Security Protocol for IMT-2000-Based Contents Service

Sang-Soo Yeo
Department of Computer Science and Communication Engineering,
Kyushu University, 744 Motooka, Nishi-ku, Fukuoka, Fukuoka 819-0395, Japan
ssyeo@msn.com

Deok Gyu Lee
Electronics and Telecommunications Research Institute
deokgyulee@etri.re.kr

Kouichi Sakurai
Department of Computer Science and Communication Engineering,
Kyushu University, 744 Motooka, Nishi-ku, Fukuoka, Fukuoka 819-0395, Japan
sakurai@csce.kyushu-u.ac.jp

Abstract

Abstract. IMT-2000 appeared in order to satisfy the desires of the uses who wish to supply through wireless most of the services being provided through wire, such as Internet services and multimedia high-speed data information.[1] However, during global roaming, the signal data and the user data get transmitted through the networks of other users. Also, it is judged that with the provision of high speed data communication the amount of data communication necessary for confidentiality protection will increase. It is planned that the recent IMT-2000 project will begin its commercial service in 2002. From this viewpoint, wireless contents, due to their special characteristics, are greatly exposed to illegal actions by third persons. As a result, it can be said that security and authentication issues in the mobile telecommunication environment are indispensable matters. For this purpose, it is intended that in this thesis through an analysis of the existent IMT-2000 authentication method, a more safe and efficient authentication method is presented and, at the same time, a security protocol necessary in the provision of wireless contents is designed.

Keyword*: Security Protocol, IMT-2000*

1. Introduction

Mobile telecommunications went through the 1st and 2nd generations, repeated rapid progress and a lot of users were generated. However, as 1st and 2nd generation mobile telecom services basically kept in mind voice-centered services in their developments, they have been unable to satisfy the demands of the consumers of such mobile multimedia services as high speed wireless Internet communication services. In the future, in wireless, it can be obtained through not voice-centered services but such heightened services as data and mobile multimedia services.

Such mobile telecom services possess the convenience of providing voice and data services without being limited by time and place. On the other hand, due to the special feature of the user possessing mobility and using electric waves as the telecom carrier, they have the weakness in terms of security. [17]

The special feature of IMT-2000, which is the third generation mobile telecom system, is that it has the goal of guaranteeing quality on the wire network while making it possible to use most of the services presently being provided on the wired networks on wireless networks. However, as the wireless networks have transmission routes exposed it has the problem that illegal stolen use by unjust users and bugging the electric waves through the transmission media by a third person possessing evil intentions are easy. In this thesis, in order to provide strong authentications, differently from providing the implied two-way authentication presented by the existent standards, a new two-way authentication protocol used in IMT-2000 has been designed. At the same time, based on this, with the encryption keys and integrity keys, a security protocol in the provision of contents is presented.

2. Introduction to IMT-2000 and Security Organization Chart

In this chapter, we will take a look at an introduction to the IMT-2000 necessary for authentication and a security organization chart. [1],[5]

2.1. Introduction to IMT-2000

IMT-2000 is the abbreviation of International Mobile Telecommunication 2000 and it means pan-world mobile telecommunication.

It was in 1996 that the term "IMT-2000" started being commonly used. Prior to this, the term "Future Public Land Mobile Telecommunication System (FPLMTS)" had been used. FPLMTS had been decided to be the project code when, in 1978, the International Electric Telecommunication Union (ITU) took the single standardization of future mobile telecommunication as the research task.

However, as FPLMTS is hard to pronounce and the meaning is not easy to understand, it brought forward the necessity of a new term. ITU took into consideration the frequency range (2000 MHz range) that FPLMTS will use and the time of introduction (around the year 2000), thought up the name "IMT-2000", and recommended that it be used together with FPLMTS. At present, the situation is that IMT-2000, which is easy to understand, has become established as the standard term. And, according to the service method, it is divided into the North American method of synchronous (cdma2000) and the European method of asynchronous (W-CDMA).

2.2. Security elements of IMT-2000

A structure for providing security in IMT-2000 has been shown. [1] Five types of security-related parts have been defined and each group is as the following.

Network access security: This provides a safe access regarding the 3G (3rd Generation) service and a function for preventing attacks by a third person on radio link. (I)

Network domain security: This provides the protection for information transmitted in the wired areas of the network and the protection regarding signaling information.(II)

User domain security: This provides the parts for safely accessing to MS(Mobile Station).(III)

Application domain security: This provides the function for having messages safely transmitted between the user and the service provider domain.(IV)

3. Global authentication of 3GPP

3.1. The authentication protocol of 3GPP

Below, the authentication protocol in 3GPP is explained. 3GPP carries out mutual authentication by showing that each knows the value of the secret key K, which is secret information between the user and the network. The value of the secret key K is stored in UIM (User Interface Module) and HE (Home Environment). [3]

The execution of the authentication takes place in the AuC within the user's HE (Home Environment) and the UIM within the user MS. The following is the execution process of the authentication.

The authentication information from HE/AuC to SN (Service Network)/VLR is delivered. At this time, in order to deliver the authentication information safely, SN/VLR assumes that HE has the trust. Also, it is assumed that a safe intra-system link exists between SN/VLR and HE. The user trusts HE.

A process for certifying and installing a new encryption key and an integrity key between SN/VLR is executed.

The authentication data from the VLR previously visited to the new VLR are transmitted. At this time, it is assumed that the link between SN/VLR is safe.

3.2. Problems

The authentication method in 3GPP possesses a procedure for executing implied two-way authentication regarding the value K of the secret key from HE to MS. And, as it provides the minimum authentication functions, it has a significant weakness in terms of security aspects. The following shows the procedure regarding the existent authentication method of 3GPP.

In the beginning, SN requests the generation of the secret shared data and the random value for the authentication of MS in HE. Also, MS generates secret shared data in order to receive services. The HE that has received the request message sends a message for the calculation of the authentication value, together with a random value, to MS through SN in order to execute the authentication process. After having received the transmitted random value, MS calculates the F function. HE executes the F function and after generating the authentication value it compares with the value received through transmission. After this, HE notifies MS whether a authentication has been made. If the value is the same, it instructs MS, which executes the functions regarding the provision of the service, to provide the service. And, if the value is different, it executes the refusal to certify, thereby finishing the authentication process.

4. Matters requiring security

The following is about the matters requiring security that must be basically possessed in the proposed methods, based on the weaknesses of the existent methods.

4.1 A safe database within the network

Regarding the authentication factors of MS and of HE, the user profiles, following illegal approaches to the database, can be obtained and manipulated to be used for threatening privacies or for illegal reproduction.

Because of such reason, a safe database for storing the authentication factors of MS and of HE is necessary.

4.2 Prior sharing of the secret key

In authentication, mutual authentications have been taking place under the assumption that MS and HE know about the secret key K. MS and HE must share the secret key prior hand.

4.3 Securing the trust between SN and HE

The securing of trust between SN and HE is very important. If SN illegally misappropriates MS information and does not provide the safe approach controls regarding the database, the service could not be provided.

4.4 A safe communication channel between SN and HE is needed

As, in the communication between SN and HE, there are the authentication variables regarding the MS authentication and the authentication variables regarding HE, it must be safe from seizures and illegal reproductions regarding the authentication variables.

5. Proposal methods

As we have seen above, the 3GPP standard proposal basically provides implied mutual authentication. In this thesis, the authentication protocols and security protocols regarding network domain security and application domain security, which provide services related to security on wireless links, are designed. Especially, in the authentication procedure, in order to make authentications from MS to HE and from HE to MS possible, two types of authentication methods have been united to design a two-way authentication protocol. And a security protocol for providing the contents has been proposed. Regarding network domain security and application domain security, which provide services related to security on wireless links, a authentication protocol and a security protocol are designed.

As a result, this proposed method has improved the weaknesses of the existent implied two-way authentication method and it can provide even more safe wireless contents services.

5.1 Organization elements

UI : As "User Interface Module", it has the variables for the provision and authentication of MS's contents. And, it includes the random number generator.

MS : As "Mobile Station", it can execute encryption and decoding, and has the capability to operate. It generates the authentication variables regarding HE. Although MS can generate sequence numbers, it must receive UI's help regarding random numbers. The functions of F1~F5 within MS and HE have not been defined.

SN/VLR : As "Service Network", it executes the authentication process after receiving help from MS and HE. Its own database stores the authentication variables. After storing the authentication variables received after delivery from MS, when HE's authentication gets completed, SN deletes the authentication variables received from MS from the database. In the opposite way, the processing regarding the authentication variables received from HE gets done in case MS has come out of SN's service.

HE/AuC : Together with MS, it shares the secret key K. It generates the authentication variables regarding MS.

5.2. System parameters

The following explains about the system counting necessary for the authentications and the protection of the contents in this thesis.

· * : (US : User, HE : Home Environment, SN : Service Network)

· RAND* : * generate Random Number

· Kh : value for protected Sequence Number

· Ka : compare value for User Generate Kh

· AUTN* : *의 Authentication Token (US : User, HE : Home Environment)

· *RES : Authentication check value

(URES : User Authentication check value, XRES : Hone Environment check value, HRES: Service Network Authentication check value)

· PAR : Parameter

· F2K : HRES generate Function

· F3K : CK generate Function

· F4K : IK generate Function

· F5K : Kh generate Function, kh to Ka verification

· CK : Cipher Key

· IK : Integrity Key

· SEQ : Sequence Number

· PAR : Parameter

· M : Contents File

· SCF : Service Contents File

· MID : Media ID

· ID : User Identity

· K : Session Key

· F2K : HRES

· KS : Storage Key

· H : Storage Key to Hash Function

· K* : Contents in use key value(IK : Integrity Key, CK : Cipher Key)

· SEQ* : * generate SEQ (US : User, HE : Home Environment)

5.3 Prior preparation phase

The following is the prior preparation phase regarding the authentication procedure and the provision of the contents.

Step 1. Exchanges regarding the secret key K must take place prior hand between MS and HE. Prior sharing takes place regarding the secret key K and it gets stored in UI and HE.

Step 2. The UI (User Interface) gets organized as a smart card. And the items to be inserted within the smart card get delivered from SN to MS off-line.

Step 3. The watermarking technique has to take place regarding the contents so that illegal reproductions can be detected.

5.4 The authentication phase from MS to HE

The demands regarding the authentication variables by MS at the time of the first interface with the service environment and the authentication procedure regarding HE are explained.

Step 1. The storage key, random number generation functions, and media-ID, get delivered from SN to the smart card.

Step 2. When MS gets located within SN, SN demands the authentication data for HE authentication.

- RANDUS(1…n)
- Kh(1…n) = F5K{RANDUS(i):K}
- AUTNHE(1…n) = Kh(i) ⊕ SEQUS(i)
- URES(1…n)

Step 3. SN generates the authentication variables regarding the demands for the authentication data regarding HE.

- RANDUS(1…n)
- AUTNHE(1…n)
- URES(1…n)

Step 4. HE delivers the generated authentication to SN.

Step 5. SN stores the authentication variables.

Step 6. SN selects one authentication variable from among n number of authentication variables and delivers to HE.

- RANDUS(i), AUTNHE(i)

Step 7. HE calculates the HRES(i) from the authentication variables delivered and received from SN.

- Kh(i) = F5K{RANDUS(i):K}
- AUTNHE(i) = {Kh(i) $\oplus$ SEQUS(i)} $\oplus$ Kh(i)
- HRES(i) = F2K{RANDUS(i) : K}

Step 8. SN compares the HRES(i) and URES(i) delivered and received from HE.

5.5 The authentication phase from HE to MS

In this phase, regarding the authentication variables the above-mentioned MS has generated, in case authentication has been completed, the authentication procedure regarding MS with the authentication variables that SN demanded from HE and received is explained. In case all of the authentication procedures have been completed, MS and SN generate IK and CK.

Step 1. For the authentication of MS, SN demands HE for authentication data.

Step 2. By comparing the two values delivered and received, if they are the same, SN deems it to have been certified and notifies MS.

Step 3. HE creates the MS authentication variables regarding SN's demands for the authentication data.

- Ka(i) = F5K{RANDHE(i):K}
- MAC(i) = F1K{SEQHE(i):Text(i):RANDHE(i):K}
- XRES(i) = F2K{RANDHE(i):K}
- CK(i) = F3K{RANDHE(i):K}
- IK(i) = F4K{RANDHE(i):K}
- AUTNUS = [(Ka(i) $\oplus$ SEQHE(i)) $\|$ Text(i) $\|$ IK(i)]

Step 4. HE delivers the authentication variables created to SN.

- RANDHE(1…n)
- XRES(1…n)
- CK(1…n)
- IK(1…n)
- AUTNUS(1…n)

Step 5. SN stores the authentication variables.

Step 6. Among the n number of authentication tokens, SN selects one authentication variable and delivers it to MS.

- RANDHE(i), AUTNUS(i)

Step 7. MS calculates the XRES(i) from the authentication variables delivered and received from SN.

- $Ka(i) = F5K\{RANDHE(i):K$
- $AUTNUS(i) = \{Ka(i) \oplus SEQHE(i)\} \oplus Ka(i)$
- $XMAC(i) = F1K\{PAR1:SEQHE(i):RAND(i):Text(i)\}$
- $XMAC(i) = MAC(i)$

Step 8. Transmit the RES(i) generated to SN.

Step 9. After transmitting the RES(i), MS calculates the IK(i) and CK(i).

Step 10. SN inspects whether the RES(i) received is the same as XRES(i). If they are the same, it will be deemed to have been certified.

Step 11. SN selects AUTNUS' IK(i) and CK(i) that HE has sent.

5.6 The phase of contents provision from MS to SN

As a authentication phase from HE to MS, this phase is the process of protecting the contents and

Step 1. MS stores the IK(i) in UI.

Step 2. Encrypt regarding the contents in SN.

(1) By making into the integrity key IK(i), encrypt the music file M.

(2) In SN, provide the created file key encryption information to MS.

- $KCK(KIK \parallel IDH)$

Step 3. MS provides the encrypted binding block to SN.

(1) By receiving the encrypted file key, check and confirm the file key.

(2) Using this, generate the binding block and transmit to SN.

- $\text{Binding Block} = KCK(H(KS) \parallel KS(KIK) \parallel MIDUS)$

Step 4. In SN, decode the binding block that came from MS, check and confirm, and then connect to the encrypted contents.

(1) Decode the binding block.

- $KCK(\text{Binding Block})$

$= KCK(KCK(H(KS) \parallel KS(KIK) \parallel MIDUS))$

$= H(KS) \parallel KS(KIK) \parallel MIDUS$

After organizing an SCF file, transmit it to an MS which uses an UI.

- $SCF = (\text{Binding Block} \parallel KIK(M))$

Step 5. User the contents delivered from MS to SN.

(1) Checking and confirming the binding block.

By using the storage key, recover the file key and compare them.

- KS(KS(KIK))

(2) By using the confirmed file key, use the contents.

6. Comparative analysis

This thesis has improved the weaknesses of the implied two-way authentication of the authentication protocol presented in the existent standard 3GPP. By adding the authentication from MS to HE, which is not the existent one-way authentication from HE to MS, it has materialized two-way authentication.

Also, considering the efficiency of MS, by using the variables included within MS, the use of yet another interface, resulting from two-way authentication, has become unnecessary. This thesis has provided a stated authentication procedure, which is not an implied two-way authentication, without greatly coming out of the standard proposal.

7. Conclusion

Through the rapid development of wireless mobile telecommunications the number of the users has been increasing in a geometric progression. However, as the first generation and second generation mobile telecommunications services were developed basically keeping in mind voice-centered services, the demands by the consumers of high-speed wireless telecommunications services, such as mobile multimedia services, could not been met. IMT-2000, the third generation mobile telecommunications system, has the goal of guaranteeing the qualities of wired networks, while making it possible to use through wireless networks most of the services presently provided on wired networks. However, wireless networks, of which the transmission routes are exposed, have the problems of illegal, embezzled usages by unjust users and the bugging of the electric waves through a shared transmission medium by a third party who possesses evil intentions.

With regard to the provision of contents, services must not be materialized, from the origin, for third parties who have not been approved. And, the services must take place for the approved users, without fail. In order to solve such problematic points, this thesis provided a two-way authentication which has supplemented the problems that the existent one-way authentication possesses. And, through this, with regard to contents provision, a security protocol has been presented.

As a result, this proposed method, having improved the weaknesses of the existent implied two-way authentication methods, can provide even more safe wireless contents services. And, also, with regard to the provision of the contents, the proposed method has been proposed taking into consideration the efficiency of MS. In addition, it can detect illegal approaches and illegal reproductions regarding the contents by third parties. It is judged that sufficient utilization is possible in the future with regard to the provision of electronic commerce multimedia contents through even more researches.

8. Reference

[1] 3GPP TS 33.102 : "3rd Generation Partnership Project(3GPP); Technical Specification Group Services and System Aspects; 3G Security; security Architecture".

[2] 3GPP TS 22.022 : "3rd Generation Partnership Project(3GPP); Technical Specification Group Services and System Aspects; Personalization of UMTS Mobile Equipment (ME); Mobile functionality specification".

[3] 3GPP TS 33.103 : "3rd Generation Partnership Project(3GPP); Technical Specification Group Services and System Aspects; 3G security; integration Guidelines".

[4] 3GPP TS 33.105 : "3rd Generation Partnership Project(3GPP); Technical Specification Group Services and System Aspects; 3G security; Cryptographic Algorithm Requirements".

[5] 3GPP TS 33.120 : "3rd Generation Partnership Project(3GPP); Technical Specification Group Services and System Aspects; 3G security; Security Principles and Objectives".

[6] 3G TR 33.901 : "3rd Generation Partnership Project(3GPP); Technical Specification Group Services and System Aspects; 3G security; Criteria for cryptographic algorithm design process".

[7] 3G TR 33.902 : "3rd Generation Partnership Project(3GPP); Technical Specification Group Services and System Aspects; 3G security; Formal Analysis of the 3G Authentication Protocol".

[8] 3G TR 33.908 : "3rd Generation Partnership Project(3GPP); Technical Specification Group Services and System Aspects; 3G security; General Report on the Design, Specification and Evaluation of 3GPP Standard Confidentiality and Integrity Algorithms".

[9] ETSI SAGE : "Security Algorithm Group of Experts(SAGE); General Report Design, Specification adn Evaluation of The MILENAGE Algorithm Set: An Example Algorithm Set for the 3GPP Authentication and Key Generation Functions".

[10] ITU : ITU-R SECURITY PRINCIPLES FOR INTERNATIONAL MOBILE : TELECOMMUNICATIONS-2000 (IMT-2000) Recommendation ITU-R M.1078

[11] ITU : EVALUATION OF SECURITY MECHANISMS FOR IMT-2000 : RECOMMENDATION ITU-R M.1223

[12] ftp://ftp.3gpp.org/TSG_SA/WG3_Security/TSGS3_14_Oslo/Report

[13] ftp://ftp.3gpp.org/TSG_SA/WG3_Security/TSGS3_15_Washington/Report