3GPP MBMS 보안 메커니즘 분석†

박윤경[O1], 임선희[1], 송동호[1], 정영준[1], 이옥연[2], 임종인[1]
[1]고려대학교 정보경영공학전문대학원
{younkpark[O], capsunny, dongdonglove, yz0415, jilim}@korea.ac.kr
[2]국민대학교 자연과학대학 수학과
oyyi@kookmin.ac.kr

Analysis on the 3GPP MBMS Security Mechanism

Youn-Kyoung Park[O1], Sun-Hee Lim[1], Dongho Song[1], Young-Jun Jung[1], Okyeon Yi[2], Jongin Lim[1]
[1]Graduate School of Information Management and Security, Korea University
[2]Department of Mathematics, Kookmin University

요 약

3GPP(3rd Generation Partnership Project) 주도의 유럽형 3세대 이동통신인 UMTS 시스템에서 제공하는 멀티미디어 방송 서비스(Multimedia Broadcast/Multicast Service)는 무선 네트워크상에서 동일한 정보를 하나의 링크를 통해 다수의 사용자에게 제공하는 point-to-multipoint 서비스이다. 콘텐츠가 무료로 제공되면 임의의 사용자들이 콘텐츠가 제공되는 채널에 액세스할 수 있다. 그러나 채널 액세스가 가입(subscription)기반이면, 가입하지 않은 사용자들은 콘텐츠를 이용할 수 없어야 한다. 이를 위해 사용자를 인증하고 안전한 방법으로 콘텐츠를 전송할 수 있는 보안 서비스가 필요하다.
본 논문은 MBMS의 전반적인 개요를 설명하여 앞으로 논의될 내용인 MBMS 보안구조에 대한 배경지식을 제공한다. 또한 브로드캐스트와 멀티캐스트 모드 각각에 대한 MBMS 구조를 설명하고, 멀티캐스트 모드에서의 보안 기능과 키관리 기법, 콘텐츠 보호 기술에 대해 상세히 분석한다.

I. 서론

3세대 단말기의 본격적인 보급과 서비스의 개발이 진행되면서 WCDMA HSDPA(High Speed Downlink Packet Access)와 같은 보다 향상된 시스템과 다양한 서비스 지원이 가능해 짐에 따라 멀티미디어 데이터 서비스의 새로운 시장이 창출되고 있다.

3GPP의 MBMS는 오디오, 비디오, 정지화상, 텍스트, 파일 등의 다양한 멀티미디어 데이터를 단방향 베어러를 통하여 다수의 사용자에게 전달하는 서비스로서 무선 및 유선 자원을 효율적으로 사용할 수 있는 장점이 있다.[1] MBMS 표준화는 사업자들의 요청에 의해 시작됐으며, 모든 태스크 그룹(Task Group)과 관련된 중요한 표준 이슈들 중의 하나이다. 스테이지(Stage) 2 작업에서는 MBMS를 제공하기 위한 기본적 사항들이 정의되었고, 세부적인 기능과 프로시저, 메시지, 프로토콜 동작 등은 스테이지 3 작업을 통해 표준화를 추진 중에 있다.

본고에서는 MBMS 구조와 두 가지 지원서비스인 브로드캐스트/멀티캐스트에 대해 설명하고, 멀티캐스트에서 중요한 키 관리 메커니즘과 콘텐츠 보호방법에 대해 분석한다.

† "본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음"
(IITA-2007-(C1090-0701-0025))

II. MBMS 개요

1. 3세대 이동통신망 MBMS 구조

MBMS는 3GPP 시스템에서의 point-to-multipoint 서비스 개념을 갖는다. 제한된 커버리지 지역에서 하나의 소스 엔티티로부터 다수의 사용자에게 단방향으로 로컬 및 개인화된 콘텐츠를 제공하는데 적합하다. 또한, 모바일 TV에서 가입자별로 대역폭을 할당해 콘텐츠를 제공하는 멀티캐스트(multicast) 방식과 DMB/DVB-H처럼 무작위로 뿌려지는 신호를 고객이 받아서 보는 브로드캐스트(broadcast) 방식을 모두 지원할 수 있는 시스템을 말한다.

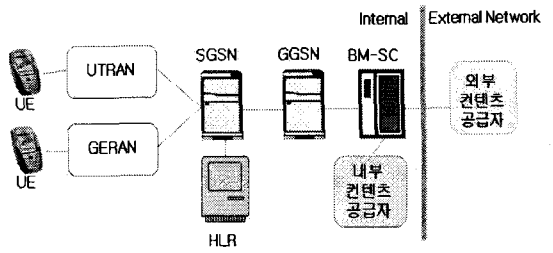

그림 1: MBMS를 위한 UMTS 시스템 구조.

그림 1은 기존의 UMTS(Universal Mobile Telecommunications System) 네트워크에 MBMS 적용을 위한 시스템 구조이다. MBMS 기능을 위하여 UMTS 시스템에 BM-SC(Broadcast Multicast Service Center)라는 엔티티를 추가하였고, BM-SC와의 연계를 위해 ME, UICC, RNS, SGSN, GGSN에서 MBMS를 지원할 수 있도록 하였다.

BM-SC는 내부 혹은 외부 방송 콘텐츠 제공자와 연결되어 수신한 데이터를 사용자에게 전송하고 스케줄링하는 기능을 수행한다. 또한, 콘텐츠 제공자에 대한 인증 및 과금 정보 수집 기능을 수행한다. 이와 같이 이동통신 사업자의 기지국에서 브로드캐스팅까지 할 수 있기 때문에 방송용 기지국의 필요성이 없고, 서비스 제공자의 비용 부담을 줄이며 인프라 구조를 단순화시키는 이점을 제공하는 것이 MBMS 기술이다.

2. MBMS의 기능

브로드캐스트와 멀티캐스트 서비스의 핵심 요구사항은 효율적인 방법으로 네트워크 자원을 사용하여 다수의 사용자들에게 동시에 콘텐츠를 제공할 수 있어야 한다는 것이다. 브로드캐스트 모드에서는 서비스를 활성화한다거나 사용자가 가입해야 하는 것에 대한 특별한 요구 사항이 없기 때문에 3GPP는 브로드캐스트 모드에 대해서는 특별한 보안 요구 사항을 정의하지 않는다. 하지만, 멀티캐스트 모드는 사용자 가입 절차를 필요로 하고, 따라서 앞으로 III장에서 본격적으로 논의될 보안 메커니즘과 연관이 있다.

2.1 브로드캐스트 모드

브로드캐스트 모드는 단일 소스 엔티티에서 특정 방송 서비스 영역에 속한 모든 사용자에게 멀티미디어 데이터를 단방향으로 전송하는 서비스로서 사용자는 자신의 단말에서 방송 서비스 수신 기능을 활성화 또는 비활성화할 수 있다. 브로드캐스트 모드의 경우 모든 사용자가 이를 수신할 수 있기 때문에 서비스 가입 절차가 필요 없으며, 사용자 과금을 위한 데이터 생성이 필요하지 않다.

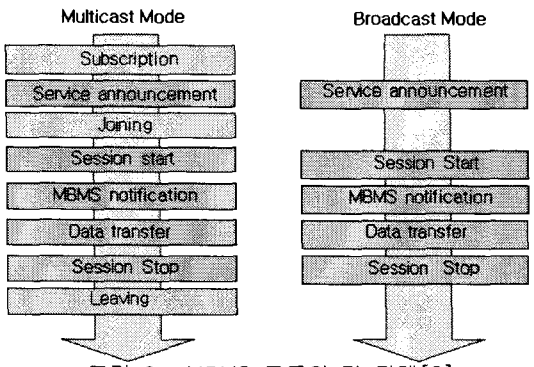

그림 2: MBMS 모드의 각 단계[2]

그림 2는 MBMS의 두 가지 서비스 타입를 보여주고 있다. 브로드캐스트의 경우 멀티캐스트에 비해 가입(subscription), 합류(joining), 탈퇴(leaving)단계가 없음을 알 수 있다.

2.2 멀티캐스트 모드

단일 소스 엔티티에서 특정 멀티캐스트 그룹으로 멀티미디어 데이터를 전송하는 서비스이다. 사용자가 특정 멀티캐스트 MBMS 서비스를 수신하기 위해서는 해당 멀티캐스트 서비스 그룹으로의 가입이 우선되어야 하며 가입된 멀티캐스트 그룹으로 합류함으로써 해당 멀티캐스트 서비스를 수신할 수 있다.[1] 따라서 사용자가 위치하고 있는 지역으로만 데이터를 전송하는 알고리즘이 요구된다.

브로드캐스트에 비해 멀티캐스트 모드의 가장 큰 특징은 과금이 가능해야 한다는 것이다. 일정 권한을 갖고 있는 사용자만 멀티캐스트 서비스를 받을 수 있어야 하며 이러한 권한은 과금과 연계된다. 권한을 가진 사용자만 데이터의 수신이 가능하도록 하기 위해서는 데이터의 암호화가 필수적이며, 암호화에 필요한 암호키 정보는 해당 서비스에 가입하여 일정 비용을 지불한 또는 지불할 사용자에게만 전달된다.

III. MBMS 보안 메커니즘

1. MBMS 보안 개요

MBMS 사용자 서비스에 대한 요구사항은 사용자들을 하나의 그룹으로 묶어 데이터를 안전하게 전송하는 것이다. 이러한 목적을 위하여 인증, 키 분배, 데이터 보호 방법이 필요하다. 일반적인 네트워크 베어러 보안기능을 제외하고 MBMS에 대한 보안기능은 BM-SC나 UE(User Equipment)에 구현된다.[3]

1.1 GBA

GBA는 Generic Bootstrapping Architecture의 약자로써 GSM/UMTS 인증과 키 동의 프로토콜을 기반으로 하는 shared secret key를 이용한 독립적인 인증 메커니즘이다. 특정 응용프로그램에서 접근 제어와 인증이 필요할 경우 GBA를 사용하는데 BM-SC와 UE사이의 공유키 생성에 있어서도 사용된다. 보안 메커니즘으로 AKA(Authentication and Key Agreement)과정을 이용한 Bootstrapping 인증 과정과 Bootstrapping 사용 과정(키 일치 과정)으로 구성된다.[4] 우선 AKA과정이 진행되었다는 전제하에 CK, IK를 가지고 GBA과정을 수행하여 두 개체는 상호 인증되고, 비밀키를 공유하게 된다.

1.2 BM-SC의 기능

BM-SC의 보안기능은 키 요청과 키 분배 역할로 나눌 수 있다. 키 요청은 BSF(Bootstrapping Server Function)로부터 GBA키를 찾아 MUK(MBMS User Key)와 MRK(MBMS Request Key)를 도출하고, MBMS 사용자 서비스를 등록/해제, MSK(MBMS Service Key)를 요청하는 것으로 요약할 수 있다.

키 분배는 등록기능으로부터 MUK를 찾고, 세션당 각 UE에 해당하는 MSK와 MTK(MBMS Traffic Key)를 생성하여 분배하는 역할을 한다.

1.3 UE에서 정의하는 보안 구조

MBMS를 위한 키 모듈은 UE안에 MGV-S(MB-MS key

Generation and Validation Storage)라는 안전한 공간을 정의하여 MGV-F(MBMS key Generation and Validation Function)기능과 함께 구현된다.

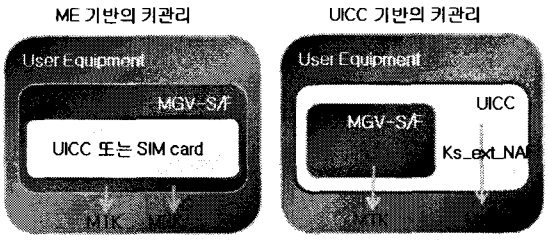

그림 3: MBMS 기능을 적용한 UE 보안 구조.

MGV-S는 ME나 UICC에 구현될 수 있는 안전한 저장 공간이다. MGV-F는 MBMS 키와 같은 보안이 요구되는 정보가 노출되는 것을 방지하기 위해 보호된 실행 환경으로써 구현된다. MGV-S는 MBMS 키들을 저장하고, MGV-F는 ME에 대한 보호되지 않는 공간으로부터의 키 노출 방지 기능을 수행한다.

2. MBMS 보안 메커니즘

2.1 GBA와 키 관리

모든 UMTS 보안 절차는 각 UE와 네트워크 사이에서 수행된다. 두 개체간의 상호인증 후에 공유된 비밀정보는 전송된 데이터에 대한 기밀성과 무결성을 확신하는데 사용된다. 그러나 MBMS의 경우 point-to-multipoint 베어러를 통해 동일한 데이터를 많은 수의 UE로 전송해야 하는데 이때에는 one-to-many로 기밀성과 무결성이 보장되어야 한다. 이것은 단일 데이터 송신자(BM-SC)가 각각의 UE와 공유하는 비밀정보를 갖고 있어야 한다는 것을 의미하고, 비밀키는 주기적으로 업데이트 되어야 하는 것이다. 이음새 없는(seamless) 서비스 수신을 위해 old 키와 new 키 개념이 도입된다. Identification 정보는 키와 함께 전송되어 키에 대한 식별자로써의 역할을 하고, 수신자는 키 식별자 정보를 통해 해당 키로 복호화할 수 있다.

UE와 BM-SC는 공유키를 만들기 위해 GBA를 이용한다. 만약 Service Announcement가 MBMS 사용자 서비스 보호를 명령한다면 생성된 공유키는 UE와 BM-SC 사이에 point-to-point 통신을 보호하기 위해 사용된다. 그러나 UE에서 이용 가능한 GBA 키들이 없다면 UE는 BSF와 GBA 실행을 시작하게 된다.

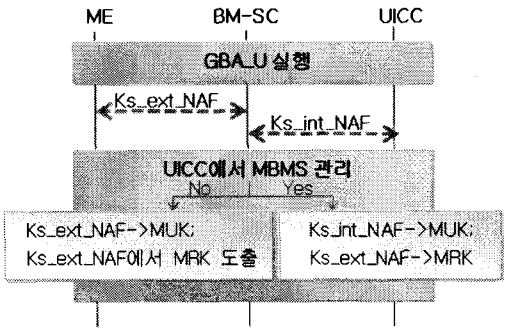

그림 4: GBA를 이용한 키 도출 과정.

그림 4는 초기에 UE와 UMTS 시스템사이에 상호인증이 완료된 후 GBA를 실행하여 Ks_ext_NAF와 Ks_int_NAF를 공유했을 때 UICC에서 MBMS를 담당할 경우와 ME에서 담당할 경우를 나누어 MUK와 MRK가 어떻게 도출되는지를 나타낸다. 사실상 콘텐츠를 암호화 할 때 실질적으로 사용하는 키는 MTK이다. 정상적인 가입자는 MSK msg를 받았을 때 그림 4에서 도출했던 MUK를 이용하여 복호화하고, MTK msg를 받았을 때 MSK로 복호화하여 MTK를 알아낼 수 있다. 그림 5는 MTK 도출과정의 일부를 보여준다. BM-SC는 ME로 $E_{MSK}(MTK)$를 전송한 후 서비스를 위한 암호화된 데이터를 전송된다.

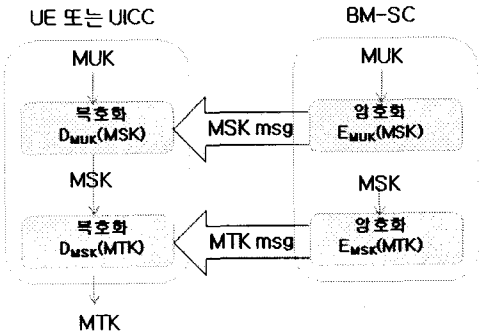

그림 5: MTK 도출 과정.

3GPP는 MBMS를 위한 키 관리 메커니즘으로 사전 공유(pre-shared) 키를 효율적으로 사용한다고 판단되는 MIKEY(Multimedia Internet KEYing, RFC 3830[6]) 기법을 권장하고 있다. MIKEY는 실시간 멀티미디어 어플리케이션을 위한 안전한 키 관리 기법으로써 일대일 통신, 그룹통신에서 이용된다. 단, MIKEY 표준에서 의무사항으로 정의한 공개키 암호, 공개키 암호화와 관련된 페이로드(payload), AES Key Wrap 알고리즘, NTP-UTC(Network Time Protocol-Coordinated Universal Time)와 NTP 페이로드 타입에 관한 구현은 제외한다.

2.2 전송 트래픽 보호

MBMS 사용자 서비스는 하나 이상의 MBMS 스트리밍 세션 또는 다운로드 세션으로 구성되어 있다. 스트리밍 세션은 오디오나 비디오와 같은 미디어에 추가적으로 텍스트나 이미지를 전송하는 형태로써 각 세션은 하나 이상의 RTP(Realtime Transport Protocol) 세션으로 되어 있다. 다운로드 세션은 다수의 수신자에게 지연 제약 없이 신뢰성 있는 이진 데이터 전송하는 것으로 파일을 예로 들 수 있다. 각 다운로드 세션은 또한 하나 이상의 FLUTE(File deLivery over Unidirectionnal Transport) 채널로 구성되어 있다. MBMS 데이터는 단방향으로만 전달되기 때문에 FEC(Forward Error Correction) 방식에 의한 오류 정정 기능을 가진다.

MBMS 사용자 서비스는 전송되는 데이터의 중요도와 서비스 형태(스트리밍 또는 다운로드)에 따라 보안의 수준을 정한다. 콘텐츠 보안을 적용할 경우 기밀성과 무결성이 요구되며, UE와 BM-SC에서 대칭키를 공유하여 양쪽에 적용된다.

MBMS 스트리밍 데이터의 경우 SRTP(Secure Real-ti-

me Transport Protocol)[7]를 이용하고, 다운로드 데이터의 경우 OMA(Open Mobile Alliance)에서 정의한 DCF 콘텐츠 포맷을 사용하여 보안을 적용한다.
DRM(Digital Rights Management) 보안은 MBMS 보안과는 독립적인 표준이므로 MBMS 콘텐츠 보안의 한 가지 방법이라 할 수 있다. 현재 TS 33.246 릴리즈7에서는 MBMS의 DCF(DRM Content Format)로 OMA DRM v2.0 DCF[5]를 제안하고 있다. MBMS 보안은 콘텐츠에 대한 전송을 보호하는 것이다. 이러한 관점에서 볼 때 사용자가 데이터를 다운로드 받은 후에는 콘텐츠의 사용이 자유롭다. 그러나 콘텐츠 자체를 보호하고 싶다면 OMA DRM v2 메커니즘으로 가능하다.[8]

IV. 결론

현재 3GPP에서는 3G 기술을 보다 진보시키기 위한 논의들이 진행 중이며, 한편으로는 Beyond 3G 또는 4G라는 이름으로 차세대 이동통신기술에 대한 논의가 진행중이다. 4세대 이동통신은 기존의 3G 이동통신을 기반으로 진화된 차세대 이동통신이 될 것이다. 또한 3G 진화기술들의 상용화가 새로운 신규기술의 상용화보다는 훨씬 가능성이 높을 것으로 보인다.
3G 멀티미디어 방송 서비스를 지원하기 위해 높은 데이터 전송률 지원, 신뢰성 있는 전송을 위한 QoS 향상, 멀티캐스트 서비스를 위한 보안 개선 등에 대한 연구가 진행 중에 있다. MBMS에서의 보안은 통신채널에서 정상적인 가입자의 프라이버시가 노출되는 경우나 기밀성을 위협받는 도청뿐만 아니라 비가입 사용자에 의한 서비스 이용도 고려해야 한다. 이처럼 point-to-point로 서비스를 제공하는 다른 보안 메커니즘과는 상이한 특성을 지니기 때문에 무선 네트워크의 효율성을 유지하면서 복호화 키를 주기적으로 업데이트하여 가입자도 예측할 수 없도록 운영되어야 한다.
최근 지상파 및 위성 DMB, DAB, DVB-H, MediaFLO 등의 기술을 이용한 다양한 이동 방송 서비스가 상용화 혹은 계획 중에 있다. 이동통신망에서의 방송 및 멀티캐스트 서비스는 3GPP의 MBMS 뿐만 아니라 3GPP2의 BCMCS(Broadcast and Multicast Service)라는 이름으로 표준화가 진행중이다.
본 논문에서는 3GPP에서 제안하는 MBMS의 구조와 기능, 서비스에 대해 연구하고, 서비스의 한 종류인 멀티캐스트 모드에서의 키관리, 콘텐츠 보안 등의 보안 메커니즘을 분석하였다.
향후 과제로는, 멀티캐스트 서비스에서 위협이 될 수 있는 공격 형태를 분석하고, 콘텐츠 보안시 필요한 기술과 요구사항에 대한 연구를 수행하는 것이다.

참고문헌

[1]신재욱; 박애순, "방송 통신 융합 서비스(MB-MS)의 3GPP 현황", 한국통신학회지 제22권 4호, 2005.4, pp. 110 ~ 120 (11pages).
[2] 3GPP TS 23.246 V7.3.0, "Multimedia Broadcast/Multicast Service (MBMS);Architecture and functional description(Release 7)".
[3] 3GPP TS 33.246 V7.4.0, "3G Security;Security of Multimedia Broadcast/Multicast Service (MBMS)".
[4] 3GPP TS 32.220 V8.0.0, "Generic Authentication Architecture (GAA); Generic bootstrapping architecture".
[5] OMA-DRM-DCF-v2_0: "OMA DRM Content Format", www.openmobilealliance.org.
[6] IETF RFC 3830 "MIKEY: Multimedia Internet KEYing"
[7] IETF RFC 3711 "Secure Real-time Transport Protocol".
[8] Valtteri Niemi, "Trends in Mobile Security Standards", Nokia Research Center.