Authentication Protocol for 3G Mobile Communication Systems

Chih-Hsing Lin[1†], Shih-Hsiung Twu[2]
[1] Institute of communications Engineering,
National Tsing Hua Univerity, Hsin-Chu, Taiwan, R.O.C
Email: lgs400@mhit.url.com.tw
[2] Department of Electrical Engineering
Chung Yuan Christian University, Chung-Li, Taiwan, R.O.C
Email:abraham@cycu.edu.tw
Telephone: 886-3-4563171ext.4823

Abstract

In this paper, we propose three new authentication mechanisms based on Asymmetric-key cryptosystems. The three authentication protocols are designed based on the security requirements of the third generation mobile communication systems, which is proposed by UMTS. The advantages of the Asymmetric-key cryptosystems are to solve a very important key management problem for key distribution. Besides, it can provide non-repudiation for the part of the transmitted data. Therefore, we adopt the Asymmetric-key cryptosystems to design our authentication schemes. The characteristic of the first schemes is that the User and the Network Operator have the public keys from each other, respectively. The characteristic of the second schemes is that we exploit the exchange of certificate to achieve the goal of exchange of the public key between the User and the Network Operator. The characteristic of the third schemes is that the Network Operator can obtain the public key from the User's certificate sent by Certificate Server. Similarly, the User can obtain the public key from the Network Operator that is sent be Certificate Server. The proposed authentication protocols for 3G mobile communication systems are analyzed to be correct to achieve the critical goals of the requirements of security and threats, and these protocols are efficient and effective because they are computationally low complexity and are simple but secure enough.

Keyword: *Authentication Protocol, 2G, 3G, Cryptography.*

1. Introduction

† Please address all correspondence related to this manuscript to Chih-Hsing Lin.

1.1 Authentication and UMTS

In recent years, mobile communication has been developed very rapidly. From the first-generation analog cellular mobile communication to the second-generation digital cellular mobile communication system, and the evolution to the third-generation mobile communication system until now, the usage of mobile and wireless communication systems has become more and more popular and convenient in spread worldwide. Nowadays, the technology of wireless mobile communication is not only beneficial for the customer better voice service but also extends to non-voice service such as image, internet service, computing data, e-mail, e-commerce and so on. People can communicate with others anytime and everywhere. However, people would be faced with the problem of serious security threats because of the openness of wireless communications. Therefore, to provide users a mechanism to protect the privacy between communicating parties is a very important issue. Since the transmission interface of the mobile communication system is through the radio channel, the actions of exchanging the private information of users or systems over insecure communication channels will increase potential threats of security, such as eavesdropping and masquerading legal users [1][2][3].

Authentication and confidentiality are essential security services, which aim to verify identities of users to prevent impersonation and to protect private communication against unauthorized eavesdropping, respectively [4].

The purpose of authentication process is to offer the communicating parties with certain guarantee so that they can identify each other. This process is called the user authentication.

Therefore, before a mobile user accesses mobile system services, he should be authenticated by the mobile system if the mobile system has an authentication protocol for transmission of a mobile user's secure information. Furthermore, if we want to transmit the private information to the mobile system by the air-interface, the content of the message can be canceled by encryption. Usage of encryption techniques, before a communication begins,

both parties should share a common session key in the secure communication.

On the 1st July 1991, the first public GSM was created, which is regarded as the second-generation mobile telecommunication. In the past ten years, GSM has become a truly universal mobile communication system. The second-generation systems mainly provide speech services. Hence, ten years later GSM has brought us onto the footprint of the third generation mobile communications system, which is Universal Mobile Telecommunication System (UMTS) in European [5]. The UMTS is designed to provide access to a wide rang of services. Many of these services and environments in which they will be used are already provided by various existing systems such as cordless, cellular, and satellite. UMTS will provide an integrated system in which users can access the desired service via uniform service access procedures irrespective of the environment they find themselves in. UMTS will provide service involving multimedia services, voice and non-voice service such as audio, video, speech, multimedia data and billing services, surfing the web, e-commerce, e-mail from a mobile user's terminal, electronic postcard, and so on. For the above descriptions of services, because of the various services operated in the hybrid mobile networks, some security issues new for the 3G should be considered particularly. There will be new and different providers of service such as content providers, data service providers, **HLR**-only service providers. 3G mobile systems will be positioned as the preferred means of communications for users. There will be active attacks on users. In active attacks, equipment is used to impersonate parts of the network to actively cause lapses in security. In passive attacks, the attacker is outside the system and listens in, hoping security lapses will occur. Non-voice services will be as important as, or more important than voice service, since the terminal will be used as a platform for e-commerce and other applications.

1.2 The Proposed Schemes

In this paper, we propose three new authentication mechanisms based on Asymmetric-key cryptosystems. The three authentication protocols are designed based on the security

requirements of the third generation mobile communication systems.

In most of the authentication protocols, generally the designer sends the all messages included in each transmission step. However it is difficult for us to understand the meaning and the relationship of these messages explicitly. Therefore, we use a representation of message flow to reconstruct the protocol in order to assist us to understand these messages and the relationship in each transmission step.

The advantages of the Asymmetric-key cryptosystems for key distribution solve a very important key management problem. Besides, it can provide non-repudiation for the part of the transmitted data. Therefore, we adopt the Asymmetric-key cryptosystems to design our authentication schemes. In our proposed authentication protocols, they have more secure than the symmetric-key cryptosystems, and we only use the exclusive OR operation to achieve authentication between the **User** and the **Network Operator**.

1.3 Organization of The Thesis

The thesis is organized as follows. In session 2, we introduce some technologies, which are concerned with the authentication protocols for mobile communication. The three new authentication mechanisms based on Asymmetric-key cryptosystems are described in session 3. In session 4, it includes the brief conclusions and discussions of the direction of our future works.

2. Review of the 2G Mobile Systems and Security Considerations for UMTS

2.1 GSM Authentication Protocol

When a mobile station attempts to access a network, which needs authentication process to ensure that the network service will not be obtained fraudulently. In the following, we review the original GSM authentication protocol [6].

GSM is the first mobile digital cellular system (second-generation mobile system) that providing a broad spectrum of communication capabilities and some digital service of

security such as user authentication, signaling traffic confidential, encryption, and roaming, etc..

In the **Challenge/Response** mechanism of GSM authentication protocol [7], each Mobile Station (**MS**) has a unique identity, which is an International Mobile Subscriber Identity (IMSI). IMSI is use to register and choose its own Home Location Register (**HLR**) to register. Between the user and the **HLR** with a share key of authentication, Ki. Therefore, in this protocol, it uses three security algorithms, A3, A8, A5, which were authentication function in the GSM system. The function A3 is a one-way function whose input is the challenge, a random number (RAND), form HLR. Between mobile station and HLR share key Ki, which generate MS's response to **HLR**'s **Challenge**, the simplicity that A3 is use to authentication MS. The function A8 is a one-way function, which uses RAND and Ki to generate a private key Kc. Kc is used for voice and data privacy. The function A5 is a symmetric-key crypto-function with key Kc, which encrypts transmitted data.

When the MS roams into the mobile system that is not controlled by **HLR**, the Visitor Location Register (**VLR**) will provide the communication service. The following steps in **Figure 1**, describe the workflow of security authentication protocol of GSM. We will use a presentation of message flow proposed by [8], which can assist us in recognizing what the meaning of each message involved in the authentication protocol.

(1) When a Mobile Station (**MS**) attempts to access service from the network, it will transmit IMSI to **VLR**. The **VLR** obtains the MS's IMSI and pass it to the **HLR**.

(2) **HLR** generates a random number RAND and uses the algorithm A3 to produces SRES and uses the algorithm A8 to produces Kc. Both A3 and A8 choose RAND and Ki as inputs. Then the **HLR** transmits Kc, RAND and SRES to the **VLR**. These messages are used in to authentication of the **MS**.

(3) The **VLR** receives these messages and forwards the RAND to MS as a **challenge** message. Then the **MS** uses the algorithm A3 to generate a corresponding message

SRES'.

(4) **MS** transmits a response message SRES' to **VLR**. When **VLR** receives SRES' from the **MS**, it can verify the SRES from the **HLR** and the SRES' from the **MS**. If they are the same, the **MS** is authenticated.

(5) **VLR** encrypts a temporary TMSI transmitting to **MS** by new session key, which is Kc. TMSI is a temporary identity to **MS** for confidentiality of **MS's** identity IMSI.

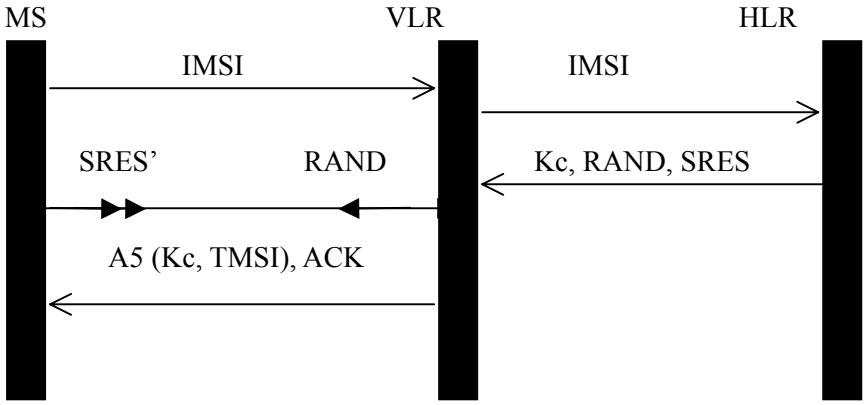

Figure 1. GSM authentication protocol

2.2 UMTS Authentication Protocol

Because the UMTS is building on the security of second-generation mobile system, therefore we will introduce the authentication protocol of the GSM mobile system and point out the weakness of the protocol [9].

In the following, we will introduce the authentication protocol of the UMTS. There are three authentication protocol schemes based on the results of the European ASPeCT (Advanced Security for Personal Communication Technologies) Project to be introduced [10] [11]. The three authentication protocol schemes are listed as follows:

(1) A Challenge/Response mechanism using symmetric key techniques (Royal Holloway College, London), (2) A public key based mechanism (Siemens), (3) A public key based mechanism (KPN). Siemens defines three authentication protocol schemes, which are called A, B, and C, respectively.

3. Three Proposed Schemes of Authentication Protocol

In this session, we use the representation of message flow proposed by [8] to propose three new authentication protocol schemes for the third generation mobile communication systems.

3.1 The First Scheme of Authentication Protocol

We use the public key cryptosystem approach to achieve the goals of authentication protocol such as authentication data, session key generation, secret data and mutual authentication, and so on.

The first protocol is applied to achieve the goals such as the mutual authentication of the **User** and the **Network Operator** and the establishment of shared session key K_S between them.

Prerequisites On Mechanism

Initially, the **Network Operator** identity is assumed to be known by the **User.** In addition,

(1) the **Network Operator** has a secret key SK_NO and a public key of the **User**- K_U .

(2) the **User** has a secret key SK_U and a public key of the **Network Operator**- K_N .

Description Of The Protocol

At first, we consider the first protocol that consists of three exchanged messages between the User and the Network Operator. The messages flows are indicated in the Figure 3.4 with M1, M2 and M3. In this protocol, the User has already registered with the Network Operator where it is roaming. The User and the Network Operator have already shared some information described above.

The notations in **Figure 2** are defined as follows:

- U: **User**. NO: **Network Operator**.

CA: **Certification Authority**. CS: **Certificate Server**.

- K_X ≡ X'S public key, where X= N, U, CS.

- K_S ≡ The session key is shard between the **User** and the **Network Operator**.

- data1||data2 : Concatenation data1 and data2 alongside the notation ||.

- $ID_X \equiv$ X'S identity, where X=CA, CS.

- $R_X \equiv$ A random number generated by X= U, N.

- $Auth_{AB} \equiv$ A authentication function between A and B.

- $AUTH_U = (R_N)_{Ks}$.

The Value of the $(R_N)_{KU}$ is to used authenticate the **User** to the **Network Operator**, generally this will be a challenge response value. The Value of the $AUTH_U$ is used to authenticate the **Network Operator** to the **User**, generally this will be a challenge response value.

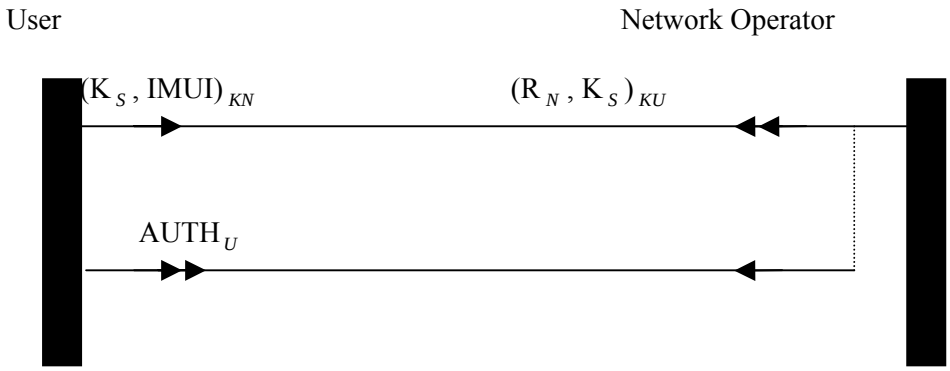

Figure 2. New message flow for the First protocol

Next, we explain the message exchanged involved in the protocol of **Figure 2** in details.

Message M1:

The **User** sends $(K_S, IMUI)_{KN}$ to the **Network Operator**. When the **Network Operator** receives the message M1, he decrypts $(K_S, IMUI)_{KN}$ based on his secret key to gets IMUI and K_S. The **Network Operator** will find the public key of the **User** to encrypt the data, afterward. At the same time, the **Network Operator** generates a random number R_N and encrypts R_N as $(R_N)_{KU}$, which is a challenge and response number.

Message M2:

The **Network Operator** sends $(R_N, K_S)_{KU}$ to the **User**. When the **User** receives the Message M2, he decrypts $(R_N, K_S)_{KU}$ based on his secret key. When **User** gets R_N and K_S, he checks the session key K_S from the **Network Operator** with the sends one. If the

calculated value is correct, the goal of the authentication of the **User** to the **Network Operator** has been achieved. Furthermore, the **User** sends the $AUTH_U$, which is the response to the **Network Operator**.

Message M3:

The **User** sends $AUTH_U$ to the **Network Operator**. When the **Network Operator** receives the Message M3, he checks the $AUTH_U$ and compares it from the **User** with the sends one. If the calculated value is correct, the goal of the authentication of the **Network Operator** to the **User** has been achieved.

Achieved Goals

The achieved goals of the first protocol are described as follows.

(1) Mutual authentication of the **User** to the **Network Operator**: (2) Assurance to the **User and Network Operator** that the Session keys are fresh. (3) Session Key authentication of the **User** to the **Network operator**: (4) Session Key confirmation of the **Network Operator** to the **User**:

Security Analysis

In the following, in order to ensure that the protocol is secure, we shall analyze and discuss the attack methods [12-19].

Attacks 1:Replay Attacks [20]

In this case, to prevent replay attacks, a message in the protocol should contain some "freshness" properties. In the message M1 and M2, the **User** and the **Network Operator** generates a session key K_S and the random number R_N respectively as the fresh messages. In the message M2, the **User** can check K_S according to $(R_N, K_S)_{KU}$ if the message is fresh in this round. In the message M3, the **Network Operator** can verify the $AUTH_U$ that knows the freshness property. Besides, the $(K_S, R_N)_{KU}$ represents the freshness property because it is encrypted by the **User**'s public key such that only the **User** can decrypt it. Similarly, $(R_N, K_S)_{KU}$ represents the freshness property since the session key encrypts it, such that only the **Network Operator** can decrypt it. Hence, the replay attacks are infeasible.

Attack 2: Parallel Session Attacks [21]

Since the messages M1, M2 and M3 fit the asymmetric condition; the parallel session attacks are infeasible.

Attack 3: Guessing Attacks [20]

The authentication with password is widely used by many security systems. However, password is vulnerable under the dictionary attack by which an attacker can guess the password successfully. Public key provides a means for preventing the guessing attack. Since, we uses the public key to encrypt the message, the guessing attacks are infeasible.

3.2 The Second Scheme of Authentication Protocol

The main idea of the second authentication protocol is the same with the First protocol. The second protocol is applied to achieve the goals, such as the mutual authentication of the **User** and the **Network Operator** and establishment of shared session key K_S between them and use a valid certification.

Prerequisites On Mechanism

The prerequisites of this protocol are the same as for the first protocol except that:

(1) The **User** has no authentic copy of the public key K_N of the **Network Operator**.

(2) The **Network Operator** has no authentic copy of the public verification key K_U of the **User**.

(3) There is a valid certificate Cert U, issued by a Certification Authority **CA**, on the public key K_U of the **User**, available at the **User**.

(4) There is a valid certificate Cert N, issued by a Certification Authority **CA** on the public key K_N of the **Network Operator**, available at the **Network Operator**.

(5) The **User** and the **Network Operator** possess the public key necessary to verify certificates issued by CA (PK_CA).

Description Of The Protocol

The difference with first protocol is that the **User** does not know the public key of the **Network Operator** and the **Network Operator** does not know the public key of the **User**.

The notations in **Figure 3** are defined as follows:

- id_{ca} is an identity of the Certification Authority.

- Cert N a valid certificate, issued by a Certification Authority **CA**, on the public key of the asymmetric signature system of the **Network Operator**, available at the **Network Operator**.

-Cert U a valid certificate, issued by a Certification Authority **CA**, on the public key of the asymmetric signature system of the **User**, available at the **User**.

-Sig_{no} is a secret signature transformation owned by the network operator.

-Sig_{u} is a secret signature transformation owned by the user.

-TS is a time stamp.

- $AUTH_N = (K_S)_{KU}$.

The Value of the $AUTH_N$ is used to authenticate the **User** to the **Network Operator**, generally this will be a challenge response value.

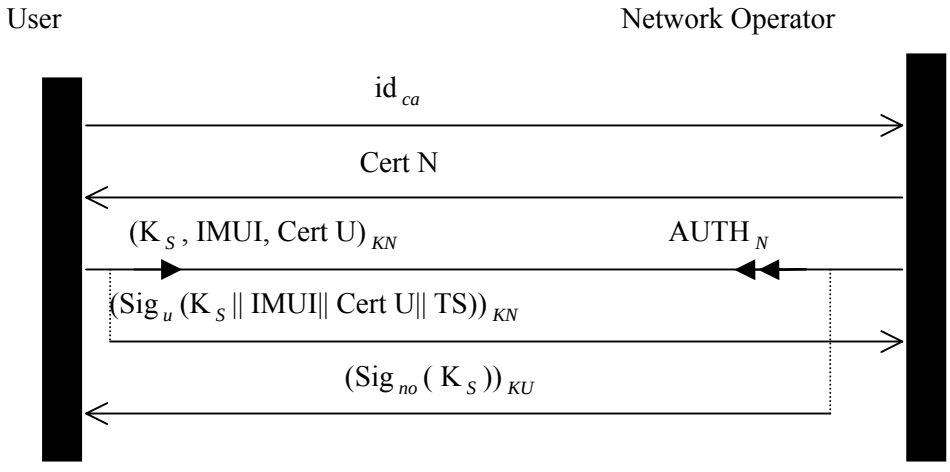

Figure 3. New message flow for the Second protocol

Next, we explain the message exchanged involved in the protocol of **Figure 3.6** in details.

Message M1:

The **User** sends id_{ca}, the identification of the **Certification Authority**, to the **Network Operator**, that the **Network Operator** can verify the signatures. When the **Network Operator** receives this message, he will send his certificate signed by the corresponding **Certification Authority** (**CA**) to uses in the Message M2.

Message M2:

Network Operator sends Cert N to **User.** The **User** can verify this certificate and retrieves the public key agreement key K_N of the **Network Operator**.

Message M3:

The **User** sends $(K_S, \text{IMUI, Cert U})_{KN}$ and $(Sig_u(K_S \| \text{IMUI} \| \text{Cert U} \| \text{TS}))_{KN}$ to the **Network Operator**, where $(K_S, \text{IMUI, Cert U})_{KN}$ is a challenge message. Cert U, IMUI and TS are based on the public key K_N of the **Network Operator**. The **User** generates K_S, which is a session key between the **User** and the **Network Operator**. When the **Network Operator** receives these messages, he decrypts $(K_S, \text{IMUI, Cert U})$ as $(K_S, \text{IMUI, Cert U})_{KN}$ based on his secret key and gets IMUI, K_S and Cert U. The **Network Operator** retrieves the public key of the **User** K_U from the User's certificate, Cert U, and checks the signature. When the **Network Operator** gets IMUI, he verifies the identification of the **User**.

Message M4:

The **Network Operator** sends $AUTH_N$ and $(Sig_{no}(K_S))_{KU}$ to the **User**. **When** the **User** gets $AUTH_N$, he compares the received $AUTH_U$ from the **Network Operator** with the sends one. If the calculated value is correct, the goal of the authentication of the **User** to the **Network Operator** has been achieved. The **User** retrieves the public key of the **Network Operator** K_N from the Network Operator's certificate, Cert N, and checks the signature.

Achieved Goals

The achieved goals of the second protocol are described as follows.

The prerequisites of this protocol are the same as for the first protocol except that:

-Exchange of certificates: id_{ca} is sent in Message M1 to indicate **Network Operator** which

certificates can be verified by the **User**. The **Network Operator** sends a certificate, Cert N, to the **User** in Message M2 and the **User** sends a certificate, Cert U, to the **User** in Message M3.

-Non-repudiation of data sent by the **User**: The User sends $(\mathrm{Sig}_u(K_S \| \mathrm{IMUI} \| \mathrm{Cert\ U} \| \mathrm{TS}))_{KN}$ to the **Network Operator**.

-Non-repudiation of data sent by the **Network Operator**: The **Network Operator** sends $(\mathrm{Sig}_{no}(K_S))_{KU}$ to the **User**.

Security Analysis

In the following, in order to ensure that the protocol is secure, we shall analyze and discuss the attack methods [12-19].

Attacks 1: Replay Attacks [20]

In this case, to prevent replay attacks, a message in the protocol should contain some "freshness" properties. In the message M3, the **User** generates a session key K_S and the time stamp TS as the fresh messages. In the message M4, the **User** can check K_S according to AUTH_N if the message is fresh in this round. Besides, the AUTH_N represents the freshness property because it is encrypted by the **User**'s public key such that only the **User** can decrypt it. Hence, the replay attacks are infeasible.

Attack 2: Parallel Session Attacks [21]

Since the messages M1, M2 and M3 fit the asymmetric condition; the parallel session attacks are infeasible.

Attack 3: Guessing Attacks [20]

The authentication with password is widely used by many security systems. However, password is vulnerable under the dictionary attack by which an attacker can guess the password successfully. Public key provides a means for preventing the guessing attack. Since, we uses the public key to encrypt the message, the guessing attacks are infeasible.

Attack 4: Man-in-the-Middle Attacks [20]

An attacker can use the man-in-the-middle attack to intervene between the **User** and the

Network Operator and masquerade as one to communicate with another bi-directional. Public key cryptosystem using certificate often provides a solution for preventing this attacks. Since, our scheme can prevent these attacks.

3.3 The Third Scheme of Authentication Protocol

The main idea of the third authentication protocol is the same with the first protocol. **Certificate Server** applies the third protocol to achieve the goals such as the mutual authentication of the **User** and the **Network Operator**, the establishment of shared session key K_S between them and valid certification provided by the **Certificate Server**.

Prerequisites On Mechanism

The prerequisites of this protocol are the same as for the first protocol except that:

(1) The **User** has a public key the **Certificate Server**-K_C.

(2) The **Network Operator** has a public key the **Certificate Server**-K_C.

Description Of The Protocol

The third protocol is no authentic copy of the public key of the **User** available at the **Network Operator** and is no authentic copy of the public key of the **Network Operator** available at the **User**.

In the third protocol, there are five exchanged messages among the **User**, the **Network Operator** and the **Certificate Server**. The messages flows are indicated in the **Figure 4**. The **certificate server CS** has to access the certificate of the **User** issued by a **Certification Authority CA**.

The notations in **Figure4** are defined as follows:

- id_{cs} is a identity of the **Certificate Server**.

- $K_S = h1(R_U \oplus R_N)$.

- $AUTH_N = h2(K_S)$.

- $AUTH_U = h3(K_S)$.

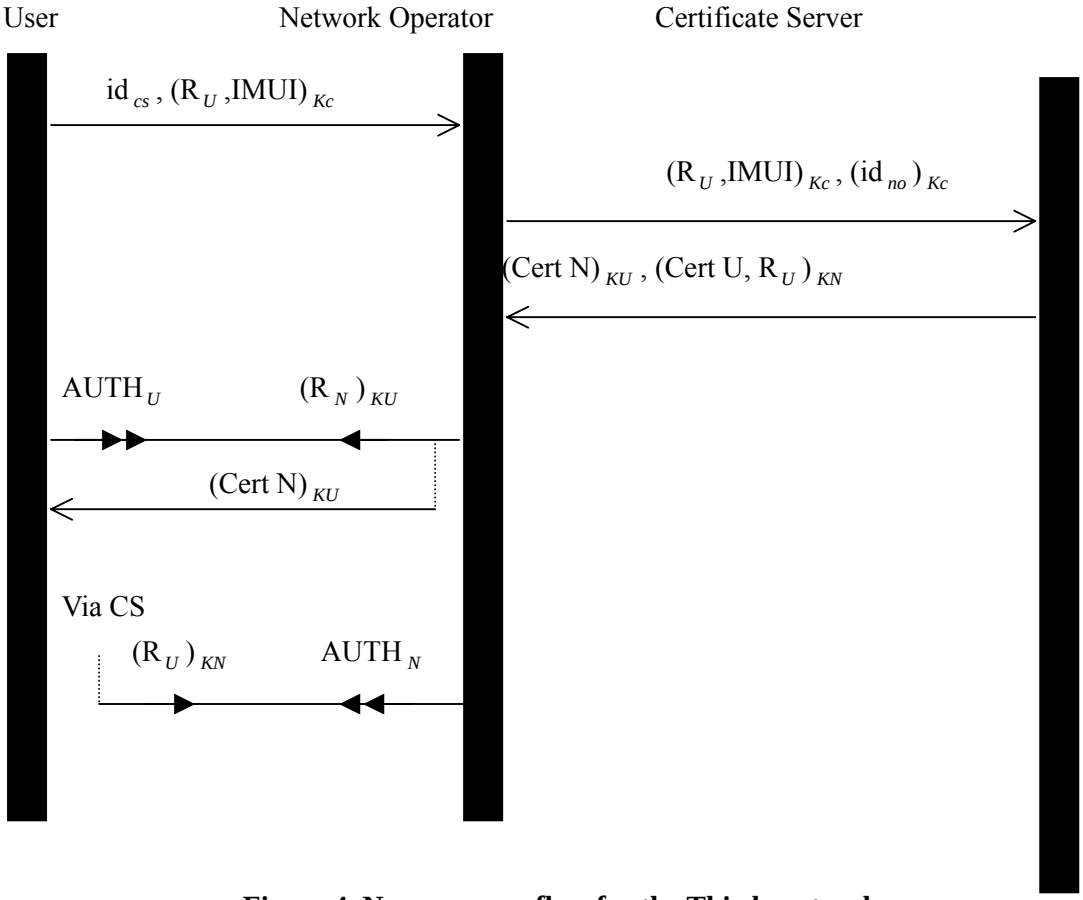

Figure 4. New message flow for the Third protocol

Next, we explain the message exchanged involved in the protocol of **Figure 4** in details.

Message M1:

User sends id_{cs} and $(R_U, IMUI)_{Kc}$ to the **Network Operator**. The id_{cs} is the identification of the **Certificate Server** that the **User** can verify signatures.

Message M2:

When the **Network Operator** receives these messages, it forwards the message of $(R_U, IMUI)_{Kc}$ and uses the **Certificate Server's** public key K_C to encrypt his identity id_{no}, then sends these messages to the **Certificate Server**. The **Certificate Server** receives these messages, he decrypts the $(R_U, IMUI)_{Kc}$ and $(id_{no})_{Kc}$ based on his secret key K_C. The **Certificate Server** gets R_U, IMUI and id_{no}. It uses IMUI and id_{no} to access the database of the **Certificate Server** to obtain Cert U and Cert N, respectively.

Message 3:

The **Certificate Server** sends $(\text{Cert N})_{KU}$ and $(\text{Cert U}, R_U)_{KN}$ to the **Network Operator**. When the **Network Operator** receives these messages, he decrypts $(\text{Cert U}, R_U)_{KN}$ based on his secret key and gets Cert U, R_U. At the same time, the **Network Operator** generates a random number R_N, and calculates the session key K_S and $AUTH_N$.

Message M4:

The **Network Operator** sends $AUTH_N$, $(\text{Cert N})_{KU}$, and $(R_N)_{KU}$ to the **User**. When the **User** receives these messages, he decrypts $(R_N)_{KU}$ and $(\text{Cert N})_{KU}$ based on his secret key and gets R_N, Cert N. Therefore, the **User** compares the received $AUTH_N$ from the **Network Operator** with the calculated one. If the calculated value is correct, the goal of the authentication of the **User** to the **Network Operator** has been achieved. Furthermore, the **User** calculates the $AUTH_U$, which is response to the **Network Operator**.

Message M5:

The **User** sends $AUTH_U$ to the **Network Operator**. When the **Network Operator** receives these messages, he compares the received $AUTH_U$ from the **User** with the calculated one. If the calculated value is correct, the goal of the authentication of the **Network Operator** to the **User** has been achieved.

Achieved Goals

The achieved goals of the third protocol are described as follows.

The same goals are achieved in the same way as for first protocol except for:

-Confidentiality of the **User** identity:

It is achieved by encrypting the **User** identity IMUI in the first message with public key K_C of the **Certificate Server**.

-Exchange of certificates:

id_{cs} is sent in message M1 to indicate to the **Certificate Server** which certificates can be verified by the **User**.

Security Analysis

In the following, in order to ensure that the protocol is secure, we shall analyze and discuss the attack methods [12-19].

Attacks 1: Replay Attacks [20]

In this case, to prevent replay attacks, a message in the protocol should contain some "freshness" properties. In the message M1 and M4, the **User** and the **Network Operator** generates a session key R_U and the random number R_N, respectively, as the fresh message. In the message M4, the **User** can check K_S according to $AUTH_N$ if the message is fresh in this round. In the message M5, the **Network Operator** can verify the $AUTH_U$ that knows the freshness property. Besides, the random number R_N represents the freshness property because it is encrypted by the **User**'s public key such that only the **User** can decrypt it. Similarly, the $(R_U)_{KN}$ represents the freshness property because it is encrypted by the **Network Operator**'s public key such that only the **Network Operator** can decrypt it. Hence, the replay attacks are infeasible.

Attack 2: Parallel Session Attacks [21]

Since the messages M1, M2, M3, M4, and M5 fit the asymmetric condition, the parallel session attacks are infeasible.

Attack 3: Guessing Attacks [20]

The authentication with password is widely used by many security systems. However, password is vulnerable under the dictionary attack by which an attacker can guess the password successfully. Public key provides a means for preventing the guessing attack. Since we use the public key to encrypt the message, the guessing attacks are infeasible.

Attack 4:Man-in-the-Middle Attacks [20]

An attacker can use the man-in-the-middle attack to intervene between the User and the Network Operator and masquerade as one to communicate with another bi-directional. Public key cryptosystem using certificate often provides a solution for preventing this attacks. Since, our scheme can prevent these attacks.

3.4 Performance Analysis

In this case, we compare the performance of our protocols and Siemens protocols. Our protocols have the feature of transmission data size within communications less than the protocols proposed by Siemens. We list the table 1 and table 2 as follows [5].

4. Conclusions and Future Research

In this paper, we have proposed three new authentication mechanisms based on Asymmetric-key cryptosystems. In our study protocols, we have build up the authentication protocols that provide a good protection of ensuring the freshness of authentication data, session key and shared secret data. Another feature is the transmission data size within communications less than the protocols proposed by Siemens. In the third generation mobile systems, there involves various services such as e-commence, Internet, computing data and so on. In this service, there are still lots of topics that are worthy to be explored in authentication protocols. They should be provided with different security considerations. In the future, we will continue to design new authentication protocols and will improve their performance by reducing the communication times during the process of authentication and also by reducing the transmission data size within communications.

Table 1. Performance Evaluation

Performance evaluation	Siemens Bits	Our Proposed Bits	Performance η
Protocol A/Protocol 1	896 bits	512 bits	57.14%
Protocol B/Protocol 2	1280 bits	924 bits	72.18%
Protocol C/Protocol 3	2176 bits	1412 bits	64.88%

- The number of bits is reference by 3GPP.

Table 2.Compare the Our Protocols and the Siemens protocols

	Siemens Protocol	Our Protocols
Protocol A	Flaws: (1)NO's private key can calculated by the User. (2) the User is not authentication the NO. (3) total messages are large.	$(K_S, IMUI)_{KN}$ Improve:(1)Via can improve the flaws and prevent impersonation the NO.(2)Total messages are reduced.
Protocol B		Improve:(1)Via $(K_S, IMUI, CertU)_{KN}$ can improve the flaws and prevent impersonation the NO.(2)Total messages are reduced.
Protocol C		Improve：Base on this protocol， design a new protocol and reduce the total messages.

Reference

[1] A. T. Khalid and A. Ali, "A new authentication protocol for Roaming users in GSM Network," *IEEE International Symposium on Computers and Communications Proceedings*, pp.93-98, 1999.

[2] V. Bharghavan and C. V. Ramamoorthy, "Security Issues in Mobile Communications," Second International Symposium on Autonomous Decentralized Systems Proceedings. ISADS 95, pp.19-24, 1995.

[3] J. Liu and Y. Wang, "A User Authentication Protocol for Digital Mobile Communication Network," *Wireless: Personal, Indoor and Mobile Radio Communications Merging onto the Information Superhighway, PIMRC'95. Sixth IEEE International Symposium* , Vol.2 , pp.608-612, 1995.

[4] W. Stallings, Cryptography and network security principles and practice, 2nd ed, Prentice Hall, Inc, 1999.

[5] K. Heikki, A. Ari, N. Valtteri, L. Lauri, N. Siamak, UMTS Network: Architecture, Mobility and Services, Wiley, Inc, 2001.

[6] Y. B. Lin, “Mobility management for PCS,” *Tutorial: First Workshop on Mobile Computing, Applied Research, Bellcore Morristown*, NJ, USA, 1995.

[7] F. G. Constantinos, I. M. Sotirios and S. V. Iakovos, “Towards the Introduction of the Asymmetric Cryptography in GSM, GPRS, and UMTS Networks,” *Computers and Communications, 2001. Proceedings. Sixth IEEE Symposium*, pp.15-21, 2001.

[8] H. T. chang, “A study on authentication protocol for UMTS,” M.S.Thesis, Dept. of Electrical Engineering, Chung Yuan Christian University, 2000.

[9] C. S. Laih, L. Harn and C. C. Chang, ``Contemporary Cryptography and Its Applications,", Unalis Corporation, 1994.

[10] S. Putz, R. Schmitz and F. Tonsing, “Authentication schemes for third generation mobile radio systems,” *The Ninth IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, Vol. 1, pp.126-130, 1998.

[11] http://www.esat.kuleuven.ac.be/cosic/aspect/aspect.html

[12] G. Li, “Optimal authentication protocols resistant to password guessing attacks,” *Proceedings of Eighth IEEE on Computer Security Foundations Workshop*, pp.24-29, 1995.

[13] G. Tsudik, E. Herreweghen, “Some remarks on protecting weak keys and poorly-chosen secrets from guessing attacks,” *Proceedings of The 12th Symposium on Reliable Distributed Systems*, pp.136-141, 1993.

[14] G. Lowe, “Some new attacks upon security protocols,” Proceedings of The *9th IEEE on Computer Security Foundations Workshop*, pp.162-169,1996.

[15] L. Gong, “Verifiable-text attacks in cryptographic protocols.” *Ninth Annual Joint Conference of the IEEE Computer and Communication Societies*, Vol.2, pp.686-693,1990.

[16] P. Syverson, “A taxonomy of replay attacks,” *Proceedings of Computer Security Foundations Workshop VII*, pp.187-191, 1994.

[17] S. Keung, K. Y. Siu, “Efficient protocols secure against guessing and replay attacks,” *Proceedings of Fourth International Conference on Computer Communications and Networks*, pp.105-112, 1995.

[18] T. Kwon, J. Song, “ Security and efficiency in authentication protocols resistant to password guessing attacks,” *Proceedings of The 22nd Annual Conference on Local Computer Networks*, pp.245-252, 1997.

[19] Y. Zheng, J. Seberry, “Immunizing public key cryptosystems against chosen ciphertext attacks,” *IEEE Journal on Selected Areas in Communications*, Vol.11, NO.5, pp.715-724, June 1993.

[20] B. Schneier, “Applied cryptography: Protocols , algorithms, and source code in C,” Wiley.

[21] R. Bird et al., “Systematic Design of Two-Party Authentication Protocols,” Advances in Cryptology-CRYPTO’91, pp. 44-61, 1991.