情報保護學會論文誌
第11券 第6號, 2001. 12

통합 멀티캐스트 서비스 지원을 위한 키 관리 구조 제안

박 희 운*, 이 임 영**

A Proposal of Key Management Structure for Providing a Integrated Multicast Service

Hee-Un Park*, Im-Yeong Lee**

요 약

그룹 기반 통신 응용 서비스의 요구가 증가함에 따라 유·무선 네트워크상에서 사용 가능한 멀티캐스트 기반 구조에 대한 연구가 활발히 진행되고 있다. 하지만 멀티캐스트 구조에 대한 안전성과 효율성 및 확장성 부분에 대한 해결책은 아직 미비한 상태이다. 본 연구에서는 유·무선 통합 멀티캐스트 서비스 지원을 위해, PKI(Public Key Infrastructure), IPsec, 도메인 Subgroup 및 구조적 이원화 기법 등에 기초하여 확장성을 제공하는 안전한 멀티캐스트 키 관리 구조를 제안한다. 또한 멀티캐스트 키 관리 서비스를 위하여, 수신자 지정 그룹 서명 방식 및 키 갱신 기법을 새로이 제안함으로서 안전성과 신뢰성을 보장하고 있다. 이를 근거로 새로이 제안된 방식과 기존의 방식들을 안전성, 효율성 및 확장성 부분에서 비교 분석함으로서 그 효용성을 검증한다.

ABSTRACT

Through the increment of requirement for group oriented communication services, the multicast infrastructure based on a wire and wireless network has become a widely discussed researching topic. However the research of the security properties that safety, efficiency and scaleability in a multicast structure, has not been enough. In this study, we propose a scalable secure multicast key management structure based on PKI(Public Key Infrastructure), IPSec, domain subgroup and structural two mode scheme to provide a integrated multicast service. Also we discuss and propose the digital nominative group signature and key refreshing method for satisfying the security and trusty on the network. At the base of this work, we certify to the usability of new proposed scheme from comparing it with conventional schemes in the part of safety, efficiency and scaleability.

keyword : *Wire-Wireless Multicast, Scaleability, Safety, Efficiency, Key Management*

Ⅰ. 서 론

정보 사회의 발전을 통해 사용자들은 단순한 통신에서 벗어나 다자간 통신 회의 및 의료 분야에서 원격 진단 및 상담 등 다양한 서비스를 요구하고 있다. 이들 서비스는 컴퓨터 및 무선기기의 보급 확산과 공용 네트워크의 발전을 통해 더욱 가속화되고 있다. 그러나 그룹에 기초한 특정 서비스를 지원하기 위해서는 기존의 일대일 통신 방식으로는 제약 사항이 생길 수 밖에 없다. 이를 해결하기 위하여 현재 각광을 받고

* 순천향대학교 정보기술공학부(phu24@hotmail.com)
** 순천향대학교 정보기술공학부(imylee@sch.ac.kr)

있는 방식 중의 하나가 멀티캐스트 기법이다[1~7].

멀티캐스트란 그룹에 참가한 멤버들 사이에서 한 송신자로부터 다수의 참여자에게 메시지 전송이 가능한 방법을 의미한다. 이때 그룹 멤버가 해당 그룹을떠나면 더 이상 정보를 수신할 수 없게 된다. 동시에 멀티캐스트 기법은 기존의 통신 방식에 대해 그룹에 참가한 송신자의 전송 오버헤드, 네트워크 대역폭 및 지연을 감소시키는 장점을 제공한다.

그러나 멀티캐스트 서비스는 인터넷과 같은 공개된 네트워크를 이용하므로 많은 부분에서 안전성과 관련하여 취약성에 노출되어 있다. 특히 불법적인 제 3자의 도청이나 전송 정보의 위조 그리고, 불법적 사용은 그 대표적인 예가 된다. 동시에 이동 통신 분야의 빠른 성장으로 많은 사람들이 이동 통신 서비스를 통해 그 편리성과 유용성을 인지하고 있다. 이러한 이동 통신 발전의 이면에는 단순한 의사 교환의 범위를 넘어서 동영상 그리고 이들을 포함해 그룹을 대상으로 하는 인터넷 서비스까지 포괄적으로 확대되고 있다. 따라서 유선 환경상의 고정 IP에만 그 적용 범위를 두고 있었던 기존의 멀티캐스트 서비스는, 이동 통신 환경상의 Mobile IP를 포함하는 통합된 환경으로 확장되어야만 한다.

그러나 무선 이동 통신상에서 제공되어질 이와 같은 그룹 서비스들은 많은 문제점에 노출될 수 있다. 이동 통신에서의 신호 교환은 무선 채널을 통해 대기 중에서 수행되므로, 도청자나 그 밖의 신뢰되지 못한 요소들로부터 위조나 불법적 변경 등과 같은 위협들에 대해서는 취약성을 지니고 있다. 동시에 무선 단말기의 분실 등은 그룹 소속원들의 공유 정보의 노출뿐 아니라 불법적 시스템 사용 등을 유발시키므로 특히 주의해야 할 사항이다[8].

이러한 불법 행위로부터 안전성과 신뢰성을 확보하기 위한 방안으로 암호 시스템이 이용되고 있다. 그러나 키의 노출 여부는 전송 정보의 안전성과 직결되므로 매우 중요시 다뤄져야 한다. 동시에 회원의 가입 및 탈퇴를 위하여 확장성이 보장되어야 한다. 그 외에도 무선 환경에 적합한 Mobile IP 기반 서비스를 위해서는 과금 관련 지불 인증을 받아야 하며, 개인 Privacy를 보호하기 위해 위치 익명성을 제공받아야 한다.

현재 멀티캐스트 그룹 키 관리 분야와 관련하여, 그 중요성에도 불구하고 해결책들은 미흡한 상황이다. 따라서 본 연구는 통합된 통신 환경 상에서 광범위하게 적용될 멀티캐스트 서비스의 신뢰성 및 확장성을 제공하기 위하여 요구되는 사항들을 고려한다. 동시에 PKI(Public Key Infrastructure), 계층적 도메인 Subgroup 및 구조적 이원화 기법 등을 이용하여 확장성을 제공하는 안전한 멀티캐스트 키 관리 구조를 제안한다. 또한 멀티캐스트 키 관리 서비스를 위하여, 수신자 지정 그룹 서명 방식 및 키 갱신 기법을 새로이 제안함으로서 안전성과 신뢰성을 보장하고 있다. 이러한 구조적 특성들과 제시된 요구 사항들을 근거로 안전성, 효율성 및 확장성 부분에서 제안 방식과 기존 방식들을 비교 분석함으로서 그 효용성을 검증할 것이다.

II. 통합 멀티캐스트 키 관리 요구사항

멀티캐스트 구조는 그 특성상 다자간 통신을 전제로 하고 있기 때문에 여러 위협 요소에 노출되어 있다. 특히 안전한 통신을 위해 사용되는 키의 관리는 매우 중요한 요소로서, 다음은 이를 위해 요구되는 사항을 기술한 것이다.

2.1 일반적 요구 사항

멀티캐스트 서비스를 수행함에 있어, 메시지 송·수신과 관련하여 정당한 멤버 및 메시지 인증이 필요하다. 그밖에도 멤버쉽을 보호하기 위한 다양한 요소들이 필요한데, 다음은 이들과 관련된 요구 사항들을 기술한 것이다.

- 무결성 : 멀티캐스트 정보는 전송 도중에 불법적인 제 3자로부터 위조 및 변경되어서는 안된다.
- 인증성 : 송·수신된 멀티캐스트 정보가 불법적인 변조 없이 정당한 참여자들로부터 생성 및 수신되었음을 확인할 수 있어야 한다.
- 접근 제어 : 정당한 그룹의 소속원만이 멀티캐스트 정보에 접근할 수 있다.
- 부인 봉쇄 : 멀티캐스트 서비스 참여자 사이에서 전송 및 수신 사실을 부인할지라도 당사자 및 제 3자가 이를 확인 할 수 있어야 한다.
- 비밀성 : 불법적인 제 3자로부터 멀티캐스트 정보는 보호되어야 한다. 이를 위해 다양한 암호 기법이 적용될 수 있다.

2.2 동적 그룹 변동에 따른 요구 사항

멀티캐스트 서비스는 그룹에 가입한 멤버를 대상

으로 하기 때문에, 멤버들만이 키를 획득할 수 있어야 한다. 동시에 그룹에서 탈퇴하는 등의 멤버쉽 변동에 대해 능동적으로 대처할 수 있어야 한다. 다음은 동적 그룹 변동에 따른 요구 사항들을 기술한 것이다.

- 공정성 : 멀티캐스트에서 사용되는 키들은 허가된 그룹 참여자에게만 안전하게 전송되어야 한다. 또한 가입 및 탈퇴에 대비해 키 갱신 프로토콜은 필수적이다. 이를 위해 서버의 독단이나 제3자와의 불법적 결탁을 방어하기 위한 수단이 확보되어야 한다.
- 확장성 : 멀티캐스트 서비스는 다자간 통신을 전제로 하므로 그룹 참여자의 변동이 생기게된다. 따라서 참여자 변동에 따른 동적인 키 관리 기법이 필요하다.

2.3 무선 및 원격 호스트 서비스를 위한 요구 사항

무선 및 원격 호스트 서비스는 그룹 가입자의 이동성을 전제로 하고 있다. 따라서, 그룹 가입자의 이동성을 보장함과 동시에 위치 불추적성을 만족해야 한다. 다음은 이들과 관련된 요구 사항들을 기술한 것이다.

- 익명성 : 멀티캐스트 멤버의 위치는 허가된 실체 외에는 확인할 수 없어야 한다.
- Hand-Off 허용 : Mobile IP상에서 가입자는 이동성을 가지고 있다. 이때 가입자가 새로운 셀(Cell) 범위로 진입할 경우, 새로운 원격 호스트와 새로운 세션키를 통해 메시지를 송·수신해야 한다. 이를 위한 인증은 필수적이며 사용자 및 메시지에 대한 안전성 또한 확보되어야 하는데, 이러한 일련의 과정을 Hand-Off 과정이라 한다. 이동성을 갖는 사용자에 있어 Hand-Off 허용 여부는 중요한 의미를 갖는다.

2.4 무선 멀티캐스트 키 분배 및 갱신관련 요구 사항

무선 멀티캐스트 서비스는 단말기의 특성상 기존의 PC와 같은 계산 능력을 가지지 못하므로, 효율성은 무엇보다 중요한 요구 사항이다. 다음은 무선 멀티캐스트 키 분배 및 갱신과 관련하여 요구되는 사항들을 기술한 것이다.

- 통신 병목 현상 : 무선 단말기의 특성상 효율성 유지를 위해 통신 메시지의 길이는 작아야 하며, 통신 횟수는 최소가 되어야 한다.
- 키 갱신 준비 단계 Overhead : 멀티캐스트 키의 분실 또는 멤버의 탈퇴에 따른 키 갱신은 별도의 준비 단계로 인한 Overhead를 최소화시켜야 한다.
- 그룹 멤버간 공모 방지 : 그룹에 속한 멤버라 할지라도 향후 사용될 멀티캐스트 키를 알 수 있어서는 안된다.
- 2명 이상의 동시 갱신 허용 : 2명 이상의 멤버가 자신들의 단말기를 분실하거나 탈퇴할지라도, 키 갱신 횟수는 최소화되어야 한다.

Ⅲ. 통합 멀티캐스트 기반 기술

본 장에서는 유·무선 통합 멀티캐스팅을 위해 필요한 기반 기술들을 분석 및 제안한다. 특히 무선 통신 멀티캐스팅 기반에서 중요하게 취급되는 인증 및 무결성을 위하여 수신자 지정 그룹 서명 방식을 제시함과 동시에 특정 그룹을 대상으로 적용 가능한 이동 통신 그룹 키 갱신 방식을 제안한다.

3.1 수신자 지정 그룹 서명 방식

본 방식은 1999년에 제시된 방식으로서, Mobile IP 상에서 멤버들의 인증 및 익명성을 제공하기 위해 사용 가능한 서명 방식이다[9~11].

3.1.1 시스템 계수

다음은 본 방식에서 사용되는 시스템 계수를 설명한 것이다.

- p, q : 큰 소수 $p \geq 512bit$, $q \geq 160bit\,(q|p-1)$
- g : 원시 생성자
- k_1, k_2 : 랜덤 수 $\{k_1, k_2\} \in {}_RZ_P$
- $D = Y_Z^{k_2} \bmod p$
- $e = g^{k_2 - k_1} \bmod p$
- H : 160비트 출력을 내는 안전한 일방향 해쉬 함수
- $R = H(g^{k_1} \bmod p \| M \| e \| D)$
- K_{SU}, K_{PG} : 서명자의 소속 서명 및 확인용 공개키 리스트
- X_Z, Y_Z 수신자 Z의 비밀키와 공개키
- M, S : 서명용 메시지 및 서명

3.1.2 소속 등록 및 키 분배 단계

소속의 등록은 TC(Trusted Center)가 관할하며, 소속에 등록 및 키를 분배받기 위해서는 다음과 같은 일련의 과정을 거친다.

1) 서명자는 자신의 신상 정보(서명자 이름, ID, 소속, 기타)를 TC에게 제공한다.
2) TC는 서명자의 소속 확인이 끝난 후 비밀키 리스트를 안전한 방식으로 전달한다.
   : $K_{SU}=K_{SL1},\ldots,K_{SLn}$ (비밀키 리스트)
   : $K_{SUk}=K_{SL1},\ldots,K_{SLk}$ (단, $1\le k\le n$)
   서명자의 비밀키는 총 n개의 분할된다. 이 키는 TC에서 만든다고 가정하며, 각 서명자의 공개키로 암호화하여 분배되거나, IC카드와 같은 물리적인 형태로 분배된다. 각 서명자는 서명 수행을 위해 분배된 키 리스트 중에서, 날짜 또는 TC의 권고에 따라 k개를 선택해 서명 수행이 가능하다. 따라서 서명 확인을 위한 공개키는 수시로 변화되므로 안전성을 확보할 수 있으며, 별도의 키 생성을 위해 TC가 연산을 수행할 필요가 없기 때문에 효율적이다. 이러한 방식은 새로운 신규 멤버 가입 역시 쉽게 이뤄지는 장점을 가진다.
3) TC는 서명자의 공개키 들을 공개키 리스트에 등록한다.
   : $K_{PGk}=g^{K_{SUk}} \bmod p$ (단, $1\le k\le n$)

3.1.3 서명 수행 단계

1) 서명자는 다음과 같은 정보를 생성한다.
   - 큰 소수 p와 q를 생성한 다음 공개한다.
   - 원시 생성자 g를 다음과 같이 계산한다.
     : $h\in\{1,\ldots,p-1\}$를 선택한다.
     : $g=h^{(p-1)/q} \bmod p$가 되는 g를 계산하여 공개한다.
2) 수신자 Z는 자신의 비밀키와 공개키를 생성한다.
   - 자신의 일반 서명용 개인키 X_Z와 공개키 Y_Z를 다음과 같이 생성한다.
     : X_Z (단, $0<XZ<q$인 난수)
     : $Y_Z=g^{XZ} \bmod p$
3) 서명자는 다음과 같이 서명 정보를 생성하여 수신자 Z에게 전송한다.
   - 랜덤 수 k_1, k_2를 다음과 같이 생성한 후 e를 계산한다.
     : $\{k_1, k_2\}\in {}_RZ_P$
     : $e=g^{k_2-k_1} \bmod p$
   - 수신자 Z의 공개키를 이용하여 다음을 계산한다.
     : $D=Y_Z^{k_2} \bmod p$
   - 해쉬 함수를 이용하여 다음을 계산한 다음 서명 정보를 생성한다.
     : $R=H(g^{k_1} \bmod p\|M\|e\|D)$
     : $S=k_1-K_{SUk}*R \bmod q$
   - 다음을 수신자에게 전송한다.
     : (M, R, e, D, S) → 수신자

3.1.4 서명 검증 단계

1) 수신자는 다음을 확인함으로서 서명자의 신분을 확인한다.
   - 해쉬를 이용하여 R이 정확한지 확인한다.
     : $H(g^S*K_{PG}^R \bmod p\|M\|e\|D)=R$
2) 확인된 R을 통해 다음 수식이 만족한다면 서명은 유효하다고 판단한다.
   : $(g^S K_{PG}^R e)^{X_Z}=D \bmod p$

[그림 1]은 제안된 수신자 지정 그룹 서명 방식

TC (Trusted Center)	서명자	공개정보 K_{PGk}, p, q, g, Y_Z	검증자(수신자)
비밀키 리스트 → $K_{SU}=K_{SL1},\ldots,K_{SLn}$	← 신상정보 (서명자 이름, ID, 소속, 기타) 서명 정보 생성 → $\{k_1, k_2\}\in {}_RZ_P$ $e=g^{k_2-k_1} \bmod p$ $D=Y_Z^{k_2} \bmod p$ $R=H(g^{k_1} \bmod p\|M\|e\|D)$ $S=k_1-K_{SUk}*R \bmod q$	(M, R, e, D, S) →	서명 검증 : $H(g^S*K_{PG}^R \bmod p\|M\|e\|D)=R$: $(g^S K_{PG}^R e)^{X_Z}=D \bmod p$

[그림 1] 수신자 지정 그룹 서명 방식 흐름도

에 대한 개략적인 흐름도를 나타낸 것이다.

3.1.5 서명 프로토콜 검증

서명 프로토콜 검증은 다음과 같은 과정을 통해 그 유효성을 입증할 수 있다.

$$
\begin{aligned}
D &= (g^S K_{PG}^R e)^{X_Z} \bmod p \\
&= (g^{k_1} g^{(-R*K_{SUB})} g^{K_{USb}*R} e)^{X_Z} \bmod p \\
&= (g^{k_1} e)^{X_Z} \bmod p \\
&= (g^{k_1} g^{k_2 - k_1})^{X_Z} \bmod p \\
&= (g^{k_2})^{X_Z} \bmod p \\
&= Y_Z^{k_2} \bmod p \\
&= D
\end{aligned}
$$

3.2 무선 그룹키 갱신 방식

무선 이동 통신 상의 그룹 서비스를 위해 현재 다양한 암호 방식들이 연구되고 있다. 일반적으로 기존 멤버가 그룹을 탈퇴할 경우, 남아 있는 그룹 멤버의 안전성을 보장하기 위해 키 갱신은 필수적인 요소이다. 그룹의 특성상 키 갱신을 위해서는 센터와 그를 중심으로 하는 성형 네트워크를 기본 조건으로 가정한다. 다음은 기존의 무선 이동 통신 그룹 키 갱신 방식들을 살펴봄과 동시에 이들 방식들의 문제점을 해결할 수 있는 새로운 방식을 제시한다.

3.2.1 대칭키 암호 기법 이용 방식

각 사용자 $i(i=\{0,1,\ldots,n\})$는 그들의 비밀키 K_i를 가지고 있으며, 그룹 키 생성 및 분배를 담당하는 센터 C는 모든 사용자의 비밀키들을 비밀리에 보관한다. 단말기 분실이 발생할 경우, 센터는 사용자 U_i를 제외하고 각 사용자들을 위한 새로운 그룹 키 K_{G_NEW}를 자신이 보유하고 있는 각 사용자의 비밀키를 사용해 개별적으로 암호화 및 분배한다[12].

단, 이때 폐지된 사용자 U_i를 식별한 다음 새로운 그룹 키 K_{G_NEW}를 암호화하고 분배하는데 n-1번 정도의 시간을 필요로 하게된다. 만약 센터가 많은 수의 사용자들을 관리하는 경우, 키 갱신을 위한 데이터 전송에 많은 시간이 요구되기 때문에 정상적인 통신을 방해할 수 있다는 문제점을 갖는다.

3.2.2 비대칭 암호 기법 이용 방식

이 방식은 기본적으로 공개키를 전제로 하고 있기 때문에 다음과 같은 과정을 통해 그룹 키 갱신이 수행되어 진다[13].

1) 각 사용자 $i(i=\{1,2,\ldots,n\})$는 자신의 공개키 e_i 및 개인키 d_i를 다음과 같이 생성한 다음, e_i를 공개한다.
   : $e_i * d_i = 1 \bmod (p-1)$ (단, p는 큰 소수)
2) 센터는 다음의 정보를 생성하여 안전하게 저장한다.
   : $Y_i = g^{ei} \bmod p$
3) 키 갱신이 필요할 경우 센터는 랜덤 값 R을 생성하여 사용자 U_i를 제외한 모든 사용자에게 다음을 전송한다.
   : $Z_j = Y_j^R \bmod p$ (단, $j \neq i, j=\{1,2,\ldots,n\}$)
4) 새로운 그룹 키 K_{G_NEW}는 다음과 같은 과정을 통해 갱신된다.
   : $K_{G\_NEW} = Z_j^{d_j} \bmod p = (Y_j^R)^{d_j}$
   $= g^{e_j * d_j * R} = g^R \bmod p$

센터가 각 사용자의 비밀키를 알지 못하기 때문에 보안 측면에서 이 방법이 바람직할 것이다. 그러나 센터는 새로운 그룹 키를 암호화하고 분배하는데 (n-1)번 정도의 시간이 필요하다는 단점이 있다.

3.2.3 Matsuzaki-Anzai(MA) 방식

본 방식은 상기 방식들과는 달리 그룹 키 갱신시 가입된 사용자의 수에 의존하지 않는다는 특징을 가지고 있다[14]. 다음은 본 방식의 프로토콜을 간결하게 기술한 것이다.

1) 시스템 계수

본 방식에서 사용되는 시스템 계수는 다음과 같다.

- T_i : 각 사용자의 터미널 $(i=\{1,2,\ldots,n\})$
- s_i : 각 사용자 i의 비밀키
  : $i \neq j$일 경우 $GCD(s_i, s_j)=1$(단, 센터는 모든 사용자의 비밀키를 보관한다.)
- p, q : 센터가 생성하는 큰 소수
- K : 새로 갱신될 그룹 키

2) 준비 단계(Preparation phase)

(1) 센터

- $GCD(s_i, s_j)=1$, $i \neq j$가 되도록 각 사용자의 비밀키 s_i를 생성하고, 각 사용자의 터미널로 안전하게 전송 및 저장한다.
- 랜덤하게 새로운 그룹 키 K를 생성한다.
- 큰 소수 p, q를 생성한 다음, $n=p*q$를 계산한다.
  센터는 안전하게 s_i, K 및 n을 보관한다.
- 센터는 각 사용자의 비밀키를 이용하여 다음을 계산한 다음, 모든 T_i에게 분배한다.
  : $X_i=K^{si} \bmod n$
  X_i의 역수가 존재함을 보증하고, 분배된 X_i를 이용하여 modular n을 인수 분해하지 못하게 하기 위해 modular n은 다음의 조건을 만족한다.
  : $gcd(X_i, n)=1$

(2) 각 사용자

- 각 사용자는 센터로부터 수신된 X_i를 자신의 터미널에 저장한다.

3) 키 갱신 단계

(1) 센터

- 터미널의 분실 또는 정책에 의해, 센터에서 터미널 T_i를 폐지해야 할 경우, 다음과 같이 터미널 T_i와 관련된 정보를 모든 사용자에게 보내야 한다.
  : $(s_i, X_i(=K^{si} \bmod n), n(=p*q))$

(2) 각 사용자

T_i를 제외한 모든 사용자들은 수신된 정보를 이용하여 다음과 같은 과정을 수행한다.

- 1 단계
  T_j는 $a*s_i+b*s_j=1$을 만족하는 a, b를 계산한다. (단, s_i와 s_j는 공통 제수를 가지고 있지 않음)
  터미널 T_j는 정수 a와 b를 확장된 유클리드 알고리즘을 이용하여 polynomial time안에 계산 가능하다.
- 2 단계
  $a<0$ 일 때, 터미널 T_j는 다음을 계산한다.
  : $(X_i^{-1})^{-a*}X_j^b \bmod n$
  $= K^{a*s_i+b*s_j} \bmod n$
  $= K(X_i, n, X_j$를 이용)
  $b<0$ 이면,
  : $X_i^{a*}(X_j^{-1})^{-b} \bmod n$
  $= K^{a*s_i+b*s_j} \bmod n$
  $= K(X_i, n, X_j$를 이용)

본 방식은 터미널 T_i에 대해서 수신된 정보가 자신의 비밀키에 해당하므로 합당한 a와 b를 생성할 수 없게 된다. 따라서 터미널을 불법적으로 취득하거나 기존의 그룹 키를 안다 하더라도, 새로운 그룹 키 K를 얻을 수 없게 된다. 그러나, 본 방식은 2회 연속 그룹 키 갱신을 수행할 경우 새로이 준비 단계를 수행해야하며, 역수 값 계산이 사용자 단말에서 수행되므로 계산상 비효율적이라는 문제점을 드러내고 있다.

3.2.4 새로운 방식 제안

본 장에서는 상기 두 방식들의 문제점을 해결하는 새로운 그룹 키 갱신 방식을 제안한다.

1) 시스템 계수

본 제안 방식에서 사용되는 시스템 계수는 다음과 같다.

- P_j : 센터가 생성하는 큰 소수(j는 키 갱신 순번)
- K_j : 그룹 키 생성 정보 ($K_j \in_R Z_{Pj}$)
- T_i : 각 사용자의 터미널 ($i=\{1,2,\ldots,n\}$)
- Y_{ij}, Y_{ij}^{-1} : 그룹 키 은닉 정보 및 역수
- S_{ij} : 사용자 i의 비밀키

2) 프로토콜

(1) System setup 및 준비 단계

(가) 센터

- 큰 소수 $P_j(j=\{1,\ldots,m\}$, $m=$갱신될 키의 최대 개수)를 생성하여 안전하게 저장하고, 다음과 같이 사용자 비밀키 정보를 계산한다.
  : $GCD(S_{ij}, S_{ik})=1$(단, $S_{ij} \neq S_{ik}$)
- 그룹 키 생성 정보 K_j를 랜덤하게 생성하고, 다음과 같이 그룹 키 은닉 정보 및 역수를 계산한다.
  : $Y_{ij}=K_j^{Sij} \bmod P_j$, Y_{ij}^{-1}
  이를 통해 사용자는 별도의 역수 계산이 필요 없게 되므로 계산상 효율성을 얻을 수 있다.

〔표 1〕 각 방식별 분석 결과

항목 \ 방식	대칭키 방식	공개키 방식	MA 방식	제안 방식
통신 병목현상 해결	X	X	O	O
키 갱신 준비 단계 Overhead 해결	X	X	X	O
사용자간 담합 해결	X	X	O	O
2명 이상의 키 갱신 해결	O	O	X	O

- 센터는 해당 사용자 i에게 (S_{i1}, Y_{i1}, Y_{i1}^{-1},..., S_{im}, Y_{im}, Y_{im}^{-1})을 스마트 카드에 저장하여 안전하게 전송한다. 이를 통해 키 갱신 준비시 발생되는 overhead를 줄일 수 있다.

(2) 키 갱신 단계

본 과정에서는 2명의 사용자가 각각 단말기 T_i 및 T_i'를 분실한 것으로 가정하고 기술한다.

(가) 센터

- 폐지 대상 단말기들을 확인하고 기지국을 통하여 스마트 카드 정보를 모든 사용자에게 동보 전송한다.

  : (P_1, S_{i1}, Y_{i1}, Y_{i1}^{-1}), (P_2, S_{i2}', Y_{i2}', $Y_{i2}'^{-1}$)

  이때, 키 갱신시 P_j를 제공함으로서 사용자 공모에 의한 그룹 키 유출을 막을 수 있다.

(나) 각 사용자

- 1 단계

  사용자 e는 수신된 정보를 이용하여 다음을 만족하는 a_t, $b_t(t \in \{1,2\})$를 계산한다.

  : $a_1 * S_{i1} + b_1 * S_{e1} = 1$

  : $a_2 * S_{i2}' + b_2 * S_{e2} = 1$

- 2 단계

  $a_t < 0$일 때, 터미널 j는 다음을 계산한다.

  : $(Y_{i1}^{-1})^{-a_1} * Y_{e_1}^{b_1} \ mod \ P_1$

  $= K_1^{a_1 * S_{i1} + b_1 * S_{e1}} \ mod \ P_1 = K_1$

  : $(Y_{i2}'^{-1})^{-a_2} * Y_{e2}^{b_2} \ mod \ P_2$

  $= K_2^{a_2 * S_{i2}' + b_2 * S_{e2}} \ mod \ P_2 = K_2$

  $b_t < 0$ 이면, 터미널 j는 다음을 계산한다.

  : $Y_{i1}^{a_1} * (Y_{e1}^{-1})^{-b_1} \ mod \ P_1$

  $= K_1^{a_1 * S_{i1} + b_1 * S_{e1}} \ mod \ P_1 = K_1$

  : $Y_{i2}'^{a_2} * (Y_{e2}^{-1})^{-b_2} \ mod \ P_2$

  $= K_2^{a_2 * S_{i2}' + b_2 * S_{e2}} \ mod \ P_2 = K_2$

- 3 단계

  각 사용자는 계산된 정보를 통해 새로운 그룹 키 K를 갱신한다.

  $K = (\prod_{i=1}^{t} K_i) \ mod \ n$

3.2.5 각 방식별 비교 분석

기존의 대칭/비대칭 암호 기법의 경우 효율성 및 공모에 의한 부정을 극복하지 못하였으며, MA 방식은 준비 단계 및 2명 이상의 터미널이 분실시 비효율성을 낳고 있다. 〔표 1〕은 기존 방식들에 대해 제안 방식의 특징을 표로 기술한 것이다.

Ⅳ. 통합 멀티캐스트 키 관리 구조 제안

본 방식은 유·무선 통합 멀티캐스트 서비스를 위해 상기 제시되었던 요구 사항을 만족함과 동시에 안전성, 신뢰성, 효율성 및 확장성을 제공하고 있다. 특히 무선 멀티캐스트 서비스를 위해 기반이 되는 수신자 지정 그룹 서명 방식과 제안된 무선 그룹 키 갱신 방식을 적용한다.

4.1 시스템 계수

다음은 본 방식에서 사용되는 시스템 계수를 기술하고 있다.

- **시스템 구성 요소**
  - DKM_i : 도메인 키 관리자 i($i=1,2,...,k$: k는 도메인 키 관리자 수)
  - DMB_i : *Domain Border* i($i=1,2,...,k$: k는 Border의 수)
  - DKA_i : 도메인 키 중간 관리자 i($i=1,2,...,j$: j는 도메인 키 중간 관리자 수)
  - SGB_i : Subgroup Border i($i=1,2,...,j$: j는 Subgroup Border의 수)
  - MGB_i : Multicast Group Border i($i=1,2,...,k$: k는 Border의 수)
  - GML : 그룹 멤버 리스트

- PKM : 도메인 키(중간)관리자들 및 각 Border의 공개키 관리자
- MBR_i : 그룹 멤버 $i(i=1,2,\ldots,n : n$은 멤버의 수)
- R, GI : 라우터 및 그룹 초기자
- RH_i : 원격 호스트 i

• **각 구성 요소들의 키 관련 정보**

- $MKey$: PKM에 의해 생성된 멀티캐스트 키
- K_{PP}, K_{PS} : PKM의 공개키 및 개인키
- K_{DPi}, K_{DSi} : 각 DKM_i의 공개키 및 개인키
- K_{DAPi}, K_{DASi} : 각 DKA_i의 공개키 및 개인키
- K_{DMBPi}, K_{DMBSi} : 각 DMB_i의 공개키 및 개인 키
- K_{MGBPi}, K_{MGBSi} : 각 MGB_i의 공개키 및 개인키
- K_{SGBPi}, K_{SGBSi} : 각 SGB_i의 공개키 및 개인키
- K_{D_DAi} : DKM_i와 DKA_i 사이의 공통키
- K_{MSi} : 그룹 멤버 MBR_i의 비밀키
- K_{DAi_Msj} : 각 DKA_i가 관리하는 멤버들과의 공통키
- K_{GSi}, K_{GVi} : 수신자지정 그룹 서명용 키 및 확인 키
- K_{RPi}, K_{RSi} : 원격 호스트 i의 공개키 및 개인키
- Ref_key : Subgroup 공통키 갱신 정보
- Y_{ij}, Y_{ij}^{-1} : Subgroup 공통키 은닉 정보 및 역 수
- S_{ij} : DKA_i에 의해 생성되는 Subgroup 멤버 i의 비밀 정보
- P_j : DKA_i가 생성하는 큰 소수(j는 키 갱신 순번)

• **전송 정보 식별 및 인증 정보**

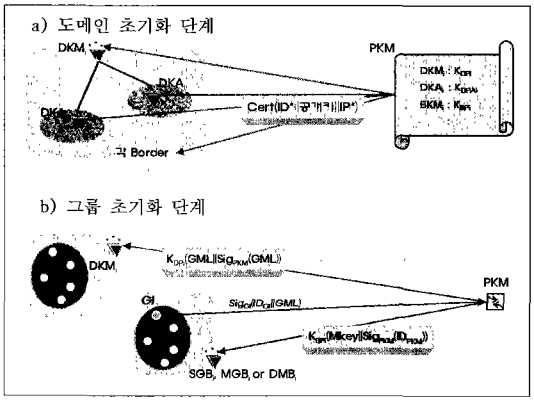
- Hdr : 메시지 전송 시 송신 그룹과 수신 그룹의 식별 정보
- $ID*, IP*, Sig*$: *의 식별자, IP 주소 및 서명
- M : 멀티캐스팅 메시지
- T, Tr : 멤버가 생성하는 Time-Stamp 및 원격 호스트가 제공하는 Time-Stamp
- Req_WMS : 무선 멀티캐스트 서비스 요청
- Ter_i : 각 사용자의 무선 터미널 $(i=\{1,2,\ldots,n\})$

4.2 시스템 프로토콜

본 방식은 멤버 가입 및 탈퇴시 최소한의 키 갱신을 유도하기 위하여 각 그룹은 계층적인 도메인 Subgroup 형식으로 분류하여 동적인 관리를 수행한다. 또한 구조적으로 PKM, DKM_i 및 DKA_i로 구성되는 제어부와 각 Border들로 구성되는 메시지 전송부로 이원화함으로서 키 관리 담당자의 부담을 줄이고 메시지 전송 과정에서 발생 가능한 부정 및 오버헤드를 막고 있다. 동시에 본 방식은 인증 및 메시지 암호화를 위하여 현재 국제 표준화 작업이 활발한 PKI(Public Key Infrastructure)를 적용한다. 이는 이질적인 통신망에서 안전성과 효율성을 높이는 효과를 제공한다.

4.2.1 도메인 초기화 단계

1) DKM_i, DKA_i 및 각 Border는 안전한 유니캐스트 채널을 통해 자신의 공개키 인증서를 PKM으로부터 수신한다.
   - PKM : $Cert(ID*\|*의\ 공개키\|IP*)\rightarrow *$
     : $*\in\{DKM_i, DKA_i, MGB_i, DMB_i, SGB_i\}$
2) 각 도메인은 DKM_i를 정점으로 멤버들을 분할하여 담당하는 각 DKA_i를 계층적으로 관리한다. 공개키 인증서 수신이 끝나게 되면 도메인 상의 각 관리자들은 상호 인증을 수행한다.



〔그림 2〕 도메인 초기화 및 그룹 초기화

4.2.2 그룹 초기화 단계

1) GI는 그룹 멤버 리스트(GML)를 작성하여 자신의 식별자 ID_{GI}와 함께 서명을 수행하여 PKM에게 전송한다.
   - GI : $Sig_{GI}(ID_{GI}\|GML)\rightarrow PKM$
     : $GML=(ID)MBR1\|\cdots\|ID_{MBRn})$
2) PKM은 서명 확인을 통해 GI 및 GML을 인증하고 멀티캐스트 서비스를 위한 MKey를 생성한다. 단, MKey는 그룹이 형성될 때, 오직 관련된 Border들(SGB_i, DMB_i, MGB_i)에게만 제

공함으로서 신뢰성을 높이고 있다.

- PKM : $K_{BPi}(MKey \| Sig_{PKM}(ID_{PKM}))$
  → 각 $Border(SGB_i, DMB_i, MGB_i)$
  : $K_{BPi} \in \{K_{SGBPi}, K_{DMBPi}, K_{MGBPi}\}$

3) PKM은 해당 Domain에게 공개키를 이용하여 안전하게 GML을 전송한다.

- PKM : $K_{DPi}(GML \| Sig_{PKM}(GML))$
  → DKM_i

4.2.3 그룹 멤버 가입 단계

1) DKM_i는 도메인 내에서 DKA_i와의 통신 시 사용할 K_{D_DAi}를 생성 및 서명을 수행하여 유니캐스트 채널을 통해 안전하게 DKA_i에게 전송한다.

- DKM_i : $K_{DAPi}(K_{D\_DAi} \| Sig_{DKM}(K_{D\_DAi}))$
  → DKA_i

2) 그룹에 멤버로 가입할 사용자들은 자신의 식별자, 비밀키 및 무선 서비스 요청에 서명을 수행함으로서 DKA_i에게 자신을 인증한다. 이때 멤버 가입 대상자들 중 무선 멀티캐스팅 서비스를 필요로 할 경우, 무선 멀티캐스트 서비스 요청을 다음과 같이 K_{DAPi}를 이용하여 안전하게 전송한다.

- MBR_i : $KDAP_i(ID_{MBRi} \| K_{MSi} \| Req\_WMS \| Sig_{MSi}(ID_{MBRi} \| K_{MSi} \| Req\_WMS)) \rightarrow DKA_i$
- $Req\_WMS = \{0,1\}$

3) DKA_i는 가입 대상자들로부터 받은 메시지를 복호화하여 인증을 수행하고 다음과 같이 그룹 가입 멤버 리스트를 생성해 DKM_i에게 전송한다.

- DKA_i : $K_{D\_DAi}(Sig_{DKAi}(ID_{MBR1} \| \cdots \| ID_{MBRi}))$
  → DKM_i

4) DKM_i는 각 DKA_i로부터 수신된 그룹 가입 멤버 리스트에 대해 복호 및 인증을 수행한 다음 GML과 비교 확인한다.

5) DKA_i는 Subgroup 키 갱신 정보를 다음과 같이 생성한 후에, 수신된 비밀키 K_{MSi}를 이용하여 각 멤버에게 K_{DAi_Ms1}, Subgroup 키 갱신 정보 및 수신자 지정 그룹 서명 키 K_{GSi}를 안전하게 전송해 준다. 동시에 이 K_{DAi_Ms1}, Subgroup 키 갱신 정보 및 K_{GSi}는 DKM_i 및 SGB_i에게 안전하게 전송된다.

- $Pj(j=\{1,\ldots,m\})$ 생성 및 멤버 비밀 정보 계산, $GCD(S_{ij}, S_{ik}) = 1$(단, $S_{ij} \neq S_{ik}$)
- K_{DAi_Msj} 생성 및 그룹 키 은닉 정보 및 역수 계산
  : $Y_{ij} = K_{DAi\_Msj}^{Sij} \bmod P_j$, Y_{ij}^{-1}
  (단, $j=\{2,\ldots,n\}$)
- Subgroup 키 갱신 정보 생성 : $Ref\_key = (S_{i1}, Y_{i1}, Y_{i1}^{-1}, \ldots, S_{im}, Y_{im}, Y_{im}^{-1})$
- DKA_i : $K_{MSi}(K_{DAi\_Ms1} \| Ref\_key \| K_{GSi})$
  → MBR_i
  : $K_{D\_DAi}(K_{DAi\_Ms1} \| Ref\_key \| K_{GSi}) \rightarrow DKM_i$
  : $K_{SGBPi}(K_{DAi\_Ms1} \| Ref\_key \| K_{GSi}) \rightarrow SGB_i$

6) 각 멤버는 무선 멀티캐스팅을 위해, 수신된 Subgroup 키 갱신 정보를 스마트 카드와 같은 저장 공간에 저장한다.

4.2.4 멀티캐스트 메시지 전송 단계

메시지 전송 단계는 멀티캐스트 메시지 전송부로서 오직 멤버들 MBR_i와 각 Border들만이 관여한다. 이 단계는 도메인 내 각 멤버들에게 메시지를 전송하는 내부 전송 과정과 타 도메인 및 다른 멀티캐스트 그룹에 속한 멤버들에게 보내는 외부 전송 과정으로 분류된다. 본 논문에서는 내부 전송 과정 중 도메인 전체 전송 부분과 외부 전송 과정 중 도메인에서 도메인으로의 전송 부분을 기술한다.

1) 내부 전송 과정 - 도메인 전체 전송

(1) 각 멤버들은 K_{DAi_Ms1}를 이용하여 멀티캐스트 메시지 M을 암호화한 다음 SGB_i에게 전송한다.

- MBR_i : $K_{DAi\_Ms}(M) \rightarrow SGB_i$

(2) SGB_i는 수신된 정보를 복호화하고, 멀티캐스트 메시지 M을 MKey로 암호화하여 각 SGB_i'에게 전송한다.

- SGB_i : $K_{DAi\_Ms1}(K_{DAi\_Ms1}(M)) = M$
  : $Mkey(M) \rightarrow SGB_i'$
  : $SGB_i \neq SGB_i'$

(3) 각 SGB_i'은 수신된 정보를 복호화하고 이를 자신이 속한 그룹의 공통키로 암호화하여 그룹 멤버들에게 전송한다.

- SGB_i' : $MKey(MKey(M)) = M$
  : $K_{DAi\_Ms1}'(M) \rightarrow MBR_i'$
  : K_{DAi_Ms1}'는 DKA_i'와 그 Subgroup에 속한 멤버들간의 Subgroup 공통키
  : $MBR_i \neq MBR_i'$

(4) 각 Subgroup의 멤버 MBR_i'는 K_{DAi_Ms1}'로 수신된 정보를 복호화하여 메시지를 확인한다.

- MBR_i' : $K_{DAi\_Ms1}'(K_{DAi\_Ms1}'(M)) = M$

2) 외부 전송 과정 - 도메인에서 도메인으로의 전송

(1) 각 멤버들은 K_{DAi_Ms1}를 이용하여 멀티캐스트 메시지 M과 식별자 Hdr을 암호화한 다음 자신이 속한 SGB_i에게 전송한다.

- MBR_i : $K_{DAi\_Ms1}(Hdr||M) \rightarrow SGB_i$

(2) SGB_i는 암호화되어 수신된 정보를 복호화한 후에 Hdr을 확인하고 자신의 서명과 함께 복호된 멀티캐스트 메시지 M을 MKey로 암호화하여 DMB_i에게 전송한다.

- SGB_i : $K_{DAi\_Ms1}(K_{DAi\_Ms1}(Hdr||M)) = Hdr||M$
  : $(Hdr||Sig_{SGBi}(Hdr)||MKey(M)) \rightarrow DMB_i$

(3) DMB_i는 Hdr을 확인하고 인접 도메인 Border DMB_{i+1}에게 전송한다.

- DMB_i : $(Hdr||Sig_{SGBi}(Hdr)|MKey(M)) \rightarrow DMB_{i+1}$

(4) DMB_{i+1}은 Hdr과 서명을 확인하고 해당 도메인에 속한 모든 SGB_{i+1}에게 전송한다.

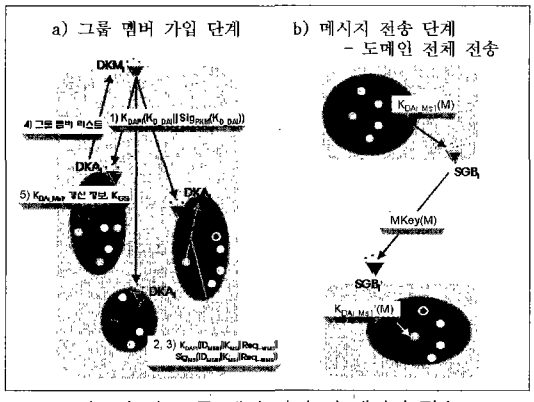
- DMB_{i+1} : $MKey(M) \rightarrow SGB_{i+1}$

(5) 전송된 메시지는 각 SGB_{i+1}에 의해 복호화된 다음 각 그룹의 모든 멤버들에게 암호화되어 전송된다.

- SGB_{i+1} : $Mkey(MKey(M)) = M$
  : $K_{DAi+1\_Ms1}(M) \rightarrow MBR_{i+1}$
  : K_{DAi+1_Ms1}는 DKA_{i+1}와 그 Subgroup에 속한 멤버들간의 Subgroup 공통키

(6) 각 DKA_{i+1}에 속한 Subgroup의 모든 멤버 MBR_{i+1}은 K_{DAi+1_Ms1}로 복호화하여 메시지를 확인한다.

- MBR_{i+1} : $K_{DAi+1\_Ms1}(K_{DAi+1\_Ms1}(M)) = M$



[그림 3] 그룹 멤버 가입 및 메시지 전송

(7) 각 DKA_{i+1}에 속한 Subgroup의 모든 멤버 MBR_{i+1}은 K_{DAi+1_Ms1}로 복호화하여 메시지를 확인한다.

- MBR_{i+1} : $K_{DAi+1\_Ms1}(K_{DAi+1\_Ms1}(M)) = M$

4.2.5 유·무선 원격 호스트 접속 및 인증

1) 원격 호스트 접속 및 인증

다양한 정보 통신 기기의 발전을 통해 그룹 멤버들은 자유로운 이동성을 가지게 되었다. 이동성을 가지는 MBR_i는 사용 매체에 따라 유선 또는 무선으로 원격 호스트를 통해 멀티캐스트 서비스를 지원받아야 하므로, 자신의 인증 과정은 필수적이다. 이때, 자신의 익명성을 제공받기 위해 가명 ID와 수신자 지정 서명을 수행한다.

(1) 멤버는 원격 호스트에서 사용할 자신의 가명 식별자 ID_N를 생성한다. 또한 서비스 개시를 위한 Time-Stamp를 생성하여, 지불 인증을 받을 DKM_i와 가명 식별자를 수신자 지정 서명을 수행해 다음과 같이 원격 호스트에게 전송한다. 가명 식별자를 사용하는 이유는 제 3자로부터 자신의 신원을 숨기기 위해서이다.

- MBR_i : $ID_N||K_{GSi}(ID_N||ID_{Nr}||DKM_i||T) \rightarrow RH_i$

(2) 원격 호스트는 수신자 지정 서명을 확인한 다음, 멀티캐스트 서비스 수행을 위해 도메인 Border와 안전한 유니 캐스트 채널을 형성한다.

2) 원격 호스트 Hand-off 및 지불 인증

(1) 멤버 MBR_i가 이동성이 빨라 Hand-off가 발생될 경우, 원격 호스트 RH_i는 다음 원격 호스트 RH_{i+1} 및 DKM_i에게 다음의 정보를 전송해 준다.

- RH_i : $K_{RHPi+1}(ID_{Nr}||Tr)||K_{GSi}(ID_N||ID_{Nr}||T) \rightarrow RH_{i+1}$
  : $K_{DPi}(ID_{Nr}||Tr)||K_{GSi}(ID_N||ID_{Nr}||DKM_i||T) \rightarrow DKM_i$

(2) 멤버 정보를 수신하면, DKM_i는 다음과 같이 지불 확인 정보를 RH_i에게 전송한다. 이를 통해 RH_i는 지불 인증을 받게 된다.

- DKM_i : $ID_{Nr}||K_{DAPi}(ID_N||Tr-T)$

(3) RH_{i+1}은 수신된 정보를 확인한 다음, 4.2.5절의 1)-(2)의 과정을 수행한다. 사용자 요구에 의해 멀티캐스트 접속이 완료되면, 멤버 MBR_i에게 다음의 정보를 각각 전송한다.

- RH_{i+1} : $ID_{Nr+1}||T_{r+1}||K_{RSi+1}(ID_N||ID_{Nr+1}||Tr||T_{r+1}) \rightarrow MBR_i$

(4) MBR_i는 수신정보를 확인한 후에, 다음 정보를 생성해 RH_{i+1}에게 전송한다.

- MBR_i : $ID_N||K_{GSi}(ID_N||ID_{Nr+1}||DKM_i||Tr||T_{r+1}) \rightarrow RH_{i+1}$

(5) RH_{i+1}은 다음의 정보를 DKM_i에게 전송한다.

- RH_{i+1} : $K_{DPi}(ID_{Nr+1}||T_{r+1})||K_{GSi}(ID_N||ID_{Nr+1}||DKM_i||T_r||T_{r+1}) \rightarrow DKM_i$

(6) DKM_i는 상기 2)-(2) 과정을 수행함으로서 지불 인증을 수행한다.

4.2.6 신규 멤버 가입 및 기존 멤버 탈퇴 단계

1) 신규 멤버 가입

신규 멤버 가입은 다음과 같은 과정을 통해 수행된다.

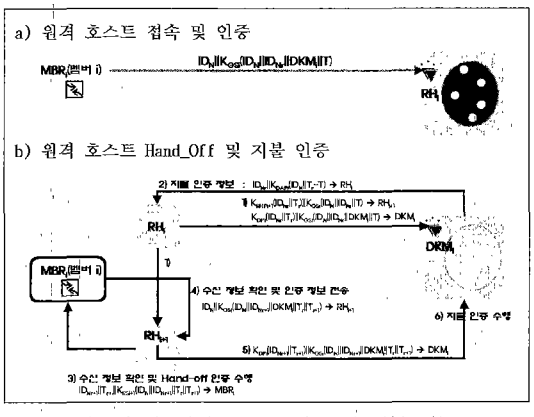
(1) 그룹에 신규 멤버로 가입할 사용자들은 자신의 신원 정보, 비밀키 및 무선 서비스 요청 내용에 서명을 수행하여 DKA_i에게 자신을 인증하고 이들 정보를 K_{DAPi}로 암호화하여 안전하게 전송한다.

- MBR_i : $K_{DAPi}(ID_{MBRi}'||K_{MSi}'||Req\_WMS||Sig_{MSi}'(ADD||ID_{MBRi}'||K_{MSi}'||Req\_WMS)) \rightarrow DKA_i$
- $Req\_WMS = \{0,1\}$

: ADD는 신규 가입 대상자임을 나타내는 식별자

(2) DKA_i는 신규 가입 대상자들로부터 받은 메시지를 복호화하여 인증을 수행하고 다음과 같이 신규 가입 멤버 정보를 생성해 DKM_i에게 전송한다.

- DKA_i : $K_{D\_DAi}(Sig_{DKAi}(ADD||ID_{MBRi}')) \rightarrow DKM_i$



(그림 4) 원격 호스트 접속 및 지불 인증

(3) DKM_i는 DKA_i로부터 수신된 그룹 신규 가입 멤버 정보에 대해 복호 및 인증을 수행한 다음 GML의 내용을 수정한다. 수정된 GML'을 PKM에게 전송한다.

- DKM_i : $GML \rightarrow GML'(=(ID_{MBR1}||\cdots||ID_{MBRn}||ID_{MBRi}'))$: $K_{DPi}(Sig_{DKMi}(GML')) \rightarrow PKM$

(4) PKM은 GML'의 수정 내용을 확인한 다음 GML을 GML'으로 교체한다.

(5) DKA_i는 4.2.3-5)와 동일한 과정을 통해 K_{DAi_Ms1}, Subgroup 키 갱신 정보 및 K_{GSi}를 안전하게 신규 가입 멤버에게 전송해 준다. 신규 멤버 가입시에는 K_{DAi_Ms1}에 대한 별도의 변화는 필요 없게 된다.

- DKA_i : $K_{MSi}'(K_{DAi\_Ms1}||Ref\_key||K_{GSi}) \rightarrow MBR_i'$

2) 기존 멤버 탈퇴 또는 무선 단말기 분실

기존 멤버 탈퇴 또는 무선 단말기 분실 시에는 기존 멤버를 보호하고 불법 사용을 방지하기 위해 기존의 K_{DAi_Ms1}을 갱신하여야 한다. 이를 통해 그룹 탈퇴자와 악성 침입자로부터 기존 멤버들에 대한 보안성을 획득할 수 있다.

(1) 그룹 탈퇴 및 무선 단말기의 분실 시, 다음과 같은 정보를 생성하여 DKA_i에게 안전하게 전송한다.

- MBR_i : $K_{DAPi}(Sig_{MSi}(DEL||ID_{MBRi})) \rightarrow DKA_i$

: DEL은 그룹 탈퇴 희망자 또는 단말기 분실 자임을 나타내는 식별자

(2) DKA_i는 다음과 같은 정보를 생성해 DKM_i에게 전송한다.

- DKA_i : $K_{D\_DAi}(Sig_{DKAi}(DEL||ID_{MBRi})) \rightarrow DKM_i$

(3) DKM_i는 DKA_i로부터 수신된 정보에 대해 복호 및 인증을 수행한 다음 GML의 내용을 수정한다. 수정된 GML'을 안전하게 PKM에게 전송한다.

- DKM_i : $GML \rightarrow GML'(=(ID_{MBR1}||\cdots||ID_{MBRi-1}||ID_{MBRi+1}||\cdots||ID_{MBRn}))$: $K_{DPi}(Sig_{DKMi}(GML')) \rightarrow PKM$

(4) PKM은 GML'의 수정 내용을 확인한 다음 GML을 GML'으로 교체한다.

(5) DKA_i는 Subgroup 키 갱신을 위해 기존의 멤버들 MBR_i', DKM_i 및 SGB_i에게 Subgroup

갱신 관련 부가 정보를 전송한다.

- $P_1, S_{i1}, Y_{i1}, Y_{i1}^{-1}, \ldots, P_j, S_{ij}, Y_{ij}, Y_{ij}^{-1}$

(6) MBR_i', DKM_i 및 SGB_i에는 다음과 같은 과정을 통해 새로운 Subgroup 공통키 K_{DAi+1_Msj}를 생성한다. 이를 통해 이동 중인 기존 멤버들도 간편하게 키 갱신을 수행할 수 있다.

- 다음을 만족하는 a_t, b_t($t \in \{1, 2\}$) 계산

: $a_1 * S_{i1} + b_1 * S_{e1} = 1$

:

: $a_j * S_{ij'} + b_j * S_{ej} = 1$

- $a_t < 0$일 때, 다음을 계산

: $(Y_{i1}^{-1})^{-a1} * Y_{e1}^{b1} \ mod \ P_1$

$= K_1^{a1*Si1 + b1*Se1} \ mod \ P_1 = K_1$

:

$(Y_{ij}^{'-1})^{-aj} * Y_{ej}^{bj} \ mod \ P_j$

$= K_j^{aj*Sij' + bj*Sej} \ mod \ P_j = K_j$

- $b_t < 0$ 이면, 다음을 계산

: $Y_{i1}^{a1} * (Y_{e1}^{-1})^{-b1} \ mod \ P_1$

$= K_1^{a1*Si1 + b1*Se1} \ mod \ P_1 = K_1$

:

$Y_{ij}^{'aj} * (Y_{ej}^{-1})^{-bj} \ mod \ P_2$

$= K_j^{aj*Sij' + bj*Sej} \ mod \ P_j = K_j$

- 계산된 정보를 통해 새로운 Subgroup 공통키 갱신

: $K_{DAi+1\_Msj} = (\prod_{j=1}^{t} K_j) \ mod \ n$

4.2.7 그룹 합병 및 그룹 분할

1) 그룹 합병

기존 두 그룹의 합병은 다음과 같은 과정을 통해 수행된다.

(1) 그룹 합병을 원하는 DKA_i는 그룹 합병 요구 메시지를 다음과 같이 통고한다.

- DKA_j : $Hdr \| K_{DAj\_Ms1}(Request) \rightarrow SGB_j$
- SGB_j : $Hdr \| Sig_{SGBi}(Hdr) \| MKey(Request) \rightarrow SGB_i$
- SGB_i : $K_{DAi\_Ms1}(Request) \rightarrow DKA_i$

(2) DKA_i는 Border를 통해 받은 전송 정보를 복호화하여 확인하고 그룹 합병을 결정한다. 그룹 합병이 결정되면 그룹 합병 승인 메시지를 DKA_j에게 전송한다.

(3) 승인 메시지를 받은 DKA_j는 그룹 멤버 리스트 GML_j를 DKA_i에게 전송한다.

(4) DKA_i는 새로운 공통키 $K_{DAi+j_{Ms}}$을 생성하여 DKM_i에게 그룹 합병 정보와 새로운 공통키 $K_{DAi+j_{Ms}}$, 공통키 갱신정보 Ref_{key} 및 DKA_j의 그룹 멤버 리스트 GML_j를 함께 전송한다.

- DKA_i : $K_{D\_DAi}(Sig_{DKAi}(Union \| GML_j \| Ref_{key} \| K_{DAi+j\_Ms1})) \rightarrow DKM_i$

: Union은 그룹 합병 정보 식별자

(5) DKM_i는 DKA_i로부터 수신된 그룹 합병 정보에 대해 복호 및 인증을 수행한 다음 새로운 그룹 멤버 리스트 GML_{i+j}를 생성하여 PKM에게 전송한다.

- DKM_i : $GML_{i+j}(=(GML_i + GML_j))$

: $K_{DPi}(Sig_{DKMi}(GML_{i+j})) \rightarrow PKM$

(6) DKA_i는 4.2.3-5)와 동일한 과정을 통해 새로운 공통키 K_{DAi+j_Ms1}, Subgroup 키 갱신 정보 및 K_{GSi}등을 모든 멤버들 MBR_i와 SGB_i에게 전송하고, DKA_j에게는 DKA_i의 그룹 멤버 리스트 GML_i를 함께 전송한다.

- DKA_i : $K_{BPi}(K_{DAi+j\_Ms1} \| Ref\_key) \rightarrow SGB_i$

: $K_{DAi\_Ms}(K_{DAi+j\_Ms1} \| Ref\_key) \rightarrow MBR_i$

: $Hdr \| K_{DAj\_Ms}(GML_i \| K_{DAi+j\_Ms1} \| Ref\_key) \rightarrow DKA_j$

(7) DKA_j는 4.2.7-(6)와 동일한 과정을 수행한다.

- DKA_j : $K_{BPj}(K_{DAi+j\_Ms1} \| Ref\_key) \rightarrow SGB_j$

: $K_{DAj\_Ms}(K_{DAi+j\_Ms1} \| Ref\_key) \rightarrow MBR_j$

: $K_{D\_DAj}(Sig_{DKAj}(Union \| GML_i DKA_j K_{DAi+j\_Ms1} \| Ref\_key)) \rightarrow DKM_j$

: Union은 그룹 합병 정보 식별자

(8) DKM_j는 DKA_j로부터 수신된 그룹 합병 정보에 대해 복호 및 인증을 수행한 다음 새로운 그룹 멤버 리스트 GML_{i+j}를 생성한다.

- DKM_j : $GML_{i+j}(=(GML_i + GML_j))$

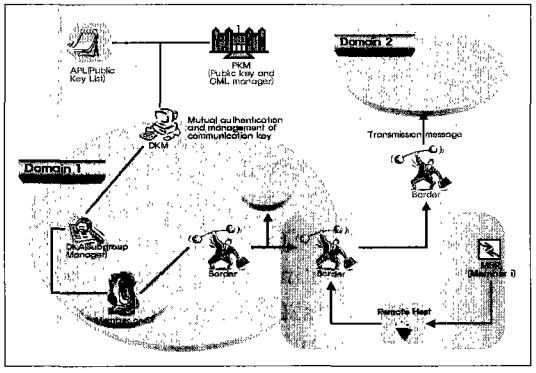
2) 그룹 분할

(1) 합병된 그룹에서의 그룹 분할

그룹의 분할은 그룹 합병과는 달리 그룹 분할 정보를 DKA_{i+j}, DKM_{i+j}, SBG_{i+j}, 모든 그룹 멤버 MBR_{i+j}에게 전달하고 이를 전달받은 각 개체는 해당 그룹 키를 삭제한다. 또한 DKM_{i+j}와 PKM_{i+j}는 그룹의 멤버 리스트 GML_{i+j}를 삭제함으로써 완료된다.

(2) 기존 그룹에서의 그룹 분할

기존 그룹DKA_i가 분할될 경우 새로 생성되는 그



〔그림 5〕 제안된 멀티캐스트 키 관리 구조도

룹의 DKA_j와 SGM_j가 생성되며, 각 그룹은 다음과 같은 과정으로 새로운 GML과 그룹 키를 생성한다.

(가) 기존 그룹의 DKA_i는 4.2.5의 기존 멤버 탈퇴 시와 같은 방식으로 GML과 그룹 키를 갱신한다.

(나) 새로 생성된 그룹의 DKA_j는 4.2.3의 그룹 멤버 가입단계와 같은 과정을 수행한다.

4.3 새로운 방식 분석

다음은 유·무선 멀티캐스트 키 관리 구조 요구사항에 기초하여 제안 방식의 특징을 분석한 결과이다.

1) 무결성 및 인증성

키 생성과 분배시 모든 정보는 대칭키 및 공개키 암호 방식을 이용하므로, 무결성 및 인증성을 획득하고 있다.

2) 접근 제어

멀티캐스트 메시지는 각 Subgroup 멤버의 공통키와 Border의 Mkey를 통해서 멤버에게 전송되므로, 멤버 이외의 사용자들은 접근이 불가능하다.

3) 부인 봉쇄

키 생성 시 전송되는 각 정보에 대해 디지털 서명 기법을 사용하므로, 부인 봉쇄가 가능하다.

4) 비밀성

멀티캐스트 정보의 송·수신시 공통키를 사용하므로 비밀성을 확보하고 있다.

5) 공정성 및 확장성

멤버 가입 및 탈퇴에 따른 그룹 참여자의 변동시 오직 Subgroup 내에서만 키 갱신이 일어나므로 확장성 부분에서 효율성을 확보하고 있으며, 키 분배 및 갱신과는 별도로 Border에게 Mkey가 제공되므로, 그룹 멤버로 가입하기 전에는 불법적 결탁이 이뤄질 수 없다.

6) 익명성 및 Hand-Off 허용

본 방식은 원격 호스트 접근시 수신자 지정 그룹 서명 방식을 사용하므로 사용자 익명성이 보장되며, 이동성 보장을 위한 Hand-Off 프로토콜이 구성되어 있다.

7) 무선 멀티캐스트 키 분배 및 갱신

본 방식은 새로이 제안된 무선 그룹 키 갱신 방식을 통해 통신 병목 현상, 키 갱신시 Overhead, 그룹 멤버간 공모 방지 및 2명 이상의 동시 키 갱신을 수행함으로서 안전성을 확보하고 있으며, 그 횟수를 최소화함으로서 효율성을 높이고 있다.

〔표 2〕는 멀티캐스트 키 관리 구조 요구사항에

〔표 2〕 각 방식별 비교 분석

항목 \ 대상	Clique	Iolus	GKMP	DK[24]	제안방식
메시지 암호키의 수	3	3	5	7	3
암호 방식 (대칭, 비대칭)	(O,O)	(O,O)	(O,X)	(O,O)	(O,O)
참가자 증가에 따른 키 증가	X	X	X	X	X
탈퇴자에 대한 참가자 보안성	O	O	O	O	O
참가자 수에 따른 중계 라우터 키의 양	변화 없음	증가	증가	증가	변화 없음
상호 인증성	O	O	O	O	O
통신 신뢰성	X	X	O	O	O
병목현상 극복	O	X	O	O	O
키 갱신 범위	ALL	Sub-Group	Sub-Group	ALL	Sub-Group
메시지 전송시 암/복호화 회수	1	j	k	1	2

k : 도메인 수 j : 중간 관리자(중계 라우터) 수

기초하여 기존 유선에서의 멀티캐스트 그룹 키 관리 구조와 제안 방식을 비교 분석한 결과이다.

V. 결 론

현대 사회는 정보 통신 분야의 발전과 더불어 다양한 멀티캐스트 관련 서비스 요구가 증대되고 있다. 그러나 멀티캐스트 서비스는 기본적으로 다자간 통신을 요구함으로서 안전성, 효율성 및 확장성 부분에서 취약성을 드러내고 있다.

또한 이동 통신 분야의 고속 성장은 음성 서비스의 차원을 넘어서 그룹을 대상으로 하는 인터넷 서비스까지 포괄적으로 적용되고 있다. 그러나 이동 통신 상에서 그룹 서비스를 지원할 경우, 보안적 위협에 대해서 취약성을 지니고 있으며, 그룹 키의 분실 및 유용으로 인한 변경, 갱신에 대해서는 연구가 미흡한 실정이다.

본 논문에서는 유·무선 통합 멀티캐스트 서비스 상에서 이러한 취약성을 극복하기 위해 필요한 요구사항을 살펴보았고, PKI(Public Key Infrastructure), 계층적 도메인 Subgroup 및 구조적 이원화 기법 등을 이용하여 확장성을 제공하는 안전한 멀티캐스트 키 관리 구조를 제안하였다. 또한 이동성을 고려하여 인증 및 익명성을 제공하기 위해 수신자 지정 그룹 서명 방식과 무선에서의 그룹키 갱신 방식을 제시하였다. 동시에 유·무선 통합 환경에 적합한 새로운 멀티캐스트 키 관리 구조를 제안하여 요구사항 만족도 및 특징을 분석하였다. 이를 통해 제안된 방식은 안전성과 확장성을 제공하면서 통합 환경에 능동적으로 대처할 수 있는 효율적인 구조로 이루어져 있음을 확인하였다. 따라서 본 방식은 향후 더욱 다양해지는 멀티캐스트 관련 서비스 분야에서 적극적으로 대처할 수 있으리라 기대된다.

참 고 문 헌

[1] M. Steiner, G. Tsudik and M. Waidner, "Diffie-Hellman Key distribution extended to group," In ACM Symposium on Computer and Communication Security, 1996.

[2] G. Caronni, M. Walldvogel and D. Plattner, "Efficient Security for Large Dynamic Multicast Groups," WETIC '98, 1998.

[3] S. Mittra, "Iolus : A Framework for Scalable Secure Multicasting," 1997.

[4] "멀티캐스트를 위한 키 분배 메커니즘 설계 및 구현" ETRI 최종 보고서, 1999.

[5] A. Ballardie, "Scalable Multicast Key distribution," RFC1949, May, 1996.

[6] A. Ballardie, "Core Based Tree(CBT) Multicast Routing Architecture," Request for Comments2201, Internet Activities Board, Oct, 1997.

[7] T. Maufer and C. Semeria, "Introduction to IP Multicast Routing," draftietfmboned-intro-multicast-00.txt, Mar, 1997.

[8] C. Perkins, "IP mobility support," RFC 2002.

[9] D. Chaum, "Group Signature," Advances in Cryptology-EUROCRYPT 91 Proceedings, Springer-Verlag, 1991, pp. 257~265.

[10] S. J. Kim, S. J. Park and D. H. Won, "Nominative Signatures," Proc. ICEIC '95, pp. II-68~II-71, 1995.

[11] 박희운, 이임영, "안전한 수신자 지정 그룹 서명 방식에 대한 고찰," 한국멀티미디어학회 추계학술발표논문집, 1999. 11.

[12] R. Lin and Kai-Min Wang, "Mobile Multicast Support in IP Network," INFOCOM 2000, Vol. 3, pp. 1664~1672, 2000.

[13] T. Hwang, "Scheme for Secure Digital Mobile Communications Based on Symmetric Key Cryptography," Information Processing Letters, 48, pp. 35~37, 1993.

[14] N. Matsuzaki and J. Anzai, "A Group Key Renewal Method Suitable for Mobile Telecommunications," Proceedings of SCIS98, 5.2.E. 1998.

[15] W. Diffie and M. Hellan, "New Direction in cryptography," IEEE Trans., It-22, pp. 644~654, 1976.

[16] I. Ingemarsson, D. Tang and C. Wong, "A Conference key distribution system," IEEE Trans., It-28, pp. 714~720, 1982.

[17] K. Koyama and K. Ohta, "Identity-based conference key distribution systems,"

Proceedings of Crypto '87, lecture Notes in Computer Science no. 293, Springer-Verlag, pp. 175~184, 1988.
[18] M. Burmester and Y. Desmedt, "A Secure and Efficient Conference Key Distribution Systems," EUROCRYPT '94, pp. 279~290, 1994.
[19] Y. Yacobi, "Attack on the Koyama-Ohta Identity-based key distribution systems," Proceedings of Cryto'87, Lecture Notes in Computer Science no. 293, Springer-Verlag, pp. 429~433, 1988.
[20] E. Brickell, P. Lee and Y. Yacobi, "Secure Audio teleconference," Advances in Cryptology-Crypto '87, Lecture Notes in Computer Science 293, pp. 418~426, 1988.
[21] 박희운, 이임영, "효율적인 회의용 키 분배 방식에 관한 연구," 한국통신정보보호학회 충청지부, 1999.
[22] J. Moyer, R. Rao and P. Rohatgi, "A Survery of Security Issues in Multicast Communications," IEEE Network, Nov/Dec, 1999.
[23] T. Hardjono, B. Cain and N. Doraswamy, "A Framework for Group key Management for Multicast Security," draftietf-ipsec-gkmframework-02.txt, Feb, 2000.
[24] "멀티캐스트를 위한 키 분배 메커니즘 설계 및 구현" ETRI 최종 보고서, 1999.

〈著者紹介〉

박 희 운 (Hee-Un Park) 학생회원
1997년 2월 : 순천향대학교 컴퓨터공학부 졸업
1999년 2월 : 순천향대학교 전산학전공 석사
1999년 3월~현재 : 순천향대학교 전산학전공 박사과정
〈관심분야〉 암호이론, 컴퓨터 보안

이 임 영 (Im-Yeong Lee) 종신 회원
1981년 8월 : 홍익대학교 전자공학과 졸업
1986년 3월 : 오사카대학 통신공학전공 석사
1989년 3월 : 오사카대학 통신공학전공 박사
1989년 1월~1994년 2월 : 한국전자통신연구원 선임연구원
1994년 3월~현재 : 순천향대학교 정보기술공학부 부교수
〈관심분야〉 암호이론, 정보이론, 컴퓨터 보안