확장성을 제공하는 안전한 멀티캐스트 키 관리 구조
(A Scalable Secure Multicast Key Management Structure)

박 희 운 † 이 임 영 †† 박 원 주 ††† 이 종 태 †††† 손 승 원 †††
(Hee-Un Park) (Im-Yeong Lee) (Won-Joo Park) (Jong-Tai Lee) (Sung-Won Sohn)

요 약 그룹에 기반한 통신 응용 서비스의 요구가 증가함에 따라 멀티캐스트 기반 구조에 대한 연구가 활발히 진행되고 있다. 하지만 멀티캐스트 구조에 대한 안전성과 효율성 및 확장성 부분에 대한 해결책은 아직 미비한 상태이다. 본 연구에서는 기존의 대표적인 멀티캐스트 키 관리 구조를 고찰함과 동시에 PKI(Public Key Infrastructure), IPsec, 도메인 Subgroup 및 구조적 이원화 기법 등에 기초하여 확장성을 제공하는 안전한 멀티캐스트 키 관리 구조를 제안한다. 또한 새로이 제안된 방식과 기존의 방식들을 안전성, 효율성 및 확장성 부분에서 비교 분석함으로서 그 효용성을 검증한다.

키워드 : 멀티캐스트, 확장성, 안전성, 효율성, 키 관리

Abstract Through the increment of requirement for group oriented communication services, on the open network, the multicast infrastructure 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 discuss conventional multicast key management structures and propose a scalable secure multicast key management structure based on PKI(Public Key Infrastructure), IPSec, domain subgroup and structural two mode scheme. Also we certify to the usability of new proposed scheme from comparing it with conventional schemes in the part of safety, efficiency and scaleability.

Key words : Multicast, Scaleability, Satety, Efficiency, Key management

1. 서 론

컴퓨터의 보급 확산과 공용 네트워크의 발전을 통해 다가오는 산업 및 사회 일반에서 정보의 의존성이 한층 가속화되고 있다. 이에 따라 일반인 누구나 인터넷 등을 통해 세계 곳곳의 정보를 한눈에 볼 수 있는 시대가 도래하고 있다.

이러한 상황에서 사용자들은 단순한 통신에서 벗어나 다자간 통신 회의 및 의료 분야에서 원격 진단 및 상담 등 다양한 서비스를 요구하고 있다. 그러나 이와 같은 서비스는 기존의 일대일 통신 방식으로는 제약 사항이 생길 수밖에 없다. 이를 해결하기 위하여 현재 각광을 받고 있는 방식 중의 하나가 멀티캐스트 기법이다[1~8].

멀티캐스트란 그룹에 참가한 멤버들 사이에서 한 송신자로부터 다수의 참여자에게 메시지 전송이 가능한 방법을 의미한다. 이때 그룹 멤버가 해당 그룹을 떠나면 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 안전성에 대한 취약성이 노출되고 있다. 특히 불법적인 제 3자의 도청이나 전송 정보의 위조는 그 대표적인 예가 된다. 이러한 불법 행위로부터 안전성과 신뢰성을 확보하기 위해 암호 시스템이 이용되고 있다. 그러나 키의 노출 여부는 전송 정보의 안전성과 직결되므로 매우 중요시 다뤄져

· 본 연구는 2001년도 한국전자통신연구원의 위탁연구과제 지원사업을 통해 수행된 것입니다.
† 학생회원 : 순천향대학교 정보기술공학부
phu24@hotmail.com
†† 정 회 원 : 순천향대학교 정보기술공학부 교수
imylee@sch.ac.kr
††† 비 회 원 : 한국전자통신연구원 정보보호연구본부 연구원
wjpark@etri.re.kr
swsohn@etri.re.kr
†††† 비 회 원 : 국가보안기술연구소 연구원
jtl@etri.re.kr
논문접수 : 2001년 1월 3일
심사완료 : 2001년 12월 24일

야 하며, 회원의 가입 및 탈퇴를 위하여 확장성이 보장되어야 한다.

현재 멀티캐스트 그룹 키 관리 분야와 관련하여, 그 중요성에도 불구하고 해결책들은 미흡한 상황이다. 따라서 본 연구는 향후 광범위하게 적용될 멀티캐스트 서비스에서 신뢰성 및 확장성을 제공하기 위하여 요구되는 사항들을 고려함은 물론 기존의 멀티캐스트 키 관리 구조들을 고찰한다. 동시에 PKI(Public Key Infrastructure), IPSec, 계층적 도메인 Subgroup 및 구조적 이원화 기법 등을 이용하여 확장성을 제공하는 안전한 멀티캐스트 키 관리 구조를 제안한다. 또한 이러한 구조적 특성들과 제시된 요구 사항들을 근거로 안전성, 효율성 및 확장성 부분에서 제안 방식과 기존 방식들을 비교 분석함으로서 그 효용성을 검증할 것이다.

2. 멀티캐스트 키 관리 요구사항

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

- 비밀성 : 불법적인 제 3자로부터 멀티캐스트 정보는 보호되어야 한다. 이를 위해 다양한 암호 기법이 적용될 수 있다.
- 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.
- 공정성 : 멀티캐스트에서 사용되는 키들은 허가된 그룹 참여자에게만 안전하게 전송되어야 한다. 또한 가입 및 탈퇴를 대비해 키 갱신 프로토콜은 필수적이다. 이를 위해 서버의 독단이나 제 3자와의 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.

3. 기존 방식 분석

현재 멀티캐스트 키 관리 서비스와 관련하여, 다양한 방식들이 제안 및 연구되고 있다. 본 연구에서는 기존에 제시된 방식들 중 버스형 또는 링형에서 사용되는 Clique, 분산 트리 구조에서 수행되는 Iolus, 인터넷 Domain 환경에서 사용 가능한 Domain GKMP 및 CBT(Core Based Tree) 모델에서 적용 가능한 DK 방식에 대해 고려할 것이다[1~7, 10]. 특히 Clique 및 Iolus에 대해서는 멀티캐스트 키 관리 개념을 이해하는 측면에서 세부적으로 살펴볼 것이다.

3.1 Clique 방식

이 방식은 Diffee-Hellman 방식을 이용하여 그룹 내에 같은 속성을 갖는 소규모 그룹을 구성하는 방식이다[1, 2].

3.1.1 프로토콜

1) 시스템 계수

- n, m : 각 그룹 멤버들의 수
- i, j, k, p : 그룹 멤버의 색인
- MBR_i : i번째 그룹 멤버
- N_i : MBR_i에 의해 생성된 랜덤 승수
- S, T : $\{N_1, .., N_n\}$의 부분 집합
- $\Pi(S)$: S상의 모든 요소들의 곱
- K_n : n명의 멤버들에게 나눠진 그룹 키

2) 그룹 초기 키 동의 과정

그룹 초기 키 동의는 다음과 같다

- $MBR_i \rightarrow MBR_{i+1}$: $\{g^{((N1...Ni)^{Nk})} \mid k \in [1, i]\}, g^{N1...Ni}$
- $MBR_n \rightarrow MBR_i$: $\{g^{((N1...Nn)^{Ni})} \mid i \in [1, n]\}$ (단, g는 원시근을 의미한다.)

3) 멤버 가입

본 방식은 버스형 또는 링(Ring)형 네트워크에 적합하도록 구성되어 있기 때문에 키 동의시 누가 마지막으로 키 동의에 참여하느냐에 따라 동적 또는 정적으로 구분된다.

가) 동적 그룹 제어

- $MBR_n \rightarrow MBR_{n+1}$: $\{g^{((N1...Nn)^{Nk})} \mid k \in [1, n]\}, g^{N1...Nn}$
- $MBR_{n+1} \rightarrow MBR_i$: $\{g^{((N1...NnNn+1)^{Ni})} \mid i \in [1, n]\}$

나) 정적 그룹 제어

- $MBR_{n+1} \rightarrow MBR_n$: $\{g^{((N1...Nn-1)^{Ni})} \mid i \in [1, n-1]\}, g^{N1...Nn-1}$
- $MBR_n \rightarrow MBR_{n+1}$: $\{g^{((N1...Nn)^{Ni})} \mid i \in [1, n]\}, g^{N1...Nn}$
- $MBR_{n+1} \rightarrow MBR_i$: $\{g^{((N1...Nn+1)^{Ni})} \mid i \in [1, n]\}$

4) 그룹 탈퇴

- $MBR_n \rightarrow MBR_i$: $\{g^{((N1...Nn)^{Ni})} \mid i \in [1, n-1] \wedge i \neq p\}$ (단, p는 탈퇴 멤버 색인)

3.1.2 특징

이 방식은 버스형 또는 링(Ring)형 네트워크 구조에

서 적용 가능한 기법이다. 키 분배를 위해서 각 멤버는 공개키 방식에 기반한 Diffie-Hellman 방식을 적용하고 있다. 이때 멀티캐스트 통신을 위해서 모든 멤버가 키 생성에 관여하므로, 새로운 멤버 가입 및 기존 멤버 탈퇴시 전 멤버 사이에 새로운 키를 생성 해야하는 번거로움이 발생한다. 또한 제 3자의 도청이 man-in the-middle attack에 의해 가능하다는 문제점을 안고 있다.

3.2 Iolus 방식

대규모 그룹을 여러 개의 소규모 그룹으로 분할하여 멤버쉽 변동에 따라 키 변경의 영향을 받는 멤버 수를 줄이는 방식이다[3].

3.2.1 프로토콜

1) 시스템 계수

- GSC : Group Security Controller
- GSI : Group Security Intermediary
- GSA : Group Security Agent
- K_{GSA_MBRi} : GSA와 멤버 i사이의 비밀키
- K_{SGRP}, K_{SGRP}' : Subgroup을 위한 공통키 및 Update 키
- Sig_{MBRi} : 멤버 i의 서명
- R, M : 랜덤 값 및 메시지
- GRP_END : 멀티캐스팅 종결 확인 메시지

2) 그룹 초기화

- GSC : 보안 정책관련 정보를 포함하는 Access Control List(ACL)를 작성한다.
- GSI : GSI 및 그 외의 멤버는 GSC의 ACL에 맞춰 그룹에 가입한다.

3) 그룹 가입

- 참여자들은 GSA에게 그룹 가입 요구서를 안전하게 전달한다.
- GSA는 그룹 가입 요구서를 확인하고 비밀키 K_{GSA_MBR}을 생성하여, 그룹 멤버들에게 안전하게 분배한다.
- 새로운 Subgroup 공통키 K_{SGRP}'를 생성한 후에, 다음 정보를 멤버들에게 전송한다.

  : GRP_KEY_UPDATE_JOIN = $K_{SGRP}(K_{SGRP}')$

4) 그룹 재 신임

- 그룹 멤버쉽을 계속 유지하려 할 경우, 안전한 유니캐스트 채널을 통해 그룹 재 신임 메시지를 전달해야 하며, GSA는 Network 구조가 최적이 되도록 재조정한다.

5) 그룹 탈퇴

- 그룹 탈퇴는 멤버가 LEAVE 요청서를 GSA에게 전송할 경우와 GSA가 멤버를 강제 탈퇴시키려 할 경우 발생한다.
- 그룹 탈퇴가 발생할 경우 GSA는 새로운 K_{SGRP}'를 생성하고, 다음 정보를 남아 있는 멤버에게 멀티캐스트 전송한다.

  : GRP_KEY_UPDATE_LEAVE

  $= K_{GSA\_MBR1}(K_{SGRP}') || K_{GSA\_MBR2}(K_{SGRP}') || .. || K_{GSA\_MBRn}(K_{SGRP}')$

6) 메시지 전송

- 송신자는 전송 메시지(M)를 K_{SGRP}로 암호화(유형 1)하거나, 랜덤 값(R)를 생성하여 암호화를 수행하고, $K_{SGRP}(R)$를 연접한 다음 자신의 서명(Sig_{MBRi})을 붙여(유형 2) local subgroup에게 전송한다.
- GSI는 수신 메시지를 확인한 다음, 동일 방법으로 하위 GSI에게 전송시킴으로써 정당성을 제공한다.
- 유형 2의 장점은 유형 1과는 달리 메시지 신뢰성 및 무결성을 제공한다는 것이다.

7) 키 갱신 및 멀티캐스팅 종결

- 키 갱신은 멤버 변동 시에 발생된다. 멀티캐스팅 종결은 GSC에 의해 수행되며, GRP_END 메시지를 해당 Subgroup에게 전송함으로써 멀티캐스팅 종결을 시킨다.

3.2.2 특징

본 방식은 각 멤버쉽이 Tree-Based 계층 구조로 구성된다. 각 멤버의 가입/탈퇴시 Subgroup 내에서만 키의 변경이 일어나므로, Clique 방식의 문제점을 개선하고 있다. 그러나 보안 관리 센터(GSC)의 오류 및 부정이 발생할 경우 멀티캐스트 서비스가 불가능하다. 동시에 각 Subgroup간의 통신시 중간 관리자간에 메시지 암/복호화를 별도로 수행해야 하고, 메시지 전송 유형 2를 사용할 경우 서명 확인을 위한 별도의 공개키 관리 센터 및 암호 방식을 적용해야 하는 단점이 발생한다.

3.3 Domain GKMP 방식

이 방식은 internet-draft로 제안된 그룹 키 관리 프로토콜로서, 각 그룹을 도메인 형식으로 구성하여 동적인 멤버쉽 변화에 유연성을 제공하고 있다[4, 10]. 그러나 멀티캐스트 메시지 전송을 위해 각 도메인 별로 각각의 멀티캐스트 키를 보유하고 있다. 따라서 도메인간의 메시지 전송 시 매번 암/복호화 과정을 수행해야 하는 번거로움이 발생한다.

3.4 DK 방식

이 방식은 네트워크 환경에서 인증, 권한 부여, 기밀성 및 무결성을 제공하고 송신자 키의 생성과 분배, 그룹 탈퇴 방법을 제공하는 CBT 기반 멀티캐스트 방식이다[5, 10]. 특히 Iolus 방식에서 지적되었던, 멀티캐스트 메시지 전송시 중간 관리자 사이에 발생되는 암/복호화

과정을 줄이기 위하여, 모든 멤버가 동일한 멀티캐스트 키를 보유하고 있다. 이를 통해 중간 관리자의 번거로움이 해결되고 있으나, 새로운 멤버 가입/탈퇴시 전 멤버의 멀티캐스트 키를 새로이 생성 및 전송해 주어야 하는 문제점이 생기고 있다.

4. 새로운 방식 제안

본 방식은 상기 제시되었던 요구 사항을 만족함과 동시에 기존 방식들-Clique 방식, Iolus 방식, DK 방식 및 Domain-GKMP 방식-이 안고 있던 문제점들을 해결하고 있다[9, 10].

4.1 시스템 계수

다음은 본 방식에서 사용되는 시스템 계수를 기술하고 있다.

- DKM_i : 도메인 키 관리자 i (i = 1, 2, 3, ... , k : k는 도메인 키 관리자 수)
- DKA_i : 도메인 키 중간 관리자 i (i = 1, 2, 3, ... , j : j는 도메인 키 중간 관리자 수)
- APL : 도메인 키 (중간)관리자들의 공개키 리스트
- GML : 그룹 멤버 리스트
- B_i : Border i (i = 1, 2, 3, ... , k : k는 Border의 수)
- PKM : 도메인 키 (중간)관리자들 및 Border의 공개키 관리자
- MBR_i : 그룹 멤버 i (i = 1, 2, 3, ... , n : n은 멤버의 수)
- R : 라우터
- GI : 그룹 초기자
- MKey : PKM에 의해 생성된 멀티캐스트 키
- K_{PP}, K_{PS} : PKM의 공개키와 개인키
- K_{DPi} : 각 DKM_i의 공개키
- K_{DAPi} : 각 DKA_i의 공개키
- K_{BPi} : 각 B_i의 공개키
- K_{D_DAi} : DKM_i와 DKA_i 사이의 공통키
- K_{MSi} : 그룹 멤버 MBR_i의 비밀키
- K_{DAi_Ms} : 각 DKA_i가 관리하는 멤버들과의 공통키
- ID_*, IP_*, Sig_* : *의 식별자, IP 주소 및 서명
- M : 멀티캐스팅 메시지

4.2 시스템 프로토콜

본 방식은 멤버 가입/탈퇴시 최소한의 키 갱신을 유도하기 위하여 각 그룹은 계층적인 도메인 Subgroup 형식으로 분류하여 동적인 관리를 수행한다. 또한 구조적으로 제어부와 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) 및 IPSec을 적용한다. 이는 이질적인 통신망에서 안전성과 효율성을 높이는 효과를 제공한다.

4.2.1 도메인 초기화 단계

1) DKM_i, DKA_i 및 B_i은 안전한 유니캐스트 채널을 통해 자신의 공개키를 APL에게 등록하고, PKM에게 인증을 요구한다.

- * : $(ID_*||*의\ 공개키||IP_{DKMi}) \rightarrow PKM$
  : * ∈ { DKM_i, DKA_i, B_i}

2) 각 관리자들은 APL을 통해 등록·인증된 자신의 공개키를 확인한다.

- APL : $(ID_*||K_{PS}(*의\ 공개키)||IP_*)$

3) 각 도메인은 DKM_i를 정점으로 멤버들을 분할하여 담당하는 각 DKA_i를 계층적으로 관리한다. 공개키 등록이 끝나면 도메인 상의 각 관리자들은 상호 인증을 수행한다.

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 관련된 B_i에게만 제공함으로서 신뢰성을 높이고 있다.

- PKM : $K_{BPi}(MKey||Sig_{PKM}(ID_{PKM})) \rightarrow B_i$

3) PKM은 해당 Domain에게 공개키를 이용하여 안전하게 GML을 전송한다.

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

4.2.3 그룹 멤버 가입 단계

1) DKM_i는 도메인 내에서 DKA_i와의 통신 시 사용할 K_{D_DAi}를 생성하여 유니캐스트 채널을 통하여 안전하게 DKA_i에게 전송한다.

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

2) 그룹에 멤버로 가입할 사용자들은 IPSec을 이용하여 DKA_i에게 자신을 인증하고 자신의 비밀키 K_{MSi}를 K_{DAPi}로 암호화하여 안전하게 전송한다.

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

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

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

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

5) DKA_i는 수신된 비밀키 K_{MSi}를 이용하여 각 멤버에게 K_{DAi_Ms}를 안전하게 전송해 준다. 동시에 이 $K_{DAi\ Ms}$는 DKM_i 및 Border B_i에게 안전하게 전송된다.

· DKA_i : $*(K_{DAi\ Ms}) \rightarrow MBR_i$, DKM_i, B_i

: $* \in \{K_{MSi}, K_{D\ DAi}, K_{BPi}\}$

4.2.4 멀티캐스트 메시지 전송 단계

메시지 전송 단계는 멀티캐스트 메시지 전송부로서 오직 멤버들 MBR_i와 각 도메인의 Border B_i만이 관여한다. 이 단계는 도메인 내 각 멤버들에게 메시지를 전송하는 내부 전송 과정과 타 도메인에 속한 멤버들에게 보내는 외부 전송 과정으로 분류된다. 본 절에서는 내부 전송 과정에 대해서만 기술한다.

1) 각 멤버들은 $K_{DAi\ Ms}$를 이용하여 멀티캐스트 메시지 M을 암호화한 다음 Border B_i에게 전송한다.

· MBR_i : $K_{DAi\ Ms}(M) \rightarrow B_i$

2) Border B_i는 암호화되어 수신된 정보를 복호화 한다.

· B_i : $K_{DAi\ Ms}(K_{DAi\ Ms}(M)) = M$

3) 내부 전송 과정

가) Border B_i는 복호된 멀티캐스트 메시지 M을 자신이 속한 도메인의 모든 그룹 멤버들에게 각각의 KDA_i와 그 Subgroup에 속한 멤버들 간의 공통키($K_{DAi\ Ms}$)로 암호화하여 전송한다.

· B_i : $K_{DAi\ Ms}(M) \rightarrow MBR_i'$

: $MBR_i \neq MBR_i'$

나) 멤버 MBR_i'는 $K_{DAi\ Ms}$로 수신된 정보를 복호화하여 메시지를 확인한다.

· MBR_i' : $K_{DAi\ Ms}(K_{DAi\ Ms}(M)) = M$

4.2.5 신규 멤버 가입 및 기존 멤버 탈퇴 단계

1) 신규 멤버 가입

신규 멤버 가입은 다음과 같은 과정을 통해 수행된다.

가) 그룹에 신규 멤버로 가입할 사용자들은 IPSec을 이용하여 DKA_i에게 자신을 인증하고 자신의 비밀키 K_{MSi}'를 K_{DAPi}로 암호화하여 안전하게 전송한다.

· MBR_i' : $K_{DAPi}(K_{MSi}'||Sig_{Mi}(ADD||ID_{MBRi}'||K_{MSi}')) \rightarrow DKA_i$

: ADD는 신규 가입 대상자임을 나타내는 식별자

나) 4.2.3절의 3), 4)와 동일한 과정을 수행한다.

다) GML'의 수정 내용을 확인한 다음 GML을 GML'으로 교체한다.

라) DKA_i는 수신된 비밀키 K_{MSi}'를 이용하여 신규 가입 멤버에게 $K_{DAi\ Ms}$를 안전하게 전송해 준다. 신규 멤버 가입시에는 $K_{DAi\ Ms}$에 대한 별도의 변화는 필요 없게 된다.

· DKA_i : $K_{MSi}'(K_{DAi\ Ms}) \rightarrow MBR_i'$

2) 기존 멤버 탈퇴

기존 멤버 탈퇴시에는 신규 멤버 가입 때와는 다르게 남아 있는 멤버들을 위해 기존의 $K_{DAi\ Ms}$를 갱신하여 분배한다. 이를 통해 그룹 탈퇴자로부터 기존 멤버들에 대한 안전성을 획득할 수 있다.

가) 그룹 탈퇴를 희망하는 멤버는 다음 정보를 생성하여 DKA_i에게 안전하게 전송한다.

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

: DEL은 그룹 탈퇴 희망자임을 나타내는 식별자

나) 기존의 멤버 MBR_i가 탈퇴할 경우 DKA_i는 다음과 같이 탈퇴 멤버 정보를 생성해 DKM_i에게 전송한다.

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

다) DKM_i는 DKA_i로부터 수신된 그룹 탈퇴 멤버 정보에 대해 복호 및 인증을 수행한 다음 GML의 내용을 수정한다. 수정된 GML'을 안전하게 PKM에게 전송한다.

· DKM_i : $GML \rightarrow GML'$

: $GML' = (ID_{MBR1}||\cdots||ID_{MBRi-1}||ID_{MBRi+1}||\cdots||ID_{MBRn})$

: $K_{DPi}(Sig_{DKMi}(GML')) \rightarrow PKM$

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

마) DKA_i는 새로운 공통키 $K_{DAi\ Ms}'$를 생성하여 남아 있는 기존의 멤버들 MBR_i', DKM_i 및 Border(B_i)에게 안전하게 전송한다.

· DKA_i : $K_{DAi\ Ms} \rightarrow K_{DAi\ Ms}'$

: $*(K_{DAi\ Ms}') \rightarrow MBR_i'$, DKM_i, B_i

: $* \in \{K_{MSi}, K_{D\ DAi}, K_{BPi}\}$

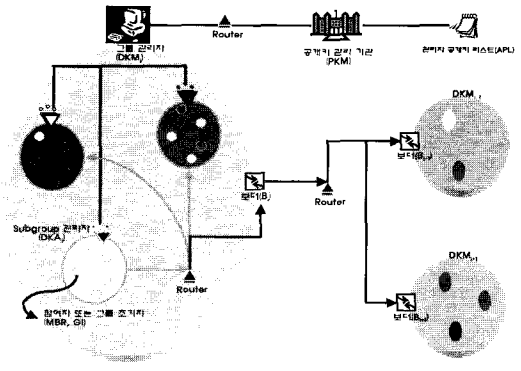

그림 1 제안된 멀티캐스트 키 관리 구조도

4.3 새로운 방식의 특징

본 제안 방식은 다음과 같은 특징을 가지고 있다.

1) Clique 방식의 문제점 해결

- 새로운 멤버 가입 및 기존 멤버 탈퇴 시 모든 멤버에게 새로운 키를 생성 및 분배하는 문제점을 해결하고 있다.
- 멤버를 도메인 상의 Subgroup으로 나누는 기법을 적용함으로서 그룹 멤버 탈퇴가 발생하는 Subgroup의 K_{DAi_Ms}만 갱신하면 된다.

2) Iolus 방식의 문제점 해결

- 도메인 관리를 위한 제어부와 메시지 전송을 위한 메시지 전송부로 구분함으로서 메시지 전송시 중간 과정에서 노출되는 것을 막는다.
- GSC의 오류 및 부정에 대한 해결 방안 제시 - Iolus 방식은 집중형 Tree Based 구조를 가지고 있으므로 최상위 노드의 오류에 대해 멤버 전체의 통신 단절을 가져 올 수 있다는 문제점이 발생하고 있다. 그러나 본 방식은 각 Subgroup을 그물형 도메인 내에 계층적으로 분포시킴과 동시에 오류에 대한 새로운 path를 지정함으로서 이 문제를 해결하고 있다.

3) Domain-GKMP 방식의 문제점 해결

- 이 방식은 도메인간의 멀티캐스트 메시지 전송시 각 인접 도메인의 키로 암/복호화가 이뤄지기 때문에 n개의 도메인에 대해 n번의 암/복호화가 이뤄진다. 그러나 제안 방식은 단 2번의 암/복화가 수행되므로 효율성을 높이고 있다.

4) DK 방식의 문제점 해결

- DK 방식은 Iolus에서 문제가 되고 있는 중간 관리자의 메시지 암/복호화의 문제점을 해결하기 위해 각 멤버가 그룹 키를 가지게 하고 있다. 그러나, 이 방식은 새로운 멤버 가입 또는 기존 멤버 탈퇴시 모든 멤버에게 새로운 그룹 키를 전송해야하는 문제점을 가지고 있다. 이에 대해 본 방식은 멤버 탈퇴 시 Subgroup의 K_{DAi_Ms}만 변경하면 되므로 DK 방식의 문제점을 해결하고 있다.

5. 각 방식별 비교 분석

다음은 기존에 제안된 그룹 키 분배 방식에 멀티캐스트 키 관리 방식을 적용했을 때 통신량과 사용자측면에서 일어나는 연산량을 구하여 각각을 비교 분석한 것이다. 통신량은 멤버들에게 키 분배가 일어날 때의 통신회수를 계산한 것이며, 연산량은 키 분배를 위해 멤버들이 수행해야 하는 연산량을 구한 것이다.

5.1 각 방식별 그룹 키 분배 방식에 따른 통신량 비교 분석

5.1.1 기존 KDC 이용 방식

기존 KDC를 이용할 경우 KDC는 각각의 멤버들과 비밀키를 공유하고 있으며, 그룹 키를 생성하고 분배한다. 이 그룹 키를 분배하기 위해서는 각 멤버들과 통신하게 되므로 n번의 통신을 하게 된다. n은 그룹 멤버의 수이다.

5.1.2 Clique 방식

이구조는 버스형 또는 링형 구조로서 그룹 키 생성을 위한 그룹 키 생성 정보 전송을 위해 n-1번의 통신을 하며, 그룹 키 전송을 위해 다시 n-1번의 통신을 한다. 따라서 그룹 키 분배를 위해 2(n-1)번의 통신회수를 갖는다.

5.1.3 Iolus 방식

이 구조는 각 그룹 멤버들을 소규모의 Subgroup으로 나누어 관리하는 방식으로 키 분배를 위해 GSA(Group Security Controller)와 Subgroup사이의 통신이 필요하며, Subgroup과 멤버 사이의 통신이 필요하다. 따라서 Subgroup 관리자를 j라하고 멤버를 s라 할 때 그룹 키 분배를 위한 통신회수는 js+j가 된다.

5.1.4 DK 방식

이 구조는 Iolus와 같은 구조를 갖고 있으며, 다른 점은 라우터에서 발생하는 암/복호화에 따른 오버헤드를 줄인 것이다. 따라서 이 구조를 그룹 키 분배 방식에 적용할 경우 Iolus와 같은 통신회수를 갖는다.

5.1.5 KL 방식

이 방식은 코어 기반 트리(CBT)를 이용하고 있으며, 그룹 키 분배는 기존의 KDC 이용 방식과 비슷하게 코어에서 확인과정과 그룹 키 분배를 담당하므로 2n번의 통신회수를 갖는다. 각 그룹 키 분배 방식들을 적용했을 경우 기존 KDC를 이용했을 때와 동일한 통신회수를 갖는다.

표 1 각 적용 방식별 통신량 비교

구조 \ 방식	Diffie-Hellman 방식	ITW 방식	KO 방식	BD 방식	PL 방식
기존 KDC	2n	5n	3n	4n	2n
Clique	2(n-1)	5(n-1)	3(n-1)	4(n-1)	2(n-1)
Iolus	2(js+j)	5(js+j)	3(js+j)	5(js+j)	2(js+j)
DK	2(j+n)	5(j+n)	3(j+n)	3(j+n)	2(j+n)
KL	2n	5n	3n	4n	2n
제안방식	2js	5js	3js	5js	2js

k:도메인 수, j: 중간 관리자(중계 라우터) 수, s:subgroup 멤버 수, n:그룹 멤버들의 수

5.1.6 제안 방식

본 방식에서는 각 그룹 멤버들을 도메인 상의 Subgroup으로 나누는 기법을 이용하고 있다. 동시에 그룹 멤버 관련 키 생성 시 오직 중간 키 관리자만이 관여하므로 js의 통신회수를 갖는다. j는 Subgroup 관리자이고 s는 멤버의 수이다.

위의 표 1은 각 적용 방식별 통신량을 보여주고 있다. 여기서 각 그룹 키 분배 방식에 있어서의 통신량이 각 구조에 적용했을 때 동일하게 나오고 있으나 BD방식은 각 구조에 따라 다른 것을 볼 수 있다. 이것은 중계 라우터가 있는 방식에서는 라우터에서 사용자 확인을 위한 통신이 필요하지만 중계 라우터가 없는 방식과 중계 라우터가 있더라도 사용자 확인을 하지 않는 방식에서는 이러한 통신이 없기 때문에 통신량이 다르게 나오고 있다. 각 적용 방식별 통신량은 표에서 나타나 있듯 각 구조에 Diffie-Hellman 방식과 제안 방식인 PL 방식을 적용했을 때 다른 방식들에 비해 좋은 것으로 나타나고 있다. 그러나 Diffie-Hellman 방식은 안전성과 보안성 및 멤버의 가입 탈퇴에 따른 그룹 키 재분배의 문제점을 가지고 있다. 반면 제안 방식은 각 구조에서 나타난 문제점들을 해결하고 있으며 멀티캐스팅 키 분배를 위한 요구 사항들을 만족하고 있기 때문에 안전성과 효율성 측면에서 좋다고 할 수 있다. 또한 제안 구조에 PL 방식을 적용했을 때 안전성을 보장하면서 다른 방식들에 비해 최적의 통신량을 보이고 있다.

5.2 각 방식별 그룹 키 분배 방식에 따른 연산량 비교 분석

각 구조를 그룹 키 분배 방식에 적용했을 경우 사용자 측면에서의 연산량을 구하여 비교 분석한 결과이다. 먼저 각 키 분배 방식에 따른 지수승(Exponential) 연산량을 구해보면 다음과 같다.

- U = 2k : Diffie-Hellman 방식의 Exponential 연산량
- W = nc : ITW 방식의 Exponential 연산량
- X = ck(3+n)+6c : KO 방식의 Exponential 연산량
- Y = c(2n+4) : BD 방식의 Exponential 연산량
- Z = c(n+2)+k(c+1) : 제안(PL) 방식의 Exponential 연산량

여기서 c는 상수이고 k는 키 크기이다. 각 방식의 Exponential 연산량은 키 분배에 참여하는 멤버와 라우터에서 계산되어 지는 연산량이므로 각 방식별 키 분배 방식에 따른 연산량을 구해보면 다음 표 2와 같다. 여기서 중계 라우터간의 키 분배에 있어 사용되어 지는 키가 불확실하며, 사용자 측면에서의 연산량을 살펴보기 때문에 라우터 간의 키 분배 연산량은 고려하지 않는다.

표 2 각 적용 방식별 연산량 비교

방식 / 구조	Diffie-Hellman 방식	ITW 방식	KO 방식	BD 방식	제안 방식 (PL 방식)
기존 KDC	U(n)	W(n)	X(n)	Y(n)	Z(n)
Clique	U(n)	W(n)	X(n)	Y(n)	Z(n)
Iolus	U(js)	W(js)	X(js)	Y(js)	Z(js)
DK	U(n)	W(n)	X(n)	Y(n)	Z(n)
KL	U(n)	W(n)	X(n)	Y(n)	Z(n)
제안방식	U(js)	W(js)	X(js)	Y(js)	Z(js)

k:도메인 수, j: 중간 관리자(중계 라우터) 수, s:subguoup 멤버 수, n:그룹 멤버들의 수

위의 표에서 보면 n은 그룹 멤버들의 수이고 js는 라우터와 Subgroup의 멤버 수 이므로 n과 js는 차이가 없다고 볼수 있으며, Exponential 연산량에서 Diffie-Hellman 방식과 ITW 방식이 연산량에 있어서 좋은 것으로 나와 있다. 그러나 이 방식들은 안전성이나 효율성 및 멤버 가입/탈퇴에 따른 그룹 키 재분배에 있어 문제점을 가지고 있다. 그 외의 다른 방식들은 제안 방식에 비해 연산량에 있어 비효율적이다

5.3 멀티캐스트 키 분배 방식별 비교 분석

다음은 멀티캐스트 키 관리 구조 요구 사항에 기초하여 기존 방식과 제안 방식을 비교 분석한 결과이다.

표 3 각 방식별 비교 분석

대상 / 항목	Clique	Iolus	GKMP	DK	제안 방식
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

6. 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.

본 논문에서는 이러한 취약성을 극복하기 위해 필요한 요구 사항을 살펴보았으며, 기존의 방식이 이에 어떻게 대처하는지 고찰하였다. 또한 요구 사항 및 기존 방식의 문제점을 해결할 수 있는 새로운 멀티캐스트 키 관리 구조를 제안하였다.

기존 방식들의 경우, 키 분배 및 갱신 시 구조적인 문제로 인해 확장성 및 효율성 부분에서 문제점을 안고 있으며, 중간 관리자들의 오류 및 부정에 대해 취약점을 제공하고 있다. 이에 대해 새로이 제안된 멀티캐스트 키 관리 구조는 키 분배 및 갱신 시 안전성과 효율성 및 확장성을 제공하기 위해 PKI 및 IPSec을 도입하였으며, 도메인을 그물형 Subgroup으로 분할하여 계층적으로 관리한다. 동시에 중간 관리자의 오류 및 부정에 대해 신뢰성을 확보하는 측면에서 멀티캐스트 메시지는 오직 보더(Border)를 통해 송·수신된다는 특징을 가지고 있다. 이러한 특성들을 근거로 본 제안 방식은 멀티캐스트 키 관리 요구 사항들을 모두 만족하고 있으며, 안전성, 효율성 및 확장성 측면에서 기존 방식들보다 우수함을 알 수 있었다. 향후 이들 멀티캐스트 키 관리 분야에 대한 다각적인 연구를 통해 더욱 다양해지는 그룹 기반 통신 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] H. Harney and C. Muckenhirn, "Group Management Protocol(GKMP) Architecture," IETF RFC 2094, 1997.

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

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

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

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

[9] 박희운, 이임영, "효율적인 회의용 키 분배 방식에 관한 연구", 한국통신정보보호학회 춘계지부, 1999.

[10] 박희운, 이임영, "효율적인 멀티캐스트 키 관리 구조 제안 및 효율성 분석", 한국정보처리학회 춘계 학술발표대회, 2001, pp.367~370.

박 희 운

1997년 2월 순천향대학교 컴퓨터공학부 졸업. 1999년 2월 순천향대학교 전산학 전공 석사. 1999년 3월 ~ 현재 순천향대학교 전산학전공 박사과정. 관심분야는 암호이론, 컴퓨터 보안

이 임 영

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. 2001년 3월 ~ 현재 순천향대학교 전자상거래 S/W 연구센터 센터장. 관심분야는 암호이론, 정보이론, 컴퓨터 보안

박 원 주

1998년 충남대학교 정보통신공학과 졸업(공학사). 2000년 충남대학교 정보통신공학과 졸업(공학석사). 2000년 한국전자통신연구원 정보보호연구본부 네트워크보안연구부/연구원. 관심분야는 IPsec, VPN, Secure multicasting, Multicasting key management

이 종 태

1984년 2월 서울대학교 물리교육학과 졸업. 1991년 10월 Indiana University 물리학과 박사. 1992년 1월 ~ 2001년 3월 한국전자통신연구원 책임연구원. 2001년 4월 ~ 현재 국가보안기술연구소 책임연구원. 관심분야는 통신정보보호, 인터넷 보안, 양자암호

손 승 원

1984년 경북대학교 전자공학과 졸업(공학사). 1994년 연세대학교 전자공학과 졸업(공학석사). 1999년 충북대학교 전자공학과 졸업(공학박사). 1991년 ~ 현재 한국전자통신연구원 정보보호연구본부 네트워크보안연구부 부장/책임연구원. 관심분야는 IC Card, Biometry, Active Network