2001년 한국정보처리학회 춘계 학술발표논문집 제8권 제1호

# 효율적인 멀티캐스트 키 관리 구조 제안 및 효율성 분석

박희운°, 이임영
순천향대학교 정보기술공학부
heeun@cse.sch.ac.kr, imylee@sch.ac.kr

# A Proposing The Efficient Multicast Key Management Structure and Analysis The Efficiency

Hee-Un Park°, Im-Yeong Lee
Division of Information Technology Eng. Soonchunhyang University

**요 약**

컴퓨터의 보급과 통신의 발전은 인터넷과 같은 공개 네트워크 상에서 그룹 기반 통신 응용 서비스에 관한 요구를 증가시키고 있다. 이에 따라 멀티캐스트 기반 구조에 관한 연구가 활발히 진행되고 있지만, 멀티캐스트 구조에 대한 안전성과 효율성 및 확장성 부분에 대한 해결책은 아직 미비한 상태이다. 본 연구에서는 기존의 대표적인 멀티캐스트 키 관리 구조를 고찰함과 동시에 안전성 및 확장성을 분석한다. 이에 기초해 확장성을 제공하는 안전한 멀티캐스트 키 관리 구조를 제안하고 기존의 그룹 키 분배 방식들을 적용해 봄으로서 기존 멀티캐스트 키 관리 구조와 비교 분석한다.

## 1. 서론

컴퓨터의 보급 확산과 공용 네트워크의 발전을 통해 세계 곳곳의 정보를 한눈에 볼 수 있는 시대가 도래하고 있다. 이러한 상황에서 사용자들은 단순한 통신에서 벗어나 다자간 통신 회의, 의료 원격 진단 및 상담 등 다양한 서비스를 요구하고 있다. 그러나 기존의 일대일 통신 방식으로는 이러한 서비스를 제공하는데 제약 사항이 생길 수밖에 없다. 이를 해결하기 위하여 현재 각광 받고 있는 방식 중의 하나가 멀티캐스트 기법이다.

멀티캐스트란 그룹에 참가한 멤버들을 대상으로 한 송신자로부터 그룹 참여자들 모두에게 안전한 데이터 전송을 수행하는 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 보안상의 취약성에 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 다뤄져야 한다. 동시에 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 고려한다. 또한 기존의 멀티캐스트 키 관리 구조들을 고찰함과 동시에 새로운 방식을 제안하여 안전성, 효율성 및 확장성 부분에서 비교 분석을 수행한다.

## 2. 멀티캐스트 키 관리를 위한 요구사항

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

- 무결성 : 멀티캐스트 정보는 전송 도중에 불법적인 제 3자로부터 위조 및 변경되어서는 안된다.
- 인증 : 송·수신 정보의 무결성 확인 및 정당한 참여자들로부터 생성 및 수신되었음을 확인가능 해야 한다.
- 접근 제어 : 정당한 그룹의 소속원만이 멀티캐스트 정보에 접근할 수 있다.
- 부인 봉쇄 : 서비스 참여자간에 전송 및 수신 사실을 부인할지라도 당사자 및 제 3자의 확인이 가능해야 한다.
- 비밀성 : 전송 및 저장되는 멀티캐스트 정보는 불법적인 제 3자로부터 보호되어야 한다.
- 공정성 : 멀티캐스트 키의 접근은 허가된 그룹 참여자만이 가능하며, 키 갱신 프로토콜은 필수적이다. 이를 위해 서버의 독단 및 제 3자와의 불법적 결탁을 방어하기 위한 공정성이 확보되어야 한다.
- 확장성 : 멀티캐스트 서비스 그룹 참여자의 변동에 따른 동적인 키 관리 기법이 필요하다.

3. 기존의 그룹 키 분배 방식 분석

본 장에서는 기존에 제안된 몇몇 대표적인 그룹 키 분배 방식들의 특징들을 살펴보고, 멀티캐스트 키 관리 방식에 적용할 경우 효율성 비교 분석에 이용한다.

3.1 Diffe-Hellman방식

이 방식은 1976년에 Diffe-Hellman에 의해 제시된 방식으로서, 별도의 키 생성 기관이 필요 없지만 프로토콜 상에서 제 3자에 의한 man-in the-middle attack이 허용된다[1]. 이는 키의 출처를 확인할 방법이 없기 때문에 발생된 문제이다. 또한, 키 생성 과정에서 각각의 가입자들 사이에 하나씩의 공통키를 생성해야 하므로, n명의 가입자에 대해 ${}_nC_2$개의 키가 필요하다. 따라서 통신 회수는 회의 참여자의 수에 의존하는 단점을 가지고 있다.

3.2 Ingemarsson-Tang-Wong(ITW)방식

본 방식은 n명의 가입자들 사이에 하나의 비밀 통신키를 생성하는 방식으로 이산 대수의 어려움에 근거한다[2]. 각 가입자로부터 온 전송 정보가 정당한 사용자로부터 온 것인지 판단할 근거가 없다는 문제점을 가지고 있지만, 통신 회수를 3회로 줄임으로서 효율성을 높이고 있다.

3.3 Koyama-Ohta(KO)방식

이 방식은 ID-based한 공개키 암호 방식을 이용하여 메시지 인증이 가능한 그룹 키 분배 방식이다[3][5]. 본 방식은 제 3자의 불법 행위를 방지하기 위해 인증성을 제공하고 있기는 하지만, 완벽하지는 않다. 즉, 네트워크 상의 불법 행위자에 의해 양방향 위장 공격이 수행될 경우 정확한 키를 제공하지 못할 수도 있다.

3.4 Burmester-Desmedt(BD)방식

이 기법은 이산 대수에 근거한 공개키 암호 시스템에 기반을 둔 방식으로 사용자 인증 및 그룹 키 계산이 가능한 방식이다[4]. 또한 가입자 수와는 무관한 통신 회수를 갖는 장점을 가지고 있다. 그러나, 인증을 위해서는 모든 가입자들의 공개키를 가지고 있어야 한다는 문제점을 가지고 있으며, 키 분배 과정과 인증 과정이 별도로 수행됨으로서 비효율적인 측면을 가지고 있다.

3.5 Park-Lee(PL) 방식

본 제안 방식은 ID-based한 공개키 암호 시스템에 근거한다[5]. 기존의 방식에 비하여 각 참여자는 키 인증 부분과 Bridge를 통해 안전성을 확보하고 있다. 또한 키 생성시 2번 정도의 통신 회수를 요구함으로서 효율성을 높이고 있다.

4. 기존의 멀티캐스트 키 관리 방식 분석

본 장에서는 기존에 제안되어진 멀티캐스트 키 관리 구조에 대한 주요 사항 및 문제점을 제시한다.

4.1 Clique 방식

이 방식은 선형 또는 Ring 형 네트워크 구조에서 적용 가능한 기법으로서, 키 분배를 위해서 각 멤버는 공개키 방식에 기반한 Diffie-Hellman 방식을 적용하고 있다[7][8]. 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 man-in the-middle attack에 의해 제 3자에 의한 도청이 가능하다는 문제점을 안고 있다.

4.2 Iolus 방식

본 방식은 각 멤버쉽이 Tree-Based 계층 구조로 구성된다[9]. 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. 또한 각 Subgroup간의 통신시 중간 관리자간에 메시지 암/복호화를 별도로 수행해야 하는 단점이 발생한다.

4.3 Domain GKMP 방식

이 방식은 각 그룹을 도메인 형식으로 구성함으로서 동적인 멤버쉽 변화에 유연성을 제공하고 있다[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.

4.4 DK 방식

이 방식은 Iolus 방식에서 지적되었던, 멀티캐스트 메시지 전송시 중간 관리자 사이에 발생되는 암/복호화 과정을 줄이기 위하여 제안된 방식이다[11]. 즉 모든 멤버가 동일한 멀티캐스트 키를 보유함으로서, 중간 관리자의 번거로움이 해결되고 있다. 그러나 새로운 멤버 가입/탈퇴시 전 멤버의 멀티캐스트 키를 새로이 생성 및 전송해 주어야 하는 문제점이 생기고 있다.

5. 새로운 방식 제안

본 방식은 상기 제시되었던 요구 사항을 만족함과 동시에 기존 방식들의 문제점들을 해결하고 있다.

5.1 구성 요소 및 시스템 계수

다음은 본 방식에서 사용되는 시스템 계수 및 구성 요소를 기술하고 있다.

- $DKM_i$ : 도메인 키 관리자 i
- $DKA_i$ : 도메인 키 중간 관리자 i
- GML : 그룹 멤버 리스트
- $SGB_i$ : Subgroup Border i
- R, $DMB_i$ : 라우터 및 도메인 Border i
- $MGB_i$ : 멀티캐스트 그룹 Border i
- PKM : 각 관리자들 및 Border의 공개키 관리자
- $MBR_i$, GI : 그룹 멤버 i 및 그룹 초기자
- MKey : PKM에 의해 생성된 멀티캐스트 키
- $K_{DPi}$, $K_{DAPi}$ : $DKM_i$의 공개키 및 $DKA_i$의 공개키
- $K_{BPi}$ : 각 $B_i$의 공개키
- $K_{D\_DAi}$ : $DKM_i$와 $DKA_i$ 사이의 공통키
- $K_{MSi}$ : 그룹 멤버 $MBR_i$의 비밀키
- $K_{DAi\_Ms}$ : 각 $DKA_i$가 관리하는 멤버들과의 공통키
- Hdr : 각 그룹의 식별 정보
- $ID_*$, $Sig_*$, $IP_*$ : *의 식별자, 서명 및 IP 주소
- M : 멀티캐스팅 메시지

5.2 시스템 프로토콜

본 방식은 멤버쉽 가입/탈퇴시 최소한의 키 갱신을 유도하기 위하여 각 그룹은 도메인 형식으로 분류하여 동적

인 관리를 수행한다. 또한 구조적으로 제어부와 데이터 전송부로 구분함으로서 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 구조를 적용한다. 이는 이질적인 통신망 상에서 안전하면서도 적용이 용이하여 효율성 및 이식성을 높이는 효과를 제공한다.

1) 도메인 초기화 단계

①$DKM_i$, $DKA_i$ 및 각 Border는 안전한 유니캐스트 채널을 통해 자신의 공개키 인증서를 $PKM_i$으로부터 수신한다.

②각 도메인은 $DKM_i$를 정점으로 멤버들을 분할하여 담당하는 각 $DKA_i$를 계층적으로 관리한다. 공개키 인증서 수신이 끝나게 되면 도메인 상의 각 관리자들은 상호 인증을 수행한다.

2) 그룹 초기화 단계

①GI는 그룹 멤버 리스트(GML)를 작성하여 자신의 식별자 $ID_{GI}$와 함께 서명을 수행하여 $PKM_i$에게 전송한다.

$Sig_{GI}(ID_{GI}||GML) \rightarrow PKM_i$, $GML = (ID_{MBR1}||\cdots||ID_{MBRn})$

②$PKM_i$은 서명 확인을 통해 GI 및 GML을 인증하고 멀티캐스트 서비스를 위한 MKey를 생성한다. 단, MKey는 그룹이 형성될 때, 오직 관련된 Border들에게만 제공함으로서 신뢰성을 높이고 있다.

③PKM은 해당 Domain에게 공개키를 이용하여 안전하게 GML을 전송한다.

3) 그룹 멤버 가입 단계

①$DKM_i$는 도메인 내에서 $DKA_i$와 통신 시 사용할 $K_{D_DAi}$를 생성하여 유니캐스트 채널을 통하여 안전하게 $DKA_i$에게 전송한다.

②그룹에 멤버로 가입할 사용자들은 자신의 서명을 이용하여 $DKA_i$에게 자신을 인증하고 자신의 비밀키 $K_{MSi}$를 $K_{DAPi}$로 암호화하여 안전하게 전송한다.

③$DKA_i$는 가입 대상자들로부터 받은 메시지를 복호화하여 인증을 수행하고 그룹 가입 멤버 리스트를 생성해 $DKM_i$에게 전송한다.

④$DKM_i$는 각 $DKA_i$로부터 수신된 그룹 가입 멤버 리스트에 대해 복호 및 인증을 수행한 다음 GML과 비교 확인한다.

⑤$DKA_i$는 수신된 비밀키 $K_{MSi}$를 이용하여 각 멤버에게 $K_{DAi_Ms}$를 안전하게 전송해 준다. 동시에 이 $K_{DAi_Ms}$는 $DKM_i$ 및 $SGB_i$에게 안전하게 전송된다.

4) 멀티캐스트 메시지 전송 단계

메시지 전송 단계는 멀티캐스트 메시지 전송부로서 오직 멤버들 $MBR_i$와 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 문서에서는 내부 전송 과정 중 도메인 전체 메시지 전송에 대한 내용을 기술한다.

①각 멤버들은 $K_{DAi_Ms}$를 이용하여 멀티캐스트 메시지 M을 암호화한 다음 Border $SGB_i$에게 전송한다.

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

②$SGB_i$는 암호화되어 수신된 정보를 복호화하여 Hdr를 확인하고 Hdr이 없다면 멀티캐스트 메시지 M을 MKey로 암호화하여 각 $SGB_i$'에게 전송한다.

③각 $SGB_i$'는 수신된 정보를 복호화하고 이를 자신이 속한 그룹의 공통키로 암호화하여 그룹 멤버들에게 전송한다.

④각 Subgroup의 멤버 $MBR_i$'는 $K_{DAi\_Ms}$'로 수신된 정보를 복호화하여 메시지를 확인한다.

기타 메시지 전송은 상기 프로토콜에 기초해 수행된다.

5) 신규 멤버 가입 및 기존 멤버 탈퇴 단계

①신규 멤버 가입은 3) 그룹 멤버 가입 단계와 같은 과정을 수행한다.

②기존 멤버 탈퇴 시에는 $DKA_i$가 새로운 $K_{DAi\_Ms}$'를 생성하여 남아 있는 기존의 멤버들 $MBR_i$', $DKM_i$ 및 $SGB_i$에게 안전하게 전송함으로서 키 갱신을 수행한다.

6) 그룹 합병 및 분할

①그룹 합병이 발생하면, 해당 그룹 관리자들은 자신의 그룹에 그룹 합병 사실을 알리고, 합병 그룹 멤버들의 리스트를 새로이 구성하여 통고한다. 합병 과정에서 하나의 그룹 관리자만이 합병 그룹의 관리를 담당한다. 합병 그룹 관리자는 새로운 공통키를 생성하여 멤버, 해당 Border에게 안전하게 분배하면 된다.

②분할 요구가 발생하면, Subgroup 키 관리자는 새로운 그룹 리스트와 기존의 멤버 리스트를 갱신하여 $DKM_i$에게 전송한다. $DKM_i$는 새로운 Subgroup의 관리자 $DKA_i$를 선정한다. 기존의 Subgroup 관리자 및 $DKA_i$는 각각 새로운 공통키를 생성하여 그룹 및 Border에게 안전하에 전송함으로서 가능하다. .

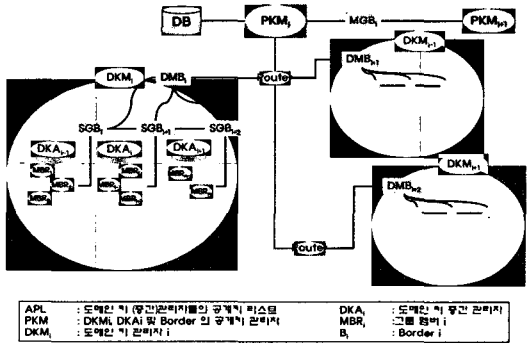


그림 1. 제안된 멀티캐스트 키 관리 구조도

5.3 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 가입 탈퇴가 발생하는 Subgroup의 $K_{subi}$만 갱신하면 된다.

2) Iolus 방식의 문제점 해결

: 도메인 관리를 위한 제어부와 메시지 전송을 위한 데이터 전송부로 구분함으로서 메시지 전송시 중간 과정에서 노출되는 것을 막는다.

: GSC의 오류 및 부정에 대한 해결 방안 제시 - 본 방식은 각 Subgroup을 그물형 도메인 내에 계층적으로 분포시킴과 동시에 오류에 대한 새로운 path를 지정

함으로서 이 문제를 해결하고 있다.

3) Domain GKMP 방식의 문제점 해결

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

4) DK 방식의 문제점 해결

: 본 방식은 멤버 가입/탈퇴 시 Subgroup의 공통키만 변경하면 되므로 DK 방식의 문제점을 해결하고 있다.

6. 각 방식별 비교 분석

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

표 1. 각 멀티캐스트 키 관리 방식별 비교 분석

| 항목 / 대상 | Clique | Iolus | GKMP | DK | 제안 방식 |
|---|---|---|---|---|---|
| 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 | m | n | 1 | 2 |

n : 도메인 수 m : 중간 관리자(중계 라우터) 수

다음의 표 2, 및 표 3은 기존의 그룹 키 분배 방식들을 멀티캐스트 키 관리 방식들 및 제안 방식에 적용할 경우 통신 및 연산량 효율성들을 비교 분석한 결과이다.

표 2. 각 적용 방식별 통신량 비교

| 방식 / 구조 | Diffie-Hellman | 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) |
| 제안방식 | 2js | 5js | 3js | 5js | 2js |

표 3. 각 적용 방식별 연산량 비교

| 방식 / 구조 | Diffie-Hellman | ITW 방식 | KO 방식 | BD 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) |
| 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

7. 결론

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 멀티캐스트 키 관리 방식이 어떻게 대처하는지 고찰하였다. 또한 기존의 그룹 키 분배 방식들을 고려하여, 요구 사항 및 기존 방식의 문제점을 해결할 수 있는 새로운 멀티캐스트 키 관리 구조를 제안하고 분석하였다. 이를 통해 향후 더욱 다양해지는 멀티캐스트 관련 서비스 분야에서 적극적으로 대처할 수 있으리라 기대된다.

참고문헌

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

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

[3] K. Koyama and K. Ohta, "Identity-based conference key distribution systems," Proceedings of Crypto '87, lecture Notes in Computer Science no. 293, Springer-Verlag, 1988, pp.175-184.

[4] M. Burmester and Y. Desmedt, "A Secure and Efficient Conference Key Distribution Systems," EUROCRYPT '94, pp.279-290

[5] 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, 1988, pp.429-433.

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

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

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

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

[10] H. Harney and C. Muckenhirn, "Group Management Protocol(GKMP) Architecture," IETF RFC 2094, 1997.

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