안전한 인터넷 멀티캐스트를 위한 확장성 있는 분산 그룹 키 분배 기법

(Scalable Distributed Group Key Distribution Scheme for Secure Internet Multicast)

장 주 만 † 김 태 윤 ††
(Ju-Man Jang) (Tai-Yun Kim)

요 약 보다 높은 대역폭에서 안전한 멀티캐스트 통신을 하고자 욕구는 기업, 정부, 그리고 인터넷을 사용하는 모든 단체에서의 고조되고 있는 주요 관심사이다. 멀티캐스트 환경에서 보안성을 제공하기 위해 최근까지 진행되어 오고 있는 연구는 주로 그룹 키 분배 기법에 관한 것들이다[1,3,4,5]. 본 논문에서는 현재까지 진행되어 오고 있는 여러 가지 그룹 키 분배 기법들에 대해 살펴보고, 보안성과 확장성을 제공해 주는 새로운 인터넷 멀티캐스트 그룹 키 분배 기법을 제안한다. 또한 제안한 기법을 기반으로 현재 사용되는 멀티캐스트 응용 프로그램에 접목하여 실험 결과를 분석한다. 실험 결과를 통해 멀티캐스트 그룹 가입과 탈퇴에 대한 키의 분배, 재분배에 관련된 처리 시간이 최소화됨을 알 수 있다.

Abstract The need for high bandwidth, very dynamic secure internet multicast communications is increasingly evident in a wide variety of commercial, government, and internet communities. One of the most recently researches is mainly about the group key distribution schemes[1,3,4,5]. In this paper, we survey related group key distribution schemes and propose a new scalable distributed group key distribution scheme which is one of the most important parts in internet multicast environment. Then, we add this scheme to the existing multicast applications and analysis the test results. The proposed SDGD minimizes the times required to distribute and redistribute keys for joining and leaving the multicast group.

1. 서 론

인터넷과 사설 인트라넷은 비즈니스, 정부와 군사기관 통신을 위해 많이 사용되며, 증가 속도 또한 매우 빠르다. 이러한 네트웍을 통한 정보의 흐름에는 인증이 필요하고 변조나 노출을 방지하기 위해 암호화가 필요하다. 멀티캐스트 환경에서는, 메시지에 대한 하나의 복사본만을 전송함으로써 멀티캐스트 그룹의 모든 회원이 수신할 수 있고, 단 하나의 그룹 키로 멀티캐스트 통신을 보호받을 수 있다[7].

† 학생회원 : 고려대학교 컴퓨터학과
jmjang@netlab.korea.ac.kr
†† 종신회원 : 고려대학교 컴퓨터학과 교수
tykim@netlab.korea.ac.kr
논문접수 : 1999년 8월 11일
심사완료 : 1999년 11월 26일

멀티미디어 화상회의와 같은 환경에서는 연결지향 접근방법을 이용하므로 심각한 단점을 가지게 되는데, 수많은 참가자를 갖는 세션으로 확장하지 못한다는 점이다. n명의 참가자들을 위해 $O(n^2)$의 연결이 필요하며, 화상회의 중 가입과 탈퇴는 모든 참가자들에게 매번 알려야 하기 때문이다. 연결이 끊기거나 새로이 설정된다면, 응용 프로그램은 더 많은 연결 관리를 제어해야만 한다. 멀티캐스트는 이러한 문제를 해결해 준다. 멀티캐스트 세션은 멀티캐스트 그룹 주소로 이뤄진다. 어떠한 호스트이든지 해당 멀티캐스트 주소를 통해 간단하게 멀티캐스트 그룹으로 전송이 가능하다. 전송자는 수신자의 위치나 IP 주소에 대해서 알 필요가 없다. 단지 호스트는 해당 멀티캐스트 그룹에 가입함으로써 세션에 참여할 수 있다. 본 논문에서는 보안성이 제공되는 멀티캐스트 환경을 구축하기 위해 그룹 키 분배 기법을 중심으로, 2장에서 현재까지 진행되어 온 관련 연구들을 살

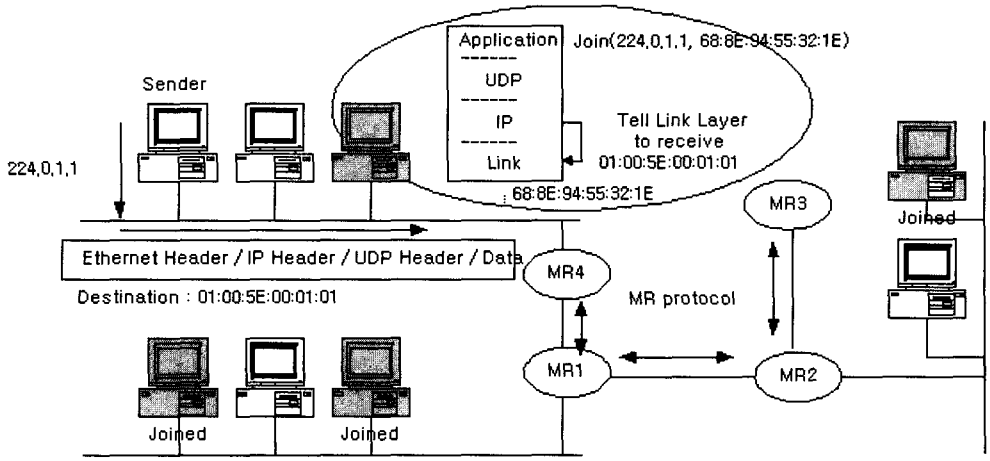

그림 1 인터넷 멀티캐스트 환경

펴보고, 3장에서는 제안한 확장성 있는 분산 그룹 키 분배 기법의 조건에 대해 기술하고, 4장에서는 실험에 필요한 환경 구현하기 위한 설계에 대해 기술하고, 5장에서 실험 환경 구현을, 6장에서는 실험 결과를 토대로 분석한다. 마지막으로 7장에서는 결론 및 향후 연구 방향을 제시한다.

2. 관련 연구

본 장에서는 현재까지 진행되어 온 멀티캐스트 그룹 키 분배 기법들을 대상으로 그룹 키 분배 기법에 대해 확장성 및 여러 가지 측면에서 분석해 보고, 연구 결과를 토대로 확장성 있는 분산 그룹 키 분배 기법을 제안하고자 한다.

2.1 GKMP(Group Key Management Protocol)

GKMP 기법은 멀티캐스트 그룹의 회원들을 관리하기 위한 대칭키를 생성하여 관리한다[2]. 이 프로토콜에서는 각각의 멀티캐스트 그룹을 그룹 컨트롤러(Group Controller)가 관리한다. 그룹 컨트롤러 역시 그룹 회원으로서, 여러 가지 주요한 프로토콜 동작을 수행한다. 예를 들면, 키 생성, 키 분배와 그룹 키 재생성(rekey) 메시지를 전달하는 역할을 하며, 또한 진행 과정에 대한 보고(report)도 담당한다. 그룹 컨트롤러는 선택된 그룹 회원와 JOINT를 통해 그룹 키를 생성한다. 각 그룹 컨트롤러와 회원만이 알고 있는 그룹 키를 통해 멀티캐스트 그룹 외부로부터 보안성을 제공해 주게 된다. 이 기법에서는 그룹 컨트롤러가 모든 그룹 회원에 대한 키 분배를 전담하므로 확장성이 떨어진다.

2.2 SMKD(Scalable Multicast Key Distribution scheme)

일반적으로, 키 분배 기능은 중앙의 네트워 호스트나, 키 분배 센터(Key Distribution Center)에서 전담해 왔다. 그러나 이러한 기법들은 광범위 멀티캐스팅에 대한 확장성이 결여되어 있다[4]. DVMRP와 MOSPF등과 같은 네트워 계층 멀티캐스트 프로토콜들은 보안이 제공되지 않아, 단지 IP자체에서 제공하는 보안에 의존해야 한다. 그러나, SMKD는 Core-Base Tree(CBT) 멀티캐스트 라우팅 프로토콜을 기반으로 구성되어, 확장성 있는 접근을 통해 CBT 그룹 트리에 안전하게 참여(joining)할 수 있게 해준다. IP 멀티캐스트 기법을 이용하여 DVMRP와 MOSPF와 같은 소스기반 전송 트리를 이용하지 않고, 한 그룹에 대하여 하나의 공유 트리를 사용한다. 공유 멀티캐스트 전송 트리는 여러 개의 핵심 라우터(core routers)들로 구성된다.

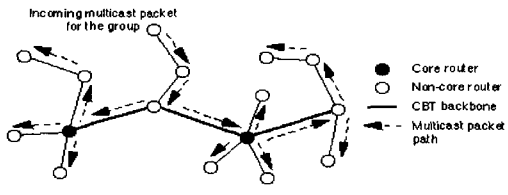

그림 2 CBT 멀티캐스트 라우팅 기법

CBT 트리가 초기화되면, 트리의 핵심 라우터는 그룹 컨트롤러처럼 작동하여 그룹 세션 키와 키 암호화 키를

생성한다[6]. 라우터가 분배 트리에 참여하게 되면, 가입 멤버들을 인증하는 기능을 대신하며, 그룹 키를 분배해 준다. 그러나 SMKD는 핵심 라우터를 선택하기 위한 별도의 알고리즘이 필요하는 문제와 핵심 라우터 주변에 트래픽이 집중되는 단점이 있다.

2.3 Iolus

Iolus 키 분배 기법에서는 멀티캐스트 그룹을 계층적으로 배열된 서브그룹들로 나눈다[5]. SDT(Secure Distribution Tree)를 만들고, 최상위에 GSC(Group Security Controller)를 두어 하위 레벨의 서브 그룹의 GSIs(Group Security Intermediaries)과 정보를 주고받는다. 여기서 GSIs는 해당 서브 그룹을 각각 나누어 담당하여 관리한다. 각각의 서브 그룹은 관리자가 선택한 고유의 서브키를 가지게 된다. GSIs는 자신의 서브 그룹과 좀 더 상위 레벨의 서브 그룹의 키들을 알고 있어 상위 레벨로의 메시지 송수신이 용이하다. 단점으로는 여러 계층을 거치는 동안 GSIs로부터 각각의 패킷을 복호화하고 재 암호화하는데 지연이 발생하는 점과 별도의 SDT를 구성하고 정보를 유지해야 하는 단점이 있다.

3. 확장성 있는 분산 그룹 키 분배 기법

3.1 확장성 있는 분산 그룹 키 분배 기법의 조건

중앙 집중식 그룹 키 분배 체계는 하나의 개체에 모든 그룹 키 분배 작업을 위임하므로, 성능저하 및 시스템 장애가 발생하기 쉽다[9]. 따라서, 가입 탈퇴가 빈번한 대규모 멀티캐스트 그룹에 있어서 확장성을 제공하기 위해서는 분산된 그룹 키 분배자를 두어 관리하는 것이 바람직하다. 그룹 키 분배자의 선택 기법은 간단하고, 그룹 키 분배자에서 관리하고 있는 그룹 정보 또한 간결해야 한다. 새로운 호스트가 가입을 요청하면 분산 그룹 키 분배자는 호스트를 인증하고 ACL(Access Control List)을 확인하여 키를 분배해 주어야 한다. 해당 그룹에서 회원이 탈퇴하면 탈퇴한 회원이 더 이상 그룹 내에 전송되는 데이타를 얻지 못하도록 탈퇴한 호스트를 제외하고 새로운 그룹 키를 분배해야 한다. 또한, 분배된 그룹 키는 장기간 사용하게 되면 노출 우려가 있으므로 그룹 키는 유효기간을 가지고 주기적으로 변경해야 한다. 마지막으로 멀티캐스트 데이타 전송자와 수신자간의 통신에 있어서는 주체간의 인증이 필요하고 메시지 안의 데이타는 무결성을 제공해야 한다.

3.2 멀티캐스트 그룹 개설자의 그룹 키 생성

멀티캐스트 그룹을 개설하고자 하는 그룹 개설자는 자신이 속해 있는 서브넷 내의 분산 그룹 키 분배자인 멀티캐스트 라우터 혹은 mrouted(멀티캐스트 라우팅 데몬)과 Key Agreement를 통해 그룹 키를 생성한다. 하나의 개체에서도 키를 만들 수 있지만, 이 경우에는 랜덤 기능이 완전히 보장되기 어렵고, 대개 특별한 하드웨어가 요구되는 단점이 있다[3]. 생성된 그룹 키에 대해서는, 그룹 개설자와 인증 받은 분산 그룹 키 분배자 만이 참조할 수 있으며, 그룹 개설자는 그룹 키에 rekey interval을 두어 주기적으로 갱신하거나 보안상의 이유로 재생성 할 수 있다. [그림 3]은 그룹 개설자가 멀티캐스트 그룹을 개설하면서 분산 그룹 키 분배자와 Key Agreement를 통해 그룹 키를 생성하는 과정을 보이고 있다.

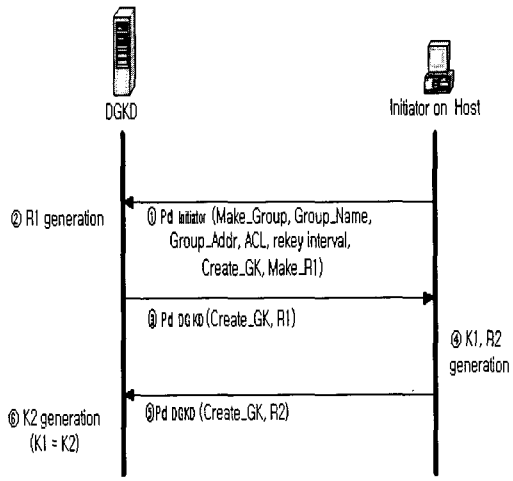

그림 3 멀티캐스트 그룹 개설과 그룹 키 생성 과정

① 멀티캐스트 그룹을 개설하고자 하는 그룹 개설자는 그룹 개설을 나타내는 Make_Group 메시지와 Group_Name, 멀티캐스트 그룹 주소, ACL, rekey interval, 또한 그룹 키를 생성하기 위해 Create_GK 메시지를 자신의 비밀키로 서명하여 DGKD에게 전송한다. 이때, 그룹 키를 생성하기 위해 Key Agreement를 하게 되는데, Diffie-Hellman 알고리즘 사용한다. 이에 필요한 난수 R1을 생성하도록 분산 그룹 키 분배자에게 알린다.

② DGKD은 유저의 공개키로 복호화 한 후, 난수 R1을 생성한다.

③ 유저에게 Create_GK 메시지와 생성한 난수 R1을 자신의 비밀키로 서명하여 전송한다.

④ 전송 받은 메시지를 DGKD의 공개키로 복호화 한 후, R1을 통해 그룹 키 K1을 생성한다. 그리고 난수

R2을 생성한다.

⑤ Create_GK 메시지와 생성된 난수 R2를 자신의 비밀키로 서명하여 DGKD에게 전송한다.

⑥ 전송 받은 메시지를 유저의 공개키로 복호화 한 후, R2를 통해 그룹 키 K2를 얻는다. 결국, K1와 K2는 같은 값이 되므로 유저와 DGKD은 같은 그룹 키를 갖게 된다. 그룹 개설자의 그룹 키 생성이 끝나면 멀티캐스트 라우팅 트리를 따라 전달된다.

Diffie-Hellman 알고리즘

1. 통신 주체인 A와 B는 공개 정보 modulus m과 integer g를 알고 있다고 가정한다.
2. A는 매우 큰 난수 r1를 생성하고 다음을 계산한다.
   $X = g^{r1} \bmod m$
3. B도 매우 큰 난수 r2를 생성하고 다음을 계산한다.
   $X = g^{r2} \bmod m$
4. A는 B에게 X를 보낸다.
5. B는 K1 = $X^{r2} \bmod m$을 계산한다.
6. B는 A에게 Y를 보낸다.
7. A는 K2 = $Y^{r1} \bmod m$을 계산한다. 결국, K1와 K2는 모두 $g^{r1r2} \bmod m$을 통해 같게 되고, 결국 공유키를 갖게 된다. 제 3자는 r1과 r2를 알지 못하기 때문에 공유키를 알아낼 수 없게 된다.

그림 4 Diffie-Hellman 알고리즘

3.3 그룹 가입 처리

그룹이 개설된 이후, 그룹에 가입하는 유저는 해당 그룹의 그룹 키를 직접 분배 받지 않고, 해당 서브넷 내의 분산 그룹 키 분배자로부터 서브 그룹 키를 분배받게 된다. 이렇게 함으로써 탈퇴 시 그룹 키를 변경해야 하는 대신에 탈퇴한 회원이 속해 있는 서브넷에 사용되는 서브 그룹 키만을 갱신하여 분배해 주면 된다.

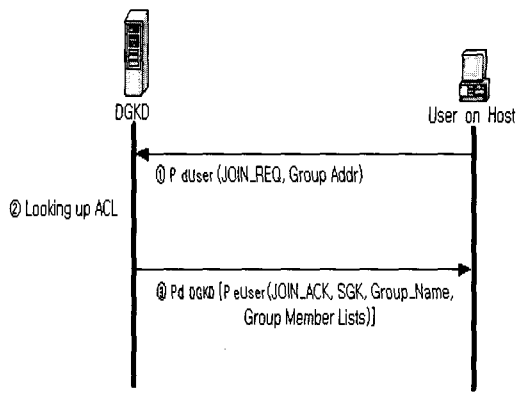

그림 5

① 그룹에 가입하고자 하는 유저는 JOIN_REQ와 해당 Group Address를 자신의 비밀키로 서명하여 DGKD에게 전송한다.

② DGKD은 해당 유저의 공개키로 복호화 한 후, ACL을 살핀다. ACL에는 참여가 규제된 리스트 정보가 있다.

③ 유저를 확인한 후, 이미 생성해 놓은 서브 그룹 키 SGK를 JOIN_ACK, 그룹 정보와 함께 유저의 공개키로 암호화 한 후, 자신의 비밀키로 서명하여 유저에게 전송한다.

3.4 그룹 탈퇴와 서브 그룹 키 재분배

키를 재분배하는 경우는 두 가지다. 첫 번째는 키의 rekey interval의 기한이 경과한 경우이고, 두 번째는 하나 이상의 회원이 합법적이거나 불법적으로 탈퇴했을 경우이다. 이 경우 해당 회원만을 제외하고 새로운 분산 그룹 키를 생성하여 재분배한다. [그림 6]는 그룹 탈퇴 처리와 서브 그룹 키 재분배 메커니즘을 보이고 있다.

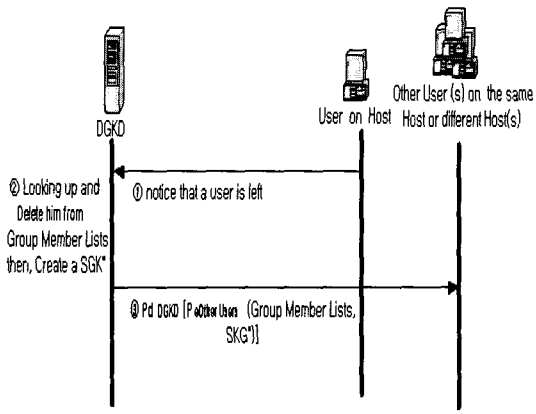

그림 6 그룹 탈퇴 및 그룹 키 재분배 과정

① 분산 그룹 키 분배자는 IGMP를 통해 해당 그룹의 회원이 탈퇴한 것을 인지한다.

② DGKM은 탈퇴한 회원을 그룹 멤버 리스트에서 찾아 삭제하고 서브넷 내에 있는 나머지 회원들을 위해 새로운 서브 그룹 키, SGK"를 생성한다.

③ 새로 생성한 서브 그룹 키는 나머지 회원의 공개키로 암호화하고 분산 그룹 키 분배자의 비밀키로 서명하여 나머지 회원에게 유니캐스트로 전송한다.

제안한 분산 그룹 키 분배 기법에 사용되는 메시지와

기호를 정리하면 (그림 7)과 같다.

Pe - 공개키 암호화 방식에서 비밀키를 이용한 암호화
Pd - 공개키 암호화 방식에서 공개키를 이용한 암호화
Make_Group - 그룹 개설자가 그룹 개설시 분산 그룹 키 분배자에게 알리는 메시지
Group_Name - 개설하고자 하는 멀티캐스트 그룹의 이름을 알리는 메시지
Group_Addr - 개설하고자 하는 멀티캐스트 그룹의 주소를 알리는 메시지
Create_GK - Key Agreement를 통해 그룹 키를 생성하도록 알리는 메시지
Make_R1 - Key Agreement를 통해 대칭키를 생성하기 위해 난수를 생성하도록 알리는 메시지
JOIN_REQ - 그룹 가입을 요청하는 메시지
JOIN_ACK - 그룹 가입을 승인하는 메시지로 그룹 정보와 서브 그룹 키를 함께 전송해준다.
GK - Key Agreement를 통해 생성되는 그룹 키
SGK - 서브넷 내에서만 사용되는 서브 그룹 키
DGKD(Distributed Group Key Distributor) - 키 분배 기능 및 보안성을 제공해 주는 멀티캐스트 라우터 혹은 mrouted

그림 7 사용된 메시지 및 기호

4. 실험 환경 설계

4.1 분산 그룹 키 분배자(DGKD)와 유저의 보안 정보

분산 그룹 키 분배자 역할을 하는 모든 멀티캐스트 라우터 혹은 mrouted 자체는 멀티캐스트 라우팅 테이블 외에, 그룹 키 분배를 위한 보안 정보 테이블을 갖는다. 보안 정보 테이블에는 (표 1)과 같이, 관리하고 있는 멀티캐스트 그룹에 대한 그룹 이름, 그룹 주소, 해당 그룹에서 사용되는 그룹 키, 그룹 키에 대한 유효 기간, 관할하고 있는 서브넷 내에서만 사용되는 서브 그룹 키, 서브 그룹 키의 유효 기간, 해당 그룹에 가입되어 있는 회원 리스트, 인증 확인이 어렵거나 보안상의 이유로 그룹에 참가하지 못하도록 규정한 호스트나 유저들에 대한 접근 제어 정보인 ACL(Access Control List)을 (그림 8)과 같은 형태로 가지고 있다. ACL은 주기적인 갱신이 필요한데, 그룹 개설자(혹은 관리자)를 통해 주기적으로 업데이트되며 rekey interval이 되면, 새로운 그룹 키와 함께 갱신된 ACL이 멀티캐스트 라우팅 프로토콜을 기반으로 구성된 멀티캐스트 라우팅 트리를 통해 각각의 서브넷 내의 분산 그룹 키 분배자에게 전송된다.

또한, 유저는 자신이 가입하고 있는 그룹에 대한 정보를 (표 2)와 같이 보안 정보 테이블 내에 가지고 있게 된다. 유저의 보안 정보 테이블에는 가입한 멀티캐스트 그룹 이름, 그룹 주소, 서브넷에서 사용되는 서브 그룹 키, 가입한 회원 리스트를 가지게 된다. 이때, 상대적으로 소규모의 인원이 참가하는 화상회의와 같은 경우 해당 그룹에 가입된 회원 리스트를 가입시 회원에게 전달해 주지만, 뉴스 서비스와 같은 다량의 회원이 있는 그룹에 경우 그룹 회원 리스트를 전달해 주지 않는다.

표 2 유저의 그룹 및 보안 정보 테이블

Group Name	Group Address	Sub Group Key	Group Member Lists
Multimedia News Site	224.20.7.13	SGK1	
Video Conference A	224.12.17.137	SGK2	==========
:	:	:	:

표 1 DGKD 내의 그룹 및 보안 정보 테이블

Multicast Group Name	Group Address	Group Key	Group Key Rekey Interval	Sub Group Key	Sub Group Key Rekey Interval	Group Member Lists	ACL
Multimedia News Site	225.20.7.13	GK1	200	SGK1	150		====
Conference A	225.12.17.137	GK2	150	SGK2	100	====	====
Weather Forcasting Site	225.199.20.11	GK3	400	SGK3	300		====
:	:	:	:	:		:	:

```
####### Access Control List #########
#
# IP-based Permission
#       Accepted:  default all
#       Denied:    163.152.*.*
#                  163.153.60.*
#                  207.603.54.224
#
  Registration Number-based Permission
       Accepted:  default all
       Denied:    701225 - 131xxxx
                  640502 - 236xxxx
#
#
```

그림 8 ACL (Access Control List)

4.2 실시간 전송

화상회의 등의 응용 프로그램에서 멀티캐스트 데이타그램을 전송하기 위해서는 전송 시간과 전송되었다는 것이 보장되어야 하는데, 이를 위해 RTP(Real Time Protocol)을 덧붙인다. RTP는 손실이 다소 있지만 실시간성을 제공해야 하는 곳에 적합하다[12,20]. RTP에는 전송되는 데이타그램이 언제 만들어진 것인지, 또 몇 번째로 만들어진 것인지를 명시하여 수신자 쪽에서 적당한 순서와 시간을 맞추어 재생할 수 있게 된다. 이런 정보 외에도 현재 전송되는 오디오나 비디오의 코딩 방식 등에 대해도 기술하고 있다.

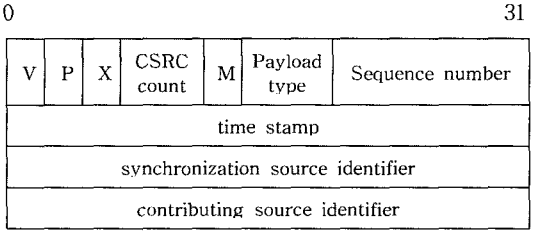

그림 9 RTP 헤더

- Multicast Authentication Data - 다양한 크기를 가질 수 있으며, 전송하고자하는 데이타를 우선 해쉬하여 일정한 크기를 갖는 메시지 다이제스트 값을 얻은 후 전송자의 비밀키로 서명한 값이다. MAD (multicast authentication data)의 길이는 32비트의 배수 크기를 갖는다. 수신자는 MAD를 통해 들어오는 패킷에 대한 무결성을 확인할 수 있다.
- V - 2비트의 크기를 가지며 RTP의 버전 정보를 나타낸다
- P - 패딩 비트를 의미한다. 이 비트가 세팅되면 하나이상의 패딩이 패킷의 종단에 붙어있음을 뜻한다.
- X - 확장 비트를 의미한다. 이 비트가 세팅되면 RTP헤더 뒤에 확장된 헤더가 더 있음을 나타낸다.
- Payload type - 7비트 크기를 가지며 RTP 패킷 내의 Payload 타입을 나타낸다. 오디오는 타입 0부터 타입23까지이고, 비디오는 타입 24부터 127까지이다.
- 16비트 Sequence number - 각각의 RTP 패킷은 시퀀스 넘버를 갖게 하여 수신자는 패킷 시퀀스를 통해 재구성하게 된다.
- time stamp - RTP 패킷이 샘플링되는 되는 시간 정보를 가지고 있다.

4.3 무결성 및 인증 기능

IP 멀티캐스트 데이타그램에 대한 무결성(Integrity)과 인증(Authentication)을 제공하기 위해 IP 계층 상위에 (그림 10)와 같이 MAH(Multicast Authentication Header)를 사용한다. 단순한 유니캐스트 환경에서 사용하는 AH(Authentication Header)는 SPI(Security Parameter Index)를 두어 두 종단간에 SA(Security Association)을 통해 안전한 통신을 할 수 있다[19]. 그러나 멀티캐스트 환경의 경우 그룹의 특성상 SPI를 이용하기는 불가능하다. 따라서, 본 논문에서는 멀티캐스트 통신에 무결성 및 인증 기능을 추가하기 위해 MAH 헤더에 데이타그램을 해쉬한 값을 비밀키로 서명하여 전송하게 된다.

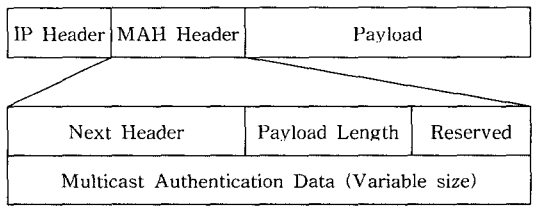

그림 10 Multicast Authentication Header

- Next Header - 8비트 크기를 가지며, MAH Header 다음에 오는 Payload의 타입을 나타낸다.
- Payload Length - 8비트 크기를 가지며, AH의 크기를 나타낸다
- Reserved - 16비트의 크기를 가지며, 후에 사용하기 위해 예약되어 있다.

그룹에 가입한 호스트는 (그림 12)와 같이 자신이 속해 있는 서브넷의 분산 그룹 키 분배자로부터 그룹 가입 및 탈퇴에 관련되어 모든 관리를 받게 된다. 결국,

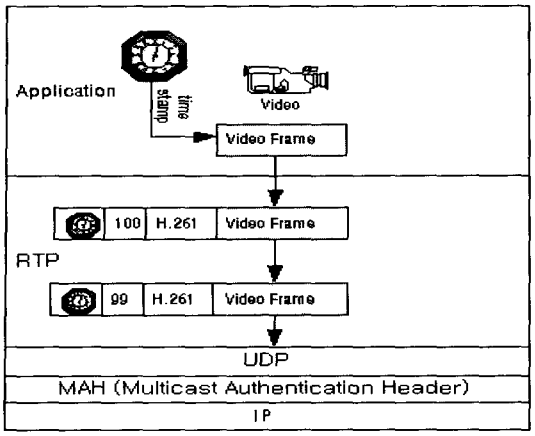

그림 11 제안한 기법의 프로토콜 스택 구조

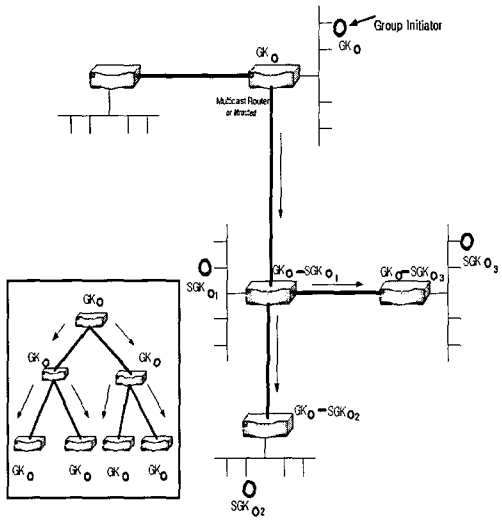

그림 12 그룹 키와 서브 그룹 키 분배

제안한 설계 사항들을 기반으로 한 멀티캐스트 통신 구조는 (그림 13)과 같이 나타낼 수 있다.

인증을 위한 디지털 서명에 있어서는 모든 데이타그램에 대해 수신자와 송신자간에 적용하지 않고 선택적으로 제공하도록 하였다. 즉, 멀티캐스트 통신 초기 시점이나 일정한 시간 간격으로 인증 확인을 하도록 하여, 공개키 암호화 기법이 가지는 시간적 지연을 줄이도록 하였다.

5. 실험 환경 구현

멀티캐스트 지원을 위한 API는 Steve Deering의 버클리 소켓 멀티캐스트 API인 set/getsockop()가 있다. 이것들은 모두 멀티캐스트 그룹 가입, 탈퇴, TTL 값 설정, 멀티캐스트 송수신을 위한 로컬 인터페이스 설정, 전송중인 멀티캐스트의 루프백 기능 설정 등에 관련된 API들이다[16,17].

표 3 BSD get/setsockopt() 멀티캐스트 관련 명령어

명령어	기능
IP ADD MEMBERSHIP	멀티캐스트 그룹 가입
IP DROP MEMBERSHIP	멀티캐스트 그룹 탈퇴
IP_MULTICAST_IF	멀티캐스트 전송을 위한 기본 인터페이스 설정
IP_MULTICAST_LOOP	전송되는 멀티캐스트 데이타그램에 대한 루프백 기능 설정
IP_MULTICAST_TTL	데이타그램에 대한 time-to-live 정보 설정

실험을 위한 구현에 있어 초점은 현재 Mbone 툴로 사용되고 있는 응용 프로그램을 가급적 적게 수정하면서도 보안 기능을 제공하는데 두었다. 기존의 멀티캐스트 응용 프로그램에 보안성을 제공하기 위해 공개 암호화 라이브러리인 CryptoLib 라이브러리[18]를 사용하여 범용성과 이식성을 고려하였다. 멀티캐스트 그룹을 개설할 때에는 동일한 그룹 주소로 먼저 생성된 그룹과 충돌을 막기 위해 SDR(Session Directory)을 사용하였다[11]. SDR은 개설하고자 하는 멀티캐스트 그룹에 유일한 멀티캐스트 주소와 포트 넘버를 할당해 주어 충돌을 막아 주고 개설된 그룹에 대해 알리는 역할을 한다. 그룹 개설과 함께 분산 그룹 키 분배자와 Key Agreement를 통해 그룹 키를 생성하기 위해 SDR의 소스를 수정하여 그룹 개설 시 Key Agreement를 위한 코드를 추가하였다. SDR은 주기적으로 개설된 멀티캐스트 그룹에 대한 광고(Advertisement)를 하면서 해당 그룹에 가입된 회원을 가지고 있는 멀티캐스트 라우팅 트리에 속해 있는 서브넷의 DGKD에게 그룹 키를 전달하도록 하였다. 또한, 개설된 그룹에 가입하는 회원을 위해 서브 그룹 키를 분배해주는 모듈도 추가하였다. 가입한 회원이 사용하는 멀티캐스트 응용 프로그램으로는 화상 통신이 가능한 vic[12]의 소스를 수정하였다. vic에는 데이타그램을 전송 혹은 수신시 자신이 가지고 있

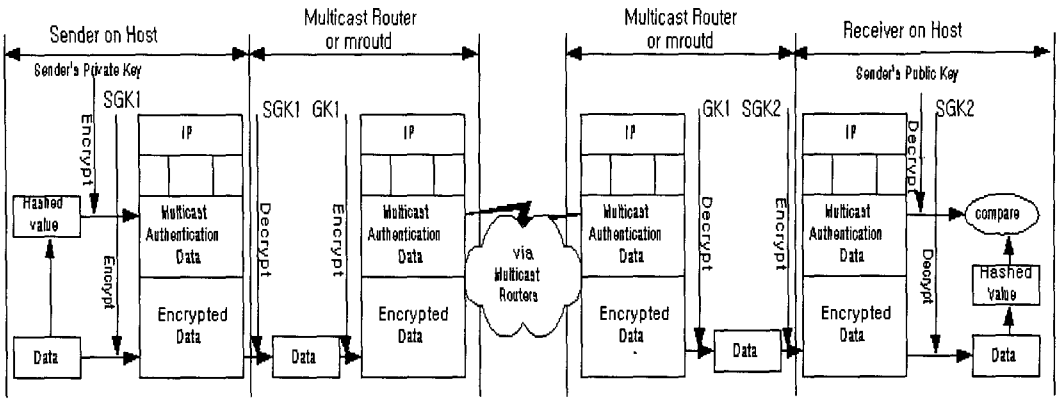

그림 13 제안한 기법에 의한 멀티캐스트 데이타그램 전송 구조

는 서브 그룹 키를 사용하도록 암호화 복호화 기능을 추가하였다. 또한 분산 그룹 키 분배자 역할을 하는 멀티캐스트 라우터(혹은 mrouted)는 공개된 mrouted 소스를 Sun 웍스테이션에 설치하고 Key Agreement 및 키 분배와 관리 모듈을 추가하였다.

6. 실험 결과 및 분석

(그림 14)는 멀티캐스트 그룹 회원이 분산 그룹 키 분배자로부터 받은 서브 그룹 키를 통해 멀티캐스트 데이타그램을 전송하여 5 홉 떨어진 수신자가 수신할 때 걸리는 시간과 순수한 멀티캐스트 데이타그램을 송수신 할때의 시간을 측정한 것이다. 순수한 멀티캐스트 데이타그램 전송(NOP)과 보안성이 제공되는 멀티캐스트 전송(DGKD)시 걸리는 Payload 사이즈 별 전송 시간의 차이를 알 수 있다. 이를 통해 보안 기능 제공으로 인한 오버헤드가 사용자가 느낄수 있을 만큼 크지 않음을 알 수 있다.

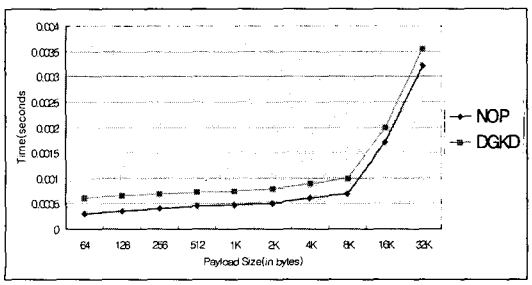

그림 14 DGKD를 이용한 멀티캐스트 데이타그램 전송 성능

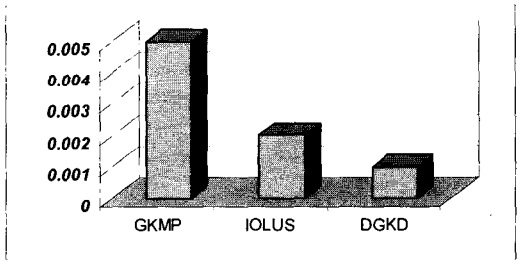

그림 15 동일 서브넷 내의 회원 탈퇴 처리 시간

(그림 15)은 임의의 멀티캐스트 그룹에 가입한 동일 서브넷 내의 회원을 10명으로 가정했을 때, 1명의 회원 탈퇴시 걸리는 탈퇴 처리 시간을 보이고 있다. 탈퇴 처리 시간은 탈퇴한 회원을 그룹 멤버 리스트에서 삭제하고 나머지 회원을 대상으로 새로운 서브 그룹 키를 분배하는데 걸리는 시간이 된다. 여기서는 실험 환경으로 그룹 개설자가 있는 서브넷은 수신자로부터 5홉 떨어진 서브넷에 위치하도록 하였다. GKMP의 경우, 회원이 탈퇴한 서브넷 뿐만 아니라, 회원이 있는 모든 서브넷의 회원을 상대로 탈퇴 처리를 해야하므로 처리 시간이 현저하게 많이 소모됨을 알 수 있다. IOLUS의 경우 여러 홉을 거치는 동안 암호화 복호화를 매 홉을 거치면서 반복하게 되므로 광범위 멀티캐스트 그룹 관리에 있어서는 비효율적이다. SMKD의 경우 멀티캐스트 라우팅 프로토콜 기반의 그룹 키 분배 기법이므로 실험 대상에서 제외시켰다. 분산 그룹 키 분배자를 사용하는 경우 암호화와 복호화는 양종단간의 서브넷에서만 일어나므로 IOLUS에 비해 소모 시간이 적게 소모됨을 알 수

표 4 제안한 분산 그룹 키 분배(DGKD) 기법과 다른 기법들과의 비교

비교 항목 \ 그룹 키 분배 기법	GKMP	SMKD	IOLUS	DGKD
확장성	X	△	△	O
그룹 키 분배자 선택	언급하지 않음	복잡함	복잡함	간단함
인증	O	O	O	O
메시지 무결성	O	O	O	O
분산된 그룹 키 분배	X	O	O	O
그룹 키 분배자의 범위	그룹 전체	그룹 전체	그룹 전체 계층화된 서브 그룹	서브 그룹
그룹 키 분배자 부하	높음	보통	낮음	낮음
토폴로지 변화	관계 있음	관계 있음	관계 있음	무관함

있다.

(표 4)는 제안한 그룹 키 분배 기법과 여러 가지 다른 그룹 키 분배 기법을 확장성, 그룹 키 분배자 선택의 용이성 등 여러 가지 비교 항목을 통해 비교하고 있다.

7. 결론 및 향후 연구 방향

본 논문에서는 현재까지 진행되어 오고 있는 여러 가지 그룹 키 분배 기법들에 대해 살펴보고, 안전한 인터넷 멀티캐스트를 위한 확장성 있는 그룹 키 분배 기법을 제안하고 기존의 멀티캐스트 응용 프로그램에 접목하여 실험 결과를 분석하였다. 제안한 기법을 통해, 멀티캐스트 그룹에 가입한 유저는 회원 인증과 메시지 무결성을 통해 안전한 멀티캐스트 통신을 할 수 있다. 뿐만 아니라 대규모의 회원을 관리해야 하는 경우, 가입과 탈퇴에 따른 그룹 키 분배자의 부하를 줄여 확장성을 제공해 준다. 현재까지는 대부분의 멀티캐스트 그룹 사이트가 무료로 화상과 음성을 제공하고 있지만 인터넷 인구의 팽창과 함께 사설 멀티캐스트 그룹 사이트가 많이 등장할 것이고 제안한 기법을 토대로 사설 유료화 서비스가 가능하게 될 것이다. 이로 인해 뉴스 사이트뿐 만 아니라 회원 권한을 필요로 하는 화상 회의나 원격 교육에도 응용이 가능하며, 활용을 위한 연구를 계속 진행하고 있다.

참 고 문 헌

[1] D.Wallner, E.Harder; R. Agee, "Key Management for Multicast: Issues and Architectures," rfc2627, June, 1999.

[2] Harney Hugh, Muchenhirn Carl and Thomas Rivers, "Group Key Management Protocol Architecture," RFC 2094, July., 1997.

[3] Harney Hugh, Muchenhirn Carl and Thomas Rivers, "Group Key Management Protocol Specification," RFC 2093, July., 1997.

[4] A. Ballardie, "Scalable Multicast Key Distribution," RFC 1949, May 1996.

[5] Suvo Mittra, "Iolus: A Framework for Scalable Secure Multicasting," Proceedings of the ACM SIGCOMM '97, September 14-18, 1997

[6] A.Ballardie Consultant, "Core Based Trees(CBT) Multicast Routing Architecture," rfc2201, Sept., 1997

[7] Chuck Semeria and Tom Maufer, "Introduction to IP Multicast Routing," http://www.3com.com/nsc/501303.html.

[8] J. Linn., "Common Authentication Technology Overview." RFC 1511, September 1993.

[9] R. Canetti; B. Pinkas, "A toxonomy of multicast security issues," Internet-Draft, May 1998.

[10] Germano Caronni; Marcel Waldvogel; Dan Sun; Bernhard Plattner, " Efficient Security for Large and Dynamic Multicast Groups" WET ICE '98, 1998.

[11] Mark Handley, "The sdr Session Directory: An Mbone Conference Scheduling and Booking System," University College London Draft 1.1, April, 1996.

[12] McCanne, S., and Jacobson, V., vic: A Flexible Framework for Packet Video, ACM Multimedia '95, 1995.

[13] Alfred J.Menezes, Paul C. van Oorschot, Scott A. Vanstone, Handbook of Applied Cryptography, CRC press, 1997.
[14] Pekka Pessi, "Secure Multicast" http://www.nixu.fi/~pnr/netsec-lopulliset/3-0-multicast.html, 1998.
[15] R.Atkinson, "Secure Architecture for the Internet Protocol" rfc1825, 1995.
[16] Stevens, Unix Network Programming, Vol.1, Prentice Hall, pp.487-580, 1998.
[17] Writing IP Multicast-enabled Applications, http://www.ipmulticast.com, 1999
[18] J.B. Lacy, D.P. Mitchell, and V.M. Schell, "CryptoLib: Cryptography in Software," Proceedings of the USENIX UNIX Security Symposium," Oct.,1995.
[19] Martin W. Murhammer, TCP/IP Tutorial and Technical Overview, IBM, pp.263-355, 1999.
[20] Schulzrinne,H., Casner, S., Frederick, R., and Jacobson, V., "RTP: A Transport Protocol for Real-Time Applications," Audio-Video Transport Working Group, Mar., 1995

장 주 만
1997년 서울산업대 공과대학 전자계산학과 졸업(공학사). 1998년 ~ 현재 고려대학교 이과대학 컴퓨터학과 석사과정. 관심분야는 멀티미디어 통신, 네트워크 보안, 전자상거래

김 태 윤
1981년 고려대학교 산업공학과 학사. 1983년 Wayne state University 전산과학과 박사. 1998년 ~ 현재 고려대학교 컴퓨터학과 교수. 관심분야는 전자상거래, 컴퓨터 네트워크, EDI, 이동통신 등