3세대 이동통신 시스템에서의 보호

박영호*, 이창순**
* 상주대학교 전자전기공학과
** 경산대학교 정보과학부

Security for the 3rd-Generation Mobile Telecommunication System

Young-Ho Park*, Chang-Soon Lee**
* Department of Electronics and Electrical Engineering in Sangju National University
** School of Information Science in Kyungsan University

요 약 문

본 논문에서는 3GPP를 근간으로 3세대 이동통신에서의 보호에 관하여 소개한다. 3세대 이동통신 시스템에 보호기술을 제공하기 위한 2세대 이동통신 시스템의 결점과 3세대 이동통신 시스템에서의 보호원칙 및 보호목적을 기술한다. 3세대 이동통신 보호시스템은 네트워크 접근 보호, 네트워크 영역 보호, 사용자 영역 보호, 응용 영역 보호 및 visibility and configurability로 분류되며 각 보호영역에서 보호서비스들이 제공된다. 또한, 3세대 이동통신에서의 인증 및 키 일치 메카니즘 및 보호알고리즘에 관해서도 기술한다.

1. 서 론

시간과 장소에 구애받지 않는 자유로운 통신을 위한 욕구에 부응하여 등장한 것이 이동통신시스템이다. 이동통신시스템은 그 기능적인 면에서 아날로그 이동통신(1세대), 디지털 셀룰러 이동통신 및 개인휴대통신(2세대), 차세대이동통신(3세대) 등으로 분류된다[1,2,3]. 차세대 이동통신시스템의 근간이 될 IS-95[4]를 기반으로 한 IMT-2000(international mobile telecommunications in the year 2000)[5]과 GSM을 기반으로 한 UMTS(universal mobile telecommunication system)[6,7]의 경우 현재 표준화 진행 단계이며, 나머지 이동통신서비스는 많은 지역에서 서비스 제공 중이다. 이러한 다양한 이동통신서버스는 전파라는 무선매체를 사용하므로써 가입자에게 통화의 편리성을 제공하는 반면 통화도용의 가능성이 높으며 감시도 어렵다는 특징을 가지므로 정보보호가 요구된다[8].

차세대 이동통신시스템을 개발하기 위하여 ARIB, ETSI, T1, TTA, 그리고 TTC의 단체에서 공동으로 1998년 12월부터 3GPP(3rd generation partnership project)[9,10,11]를 수행하고 있으며 radio access network, core network 그리고 terminal 의 그룹으로 분류하여 개발하고 있다.

본 논문에서는 3GPP를 근간으로 3세대 이동통신에서의 보호에 관하여 소개한다. 3세대 이동통신 시스템에 보호기술을 제공하기 위해서 2세대 이동통신 시스템의 결점을 파악하며 3세대 이동통신 시스템에서의 보호원칙 및 보호목적을 제시하고 3세대 이동통신 시스템에서의 보호구조 및 각 보호영역에서 제공되는 보호서비스들을 기술한다. 또한, 3세대 이동통신에서 사용될 인증 및 키 일치 메카니즘 및 보호 알고리즘들을 기술한다.

2. 3G의 보호원칙 및 목적

2.1 보호원칙

3G 보호는 다음의 세가지 원칙이 있다.

1) 3G 보호는 2세대 시스템의 보호기반에서 구축된다. 3세대 보호를 위해 필요하거나 좋다고 입증된 GSM과 다른 2세대 시스템의 보호방식들은 3세대 보호에 채택된다.
2) 3G 보호는 2세대 시스템의 보호를 개선시킨다. 3G 보호는 2세대 시스템에서 인지된 결점들을 수정한다.
3) 3G 보호는 새로운 보호 특성들을 제공하고 3G에서 제공된 새로운 서비스들을 보호한다.

2.1.1 3G에서 사용하는 2세대 보호방식

3G에서는 다음의 2세대 보호방식들을 사용한다.

1) 서비스 접근을 위한 가입자 인증
2) 무선 인터페이스 암호화
3) 무선 인터페이스 상에서 가입자 신분 비밀보장
4) SIM(subscriber identity module)
5) SIM과 HN(home network) 서버 사이에 안전한 응용 계층 채널을 제공하는 SIM 응용 toolkit 보호 특성들
6) 사용자와 독립적인 보호 특성들의 동작
7) 보호기능의 단순화를 위하여 HE(home environment)는 SN(serving network)을 신뢰한다.

2.1.2 2세대 보호의 결점

3G 보호는 GSM 및 다른 2세대 시스템의 보호에서 다음의 결점들을 보완한다.

1) "false BTS"를 사용한 능동 공격이 가능
2) 암호화 키와 인증 데이터가 네트워크 사이와 네트워크 내에서 평문으로 전송되는 것
3) 암호화가 중심 네트워크까지 충분히 확장되지 않아서 무선 링크를 통한 사용자 데이터와 신호 데이터가 평문으로 전송 (GSM의 경우 BTS로부터 BSC까지)
4) 이전에 발생된 암호 키를 사용한 사용자 인증과 채널 가로채기에 대한 보호는 암호화의 사용에 의존하고 implicit 사용자 인증을 제공한다. 그러나 암호화는 어떤 네트워크에서는 사용되지 않으며 이 경우 부정조작의 가능성이 존재
5) 데이터 무결성이 제공되지 않음
6) IMEI(international mobile equipment identifier)는 안전하지 않음
7) 부정조작 및 LI(lawful interception)는 2세대 시스템의 설계시 고려되지 않았음
8) SN은 SN에서 로밍하고 있는 HE 가입자들을 위한 인증 파라메터들을 어떻게 사용하고 있는지에 대한 HE 인식 또는 제어가 전혀 없음
9) 2세대 시스템은 보호기능을 개선시킬 적응성을 가지지 않음

2.1.3 3G에서의 새로운 보호 특성 및 서비스 보호

현재 시점에서는 보호될 새로운 서비스 특성들을 열거할 수 없으나 이러한 특성들이 개발될 수 있는 환경은 기술할 수 있다. 3G 보호는 이러한 환경을 보호할 것이다. 새로운 서비스들이 개발될 환경은 다음 측면들로 분류된다.

1) 새롭고 다른 서비스 제공자들이 있을 것이다.
2) 3G 이동 시스템들은 사용자들을 위한 선호되는 통신 방법이 될 것이다.
3) 다양한 선불과 사용자 선택 지불 서비스들이 제공될 것이다.
4) 사용자들의 서비스 프로파일과 단말기의 성능에 대하여 사용자들이 증가된 제어를 가질 것이다.
5) 사용자들에 대한 능동적인 공격들이 있을 것이다.
6) 비음성 서비스들이 음성 서비스들과 같거나 더 중요한 서비스가 될 것이다.

7) 단말기가 전자상거래와 다른 응용들을 위한 플랫폼으로 사용될 것이다.

2.2 보호목적

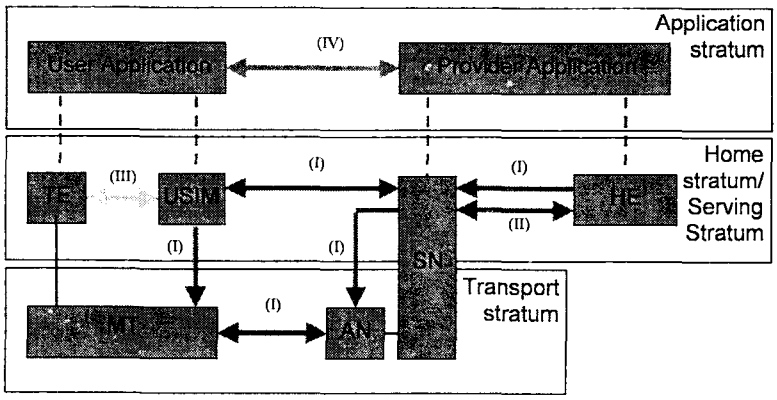
3G 보호를 위해 앞 절에서 언급된 것 외에도 다음의 목적들이 있다.

1) 사용자에 의해 생성되거나 사용자와 관련된 정보가 오용 또는 남용에 대해 적절하게 보호되는 것을 보장하는 것
2) 서비스 제공 네트워크들과 home 환경들이 제공하는 자원들과 서비스들이 오용 또는 남용에 대해 적절하게 보호되는 것을 보장하는 것
3) 표준화된 보호 특성들이 세계 어디서나 사용할 수 있도록 호환성을 유지하는 것을 보장하는 것
4) 보호 특성들이 범세계적인 상호작동과 다른 서비스 제공 네트워크들간의 로밍을 보장하기 위하여 적절하게 표준화되는 것을 보장하는 것
5) 사용자들과 서비스 제공자들이 사용할 수 있는 보호 수준이 현재의 고정망과 이동망들에서 제공되는 것보다 우수하다는 것을 보장하는 것
6) 3GPP 보호 특성들과 메카니즘들의 구현이 새로운 위협들과 서비스들의 요구에 따라 확장되거나 강화될 수 있는 것을 보장하는 것

3. 3G의 보호구조

3G 보호는 보호를 다음과 같이 5개의 영역으로 분류하여 정의하며 구조는 그림 1과 같다.

1) 네트워크 접근 보호 (network access security)
   네트워크 접근 보호는 3G 서비스에 안전한 접근을 제공하며 특히, 무선 접근 링크 상에서의 공격에 대해 보호한다.
2) 네트워크 영역 보호 (network domain security)
   네트워크 영역 보호는 서비스 제공 영역의 노드들이 신호 데이터를 안전하게 교환하도록 하며 유선 네트워크 상에서의 공격에 대해 보호한다.
3) 사용자 영역 보호 (user domain security)
   사용자 영역 보호는 이동국으로의 안전한 접근을 가능하게 한다.
4) 응용 영역 보호 (application domain security)
   응용 영역 보호는 사용자와 서비스 제공 영역에서의 응용들이 안전한 메시지 교환이 가능하게 한다.
5) visibility and configurability
   visibility and configurability는 보호 특성들이 동작되는지 그리고 서비스들의 사용이 보호 특성에 관계되는지를 사용자에게 통보를 가능하게 한다.



(I) Network access security
(II) Network domain security

(III) User domain security
(IV) Application domain security

Fig 1. Overview of the security architecture.

3.1 네트워크 접근 보호

3.1.1 사용자 신분 비밀보장

사용자 신분 비밀보장에 관련된 보호특성들은 다음과 같다.

- 사용자 신분 비밀보장
- 사용자 위치 비밀보장
- 사용자 추적불능

이러한 특성들을 제공하기 위해서, 사용자는 방문 네트워크에 알려진 일시적인 식별이나 암호화된 영구적인 식별자에 의해 식별되어진다. 사용자 추적을 피하기 위해서는 사용자는 동일한 식별자(일시적인 혹은 암호화된)의 방법에 의하여 오랜 기간동안 식별되지 않아야 한다. 이러한 특성들을 제공하기 위해서는 사용자 식별을 나타내는 어떤 신호와 사용자 데이터는 무선링크 상에서 암호화되어야 한다는 것이 요구된다.

3.1.2 개체 인증

개체 인증에 관련된 보호특성들은 다음과 같다.

- 인증 메카니즘 일치
- 사용자 인증
- 네트워크 인증

이러한 특성들을 제공하기 위해서는 사용자와 네트워크 사이에서 각각의 접속 설립시 개체인증이 이루어져야 한다고 가정된다. 개체 인증은 사용자의 ME에 의해 서비스 제공 네트워크로 전달된 인증 벡터를 사용한 인증 메카니즘과 사용자와 서비스 제공 네트워크 사이에 설립된 무결성 키를 사용한 국부 인증 메카니즘을 포함한다.

3.1.3 비밀보장

네트워크 링크 상에서 데이터의 비밀보장에 관련된 보호특성들은 다음과 같다.

- 암호화 알고리즘 일치
- 암호화 키 일치
- 사용자 데이터의 비밀보장
- 신호 데이터의 비밀보장

암호화 키 일치는 인증과 키 일치를 위한 메카니즘의 실행과정에서 이루어진다. 암호화 알고리즘 일치는 사용자와 네트워크 사이의 보호 모드 협상을 위한 메카니즘의 방법들에 의해 이루어진다.

3.1.4 데이터 무결성

네트워크 링크 상에서 데이터의 무결성에 관련된 보호특성들은 다음과 같다.

- 무결성 알고리즘 일치
- 무결성 키 일치
- 신호 데이터의 데이터 무결성과 발신지 인증

무결성 키 일치는 인증과 키 일치를 위한 메카니즘의 실행과정에서 이루어진다. 무결성 알고리즘 일치는 사용자와 네트워크 사이의 보호 모드 협상을 위한 메카니즘의 방법들에 의해 이루어진다.

3.1.5 이동 장비 식별

SN은 MS에게 터미널의 이동장비 식별을 보내도록 요구할 수 있다. 이동장비 식별은 긴급 call의 경

우를 제외하고는 SN의 인증 후에 보내진다. IMEI는 터미널 내에 안전하게 저장되어야 한다. 그러나, 네트워크에 이 식별의 공개는 보호특성이 아니며 IMEI의 전송이 보호되지 않는다. 비록 이 특성이 보호특성은 아니지만 다른 목적들에 유용하므로 UMTS(universal mobile telecommunication system)로부터 제거되어서는 안된다.

3.2 네트워크 영역 보호

3.2.1 개체 인증

네트워크 요소의 인증에 관련된 특성들은 다음과 같다.

- 인증 메카니즘 일치
- 네트워크 요소 인증

개체 인증 보호특성은 고의적으로 동작하는 혹은 지속적 명령어들이 침입자에 의하여 네트워크 영역으로 들어오지 못하게 한다. 이 특성은 데이터 교환전에 각각 다른 식별들을 증명할 수 있는 가능성을 가진 네트워크 요소들을 제공한다. 개체 인증은 explicit 나 implicit 인증 메카니즘에 의하여 이루어진다. Implicit 인증 메카니즘은 단지 암호화된 메시지를 교환함으로써 실현되며 분배된 키를 가진 개체는 데이터를 사용할 수 있다. Explicit 인증 메카니즘은 비대칭 프로토콜 혹은 대칭 프로토콜을 사용하여 실현될 수 있다.

3.2.2 데이터 비밀보장

네트워크 요소들 사이에 교환된 데이터 비밀보장에 관련된 보호특성들은 다음과 같다.

- 암호화 알고리즘 일치
- 암호화 키 일치
- 교환 데이터의 비밀보장

인증 데이터가 네트워크 영역에서 도청될 경우 심각한 부정적 문제들이 발생한다. 따라서 위의 보호특성들은 민감한 데이터의 비밀보장을 가능하게 한다. 암호화 알고리즘 일치와 암호화 키 일치 특성들은 네트워크 요소들에 의해 수행된 인증 메카니즘의 관점에서 실현될 수 있으며 일치된 암호화 키는 일치된 암호화 알고리즘에 의해 신호와 사용자 데이터를 보호하는데 사용된다.

3.2.3 데이터 무결성

두 네트워크 요소들 사이에 교환된 데이터 무결성에 관련된 보호특성들은 다음과 같다.

- 무결성 알고리즘 일치
- 무결성 키 일치
- 신호데이타의 데이터 무결성과 발신인증

신호데이터의 데이터 무결성 특성은 동작과 유지 명령어들 혹은 두 네트워크 요소들 사이에 교환된 사용자 데이터가 침입자에 의해 변경되지 않게 한다. 반면에 신호데이타의 데이터 무결성과 발신인증 특성은 고의적 동작과 유지 명령들이 침입자에 의해 네트워크 영역으로 들어올 수 없게 한다. 무결성 알고리즘과 키 일치 특성들은 네트워크 개체들에 의해 수신된 인증 메카니즘에 의해 실현되며 일치된 무결성 키는 일치된 무결성 알고리즘의 방법들에 의해 교환된 데이터의 무결성에 사용된다.

3.3 사용자 영역 보호

3.3.1 사용자와 USIM 간 인증

이 특성은 USIM이 사용자를 인증할 때까지 USIM로의 접근을 제한하는 것이다. 따라서, USIM에 접근은 권한이 부여된 사용자나 권한이 부여된 사용자들의 집단으로 제한 할 수 있다. 이 특성을 이루기 위해서는 사용자와 USIM은 USIM에 안전하게 저장된 비밀정보(PIN)를 공유해야 한다. 비밀정보를 가진 사용자만이 USIM에 접근한다.

3.3.2 USIM-터미널 링크

이 특성은 터미널이나 다른 사용자 장비에 대한 접근이 권한 있는 USIM로 제한하는 것이다. USIM과 터미널은 USIM과 터미널에 안전하게 저장된 비밀정보를 공유해야 한다. 만약, USIM이 비밀정보를 모르면 터미널에 접근할 수 없다.

3.4 응용 보호

3GMS 네트워크 상의 USIM에서 응용에 전송된 메시지를 보호하는데 관련된 보호특성들은 다음과 같다.

- 응용들의 개체 인증
- 응용 데이터의 데이터 발신처 인증
- 응용 데이터의 데이터 무결성
- 응용 데이터의 재사용 감지
- 응용 데이터의 순서 무결성
- 수신 증명
- 응용 데이터의 비밀보장

또한, 응용보호에는 네트워크 확장 사용자 트래픽 비밀보장, 사용자 프로파일 데이터 접근 및 IP 보호의 특성들이 있다.

3.5 visibility and configurability

3.5.1 visibility

일반적으로 보호 특성들은 사용자에 대해 투명해야 하지만, 특정 사건들에 대해서나 사용자의 관심에 따라서는 더 높은 보호 특성의 동작 투명성이 제공되어져야 한다. 이것은 사용자에게 보호관련 사건들을 통보하는 특성들을 가져온다.

- 접근 네트워크 암호화 표시
- 네트워크-확장 암호화 표시
- 보호 레벨 표시

3.5.2 configurability

사용자와 사용자의 HE가 서비스의 사용 또는 제공이 보호 특성이 동작중인지 아닌지에 의존해야 하는지의 여부를 설정할 수 있는 성질이다. 서비스는 서비스와 관계되고 사용자 또는 사용자의 HE의 구성들에 의하여 요구되는 모든 보호 특성들이 동작중인 경우에만 사용될 수 있다. 다음은 configurability 특성들이다.

- 사용자-USIM 인증 가능/불능
- 수신 비암화 call 수락/거부
- 비암호화 call 설정 혹은 비설정
- 암호화 알고리듬 사용 수락/거부

4. 인증 및 키 일치 메카니즘

이 메카니즘은 USIM과 사용자 HE의 AuC 사이에 분배된 비밀키 K로 사용자와 네트워크 사이에 상호인증을 한다. 이 방법은 현재 GSM 보호구조와 GSM에서 UMTS로의 이동을 가능하도록 하는 호환성을 가진 방식이다. 이 방식은 GSM 가입자 인증과 키 설정 프로토콜에 사용된 시도/응답 프로토콜과 ISO/IEC 9798-4에서 인용된 네트워크 인증을 위한 SN에 기초한 일방향 프로토콜의 결합된 방식이다. 그림 2는 인증 및 키 일치 메카니즘의 개략적 구조를 나타낸 것이다.

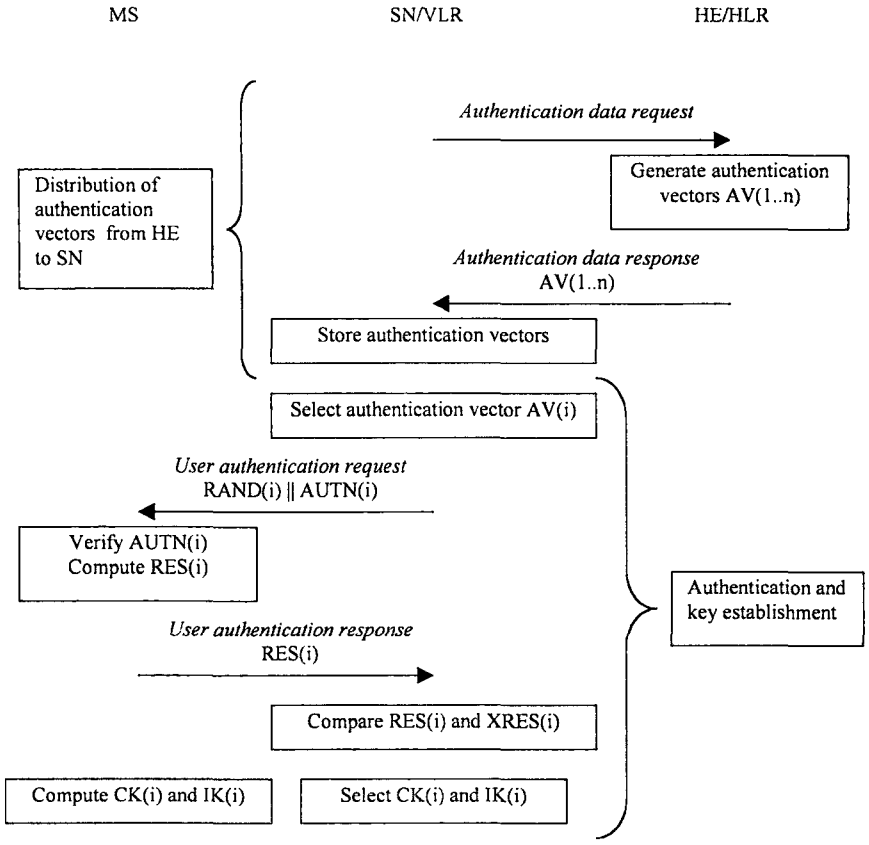


Fig. 2. Authentication and key agreement mechanism.

SN/VLR로부터 인증 데이타 요구를 수신하면 HE/AuC는 n개의 인증 벡터들의 열을 SN/VLR에 보낸다. 각 인증 벡터는 RAND, XRES, CK, IK 그리고 AUTN로 구성되며 SN/VLR과 USIM 사이에 인증과 키 일치를 위해 사용된다.

SN/VLR이 인증과 키 일치 과정을 시작하면 SN/VLR은 인증 벡터 열로부터 다음에 사용할 인증벡터를 선택하고 RAND와 AUTN을 사용자에게 전송한다. USIM은 수신된 AUTN 값을 검사한다. 만약, AUTN 값이 정확하면 SN/VLR에 보낼 RES 값을 발생한 후 CK와 IK 값을 구한다. SN/VLR은 수신된 RES와 XRES 값을 비교한다. 만약, 두 값이 일치하면 SN/VLR은 인증 및 키 분배 과정이 성공적으로 이루어졌다고 여긴다. 설정된 CK와 IK 값은 SN/VLR에 의해 암호화와 무결성 기능을 수행할 개체들로 전송된다.

4.1 인증 데이터 분배

이 절차는 사용자 인증을 수행하기 위해 HE로부터 인증 벡터열을 SN/VLR에 전송한다. 그림 3은 인증 데이터 분배 과정을 나타낸 것이다.

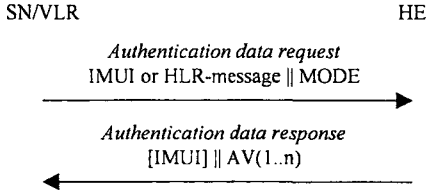


Fig. 3. Distribution of authentication data from HE to SN/VLR.

인증데이터 요구신호는 사용자 식별과 파라미터 모드로 구성되며 파라미터 모드는 요구노드가 PS 노

드인지 CS 노드인지를 나타낸다. 사용자가 IMUI에 의해 SN/VLR에서 식별된다면 인증데이터 요구신호는 IMUI를 포함한다. 사용자가 암호화된 영구 식별자에 의해 식별된다면 인증데이타 요구신호는 HLR-메세지를 포함하고 HLR에 사용자 식별 요구절차가 요구된다.

HE가 SN/VLR로부터 인증 요구신호를 수신하면 HE/AuC는 n개의 인증벡터 AV(1...n) 열을 SN/VLR로 전송한다. 인증벡터는 HLR 데이터 베이스에서 취할 수 있으며 요구에 따라 계산할 수도 있다. 그림 4는 HE/AuC에서의 인증벡터 발생을 나타낸 것이다.

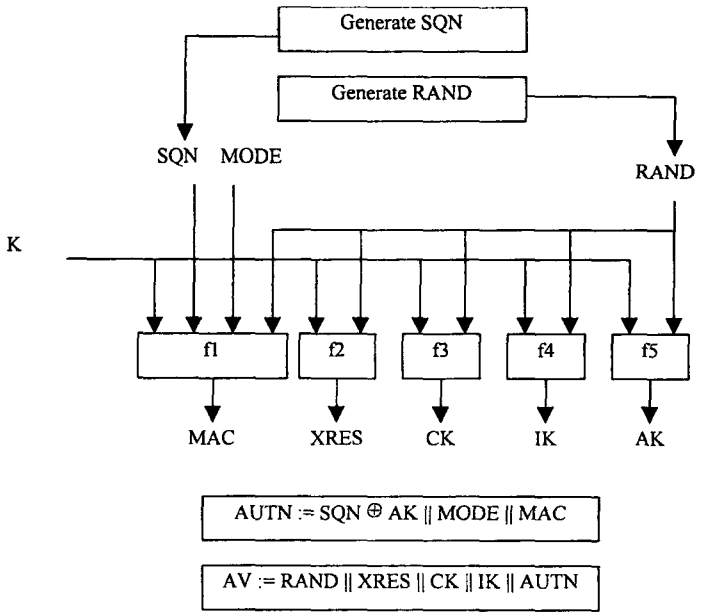


Fig. 4. Generation of an authentication vector.

HE/AuC는 새로운 순서번호 SQN과 예측할 수 없는 시도값 RAND를 발생한다. HE/AuC는 각 사용자에 대해 $SQN_{HE/CS}$와 $SQN_{HE/PS}$를 가진다. 여기서 $SQN_{HE/CS}$는 CS CN 노드들에서 시작된 인증을 위한 값이며 $SQN_{HE/PS}$는 PS CN 노드들에서 시작된 인증을 위한 값이다. 새로운 순서번호를 발생하기 위하여 카운터 값이 증가되며 추후 SQN은 새로운 값으로 설정된다. MAC, XRES, CK, IK 및 AK는 다음과 같이 발생된다.

$MAC = f1_k(SQN \,||\, RAND \,||\, MODE)$

$XRES = f2_k(RAND)$

$CK = f3_k(RAND)$

$IK = f4_k(RAND)$

$AK = f5_k(RAND)$

여기서, f1 및 f2는 메시지 인증 함수이며 f3, f4 및 f5는 키 발생함수이다. 또한, AK는 사용자 식별과 위치를 노출할 수 있는 순서번호를 보호하는데 사용된 익명의 키다. 인증 토큰 값은 $AUTN = SQN \oplus AK \,||\, MODE \,||\, MAC$ 과 같이 구성된다.

4.2 인증과 키 일치

이 절차의 목적은 사용자를 인증하고 SN/VLR과 MS 사이에 암호화와 무결성 키를 설정하는 것이다. 그림 5는 인증과 키 설정 과정을 나타낸 것이다.

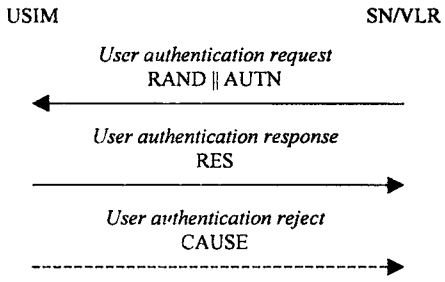


Fig. 5. Authentication and key establishment.

SN/VLR은 VLR 데이터 베이스의 인증벡터 열로부터 사용하지 않은 인증벡터를 선택한다. SN/VLR은 랜덤 시도값 RAND와 인증 토큰 AUTN을 전송한다. 사용자 인증 요구신호를 수신한 사용자는 그림 6의 과정을 수행한다.

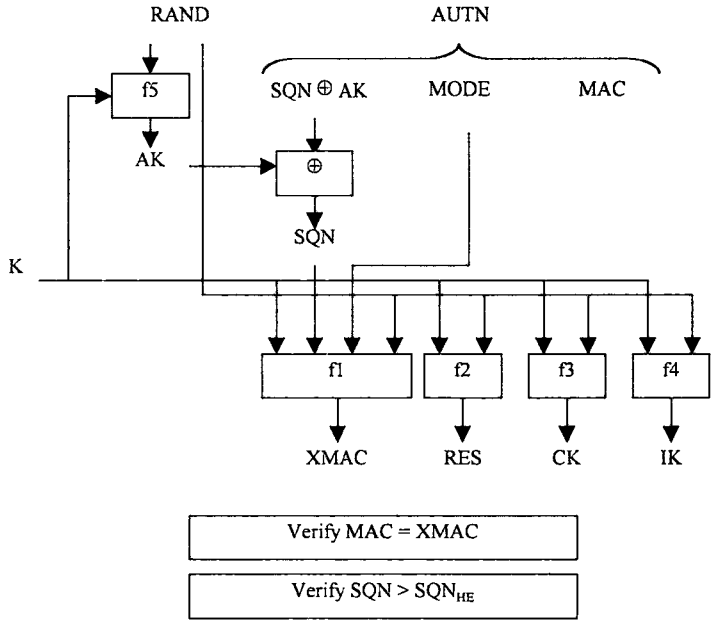


Fig. 6. User authentication function in the USIM.

RAND와 AUTN을 수신한 사용자는 먼저 AK를 계산하고 SQN을 계산한다. 다음에 사용자는 XMAC = $f1_k$(SQN || RAND || MODE)를 계산하고 AUTN에 포함된 MAC 값과 비교한다. 만약 두 값이 다르면 SN/VLR에 사용자 인증 거부 신호를 전송한다. 수신된 SQN 값이 정확한 범위에 있는지를 검사한다. USIM은 각 모드에 대해 하나의 카운터 경로를 가진다. $SQN_{MS/CS}$는 CS CN 노드들에서 시작된 인증을 위한 값이며 $SQN_{MS/PS}$는 PS CN 노드들에서 시작된 인증을 위한 값이다.

순서번호 SQN이 정확한 범위에 있는지 검사하기 위하여 USIM은 SQN과 $SQN_{MS/MODE}$ 값을 비교한다. 만약 SQN 값이 $SQN_{MS/MODE}$ 값보다 크면 MS는 순서번호가 정확한 범위에 있는 것으로 간주하고 $SQN_{MS/MODE}$ 값을 SQN 값으로 대치한다. 만약 순서번호가 정확한 범위에 있지 않으면 사용자는 SN/VLR에 동기 실패 신호를 전송하고 이후 절차를 포기한다. 동기실패 메시지는 $RAND_{MS}$와 AUTS로 구성된다. $RAND_{MS}$는 MS에 저장된 랜덤 값이며 SQN_{MS}의 최근 갱신에 의한 사용자 인증요구 신호에서 수신된다. AUTS, $Conc(SQN_{MS})$ 및 MACS 값은 다음의 과정에 의해 계산된다.

$AUTS = Conc(SQN_{MS}) \,||\, MACS.$

$Conc(SQN_{MS}) = SQN_{MS} \oplus f5_K(RAND_{MS})$

$MACS = f1^*_k(SQN_{MS} \,||\, RAND \,||\, MODE)$

여기서, $Conc(SQN_{MS})$는 MS에서 SQN_{MS}를 보호한 값이고 RAND는 현재 사용자 인증 요구에서 수신된 랜덤 값이며 $f1^*$는 MAC 발생 함수 값이다. 그림 7은 AUTS 구성을 나타낸 것이다.

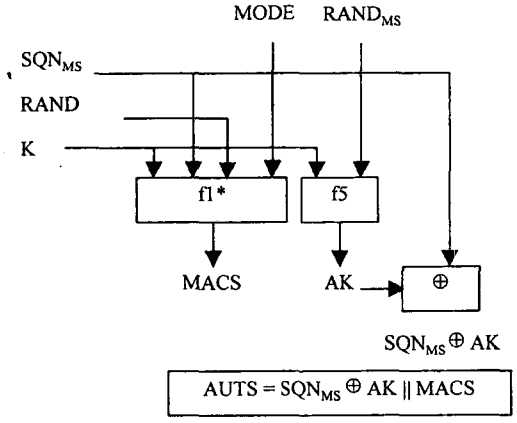


Fig. 7. Construction of the parameter AUTS.

만약, 순서번호가 정확한 범위에 있으면 사용자는 $RES = f2_k(RAND)$ 값을 구하고 암호 키 $CK = f3_k(RAND)$ 와 무결성 키 $IK = f4_k(RAND)$를 계산한다.
SN/VLR은 사용자 인증 응답신호를 수신하면 수신된 RES 값와 인증벡터 내의 XRES 값을 비교한다. 만약, 두 값이 일치하면 SN/VLR은 사용자 인증이 이루어 진다고 여기고 선택된 인증벡터로부터 CK와 IK 값을 선택한다.

4.3 보호 알고리즘

3G의 인증 및 키 일치 알고리즘에 사용된 보호 알고리즘의 형태 및 기능은 다음과 같다.

1) f0

f0는 랜덤 수 발생 함수이며 128 비트의 RAND 값을 발생한다.

f0 : (internal state) -> RAND

2) f1

f1은 네트워크 인증 함수이며 64 비트의 MAC 값을 발생한다.

f1 : (K: SQN, RAND, MODE) -> MAC-A(or XMAC-A)

여기서, SQN은 32 혹은 64비트의 순서 번호이며 MODE는 1비트로 하나 이상의 이동관리 실체가 한 사용자에 대해 동시에 동작되었을 때 이동관리의 실체를 식별한다. 사용된 키 K는 128비트이고 발생된 MAC 값은 64비트이다.

3) f1*

f1*은 재동기 메시지 인증 함수이며 64 비트의 MAC 값을 발생한다.

f1* : (K: SQN, RAND, MODE) -> MAC-S(or XMAC-S)

4) f2

f2는 사용자 인증함수이며 128 비트(최소 32비트)의 RES 값을 발생한다.

f2 : (K: RAND) -> RES(or XRES)

5) f3

f3은 암호화 키 발생함수이며 128비트의 CK 값을 발생한다.

f3 : (K: RAND) -> CK

6) f4

f4는 무결성 키 발생함수이며 128비트의 IK 값을 발생한다.

f4 : (K: RAND) -> IK

7) f5
f5는 익명 키 발생함수이며 32 혹은 64비트의 AK 값을 발생한다.
f5 : (K: RAND) -> AK

위의 함수들에 사용된 키 K는 128비트로 USIM과 AuC에 저장된 long term 비밀 키이다.

5. 결 론

본 논문에서는 3GPP를 근간으로 3세대 이동통신에서의 보호에 관하여 기술하였다. 3세대 이동통신 시스템에 보호기술을 제공하기 위한 2세대 이동통신 시스템의 결점과 3세대 이동통신 시스템에서의 보호원칙 및 보호목적을 기술하였다. 3세대 이동통신 보호시스템은 네트워크 접근 보호, 네트워크 영역 보호, 사용자 영역 보호, 응용 영역 보호 및 visibility and configurability로 분류되며 각 보호영역에서 보호서비스들이 제공된다. 3세대 이동통신에서의 인증 및 키 일치 메카니즘은 GSM 가입자 인증과 키 설정 프로토콜에 사용된 시도/응답 프로토콜과 ISO/IEC 9798-4의 네트워크 인증을 위한 SN에 기초한 일방향 프로토콜의 결합된 방식이며 인증 벡터를 사용한다. 3GPP의 연구결과는 3세대 이동통신 보호시스템의 근간이 될 것이며 차후 이러한 내용에 기초하여 새로운 방식의 보호 메카니즘 및 보호 알고리즘들이 개발될 것이다.

참 고 문 헌

[1] L.N.Kriaras, A.W.Jarvis, V.E.Phillips, and D.J.Richards,"Third-Generation Mobile Network Architecture for the Universal Mobile Telecommunications System," Bell Labs Technical Journal, pp.99-117, Summer 1997.

[2] E.Dahlman, B.Gudmundson, M.Nilsson, and J.Skold,"UMTS/IMT-2000 Based on Wideband CDMA," IEEE Communications Magazine, pp.70-80, September 1998.

[3] L.Hagen, M.Breugst, and T.Magedanz,"Impacts of Mobile Agent Technology on Mobile Communication System Evolution," IEEE Personal Communications, pp.56-69, August 1998.

[4] TIA IS-54 Appendix A. *Dual Mode Cellular System: Authentication, Message Encryption, Voice Privacy Mask Generation, Shared Secret Data Generation, A key Verification, and Test Data*, Feb. 1992.

[5] T. Ojanpera and R.Prasad "An Overview of Air Interface Multiple Access for IMT-2000/UMTS," IEEE Communications Magazine, pp.82-95, September 1998.

[6] ETSI, *European Digital Cellular Telecommunication System(phase 2) - Security Related Network Functions*, July 1993.

[7] J. C. Francis, H. Herbrig, and N. Jefferies, "Secure Provision of UMTS Services over Diverse Access Networks", IEEE Communications Magazine, pp.128-136, Feb. 1998.

[8] M.S.Greenberg, J.C.Byington, and D.G.Harper "Mobile Agents and Security," IEEE Communications Magazine, pp.76-85, July 1998.

[9] 3G TS 33.102, *Security Architecture*, 3rd Generation Partnership Project(3GPP): Technical Specification Group(TGS) SA: 3G Security, July 1999

[10] 3G TS 33.105, *Cryptographic Algorithm Requirements*, 3rd Generation Partnership Project(3GPP): Technical Specification Group(TGS) SA: 3G Security, July 1999

[11] 3G TS 33.120, *Security Principles and Objectives*, 3rd Generation Partnership Project(3GPP): Technical Specification Group(TGS) SA: 3G Security, May 1999