D_2 with HLR_2 (shown in Figure 4), where a domain means some telecommunication company. VLR_2 is controlled by HLR_2. In this protocol, if $\mathrm{Cert}_{\mathrm{HLR}_1}$ and $\mathrm{Cert}_{\mathrm{HLR}_2}$ are nulls, then the IRCBA protocol is equal to the CBA

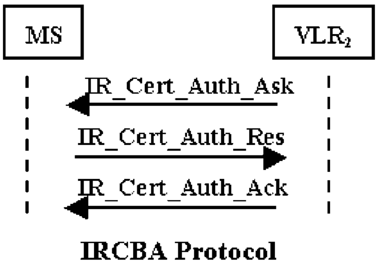

Figure 5. IRCBA protocol.

protocol. The IRCBA protocol is described as follows.

1. IR_Cert_Auth_Ask: $Cert_{HLR_2}$, $Cert_{VLR_2}$, R_1
2. IR_Cert_Auth_Resp: $(K_s)_{KU_{VLR_2}}$, $(Cert_{HLR_1}||Cert_{MS}||(R_2||R_1)_{KR_{MS}})_{K_s}$
3. IR_Cert_Auth_Ack: $(Ticket||(R_1||R_2)_{KR_{VLR_2}})_{K_s}$

(the session key: $R_1 \oplus R_2$)

- *Step 1:* When MS roams to D_2 and asks a service. If D_2 is not a member of the world-wide telecommunication organization, VLR_2 rejects the request of MS. Otherwise, VLR_2 should construct a IR_Cert_Auth_Ask message and send it to MS. The message consists of $Cert_{HLR_2}$, $Cert_{VLR_2}$, and a random number R_1. MS then uses certificate $Cert_{TC}$ to check the validity of $Cert_{HLR_2}$. If it is correct, MS uses certificate $Cert_{HLR_2}$ to verify $Cert_{VLR_2}$. If $Cert_{VLR_2}$ is valid, MS records $Cert_{VLR_2}$ and R_1. Then, MS generates a response message similar to that of the CBA protocol, but with $Cert_{HLR_1}$ added.
- *Step 2:* After receiving IR_Cert_Auth_Resp from MS, VLR_2 decrypts the message $(K_s)_{KU_{VLR_2}}$ to get K_s and uses K_s to decrypt the message to get $Cert_{HLR_1}$, $Cert_{MS}$, and $(R_2||R_1)_{KR_{MS}}$. VLR_2 verifies $Cert_{HLR_1}$ by the certificate $Cert_{TC}$. If $Cert_{HLR_1}$ is valid, VLR_2 uses $Cert_{HLR_1}$ to verify $Cert_{MS}$. If $Cert_{MS}$ is valid, then VLR_2 opens $(R_2||R_1)_{KR_{MS}}$ using the public key of MS to get R_2 and R_1. Then, VLR_2 checks if R_1 is correct. If it is, VLR_2 should construct an IR_Cert_Auth_Ack message and send it to MS. IR_Cert_Auth_Ack consists of a ticket and the signature of $(R_1||R_2)$. Then, VLR_2 produces a session key for MS.
- *Step 3:* In addition, when MS receives IR_Cert_Auth_Ack from VLR_2, it checks whether the message is valid. First, MS opens the message to get the ticket and $(R_1||R_2)_{KR_{VLR_2}}$ using K_s. Then, MS recovers $(R_1||R_2)$ using the public key of VLR_2. Furthermore, MS checks if $(R_1||R_2)$ is correct. If it is, it stores the ticket and generates and saves a session key.

If the protocol fails at any step, it terminates and restarts.

4. Protocols Analysis

We analyzed correctness of our protocols using BAN-Logic and security arguments.

4.1. BAN-Logic Analysis

First, we analyzed the CBA protocol to get the result shown in Theorem 1, which tells us that *VLR believes that* R_2 *is shared between MS and VLR* and *MS believes that* R_1 *is shared between VLR and MS* eventually. From the facts, VLR and MS can both compute a common session key via the shared R_2 and R_1. This fact guarantees correctness of the CBA protocol. In Theorem 2, we show that the TBA protocol is correct using an analogous argument. We state the two theorems here and put the proof in the Appendix.

THEOREM 1. *Using BAN-logic analysis of the certificate-based authentication protocol, we get the results:*

1. *MS believes* KU_{VLR}.
2. *VLR believes* KU_{MS}.
3. *VLR believes (VLR and MS share* R_2*).*
4. *MS believes (MS and VLR share* R_1*).*

THEOREM 2. *Using BAN-logic analysis of the ticket-based authentication protocol, we get the results:*

1. *VLR believes (VLR and MS share* R_1*).*
2. *MS believes (MS and VLR share* R_2*).*

The result of the IRCBA protocol is similar to that of the CBA protocol.

4.2. Security Analysis

Here, we discuss the security of the CBA protocol.

1. *Satisfying the security requirements of third-generation mobile systems*

   (a) Authentication and key exchange: Mobile users are authenticated by their certificates and the corresponding private key. Network operators are also authenticated by their certificates and private keys. Since obtaining private keys is almost impossible, our protocols provide mutual authentication between MSs and network operators. Moreover, by BAN-logic analysis, we get the results: VLR believes (VLR and MS share R_2) and MS believes (MS and VLR share R_1). Hence, both MS and VLR get the session key $R_1 \oplus R_2$.

   (b) Location privacy and anonymity: Since the identity of MS is not disclosed over the air, an attacker cannot track the location of a specific user. Furthermore, an attacker cannot obtain the identity of MS by comparing patterns of messages that are encrypted with session key K_s.

   (c) Data privacy: A random session key protects the messages communicating between MS and VLR; hence, a malicious third party gets nothing from the radio channel.

   (d) Perfect forward secrecy: Even if a session key is disclosed, due to the freshness of R_1 and R_2 in each session, a third party cannot compute old or new session keys.

   (e) Avoidance of cloning: In our protocol, VLR can get the certificate of MS. Since MS’s private key never leaves MS’s SIM card, VLR cannot clone MS. Furthermore, since MS’s certificate is not disclosed over the air, a malicious third party cannot get information about MS and thus cannot clone the user. In fact, cloning is possible only if one can clone MS's SIM card.

2. *Unforgability of VLR.* If a malicious third party wants to fake VLR, he needs to pass the authentication of the mobile users. Since message 1 in the CBA protocol is sent by clear text, the faked VLR can replay this message. After receiving message 2 from MS, the faked VLR needs the private key of the real VLR to open this message to get K_s. However, since the faked VLR does not have this key, he can only guess K_s. The success probability is one of $2^{|K_s|}$, where $|X|$ means the length of X. Although the faked VLR can get K_s by guessing, he also has to make $(R_1||R_2)_{KR_{VLR}}$. The success probability of making $(R_1||R_2)_{KR_{VLR}}$ is related to the length of this signature. For example, if the signature is done with 1024-bit RSA, the success probability is one of 2^{1024}. Therefore, the total success probability of faking VLR is one of 2^{1024}. Even though a malicious third party can get old R_1, R_2, and $(R_1||R_2)_{KR_{VLR}}$, he cannot apply the replay attack since R_2 is fresh.
3. *Unforgability of MS.* Suppose that an illegal MS got $Cert_{MS}$, R_1, R_2, and $(R_2||R_1)_{KR_{MS}}$. When VLR pages him with its certificate $Cert_{VLR}$ and a new R_1, the illegal MS cannot use the old data to convince VLR. If the length of $(R_2||R_1)_{KR_{MS}}$ is 1024 bits, then the illegal user has a success probability of one in 2^{1024} to try $(R_2||R_1)_{KR_{MS}}$ each time.
4. *Security of the session key.* In the CBA protocol, one can get R_1 because R_1 was sent in clear text, but only MS and VLR can get R_2. Since a random number XORing a given number is still random, we cannot get the information about the session key. By guessing a session key K, the success probability is one of $2^{|K|}$, where $K = R_1 \oplus R_2$.

Security functions in the IRCBA protocol are the same as those of the CBA protocol. In the TBA protocol, the security is based on the previous session key. If the previous session key was disclosed, an illegal MS could cheat the legal VLR or an illegal VLR could convince the legal MS. However, as the duration of this cheating is only the lifetime of the ticket, this will not be a serious security hole.

5. Discussion

5.1. Efficiency

There are two key properties in our protocol suite. These properties improve performance over second-generation mobile systems and satisfy the requirements of third-generation mobile systems.

- *Minimum long-distance real-time signaling.* In most cases, only MS and VLR participate in our protocol. Even in international roaming, HLR need not be involved. Thus, our protocol can support worldwide roaming with minimum long-distance real-time signaling.
- *Minimum bilateral pre-arrangements between service providers and network operators.* When HLR issues a SIM card, the SIM card contains the certificate of TC. Therefore, the service provider can support international roaming.

The storage costs and complexity of our protocols are summarized in Table 2. Storage costs mean the information needed in these protocols. The complexity includes the number of messages, the number of parties, and computational complexity.

There are four proposed schemes, UMTS/A, UMTS/B, UMTS/C, and UMTS/D for UMTS [21]. The last three schemes use asymmetric cryptosystems for authentication. In contrast to

Table 2. Complexity.

Protocols	CBA protocol		TBA protocol		IRCBA protocol	
items	MS	VLR	MS	VLR	MS	VLR
Storage cost	KR_{MS} $Cert_{MS}$ $Cert_{HLR}$	K_{VLR} KR_{VLR} $Cert_{VLR}$ $Cert_{HLR}$	A ticket K_{SK}	A ticket K_{SK}	KR_{MS} $Cert_{MS}$ $Cert_{HLR}$ $Cert_{TC}$	K_{VLR} KR_{VLR} $Cert_{MS}$ $Cert_{HLR}$ $Cert_{TC}$
Involved parties	Two parties: VLR and MS		Two parties: VLR and MS		Two parties: VLR and MS	
Message complexity	#Messages: 3		#Messages: 2		#Messages: 3	
Computational complexity	#Signature: 3/1[a] #Exponentiations: 5/3				#Signature: 3/1 #Exponentiations: 7/4	

[a] 3/1 means that VLR and MS do 3 private-key operations and MS alone does one private-key operation.

our CBA protocol, three proposed schemes of UMTS, UMTS/B, UMTS/C, and UMTS/D, need a trusted third party. Since our protocol does not need a trusted third center, entities in our protocols store more information. However, the number of messages exchanged between entities in our protocols is less than that of the UMTS schemes. Furthermore, our authentication protocol reduces the cost of international real-time signaling back to HLR of MS during international roaming.

5.2. Speed Up Handover Procedure

We use the TBA protocol to speed up the handover procedure. But, like GSM, the TBA-based handover protocol involves three parties. The TBA-based authentication procedure for handover is as follows:

1. MS → VLR_n: Ticket_Auth_Com.
2. VLR_n → VLR_o: VLR_n, TID.
3. VLR_o → VLR_n: K_o (or Fail).
4. VLR_n → MS: Ticket_Auth_Result.

where VLR_n denotes the new VLR and VLR_o denotes the old VLR. Note that if the old VLR crashes, this procedure will not work. Thus, the new VLR can ask the MS to run the CBA protocol for authentication.

5.3. Certificate Revocation Procedure

To revoke a user, each HLR should maintain a revocation list (CRL) [27]. When a subscriber would like to terminate the service or carelessly damages the SIM card, HLR should reclaim the SIM card and add the identity to the CRL. We need to check each time whether a certificate is valid when executing the CBA protocol.

6. Conclusions

In this paper, we propose an authentication protocol suite that satisfies the security requirements of third-generation mobile systems. In particular, this protocol suite possesses the properties of complete location privacy, mutual authentication, minimum long-distance real-time signaling, and minimum bilateral pre-arrangements between service providers and network operators. Our protocol suite is analyzed formally for security.

References

1. A. Aziz and W. Diffie, "Privacy and Authentication for Wireless Local Area Networks", *IEEE Personal Communications*, Vol. 1, No. 1, pp. 25–31, 1994.
2. M.J. Beller, L.F. Chang and Y. Yacobi, "Privacy and Authentication on a Portable Communication System", *IEEE Journal on Selected Areas in Communications*, Vol. 11, No. 6, pp. 821–829, 1993.
3. V. Bharghavan, "Secure Wireless LANs", in *Proceedings of ACM Conference on Computer and Communications Security*, 1994, pp. 10–17.
4. D. Brown, "Techniques for Privacy and Authentication in Personal Communication Systems", *IEEE Personal Communications*, Vol. 2, No. 4, pp. 6–10, 1995.
5. M. Burrows, M. Abadi and R.M. Needham, "A Logic of Authentication", *ACM Transactions on Computer Systems*, Vol. 8, No. 1, pp. 18–36, 1990.
6. U. Carlsen, "Optimal Privacy and Authentication on a Portable Communication System", *Operating Systems Review*, Vol. 28, No. 3, 16–23, 1994.
7. B.E. Fernandes, "Towards 3rd-Generation Mobile Systems", in *Proceedings of IEEE International Conference on Personal Wireless Communications '96*, 1996, pp. 507–512.
8. Y. Frankel, A. Herzberg, P.A. Karger, H. Krawczyk, C.A. Kunzinger and M. Yung, "Security Issues in a CDPD Wireless Network", *IEEE Personal Communications*, Vol. 2, No. 4, 16–27, 1995.
9. D. Kesdogan, H. Federrath, A. Jerichow and A. Pfitzmann, "Location Management Strategies Increasing Privacy in Mobile Communication", in *Proceedings of Information Systems Security Facing the Information Society of the 21st Century*, IFIP, 1996, pp. 39–48.
10. N.Y. Lee and T. Hwang, "On the Security of Park et al.'s Key Distribution Protocol for Digital Mobile Communications", in *Proceedings of the Seventh IEEE International Symposium on Personal Indoor and Mobile Radio Communications '96*, 1996, pp. 1248–1251.
11. H.Y. Lin and L. Harn, "Authentication in Wireless Communications", in *Proceedings of IEEE Global Telecommunications Conference, Including a Communications Theory Mini-Conference Technical Program Conference Record '93*, 1993, pp. 550–554.
12. H.Y. Lin and L. Harn, "Authentication Protocols for Personal Communication Systems", manuscript.
13. J. Liu and Y. Wang, "Authentication of Mobile Users in Personal Communication System", in *Proceedings of the Seventh IEEE International Symposium on Personal Indoor and Mobile Radio Communications '96*, 1996, pp. 1239–1242.
14. S. Mohan, "Privacy and Authentication Protocol for PCS", *IEEE Personal Communications*, pp. 34–38, 1996.
15. R. Molva, D. Samfat and . Tsudik, "Authentication of Mobile Users", *IEEE Network*, Vol. 8, No. 2, pp. 26–34, 1994.
16. R. Pandya, D. Grillo, E. Lycksell, P. Mieybegue, H. Okinaka and M. Yabusaki, "IMT-2000 Standards: Network Aspects", *IEEE Personal Communications*, Vol. 4, No. 4, pp. 20–29, 1997.
17. C.S. Park, "On Certificate-Based Security Protocols for Wireless Mobile Communication Systems", *IEEE Network*, pp. 50–55, 1997.
18. C. Park, K. Kurosawa, T. Okamoto and S. Tsujii, "On Key Distribution and Authentication in Mobile Radio Networks", in *Proceedings of Advances in Cryptology-Eurocrypt '93*, 1993, pp. 461–465.
19. S. Patel, "Location, Identity and Wireless Fraud Detection", in *Proceedings of IEEE International Conference on Personal Wireless Communications '97*, 1997, pp. 515–521.
20. "Weaknesses of North American Wireless Authentication Protocol", *IEEE Personal Communications*, Vol. 4, No. 3, pp. 40–44, 1997.

21. S. Putz, R. Schmitz and F. Tonsing, “Authentication Schemes for Third Generation Mobile Radio Systems”, in *Proceedings of the Ninth IEEE International Symposium on Personal Indoor and Mobile Radio Communications ’98*, 1998, pp. 126–130.
22. S.P. Shieh, C.T. Lin and J.T. Hsueh, “Secure Communication in Global Systems for Mobile Telecommunication”, in *Proceedings of the First Workshop on Mobile Computing*, 1994, pp. 136–142.
23. F. Stoll, “The Need for Decentralization and Privacy in Mobile Communications Networks”, *Computers and Security*, Vol. 14, No. 6, pp. 527–539, 1995.
24. M. Tatebayashi and D.B. Newman, “Key Distribution Protocol for Digital Mobile Communication Systems”, in *Proceedings of Advances in Cryptology-Crypto ’89*, 1989, pp. 324–333.
25. V. Varadharajan and Y. Mu, “Preserving Privacy in Mobile Communications: A Hybrid Method”, in *Proceedings of IEEE International Conference on Personal Wireless Communications ’97*, 1997, pp. 532–536.
26. J.E. Wilkes, “Privacy and Authentication Needs of PCS”, *IEEE Personal Communications*, Vol. 2, No. 4, pp. 11–15, 1995.
27. ITU-T Recommendation X.509, “The Directory: Authentication Framework”, 1993.

Appendix

THEOREM 1. *Using BAN-logic analysis of the certificate-based authentication protocol, we get the results:*

1. *MS believes KU_{VLR}.*
2. *VLR believes KU_{MS}.*
3. *VLR believes (VLR and MS share R_2).*
4. *MS believes (MS and VLR share R_1).*

Proof. In the inference of the BAN logic, we should have some basic assumptions:

1. MS believes $\overset{KU_{MS}}{\mapsto}$ MS
2. MS believes $\overset{KU_{HLR}}{\mapsto}$ HLR
3. VLR believes $\overset{KU_{VLR}}{\mapsto}$ VLR
4. VLR believes $\overset{KU_{HLR}}{\mapsto}$ HLR
5. VLR believes fresh (R_1)
6. MS believes fresh (R_2)
7. VLR believes fresh (D_{MS})
8. MS believes fresh (D_{VLR})
9. MS believes fresh (K_s)
10. MS believes (HLR controls $\overset{K}{\mapsto}$ VLR)
11. MS believes (VLR controls MS $\overset{R_1}{\leftrightarrow}$ VLR)
12. VLR believes (MS controls VLR $\overset{R_2}{\leftrightarrow}$ MS)
13. MS believes (MS $\overset{R_2}{\leftrightarrow}$ VLR)
14. VLR believes (VLR $\overset{R_1}{\leftrightarrow}$ MS)
15. VLR believes (HLR controls $\overset{K}{\mapsto}$ MS)
16. MS believes (MS $\overset{K_s}{\leftrightarrow}$ VLR)
17. VLR believes (MS controls VLR $\overset{K_s}{\leftrightarrow}$ MS)

First, we simplify the certificate as follows: $\mathrm{Cert}_{MS} = \{KU_{MS}, D_{MS}, (KU_{MS}, D_{MS})_{KR_{HLR}}\}$, $\mathrm{Cert}_{VLR} = \{KU_{VLR}, D_{VLR}, (KU_{VLR}, D_{VLR})_{KR_{HLR}}\}$ where D means the valid date.

(1) *From message 1:*

(1.1) MS sees (Cert_{VLR}, R_1) and assumption (2) holds. Hence, we get *MS believes HLR said* $\{KU_{VLR}, D_{VLR}\}$.
(1.2) From assumption (8) and the result of (1.1), we get *MS believes fresh* $\{KU_{VLR}, D_{VLR}\}$.
(1.3) From the result of (1.1) and (1.2), we get *MS believes HLR believes* KU_{VLR}.
(1.4) From assumption (10) and the result of (1.3), we get *MS believes* KU_{VLR}.

(2) *From message 2:*

(2.1) From assumption (3) and VLR sees $(\mathrm{K_s})_{\mathrm{KU_{VLR}}}$, we get *VLR sees K_s*.

(2.2) From (2.1) and VLR sees $(\mathrm{Cert_{MS}}||(\mathrm{R_2}||\mathrm{R_1})_{\mathrm{KR_{MS}}})_{\mathrm{K_s}}$, we get *VLR sees $(Cert_{MS}||(R_2||R_1)_{KR_{MS}})$*.

(2.3) From assumption (4) and the result of (2.2), we get *VLR believes HLR said $\{KU_{MS}, D_{MS}\}$*.

(2.4) From assumption (7) and the result of (2.3), we get *VLR believes fresh $\{KU_{MS}, D_{MS}\}$*.

(2.5) From the result of (2.3) and (2.4), we get *VLR believes HLR believes KU_{MS}*.

(2.6) From assumption (15) and the result of (2.5), we get *VLR believes KU_{MS}*.

(2.7) From the result of (2.6) and VLR sees $(\mathrm{R_2}||\mathrm{R_1})_{\mathrm{KR_{MS}}}$, we get *VLR believes MS said $(R_2||R_1)$*.

(2.8) From assumption (5) and the result of (2.7), we get *VLR believes fresh $(R_2||R_1)$*.

(2.9) From the result of (2.7) and (2.8), we get *VLR believes MS believes $(R_2||R_1)$*.

(2.10) From assumption (12) and the result of (2.9), we get *VLR believes (VLR and MS shares R_2)* by jurisdiction rule.

(3) *From message 3:* We simplify message 3 as $((\mathrm{R_1}||\mathrm{R_2})_{\mathrm{KR_{VLR}}})_{\mathrm{K_s}}$.

(3.1) From assumption (16) and MS sees $((\mathrm{R_1}||\mathrm{R_2})_{\mathrm{KR_{VLR}}})_{\mathrm{K_s}}$, we get *MS sees $((R_1||R_2)_{KR_{VLR}})$*.

(3.2) From the result of (1.4) and (3.1), we get *MS believes VLR said $(R_1||R_2)$*.

(3.3) From assumption (6) and the result of (3.2), we get *MS believes fresh $(R_1||R_2)$*.

(3.4) From the result of (3.2) and (3.3), we get *MS believes VLR believes (R_2)*.

(3.5) From assumption (11) and the result of (3.4), we get *MS believes (MS and VLR shares R_1)* by jurisdiction rule.

This completes the proof. □

THEOREM 2. *Using BAN-logic analysis of the ticket-based authentication protocol, we get the results:*

1. *VLR believes (VLR and MS share R_1).*
2. *MS believes (MS and VLR share R_2).*

Proof. In the inference of the BAN logic, we should have some basic assumptions:

1. MS believes (MS $\overset{\mathrm{K_o}}{\leftrightarrow}$ VLR)
2. VLR believes (VLR $\overset{\mathrm{K_o}}{\leftrightarrow}$ MS)
3. VLR believes fresh ($\mathrm{R_2}$)
4. MS believes fresh ($\mathrm{R_1}$)
5. VLR believes fresh (Ticket)
6. MS believes fresh (Ticket)
7. MS believes (VLR controls MS $\overset{\mathrm{R_2}}{\leftrightarrow}$ VLR)
8. VLR believes (MS controls VLR $\overset{\mathrm{R_1}}{\leftrightarrow}$ MS)
9. MS believes (MS $\overset{\mathrm{R_1}}{\leftrightarrow}$ VLR)
10. VLR believes (VLR $\overset{\mathrm{R_2}}{\leftrightarrow}$ MS)

Let us simplify message 1 to be $(\mathrm{Ticket}||\mathrm{R_1})_{\mathrm{K_o}}$ and message 2 to be $(\mathrm{R_2}||\mathrm{R_1})_{\mathrm{K_o}}$.

(1) *From message 1:*

(1.1) From assumption (2) and VLR sees $(\mathrm{Ticket}||\mathrm{R_1})_{\mathrm{K_o}}$, we get *VLR believes MS said $(Ticket||R_1)$*.

(1.2) From assumption (5) and the result of (1.1), we get *VLR believes fresh $(Ticket||R_1)$*.

(1.3) From the result of (1.1) and (1.2), we get *VLR believes MS believes $(Ticket||R_1)$*.

(1.4) By breaking a conjunction, we get *VLR believes MS believes R_1*.

(1.5) From the result of (1.4) and assumption (8), we get *VLR believes (VLR and MS shares R_1)*.

(2) *From message 2:*

(2.1) From assumption (1) and MS sees $(R_2||R_1)_{K_o}$, we get *MS believes VLR said* $(R_2||R_1)$.
(2.2) From assumption (4) and the result of (2.1), we get *MS believes fresh* $(R_2||R_1)$.
(2.3) From the result of (2.1) and (2.2), we get *MS believes VLR believes* $(R_2||R_1)$.
(2.4) By breaking a conjunction, we get *MS believes VLR believes* R_2.
(2.5) From the result of (2.4) and assumption (7), we get *MS believes (MS and VLR shares* R_2*)*.

This completes the proof. □

Wen-Guey Tzeng graduated from National Taiwan University in 1985. He received his Master's and Ph.D. degrees in 1987 and 1991, respectively, from the State University of New York at Stony Brook. He joined the Department of Computer and Information Science, National Chiao Tung University, in 1991. Dr. Tzeng's current research interests include cryptology and information security.

Zhi-Jia Tzeng graduated from Chinese Culture University in 1995. He received his Master’s degree in Computer and Information Science from National Chiao Tung University (NCTU) in 1997. He is currently a student at the Department of Computer and Information Science, working on his Ph.D. thesis in the area of information security. His research interests include communication security, network security, and secure protocol design.