차세대 이동통신 시스템에서 유동적 USIM 카드를 이용한 인증 시스템

최동욱* · 황재영* · 정연호**

Flexible USIM Authentication System for Next Generation Mobile Radio Communication Systems

Dong wook Choi* · Jae-young Hwang* · Yeon-ho Chung**

요 약

본 논문은 유동적 USIM(Universal Subscriber Identity Module)을 이용한 사용자 편의를 위한 인증시스템을 제안한다. 유동적 USIM 카드는 이동통신망 이용자에게 시스템에서 단말의 할당된 고유번호나 주민등록번호와 같은 개인화 정보를 인증의 인자로 이용하여 제한된 횟수나 사용시간을 허가하는 인증 방법이다. 본 연구에서 제안하는 모듈을 검증하기 위해 시뮬레이션을 수행하였으며 제안한 알고리즘 및 시스템이 현재의 시스템에서 완벽하게 동작하며, 기존의 USIM 카드를 사용하는 인증방법과도 높은 호환성을 확인하였다. 또한 유동적 USIM 카드를 이용하여 또 다른 인증방식을 설계할 수도 있음을 제시하였다. 제안하는 유동적 USIM 기술을 적용할 경우 간단하면서도 강력한 인증방법과 시스템을 개발할 수 있을 것이며 사용자 환경과 독립적으로 이동통신망 접근을 가능하게 해 줄 수 있다.

ABSTRACT

This paper presents a user-friendly authentication system using a flexible USIM. In the proposed method and its system, the flexible USIM utilizes personalized data such as Mobile Directory Number(MDN) and social security number as the key to user authentication. The authentication method proposed in this paper permits limited times of use and/or limited duration of use. A simple simulation model shows that the proposed algorithm works well and shows high compatibility with existing authentication methods. In addition, an alternative or more advanced authentication system can be developed with the proposed flexible USIM card. It is seen that this simple alternative method will eventually be able to make wireless communication networks more easily accessible for subscribers, irrespective of user environments.

키워드

USIM 카드, 인증, 차세대 이동통신, 호처리

Key word

USIM card, Authentication, Next Generation Mobile Network, Call Flow

* 준회원 : 부경대학교 정보통신공학과 (gutmatt@gmail.com)
** 정회원 : 부경대학교 정보통신공학과 (교신저자)

접수일자 : 2011. 09. 02
심사완료일자 : 2011. 10. 10

Ⅰ. 서 론

USIM 카드는 사용자 정보를 포함하는 가입자 개체모듈 (SIM : Subscriber Identity Module)과 범용 직접회로카드 (UICC : Universal Integrated Circuit Card)인 두 부분으로 구성되어 있다[1]. 이 USIM 카드는 제3세대 이동통신시스템 (UMTS : Universal Mobile Telecommunication System)에서 사용자 인증, 국제로밍 및 금융거래의 주요 인자로 사용되고 있다[2]. 일반적인 USIM 카드는 스마트 카드의 한 종류로서 가입자가 위치와 무관하게 2Mbps이상의 전송속도를 보장하며 대용량 문자 서비스나, 음성신호, 동영상 서비스를 받을 수 있게 해주는 역할을 한다[3]. 제 3세대 혹은 그 이상의 이동통신에서는, 단말에 USIM 카드가 장착되어 있지 않은 상태에서도 긴급통화는 가능하도록 설계되어 있다. USIM은 이동통신 시스템에서의 단말이 망에 접근하는 것을 제어 하거나, 과금을 하는 용도로 설계되었다. 상기 기능을 구현하기 위해 USIM카드 내에는 직접 회로카드 개체 (ICC-ID : Integrated Circuit Card-Identification), 국제 이동통신 가입자코드 (IMSI : International Mobile Subscriber Identity) 그리고 이동통신국에 접속하기 위한 인증부호 정보 등이 저장된다. 이동전화 사용자가 USIM 카드를 최초로 획득하게 되면, 수동의 등록절차 없이도 이동통신망 내 어떠한 단말기에서든 서비스를 이용할 수 있다. 이러한 USIM 카드의 등장은 시장에서 가입자들이 동일한 USIM 카드 하나만을 가지고도 여러 개의 단말기를 사용할 수 있는 환경을 만들었다[4]. 그러나 이동통신망 가입자가 자신의 USIM 카드를 소지하지 않은 상황에서 자신에게 할당된 고유의 번호로만 발신을 하거나 수신을 해야 하는 경우를 가정할 수 있다. 이러한 특별한 상황에서 새로운 USIM 카드를 획득한 후, 이동통신망 제공자의 데이터베이스에 기존의 자신의 정보를 갱신 및 폐기하고 생성하는 작업은 비용을 증가시킨다. 또한 새로운 USIM 카드를 등록하는 절차는 매우 복잡할 뿐만 아니라, 영업시간 이후에 이러한 수동 등록 작업을 수행하는 것은 불가능하다.

본 논문에서는 이러한 문제점을 해결하고 보다 친사용자 편의를 위한 유동적 USIM 카드를 이용한 인증 시스템을 제안하고자 한다. 이 기술은 유동적 USIM 카드를 사용하여 이동통신망 이용자에게 제한된 횟수나 통화시간을 허용하는 방식이다.

2장에서는 유동적 USIM 카드를 이용하는 시스템에 대하여 설명하고, 3장에서는 제안하는 유동적 USIM 카드의 기술적인 모델인 알고리즘에 대해서 기술하였다. 4장에서는 제안된 시스템에 대한 시뮬레이션 검증을 통하여 알고리즘에 대한 평가 및 분석을 제시한다. 마지막으로 5장에서는 제안된 알고리즘과 시스템에 대한 결론을 도출하고 향후 연구방향에 대한 의견을 제시한다.

Ⅱ. Flexbilte USIM 카드

일반적으로 이동통신망 시스템의 호처리에서 가입자에 대한 인증 절차는 최우선으로 진행되는 작업이다. 그 이유는 이동통신망에서 USIM 카드가 가입자간을 구별해 주는 유일한 장치이며 인증을 통한 가입자간 구별을 가능하게 해주기 때문이다[5]. 이러한 SIM 카드를 이용한 간단한 가입자 인증 과정은 다음과 같이 기술할 수 있다[6]. 단말기에 전원이 공급되면, SIM 카드로부터 국제 이동통신 가입자코드를 획득하게 된다. 그리고 이 값을 기반으로 단말은 이동통신망에 접속과 인증을 요청한다. 이동통신단말은 이러한 개인정보를 사용자에게 노출하기 전에 SIM 카드로 부터 개인 확인번호 (PIN : Personal Identification Number)의 입력을 요구 받을 수도 있다. 이동통신망은 요청된 국제 이동통신 가입자 코드값을 기반으로 데이터베이스 내의 연관된 인증키를 찾는다. 그리고 난수값 (RAND)을 발생시켜 국제이동통신가입자코드에 연관된 인증키를 할당하여 SRES 1이라고 하는 숫자를 생성한다. 그리고 난수값 (기존의 국제이동통신가입자코드에 의해 생성된)을 단말로 전송하고, 이 값은 SIM 카드에 전달된다. 그러면 가입자 개체모듈카드는 단말에 할당된 인증키를 이용하여 SRES 2 라고 하는 값을 생성하고, 단말은 생성된 SRES 2를 이동통신망에 전달한다. 이동통신망은 계산된 SRES 1과 단말로부터 전달받은 SRES 2를 비교한다. 두 값이 정확히 맞으면 SIM 카드는 이동통신망으로부터 접속에 대한 허가를 얻게 된다. 인증통과 이후 단말의 인증키(Kc)는 이동통신망과의 통신에서 모든 암호화에 이용되게 된다.

본 논문에서는 상기에 설명된 인증방식을 기반으로 하는 유동적 USIM 카드를 이용한 인증 시스템을 제안한다. 구체적인 인증 방식은 다음과 같이 설명할 수 있다. 유동적 USIM 카드를 이용한 단말기에서는 유동적 USIM 카드가 단말에 장착되게 되면 가입자 종속적인 인증 정보가 생성된다. 그림 1에서 유동적 USIM 카드를 이용하는 사용자가 이동통신망으로부터 인증을 받기 위하여 필요한 필수적인 전달인자를 명시하고 있다.

그림 1. 유동적 USIM 카드를 이용한 가입자 인증시의 필수 전달인자
Fig. 1 Essential parameters for user authentication in the flexible USIM method

유동적 USIM 카드를 장착한 단말기는 그림 2에서 보여주고 있는 것처럼 디스플레이부, 입력부, 제어부, 저장부 그리고 USIM 인터페이스부로 구성되어 있다. 유동적 USIM 카드가 단말의 USIM 인터페이스 부에 장착되면, 디스플레이부에서는 가입자에게 가입자 식별번호 (MDN : Mobile Directory Number)나 주민등록번호와 같은 개인화 정보를 요청하게 된다. 그리고 제어부는 이동통신기지국으로부터 할당받은 비밀키와 입력부로부터 받은 개인화 정보를 조합하여 부호화 된 코드를 생성한다. 이 부호화된 코드는 통신부의 제어하에 이동통신망을 통하여 인증센터로 전송된다. 본 유동적 USIM 카드를 이용한 사용자 인증 방법에서는 미리 공개되어 있는 가입자 식별번호나 주민등록번호와 같은 값들이 인증절차를 수행하는데 있어서 핵심이 되는 정보이다.

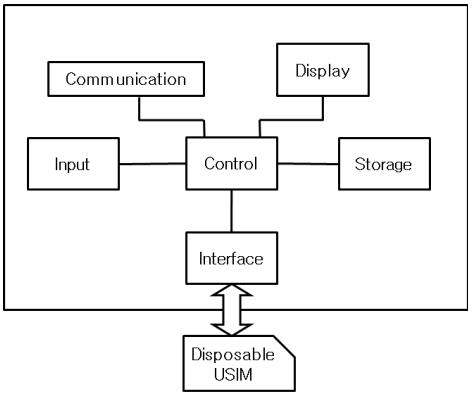

그림 2. 유동적 USIM 카드의 구성요소
Fig. 2 Components of the flexible USIM card

단말기로부터 생성된 인증코드가 인증서버에 전송되어지면, 서버로부터의 인증절차가 진행된다.

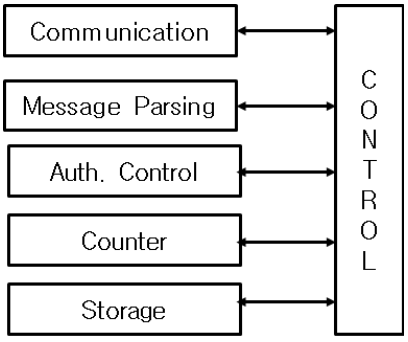

그림 3. 유동적 USIM 카드처리를 위한 인증센터의 구성요소
Fig. 3 Processing modules for the flexible USIM card in authentication center

서버측에서는 제어부의 통제하에 통신모듈이 단말로부터 전송된 메시지를 수신한다. 그리고 메시지 분석부가 수신된 메시지를 분석하고 그 중 인증과 관련된 코드를 분리한다. 인증처리부는 서버내에 저장되어 있는 가입자의 인증코드와 단말로부터 수신된 가입자의 인증코드를 비교한다. 유동적 USIM 카드를 장착한 가입자가 인증절차를 통과하게 되면, 매번 호를 실행할 때마다 인증서버내의 카운터부가 가입자의 호를 레지스터에 기록한다. 전술한 인증서버내 논리적 구현도는 그림 3에 표시하였다.

Ⅲ. Flexible USIM 카드의 알고리즘

유동적 USIM 카드를 이용하는 방법에 있어서 본 논문에서는 시간기록계를 사용하는 방법과 유효횟수 확인 레지스터를 이용하는 방법을 제시하고자 한다. 다시 말해 사용자의 입장에서는 유동적 USIM 카드의 사용 시간과 횟수에 대한 제약 사항이 된다. 유동적 USIM 카드가 단말기에 장착되면, 기존의 USIM 카드를 통해 진행되었던 인증 절차에 대한 결과는 인증센터에서 잠시 비활성화 상태가 된다. 유동적 USIM 카드를 장착한 단말기의 전원이 인가되면, 단말기는 유동적 USIM 카드를 인지하게 되고, 디스플레이부로부터 사용자에 대한 정보를 받을 준비를 하게 된다. 이 유동적 USIM 카드를 이용한 인증절차가 진행되기 전에, 단말과 이동통신국 간의 안전한 통신을 위해 사용되는 비밀키 값이 사전에 공유되어야 한다. 식 1 에서와 같이 이동통신국이 인증센터로부터 특정한 비밀키 값을 수신하게 되면 식 2에서 보여주고 있듯이 단말기로 전달할 암호화된 킷값 (K1)을 이동통신국 고유값 (CellID)과 조합하여 생성하게 된다.

$$Auc: SecKey \rightarrow MobileStation \quad (1)$$

$$MobileStation: E(SecKey, CellID) = K_1 \rightarrow Mobile \quad (2)$$

다음으로 유동적 USIM 카드 사용자는 인증 절차에 따라 가입자번호 (A:MDN)와 주민등록번호 (B:ID)등의 개인화 정보를 단말에 입력한다. 이러한 사전정보는 가입자 인증을 위해 인증센터에 미리 공유되는 정보들이다. 단말기는 사용자로부터 입력 받은 정보에 근거하여 식3의 Update USIM Info 메시지 (K2)를 생성하게 된다.

$$Mobile: E(K_1, A+B) = K_2 \rightarrow MobileStation \quad (3)$$

Update USIM Info 메시지 (K2)는 이동통신국으로 전달된다. 이동통신국은 Update USIM Info 메시지를 이동통신국 고유값 (CellID)을 기반으로 복호화하여 인증확인 메시지 (K3)를 생성하여 인증센터로 전달한다(식4). 인증센터가 인증 확인 메시지를 전달받으면 메시지 분석부는 식5에 의해 메시지를 분석한다.

$$MobileStation: D(K_2, CellID) = K_3 \rightarrow Auc \quad (4)$$

$$Auc: D(K_3, SecKey) \quad (5)$$

분석된 메시지를 기반으로 유동적 USIM 에서 입력받은 값 (A:MDN), (B:ID)를 인증센터에 사전에 공유된 값 (MDN, ID)과 비교하게 된다. 두 값들이 서로 같음이 확인되면, 유동적 USIM 카드를 사용하기 위한 첫 인증단계가 완료된다.

3.1 시간기록계를 이용한 Flexible USIM 카드

다음은 시간기록계를 이용한 유동적 USIM 카드의 사용 제한방법이다. 사용자가 유동적 USIM 카드 사용등록을 하게 되면, 그 첫 사용시점에 대한 시간을 인증센터에 기록하게 된다. 미리 설정된 time_to_alive 전달인자에 따라 사용자가 매번 호를 시도할 때마다, 인증센터는 현재 시간과 최초 등록 시간을 확인하게 된다.

$$T_{available} = T_{current} - T_{activate} \quad (6)$$

$$T_{available} \begin{cases} \geq time\_to\_alive & (7) \\ < time\_to\_alive & (8) \end{cases}$$

$T_{available}$ 전달인자 값이(식6) time_to_alive 전달인자 값보다 작게 되면 인증센터는 이동통신국에 성공 메시지를 반환한다(식8). 만일 그렇지 않은 경우에는 이동통신국으로 실패 메시지를 반환하게 된다(식7). 이동통신국은 인증센터에서 받은 메시지를 근간으로 다음 호처리 절차를 진행하게 된다. 그림 4에서는 전술한 호처리의 내역을 단말기 (Mobile), 이동통신 교환국 (Switching Center) 그리고 인증센터(Auc)의 호 처리도를 통해 설명하고 있다. 인증센터가 Auth, Terminate Info. 메시지를 교환국에 전달하게 되면, 인증센터에 일시적으로 보류되었던 기존의 USIM 카드의 인증정보가 다시 활성화 되며, 유동적 USIM 카드는 비활성화 상태가 된다.

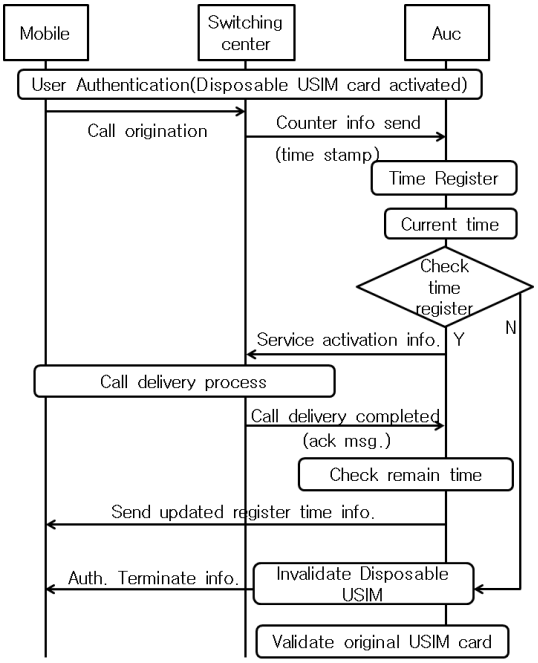

그림 4. 시간기록계를 이용한 유동적 범용가입 자개체모듈 카드 호처리도
Fig. 4 Call flow of flexible USIM card with timestamp

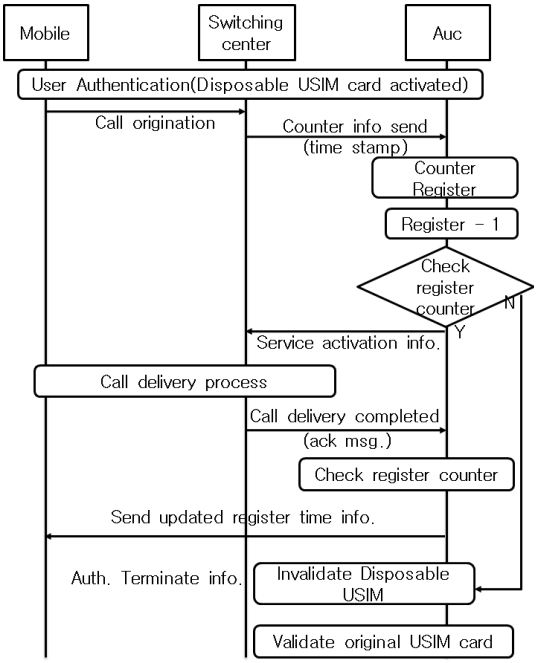

그림 5. 유효횟수 레지스터를 이용한 유동적 USIM 카드 호처리도
Fig. 5 Call flow of flexible USIM card with validation register

3.2 유효기간 레지스터를 이용한 Flexible USIM 카드

유효횟수 레지스터를 이용한 유동적 USIM 카드의 이용제한은 시간기록계를 사용한 방법과 유사하나 사용하는 횟수를 제한한다는 점에서 차이가 있다. 각각의 유동적 USIM 카드에는 호를 제한 할 수 있는 R_{active} 전달인자 있다. 인증센터는 이동통신국으로부터 전달받은 호 요청 메시지 횟수를 기록하는 R_{call} 전달인자를 이용하게 된다.

$$R_{available} = R_{active} - R_{call} \quad (9)$$

$$R_{available} \begin{cases} = 0 & (10) \\ > 0 & (11) \end{cases}$$

$R_{available}$ 전달인자가(식9) 0값을 가지게 되면 인증센터는 이동통신국에 실패 메시지를 반환하고 호를 종료시킨다(식10). $R_{available}$ 값이 0 보다 클 경우에는 계속하여 호를 진행한다(식11).

그림 5에서는 진술한 유효기간 레지스터를 이용한 알고리즘을 사용한 호 처리 내역을, 단말기(Mobile), 이동통신 교환국 (Switching Center) 그리고 인증센터 (Auc)의 호 처리도로 표시하였다. 마지막 호처리 단계에서 Auth. Terminate Info. 메세지를 인증센터가 발송하게 되면, 일시적으로 보류되었던 기존 USIM 인증 상태로 복구된다.

Ⅳ. 시뮬레이션 결과

본 장에서는 제안한 유동적 USIM 카드 인증시스템을 평가하기 위해 시스템을 구현해서 시뮬레이션을 수행하였다. 본 시뮬레이션에서 가상화를 통한 Windows

server 2008 R2 64bit 운영체제에서 4core/16Gbit memory 그리고 247GB HDD가 장착된 장비에서 C#언어를 이용하여 소켓 통신을 할 수 있는 프로그램을 하였다[7]. 시뮬레이션에서는 인증센터와 단말을 위한 가상의 client를 만들어 소켓통신을 하면서, 필요한 파라메터의 전달을 통해 통신결과를 테스트하였다. 유동적 USIM 카드를 시뮬레이션하기 위해 사용한 전달인자는 다음과 같다. 2장에 소개된 유동적 USIM 카드를 통한 사용자 인증을 위해 입력 받는 개인화 정보로, 1)가입자번호(MDN)는 11자리의 데이터를, 2)주민등록번호 (ID)는 13자리의 데이터를 사용한다. 시뮬레이션 모델을 구현하기 위해 6개의 추가적인 전달인자를 생성하여 유동적 USIM 카드의 상태를 표현하였다. 유동적 USIM 카드의 상태를 나타내는 3)Status (Active|Inactive) 전달인자, 최초 활성화 된 시간을 나타내는 4)Activation time, 만료시간을 나타내는데 사용되는 5)Expiration time (YYYYMMDDHHMM), 시도한 호의 수를 나타내는 6)Number of Calls(String), 시도할 수 있는 횟수 제한을 표현하는데 사용되는 7)Reg Available(String) 그리고 마지막까지 시도된 호의 횟수를 표현하는 8)Reg Last Call(String) 전달인자이다.

본 시뮬레이션을 통하여 소켓통신을 이용하여 필요한 파라메터들의 전달이 정상적으로 송수신 되는 것을 확인하였고 실제 H/W에 탑재 시에도 동일한 모듈을 사용 할 수 있다. 그림 6은 유동적 USIM 카드가 활성화 되었을 시의 인증센터 정보 3)Active를 나타낸다. 사용자는 시간기록계를 이용한 유동적 USIM 카드를 이용하고 있으며, 최초로 인증이 시작된 시간은 4)2011/08/01 23:30이다. 그리고 5) Expiration Time 전달인자에서 확인할 수 있듯이 사용에 대한 만료기간은 최초의 인증으로부터 24시간 뒤인 2011/08/02 23:30이다. 시간기록계 방식을 사용하고 있으므로, 유효횟수 레지스터를 이용시에 활성화되는 전달인자들은 비활성화되어 있음을 확인할 수 있다(그림 6의 7),8)). 유동적 USIM 카드의 상태확인 전달인자는 5) Expiration time 전달인자의 시간이 현재시간으로 도래하게 되면 Inactive 상태로 바뀌게 된다.

```
Mobile Station Category          : ORDINARY
Subscription Restriction         : NONE
Multi Number Flag                : OFF
Trace Activate In VLR            : OFF
IST Status                       : OFF
LCS Status                       : OFF
LSA Status                       : OFF
Regional Status                  : OFF
Password                         : 9696
Wrong Password Count             : 0
Check SS Indicator               : OFF
Preferred CID                    : 00345
CS Allocation/Retention priority : OFF
Send Routing Information         : All
Authentication Capability        : OFF
Origination Indicator            : World_Zone1
Authorization Period             : Indefinite
Authorization Period Value       : 0
Service Capability               : IMT-2000
RUIM                             : OFF
-------------------------------------------------
Mobile Directory Number          : 01012345678        1)
Social Security Number           : 8101171234567      2)
-------------------------------------------------
Disposable USIM Status           : Active             3)
Activation time                  : 2011080123:30      4)
Expiration time                  : 2011080223:30      5)
Number of Calls                  : 24                 6)
Reg Available                    : OFF                7)
Reg Last Call                    : OFF                8)
COMPLETED
```

그림 6. 유동적 USIM 카드를 이용한 가입자 정보
Fig. 6 Subscriber information with flexible USIM

V. 결 론

본 논문에서는 기존의 USIM 카드를 보다 사용자 편의 환경에서 사용할 수 있는 유동적 USIM 카드의 인증 시스템을 제안하였다. 특히 시간기록계를 이용하는 알고리즘과 유효횟수 레지스터를 이용한 알고리즘을 분석하였다. 시뮬레이션 결과 소켓통신을 이용하여 제안한 알고리즘 및 인증시스템이 잘 동작함을 확인하였으며 기존의 USIM 카드를 사용하는 인증방식과 잘 호환됨을 확인하였다. 제안한 유동적 USIM 카드를 이용하여 또 다른 인증방식을 설계할 수 있을 것이며 본 논문에서 소개된 방법을 통하여, 이동통신망 혹은 외부 환경요인에 무관한 자기 인증을 통한 접속을 가입자 및 망 운용자에게 제공할 수 있을 것이다. 본 제안을 토대로 제4세대 이동통신 단말에서의 유동적 USIM을 적용하는 방안에 대해서 더 많은 연구를 수행할 계획이다.

참고문헌

[1] ETSI. GSM Technical Specification. GSM 02.09 Security Aspects. Version 3.0.1, 1992

[2] 3GPP TR 33.919 v.7.2.0. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Generic Authentication Architecture (GAA); System description, Release 7, Mar. 2007.

[3] D. Song, S. Lim, O. Yi, J. Lim, "A Digital ID Purse Mechanism using USIM in a Mobile Environment," IIT 4th International Conf., pp. 670-674, Nov. 2007

[4] Jeong-Tae Kim, "A study on the efficient promotion of USIM-related services in Korea," ICACT. 11th International Conf., pp.347-349, Feb. 2009

[5] Josifovska, S., "The Queen of SIMs [mobile phones]," IEE Review. Comm. Vol.50, No.1, pp.26-27, Jan. 2004

[6] 3GPP.TS 33.102 V8.0.0. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture , Release 8, Jun. 2008

[7] Microsoft, http://www.microsoft.com

저자소개

최동욱(Dong wook Choi)

2005년 부경대 전자정보통신 공학과 (공학사)
2011년 부경대 정보통신공학과 석사과정수료

※관심분야 : 채널코딩, 다중접속기술 ,LBS

황재영(Jae-young Hwang)

2010년 부경대 전자정보통신 공학과 (공학사)
2010년~현재 부경대 정보통신공학과 석사과정

※관심분야 : 이동통신, 클라우드컴퓨팅

정연호(Yeon-ho Chung)

1984년 경북대학교 전자공학과 (공학사)
1992년 The Imperial College, University of London, U.K. (공학석사)
1996년 Liverpool University U.K. (공학박사)
1995년 영국 Freshfield Communications Ltd. 연구원
2004년 영국 Plymouth University 초빙연구원
2006년 미국 펜실베니아주립대학교 객원교수
2001년-현재 부경대학교 정보통신공학 교수

※관심분야 : 적응 변조 및 부호화 기술, OFDM, 반송파 간섭신호 기술, IDMA