韓國컴퓨터情報學會 論文誌
第14卷 第3號, 2009. 3.

2009-14-3-2-5

실시간 디지털 콘텐츠 데이터 전송을 위한 효율적인 OKTEK(One-way Key-chain for TEK) 기법에 관한 연구

전 상 훈*

A study on the Efficient OKTEK(One-way Key-chain for TEK) for Realtime Digital Contents Transmission

Sang Hoon, Jeon*

요 약

일반적으로 사용하고 있는 와이브로는 실시간 데이터를 전송하는 기술로 단말이 이동함으로서 기지국 변경으로 인한 빈번한 키 분배, 사용자 인증 및 재 인증 등의 처리과정이 요구되며, 이에 사용하는 보안기술은 빠르게 처리되어야 하는 제한적인 요구를 갖는다. 특히 키 재생성 및 재분배와 같은 키 관리 메커니즘은 와이브로 환경뿐만 아닌 일반적인 이기종 무선 환경에서도 실시간 디지털 콘텐츠 전송 서비스에 많은 영향을 주게 된다. 따라서 본 연구에서는 IPTV와 같은 실시간 디지털 콘텐츠 전송을 위해 서버 또는 기지국간의 키와 메시지 교환 처리과정의 부담을 줄여 단말과 기지국간의 효율적인 데이터 전송을 위해 제안하는 OKTEK 키 체인을 통한 트래픽 관리 기법을 제안한다.

Abstract

IEEE 802.16e(Wibro) standard, providing robust mobile realtime data transmission technology, requires of faster and smooth execution of security mechanisms, such as key distribution and user authentications, during base station hopping. In particular, key management mechanisms such as redistribution and regeneration have an impact on digital contents transmission and realtime data transmission, not only in 802.16e environment, but also in typical transmission environment as well. This paper presents traffic management mechanisms designed to realtime digital contents (such as IPTV)transmission efficiency and increase the QoE by utilizing OKTEK methodology.

▸ Keyword : Digital contents transmission, Key chain, 802.16e, QoE, Authentication

• 제1저자 : 전상훈
• 투고일 : 2009. 2. 27, 심사일 : 2009. 2. 28, 게재확정일 : 2009. 3. 11.
* 숭실대학교 일반대학원 컴퓨터학과 컴퓨터통신 연구실

Ⅰ. 서 론

전화, 방송, 인터넷 기술은 네트워크의 광대역화 및 방송의 디지털화에 따라 광대역 네트워크를 통해 융합하고 있는 현재에 이종산업 간의 융합된 대표적인 서비스가 IPTV이다. 음성, 데이터, 방송이라는 세 가지 미디어의 결합을 의미하는 TPS(Triple Play Service)에서 이동성과 QPS(Quadruple Play Service)로 발전하고 있으며, VOD나 IPTV와 같은 실시간 방송을 위한 효율적인 디지털 콘텐츠 전송 서비스 기술이 요구되고 있다. IPTV와 같은 기술은 IP기반의 이동성을 보장하는 방식으로 연구가 진행되고 있으며, BcN은 통신, 방송, 인터넷이 융합된 품질 보장형 멀티미디어 서비스를 광대역으로 이용할 수 있는 통합 네트워크의 구현을 목적으로 사용자가 멀티미디어 서비스를 이용할 때 다양한 액세스 망을 통한 단말 이동을 전제로 하고 있다. 그리고 공유된 네트워크를 이용하여 방송 및 콘텐츠를 제공하기 때문에, 서비스의 품질이 가변적이며, 동일한 전송 에러에 대해서도 품질저하의 정도는 큰 차이를 나타낸다.

QoE(Quality of Experience)은 종단 시스템에 포함되는 터미널, 네트워크, 서비스 인프라 구조 등에 영향을 받는 서비스 품질 모두를 포함하며, 사용자의 경험이나 환경에 영향을 받게 된다. 멀티미디어의 실시간 전송에 따르는 미디어 품질(최소의 비트율, 최대 패킷 손실), 보안성(콘텐츠의 저작권 보호, 사용자의 인증), 사용성(사용자 인터페이스, EPG), 콘텐츠 품질(비디오, 오디오) 등 실시간 전송의 품질(QoE) 요소에 영향을 주는 요인이 되고 있다. 그리고 이러한 요소들로는 비디오/오디오(압축코덱, 비트율), 네트워크 전송(손실, 지연, 지터), 제어기능(인터넷 관리 그룹, 프로토콜 지연, 버퍼링 지연, 복호화 지연)이 있다[1][2][3][4][13][14]. 방송 또는 대용량 디지털 콘텐츠를 전송하는데 주기적인 인증 요청과 응답을 처리하는데 매번 사용자에 대한 인증 과정을 거쳐야 하기 때문에, 서비스를 제공하는 서버에 부하를 초래하고, 네트워크에 과도한 트래픽으로 패킷 손실과 지연 등으로 전송 품질을 저하시킨다. 따라서 본 연구에서는 와이브로 환경내의 대용량 디지털 콘텐츠 데이터 전송위해 교환하는 키 및 메시지 정보 교환을 최소화하고 과도한 트래픽을 줄여 품질을 향상시키고, 데이터 암 ·복호화 수행시간을 경감시키기 위한 효율적인 키 체인 관리 기법을 제안하고자 한다.

본 논문의 구성은 2장에서 IPTV를 위한 멀티캐스트 기술과 현행 IEEE 802.16e의 PKM, PKM2 프로토콜을 설명하고 3장에서 본 연구에서 디지털 콘텐츠 전송을 위해 트래픽 감소시키는 효율적인 제안기법 설명한다. 그리고 4장에서는 IEEE 802.16e의 기존 프로토콜과 제안 프로토콜을 비교 분석하여 프로토콜의 효율성을 평가하고 5장의 결론으로 마치도록 한다.

Ⅱ. 관련 연구

2.1. 멀티캐스트 서비스

실시간 IPTV 서비스와 같은 실시간 디지털 콘텐츠 서비스를 제공하기 위해서는 반드시 멀티캐스트 기능을 지원해야 한다. 일반적인 IP 멀티캐스트 기술을 이용하면 라우팅 프로토콜을 통해 전송 경로를 구성하고 모든 참가자에 멀티캐스트 패킷을 전달 하지만, 이러한 방법은 모든 라우터가 멀티캐스트 라우터로 교체되어야 하며, 많은 비용이 요구된다. 따라서 현재 다양한 대안 멀티캐스트 기술이 고려되고 있다.

서버 기반 멀티캐스트 방식과 CDN(Contents Distribution Network) 기반은 IPTV와 같은 대용량 데이터 전송서비스를 구현하기 가장 쉽다. 서비스 제공자가 관리하는 미디어 서버 또는 서버 풀을 통해, 직접 유니캐스트 방식으로 서비스를 제공하거나, CDN 서버로 서비스 제공할 수 있다. 그러나 서비스를 제공하는 서버의 부하와 대역폭 고갈을 초래하고, 서비스 그룹의 크기가 제한되며, 네트워크 대역에 큰 영향을 미치게 된다. 또한 개인 PC의 성능의 발달에 따라 P2P(Peer to Peer) 기반 멀티캐스트 방식은 디지털콘텐츠 서비스를 제공하기 위해 수신자가 송 ·수신자의 기능을 하는 전송 방법으로 부하의 분산시킬 수 있는 장점이 있지만, 각 노드들의 PC의 성능에 따라 실시간 데이터 전송을 보장할 수 없는 단점도 있다. 그리고 오버레이(Overlay) 기반 멀티캐스트 방식은 서비스를 제공하는 서버나 특정 노드를 이용하여 멀티캐스트 전송 방식으로 서비스 제공자의 관리 하에 따라 IPTV 서비스를 위한 멀티캐스트가 제공된다면, 일반 종단 사용자의 PC를 이용하는 방식보다 안정적인 서비스가 제공될 수 있다. 그러나 앞서 언급한 멀티캐스트 방식을 독립적으로 사용하지 않고 각 방식의 장점을 혼용하여, 멀티캐스트-P2P 방식이나 CDN-P2P 멀티캐스트 방식과 같이 하이브리드 멀티캐스트 방식을 사용하고 있다[2][15].

2.2. PKM(Privacy key Management)

IEEE 802.16e 표준은 물리계층(PHY), 매체접근제어계층(MAC)에 대해 기술하고 있다. MAC은 연결 설정, 시스템

접속, 대역폭 할당 및 관리 기능을 담당하며, 매체 접근제어 계층 중 최하위에 보안기능을 제공하는 보안 부계층으로 정의하고 있다.

표 1. PKMv1과 PKMv2의 인증방식 및 사용 키
Table 1.PKMv1 & PKMv2 authentication method

구분	PKMv1	PKMv2
인증내용	단말 (단방향)인증	단말/사용자 (양방향)인증
인증방식	RSA기반 인증	RSA기반/ EAP기반 인증
데이터 무결성	No MAC, HMAC	No MAC, HMAC/CMAC
TEK 암호화	3DES	3DES-EDE, RSA AES-EBC/KEY-WRAP
데이터 암호화	No Encryption DES	No Encryption/ DES-CBC, 3DES,RSA AES-CCM/CBC/CTR
인증키 교환	기지국은 단말의 공개키로 암호화하여 인증키를 직접 분배	RSA 기반: 기지국은 pre-PAK을 단말의 공개키로 암호화하여 분배하고 pre-PAK으로부터 단말과 기지국은 인증키 자체생성. EAP기반: 인증서버는 AAA-Key를 단말에 분배하고, AAA-Key로부터 단말,인증 서버는 인증키 자체생성.

보안 부계층(Security Sublayer)은 망에 접근하는 단말 또는 사용자 인증, 세션 그리고 데이터 암호화를 위한 키 생성 및 교환, 암호화된 데이터 송수신, 메시지 무결성 검증하는 부분으로 구성되며, 인증 및 키 교환을 위해 PKM(Privacy key Management) 프로토콜을 사용한다.

PKM 프로토콜은 단말과 기지국의 단·양방향 인증과 주기적인 재 인증, 그리고 키 갱신을 수행하며, 트래픽에 대한 키 관리는 클라이언트/서버 모델에 따라 수행된다. 그러나 단말과 기지국간의 인증을 위해 다수의 키와 메시지를 교환해야하며, 대용량 데이터를 전송하기 위해서는 과다한 또는 불필요한 트래픽을 제어 및 관리를 위한 기술이 요구된다. 표1의 PKMv1은 단말이 망에 접속하기 위해 X.509 인증서를 사용하며, 단말은 제조될 때 자신의 MAC 주소 및 RSA 기반 공개키가 결합된 인증서를 갖는다. 단말(SS: Subscriber Station)은 인증서를 기반으로 기지국(BS: Base Station)에 인증 요청을 하고, 기지국은 인증서를 기반으로 단말을 인증한다. 그리고 기지국은 인증키(AK: Authorization Key)를 생성한 후 단말의 공개키로 암호화해 단말에 전송하며, 단말은 자신의 비밀키로 복호화하여 인증키를 얻게 된다. 공유된 인증키는 각각 KEK와 무결성 검사키를 생성하는데 사용되며, 여기서 KEK(Key Encryption Key)는 단말/기지국간 TEK(Traffic Encryption Key)를 안전하게 전달하기 위해 사용되는 키로써, 단말은 TEK를 요청하고, 기지국은 TEK를 KEK로 암호화해 단말에 분배한다. 그리고 사용자의 트래픽은 TEK로 암호화해 안전하게 전달된다.

PKMv2는 단말이 기지국을 인증하고, 기지국이 단말을 인증하는 양방향 인증방식을 사용하며, 표1과 같이 RSA 기반 인증방식과 EAP(Extensible Authentication Protocol) 기반 인증방식을 지원한다. 여기서 RSA 기반 인증방식은 PKMv1과 같은 RSA 기반의 공개키와 단말의 MAC 주소를 결합한 X.509 인증서를 사용하지만, 기지국도 단말에 인증서를 제공하는 양방향 인증방식을 사용하며, 인증시, 메시지 무결성 보장을 위해 전자서명이 포함된다. PKMv2의 EAP-AKA 인증방식의 EAP-AKA 프로토콜은 단말과 인증 서버 간에 동일키를 공유하여 상호 인증하는 알고리즘을 사용하고 있다. 기지국은 단말에 인증을 요청하고, 단말은 자신의 Identity를 NAI(Network Access Identifier) 형식으로 제공하며, 인증서버는 단말의 NAI에 맞는 Challenge 값을 전달한다. 그리고 단말은 이에 대한 응답(Response)을 인증서버(AAA)에 전송한다[6][12]. 이와 같이 다양한 제어 및 암호 기술로 인해 서버의 부담을 유발시키게 된다. 현재 PKMv2 프로토콜 인증기법은 공격자로부터 사용자 또는 단말인증, 안전한 데이터 송 ·수신을 위해 보다 보안성이 강화되고 있으나, 강화된 인증 수행 과정은 수많은 트래픽을 발생시켜, 프로토콜의 지연 암·복호화 수행에 따른 네트워크 지연 및 손실로 대용량 데이터 전송 서비스에 큰 영향을 미친다.

2.3. PKM 인증 및 TEK 관리

PKM 프로토콜은 단말(SS)과 기지국(BS)간의 인증을 제공하고 끊김 없는 데이터 송·수신을 위해 단말과 기지국간에 단말 또는 사용자를 인증 및 갱신하기 위해 그림1과 같이 6개의 상태 머신을 갖는다[4].

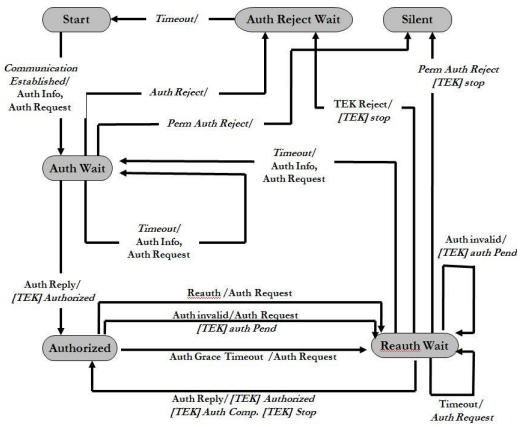

그림 1. 인증상태 머신
Fig. 1. authentication state machine

- Start: 인증 초기 상태를 나타내며, 어떠한 자원도 인증 상태 머신에 의해서 사용되거나 할당되지 않는다.
- Authorize Wait (Auth Wait): 단말이 기지국과의 협상 단계가 완료되었음을 나타내며, "Communication Established" 이벤트를 수신하여, 이벤트에 대한 응답으로 인증정보 메시지와 Auth Request 메시지를 BS로 전송하고 응답을 기다리는 상태이다.
- Authorized: 해당 단말에게 유효한 SAID 리스트를 포함한 Auth Reply 메시지를 수신한다.
- Reauthorize Wait (Reauth Wait): 단말이 재 인증을 요청하는 상태로, 인증키가 만료되었거나 유효하지 않음을 기지국으로부터 통보받아, Authorization Invalid 메시지를 기지국으로 Auth Request 메시지를 송신하고, 응답을 기다리는 상태이다.
- Authorize Reject Wait (Auth Reject Wait): 최근 전송한 Auth Request 메시지를 기지국으로부터 Authorization Reject(Auth Reject) 수신한다.
- Silent: 단말은 최근에 전송한 Auth Request 메시지에 대해 기지국으로부터 Auth Reject 메시지를 수신한 상태로, Auth Reject의 에러 코드는 영구적 인증 실패를 나타낸다. 그리고 단말에게 트래픽 데이터를 제공하지 않는 Silent 상태로 천이된다.

단말은 지속적으로 재 인증 절차를 요청하여 인증상태와 유효한 인증키를 유지해야 하며, 할당 받은 인증키는 주기적으로 갱신해야한다. 또한 기지국에 Auth Request 메시지를 전송함으로써 인증키를 갱신해야한다. 이와 같이 현행 PMK 프로토콜은 단말을 인증하기 위해 메시지를 송·수신하고 키를 도출하고 계산되어야 하며, 인증키의 유효시간을 계산하여 인증 상태를 유지 또는 관리해야만 한다. 따라서 단말 인증된 SAID 당 두 개의 트래픽 키 관리를 해야 하고, 암호화 키 상태 머신의 운용으로 단말은 키가 만료되기 전에 미리 설정된 TEK Grace Time의 시간에 새로운 키 정보들을 요청한다. 인증된 SAID 각각에 대하여 단말은 상향 링크 TEK를 위해 두 개의 TEK 중, 새로운 암호화키를 사용하고, 하향 링크 트래픽을 복호화하기 위해 두 개의 암호화 키 중, 하나의 TEK를 사용한다. 그리고 단말의 SA TEK 사용 정책을 그림2의 좌측면에서 확인할 수 있으며, TEK의 유효시간의 음영지역은 MAC PDU의 암호화를 위해 처리과정과 적용구간이다.

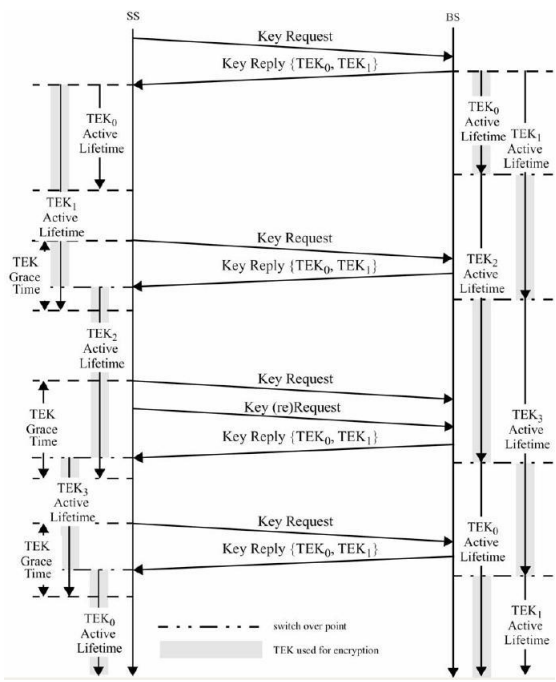

그림 2. 단말과 기지국간의 TEK 관리
Fig. 2. TEK Management

이와 같이 PKM 프로토콜은 기지국과 단말의 상호 단·양방향 인증을 수행함으로써 보안성을 강화하지만, 데이터 전송 중에 인증 및 키 갱신을 위한 메시지 및 키 교환을 필요로 한다. 이러한 점은 대용량 데이터 전송에 서비스 품질의 저하요인이 되며, 네트워크의 지연에 따른 재 인증이 요구되어, 서버의 부하를 가중시킨다. 따라서 본 논문에서 제안하는 키 체인 기법을 통해, 단말과 기지국간에 교환하는 메시지 트래픽과 키 도출 및 처리시간을 경감시키고, 효율적인 대용량 데이터 전송 서비스가 필요하다.

III. 제안하는 OKTEK 관리 및 인증

전송 데이터의 품질 향상을 위한 기법은 와이브로에서 사용하고 있는 키 및 메시지 교환 트래픽과 단말과 기지국간의 트래픽 및 암·복호 수행시간을 경감하여 대용량 콘텐츠 전송 서비스의 효율성을 향상시키고자 한다.

3.1. OKTEK(One-way Key-chain for TEK)

S/Key[8]나 TESLA[9]와 같은 단방향 키 체인(One-way Key-chain)기법은 K1, K2, K3,… Ki와 같은 키 리스트에서 어떤 특정키가 노출될 경우, 이전 키 또는 마지막 키를 쉽게 유도할 수 없다. 따라서 단말과 기지국간에 교환하는 트래픽을 경감과 효율적인 키 교환을 위해 OKTEK(One-way Key-chain for TEK) 기법에 적용하였다.

다항식 P, 충분히 큰 수 n, 시간을 이용한 공격 F 다항식이 존재한다고 가정할 때, 다음 두 조건을 만족한다(1)(2).

$$\forall_i, j \in 1,2,\ldots t, i > j \ \exists\ F, F(k_j) = k_i \quad \cdots\cdots\cdots (1)$$

$$\forall_i, j \in 1,2,\ldots t, i > j \ \forall F, P[F(k_i) = k_j] < \frac{1}{p(n)} \quad \cdots\cdots\cdots (2)$$

단방향 함수를 f라 하고 $j-i$ 반복적으로 계산된 f^{j-i}라면, 단방향 키 체인을 (3)과 같이 유도할 수 있다.

$$\forall_i, j \in 1,2,\ldots t, i < j,\ TEK_j = f^{j-i}(TEK_i) \quad (3)$$

따라서 본 연구에서 제안하는 OKTEK은 다음과 같이 TEK 체인을 생성할 수 있다(4).

$$TEK^{i-1} \xrightarrow{F(TEK_{i-1}, SN_i, N_{i-1})} TEK_i \xrightarrow{F(TEK_i, SN_i, N_i)} TEK_{i+1} \quad \cdots\cdots (4)$$

최초 TEK0는 인증 과정 중에 얻는 AK(Authorization Key), SN_Info, 초기 Nonce 값으로 생성하고, 두 번째 TEK1은 TEK0과 SN_Info로 설정된 Sni, 증감시키는 방식의 고유의 카운터 기능을 하는 Nonce 값을 생성하여, 지속적인 인증을 수행하지 않고 Nonce의 값을 검증함으로 단말과 기지국간에 추가적인 인증 또는 메시지를 교환하지 않아도 각각 단말과 기지국은 OKTEK에서 이전 키와 다음 키를 Nonce값을 각각 도출할 수 있어, AK 인증 및 갱신 또는 트래픽을 암·복호화 하기 위한 이전 TEK(Older_TEK)와 다음 TEK(Newer_TEK)를 각각 단말과 기지국이 유도하여 메시지를 교환할 필요가 없다. 따라서 race time에 재 인증을 위한 메시지와 인증 재 요청과정을 필요로 하지 않음으로 트래픽 전송을 위한 메시지 교환하기 위한 트래픽을 효과적으로 경감시킬 수 있다.

3.2. OKTEK의 관리

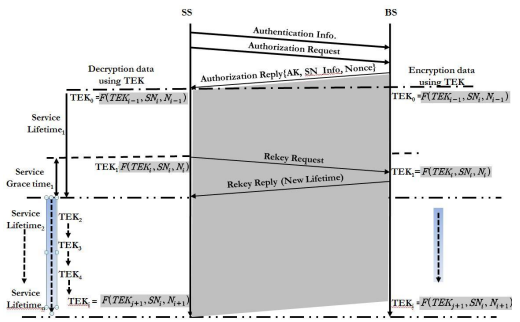

그림 3. 단말과 기지국간의 제안 OKTEK 흐름도
Fig. 3. Proposed OKTEK Flow

초기 단말(SS)와 기지국(BS)간의 인증 수행이 완료되면, (4)를 통해 단말과 기지국은 제안 OKTEK 기법에서 키 체인을 위해 AK(Authorization Key), 키의 SN_Info, N(Nonce)를 이용하여, 대용량의 멀티캐스트 데이터의 암·복호화를 위한 TEK 키를 각각 생성한다. 키 갱신 주기는 Service Lifetime이 만료시점에 Grace Time에 수행하며, 단말과 기지국간의 TEK 교환과정을 그림3과 같이 표현하였다. 초기 TEK를 유지 및 관리하기 위해서는 SS로부터 수신한 인증정보를 BS가 수신하여 단방향 키 체인을 이용한 키 생성을 하고 SS로 전송한다. 그리고 수신된 TEK1은 BS에서 Nonce값에 포함된 시퀀스에 의해 SS가 수신한 TEK1과 동일키임을 단말과 기지국이 각각 검증과 동기화하여, 단말과 기지국 또는 서버의 수행과정을 줄이고, 교환 메시지와 키와 같은 트래픽의 양을 감소시킨다. 단말과 기지국이 각각 TEK(Newer_Key)와 TEK(Older_Key)를 도출해야하지만, OKTEK에서는 TEK를 도출하기 위한 갱신 요청/응답(Rekey Request/Reply) 메시지 교환 이후, 발생하는 추가적인 메시지 교환이 필요 없어, 단말과 기지국 간의 생성된 TEK(Newer_Key)와 TEK(Older_Key)의 교환메시지 수 및 검증시간을 경감시킨다.

그림3의 음영영역은 키 체인(Key Chain)으로 암·복호화

가 가능한 영역을 나타낸 것으로 데이터 전송 구간을 의미한다. 데이터 전송 중에 인증 및 키 갱신을 위한 메시지 교환을 최소화하고, 지속적인 양방향 인증과 키 갱신을 동시에 수행하므로 단말과 기지국간에 인증수행 과정에 필요한 메시지 교환횟수를 경감할 수 있다. 그리고 단말 인증은 초기 인증과정에서 단말이 갖는 인증관련 정보를 서버에 전송함으로써 이뤄지며, 802.16e의 요구사항에 의해 제한된 서비스 주기(Service Lifetime)를 갖는다. 한 주기 동안 여러 개의 TEK가 사용되며, 주기가 종료되기 전에, 갱신을 위한 갱신 요청(Rekey Request)을 하면서, 서버와 단말의 Service Grace time을 두고 주기를 재설정한다[4][7][10].

3.3. OKTEK의 인증

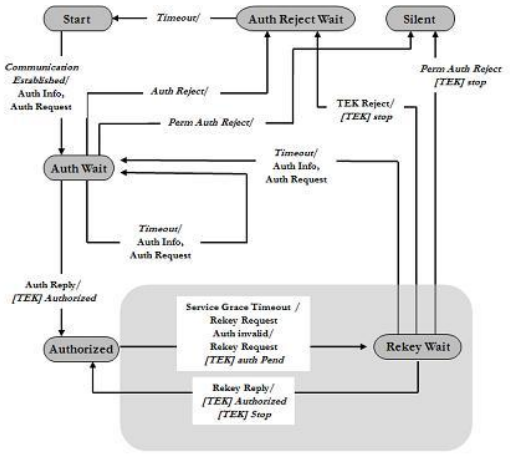

그림 4. 제안기법 인증 상태머신
Fig.4. Proposed authentication state machine

PKM 프로토콜의 인증과정은 6개의 상태와 8개의 이벤트, 키 관리는 6개의 상태와 9개의 이벤트를 갖는다. OKTEK는 인증과 Key 관리를 통합하여 6개의 상태와 9개의 이벤트, 6개의 메시지를 가지며, 갱신을 위한 상태와 메시지가 필요 없다. 그리고 인증 상태머신은 Rekey Wait 상태를 제외하고는 PKM 프로토콜의 인증 상태머신과 동일하며, 재 인증 과정 없이 할당된 시퀀스에 의해 단말과 기지국이 각각 생성되고 이에 대한 상태천이와 이벤트는 없다. 그리고 Lifetime 갱신을 위해서는 Rekey Request/Reply 메시지를 송·수신하는 "Rekey Wait" 상태를 적용하였으며, 이를 그림4로 표현하였다. 그림4의 음영영역에 나타낸 Rekey Wait 상태는 단말의 Service Lifetime이 만료되거나 인증을 갱신하는 경우, 단말이 해당 SAID에 대한 갱신 요청을 대기하는 상태로, Rekey Request 메시지를 송신하고 Rekey Reply 메시지를 수신하면, Authorized 상태로 천이된다. 이때 기지국은 Rekey Reply를 통해 그림3과 같이 OKTEK를 이용하여, TEK를 갱신하기 때문에, 재 인증 또는 갱신을 위한 메시지나 키를 교환할 필요가 없다. 그리고 OKTEK의 인증상태머신은 Start, Auth Wait, Auth Reject Wait, Authorized, Authorized, Silent의 현행 인증 머신과 동일한 기능을 수행하지만 Rekey Wait 상태와는 달리, 각 상태로 전이하기 위한 이벤트로 다음과 같은 메시지가 있다.

- Communication Established: 협상 단계가 완료되면, Start 상태에 현 이벤트를 생성하며, 단말이 키를 얻기 위한 과정을 시작한다.
- Timeout: 재전송이나 응답을 기다리는 시간이 만료되었음을 의미한다.
- Authorize: 단말이 인증이 완료되어 Auth Reply 메시지를 수신하면, 이벤트 된다.
- Auth Reject: 단말이 Auth Reject 메시지를 수신하면, Auth Reject Wait 상태로 천이되며, 단말은 타이머가 만료될 때가지 상태를 유지하고 타이머가 만료되는 시점에서 단말은 재 인증을 시도한다.
- Service Life Timeout: 단말에 할당된 Service Life Timer가 만료됨을 의미한다. 타이머는 현재 사용되고 있는 AK가 만료되기 전에 설정 가능한 Grace Time을 갖으며, 단말은 Grace Time이 만료되기 전, Service Time을 갱신하기 위한 요청을 해야만 한다.
- Rekey Allow: 단말이 Rekey Reply 메시지를 수신하면 발생하는 이벤트로서, 단말의 Service Life Time이 갱신됨을 나타내며, Authorized 상태로 천이된다.

Start 상태에서 Communication Established 이벤트가 발생하면 Auth Wait 상태로 천이된다. 이 때 표2에서 나타내고 있는 OKTEK의 메시지 중, 단말은 서버에게 Authentication Info와 Authorization Request를 전송한다.

표 2. 제안 OKTEK에서 사용하는 메시지
Table 2.OKTEK Message

메시지	설 명
Auth Info	단말이 인증을 받는데 필요한 정보를 전송하는 메시지
Auth Request	단말이 인증을 요청하는 메시지 (Auth Info와 함께 전송)

Auth Reply	인증이 완료되면 전송되는 메시지 (AK, SN_Info, Nonce 포함)
Auth Reject	단말이 인증이 실패했을 때, 수신하는 메시지
Rekey Request	단말이 Service Life Time 갱신을 위해 전송하는 메시지
Rekey Reply	LifeTime 갱신이 승인되면 단말에게 전송되는 메시지

그리고 Auth Wait 상태에서 인증이 정상적으로 처리되면 Authorized 상태로, Auth Reject 이벤트가 발생하면 Auth Reject Wait 상태로 천이된다. 또한 Auth Reject Wait 상태에서 Timeout 이벤트가 발생하면 최초 Start 상태로 되돌아가 전송이 중지된다. Authorized 상태는 암호화된 데이터가 단말로 보내지며, Service Lifetime이 만기되면 Service Life Timeout 이벤트가 발생하여 Rekey Wait 상태로 천이된다. 이때 Rekey Reply 메시지를 받게 되면 Rekey Allow 이벤트가 발생하여 Service Lifetime이 갱신되고 Authorized 상태로 복귀한다. 동기화를 위해, Rekey Request가 없으면 재 인증을 위해 Auth Wait 상태로 복귀한다.

IV. 성능비교 및 분석

PKM, PKMv2 프로토콜과 제안 OKTEK의 Storage, Communication, Computation 세 가지 요소에 대해 비교 분석한다. 멀티캐스트 환경을 고려한 비교를 위해 n개의 단말에 m번의 주기적인 인증 및 키 갱신이 일어나고 키 갱신 주기는 Service Lifetime이 만료되었을 때를 가정한다. 그리고 Storage cost는 기지국과 단말에서 사용되고 있는 키의 수를 의미하며, 표3과 같다. IEEE 802.16e의 PKM은 인증에 사용하는 키와 트래픽을 암호화에 사용되는 키는 구분되어 있으며, Service Lifetime이 만료되기 전, Grace Time 동안에 유지되는 키이다. n개의 단말이 기지국과 연결유지를 위해 기지국에 6n개, 단말에 6개의 키를 유지해야하고, 사용되는 키는 AK, 공개키와 HMAC, KEK, 데이터 암·복호화에 Older_TEK, Newer_TEK가 사용된다. 그리고 멀티캐스트를 지원하기 위한 PKMv2는 인증키 교환방식에 따라 키가 추가된다.

본 연구에서는 인증에 사용하는 키와 트래픽에 사용하는 키를 초기 인증 후, 그림3과 같이 기지국과 단말에서 각각 생성하기 때문에, 유지하는 키에 대한 Storage cost에 대해 표3과 같다.

표 3. 프로토콜 비교 (단위: 메시지 수)
Table 3. Comparison of Protocols

프로토콜	키 수		암·복호화 수행		메시지
	기지국	단말	기지국	단말	교환 메시지
PKM	6n	6	nmTc	mTd	15
PKMv2	6n+2	6	m(nTc+Tc)	2mTd	15+4
OKTEK	4n	4	mTh	mTh	13

Communication cost는 인증과 키 갱신을 위해 교환하는 메시지의 수에 대한 cost이다. PKMv1 프로토콜이 인증 및 키를 교환하기위해 15개의 메시지를 사용하며, PKMv2는 멀티캐스트를 위해 그룹 관리를 위한 추가적인 요청 및 응답 메시지가 필요하다. 그리고 Computation cost로 사용되는 인증 및 키 갱신에 관련된 메시지의 암·복호화에 소비되는 시간을 비교하면, 암호화에 소비되는 시간을 Tc, 복호화에 소비되는 시간을 Td, 단방향 함수 수행에 소비되는 시간을 Th로 정의하고 단방향 함수 수행에 시간 Th와 암·복호화에 소비되는 함수를 비교하면 Tc〉〉Th, Td〉〉Th 이다. 여기서 PKMv1은 n개의 단말에 대해 키 갱신을 위한 암호화가 m번 주기적으로 수행하며, 단말의 경우 자신의 키 갱신에 대한 복호화를 m번 수행한다. PKMv2는 그룹 키 갱신에 대한 암·복호화가 추가적으로 수행되기 때문에 표3에 나타낸 시간이 소모된다. 제안하는 OKTEK 기법은 주기적인 키 갱신을 기지국과 단말이 개별적으로 수행하기 때문에 중간 단계에서 수행하는 암·복호화가 없고 Tc〉〉Th, Td〉〉Th 이므로 mTd〉〉mTh이기 때문에 단말에서 수행되는 시간도 PKM보다 매우 적음을 표3에서 확인하였다.

PKMv1과 OKTEK의 암·복호화의 수행시간을 확인하기 위한 실험환경으로는 Windows XP SP3,Intel core2 Duo CPU E6550 2.33GHz, 2.00GB RAM, Python2.4.2 환경에서 단말에서 임의의 데이터 블록(64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536 KB)을 암호화 수행시간을 측정하였다.

표 4. OKTEK 암호화 수행시간
Table 4.OKTEK Process time

	64(KB)	128	1024	4096	16384	65536
1회	4.72E-06	4.85E-06	5.74E-06	5.92E-06	5.97E-06	5.97E-06
2회	4.77E-06	4.86E-06	5.73E-06	5.92E-06	5.98E-06	5.97E-06

3회	4.75E-06	4.85E-06	5.74E-06	5.93E-06	5.97E-06	5.95E-06
4회	4.76E-06	4.87E-06	5.74E-06	5.92E-06	5.97E-06	6.00E-06
5회	4.75E-06	4.85E-06	5.74E-06	5.92E-06	5.96E-06	5.96E-06
6회	4.76E-06	4.86E-06	5.73E-06	5.92E-06	5.96E-06	5.98E-06
7회	4.75E-06	4.85E-06	5.74E-06	5.92E-06	5.96E-06	5.98E-06
8회	4.76E-06	4.87E-06	5.73E-06	5.92E-06	5.97E-06	5.96E-06
9회	4.75E-06	4.85E-06	5.74E-06	5.92E-06	5.96E-06	5.99E-06
10회	4.76E-06	4.86E-06	5.73E-06	5.92E-06	5.97E-06	5.94E-06

그리고 OKTEK 기법의 암호화 수행 시간의 결과는 표4와 같다. 실험은 단말에서 사용하는 메시지 수, 사용키 수를 각각 포함시켜 10회 암호화 수행시간을 제안 기법과 동일한 방법으로 PKMv1을 각각 실험하여, 평균 수행 시간 측정함으로서 제안 기법의 수행시간이 단축됨을 그림5로 확인하였다.

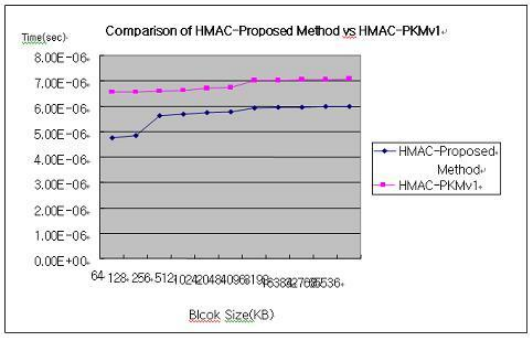

그림 5. PKMv1과 제안 OKTEK 수행시간 비교
Fig. 5. Comparison of PKMv1 and Proposed OKTEK

V. 결 론

본 논문은 IEEE 802.16e환경내의 실시간 디지털 콘텐츠 데이터 전송을 위해 키 및 메시지 정보 교환을 최소화하고 과도한 트래픽을 줄여 서비스의 품질을 향상시킬 수 있는 방안을 제안하였다. 그리고 단말과 기지국간에 교환 메시지의 수를 줄이고 데이터 암·복호화 수행시간을 경감할 수 있었으며, 멀티캐스트 전송에서 다수의 멤버 인증을 위해 요구되는 기지국의 오버헤드를 최소화할 수 있었다. 제안하는 OKTEK 는 IEEE 802.16e환경을 위해 설계되었지만, 이종 간의 실시간 데이터 처리를 위한 프로토콜에 적용하여 대용량 데이터의 전송을 보다 효율적으로 수행할 수 있으리라 기대되며, 향후에는, 멀티캐스트 멤버의 가입 및 탈퇴 시, 키 갱신을 위한 효율적인 기법을 보완하여야 할 것이다.

참고문헌

〔1〕 M.J. Kim, Y.J. Park, S.J. Koh, "*A study on the Trend and Forecast of IPTV Server*" 전자통신동향분석 제21권 제2호, 53-65쪽, 2006년 4월.

〔2〕 윤장우, 이현우, 류원, 김봉태, "IPTV 서비스 및 기술 진화방향," 한국통신학회지, 제25권 제 8호, 3-11쪽, 2008년 8월.

〔3〕 이철희, 이상욱, 이종화, "IPTV 서비스의 체감품질 보장과 모니터링," 한국통신학회지, 제25권, 제8호, 12-19쪽, 2008년 8월.

〔4〕 IEEE, "Air Interface for Fixed and Mobile Broadband Wireless Access Systems," IEEE Std 802.16e, 2006.

〔5〕 강신각, 박주영, 서영일, "IPTV multicast," 한국통신학회지, 제25권 제8호, 20-31쪽, 2008년 8월.

〔6〕 "*와이브로 인증, 키 관리 기술 동향*," 정보보호뉴스 제105호, 2006년 6월.

〔7〕 A. Perrig, R. Canetti, D. Song, and J.D.Tygar, "Timed Efficient Stream Loss- Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction," IETF RFC4082, 2005.

〔8〕 N.M. Haller, "The S/KEY one-time password system," Internet Soc. Symp. on Network and Distribute System, 1994.

〔9〕 A. Perrig, R. Canetti, D. Song, and J.D.Tygar, "Efficient and Secure Source Authentication for Multicast," In Symposium on Network and Distributed Systems Security(NDSS 2001), 2001.

〔10〕 Wan Fang, Wang Dazhen. "An group key distribution protocol for secure group communications," Proceedings of the 6th WSEAS International Conference on Applied Computer Science, pp. 519-527, 2007.

〔11〕 D. Wallner, E. Harder and R. Age, "Key Management for Multicast: Issues and Architectures," IETF RFC 2627, 1999.

〔12〕 S.H. Lim, Okyeon yi, Sungikm jun, Jin-hee Han, "A Study on EAP-AK Authentication

Architecture for WiBro Wireless Network", 한국통신학회논문지, 제31권, 제 4C권, 441-450쪽, 2006년 4월.
〔13〕 이정근, 정진도, "IPTV 양방향성 콘텐츠의 미디어 수용의사와 만족도 상관관계 연구", 한국컴퓨터정보학회논문지, 제13권, 제 1호, 99~108쪽, 2008년 1월
〔14〕 김성철, 김동민, "무선센서 네트워크에서 네트워크 성능을 향상시키는 하이브리드 MAC 프로토콜," 한국컴퓨터정보학회논문지, 제 13권, 제 2호, 177-183쪽, 2008년 3월.
〔15〕 김현주, 남정현, 김승주, 원동호, "통합 멀티캐스팅 환경에서 효율적인 그룹 통신에 관한 연구," 한국컴퓨터정보학회논문지, 제10권, 제 2호, 159-167쪽, 2005년 5월.

저 자 소 개

전 상 훈

2000년 한신대학교 정보통신학 (이학사)
2002년 숭실대학교 컴퓨터학 (공학석사)
2005년 숭실대학교 컴퓨터학 (박사수료)
〈관심분야〉 디지털콘텐츠 보안, 네트워크 보안, 스마트카드,