情報保護學會論文誌
第13券 第4號, 2003. 8

UMTS와 GSM 사이의 AKA와 핸드오버 분석

이 세 광*, 조 승 환*, 이 옥 연**, 서 창 호***

Analysis of AKA and handover between UMTS and GSM

Se-Kwang Lee*, Seung-Hwan Jo*, Ok-Yeon Yi**, Chang-Ho Seo***

요 약

본 논문은 GSM(유럽형 2세대 이동통신) 시스템과 UMTS(유럽형 3세대 이동통신) 시스템 사이의 키 일치 관점에서의 핸드오버를 알아보기 위해 GSM 시스템과 UMTS 시스템의 네트워크 구조[1]를 분석하고, 무선구간에서의 안전한 통신을 위해 필요한 각 시스템의 인증과 키 일치(AKA)과정을 분석하였다. 서비스를 이용하고자 하는 이동통신 가입자가 위치해 있는 시스템에서 인증과 키 일치가 이루어지는 과정을 가능한 여러 가지 경우로 나누어 분석하고, 핸드오버 시 무선 구간에서 안전하게 사용자 데이터를 주고받기 위해 키 일치가 이루어지는 과정을 CS-Domain과 PS-Domain으로 나누어 분석하였다.

ABSTRACT

In this paper, we analyze the network architecture, authentication, and key agreement of GSM and UMTS to compare the handover between the systems. And then, we divide authentication and key agreement procedure of mobile subscribers into several cases and finally analyze the key agreement procedure when a handover occurs in a CS-Domain and a PS-Domain.

keyword : *GSM, UMTS, AKA, 핸드오버*

Ⅰ. 소 개

주로 유럽에서 서비스가 제공되고 있는 비동기식 이동통신은 암호학적 메커니즘을 사용하기 시작한 2세대 이동통신 GSM에서 출발하여 3세대 이동통신인 UMTS가 현재 진행 중에 있다. 한편, 국내에서는 아날로그 방식의 1세대를 거쳐 현재 동기식의 2세대가 서비스되고 있으며 비동기식과 동기식의 3세대 이동통신의 상용서비스가 준비되고 있는 상황이다.

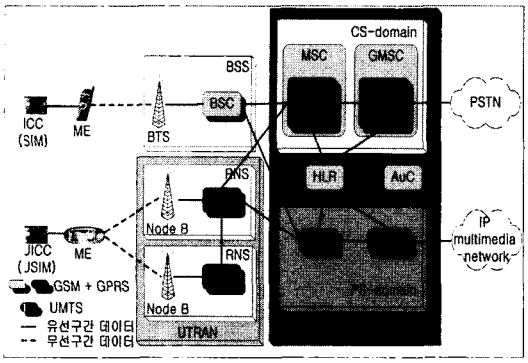
이처럼 2세대 네트워크가 구축되어 있는 상황에서 3세대 네트워크를 지원하는 시스템이 개발 될 때는 2세대와 3세대 이동통신의 로밍이 원활하게 이루어져야 할 것이다. 국내에서 비동기식 3세대 이동통신 서비스를 사용한다면 네트워크 전체가 비동기식 3세대에 맞춰져 있어서 문제가 되지 않을 수도 있지만, 국제 로밍이 이루어지기 위해서는 3세대뿐만 아니라 2세대 이동통신 서비스가 지원되어야 한다.

본 논문은 GSM이나 UMTS 가입자에게 필요한 시스템간의 핸드오버를 인증과 키 일치를 중심으로 살펴본다.

Ⅱ. 네트워크 아키텍쳐

이 절은 핸드오버를 위한 GSM과 UMTS의 전체적

* 고려대학교 정보보호대학원({gausslee, hongcha}@cist.korea.ac.kr)
** 국민대학교 자연과학대학 수학과(oyyi@kookmin.ac.kr)
*** 공주대학교 응용수학과(chseo@kongju.ac.kr)



〔그림 1〕 GSM과 UMTS의 기본 아키텍쳐

인 시스템 구성 요소와 구조를 설명한다.

위 [그림 1]은 GPRS(General Packet Radio Service)를 지원하는 GSM과 UMTS의 기본 아키텍쳐를 나타내고 있다.

1) ICC(Integrated Circuit Card) : 물리적이고 논리적인 entity로서 SIM application이 지원된다.
   - SIM(GSM Subscriber Identity Module) : ME에 삽입될 ICC에서 실행되는 모듈로서, GSM AKA (Authentication and Key Agreement)를 위해 필요한 가입자 고유의 키(K_i)와 IMSI(International Mobile Subscriber Identity) 등의 사용자 비밀 정보와 암호 알고리즘이 저장되어 있다.
2) UICC(Universal Intergrated Circuit Card) : UMTS에 대한 물리적이고 논리적인 플랫폼으로서, USIM application이 지원되며 SIM application이 지원되기도 한다.
   - USIM(Universal Subscriber Identity Module) : SIM과 유사한 기능을 수행하며, UMTS AKA를 위해 필요한 가입자 고유 키(K)와 IMSI 등의 사용자 비밀 정보와 암호 알고리즘이 저장되어 있다.
3) ME(Mobile Equipment) : ICC나 UICC가 삽입될 단말기로서, BTS나 Node B와의 무선 구간에서 암복호화나 무결성을 확인하는 기능을 보유하고 있다.
4) BSS(Base Station System) : GSM 네트워크에서 ME와 CN(Core Network)을 연결하는 GSM에서의 AN (Access Network)으로서, BTS와 BSC로 구성되어 있다.
   - BTS(Base Transceiver Station) : ME와 무선 구간으로 연결되며, GSM에서 암복호화 기능을 보유하고 있다.
   - BSC(Base Station Controller) : BTS를 제어하는 노드로서, MSC/VLR이나 SGSN과 연결된다.
5) UTRAN(Universal Terrestrial Radio Access Network) : ME와 CN을 연결하는 UMTS에서의 AN으로서 RNS의 집합체이다.
6) RNS(Radio Network Subsystem) : UMTS 네트워크에서 ME와 CN를 연결하며, Node B와 RNC로 구성되어 있다.
   - Node B : UMTS에서 BTS이며, BSS의 BTS와는 달리 암복호화 기능을 보유하고 있지 않다.
   - RNC(Radio Network Controller) : Node B를 제어하며, MSC/VLR이나 SGSN과 연결된다. 암복호화 및 무결성 서비스를 수행한다.
7) MSC/VLR(Mobile Switching Centre/ Visitor Location Register) : MSC/VLR area에 위치하는 모든 MS (ME + SIM/USIM)에 대한 정보를 등록하고 다른 MSC/VLR이나 SGSN에게 그 정보들을 전달한다. CS(Circuit Switched) 서비스를 제공한다. 사용자가 BSS에 접근했을 때, 사용자가 MSC/VLR로부터 서비스를 받으면 GSM 암호화 키 Kc를 BTS에게 전송한다. 핸드오버 시 처음의 MSC/VLR는 서비스 전체에 걸쳐서 anchor point의 역할을 한다.
8) GMSC(Gateway MSC) : MS의 실제 위치에서 라우팅 기능을 이행할 수 있게 하는 MSC이다.
9) GPRS(General Packet Radio Service) : SGSN과 GGSN으로 구성되며 packet service를 지원한다.
   - SGSN(Serving GPRS Support Node) : SGSN area에 위치하는 각각의 가입자에 대한 PS(Packet Switched) service에 대하여 가입정보와 위치정보를 저장한다. 다른 MSC/VLR이나 SGSN에게 그 정보들을 전달한다. 사용자가 BSS에 접근했을 때, 사용자가 SGSN으로부터 서비스를 받으면 GSM 암호화 키 Kc를 자체적으로 사용한다. 핸드오버 시 이동하게 된 다른 SGSN이 서비스 전체에 걸쳐서 anchor point의 역할을 한다.
   - GGSN(Gateway GPRS Support Node) : HLR과 SGSN에서 수신한 가입자 데이터를 저장한다.
10) HLR(Home Location Register) : Mobile 가입자에 대한 가입정보를 등록하며, MSC/VLR이나 SGSN에게 전달한다.
11) AuC(Authentication Centre) : 가입자나 네트워크(MSC/VLR이나 SGSN)가 상호인증을 위해 사용하는 정보(IMSI, K, K_i 등)를 저장하고 HLR에게 전달한다. 또한 인증에 필요한 RAND 등을 생성

한다.

Ⅲ. 인증과 키 일치(AKA, Authentication and Key Agreement)

이 절은 이동통신 서비스 가입자가 사용자에 대한 인증 절차(Authentication)와 무선 구간에서 암복호화와 무결성 보호를 하기 위해 필요한 동일한 키 값을 서로 공유하기 위한 과정(Key Agreement)을 GSM과 UMTS로 나누어 설명한다.

3.1 GSM AKA[2]

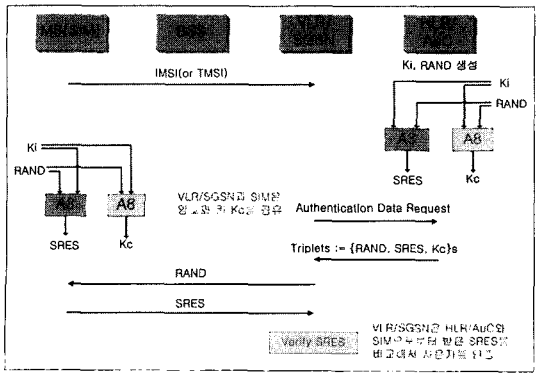
GSM AKA는 네트워크가 가입자를 인증하기 위해 필요한 정보와 무선구간에서 암복호화를 위해 사용될 암호화 키(Kc)를 SIM과 MSC/VLR이 공유하기 위한 과정이다. [그림 2]는 GSM 네트워크에서 행해지는 인증과 키 일치 과정을 보여준다.

1) K_i : 각각의 가입자에 대한 고유 비밀키로서, AuC와 SIM내에 저장되며 A3, A8의 입력값으로 사용된다.
2) RAND : AuC가 생성하는 난수로서 VLR/SGSN을 통해 SIM에 전달되며 A3, A8의 입력으로 사용된다.
3) TMSI(Temporary Mobile Subscriber Identity) : 임시 가입자 식별값으로서 VLR/SGSN에서 생성되며 SIM과 VLR/SGSN에 저장된다.
4) IMSI(International Mobile Subscriber Identity) : 영구적 가입자 식별값으로서 AuC에서 각 사용자마다 다른 값을 저장하고 SIM에도 저장한다. 초기에 가입자를 식별할 때나 TMSI로 식별이 되지 않을 때 사용된다.
5) A3 : 인증 알고리즘으로서 K_i와 RAND를 통해 SRES를 생성하며 AuC와 SIM 내에서 실행된다.
6) A8 : 암호화 키 생성 알고리즘으로서 K_i 와 RAND를 통해 암호화 키 Kc를 생성하며 AuC와 SIM 내에서 실행된다.
7) Triplet : GSM에서 사용되는 인증 벡터로서 AuC에 의해 생성되고 VLR/SGSN에게 전달된다. Kc, RAND, SRES로 구성된다.
8) SRES : 네트워크(VLR/SGSN)가 사용자를 인증하기 위해 필요한 값으로 AuC가 A3을 통해 얻은 다음 VLR/SGSN에게 전송한다.
9) Kc : 무선구간에서 암복호화 시 사용되는 키 값으로 AuC와 SIM에서 A8을 통해 얻어지고 암복호화에 사용된다.

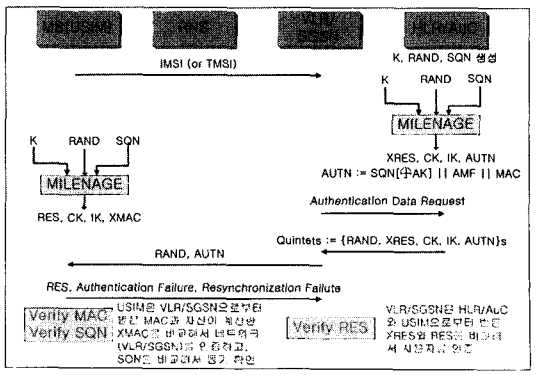
3.2 UMTS AKA[3]

UMTS AKA는 네트워크가 가입자를 인증하고 가입자가 네트워크를 인증하는 양방향 인증을 제공하고, 무선구간에서 암복호화와 무결성을 확인하기 위해 사용할 암호화 키(CK)와 무결성 키(IK)를 USIM과 VLR/SGSN이 서로 공유하기 위한 과정이다. [그림 3]은 UMTS 네트워크에서 행해지는 인증과 키 일치 과정을 보여준다.

1) f0 : 난수 생성 함수로서 RAND를 생성한다.
2) f1 : 네트워크 인증 함수로서 K, AMF, SQN(Sequence number), RAND를 통해서 MAC-A(XMAC-A)를 생성한다.
3) f1* : 재동기 시 필요한 네트워크 인증 함수로서 K, AMF, SQN, RAND를 통해 MAC-S(XMAC-S)를 생성한다.



〔그림 2〕 GSM에서의 인증과 키 일치 과정



〔그림 3〕 UMTS에서의 인증과 키 일치 과정

4) f2 : 사용자 인증 함수로서 K와 RAND를 통해 RES (XRES)를 생성한다.
5) f3 : 암호화 키 생성 함수로서 K, RAND를 통해 CK를 생성한다.
6) f4 : 무결성 키 생성 함수로서 K, RAND를 통해 IK를 생성한다.
7) f5 : 익명성 키 생성 함수로서 K, RAND를 통해 AK를 생성한다.
8) f5* : 재동기 시 필요한 익명성 키 생성 함수로서 K, RAND를 통해 AK를 생성한다.
9) AMF(Authentication Management Field) : 인증 관리 필드로서, 특정 인증 벡터를 생성하기 위해 사용되는 알고리즘과 키를 지적하는 것에 사용되어진다. 이 값의 사용은 표준화되지 않았다.
10) MILENAGE(3G 알고리즘) : 3GPP 표준에 제안된 UMTS에서의 인증 메커니즘이다.
11) TMSI(Temporary Mobile Subscriber Identity) : GSM에서와 동일하며, GSM에서와 다른 점은 이 값이 USIM과 VLR/SGSN에 저장된다는 것이다.
12) IMSI(International Mobile Subscriber Identity) : GSM에서와 동일하며, GSM에서와 다른 점은 이 값이 USIM에 저장된다는 것이다.
13) K : 각각의 가입자에 대한 고유 비밀키로서, AuC와 USIM내에 저장되며 f1, f1*, f2, f3, f4, f5, f5*의 입력값으로 사용된다.
14) Quintet : UMTS에서 사용되는 인증 벡터로서, AuC에 의해 생성되고 VLR/SGSN에게 전달된다. RAND, XRES, CK, IK, AUTN으로 구성된다.
15) RAND : AuC에 의해 생성되는 난수로서 f1, f1*, f2, f3, f4, f5, f5*의 입력값으로 사용된다.
16) XRES(또는 RES) : 네트워크(VLR/SGSN)가 가입자를 인증하기 위해 사용하는 값으로, AuC(또는 USIM)가 f2 함수를 통해 얻은 다음 네트워크에게 전송한다.
17) CK : 무선구간에서 암복호화를 하기 위해 사용되는 암호화 키로서, AuC와 USIM이 f3 함수를 통해 얻은 다음 암복호화에 사용된다.
18) IK : 무선구간에서 무결성 보호를 위해 사용되는 무결성 키로서, AuC와 USIM이 f4 함수를 통해 얻은 다음 무결성을 보호하는 데에 사용된다.
19) AUTN : 가입자가 네트워크를 인증하기 위해 사용되는 값으로, SQN[⊕AK], AMF, MAC으로 구성된다.

Ⅳ. UICC와 ICC 사용자에 대한 AKA

4.1 용어 설명

UMTS 네트워크나 GSM 네트워크를 통해 가입자에 대한 인증과 키 일치를 위해 필요한 각 노드를 2G와 3G로 나누어 살펴보고, 본 논문에서 사용되어지는 용어와 서비스에 대한 내용에 대해서 살펴보겠다.

1) 2G = GSM = Release 98-
2) 3G = UMTS = Release 99+
3) HLR/AuC
   - Release 98- : R97이나 R98 버전을 따르는 HLR/AuC로서 GSM과 GPRS 서비스를 지원하며, 인증벡터 Triplet을 생성한다. 단지 GSM AKA만을 실행하고, 변환 함수를 지원하지 않는다.
   - Release 99+ : R99나 그 이후 버전을 따르는 HLR/AuC로서 UMTS 서비스를 지원하며, 인증벡터 Quintet을 생성한다. 핸드오버를 위해 c2와 c3 함수가 제공되어야 한다.
4) VLR/SGSN
   - Release 98- : R97이나 R98 버전을 따르는 VLR/SGSN으로서 BSS만을 구성하고 있다. 기본적으로 GSM과 GPRS 서비스를 지원하며, Triplets을 저장하고 필요한 Triplet 요소를 전송한다. 즉 GSM AKA를 지원하고, 변환 함수를 지원하지 않는다.
   - Release 99+ : R99나 그 이후 버전을 따르는 VLR/SGSN으로서 UTRAN과 BSS 모두 구성하고 있다. 기본적으로 UMTS 서비스를 지원하며, Quintets을 저장하고 필요한 Quintet 요소를 전송한다. c2, c3, c4 함수가 제공되어야 한다.
5) UTRAN: UMTS 무선 접속 네트워크로서 UMTS AKA를 지원한다.
6) BSS : GSM 무선 접속 네트워크로서 GSM AKA를 지원한다.
7) ME
   - Release 98- : R97이나 R98 버전을 따르는 ME로서 GSM AKA를 지원한다.
   - Release 99+ : R99나 그 이후 버전을 따르는 ME로서 UMTS AKA를 지원하며 GSM AKA도 지원한다. UTRAN에서만 가능한 3G single mode ME와 GSM BSS와 UTRAN 모두 가능한 2G/3G dual mode ME로 구분된다.

8) SIM : GSM 서비스 가입자 식별 모듈로서 GSM AKA를 지원한다.
9) USIM : UMTS 서비스 가입자 식별 모듈로서 UMTS AKA를 지원한다. 또한 GSM AKA 과정을 실행하기 위해서는 변환 함수 c2, c3가 제공되어야 하고, SIM-ME 인터페이스가 지원 가능할 수도 있다.
10) USIM에서 2G backward compatibility를 지원하기 위한 기능은 다음과 같다.
- Service n° 27 : "GSM Access", 이 서비스는 GSM BSS가 참여할 때 필수적인 서비스이다. USIM은 GSM 암호화 키 Kc를 생성한다. Security 관점에서 이 서비스는 "3G+Kc mode"로서 특성화된다.
- Service n° 38 : "GSM Security Context", 이 서비스는 R98- VLR/SGSN이나 R98- HLR/AuC가 참여할 때 요구된다. 이때 USIM은 GSM AKA를 실행한다. Security 관점에서 이 서비스는 "virtual 2G mode"로서 특성화된다.
- USIM에서 service n° 27과 service n° 38이 지원되지 않으면, SIM 기능이 가능하더라도 network access는 2G/3G 환경에서 불가능하다.
- Service n° 27과 service n° 38은 선택적이다. 따라서 네트워크 제공자가 이 서비스를 제공하지 않으면 security level이 더 낮아질 것이다.

11) Security 관점에서, compatibility service가 가능하게 하는 다음의 운영 모드가 있다.
- Normal 3G mode : 3G 알고리즘의 결과는 어떤 변화도 주지 않고 ME에게 전송된다. 즉, USIM이 RAND, AUTN을 받으면 ME에게 RES, CK, IK를 전송한다.
- 3G+Kc mode : USIM은 RAND, AUTN를 받으면, CK, IK로부터 Kc를 생성하여 ME에게 RES, CK, IK, Kc를 전송한다. 따라서, 변환 함수 c3이 요구된다. Service n° 27이 USIM에서 유용하면, 이 모드는 항상 active하다.
- Virtual 2G mode : USIM은 RAND를 받으면, RES로부터 SRES를 계산하고 CK, IK로 Kc를 계산해서 ME에게 전송한다. 따라서 변환함수 c2, c3이 요구된다.

12) 변환 함수

$c1 : RAND_{[GSM]} = RAND$

$c2 : SRES_{[GSM]} = XRES*_1 \oplus XRES*_2 \oplus XRES*_3 \oplus XRES*_4$

$XRES* : 16octets$

$XRES* = XRES (XRES가\ 16octets인\ 경우)$

$XRES* = XRES \parallel 0 \cdots 0$ ($XRES$가 $16octets$보다 작은 경우)

$XRES*_i : 4octets$

$XRES* = XRES*_1 \| XRES*_2 \| XRES*_3 \| XRES*_4$

$c3 : Kc_{[GSM]} = CK_1 \oplus CK_2 \oplus IK_1 \oplus IK_2$

$CK_i, IK_i : 64bits$

$CK = CK_1 \parallel CK_2$

$IK = IK_1 \parallel IK_2$

$c4 : CK_{[UMTS]} = Kc \parallel Kc$

$c5 : IK_{[UMTS]} = Kc_1 \oplus Kc_2 \parallel Kc \parallel Kc_1 \oplus Kc_2$

$Kc_i : 32bits,\ Kc = Kc_1 \parallel Kc_2$

4.2 UICC 사용자에 대한 AKA

이 절에서는 UICC 사용자가 2G 또는 3G를 지원하는 각 노드에서 서비스를 받기 위해 이루어져야 하는 AKA과정을 가능한 시나리오 별로 나누어 분석한다. 여러 가지 시나리오에서의 과정을 설명하기 전에 각각의 시나리오에서 필요한 기능들을 먼저 [표 1]에서 보여주고 있다. 여기서 UICC 사용자는 3G 가입자로서, 기본적으로 USIM application에 따른 서비스가 이루어지며 UMTS AKA 과정을 실행하게 된다. 만약 UICC가 R98- ME에서 기능을 수행하기 위해서는 SIM application 기능을 포함하고 있어야만 한다.

여기서 AKA 과정은 모든 상황이 성공적으로 이루어졌을 때의 과정에 대해서 설명하고 있으며, 모든 과정은 VLR/SGSN이 AuC에게 Authentication Data Request를 보냄으로써 시작된다.

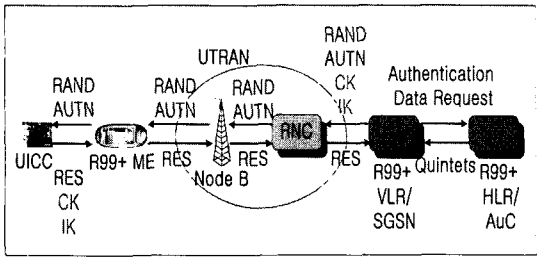
4.2.1 시나리오 1(UMTS AKA 과정 실행)

1) 구성 요소
- R99+ HLR/AuC : Quintet을 생성
- R99+ VLR/SGSN
- UTRAN(RNC, Node B)
- R99+ ME : USIM-ME 인터페이스를 지원
- UICC : USIM

2) 설명 : 3G 가입자가 R99+ VLR/SGSN 내 UTRAN에 접근했을 때 이루어지는 UMTS AKA 과정을 설명하고 있다. UMTS security context가 설립된다. 네트워크에 의한 사용자 인증을 위해 RES가 필요하고, 사용자에 의한 네트워크 인증을 위해 AUTN

〔표 1〕 UICC 사용자에 대한 다양한 서비스 시나리오

시나리오	ICC	ME	BSS	VLR/SGSN	HLR/AuC	AKA	특징	그림
1	3G	3G	3G	3G	3G	UMTS	- 전형적인 UMTS AKA 과정	4
2	3G	3G	2G	3G	3G		- VLR/SGSN : c3 함수 제공 - ME : 2G/3G dual mode - ICC : service n° 27 제공	5
3	3G	3G	2G	2G	3G	GSM	- HLR/AuC : c2, c3 함수 제공 - ME : 2G/3G dual mode - ICC : service n° 27, 38 제공	6
4	3G	3G	2G	3G	2G		- ME : 2G/3G dual mode - ICC : service n° 27, 38 제공	7
5	3G	3G	2G	2G	2G		- 시나리오 4와 거의 동일	8
6	3G	2G	2G	3G	3G		- VLR/SGSN : c2, c3 함수 제공 - ICC : SIM application 제공	9
7	3G	2G	2G	2G	3G		- HLR/AuC : c2, c3 함수 제공 - ICC : SIM application 제공	10
8	3G	2G	2G	3G	2G		- ICC : SIM application 제공	11
9	3G	2G	2G	2G	2G		- 시나리오 8과 거의 동일	12
10	3G	3G	3G	2G	3G	·	- 서비스가 이루어지지 않는다.	·
11	3G	3G	3G	3G	2G	·	- 서비스가 이루어지지 않는다.	·
12	3G	3G	3G	2G	2G	·	- 서비스가 이루어지지 않는다.	·
13	3G	2G	3G	3G	3G	·	- 서비스가 이루어지지 않는다.	·
14	3G	2G	3G	2G	3G	·	- 서비스가 이루어지지 않는다.	·
15	3G	2G	3G	3G	2G	·	- 서비스가 이루어지지 않는다.	·
16	3G	2G	3G	2G	2G	·	- 서비스가 이루어지지 않는다.	·



〔그림 4〕 시나리오 1(3G 가입자, UMTS AKA과정 실행)

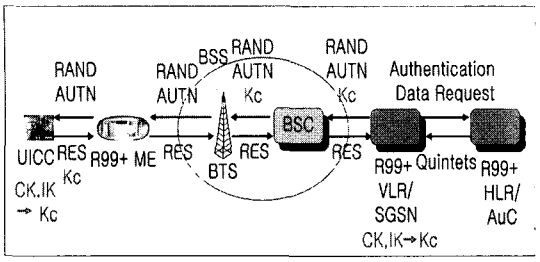
의 XMAC이 필요하며, 암복호화와 무결성 보호를 위해 CK, IK가 필요하다. 만약 service n° 27이 USIM에서 active하면, 변환 함수 c3에 의해 Kc를 생성해서 ME에게 CK, IK와 함께 전송되지만 이 시나리오에서는 필요로 하지 않으므로 ME는 받은 Kc를 버린다.

3) 과정 : AuC는 인증 벡터 Quintets을 생성해서 그것을 VLR/SGSN에게 전송한다. 그리고 나서 VLR/SGSN은 받은 Quintets을 저장하고 그 중 한 묶음에서 RAND, AUTN을 RNC, Node B, ME를 거쳐 UICC에게 전송한다. UICC에서 USIM applicaton에 의해, 받은 RAND와 저장하고 있는 K를 통해 XMAC, RES, CK, IK를 생성한다. 그리고 USIM은 네트워크를 인증하기 위해 VLR/SGSN으로부터 받은 AUTN에서 MAC과 XMAC을 비교해서 확인하고 같으면 VLR/SGSN에게 RES를 전송한다. VLR/SGSN은 사용자를 인증하기 위해 UICC로부터 받은 RES와 Quintet에 있는 XRES와 비교한다. 그리고 암복호화와 무결성 보호를 하기 위해 사용자 쪽에서는 UICC가 ME에게 CK, IK를 전송하고 네트워크 쪽에서는 VLR/SGSN이 RNC에게 CK, IK를 전송한다. 이 과정은 [그림 4]에 나타나있다.

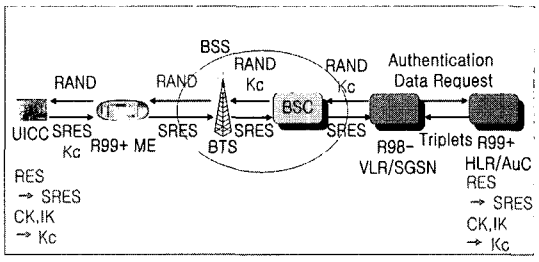
4.2.2 시나리오 2(UMTS AKA 과정 실행)

1) 구성 요소

- R99+ HLR/AuC : Quintet을 생성
- R99+ VLR/SGSN : c3 함수가 제공
- BSS(BSC, BTS)
- R99+ ME : 2G/3G dual mode ME,



〔그림 5〕 시나리오 2(3G 가입자, UMTS AKA과정 실행)



〔그림 6〕 시나리오 3(3G 가입자, GSM AKA과정 실행)

USIM-ME 인터페이스를 지원

- UICC : USIM application. Kc 생성을 위해 service n° 27이 제공

2) 설명 : 3G 가입자가 R99 + VLR/SGSN 내 GSM BSS에 접근했을 때 이루어지는 UMTS AKA 과정을 설명하고 있다. UMTS security context가 설립된다. ME와 BTS가 암복호화를 하기 위해 VLR/SGSN과 USIM에서 Kc의 변환이 필요하다. 3G single mode ME에서는 서비스가 제공되지 않는다. Service n° 27이 유용하면, c3 함수를 통해 Kc를 생성한다. USIM이 service n° 27을 지원하지 않으면 네트워크 접속은 이루어지지 않는다.

3) 과정 : Quintets, RAND, AUTN의 전송과 사용자와 네트워크간의 양방향 인증은 시나리오 1과 동일하다. 그리고 암복호화를 하기 위해 사용자 쪽에서는 USIM이 c3 함수를 이용해서 Kc를 계산한 다음 ME에게 전송한다. 만약 USIM이 c3 함수를 지원하지 않으면, R99+ ME에게 알려준다. 네트워크 쪽에서는 VLR/SGSN이 c3 함수를 이용해서 Kc를 계산하고 나서 사용자가 VLR으로부터 서비스를 받을 때는 BTS가 암복호화를 하므로 Kc를 BTS에게 전송하고 SGSN으로부터 서비스를 받을 때는 Kc를 SGSN 자체적으로 사용한다. 이 과정은 [그림 5]에 나타나있다.

4.2.3 시나리오 3(GSM AKA 과정 실행)

1) 구성 요소

- R99+ HLR/AuC : Triplet을 생성. c2, c3 함수가 제공
- R98- VLR/SGSN
- BSS(BSC, BTS)
- R99+ ME : 2G/3G dual mode ME
- UICC : USIM application. SRES, Kc 생성을 위해 service n° 27과 service n° 38이 제공

2) 설명 : 3G 가입자가 R98- VLR/SGSN 내 GSM BSS에 접근했을 때 이루어지는 GSM AKA 과정을 설명하고 있다. 네트워크에서 사용자를 인증하기 위해 USIM에서 SRES의 변환이 필요하고, ME와 BTS가 암복호화를 하기 위해 USIM에서 Kc의 변환이 필요하다. Service n° 38이 제공되기 위해 USIM에서는 virtual 2G mode가 지원되어야 하고, GSM BSS에 접속이 되므로 service n° 27이 필요하다. 3G single mode ME에서는 서비스가 제공되지 않으므로 ME는 2G/3G dual mode이어야 하고, service n° 27과 service n° 38을 지원하지 않는 USIM에 대해서는 네트워크 접속이 이루어지지 않는다.

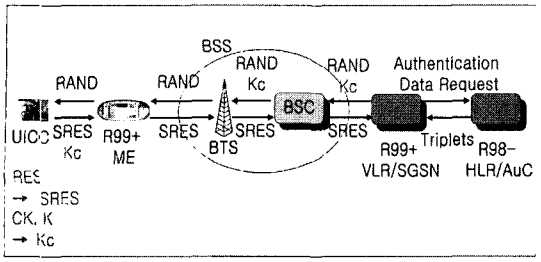
3) 과정 : AuC는 인증 벡터 Quintes을 생성하여 c2, c3 함수를 통해 Triplets을 생성해서 그것을 VLR/SGSN에게 전송한다. 그리고 나서 VLR/SGSN은 받은 Triplets을 저장하고 그 중 한 묶음에서 RAND를 UICC에게 전송한다. USIM은 받은 RAND와 저장하고 있는 K를 통해 RES, CK, IK를 생성한다. 그리고 나서 USIM은 c2 함수를 이용해서 SRES를 계산해서 VLR/SGSN에게 전송하고, c3 함수를 사용해서 Kc를 계산하여 ME에게 전송한다. 또한 네트워크 쪽에서는 사용자가 VLR으로부터 서비스를 받을 때는 BTS가 암복호화를 하므로 Kc를 BTS에게 전송하고 SGSN으로부터 서비스를 받을 때는 Kc를 SGSN 자체적으로 사용한다. 이 과정은 [그림 6]에 나타나있다.

4.2.4 시나리오 4(GSM AKA 과정 실행)

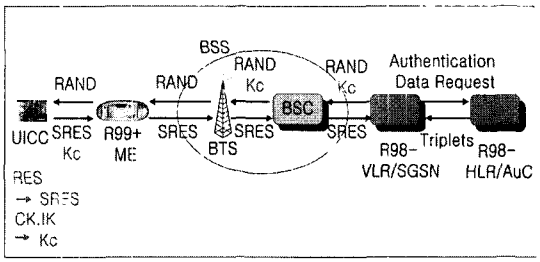
1) 구성 요소

- R98- HLR/AuC : Triplet을 생성
- R99+ VLR/SGSN
- BSS(BSC, BTS)
- R99+ ME : 2G/3G dual mode ME
- UICC : USIM application. SRES, Kc 생성을 위해 service n° 27과 service n° 38이 제공

2) 설명 : 3G 가입자가 R99+ VLR/SGSN 내 GSM BSS



[그림 7] 시나리오 4(3G 가입자, GSM AKA과정 실행)



[그림 8] 시나리오 5(3G 가입자, GSM AKA과정 실행)

에 접근했을 때 이루어지는 GSM AKA 과정을 설명하고 있다. ME와 USIM에서의 기능은 시나리오 3과 동일하다.

3) 과정 : AuC는 인증 벡터 Triplets을 생성해서 그것을 VLR/SGSN에게 전송한다. 이 이후의 과정은 VLR/SGSN이 R98-에서 R99+로 바뀐 것 외에는 시나리오 3과 동일하게 진행된다. 이 과정은 [그림 7]에 나타나있다.

4.2.5 시나리오 5(GSM AKA 과정 실행)

1) 구성 요소
- R98- HLR/AuC : Triplet을 생성
- R98- VLR/SGSN
- BSS(BSC, BTS)
- R99+ ME : 2G/3G dual mode ME
- UICC : USIM application. SRES, Kc 생성을 위해 service n° 27과 service n° 38이 제공

2) 설명 : 3G 가입자가 R98- VLR/SGSN 내 GSM BSS에 접근했을 때 이루어지는 GSM AKA 과정을 설명하고 있다. VLR/SGSN이 R99+에서 R98-로 바뀐 것 외에는 시나리오 4와 동일하다.

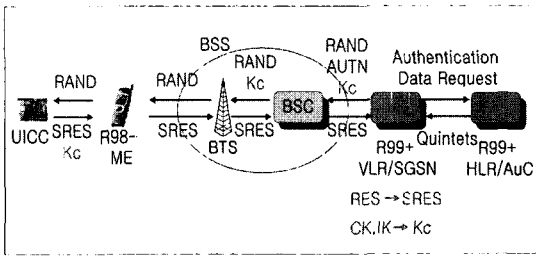
3) 과정 : 여기서의 과정은 VLR/SGSN이 R99+에서 R98-로 바뀐 것 외에는 시나리오 4와 동일하다. 이 과정은 [그림 8]에 나타나있다.

4.2.6 시나리오 6(GSM AKA 과정 실행)

1) 구성 요소
- R99+ HLR/AuC : Quintet을 생성
- R99+ VLR/SGSN : c2, c3 함수가 제공
- BSS(BSC, BTS)
- R98- ME : SIM-ME 인터페이스를 지원
- UICC : USIM application. R98- ME에서 서비스를 받기 위해 SIM application이 지원

2) 설명 : 3G 가입자가 R99+ VLR/SGSN 내 GSM BSS에 접근했을 때 이루어지는 GSM AKA 과정을 설명하고 있다. 네트워크에서 사용자를 인증하기 위해 VLR/SGSN에서 SRES의 변환이 필요하고, ME와 BTS가 암복호화를 하기 위해 VLR/SGSN에서 Kc의 변환이 필요하다. 이 시나리오에서는 UICC 내 SIM application이 작용하게 된다. UICC가 SIM application을 포함하고 있지 않으면 서비스는 이루어지지 않는다.

3) 과정 : AuC는 인증 벡터 Quintets을 생성해서 그것을 VLR/SGSN에게 전송한다. 그리고 VLR/SGSN은 수신한 Quintets을 저장하고 그 중 한 묶음에서 RAND, AUTN을 ME에게 전송한다. ME는 AUTN을 무시하고 RAND를 UICC에게 전송한다. UICC 내 SIM application은 받은 RAND와 저장하고 있는 K_i를 통해 SRES, Kc를 생성한다. 그리고 SRES를 VLR/SGSN에게 전송한다. 만약 이때 R99+ VLR/SGSN은 SRES를 Iu-interface(RNC와 VLR/SGSN 사이의 interface) 상에서 받으면 거절하고, A(BSC와 VLR 사이의 interface) 또는 Gb-interface (BSC와 SGSN 사이의 interface) 상에서 받으면 인증을 수용한다. VLR/SGSN은 사용자를 인증하기 위해 UICC로부터 받은 SRES와 Quintet에 있는 XRES를 c2 함수를 이용해서 계산한 SRES와 비교한다. 그리고 암복호화를 하기 위해 UICC는 Kc를 ME에게 전송하고 네트워크 쪽에서는 VLR/SGSN이 c3 함수를 이용해서 Kc를 계산하고 나서 사용자가 VLR으로부터 서비스를 받을 때는 Kc를 BTS에게

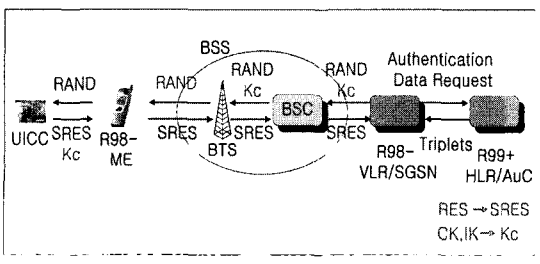


[그림 9] 시나리오 6(3G 가입자, GSM AKA과정 실행)

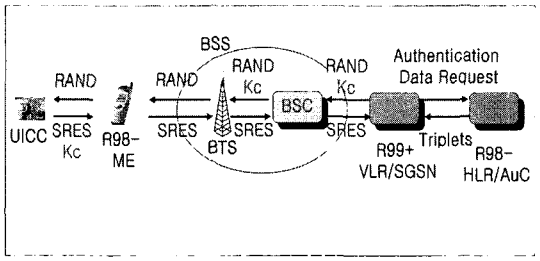
전송하고 SGSN으로부터 서비스를 받을 때는 Kc를 SGSN 자체적으로 사용한다. 이 과정은 [그림 9]에 나타나있다.

4.2.7 시나리오 7(GSM AKA 과정 실행)

1) 구성 요소
   - R99+ HLR/AuC : Triplet을 생성. c2, c3 함수가 제공
   - R98- VLR/SGSN
   - BSS(BSC, BTS)
   - R98- ME : SIM-ME 인터페이스를 지원
   - UICC : USIM application. R98- ME에서 서비스를 받기 위해 SIM application이 지원
2) 설명 : 3G 가입자가 R98- VLR/SGSN 내 GSM BSS에 접근했을 때 이루어지는 GSM AKA 과정을 설명하고 있다. 이 시나리오에서는 시나리오 6과 마찬가지로, UICC 내 SIM application이 작용하게 되고 UICC가 SIM application을 포함하고 있지 않으면 서비스는 이루어지지 않는다.
3) 과정 : AuC는 인증 벡터 Quintets을 생성한 다음, c2, c3 함수를 이용해서 Kc, SRES를 계산하여 Triplets을 생성한다. 이 Triplets을 VLR/SGSN에게 전송한다. 그리고 VLR/SGSN은 받은 Triplets을 저장하고 그 중 한 묶음에서 RAND를 UICC에게 전송한다. UICC 내 SIM application은 받은 RAND와 저장하고 있는 K_i를 통해 SRES, Kc를 생성한다. 그리고 SRES를 VLR/SGSN에게 전송한다. VLR/SGSN은 사용자를 인증하기 위해 UICC로부터 받은 SRES와 Triplet에 있는 SRES를 비교한다. 그리고 암복호화를 하기 위해 UICC는 Kc를 ME에게 전송하고 네트워크 쪽에서는 VLR/SGSN이 사용자가 VLR으로부터 서비스를 받을 때는 Kc를 BTS에게 전송하고 SGSN으로부터 서비스를 받을 때는 Kc를 SGSN 자체적으로 사용한다. 이 과정은 [그림 10]에 나타나있다.



〔그림 10〕 시나리오 7(3G 가입자, GSM AKA과정 실행)



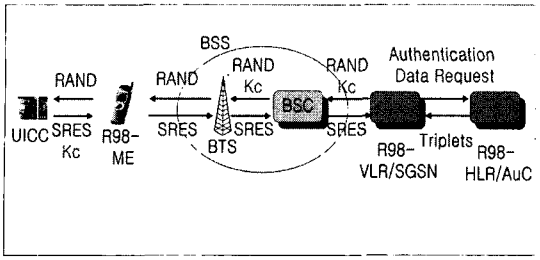
〔그림 11〕 시나리오 8(3G 가입자, GSM AKA과정실행)

4.2.8 시나리오 8(GSM AKA 과정 실행)

1) 구성 요소
   - R98- HLR/AuC
   - R99+ VLR/SGSN
   - BSS(BSC, BTS)
   - R98- ME : SIM-ME 인터페이스를 지원
   - UICC : USIM application. R98- ME에서 서비스를 받기 위해 SIM application이 지원
2) 설명 : 3G 가입자가 R99+ VLR/SGSN 내 GSM BSS에 접근했을 때 이루어지는 GSM AKA 과정을 설명하고 있다. 이 시나리오에서는 시나리오 6, 7과 마찬가지로, UICC 내 SIM application이 작용하게 되고 UICC가 SIM application을 포함하고 있지 않으면 서비스는 이루어지지 않는다.
3) 과정 : AuC는 인증 벡터 Triplets을 생성해서 그것을 VLR/SGSN에게 전송한다. 이 이후의 과정은 시나리오 7과 동일하게 진행된다. 이 과정은 [그림 11]에 나타나있다.

4.2.9 시나리오 9(GSM AKA 과정 실행)

1) 구성 요소
   - R98- HLR/AuC
   - R98- VLR/SGSN
   - BSS(BSC, BTS)
   - R98- ME
   - UICC : USIM application. R98- ME에서 서비스를 받기 위해 SIM application이 지원
2) 설명 : 3G 가입자가 R98-VLR/SGSN 내 GSM BSS에 접근했을 때 이루어지는 GSM AKA 과정을 설명하고 있다. 이 시나리오에서는 시나리오 6, 7, 8과 마찬가지로, UICC 내 SIM application이 작용하게 되고 UICC가 SIM application을 포함하고 있지 않으면 서비스는 이루어지지 않는다.
3) 과정 : R99+ VLR/SGSN이 참여한 것에서 R98-VLR/SGSN이 참여하는 것 외에는 시나리오 8의 과정



[그림 12] 시나리오 9(3G 가입자, GSM AKA과정실행)

과 동일하다. 이 과정은 [그림 12]에 나타나있다.

4.2.10 시나리오 10

1) 구성 요소
   - R99+ HLR/AuC
   - R98- VLR/SGSN
   - UTRAN(RNC, Node B)
   - R99+ ME
   - UICC : USIM application
2) 설명 : R98- VLR/SGSN 내에 UTRAN의 참여가 불가능하므로 이 시나리오에서는 서비스가 이루어지지 않는다.

4.2.11 시나리오 11

1) 구성 요소
   - R98- HLR/AuC
   - R99+ VLR/SGSN
   - UTRAN(RNC, Node B)
   - R99+ ME
   - UICC : USIM application
2) 설명 : 이 시나리오는 GSM AKA 과정을 실행하지만, 비록 3G 데이터의 변환이 가능하더라도 정당하지 않은 구성이다. 이는, 네트워크 제공자(HLR/AuC)가 3G 가입자에게 3G 접속 네트워크(UTRAN)에 접속할 때 UMTS AKA 과정이 실행되도록 설정이 되기 때문에 GSM AKA 과정이 이루어지지 않게 되어 결국은 인증이 실패하게 된다. 따라서 이 시나리오에서는 서비스가 제공되지 않는다.

4.2.12 시나리오 12

1) 구성 요소
   - R98- HLR/AuC
   - R98- VLR/SGSN
   - UTRAN(RNC, Node B)
   - R99+ ME
   - UICC : USIM application
2) 설명 : R98- VLR/SGSN 내에 UTRAN의 참여가 불가능하므로 시나리오 10과 마찬가지로 서비스가 이루어지지 않는다.

4.2.13 시나리오 13

1) 구성 요소
   - R99+ HLR/AuC
   - R99+ VLR/SGSN
   - UTRAN(RNC, Node B)
   - R98- ME
   - UICC : USIM application, SIM application
2) 설명 : R98- ME는 UTRAN에서 서비스가 가능하지 않으므로 이 시나리오에서는 서비스가 이루어지지 않는다.

4.2.14 시나리오 14

1) 구성 요소
   - R99+ HLR/AuC
   - R98- VLR/SGSN
   - UTRAN(RNC, Node B)
   - R98- ME
   - UICC : USIM application, SIM application
2) 설명 : R98- VLR/SGSN 내에 UTRAN의 참여가 불가능하고 R98- ME는 UTRAN에서 서비스가 가능하지 않으므로 서비스가 이루어지지 않는다.

4.2.15 시나리오 15

1) 구성 요소
   - R98- HLR/AuC
   - R99+ VLR/SGSN
   - UTRAN(RNC, Node B)
   - R98- ME
   - UICC : USIM application, SIM application
2) 설명 : 시나리오 13과 같이 R98- ME는 UTRAN에서 서비스가 가능하지 않으므로 서비스가 이루어지지 않는다.

4.2.16 시나리오 16

1) 구성 요소
   - R98- HLR/AuC
   - R98- VLR/SGSN
   - UTRAN(RNC, Node B)
   - R98- ME

〔표 2〕 ICC 사용자에 대한 다양한 서비스 시나리오

시나리오	ICC	ME	BSS	VLR/SGSN	HLR/AuC	AKA	특징	그림
1	2G	3G	3G	3G	2G 또는 3G	GSM	- VLR/SGSN, ME : c4 함수 제공	13
2	2G	3G	2G	3G			- ME : 2G/3G dual mode	14
3	2G	3G	2G	2G			- ME : 2G/3G dual mode	15
4	2G	2G	2G	3G			- 시나리오 3과 거의 동일	16
5	2G	2G	2G	2G			- 전형적인 GSM AKA 과정	17
6	2G	3G	3G	2G		·	- 서비스가 이루어지지 않는다.	·
7	2G	2G	3G	3G		·	- 서비스가 이루어지지 않는다.	·
8	2G	2G	3G	2G		·	- 서비스가 이루어지지 않는다.	·

- UICC : USIM application, SIM application

2) 설명 : 시나리오 14와 같이 R98- VLR/SGSN 내에 UTRAN의 참여가 불가능하고 R98- ME는 UTRAN에서 서비스가 가능하지 않으므로 서비스가 이루어지지 않는다.

4.3 ICC 사용자에 대한 AKA

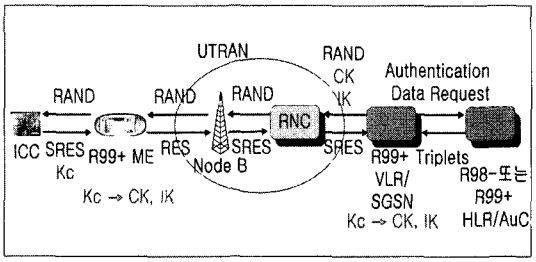
이 절에서는 ICC 사용자가 2G 또는 3G를 지원하는 각 노드에서 서비스를 받기 위해 이루어져야하는 AKA 과정을 가능한 시나리오 별로 나누어 분석한다. 여러 가지 시나리오에서의 과정을 설명하기 전에 각각의 시나리오에서 필요한 기능들을 먼저 [표 2]에서 보여주고 있다. 2G 가입자에 대해서는 3G 가입자보다 제한적이기 때문에 3G에서보다 가능한 시나리오가 더 적게 나타난다. 여기서 ICC 사용자는 2G 가입자로서, 기본적으로 SIM application에 따른 서비스가 이루어지며 GSM AKA 과정을 실행하게 된다.

여기서 AKA 과정은 모든 상황이 성공적으로 이루어졌을 때의 과정에 대해서 설명하고 있으며, 모든 과정은 VLR/SGSN이 HLR/AuC에게 Authentication Data Request를 보냄으로써 시작된다. ICC 사용자에 대해서는 항상 GSM AKA 과정이 실행된다.

4.3.1 시나리오 1(GSM AKA 과정 실행)

1) 구성 요소
- R98- 또는 R99+ HLR/AuC : Triplet을 생성
- R99+ VLR/SGSN : c4 함수가 제공
- UTRAN(RNC, Node B)
- R99+ ME : c4 함수가 제공
- ICC : SIM

2) 설명 : 2G 가입자가 R99+ VLR/SGSN 내 UTRAN에 접근했을 때 이루어지는 GSM AKA 과정을 설명하고 있다. ME와 RNC가 암복호화와 무결성 보호를 하기 위해 CK, IK로의 변환이 필요하다. ME와 RNC가 CK, IK를 사용하더라도 security는 Kc에 기반 한다. 즉, GSM security context가 설립된다.

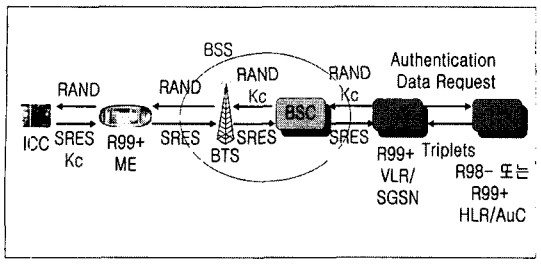


〔그림 13〕 시나리오 1(2G 가입자, GSM AKA과정실행)

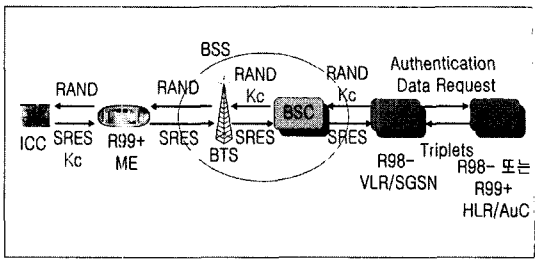
3) 과정 : AuC는 인증 벡터 Triplets을 생성해서 그것을 VLR/SGSN에게 전송한다. 그리고 VLR/SGSN은 받은 Triplets을 저장하고 그 중 한 묶음에서 RAND를 ICC에게 전송한다. ICC 내 SIM은 받은 RAND와 저장하고 있는 K_i를 통해 SRES, Kc를 생성한다. 그리고 SIM은 SRES를 VLR/SGSN에게 전송한다. VLR/SGSN은 사용자를 인증하기 위해 SIM으로부터 받은 SRES와 Triplet에 있는 SRES를 비교한다. 그리고 암복호화를 하기 위해 사용자 쪽에서는 SIM이 계산한 Kc를 ME에게 전송하여 ME는 c4 함수를 이용해서 CK, IK를 계산하고, 네트워크 쪽에서는 VLR/SGSN이 c4 함수를 이용해서 CK, IK를 계산하고 나서 RNC에게 전송한다. 이 과정은 [그림 13]에 나타나있다.

4.3.2 시나리오 2(GSM AKA 과정 실행)

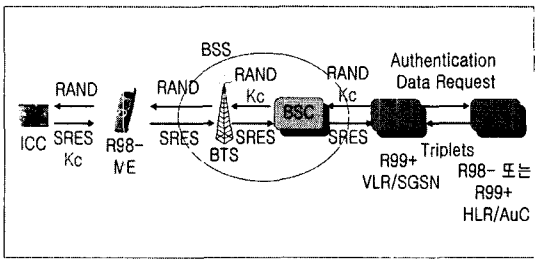
1) 구성 요소
- R98- 또는 R99+ HLR/AuC : Triplet을 생성
- R99+ VLR/SGSN
- BSS(BSC, BTS)



〔그림 14〕 시나리오 2(2G 가입자, GSM AKA과정 실행)



〔그림 15〕 시나리오 3(2G 가입자, GSM AKA과정 실행)



〔그림 16〕 시나리오 4(2G 가입자, GSM AKA과정 실행)

- R99+ ME : 2G/3G dual mode ME가 요구됨
- ICC : SIM

2) 설명 : 2G 가입자가 R99+ VLR/SGSN 내 GSM BSS에 접근했을 때 이루어지는 GSM AKA 과정을 설명하고 있다. GSM BSS에서 GSM AKA 과정을 하기 위해 2G/3G dual mode ME가 요구되며, 3G single mode ME인 경우에서는 서비스가 이루어지지 않는다.

3) 과정 : AuC는 인증 벡터 Triplets을 생성해서 그것을 VLR/SGSN에게 전송한다. 그리고 나서 VLR/SGSN은 받은 Triplets을 저장하고 그 중 한 묶음에서 RAND를 ICC에게 전송한다. ICC 내 SIM은 받은 RAND와 저장하고 있는 K_i를 통해 SRES, Kc를 생성한다. 그리고 SIM은 SRES를 VLR/SGSN에게 전송한다. VLR/SGSN은 사용자를 인증하기 위해 SIM으로부터 받은 SRES와 Triplet에 있는 SRES를 비교한다. 그리고 암복호화를 하기 위해 사용자 쪽에서는 SIM이 계산한 Kc를 ME에게 전송하고, 네트워크 쪽에서는 사용자가 VLR로부터 서비스를 받을 때는 Kc를 BTS에게 전송하고 SGSN으로부터 서비스를 받을 때는 SGSN 자체적으로 사용한다. SGSN으로부터 서비스를 받는 경우는 Kc를 BTS에게 전송하지 않는다. 이 과정은 [그림 14]에 나타나있다.

4.3.3 시나리오 3(GSM AKA 과정 실행)

1) 구성 요소
- R98- 또는 R99+ HLR/AuC : Triplet을 생성
- R98- VLR/SGSN
- BSS(BSC, BTS)
- R99+ ME : 2G/3G dual mode ME가 요구됨
- ICC : SIM

2) 설명 : 2G 가입자가 R98- VLR/SGSN 내 GSM BSS에 접근했을 때 이루어지는 GSM AKA 과정을 설명하고 있다. 시나리오 2와 마찬가지로, GSM BSS에서 GSM AKA 과정을 하기 위해 2G/3G dual mode ME가 요구되며, 3G single mode ME인 경우에서는 서비스가 이루어지지 않는다.

3) 과정 : 이 시나리오의 과정은 VLR/SGSN이 R99+에서 R98-로 바뀐 것 외에는 시나리오 2와 동일한 과정을 수행하게 된다. 이 과정은 [그림 15]에 나타나있다.

4.3.4 시나리오 4(GSM AKA 과정 실행)

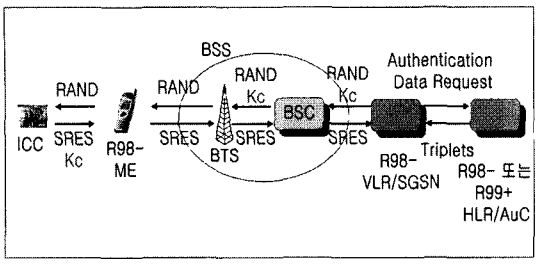
1) 구성 요소
- R98- 또는 R99+HLR/AuC : Triplet을 생성
- R99+ VLR/SGSN
- BSS(BSC, BTS)
- R98- ME
- ICC : SIM

2) 설명 : 2G 가입자가 R99+ VLR/SGSN 내 GSM BSS에 접근했을 때 이루어지는 GSM AKA 과정을 설명하고 있다. VLR/SGSN은 backward compatible하다.

3) 과정 : R98- VLR/SGSN이 R99+ VLR/SGSN으로 바뀐 것 외에는 시나리오 4와 과정이 동일하다. 이 과정은 [그림 16]에 나타나있다.

4.3.5 시나리오 5(GSM AKA 과정 실행)

1) 구성 요소
- R98- 또는 R99+ HLR/AuC : Triplet을 생성



〔그림 17〕 시나리오 5(2G 가입자, GSM AKA과정 실행)

- R98- VLR/SGSN
- BSS(BSC, BTS)
- R98- ME
- ICC : SIM

2) 설명 : 2G 가입자가 R98- VLR/SGSN 내 GSM BSS에 접근했을 때 이루어지는 GSM AKA 과정을 설명한다.
3) 과정 : 일반적인 GSM AKA 과정과 동일하다. 이 과정은 [그림 17]에 나타나 있다.

4.3.6 시나리오 6

1) 구성 요소
- R98- 또는 R99+ HLR/AuC : Triplet을 생성
- R98- VLR/SGSN
- UTRAN(RNC, Node B)
- R99+ ME : 2G/3G dual mode ME가 요구됨
- ICC : SIM

2) 설명 : R98- VLR/SGSN 내에 UTRAN의 참여가 불가능하므로 서비스가 이루어지지 않는다.

4.3.7 시나리오 7

1) 구성 요소
- R98- 또는 R99+ HLR/AuC
- R99+ VLR/SGSN
- UTRAN(RNC, Node B)
- R98- ME
- ICC : SIM

2) 설명 : R98- ME는 UTRAN에서 서비스가 가능하지 않으므로 서비스가 이루어지지 않는다.

4.3.8 시나리오 8

1) 구성 요소
- R98- 또는 R99+ HLR/AuC
- R98- VLR/SGSN
- UTRAN(RNC, Node B)
- R98- ME
- ICC : SIM

2) 설명 : R98- VLR/SGSN 내에 UTRAN의 참여가 불가능하고 R98- ME는 UTRAN에서 서비스가 가능하지 않으므로 서비스가 이루어지지 않는다.

V. UMTS와 GSM에서의 핸드오버

이 절에서는 UMTS와 GSM에서 핸드오버가 필요한 경우 RNC(또는 BTS)와 ME 사이의 암복호화나 무결성 보호를 위해 필요한 키 값의 전송을 CS-Domain 서비스와 PS-Domain 서비스를 나누어 분석한다. 이러한 UMTS와 GSM 사이의 핸드오버의 가능한 경우를 [표 3]에서 요약하고 있다.

5.1 CS-Domain 서비스에 대한 핸드오버

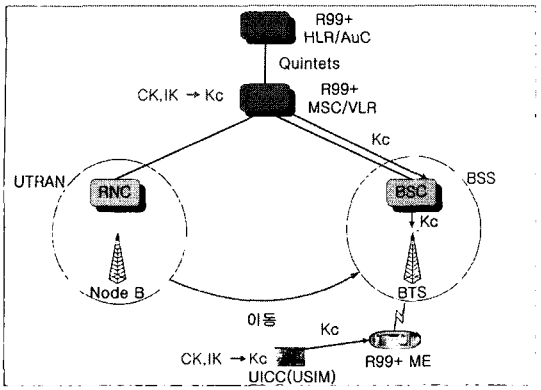
CS-Domain 서비스를 제공하는 경우에는 MSC/VLR이 참여를 하므로 MSC/VLR을 중심으로 설명을 한다.

5.1.1 UTRAN에서 GSM BSS로의 핸드오버

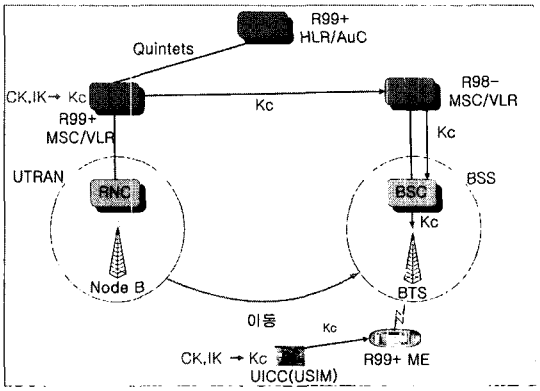
이 경우는 BSS에서 암복호화 만을 제공하므로 시그널 메시지에 대한 무결성 보호는 더 이상 이루어지지 않는다. 또한 이 핸드오버는 UEA(UMTS Enc-

〔표 3〕 UMTS와 GSM 사이의 가능한 핸드오버

	가입자	CS-Domain(MSC/VLR)		PS-Domain(SGSN)	
핸드오버		UTRAN → BSS	BSS → UTRAN	UTRAN → BSS	BSS → UTRAN
UMTS security context	2G/3G	1) 3G → 동일한 3G 2) 3G → 2G 3) 3G → 다른 3G	1) 3G → 동일한 3G 2) 3G → 2G 또는 3G	CS-Domain과 동일	CS-Domain과 동일
GSM security context	2G	1) 3G → 동일한 3G 2) 3G → 2G 또는 다른 3G	1) 3G → 동일한 3G 2) 2G 또는 3G → 3G	CS-Domain과 동일	CS-Domain과 동일
	3G	2G 가입자와 동일	2G 가입자와 동일	2G 가입자와 동일	2G → 3G



〔그림 18〕 동일한 R99+ MSC/VLR사이의 핸드오버(UMTS security context)



〔그림 19〕 R99+ MSC/VLR에서 R98- MSC/VLR로의 핸드오버(UMTS security context)

ryption Algorithm)에서 GSM A5로 암호 알고리즘이 변경되었다는 것을 암시하게 된다.

5.1.1.1 UMTS security context

UMTS AKA의 능력이 있는 R99+ ME를 사용하는 3G 가입자에 대해서만 이루어진다. 이때, R99+ HLR/AuC가 핸드오버에 참여하며 R99+ MSC/VLR에게 Quintet을 제공한다. 이러한 UMTS security context는 UMTS AKA 과정 실행 후 사용자와 네트워크간에 CK, IK 등의 정보를 저장하게 된다.

다음은 네트워크 관점에서 일어날 수 있는 세 가지 핸드오버의 경우에 대해서 설명하고 있으며, 동일하지 않은 MSC/VLR로의 핸드오버 시에는 처음의 MSC/VLR이 서비스 전체에 걸쳐 anchor point로서의 역할을 하게 된다.

1) 동일한 R99+ MSC/VLR 사이의 핸드오버

a) 설명 : 3G 가입자가 동일한 R99+ MSC/VLR이 제어하는 UTRAN에서 GSM BSS로 이동했을 경우로서, BTS와 ME가 암복호화를 할 수 있도록 키 값의 전송 과정을 보여주고 있다. R99+ MSC/VLR과 USIM은 Kc를 얻기 위해 c3 함수가 필요하다.

b) 과정 : R99+ MSC/VLR은 BTS가 암복호화를 할 수 있도록 자신이 저장하고 있는 Quintet의 CK, IK로부터 Kc를 계산하여 target BSC에게 Kc를 보내고, 다시 BTS에게 전송한다. 사용자 측면에서는 USIM이 저장하고 있는 CK, IK로 Kc를 계산해서 ME에게 전송한다. 이 과정은 [그림 18]에 나타나 있다.

2) R99+ MSC/VLR에서 R98- MSC/VLR로의 핸드오버

a) 설명 : 3G 가입자가 R99+ MSC/VLR이 제어하는 UTRAN에서 R98- MSC/VLR이 제어하는 GSM BSS로 이동했을 경우로서, BTS와 ME가 암복호화를 할 수 있도록 키 값의 전송 과정을 보여주고 있다. R99+ MSC/VLR과 USIM은 Kc를 얻기 위해 c3 함수가 필요하다.

b) 과정 : 처음의 R99+ MSC/VLR은 R98- MSC/VLR이 제어하는 BTS가 암복호화를 할 수 있도록 자신이 저장하고 있는 CK, IK로부터 Kc를 계산하여 새로운 R98- MSC/VLR에게 전송한다. 그 이후의 과정은 동일한 R99+ MSC/VLR 사이의 핸드오버와 동일하다. 이 과정은 [그림 19]에 나타나있다.

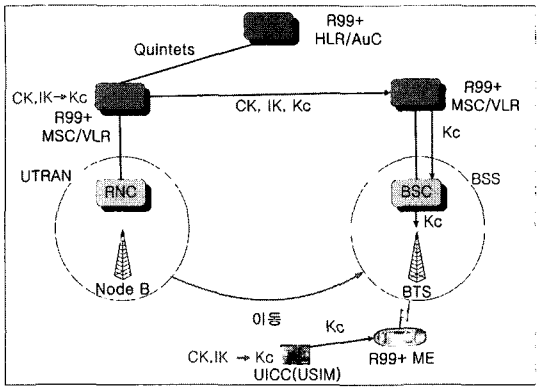
3) R99+ MSC/VLR에서 다른 R99+ MSC/VLR로의 핸드오버

a) 설명 : 3G 가입자가 R99+ MSC/VLR이 제어하는 UTRAN에서 다른 R99+ MSC/VLR이 제어하는 GSM BSS로 이동했을 경우로서, BTS와 ME가 암복호화를 할 수 있도록 키 값의 전송과정을 보여주고 있다. R99+ MSC/VLR과 USIM은 Kc를 얻기 위해 c3 함수가 필요하다.

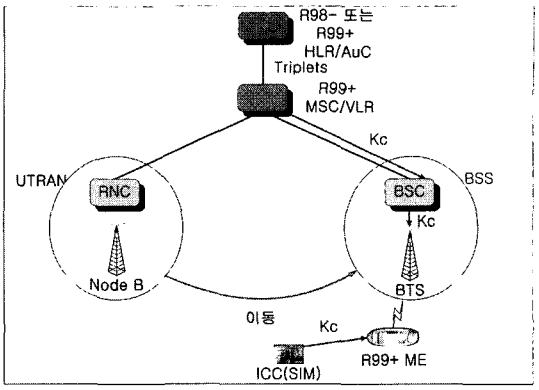
b) 과정 : 처음의 R99+ MSC/VLR은 다른 R99+ MSC/VLR이 제어하는 BTS가 암복호화를 할 수 있도록 자신이 저장하고 있는 CK, IK로부터 Kc를 계산하고 새로운 R99+ MSC/VLR에게 CK, IK, Kc를 전송한다. 이후의 과정과 사용자 측면에서의 과정은 동일한 R99+ MSC/VLR 사이의 핸드오버와 동일하다. 이 과정은 [그림 20]에 나타나있다.

5.1.1.2 GSM security context

R99+ ME를 사용하는 2G 가입자에 대해서만 이루어진다. R98- 또는 R99+ HLR/AuC가 핸드오버에 참여하며, R99+ MSC/VLR에게 Triplet을 제공한다. 이



〔그림 20〕 R99+ MSC/VLR에서 다른 R99+ MSC/VLR로의 핸드오버(UMTS security context)



〔그림 21〕 동일한 R99+ MSC/VLR에서의 핸드오버(GSM security context)

GSM security context는 GSM AKA 과정 실행 후 사용자와 네트워크간에 Kc 등의 정보를 저장하게 된다.

다음은 네트워크 관점에서 두 가지 핸드오버의 경우에 대해서 설명하고 있다.

1) 동일한 R99+ MSC/VLR 사이의 핸드오버

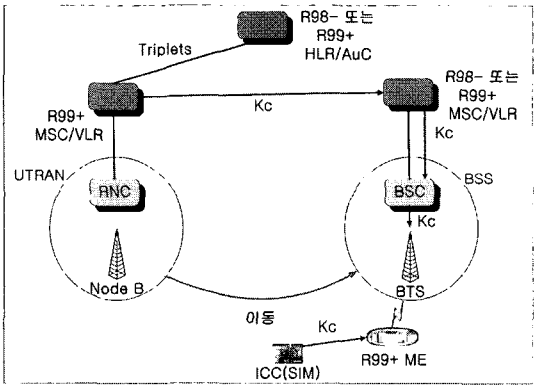
a) 설명 : 2G 가입자가 동일한 R99+ MSC/VLR이 제어하는 UTRAN에서 GSM BSS로 이동했을 경우로서, BTS와 ME가 암복호화를 할 수 있도록 키 값의 전송 과정을 보여주고 있다.

b) 과정 : R99+ MSC/VLR은 BTS가 암복호화를 할 수 있도록 자신이 저장하고 있는 Triplet의 Kc를 target BSC에게 보내고 다시 BTS에게 전송한다. 사용자 측면에서는 SIM이 저장하고 있는 Kc를 ME에게 전송한다. 이 과정은 [그림 21]에 나타나있다.

2) R99+ MSC/VLR에서 다른 R98- 또는 R99+ MSC/VLR로의 핸드오버

a) 설명 : 2G 가입자가 R99+ MSC/VLR이 제어하는 UTRAN에서 R98- 또는 R99+ MSC/VLR이 제어하는 GSM BSS로 이동했을 경우로서, BTS와 ME가 암복호화를 할 수 있도록 키 값의 전송 과정을 보여주고 있다. 처음의 R99+ MSC/VLR은 CK, IK를 생성하기 위해 c4, c5 함수가 필요하다.

b) 과정 : 처음의 R99+ MSC/VLR은 R98- 또는 R99+ MSC/VLR이 제어하는 BTS가 암복호화를 할 수 있도록 자신이 저장하고 있는 Triplet의 Kc를 새로운 R98- 또는 R99+ MSC/VLR을 경유해서 target BSC에게 Kc를 보내고 다시 BTS에게 전송한다. 처음의 MSC/VLR은 서비스 전체에 걸쳐 anchor point로서의 역할을 하게 된다. 사용자 측면에서는 SIM이 저장하고 있는 Kc를 ME에게 전송한다. 이

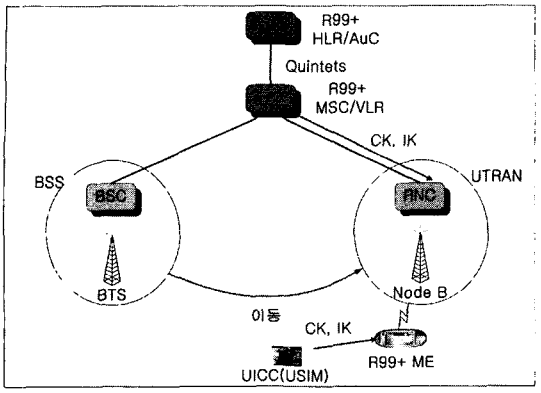


〔그림 22〕 R99+ MSC/VLR에서 다른 R98- 또는 R99+ MSC/VLR로의 핸드오버(GSM security context)

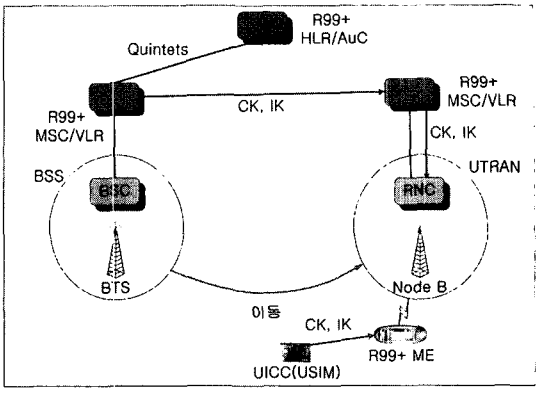
때, 만약 non-anchor MSC/VLR이 R99+이면 anchor MSC/VLR은 CK, IK를 생성하고 non-anchor MSC/VLR에게 전송한다. Non-anchor MSC/VLR은 이 키를 저장한다. 따라서 이 경우에 anchor MSC/VLR은 c4, c5 함수가 필요하다. 이 과정은 [그림 22]에 나타나있다.

5.1.2 GSM BSS에서 UTRAN으로의 핸드오버

이 경우는 BSS에서 암복호화만이 제공을 하므로 핸드오버가 완료된 후에 시그널 메시지에 대한 무결성에 대한 보호는 즉시 이루어져야 한다. 이 무결성 보호는 Serving RNC가 ME로부터 RRC message를 받을 때 RRC security mode control 과정의 시작과 함께 개시된다. 또한 이 핸드오버는 GSM A5에서 UEA (UMTS Encryption Algorithm)로 암호 알고리즘이 변경되었다는 것을 암시하게 된다.



〔그림 23〕 동일한 R99+ MSC/VLR에서의 핸드오버 (UMTS security context)



〔그림 24〕 R99+ MSC/VLR에서 다른 R99+ MSC/VLR로의 핸드오버(UMTS security context)

5.1.2.1 UMTS security context

R99+ MSC/VLR에 의해 제어되는 GSM BSS 하에서 UMTS AKA의 능력이 있는 R99+ ME를 사용하는 3G 가입자에 대해서만 이루어진다. 이때, R99+ HLR/AuC가 핸드오버에 참여하며 R99+ MSC/VLR에게 Quintets을 제공한다. 이 UMTS security context는 UMTS AKA 과정 실행 후 사용자와 네트워크간에 CK, IK 등의 정보를 저장하게 된다.

다음은 네트워크 관점에서 일어날 수 있는 두 가지 핸드오버의 경우에 대해서 설명하고 있다.

1) 동일한 R99+ MSC/VLR에서의 핸드오버

a) 설명 : 3G 가입자가 동일한 R99+ MSC/VLR이 제어하는 GSM BSS에서 UTRAN로 이동했을 경우로서, RNC와 ME가 암복호화와 무결성 보호를 할 수 있도록 키 값의 전송 과정을 보여주고 있다.

b) 과정 : R99+ MSC/VLR은 RNC가 암복호화와 무결성 보호를 할 수 있도록 자신이 저장하고 있는 Quintet의 CK, IK를 target RNC에게 전송한다. 사용자 측면에서는 USIM이 저장하고 있는 CK, IK를 ME에게 전송한다. 이 과정은 [그림 23]에 나타나있다.

2) R99+ MSC/VLR에서 다른 R99+ MSC/VLR로의 핸드오버

a) 설명 : 3G 가입자가 R99+ MSC/VLR이 제어하는 GSM BSS에서 다른 R99+ MSC/VLR이 제어하는 UTRAN로 이동했을 경우로서, RNC와 ME가 암복호화와 무결성 보호를 할 수 있도록 키 값의 전송 과정을 보여준다.

b) 과정 : 처음의 R99+ MSC/VLR은 다른 R99+ MSC/VLR이 제어하는 RNC가 암복호화와 무결성 보호를 할 수 있도록 자신이 저장하고 있는 Quintet의 CK, IK를 새로운 R99+ MSC/VLR에게 전송한다. 그 이후의 과정과 사용자 측면에서의 과정은 동일한 R99+ MSC/VLR에서의 핸드오버와 동일하다. 처음의 MSC/VLR은 서비스 전체에 걸쳐 anchor point로서의 역할을 하게 된다. 이 과정은 [그림 24]에 나타나있다.

5.1.2.2 GSM security context

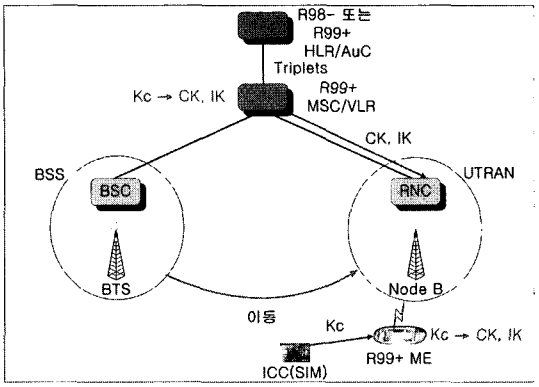
처음의 MSC/VLR이 R98- 일 때 R99+ ME를 사용하는 2G 가입자 또는 R99+ ME를 사용하는 3G 가입자에 대해서 가능하다. R98- 또는 R99+ HLR/ AuC가 핸드오버에 참여하며, R99+ MSC/VLR에게 Triplets을 제공한다. 이 GSM security context는 GSM AKA 과정 실행 후 사용자와 네트워크간에 Kc 등의 정보를 저장하게 된다.

다음은 네트워크 관점에서 두 가지 핸드오버의 경우에 대해서 설명하고 있다.

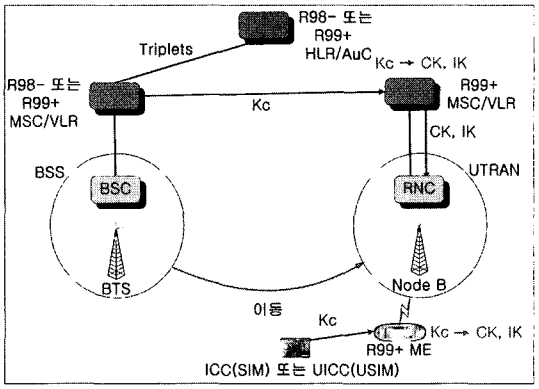
1) 동일한 R99+ MSC/VLR에서의 핸드오버

a) 설명 : 2G 가입자가 동일한 R99+ MSC/VLR이 제어하는 GSM BSS에서 UTRAN로 이동했을 경우로서, RNC와 ME가 암복호화와 무결성 보호를 할 수 있도록 키 값의 전송 과정을 보여주고 있다. R99+ MSC/VLR과 R99+ ME는 CK, IK를 생성하기 위해 c4, c5 함수가 필요하다.

b) 과정 : R99+ MSC/VLR은 RNC가 암복호화와 무결성 보호를 할 수 있도록 자신이 저장하고 있는 Triplet의 Kc로 CK, IK를 계산해서 target RNC에게 전송한다. 사용자 측면에서는 SIM이 저장하고 있



〔그림 25〕 동일한 R99+ MSC/VLR에서의 핸드오버 (GSM security context)v



〔그림 26〕 R98- 또는 R99+ MSC/VLR에서 R99+ MSC/VLR로의 핸드오버(GSM security context)

는 Kc를 ME에게 전송한 다음, ME는 그 Kc로 CK, IK를 생성한다. 이 과정은 [그림 25]에 나타나 있다.

2) R98- 또는 R99+ MSC/VLR에서 R99+ MSC/VLR로의 핸드오버

a) 설명 : 3G 가입자에 대해서는 R98- MSC/VLR이 제어하는 GSM BSS에서 R99+ MSC/VLR이 제어하는 UTRAN으로 이동했을 경우이고, 2G 가입자에 대해서는 R98- 또는 R99+ MSC/VLR이 제어하는 GSM BSS에서 R99+ MSC/VLR이 제어하는 UTRAN으로 이동했을 경우로서, RNC와 ME가 암복호화와 무결성 보호를 할 수 있도록 키 값의 전송 과정을 보여주고 있다.

b) 과정 : 처음의 R98- 또는 R99+ MSC/VLR은 R99+ MSC/VLR이 제어하는 RNC가 암복호화 와 무결성 보호를 할 수 있도록 자신이 저장하고 있는 Triplet의 Kc를 새로운 R99+ MSC/VLR에게 전송한다. 그리고 새로운 R99+ MSC/VLR은 받은 Kc로부터 CK, IK를 생성해서 target RNC에게 전송한다. 처음의 MSC/VLR은 서비스 전체에 걸쳐 anchor point로서의 역할을 하게 된다. 사용자 측면에서는 SIM 또는 USIM이 저장하고 있는 Kc를 ME에게 전송한다. 그리고 ME는 받은 Kc로 CK, IK를 생성한다. R99+ MSC/VLR과 R99+ ME는 CK, IK를 생성하기 위해 c4, c5 함수가 필요하다. 이 과정은 [그림 26]에 나타나있다.

5.2 PS-Domain 서비스에 대한 핸드오버

PS-Domain 서비스를 제공하는 경우에는 SGSN이 참여를 하므로 SGSN을 중심으로 설명을 한다.

5.2.1 UTRAN에서 GSM BSS로의 핸드오버

이 경우는 CS-Domain 서비스에서 MSC/VLR이 과정에 참여하는 것에서 SGSN이 이 과정에 참여 하는 것으로 바뀐 것 외에는 동일한 과정을 행하게 된다. 그리고 다른 SGSN으로의 핸드오버 시 새로운 SGSN이 새로운 anchor point의 역할을 한다.

5.2.2 GSM BSS에서 UTRAN로의 핸드오버

5.2.2.1 UMTS security context

이 경우 SGSN이 CS-Domain 서비스와 동일한 과정을 수행한다. 또한 새로운 SGSN이 서비스에 대해서 새로운 anchor point의 역할을 하게 된다.

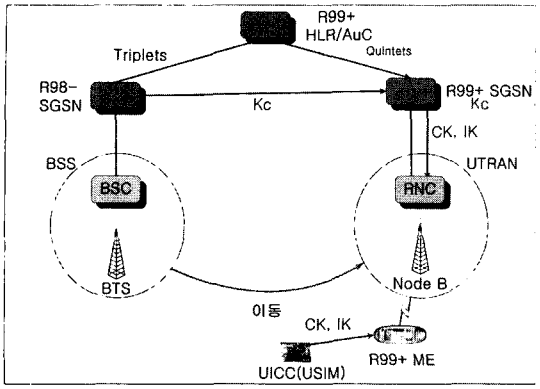
5.2.2.2 GSM security context

이 경우는 3G 가입자와 2G 가입자로 구분해서 고려될 수 있다.

• 3G 가입자

처음에 R98- SGSN 내에서 사용자가 R98- ME나 UMTS AKA가 가능하지 않은 R99+ ME을 사용하거나, R99+ ME를 사용하다가 R99+ SGSN으로 핸드오버가 일어날 경우이다. 3G 가입자가 GSM security context를 사용하려면 R99+ HLR/AuC으로부터 Triplet을 받는 경우인데, 이 경우는 처음의 SGSN이 R98-인 한가지 경우 밖에 생기지 않는다.

1) 설명 : R98- SGSN이 제어하는 GSM BSS에서 R99+ SGSN이 제어하는 UTRAN으로 이동했을 경우로서, RNC와 ME가 암복호화와 무결성 보호를 할 수 있도록 키 값의 전송 과정을 보여주고 있다.



[그림 27] R98- SGSN에서 R99+ SGSN으로의 핸드오버(GSM security context)

2) 과정 : 처음의 R98- SGSN은 저장하고 있는 Kc를 새로운 R99+ SGSN에게 전송하고 나서, 새로운 R99+ SGSN은 가입자가 2G인지 3G인지에 대한 지적이 없기 때문에 R99+ SGSN과 USIM 사이에 새로운 UMTS AKA 과정을 실행하게 되고 새로운 키 값을 공유하게 된다. 새로운 R99+ SGSN은 서비스 전체에 걸쳐 anchor point로서의 역할을 하게 된다. 이 과정은 [그림 27]에 나타나 있다.

• 2G 가입자

이 경우는 UTRAN으로의 핸드오버가 이루어 진 후 CK, IK를 생성할 수 있어야 하므로 사용자가 R99+ ME를 사용하는 경우에만 가능하다.

다음은 네트워크 관점에서 세 가지 핸드오버의 경우에 대해서 설명하고 있으며, MSC/VLR이 참여하던 것에서 SGSN이 참여하는 것으로 바뀐 것 외에는 CS-Domain 서비스에서와 동일하고, 새로운 SGSN이 그 서비스에서 새로운 anchor point가 된다는 점에서 차이가 있다.

1) 동일한 R99+ SGSN에서의 핸드오버
2) R99+ SGSN에서 다른 R99+ SGSN로의 핸드오버
3) R98- SGSN에서 다른 R99+ SGSN로의 핸드오버

Ⅵ. 결 론

본 논문은 2G 가입자나 3G 가입자가 네트워크 이동시 이동통신 서비스를 제공받기 위해서 필요한 무선 구간에서의 암복호화나 무결성 보호를 위해 사용되는 암호화 키와 무결성 키를 공유하는 과정을 보여주고 있다. 이를 이해하기 위해 GSM과 UMTS 네트워크 구조를 살펴보았고, 2G와 3G 가입자가 등록 후 시스템에서의 인증과 키 일치 과정을 분석하였다.

또한 2G와 3G 가입자가 위치하는 다양한 시스템의 버전에 따라 여러 가지 경우로 나누어 인증과 키 일치 과정을 분석하였으며 이를 통해, 가입자가 어떠한 시스템에 등록해서 처음에 어떻게 인증과 키 일치 과정이 이루어졌으며, 그 이후에 다른 네트워크로 이동할 때 새로운 인증과 키 일치 과정을 CS와 PS 도메인으로 나누어 분석하였다.

참 고 문 헌

[1] 3GPP TS 23.002 V5.9.0, "Network architecture", *3rd Generation Partnership Project, Technical Specification Group*, Valbonne, France, 2002.12.

[2] 3GPP TS 03.20 V8.1.0, "Security related network functions", *3rd Generation Partnership Project, Technical Specification Group*, Valbonne, France, 2000. 10.

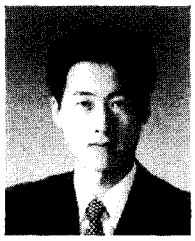
[3] 3GPP TS 33.102 V5.1.0, "Security Architecture", *3rd Generation Partnership Project, Technical Specification Group*, 3G Security, Valbonne, France, 2002.12.

[4] 3GPP TS 21.905 V5.5.0, "Vocabulary for 3GPP Specification", *3rd Generation Partnership Project, Technical Specification Group*, System Aspect, Valbonne, France, 2002.12.

[5] 3GPP TR 31.900 V5.1.0, "SIM/USIM Internal and External Interworking Aspects", *3rd Generation Partnership Project, Technical Specification Group*, Valbonne, France, 2002.06.

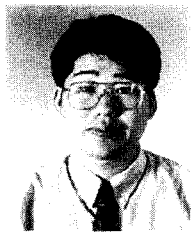
〈著者紹介〉

이 세 광 (Se-Kwang Lee)
2002년 3월~현재 : 고려대학교 정보보호대학원 석사과정
<관심분야> 정보보호, 이동통신



조 승 환 (Seung-Hwan Jo)
2001년 9월~현재 : 고려대학교 정보보호대학원 석사과정
<관심분야> 정보보호, 이동통신

이 옥 연 (Ok-Yeon Yi)
1999년 7월~2001년 8월 : 한국전자통신연구원 정보보호기술연구본부 선임연구원
2001년 9월~현재 : 국민대학교 자연과학대학 수학과 전임강사
<관심분야> 정보보호, 이동통신, 암호론



서 창 호 (Chang-Ho Seo)
1996년~2000년 2월 : 한국전자통신연구원 부호기술부 선임연구원
2000년 3월~현재 : 공주대학교 응용수학과 부교수
<관심분야> 정보보호, 이동통신, 암호론