DOI: 10.3745/KIPSTC.2009.16-C.2.199

IP기반의 Pay-TV 시스템을 위한 안전하고 효율적인 그룹 키 분배 프로토콜

김 정 윤[†] · 최 형 기[††]

요 약

최근 몇 년간, IP-TV 등 IP 기반의 방송 서비스들이 급속도로 보급되고 있다. 이러한 IP기반의 Pay-TV 서비스들은 미디어 컨텐츠를 보호하기 위한 보안 시스템을 필요로 한다. 본 논문은 IP기반의 Pay-TV 보안 시스템인 Conditional Access System을 분석하고, 현재의 Conditional Access System이 비효율적인 방식으로 그룹 키를 분배한다는 사실을 제시한다. 본 논문은 Conditional Access System의 성능을 향상시키기 위해서, 안전하고 효율적인 그룹 키 분배 프로토콜을 제안한다. 본 논문에서 제안하는 프로토콜은 간단한 사칙연산 만으로 그룹 키의 분배가 가능하다. 성능 분석 결과는 본 논문에서 제안하는 프로토콜이 Conditional Access System보다 효율적이라는 것을 보여준다. 뿐만 아니라, 본 논문에서 제안하는 프로토콜에서는 그룹 키를 분배하는 과정에서 서버와 단말 둘만이 공유하게 되는 비밀 값을 쉽게 획득할 수 있다. 이 비밀 값은 서버와 단말이 공유하고 있는 마스터 키를 대체할 수 있으며, 이는 마스터 키의 반복된 사용에 의해 발생되는 공격들로부터 시스템을 안전하게 보호한다.

키워드 : 키분배, 그룹키, 그룹통신, 접근제어시스템

An Efficient and Secure Group Key Distribution Protocol for IP-based Pay-TV Systems

Jung-Yoon Kim[†] · Hyoung-Kee Choi[††]

ABSTRACT

Recently,IP-based broadcasting systems,such as Mobile-TV and IP-TV, have been widely deployed. These systems require a security system to allow only authorized subscribers access to broadcasting services. We analyzed the Conditional Access System, which is a security system used in the IP-based Pay-TV systems. A weakness of the system is that it does not scale well when the system experiences frequent membership changes. In this paper, we propose a group key distribution protocol which overcomes the scalability problem by reducing communication and computation overheads without loss of security strength. Our experimental results show that computation delay of the proposed protocol is smaller than one of the Conditional Access System. This is attributed to the fact that the proposed protocol replaces expensive encryption and decryption with relatively inexpensive arithmetic operations. In addition, the proposed protocol can help to set up a secure channel between a server and a client with the minimum additional overhead.

Keywords : Key Distribution, Group Key, Pay-TV, Conditional Access System

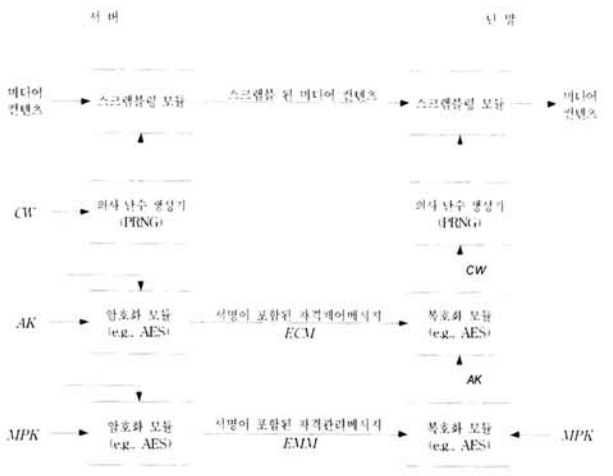
1. 서 론

최근 IP-TV 관련 기술이 발전함에 따라, Digital Video Broadcasting (DVB)을 비롯한 각종 IP 기반의 Pay-TV 서비스들이 각광받고있다. 이에 따라 방송 서비스의 보호와 과금처리가 주요한 과제로 떠오르면서, 각종 방송 사업자들은 미디어 컨텐츠에 대한 접근제어를 필요로 하고 있다.

Conditional Access System (CAS)은 요금을 지불한 가입자 만이 미디어 컨텐츠에 접근할 수 있도록 허용하는 방송용 보안 시스템이다 [1-5. DVB, Digital Audio Broadcasting (DAB), Digital Multimedia Broadcasting (DMB) 등 대부분의 Mobile-TV 및 IP-TV 서비스들이 CAS를 사용하고 있다.

CAS는 미디어 컨텐츠를 보호하기 위해, 스크램블링 키 (Scrambling Key, *SK*), 인증 키 (Authorization Key, *AK*), 마스터 키 (Master Private Key, *MPK*) 로 구성된 3단계 키 체계를 사용한다 [1-5]. *SK*는 CAS 서버가 미디어 컨텐츠를 스크램블링 할 때 사용하며, Control Word (*CW*)를 의사 난수 생성기 (Pseudo Random Number Generator, PRNG)로 연산한 결과값이다. *CW*는 일반적으로 5~20초 정

† 준 회 원 : 성균관대학교 휴대폰학과 박사과정
†† 정 회 원 : 성균관대학교 정보통신공학부 조교수
논문접수 : 2008년 12월 2일
수 정 일 : 1차 2009년 1월 15일
심사완료 : 2009년 1월 20일

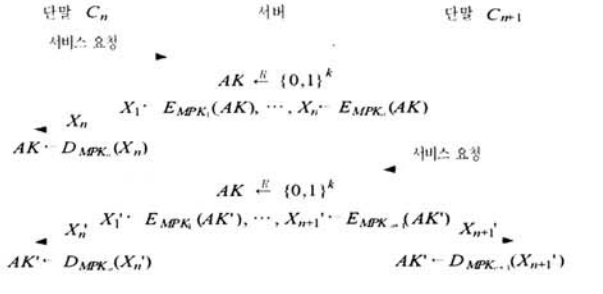


(그림 1) CAS의 키 구조 및 키 전달 과정

도의 간격으로 CAS 서버에 의해 갱신되는데, 이는 공격자에 의한 기지 평문 공격 (known-plaintext attack)의 위험을 줄이기 위함이다 [1], [5]. AK는 *CW*를 암호화하여 그룹에게 전송할 때 사용하는그룹 키 이다. 마지막으로 *MPK*는 *AK*를 암호화하여 각 단말에게 전송할 때 사용한다.

(그림 1)은 CAS 서버가 *CW* 및 *AK*를 전송하는 과정을 나타낸다. (그림 1)에 표시된 자격제어메시지 (Entitlement Control Message, *ECM*)는 각 방송 채널 (그룹) 마다 존재하는 값으로서, 여기에는 해당 채널에 대한 정보와 *AK*로 암호화 된 *CW*가 포함되어 있다. CAS 서버는 *ECM*을 서명한 후, 미디어 컨텐츠와 함께 멀티캐스트를 통해 가입자들에게 전송한다. 자격관리메시지(Entitlement Management Message, *EMM*)는 각 가입자 마다 존재하는 값으로서, 여기에는 각 가입자에 대한 정보와 MPK_i로 암호화 된 *AK*가 포함되어 있다. CAS 서버는 *EMM*을 서명한 후, 각 가입자에게 유니캐스트를 통해 전송한다.

(그림 2)는 임의의 단말이 그룹에 가입했을 때, CAS 서버가 그룹 키 *AK*를 분배하는 과정을 나타낸다. 그룹에 n개의 단말이 가입한 상태에서 n+1번째 단말인 C_{n+1}이 가입할 경우, 서버는 *AK*를 MPK_i ($1 \le i \le n+1$) 로 암호화하여 각 단말에게 전송하게 된다. 마찬가지로, 단말 C_j가 탈퇴할 경우, 서버는 *AK*를 MPK_i ($1 \le i \le n, i \neq j$) 로 암호화하여 MPK_j를 제외한 모든 단말에 전송하게 된다.



(그림 2) 단말이 그룹에 가입했을 때, CAS 서버가 그룹 키를 분배하는 과정

이러한 시스템은 IP-TV와 같이 그룹 맴버쉽의 변화가 빈번한 대규모 그룹 통신에 적용될 경우, 심각한 지연 시간 (delay)을 유발할 수 있다. 실시간 방송 서비스에서 지연 시간은 민감한 요소이고 서비스의 품질과 직결되기 때문에, 효율적인 그룹 키 분배에 관한 연구는 매우 중요하다. 특히, 모바일 환경에서의 방송 서비스는 단말의 한정된 배터리 및 제한된 성능으로 인해 연산 오버헤드를 최소화 시키는 것이 필수적이다.

본 논문은 CAS에서 수행하는 그룹 키 분배 방식의 문제점을 분석하고, CAS의 성능을 개선하기 위한 새로운 그룹 키 분배 프로토콜을 제안한다. 제안하는 프로토콜의 성능 및 안전성을 분석한 결과, 본 논문에서 제안한 프로토콜은 기존 CAS에 비해 성능이 크게 향상되며, IP기반의 Pay-TV에 필요한 보안 요구사항들을 만족한다.

본 논문의 이후 구성은 다음과 같다: 2장은 관련 연구를 소개하며, 3장은 그룹 키 분배에 필요한 보안 요구사항을 설명한다. 4장에서는 제안하는 프로토콜을 설명한다. 5장에서는 제안하는 프로토콜을 실제 IP기반의 pay-TV 시스템에 적용할 수 있도록, 제안하는 프로토콜의 확장 방안을 제안한다. 6장과 7장에서는 각각 제안하는 프로토콜의 성능과 안전성을 분석하며, 8장에서는 본 논문의 결론을 내린다.

2. 관련 연구

단말에게 그룹 키를 분배하기 위한 방식에는, 키 전달 프로토콜과 키 동의 프로토콜이 존재한다. 키 전달 프로토콜은, 하나의 키 관리 서버가 그룹 키를 생성 및 전달하는 방식을 의미한다. 키 동의 프로토콜은, 별도의 키 관리 서버 없이, 단말들이 키 생성에 필요한 메시지들을 송수신하여 그룹 키를 공유하게 되는 방식을 의미한다. 본 논문에서는 기존에 연구된 키 전달 프로토콜과 키 동의 프로토콜을 분석하며, 그 설명은 다음과 같다.

2.1 키 동의 프로토콜

Alan T. Sherman과David A. McGrew는 Merkle Tree를 이용한 그룹 키 분배 프로토콜인 One-way Function Trees (OFT) 를 제안하였다 [6]. OFT의 뿌리 노드 (root node)는 그룹 키를 의미하고, 종단 노드 (leaf node)는 단말과 키 관리 서버가 공유하는 비밀 값을 의미한다. 단말은 그룹 키를 획득하기 위해, 먼저 종단 노드에 해당하는 비밀 값을 해쉬 함수 (hash function)로 연산한 값과, 형제 노드 (sibling node)에 해당하는 비밀 값을 해쉬 함수로 연산한 값을 XOR 함으로써, 부모 노드 (parent node)를 갖게 된다. 그리고 이 부모 노드에 대해서도 위와 같은 과정을 거쳐, 궁극적으로 그룹 키인 뿌리 노드가 계산된다. OFT는, 단말의 가입이나 탈퇴가 발생할 때마다, 대칭 키 기반 암호화 알고리즘과 해쉬 함수를 각각 $\log_2(n+1)$ 씩 수행해야 한다.

Bae Eun Jung은 연산 자원이 제한된 단말들이 효율적으로 그룹 키를 공유하기 위한 키 동의 프로토콜을 제안하였다 [7].

Jung의 프로토콜은 디피-헬만 (Diffie-Hellman) 기반의 그룹 키 동의 방식을 사용하고 있으며, XOR, 해쉬 등 가벼운 연산만으로 구현이 가능하다. 그러나, Su Mi Lee와Dong Hoon Lee는 Jung의 프로토콜에 보안 취약점이 존재한다는 사실을 증명하였다 [8]. Lee 등에 따르면, Jung의 프로토콜은 내부 공격자에 의한 서비스 거부 공격이 발생할 수 있다.

2.2 키 전달 프로토콜

Lakshminath R. Dondeti 등은 그룹의 계층 구조에 기반하여 그룹 키를 분배하는 Dual-Encryption Protocol (DEP) 을 제안하였다 [9]. 이 연구에 의하면, 그룹 키를 효율적으로 갱신하기 위해서는, 하나의 그룹을 다수 개의 서브 그룹으로 분할해야 하며, 각 서브 그룹의 그룹 키를 관리하는 서브 그룹 매니저가 존재해야 한다. 또한, 서브 그룹 매니저가 그룹 통신을 수신할 권한이 없는 경우, 서브 그룹 매니저의 접근을 제한하기 위해, 키 관리 서버는 그룹 가입자에게만 알려진 그룹 키를 이용하여 메시지를 암호화 한다. DEP는 서브 그룹 매니저의 접근 제어가 필요한 상황에는 적합하지만, 그렇지 않은 경우에는 불필요한 암호화에 의한 오버헤드가 발생한다.

Hung-Min Sun 등은 IP기반의 Pay-TV에 적합한 새로운 CAS를 제안했다 [1]. 그들이 제안한 CAS의 그룹 키 분배 기법은 일반적인 키 전달 프로토콜과 달리, 그룹 키 전달에 사용되는 모든 값들을 사전에 오프라인으로 전달하는 방식을 사용한다. 즉, 저자들은 단말 마다 저장해야 하는 정보를 늘리는 대신, 전송 오버헤드 및 연산 오버헤드를 크게 감소시키는 그룹 키 분배 프로토콜을 제안했다. 시스템에 존재하는 모든 단말 C_i ($1 \le i \le n$)에는 각 단말과 관련된 고유 정보 I_i ($1 \le i \le n$)가 있으며, I_i는 C_i를 제외한 나머지 n-1개의 단말들이 모두 알고 있는 값이다. 만약 단말 C_i가 탈퇴를 하면, 나머지 n-1개의 단말들은 탈퇴한 단말과 관련된 정보 I_i를 기존 키에 XOR 함으로써 새로운 키를 획득하게 된다. 따라서, 탈퇴한 단말은 갱신된 키를 알 수 없고, 탈퇴한 단말을 제외한 모든 단말은 갱신된 키를 알 수 있다.

3. 그룹 키 분배를 위한 보안 요구사항

IP기반의 Pay-TV 시스템에서의 그룹키 분배 시 요구되는 보안성을 만족하기 위해서는 다음의 다섯 가지 요구사항을 만족해야 하며, 각각의 요구 사항에 대한 정의는 다음과 같다.

전방향 안전성 (Forward secrecy) : 전방향 안전성은, 그룹을 탈퇴한 단말이 과거의 그룹 키를 이용하여 현재의 암호문 및 미래의 암호문을 복호화 할 수 없는 것을 의미한다. IP기반의 Pay-TV 시스템에서의 전방향 안전성은, 임의의 가입자가 특정 채널에서 탈퇴한 이후에 과거의 그룹 키 AK를 이용하여 해당 채널의 암호화 된 컨텐츠를 복호화 할 수 없는 것을 의미한다.

후방향 안전성 (Backward secrecy) : 후방향 안전성은, 그룹에 가입한 단말이 현재의 그룹 키 및 미래의 그룹 키를 이용하여 과거의 암호문을 복호화 할 수 없는 것을 의미한다. IP기반의 Pay-TV 시스템에서의 후방향 안전성은, 임의의 가입자가 특정 채널에 가입한 이후에 현재의 그룹 키 및 미래의 그룹 키 AK를 이용하여 과거에 전송되었던 컨텐츠를 복호화 할 수 없는 것을 의미한다.

내부/외부 공격 방지 (Prevention of insider / outsider attacks) : IP기반의 Pay-TV 시스템은 외부 공격자로부터 안전하게 보호되어야 하며, 나아가서 내부 공격자에 의한 공격도 차단할 수 있어야 한다. 즉, 특정 채널에 가입하지 않은 사용자가 불법으로 미디어 컨텐츠를 시청하기 위해 그룹 키 획득을 시도할 수 있다. 또한, 임의의 가입자가 해당 채널에서 탈퇴한 이후에도 지속적으로 미디어 컨텐츠를 시청하기 위해 다른 가입자의 가입 정보 수집을 시도할 수 있다. 이러한 공격자들의 다양한 시도가 발생하더라도, CAS는 모든 가입자들이 어떠한 피해도 받지 않도록 안전하게 시스템을 보호해야 한다.

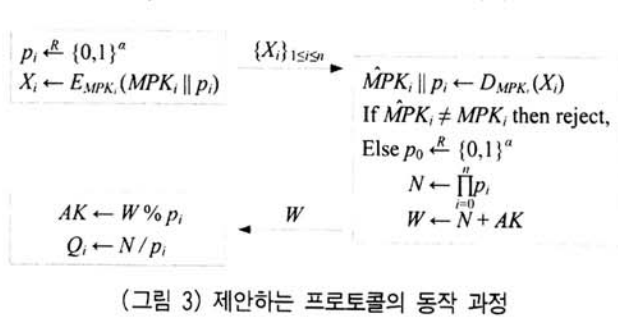
재전송 공격 방지 (Prevention of replay attacks) : 인증 혹은 키 갱신을 위해 송신된 메시지를 저장해둔 공격자가, 추후에 해당 메시지를 재전송하였을 때 인증이나 키 갱신에 성공해서는 안된다. 즉, 인증 및 키 갱신에 사용되는 메시지는 신규성 (freshness)이 보장되어야 한다.

공모 공격 방지(Prevention of collusion attacks) : 위에서 설명한 각종 위협 및 공격들을 성공시키기 위해, 둘 이상의 내부/외부 공격자들이 공모하여 공격을 시도할 수 있다. IP기반의 Pay-TV 시스템을 안전하게 보호하기 위해서는, 아무리 많은 수의 공격자들이 공모 공격을 수행하더라도 모두 차단할 수 있어야 한다.

4. 제안하는 그룹 키 분배 프로토콜

(그림 3)은 본 논문이 제안하는 그룹 키 분배 프로토콜의 동작 과정을 나타낸다.

(그림 3)을 보면, 모든 단말 C_i ($1 \le i \le n$) 는 a비트를 갖는 소수 p_i를 선택한 후, MPK_i와 p_i를 암호화한 값인 X_i를 서버에게전송한다. 단, a는 보안 파라미터 (security parameter)이며, 충분히 큰 정수이다. 암호화는 MPK_i를 키로 하여 AES (Advanced Encryption Standard)와 같은 대칭 키 기반 알고리즘으로 이루어진다. 서버는 X_i를 MPK_i로 복호화하여 MPK_i와 p_i를 얻고, 서버에 저장되어 있는 단말 C_i의 MPK_i와, X_i를 복호화하여 얻은 MPK_i를 비교하여 단말 C_i를 인증한다. 인증에 성공하면 서버는 $N = p_0 \times p_1 \times \cdots \times p_n$을 계산한다. p_i (1



(그림 3) 제안하는 프로토콜의 동작 과정

$\leq i \leq n$)는 단말 C_i가 비밀리에 서버에게 전송한 소수이고, $p_0 < \min(p_1, p_2, \cdots, p_n)$ 는 서버가 선택한 소수이다. 서버는 그룹 키로 사용할 $AK < \min(p_1, p_2, \cdots, p_n)$ 를 생성하고, $W = N + AK$를 계산하여 그룹 내의 모든 단말에게 브로드캐스트 한다. W를 수신한 단말 C_i는 $W \bmod p_i$를 계산하여 AK를 얻는다.

$$N' = \frac{N \times p_0' \times p_{n+1}}{p_0} \quad (1)$$

한편, 새로운 단말 C_{n+1}이 가입한 경우, 서버는 P_{n+1}을 해당 단말로부터 수신하고, p_0와 다른 소수 p_0'을 선택한다. 그리고 식 (1)과 같이 N'을 생성하고, $W' = N' + AK'$를 계산한 후 W'를 그룹 내의 모든 단말에게 브로드캐스트 한다.

$$N'' = \frac{N \times p_0''}{p_0 \times p_j} \quad (2)$$

단말 C_j가 탈퇴할 경우, 서버는 p_0와 다른 소수 p_0''을 선택하고 식 (2)와 같이 N''을 생성한다. 그리고 $W'' = N'' + AK''$를 계산한 후, W''를 그룹 내의 모든 단말에게 브로드캐스트 한다.

또한, W를 p_i로 나눈 몫인 $Q_i = N / p_i$를 계산하여, 서버와 단말 C_i 둘만이 공유하는 세션 키로 사용할 수 있다. 즉, 본 논문에서 제안하는 프로토콜에서는 MPK_i를 몫 Q_i로 갱신함으로써, 동일한 MPK_i의 사용 빈도를 최소화 시킬 수 있다. 이러한 MPK_i의 갱신은 필요에 따라 일부 단말에 대해 선택적으로 수행하게 된다.

제안하는 프로토콜의 경우, 가입자의 수와 관계없이 1개의 W를 계산하여 모든 단말에게 브로드캐스트한다. 그러나 CAS의 경우, 서버는 n개의 세션을 유지해야 하며, 이는 서버가 모든 단말의 IP주소를 저장해야 한다는 것을 의미한다. 또한, CAS의 경우, 각각의 메시지에 대해 각각의 헤더가 누적되어야 한다. 제안하는 프로토콜의 경우, 서버는 1개의 세션만으로 메시지의 전송이 가능하다. 또한, 멀티캐스트 세션을 이용하여 그룹 키를 전송하면, 서버는 각 단말의 IP주소를 저장할 필요가 없다.

제안하는 프로토콜은 대규모 가입자가 존재하는 단일 서버 환경에 적합한 그룹 키 분배 프로토콜이다. [10], [11]에 따르면, 대규모 그룹에서의 가입자의 수는 기껏해야 10^5명이다. 제안하는 프로토콜의 경우, 2^{17}명 ($> 10^5$명)의 가입자가 존재할 때에도 서버 측 연산은 250ms 이내에 완료된다. 따라서, 제안하는 프로토콜은 한 대의 서버가 약 10~20만명의 가입자를 관리하는 대규모 환경에 적용하기에 적합하다. 그러나, 실제 IP 기반의 pay-TV 시스템에서는 수백만명의 가입자가 존재하는 환경을 가정하기 때문에, 제안하는 프로토콜은 수백만명의 가입자를 처리할 수 있도록 확장되어야 한다.

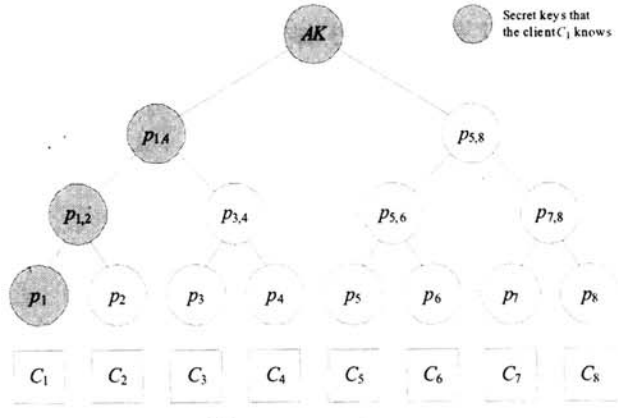
5. 제안하는 프로토콜의 확장

제안하는 프로토콜에서는, 가입자의 수가 증가함에 따라 N의 크기가 증가한다. N의 크기가 증가하면 곱셈에 소요되는 시간이 증가하고, 서버가 송신해야 하는 메시지의 크기가 증가한다. 이러한 이유로 인해서, 제안하는 프로토콜은 수백만명의 가입자가 존재하는 IP기반의 pay-TV 시스템에 적용하기 위한 확장이 필요하다.

본 장에서는 머클트리 (merkle tree)를 이용하여 제안하는 프로토콜의 성능을 향상시키고, 대규모 가입자가 존재하는 환경에 적용할 수 있도록 제안하는 프로토콜을 확장한다. 확장된 프로토콜의 경우, 그룹에 존재하는 가입자의 수가 n명이라고 할 때, 각 가입자는 $\log_2 n$개의 서로 다른 큰 소수를 가지고 있다. (그림 4)는 확장된 프로토콜의 키 구조를 나타낸다. (그림 4)에서 볼 수 있듯이, 단말 C_1은 소수 p_1, $p_{1,2}$, $p_{1,4}$, 그리고 그룹키 AK를 가지고 있다. p_1은 단말 C_1의 최초 인증 시, 단말이 생성하여 서버에게 MPK_1로 암호화 하여 전달하는 소수이고, p_0, $p_{1,2}$, $p_{1,4}$는 모두 서버가 생성한 소수이다. 즉, 트리의 리프노드 (leaf node)에 해당하는 소수들은 각 단말들이 생성하여 서버와의 최초 인증 시 비밀리에 서버에게 전달하는 소수이며, 리프노드와 루트노드 (root node)를 제외한 나머지 모든 노드는 서버가 생성하여 단말에게 전달하는 소수이다.

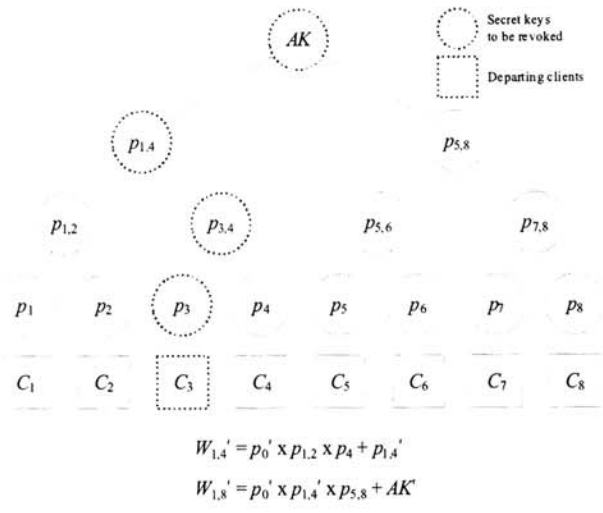
(그림 4)에서 볼 수 있듯이, 서버는 초기 시스템 셋업 과정에서 n-2개의 소수를 미리 생성하여 소수 풀 (pool)을 유지해야 한다. 펜티엄4 2.66GHz, 4GB RAM 환경에서 256비트의 소수 1개를 생성하는데 소요되는 시간을 측정한 결과, 평균 0.006초가 소요되었다. 따라서, 100만개의 소수를 생성하는데 소요되는 시간은 약 1시간 40분에 불과하며, 초기 시스템 셋업 시 1회만 수행하면 되기 때문에, 실제 서비스의 품질에는 아무런 영향을 미치지 않는다. 512비트의 소수를 생성하는 경우에도, 15시간 이내에 100만개의 소수를 생성할 수 있다. 이러한 소수 생성 작업은 시스템의 초기 셋업 시에만 수행하기 때문에, 현실에서 충분히 적용 가능하다.

한편, 임의의 가입자가 그룹에 가입하거나 탈퇴할 때, 서버는 (그림 5)와 같이 본 논문의 4장에서 설명한 기본 프로토콜을 이용하여 각 단말에게 갱신된 소수를 전달한다. (그림 5)의



$W_{1,2} = p_0 \times p_1 \times p_2 + p_{1,2}$
$W_{1,4} = p_0 \times p_{1,2} \times p_{3,4} + p_{1,4}$
$W_{1,8} = p_0 \times p_{1,4} \times p_{5,8} + AK$

(그림 4) 확장된 프로토콜의 키 구조



(그림 5) 확장된 프로토콜에서 단말 C3이 탈퇴할 경우의 키 갱신 과정의 예시

경우, 서버는 탈퇴한 단말 C_3의 소수 p_3을 폐기한다. 그리고 서버는 단말 C_1부터 단말 C_4까지 공유하고 있는 소수 $p_{1,4}$를 $p_{1,4}'$으로 갱신하여, (그림 5)에 표기되어 있는 식과 같이 $W_{1,4}'$를 계산하여 단말 C_1, C_2, C_4에게 브로드캐스트 한다. 이를 수신한 단말 C_1, C_2, C_4는, 본 논문의 4장에 설명되어 있는 기본 프로토콜을 통해 갱신된 소수를 획득할 수 있다. 그리고 서버는 그룹키 AK를 AK'으로 갱신한 후, (그림 5)에 표기되어 있는 식과 같이 $W_{1,8}'$를 계산하여 그룹에 존재하는 모든 단말에게 브로드캐스트 한다. 이를 수신한 모든 단말은, 본 논문의 4장에 설명되어 있는 기본 프로토콜을 통해 갱신된 그룹키 AK'를 획득할 수 있다.

6. 성능평가

본 장에서는 이론적 분석 및 연산 횟수 비교, 그리고 송신 메시지의 개수 비교를 통해 기존 CAS와 본 논문에서 제안하는 프로토콜의 성능을 비교하고 분석한다. 이론적 분석은 M/M/∞ 큐잉 시스템에 기반한 모델링을 통해, 기존 CAS와 본 논문에서 제안하는 프로토콜의 연산 시간에 대한 비교 및 분석 결과를 제시한다. 그리고 표를 통해 CAS, 다른 IP기반의 pay-TV 프로토콜, 그리고 본 논문에서 제안하는 확장된 프로토콜의 연산 횟수 및 송신 메시지의 개수를 비교하고, 그 성능을 평가한다.

6.1 이론적 분석

IP-TV는 멀티캐스트 기반으로 서비스를 제공한다 [12-15]. 한편, 멀티캐스트에서 서비스 요청의 도착 과정은 포아송 분포를 따르고, 평균 서비스 시간은 지수 분포를 따른다 [16-21]. 또한, 멀티캐스트 서비스를 M/M/∞ 큐잉 시스템으로 모델링 할 수 있다 [18], [21]. 따라서, 본 논문에서는 IP-TV 시스템을 M/M/∞ 큐잉 시스템으로 가정하고, 평균 도착률과 평균 서비스 시간을 각각 λ, $1/\mu$라고 정의한다. 본 논문에서는, CAS와 제안하는 프로토콜 각각에 대해, AK 분배에 소요되는 연산 시간 (computational delay)인 C_{total}을 식 (3)과 같이 구할 수 있다. 식 (3)에서 $p(n)$은 그룹 내에 존재하는 단말이 n개일 확률을 의미한다. C_{join}은 단말이 그룹에 가입할 경우에 발생하는 시간 (delay)을 의미하고, C_{leave}는 단말이 그룹으로부터 탈퇴할 경우에 발생하는 시간을 의미한다.

$$C_{total} = \sum_{n=0}^{\infty} \left(p(n) \times \left(\lambda \times C_{join} + n \times \mu \times C_{leave} \right) \right) \quad (3)$$

CAS의 경우, 그룹 내에 존재하는 단말이 n개 일 때, $(n+1)$번째 단말이 그룹에 가입하면, 서버는 AK를 갱신하기 위해 $(n+1)$번의 대칭 키 기반 암호화 (symmetric encryption)를 수행해야 한다. 또한, 그룹 내에 존재하는 단말이 n개 일 때, 임의의 단말이 그룹으로부터 탈퇴하면, 서버는 $(n-1)$번의 대칭 키 기반 암호화를 수행해야 한다. 따라서, AK분배에 소요되는 CAS의 연산 시간인 $C_{total\text{-}CAS}$는, 식 (4)과 같이 대칭 키 기반 암호화에 소요되는 시간인 C_{enc}와 $p(n)$으로 나타낼 수 있다.

$$\begin{aligned} C_{total-CAS} &= C_{enc} \times \sum_{n=0}^{\infty} \left(p(n) \times \left(\lambda \times (n+1) + n \times \mu \times (n-1) \right) \right) \\ &= C_{enc} \times \sum_{n=0}^{\infty} \left(p(n) \times \left(\mu \times n^2 + (\lambda - \mu) \times n + \lambda \right) \right) \end{aligned} \quad (4)$$

한편, 그룹 내에 존재하는 단말의 수는 비율이 λ / μ인 포아송 랜덤 변수이므로 [18,20], $p(n)$는 식 (5)와 같이 나타낼 수 있다.

$$p(n) = \left(\frac{(\lambda/\mu)^n}{n!} \right) \times e^{-(\lambda/\mu)} \quad (5)$$

그리고 (5)를 (4)에 대입하여 정리하면, (6)과 같은 식을 얻을 수 있다.

$$C_{total-CAS} = C_{enc} \times \left(\frac{\lambda \times (2 \times \lambda + \mu)}{\mu} \right) \quad (6)$$

제안하는 프로토콜의 경우, 새로운 단말이 그룹에 가입하면, 한 번의 대칭 키 기반 복호화 (symmetric decryption)와 두 번의 곱셈, 그리고 한 번의 덧셈을 수행해야 한다. 또한, 임의의 단말이 그룹으로부터 탈퇴하면, 두 번의 곱셈과 한 번의 나눗셈, 그리고 한 번의 덧셈을 수행해야 한다. 이는 식 (1), (2)와 비교하여 나눗셈이 각각 한 번씩 줄어든 횟수인데, AK의 갱신이 필요할 때 서버는 기존에 계산된 $p_1 \times p_2 \times \cdots \times p_n$ 에다가 p_0'을 곱하기만 하면 N'을 생성할 수 있기 때문에, 실제로 프로토콜을 구현할 때에는 식 (1), (2)와 달리 p_0를 나눌 필요가 없다. 제안하는 프로토콜의 연산 시간인 $C_{total\text{-}proposed}$는 식 (7)과 같이 대칭 키 기반 복호화에 소요되는 시간인 C_{dec}와 곱셈 및 나눗셈, 덧셈에 소요되는 시간인 C_{mul}, C_{div}, C_{add}로 나타낼 수 있다.

$$\begin{aligned} C_{total-proposed} &= \left(C_{dec} + 2 \times C_{mul} + C_{add} \right) \times \sum_{n=0}^{\infty} \left(p(n) \times \lambda \right) \\ &\quad + \left(C_{mul} + C_{div} + C_{add} \right) \times \sum_{n=0}^{\infty} \left(p(n) \times n \times \mu \right) \end{aligned} \quad (7)$$

〈표 1〉 대칭 키 기반 암/복호화 및 사칙연산에 소요되는 수행시간

		표기	연산 시간 (μs)
대칭 키 기반 암/복호화	AES-128 bits 암호화	C_{enc}	5.517
	AES-128 bits 복호화	C_{dec}	2.798
사칙연산	1024 bits x 1024 bits 곱셈	C_{mul}	1.018
	1024 bits / 1024 bits 나눗셈	C_{div}	1.893
	1024 bits + 1024 bits 덧셈	C_{add}	0.588

그리고 (5)를 (7)에 대입하여 정리하면, (8)과 같은 식을 얻을 수 있다.

$$C_{total-proposed} = (C_{dec} + 3 \times C_{mul} + 2 \times C_{add} + C_{div}) \times \lambda \quad (8)$$

이제, 식 (8)을 식 (6)으로 나누면, 제안하는 프로토콜과 CAS의 상대적 delay 크기를 나타내는 $C_{total-proposed}$ / $C_{total-CAS}$를 구할 수 있다. 본 논문에서는 이것을 성능비율(performance ratio)이라고 부를 것이며, η라고 표기한다. 식 (9)는 성능비율 η를 나타낸다.

$$\eta = \frac{C_{total-proposed}}{C_{total-CAS}} = \frac{C_{dec} + 3 \times C_{mul} + 2 \times C_{add} + C_{div}}{C_{enc} \times (2 \times (\lambda / \mu) + 1)} \quad (9)$$

본 논문에서는 C_{enc}, C_{dec}, C_{mul}, C_{div}, C_{add}의 실제 값을 구하기 위해, AES-128의 암호화 및 복호화 수행시간과, 1024비트 숫자들 간의 사칙연산에 소요되는 시간을 직접 수행하여 측정한 결과를 보여준다. 측정 장비는 CAS 서버와 유사하게 구성하기 위해 높은 성능을 갖는 PC를 사용하였다. 측정 장비의 CPU는 펜티엄 4 쿼드코어 2.66GHz이며, 메모리는 4GB이고, 측정 결과는 <표 1>과 같다. 본 논문에서는 이 측정 결과를 식 (9)에 대입한 후, 성능비율 η를 계산한다. (그림 6)는 λ / μ에 따른 성능비율 η의 변화를 나타낸다. 성능비율 η가 1보다 작다는 것은, 제안하는 프로토콜의 연산 시간이 CAS보다 작다는 것을 의미한다. 성능비율 η가 1보다 작아지는 λ / μ의 임계치는 약 0.31이다.

(그림 6) 도착률 × 서비스 시간에 따른 성능비율 (performance ratio)의 변화

6.2 연산 횟수 및 송신 메시지 개수 비교

본 논문에서 제안하는 확장된 프로토콜의 성능을 측정하기 위한 방법으로는, <표 2>와 같이 각각의 연산 횟수 및 송신 메시지의 개수를 CAS 및 다른 IP기반의 pay-TV 보안 프로토콜과 비교하는 방법이 있다. CAS의 경우, 임의의 단말이 그룹에 참가하거나 그룹으로부터 탈퇴할 때, 서버 측의 연산 횟수는 단말의 개수에 비례하는 반면, 단말 측의 연산 횟수는 1이다. [4,22]의 경우, 서버는 사칙연산과 해쉬 함수를 이용하여 하나의 다항식을 생성하여 단말에게 전달하고, 단말은 n번의 곱셈과 n번의 덧셈, 그리고 1번의 모듈로 연산을 수행한다. 본 논문에서 제안하는 확장된 프로토콜의 경우, 서버 측과 단말 측 모두 연산 횟수가 $\log_2 n$에 비례하며, 따라서 연산 횟수의 시간복잡도(time complexity)는 $O(\log_2 n)$ 이다. 또한, 확장된 프로토콜에서 수행하는 연산은 간단한 사칙연산으로서, CAS에서 수행하는 대칭 키 기반 암호화/복호화 보다 수행 속도가 빠르다.

한편, CAS에서 AK를 갱신할 때, 서버는 AK를 MPK_i ($1 \le i \le n$) 로 각각 암호화 하고, n개의 단말에게 각각 유니캐스팅 방식으로 암호화된 AK를 전송한다. [4], [22]의 경우, 서버는 하나의 다항식을 생성하여 단말에게 전달한다. 반면, 본 논문에서 제안하는 확장된 프로토콜의 경우, 서버는 W를 $\log_2 n$개 계산하고, 그룹 내의 모든 단말에게 각 W를 브로드캐스팅 한다. 각각의 W는 단말의 수와 관계없이 고정된 크기를 갖는다.

7. 프로토콜의 보안성 및 안전성 분석

본 장에서는 제안하는 프로토콜의 보안성 및 안전성을 분석한다. 제안하는 프로토콜은 3장에서 정의한 보안 요구사항을 모두 만족하며, 추가적으로 시그널링 채널의 안전성을 향상시키는 기능을 제공한다.

7.1 전방향 안전성 (Forward secrecy)

전방향 안전성은, 그룹에 가입한 단말이 과거의 그룹 키인 AK를이용하여 현재의 암호문을 복호화 할 수 없는 것을 의미한다. 제안하는 프로토콜의 경우, 그룹으로부터 탈퇴한 단말이 과거의 그룹 키인 AK와 N를 알고 있더라도, 더 이상 새로운 그룹 키인 AK''를 획득할 수 없다. 따라서, 제안하는 프로토콜은 전방향 안전성을 제공한다.

식 (2)에서 볼 수 있듯이, 단말 C_j가 그룹으로부터 탈퇴하였을 때, 서버는 N과 AK를 각각 N''과 AK''으로 갱신한다. N''에는 탈퇴한 단말 C_j의 비밀 값인 p_j가 인수로 포함되어 있지 않기 때문에, 단말 C_j는 W''으로부터 N''과 AK''을 찾아낼 수 없다. 또한, 단말 C_j가 그룹으로부터 탈퇴하였을 때, 서버는 N의 인수인 p_0를 p_0''으로 갱신한다. 만약, 서버가 N의 인수인 p_0를 p_0''으로 갱신하지 않는다면, 단말 C_j는 N / p_j를 계산함으로써 N''을 추측할 수 있을 것이다. 제안하는 프로토콜에서는, 서버만이 알고 있는 p_0''으로 p_0를 갱신하기 때문에, 탈퇴한 단말 C_j는 W로부터 N''과 AK''을 찾아낼 수 없다.

7.2 후방향 안전성 (Backward secrecy)

후방향 안전성은, 그룹에 가입한 단말이 현재의 그룹 키인

〈표 2〉 연산 횟수 및 송신 메시지 개수 비교

			연산 횟수		송신 메시지 개수		
			대칭 키 기반 암호화 및 복호화	사칙연산	총 메시지	유니캐스트	브로드캐스트
CAS	가입 시	서버	n+1	0	n+1	n+1	0
		가입한 단말	1	0			
		나머지 단말	1	0			
	탈퇴 시	서버	n-1	0	n-1	n-1	0
		나머지 단말	1	0			
		탈퇴한 단말	0				
[4], [22]	가입 시	서버	0	2n+2	1	0	1
		가입한 단말	0	2n+3			
		나머지 단말	0	2n+3			
	탈퇴 시	서버	0	2n-2	1	0	1
		나머지 단말	0	2n-1			
		탈퇴한 단말	0				
제안하는 프로토콜의 확장	가입 시	서버	1	3 x $\log_2 n$	$\log_2 n$	0	$\log_2 n$
		가입한 단말	1	$\log_2 n$			
		나머지 단말	0	1~$\log_2 n$			
	탈퇴 시	서버	0	3 x $\log_2 n$	$\log_2 n$	0	$\log_2 n$
		나머지 단말	0	1~$\log_2 n$			
		탈퇴한 단말	0				

AK'를 이용하여 과거의 암호문을 복호화 할 수 없는 것을 의미한다. 즉, 단말 C_{n+1}이 그룹에 가입하기 이전에 암호문을 수집하고 있다가, 그룹에 가입한 이후에 AK를 획득하여 수집했던 암호문을 복호화 한다면, 접근제어가 올바르게 제공되었다고 볼 수 없다.

식 (1)에서 볼 수 있듯이, 단말 C_{n+1}이 그룹에 가입하였을 때, 서버는 N과 AK를 각각 N'과 AK'으로 갱신한다. N에는 가입한 단말 C_{n+1}의 비밀 값인 p_{n+1}이 인수로 포함되어 있지 않기 때문에, 단말 C_{n+1}은 W로부터 N과 AK를 찾아낼 수 없다. 또한, 단말 C_{n+1}이 그룹에 가입하였을 때, 서버는 N의인수인 p_0를 p_0'으로 갱신한다. 만약, 서버가 N의 인수인 p_0를 p_0'으로 갱신하지 않는다면, 단말 C_{n+1}은 N/p_{n+1}을 계산함으로써, N을 추측할 수 있을 것이다. 제안하는 프로토콜에서는, 서버만이 알고 있는 p_0'으로 p_0를 갱신하기 때문에, 단말 C_{n+1}은 W'으로부터 N과 AK를 찾아낼 수 없다.

7.3 그룹 키 및 비밀 정보의 노출 방지 (Prevention leakages of the group key AK and the secret pi)

제안하는 프로토콜은, 그룹 키 AK 및 단말 C_i의 비밀 값 p_i가 그룹 외부의 공격자에게 노출되는 것을 방지할 수 있다. 뿐만 아니라, 그룹 내부의 단말 C_i가 또 다른 그룹 내부의 단말 C_j의 비밀 값인 p_j를 획득하는 것을 방지할 수 있다. 각각의 경우에 대한 설명은 다음과 같다.

(1) 그룹 외부의 공격자로부터 그룹 키 AK 및 비밀 정보 pi의 노출 방지

서버는 단말에게 AK를 전달하기 위해, $W = N + AK$를 계산하여 그룹 내의 모든 단말에게 전달한다. 이 때, 그룹 외부의 공격자가 W를 수신하더라도, AK보다 큰 N의 인수를 모르는 상태에서 $W = N + AK$로부터AK를 찾아내는 방법은, 전수조사 외에는 존재하지 않는다. p_0를 제외한 p_i ($1 \le i \le n$)는, 단말에 의해 암호화 되어 서버에게 전송되고, p_0는 서버만이 알고 있는 비밀 값이기 때문에, 공격자는 AK보다 큰 N의 인수를 찾을 수 없다.

한편, 전수조사는 공격자가 AK에 관해 아무런 정보를 가지고 있지 않은 상태에서 AK를 찾아내기 위해 AK가 될 수 있는 모든 수를 사용하여 암호문의 복호화를 성공할 때까지 시도하는 방법이다. 만약 AK가 k비트라면, 공격자는 최대 2^k만큼 복호화를 반복해야 한다. <표 1>에서 볼 수 있듯이, 복호화 1회에 소요되는 시간은 약 2.798μs 이기 때문에, AK가 128비트일 경우, 공격자는 전수조사를 위해 최대 3×10^{25}년의 시간이 필요하다. 제안하는 프로토콜에서는, 맴버쉽의 변화가 발생할 때마다 AK가 갱신되기 때문에, 전수조사로부터 AK를 찾아내는 것은 불가능하다. 만약, 공격자가 AK를 찾아내더라도, 이후에 갱신된 AK를 다시 찾기 위해서는 전수조사를 다시 반복해야 한다.

(2) 그룹 내부의 공격자로부터 비밀 정보 pj의 노출 방지

그룹 내부의 단말 C_i가 또 다른 단말 C_j의 비밀 값인 p_j를 획득하게 된다면, 단말 C_i는 그룹으로부터 탈퇴한 이후에도 p_j를 사용하여 서비스를 제공받을 수 있게 된다. 이러한 불법적인 서비스 수신은, 단말 C_j가 그룹으로부터 탈퇴하거나, 혹은 단말 C_j가 비밀 값 p_j를 갱신하기 전까지 가능하다. 따라서, 시스템을 보호하기 위해서는 단말 C_i가 또 다른 단말 C_j의 비밀 값인 p_j를 획득하는 것을 방지할 수 있어야 한다.

단말 C_i가 또 다른 단말 C_j의 비밀 값인 p_j를 획득하기 위

해서는, 그룹 맴버쉽의변화가 발생하기 전까지 AK보다 큰 N의 인수를 찾아야 하고, 이를 위해서는 인수분해를 수행해야 한다. 그러나, p_0, p_1, ..., p_n은 임의의 큰 소수이며, 이러한 큰 소수들의 곱으로 이루어진 합성수 N을 인수분해 하는 것은 소인수 분해 문제에 의해 오랜 시간을 필요로 한다. 따라서, 단말 C_i가 또 다른 단말 C_j의 비밀 값 p_j를 찾아내는 것은 어렵다.

한편, 제안하는 프로토콜에서 사용되는 소수 p_i는, 일반적인 RSA의 응용에서 사용되는 소수보다 크기가 작다. 왜냐하면, 동일 채널에 대해 짧게는 1개월, 길어도 1년 단위로 재계약을 수행하는 방송 서비스와달리, 일반적으로 RSA의 경우 한번 키를 생성하면 반영구적으로 인수분해가 되지 않는 것을 가정하기 때문이다. 또한, 지난 2005년 11월에 30대의 컴퓨터로 이루어진 그리드 컴퓨팅 (grid computing)으로 5개월 이상 인수분해를 수행한 결과, 두 개의 큰 소수로 이루어진 640비트 합성수의 인수분해를 성공하였다는 연구 결과가 있지만 [23], 이러한 그리드 컴퓨팅의 구성 및 인수분해 수행에 소요되는 비용은 pay-TV 채널 1개의 방송 내용을 획득하는 비용보다 훨씬 크다. 이러한 이유로 인해서, 그리드 컴퓨팅을 이용한 인수분해 공격은 제안하는 프로토콜에 대해서는 무의미하다. 뿐만 아니라, 공격에 성공하더라도 방송 서비스의 경우 길어야 1년 이내에 재계약이 이루어지고 키가 갱신되기때문에, 공격자는 공격에 성공한 이후에도 거의 이득을 볼 수 없다. 따라서, 제안하는 프로토콜의 경우, RSA에서 사용되는 소수보다 크기가 작은 소수를 사용하더라도 충분히 높은 안전성을 유지할 수 있다.

(3) 공모 공격에 의한 비밀 정보 pj의 노출 방지

둘 이상의 단말이 공모 공격을 시도하여도, 제안하는 프로토콜에서는 어떠한 정보도 노출되지 않는다. 그룹 내에 n개의 단말이 존재할 때, N은 총 n+1개의 소수들의 곱으로 구성되어 있다. 이 때, n-1개의 단말이 서로 비밀 정보 p_i를 공유하여 공모 공격을 시도하여도, N에는 공격자들이 모르는 2개의 소수의 곱이 존재하기 때문에, 이를 소인수분해 하는 것은 N을 소인수분해 하는 것과 동일한 보안 강도를 갖는다. 이 2개의 소수 중 1개의 소수 (p_0)는 임의의 단말이 탈퇴하는 순간 서버가 갱신하는 값이기 때문에, 공격자들이 공모 공격을 통해 얻을 수 있는 이득은 전혀 없다. 본 논문에서 제안하는 확장된 프로토콜 또한 동일한 원리에 의해 공모 공격에 대해서도 안전하다.

7.4 재전송 공격 방지 (Resilience to replay attacks)

일반적인 인증 프로토콜이나 키 분배 프로토콜은, 재전송 공격을 방지하기 위해 타임스탬프나 넌스 등을 사용한다. 즉, 단말은 인증할 때마다 각각 다른 타임스탬프나 넌스를 암호화하여 서버에게 전송함으로써, 재전송 공격을 방지할 수 있다. 그러나, 타임스탬프를 사용할 경우, 서버와 단말은 둘 사이의 시간 동기화를 맞추어야 하는데, 인터넷 상에서는 통신 지연 (communication delay)이 불규칙하게 발생하기 때문에, 정확한 시간 동기화를 맞추는 것은 어렵다. 또한, 공격자가 타임스탬프 메시지를 위조하여 보낼 수 있기 때문에, 이에 대한 메시지 무결성도 제공해야 하므로, 타임스탬프를 이용한 재전송 공격 방지는 오버헤드가 크다. 한편, 넌스를 사용할 경우, 단지 인증을 위한 목적으로 넌스를 전송해야 하기 때문에, 불필요한 통신 오버헤드를 유발한다.

제안하는 프로토콜에서는, 추가적인 오버헤드 없이 인증 과정의 재전송 공격을 효과적으로 방지할 수 있다. 만약, 공격자가 단말 C_i로 위장하기 위해 C_i가 전송했던 X_i ((그림 3) 참조)를 서버에게 재전송하게 되면, 서버는 자신이 저장하고 있는 p_i와, 수신한 X_i로부터 추출한 p_i를 대조하여 동일 여부를 확인한다. 만약 두 p_i가 동일하다면 이는 재전송 공격으로 간주되어 인증에 실패한다. 반면, 합법적인 단말 C_i는 그룹에 가입할 때마다 비밀 값인 p_i를 갱신하게 되므로, 인증에 성공할 수 있다.

한편, 단말 C_i가 그룹으로부터 탈퇴하면, 식 (2)와 같이 N을 갱신해야 하므로, 서버는 C_i의 비밀 값인 p_i를 저장하고 있어야 한다. 따라서, 서버가 p_i를 저장하는 것은, 재전송 공격을 막기 위해 추가적으로 발생하는 오버헤드가 아니다.

7.5 시그널링 채널의 안전성 향상 (Security improvement of a signaling channel)

CAS에서는 시그널링 채널을 보호하기 위해 마스터 키 MPK_i를 사용한다. 즉, 그룹 키를 전달하거나, 세션 정보를 송수신할 때, 서버와 단말 C_i는 둘만이 공유하고 있는 MPK_i를 대칭 키 (symmetric key)로 사용하여 메시지를 안전하게 보호한다. 그러나, 동일한 MPK_i로 암호화한 암호문이 빈번하게 노출될 경우, 이는 시스템에 대한 각종 위협의 원인이 된다.

제안하는 프로토콜에서는, 그룹 키 AK를 분배하고 획득하는 과정에서 마스터 키 MPK_i를 쉽게 갱신할 수 있다. 즉, 단말 C_i는 W % p_i 연산을 통해 AK를 획득할 수 있고, N / p_i 연산을 통해 새로운 마스터 키 Q_i를 획득할 수 있다. p_i는 단말 C_i와 서버 둘만이 공유하고 있는 비밀 값이기 때문에, Q_i = N / p_i도 단말 C_i와 서버 둘만이 공유하게 된다. 또한, N은 그룹 맴버쉽의 변화에 따라 지속적으로 변화하기 때문에, Q_i도 지속적으로 갱신된다. 결과적으로, 서버는 W 하나만 전송함으로써, 모든 단말 C_i ($1 \le i \le n$) 에게 AK 뿐 아니라 Q_i도 안전하게 전달할 수 있다. 물론, 이를 위해서는 추가적인 연산이 필요하며, 따라서 매번 Q_i를 새로운 MPK_i로 갱신하지 않고, MPK_i를 자주 사용하는 단말에 한해 선택적으로 Q_i를 새로운 MPK_i로 교체하여 사용할 수 있다.

8. 결 론

본 논문은 기존 CAS와 그 문제점을 분석한 결과를 보여준다. CAS는 미디어 컨텐츠의 보호를 위해 그룹 키의 재분배 기능을 제공한다. 그러나CAS의 경우, 그룹 맴버쉽의 변화가 발생할 때마다 서버는 그룹 내에 존재하는 단말의 수 n만큼 대칭 키 기반 암호화를 수행해야 한다. 이는 서버 측에 심각한

오버헤드를 유발하며, CAS를 사용하는 IP-TV 서비스의 품질을 저하시킨다. 반면, 제안하는 프로토콜의 경우, 그룹 내에 존재하는 단말의 수와 상관없이 서버는 하나의 값을 계산하여 그룹 내의 모든 단말에게 브로드캐스트 한다. 이 때 계산되는 값은 간단한 사칙연산 만을 사용하기 때문에, 효율적인 그룹 키의 재분배가 가능하다. 특히, 본 논문에서 제안하는 확장된 프로토콜의 경우, 수행하는 사칙연산의 횟수가 $\log_2 n$에 비례하기 때문에, 확장된 프로토콜은 가입자의 수가 수백만명인 그룹에서도 충분히 적용 가능하다. 또한, 제안하는 프로토콜과 확장된 프로토콜은, 본 논문에서 정의한 IP기반의 Pay-TV 시스템의 보안 요구사항을 모두 만족한다. 뿐만 아니라, 단말 인증 등에 사용되는 마스터 키의 반복된 사용으로 인해, 각종 공격에 노출될 수 있는 CAS와 달리, 제안하는 프로토콜에서는 마스터 키를 빈번하게 갱신할 수 있다. 마스터 키는 그룹 키를 계산하는 과정에서 쉽게 획득할 수 있는 값이므로, 마스터 키의 갱신을 위한 추가적인 오버헤드는 거의 없다. 결과적으로, 제안하는 프로토콜은 IP기반의 Pay-TV 시스템의 보안 요구사항을 만족하는 동시에 CAS의 그룹 키 분배 문제를 해결한다.

향후에는, Mobile-TV와 같이 성능이 제한된 환경에서도, 단말의 배터리 및 저장공간 등의 자원 소모를 최소화 할 수 있는 프로토콜을 연구할 수 있을 것이다.

참 고 문 헌

[1] H. M. Sun, C. M. Chen, and C. Z. Shieh, "Flexible-Pay-Per-Channel: A New Model for Content Access Control in Pay-TV Broadcasting Systems," IEEE Transactions on Multimedia, Vol.10, No.6, pp.1109-1120, Oct., 2008.

[2] T. Yoshimura, "Conditional Access System for Digital Broadcasting in Japan," Proceedings of the IEEE, Vol.94, No.1, pp.318-322, Jan., 2006.

[3] Y. Huang, S. Shieh, F. Ho, and J. Wang, "Efficient Key Distribution Schemes for Secure Media Delivery in Pay-TV Systems," IEEE Transactions on Multimedia, Vol.6, No.5, pp.760-769, Oct., 2004.

[4] B. Liu, W. Zhang, and T. Jiang, "A Scalable Key Distribution Scheme for Conditional Access System in Digital Pay-TV System," IEEE Transactions on Consumer Electronics, Vol.50, No.2, pp.632-637, May, 2004.

[5] T. Jiang, S. Zheng, and B. Liu, "Key Distribution Based on Hierarchical Access Control for Conditional Access System in DTV Broadcast," IEEE Transactions on Consumer Electronics, Vol.50, No.1, pp.225-230, Feb., 2004.

[6] A. T. Sherman and D. A. McGrew, "Key Establishment in Large Dynamic Groups Using One-Way Function Trees," IEEE Transactions on Software Engineering, Vol.29, No.5, pp.444-458, May, 2003.

[7] B. E. Jung, "An Efficient Group Key Agreement Protocol," IEEE Communications Letters, Vol.10, No.2, pp.106-107, Feb., 2006.

[8] S. M. Lee and D. H. Lee, "Analysis of an Efficient Group Key Agreement Protocol," IEEE Communications Letters, Vol.10, No.8, pp.638-639, Aug., 2006.

[9] L. R. Dondeti, S. Mukherjee, and A. Samal, "Scalable Secure One-to-many Group Communication using Dual Encryption," Computer Communications, Vol.23, No.17, pp.1681-1701, Nov., 2000.

[10] A. Perrig, D. Song, and D. Tygar, "ELK, a new protocol for efficient large-group key distribution," Proc. IEEE Symp. on Security and Privacy, California, USA, pp.247-262, May, 2001.

[11] A. Ganesh, A. M. Kermarrec, and L. Massoulie, "Peer-to-Peer Membership Management for Gossip-based Protocols," IEEE Transactions on Computer, Vol.52, pp.139-149, Feb., 2003.

[12] Y. Xiao, X. Du, J. Zhang, F. Hu, and S. Guizani, "Internet Protocol Television (IPTV): The Killer Application for the Next-Generation Internet," IEEE Communications Magazine, Vol.45, No.11, pp.126-134, Nov., 2007.

[13] C. Luo, J. Sun, and H. Xiong, "Monitoring and Troubleshooting in Operational IP-TV System," IEEE Transactions on Broadcasting, Vol.53, No.3, pp.711-718, Sep., 2007.

[14] J. She, F. Hou, P. H. Ho, and L. L. Xie, "IPTV over WiMAX: Key Success Factors, Challenges, and Solutions," IEEE Communications Magazine, Vol.45, No.8, pp.87-93, Aug., 2007.

[15] A. Ganjam and H. Zhang, "Internet Multicast Video Delivery," Proceedings of the IEEE, Vol.93, No.1, pp.159-170, Jan., 2005.

[16] Y. L. Sun and K. J. R. Liu, "Analysis and Protection of Dynamic Membership Information for Group Key Distribution Schemes," IEEE Transactions on Information Forensics and Security, Vol.2, No.2, pp.213-226, Jun., 2007.

[17] Y. Li and J. Z. Wang, "Cost analysis and optimization for IP multicast group management," Computer Communications, Vol.30, No.8, pp.1721-1730, Jun., 2007.

[18] R. Gau, "Performance Analysis of Multicast Key Backbone for Secure Group Communications," IEEE Communications Letters, Vol.10, No.7, pp.555-557, Jul., 2006.

[19] Z. Zhang and Y. Yang, "Performance Analysis of k-Fold Multicast Networks," IEEE Transactions on Communications, Vol.53, No.2, pp.308-314, Feb., 2005.

[20] Y. Sun, W. Trappe, and K. J. R. Liu, "A Scalable Multicast Key Management Scheme for Heterogeneous Wireless Networks," IEEE/ACM Transactions on Networking, Vol.12, No.4, pp.653-666, Aug., 2004.

[21] S. Alouf, E. Altman, C. Barakat, and P. Nain, "Optimal

Estimation of Multicast Membership," IEEE Transactions on Signal Processing, Vol.51, No.8, pp.2165-2176, Aug., 2003.

[22] K. P. Wu, S. J. Ruan, F. Lai, and C. K. Tseng, "On Key Distribution in Secure Multicasting," Proc. 25th Annual IEEE Conf. on Local Computer Networks, Florida, USA, pp.208-212, Nov., 2000.

[23] RSA Laboratories, available at http://www.rsa.com/rsalabs/node.asp?id=2964

김 정 윤

e-mail : steal83@ece.skku.ac.kr

2004년~2005년 안철수연구소 인턴사원 근무

2006년 성균관대학교 컴퓨터공학전공(학사)

2008년 성균관대학교 전자전기컴퓨터공학과 (석사)

2008년~현 재 성균관대학교 휴대폰학과 박사과정

관심분야 : 차량 간 통신 보안, Pay-TV 보안, 무선통신망 보안

최 형 기

e-mail : hkchoi@ece.skku.ac.kr

1992년 성균관대학교 전자공학과(학사)

1996년 Polytechnic University in Brooklyn, NY(석사)

2001년 Georgia Institute of Technology in Atlanta, GA(박사)

2001년~2004년 Lancope 근무

2004년~현 재 성균관대학교 정보통신공학부 조교수

관심분야 : 네트워크보안, Traffic characterization and modeling