3GPP2/BCMCS 개요

2006년 8월

경북대학교 통신프로토콜연구실

박재성 (knucsid@gmail.com)

요 약

이 문서는 3GPP2의 BCMCS에 관한 내용을 정리한다. BCMCS(Broadcast Multicast Services)는 3GPP2에서 표준화 작업을 하고 있는 것으로써 멀티미디어 데이터 전송을 목적으로 다수의 사용자에게 하나의 링크로 제공하는 서비스이다. 3GPP의 MBMS와 유사한 서비스이다.

목 차

1. 서론

BCMCS(Broadcast Multicast Services)는 3GPP2에서 표준화 작업을 하고 있는 것으로써 멀티미디어 데이터 전송을 목적으로 다수의 사용자에게 하나의 링크로 제공하는 서비스이다. 그리고 무선 네트워크상에서 동일 정보의 불필요한 반복 전송을 제거하는 서비스이다. 3GPP의 MBMS와 유사한 서비스이지만 IP 멀티캐스트는 아니다.

BCMCS는 CDMA 대역에서 멀티미디어 방송 서비스가 가능하도록 정의하고 있다. 즉, 브로드캐스트와 멀티캐스트 서비스를 CDMA2000의 동작 기반을 둔 무선 이동통신 네트워크라고 생각할 수 있다. 최근에는 위성 디지털 미디어 방송 서비스(DMB)의 대안으로 고려된다.

BCMCS가 의미하듯이 BCS(Broadcast Service)와 MCS(Multicast Service)로 나눌 수 있다. 쉽게 생각해서 BCS는 특정 지역에 한해 서비스를 하는 방식이고 MCS는 가입된 사용자에게 서비스를 하는 방식이다.

2. 요구사항

BCMCS의 대략적인 요구사항은 다음과 같다.

- 송수신 영역 : Operator는 BCMCS 전송범위를 정의할 수 있어야 한다. 각각의 전송 범위는 같은 네트워크의 다양한 유효범위를 사용하여야 한다.

- BCMCS를 위한 개발 : BCMCS를 위해 예를 들면 암호화와 같은 이용 가능한 프로그램을 개발해야 한다.

- 암호화 : BCMCS는 BCMCS 프로그램의 암호화를 이용할 수 있게 지원해 주어야 한다.

- 인터넷 연결 지원 : BCMCS 프로그램은 인터넷 기반의 멀티캐스트 서비스를 사용하는 사용자를 차단해서는 안된다.

- 모든 멀티미디어 타입 지원 : 예를 들면 비디오와 오디오 같은 모든 멀티미디어 타입을 지원해야 한다.

- QoS : 비디오나 오디오 같은 서비스에서 실시간 서비스를 지원할 필요가 있다.

- 특정한 프로그램의 사용자 권한부여 : 특정한 BCMCS 프로그램에 BCMCS 사용자 인증을 가능하게 해야한다.

- 다양한 프로그램 : BCMCS는 다양한 프로그램을 지원해야 한다.

- 우선순위 : 멀티캐스트 IP 흐름을 위한 다양한 우선 순위를 두어야 한다.

- 전화가 왔을 경우 통보 : BCMCS 프로그램을 받는 동안 전화가 오면 그 전화를 받을 수 있어야 한다.

- 전용 Radio 채널 지원 : BCMCS의 컨텐츠를 교신할 수 있는 공유하거나 분리된 채널이 필요하다.

3. BCMCS 구조

3.1 BCMCS의 기본 구조

아래 <그림 1>은 BCMCS의 전체적인 구조를 나타내고 있다. 그림에서와 같이 BCMCS의 콘텐츠는 콘텐츠 프로바이더가 생성하여 콘텐츠 서버로 보낸다. 콘텐츠 서버는 여러 곳에서 제공받은 콘텐츠를 하나로 합치고 이를 암호화한다. 암호화한 콘텐츠는 변환 후 BSN으로 전송한다. PDSN은 BSC/PCF와 통신하여 필요한 부분을 처리한 후 BSN은 MU/UIM으로 최종적으로 전송된다. BSC/PCF는 PDSN과 MS/UIM 사이에서 bearer 채널의 설정 및 제거 기능을 담당한다.

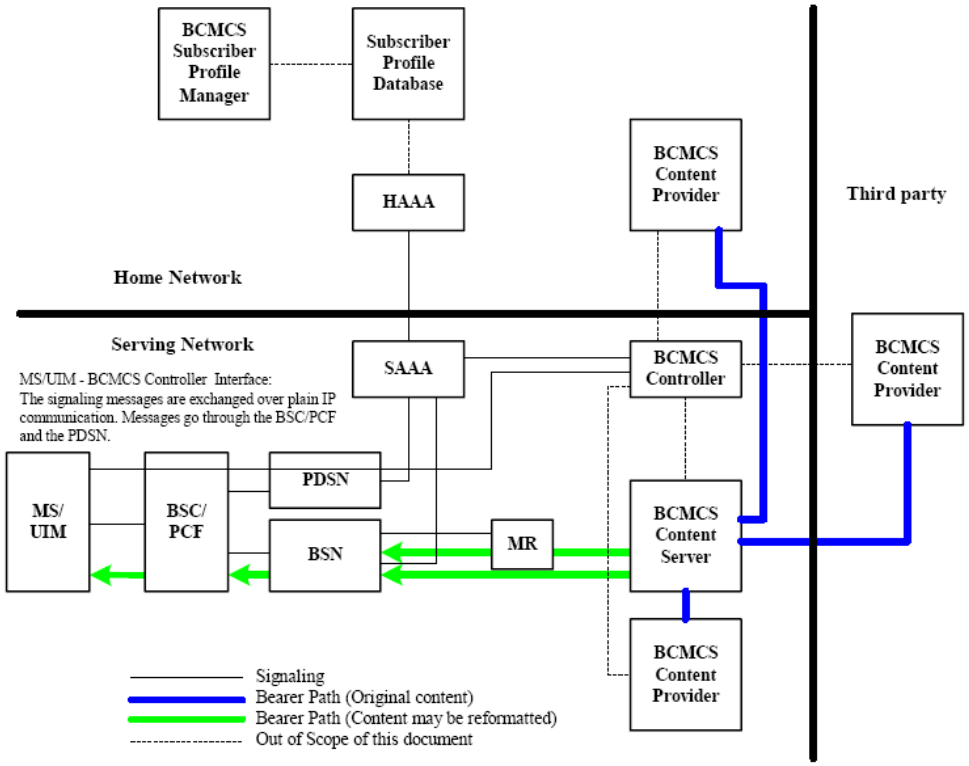

그림 1. BCMCS 구조

BCMCS Controller는 Serving Network 부분으로 네트워크에서 전반적인 제어 동작을 수행한다. BCMCS 세션 정보를 PDSN, MS, Content Server에 제공하고 관리한다. BAK Distributor와 Generator 기능을 수행한다. 그리고 MS에 사용할 권한을 부여한다.

BCMCS Content Server는 Serving Network 부분으로 콘텐츠 프로바이더로부터 받은 콘텐츠를 통합하는 기능을 한다. 여러 프로바이더로부터 콘텐츠를 받을 수 있기 때문에 그것을 받은 콘텐츠 서버는 일련되게 통합하고 보안을 위하여 암호화하는 기능을 한다.

BCMCS Content Provider는 콘텐츠를 생성하거나 콘텐츠의 소스를 의미한다. 콘텐츠 프로바이더는 네트워크 어느 부분에서든지 가능하다.

BCMCS Subscriber Profile Manager는 Home Network 부분으로 회원 프로파일을 관리하고 업데이트 역할을 한다. 응용이라고 보면 된다.

AAA는 Authentication, Authorization and Accounting을 의미하는 것으로 Home Network에서는 H-AAA가 Serving Network에서는 S-AAA가 존재한다.

Subscriber Profile Database는 Home Network 부분으로 회원 프로파일을 저장하고 있는 곳이다. 이곳에서 H-AAA와 통신하여 정보를 제공하는 역할을 한다.

PDSN는 Packet Data Serving Node으로 Serving Network 부분이다. PDSN은 패킷 데이터 세션 설립, IP Flows의 추가, 삭제 등을 위해 유니캐스트 패킷 데이터 서비스를 이용하여 MS와 통신한다.

BSN은 멀티캐스트 IP Flows의 추가 삭제를 위해 BSC/PCF와 통신한다. 그리고 콘텐츠 서버에서 수신한 콘텐츠를 해당 처리를 하여 전송한다.

MR은 Multicast Router로 선택적이다. 이 부분을 거치고 전송될 수도 있고 거치지 않고 전송될 수도 있다. 콘텐츠가 PDSN과 콘텐츠 서버사이의 제공된 터널위에서 전송된다면 거치지 않고 전송할 수 있다.

MS는 BCMCS 정보 획득, 등록하고 멀티캐스트 IP Flows을 수신하는 역할을 한다.

BSC/PCF는 Serving Network 부분으로 PDSN과 MS 사이에서 베어러 채널의 시그널링, 설립, 해제를 담당한다. 그리고 링크 계층에서 암호화가 되었다면 SK 관리도 제공한다. 또한 요구되는 QoS 보장, 자원 최적화에 맞는 최상의 베어러 채널을 선택한다.

3.2 BCMCS Flow ID 구조

<그림 2>는 BCMCS Flow ID 구조의 한 예제이다. BCMCS Flow ID의 Length를 16비트로 사용한 예제이다. 3비트는 Flow Discriminator의 Length를 나타낸다. 3비트에 의해 BCMCS Program ID와 Flow Discriminator를 구분한다. 아래의 예제에서는 Length = 111, 즉 7비트이므로 13비트 중 7비트는 Flow Discriminator가 되고 나머지 6비트는 BCMCS Program ID가 되는 것이다. 따라서 BCMCS Program ID 하나당 최대 2^7까지 다른 Flow Discriminators를 가질 수 있다.

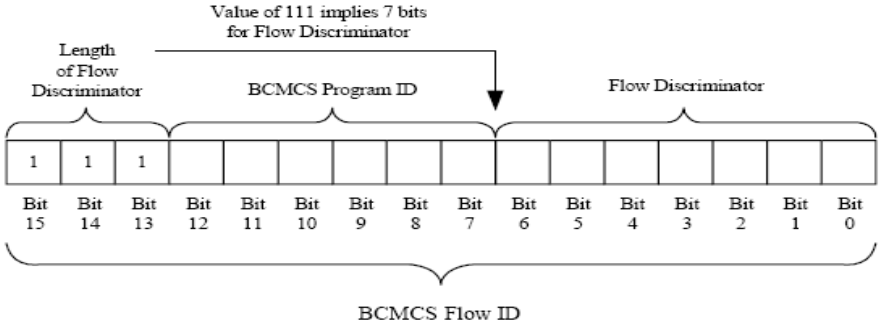

그림 2. BCMCS Flow ID 구조의 예

3.3 Data Air Interface 구조

<그림 3>은 Air Interface 모델을 보여주고 있다. Access Terminal과 Access Network 사이에 위치하고 있다. <그림 4>는 무선에서 사용되는 브로드캐스트 프로토콜의 형태를 나타내고 있다.

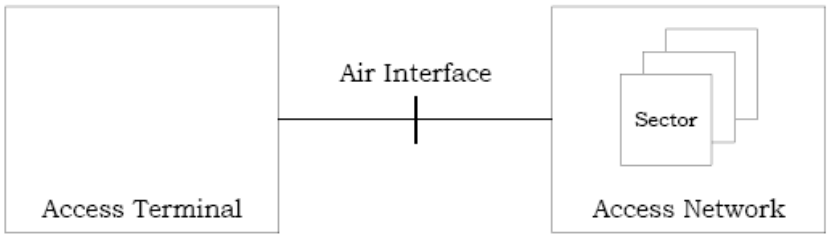

그림 3. Air Interface 모델

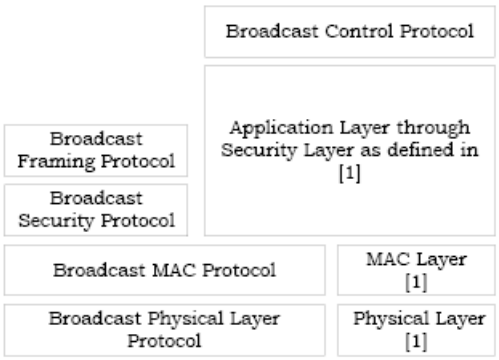

그림 4. 브로드캐스트 프로토콜

4. BCMCS 절차

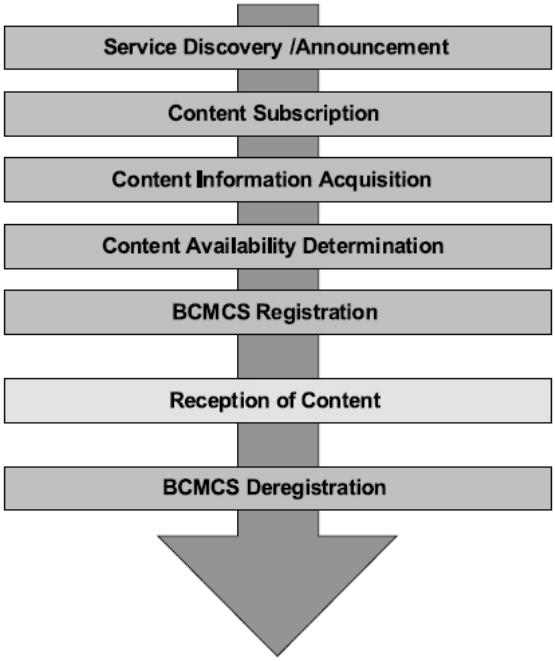

그림 5. BCMCS 기본 절차

1) Service Discovery / Announcement

BCMCS 서비스를 원하는 MS는 BCMCS 제어기, 광고, SMS, WAP, 웹사이트 등을 통해 BCMCS 콘텐츠 종류와 스케줄을 확인한다.

2) Content Subscription

MS Subscription Manager를 통하여 자신이 원하는 콘텐츠를 등록하는 단계이다. 항상 필요한 단계는 아니며 Service Discovery / Announcement 단계 전에 수행될 수도 있다. 암호화를 위해서 RK가 UIM과 Subscription Database에 제공된다.

3) Content Information Acquisition

MS가 BCMCS 제어기로부터 Flow 식별자, IP 주소, 포트, 헤더 정보, Transport / Application 프로토콜 정보, 암호키 등의 정보를 수신한다.

4) Content Availability Determination

MS가 BS의 오버헤드 메시지를 통해 특정 Multicast IP가 Flow가 가용한지 판단하고, MS가 원하는 콘텐츠에 대한 정보가 없으면 원하는 IP Flow를 요구할 수 있다.

5) BCMCS Registration

MS가 원하는 IP Flow의 전송을 요구하는 등록절차를 수행한다. Dynamic Broadcast의 경우에는 MS가 등록을 한 경우에만 PDSN을 통해 콘텐츠를 전송하고, Static Broadcast의 경우에는 MS의 등록여부와 관계없이 콘텐츠를 전송한다.

6) Reception of Content

MS가 BCMCS 콘텐츠를 수신한다.

7) BCMCS Deregistration

MS가 더 이상 특정 IP Flow를 수신하지 않는다는 사실을 BS에게 알려주기 위해 수행한다. BS에서의 타임아웃(BCMCS Registration의 Lifetime이 종료되고 BCMCS Re-registration이 없는 경우)에 의해서도 수행될 수 있다.

5. BCMCS 동작방식

5.1 BCMCS Bearer Path Setup Flow

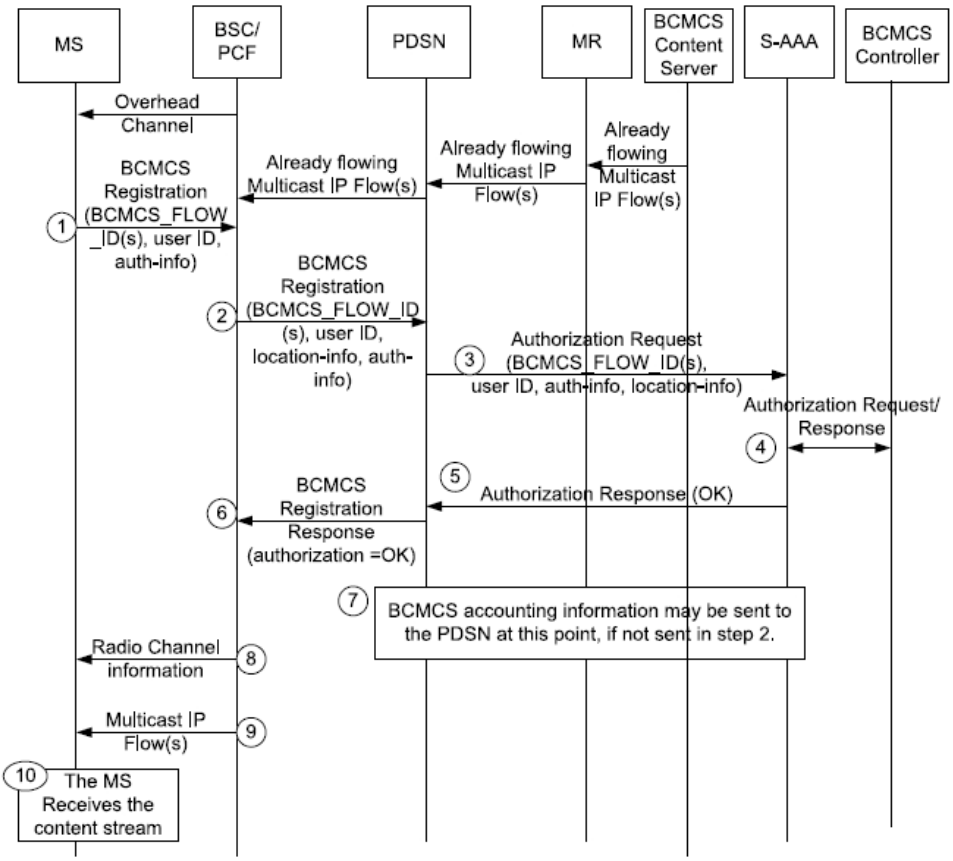

그림 6. Bearer 경로 설정 흐름

Static 브로드캐스트 서비스에서는 BCMCS Bearer 경로는 언제라도 Static 규정에 의해 설정되거나 해제된다. Dynamic 브로드캐스트 서비스에서는 BCMCS Bearer 경로는 MS의 첫번째 등록을 바탕으로 시작되거나 BCMCS Flow가 요구하는 전송으로 RN 결정될 때 설정된다.

위의 <그림 6>는 MS가 IP Flow를 요구하여 BCMCS Bearer 경로가 설정되는 메시지 흐름도를 나타내고 있다. MS는 초과한 채널을 통해 IP Flow에 대한 정보를 얻기 위하여 BCMCS Registration을 전송한다. 이것을 받아 인증 단계를 거쳐 BCMCS Controller가 그것에 관한 응답 및 권한을 부여하고 MS에게는 Radio 채널 정보가 전송된다. 그 후 멀티캐스트 IP Flow를 수신할 수 있게 된다.

5.2 BCMCS Information Acquisition

MS가 BCMCS Controller IP 주소를 발견한 후 MS는 각각의 Multicast Flow 또는 프로그램에 Flow Identity 정보, BCMCS 응용 정보, BCMCS 링크 계층 정보, BCMCS 보안 매개변수 4가지 사항을 요청한다.

MS는 동시에 여러 개의 프로그램이나 Flow에 대한 정보를 요청할 수도 있다. Flow Identity 정보는 BCMCS Controller로부터 BCMCS Information Acquisition Response를 받는다. 그것은 멀티캐스트 IP Address/Port와 BCMCS_FLOW_ID 사이의 Mapping 정보와 등록 시간이 허용된 프로그램에 대한 것을 포함한다. 여기서 등록 시간에 시간은 MS가 BCMCS 프로그램에 등록을 허용하기 전의 시간을 말한다. 다시 말해서 MS는 단지 프로그램의 종료시간과 특정 허용된 등록시간 사이에 등록된 BCMCS 프로그램만을 허용한다는 말이다.

BCMCS 응용 정보는 BCMCS Controller로부터 다음 BCMCS Information Acquisition Response로부터 프로그램 이름, 프로그램 종류, 프로그램 스케줄 시간(시작시간과 종료시간), 각각의 IP Flow에 대응하는 정보에 대한 목록을 받는다. IP Flow에 대응하는 정보에 대한 목록이란 Flow 종류, 멀티캐스트 IP Address/Port, 운송 프로토콜, 응용 프로토콜을 의미한다. 운송 프로토콜이란 예를 들어 RTP/UDP 등을 의미하고 응용 프로토콜이란 예를 들어 MPEG4 등을 의미한다.

BCMCS 링크 계층 정보는 BCMCS Controller로부터 MS에게 암호해독 종류와 헤더 압축 정보에 대한 정보를 전달해준다. 암호해독 종류는 링크 계층 또는 그 상위 계층에 관한 종류를 포함하고 있고 헤더 압축 정보에는 알고리즘, 구성요소 같은 정보가 포함된다. 만약 링크 계층 정보가 무선 통신을 통해 MS에게 제공된다면 BCMCS Controller에 의해 링크 계층 정보의 우선 순위가 결정된다.

BCMCS의 보안 매개변수는 BCMCS Controller로부터 MS에게 TK_RAID, 매개변수와 연관된 Key, 복호화된 각각의 IP Flow에 해당하는 정보들의 목록을 전달받는다. 앞에서 말하는 목록은 BAK_ID, BAK 그리고 BAK 종료시간, 등록 권한 지시자를 포함한다.

5.3 BSN Session Discovery

BCMCS 세션 정보는 아래와 같다.

- BCMCS_FLOW_ID 또는 프로그램 ID와 (멀티캐스트 IP 주소, 종착지 Port 번호)
- 헤더 압축 정보 : 알고리즘과 구성 정보
- 암호화 메커니즘 (링크 계층 암호화 vs. 상위 계층 암호화)
- BAK_ID, BAK, BAK 만료 시간
- 요청된 Flag의 권한부여
- 프로그램 스케줄 (시작 시간, 종료 시간, 허용된 등록 시간)
- BCMCS 세션의 대역폭

BAK가 BSN을 통과한다면 BAK는 SAAA/ BCMCS Controller로부터 BSN에게 안전하게 전달된다.

6. 보안

BCMCS의 보안에 관해서는 현재 브로드캐스트 서비스에 대한 보안 프레임워크를 작성하여 논의 중에 있다. 아직 멀티캐스트 서비스에 대한 보안은 논의하지 않고 있다.

6.1 보안 기능적 구조 및 키 분배

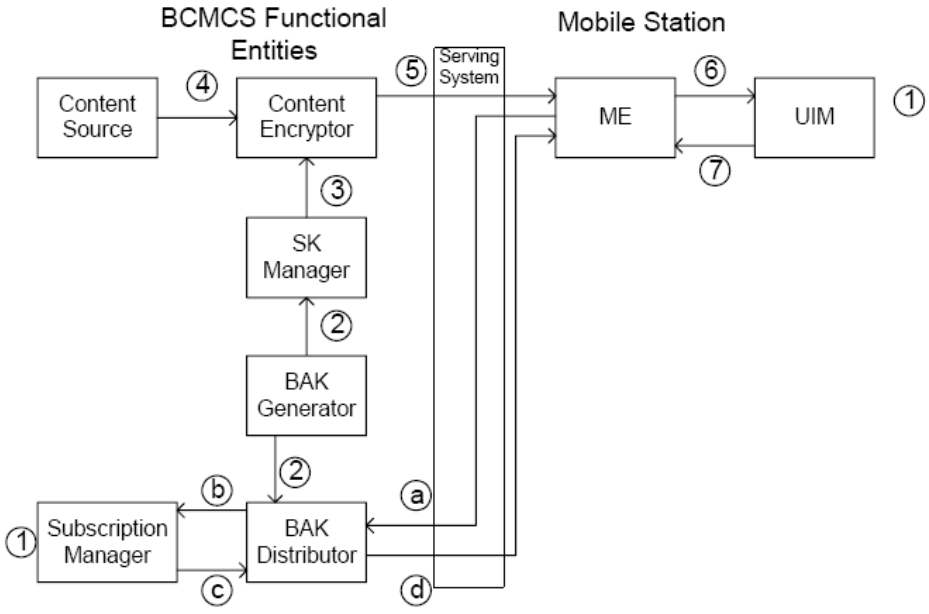

그림 7. BCMCS 보안 기능적 구조

<그림 7>는 보안에서의 기능적 구조에 대해서 나타내고 있다. 1, 2의 동작은 BAK 생성을 위한 동작이고 3~7의 동작은 BAK가 변화하지 않았을 때 멀티캐스트 IP Flow 암호화를 위한 일반적 절차를 나타내고 있다. a~d의 과정은 BAK가 변화했거나 이용할수 없는 경우에 절차를 나타내고 있다.

아래 표는 보안에 사용되어지는 키들을 나타내고 있다.

Keys	Lifetime (usu.)	Purpose
RK	Permanent usu.	Identify the User. The Shared Master Key
TK	Very short	Encrypt BAK for delivery to MS
BAK	A BCMCS Session	Encrypt Session (with SK)
SK	A short time span	Encrypt Content pieces (with BAK)
Auth_Key	.	Authentication for BCMCS Info Acquisition
Auth_Sig	.	Authorization for network access

표 1. Keys in BCMCS

6.2 브로드캐스트 서비스에 관한 보안

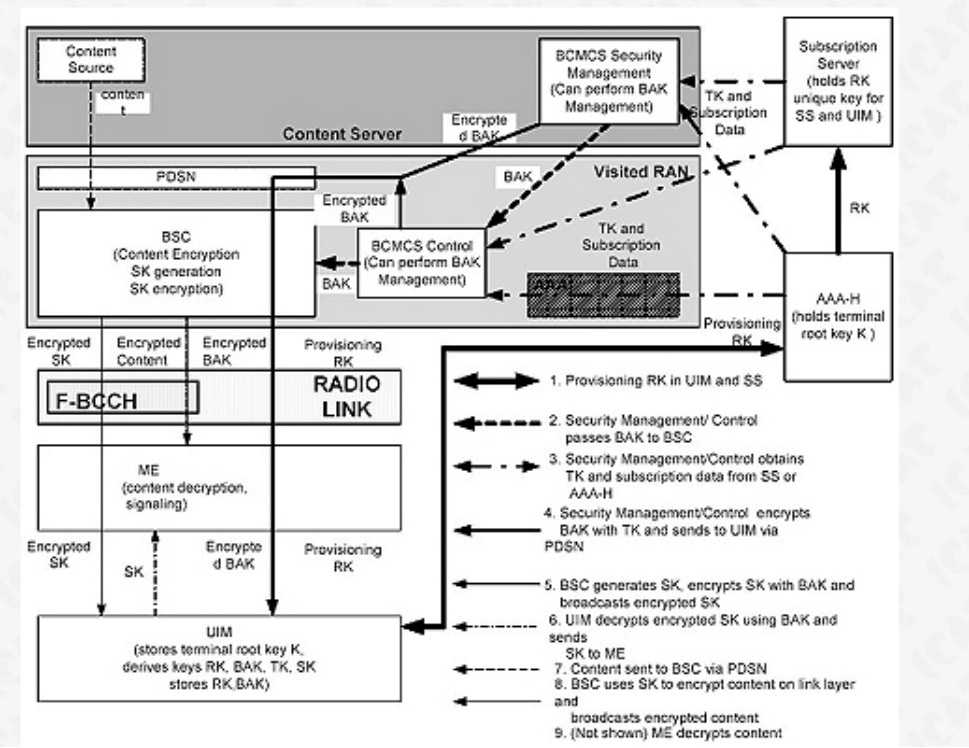

그림 8. 링크계층 암호화가 적용되는 경우의 보안 아키텍처

위의<그림 8> 는 링크계층 암호화가 적용되는 경우의 브로드캐스트 보안 아키텍처를 나타낸다.

3GPP2는 3GPP와 달리 브로드캐스트 서비스에 대해서도 사용자 가입절차를 고려하고 있다. 그러므로 가입되지 않은 사용자가 브로드캐스트 서비스에 접근하여 사용하는 것을 방지하기 위해 보안 메커니즘을 적용해야 한다.

퀄컴에서 제안한 "브로드캐스트 보안 프레임워크"는 BCMCS의 브로드캐스트 서비스 단계를 위한 보안 프레임워크를 정의한 것으로, 콘텐츠를 암호화하고, 복호화 키를 가입한 사용자들에게만 제공하도록 한다. 그렇게 함으로써 비용을 지불하지 않고 콘텐츠에 접근하려는 사용자들을 방지할 수 있다. 퀄컴에서 제안한 이 내용의 주요 초점은 키 관리문제이고, 퀄컴이 제안한 키 관리는 다음과 같다.

먼저 사용자가 특정 Subscription Server에 처음 가입하면 H-AAA는 UIM과 SS에 RK를 제공한다. RK는 SS와 관련된 키들을 전송하기 위해 사용된다. BCMCS에서 BAK의 관리는 CS의 BCMCS 보안 관리자나 서비스 프로바이더의 BCMCS 제어에서 수행될 수 있다. 이 개체들은 UIM에서 TK로 암호화된 BAK를 제공한다. 여기서 TK는 RK로부터 유도된다. 따라서 정당한 UIM만이 암호화된 BAK를 복호화하여 BAK를 얻을 수 있다. 현재 BAK는 그 채널의 모든 가입자에 대해 동일하다. BAK는 운영자에 의해 결정된 시간동안 접근을 제공한다. 현재 BAK는 그 채널의 모든 가입자에 대해 동일한다.

콘텐츠는 빈번하게 변경되는 SK를 사용하여 링크계층 또는 IP 계층에서 암호화되고, ME는 SK를 사용하여 콘텐츠를 복호화한다. BCMCS에 가입하지 않은 사용자의 단말기로 SK를 전달하는 것을 방지하기 위해 SK는 빈번하게 변경된다. 링크계층 암호화가 적용되면, SK의 암호화된 값이 브로드캐스트 되며, 브로드캐스트로부터 SK를 복호화하기 위해서는 BAK가 필요하다. IP 계층 암호화가 적용되면, SK는 BAK와 28비트 난수로부터 유도되고, 난수는 SK를 사용하여 암호화된 콘텐츠와 함께 브로드캐스트 된다. 따라서 MS는 BAK와 브로드캐스트된 난수로부터 SK를 유도할 수 있다. 따라서 UIM이 BAK를 한번 획득하면, UIM은 브로드캐스트를 복호화하기 위해 ME에게 필요한 SK를 계산할 수 있다.

7. 결론

지금까지 본 문서에서는 3GPP2의 BCMCS의 기본적인 개념, 구조, 특징에 대해 살펴보았다. BCMCS는 멀티미디어 데이터를 전송하는데 있어 반복 전송을 최소화하기 때문에 효율적이다. BCMCS는 현재 퀄컴의 뒤를 이어 삼성전자, 노키아 등이 표준화에 참여하고 있다.

특히, MBMS와는 달리 브로드캐스트 서비스에서도 가입을 요구한다. 따라서 기존과는 다른 브로드캐스트 서비스를 제공할 수 있을 것이다. 향후 브로드캐스트 서비스에도 가입과 보안 요소가 요구되면 다른 표준에 비해 활성화 될 것이다. 그러나 멀티캐스트 서비스와의 차이점이 모호한 것은 풀어야할 과제이다. 또한 BCMCS의 멀티캐스트 분야도 계속 연구해나가야 한다.

참고 문헌

[1] 3GPP2 S.R0030-A Version 1.0 “Broadcast/Multicast Services - Stage 1”, 15 Jan 2004.

[2] 3GPP2 S.S0083-A Version 1.0 “Broadcast-Multicast Service Security Framework”, 26 Aug 2004.

[3] 3GPP2 X.S0020-0 Version 1.0 “Broadcast and Multicast Service in cdma2000 Wireless IP network”, Dec 2004.

[4] 3GPP2 C.S0054-0 Version 2.0 “cdma2000 High Rate Broadcast-Multicast Packet Data Air Interface Specification”, Jul 2004.