계층 구조를 이용한 안전한 멀티캐스트 데이터 전달을 위한 효율적인 그룹 관리 메커니즘에 관한 연구

고훈*, 신용태*
*대진대학교 컴퓨터공학과
**숭실대학교 컴퓨터학과
e-mail:skoh21@daejin.ac.kr, shin@comp.ssu.ac.kr

A Study of Effective Group Management Mechanism to Secure Multicast Data Transmission using Hierarchical Structure

Hoon Ko*, Yong-tae Shin**
*Dept of Computer Engineering, Dae-jin University
**Dept of Computer Science, Soong-sil University

요 약

인터넷을 통해서 많은 중요한 정보들이 송수신되고 있다. 그러나 이러한 중요한 정보는 많은 위험에 노출되어 있다. 또한 멀티캐스트 서비스도 다양해지고 보편화 되고 있다. 그만큼 서비스의 폭도 넓어지고 있다. 멀티캐스트 통신에서 그룹에 새로운 멤버가 가입하거나 탈퇴하는 경우 기존 멤버가 사용하던 그룹 키는 새로이 생신되어야 한다. 본 논문에서는 안전한 멀티캐스트 데이터 전달을 위해서 가입과 탈퇴가 빈번한 멀티캐스트 그룹에 대해서 안전한 데이터 전달을 위한 효율적인 그룹 관리 메커니즘을 제공하고자 한다.

1. 서론

최근 급속하게 발전하고 있는 인터넷을 이용한 전자상거래가 활성화 되면서 이를 이용한 금융, 증권 등의 분야에 응용되어 새로운 서비스를 제공되고 있다. 특히 공개키 기반 구조(Public Key Infrastructure : PKI)의 이용은 개인 인증서 사용이란 기술을 탄생시켰다. 특히, 유·무선이 결합된 초고속망의 구조와 실시간 멀티미디어 중심의 서비스를 위한 기반 환경을 조성할 수 있는 멀티캐스트 기술에 대한 연구가 활발히 진행 중에 있다. 멀티캐스트는 원격 교육과 원격 회의, 주요 스포츠 이벤트의 방송, 분산 데이터베이스 접근 등에 적용될 수 있다. 최근에는 인터넷을 기반으로 한 많은 응용들이 등장하고 있다. 예를 들면 경매사이트, 주식투자 사이트, 온라인 그룹 강의 등 많은 응용들이 개발되고 있다. 멀티캐스트는 원격 교육과 원격 회의, 주요 스포츠 이벤트의 방송, 분산 데이터베이스 접근 등에 적용될 수 있다. 최근에는 인터넷을 기반으로 한 많은 응용들이 등장하고 있다. 예를 들면 경매사이트, 주식투자 사이트, 온라인 그룹 강의 등 많은 응용들이 개발되고 있다.

이들은 대부분 유료 서비스 혹은 비밀성을 요하는 서비스를 요구하고 있다. 그러나 이들 대부분은 보안성을 위한 인증과 접근 제어를 위해서 아이디, 패스워드 방식을 대부분 채택하고 있다. 안전한 멀티캐스트 시스템을 연구하고 설계함에 있어서 고려되어야 할 사항은 인증과 접근 제어 그리고 비밀성, 무결성, 부인봉쇄 등을 제공하는 것이다. 본 논문에서는 그룹관리와 데이터의 비밀성 측면에 초점을 맞추었다. 본 논문의 구성은 다음과 같다. Ⅱ장에서는 제안한 방법인 안전한 그룹 관리와 그룹 키 생성 및 분배 기법에 대해서 설명을 하고 Ⅲ장에서는 제안한 방법에 대한 모델 분석 및 간단한 실험을 하고 Ⅳ장에서는 결론을 맺는다.

2. 안전한 그룹 관리

안전한 멀티캐스트 시스템을 설계하고 구현하는데 있어서 고려되어야 할 보안 서비스는 인증과 접근제어, 비밀성, 무결성, 부인봉쇄 등이 있다. 본 논문에서 제안하는 모델의 고려사항은 다음과 같다.

(1) 신뢰성을 제공해야 한다.
(2) 확장성을 제공해야 한다.
(3) 보안 메커니즘으로 인한 오버헤드가 없어야 한다.

2-1. 그룹 구조

그룹통신은 그룹 멤버쉽을 관리하고 멤버들의 접근 제어와 키 분배 수행과 이 키를 이용한 데이터의 암호, 복호, 서명 등 보안 메커니즘을 적용하여 전송하는 데이터 전송 측면으로 구성된다. 제안하는 안전한 그룹 관리 구조는 [그림 1] 과 같다. 보안 서버가 그룹을 관리, 즉 키 분배 키 생성 등을 관리하게 된다. 또한 그룹 가입 요청이 들어오면 이에 대한 응답을 담당하게 된다. 안전한 그룹 구조의 구성요소는 다음과 같다.

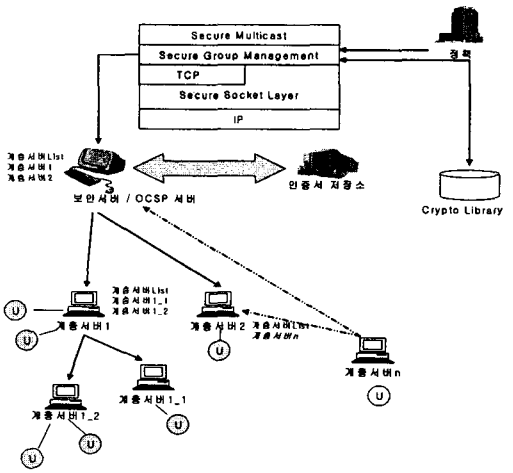

그림 1. 안전한 그룹 계층구조

- 송신자(인증서 저장소) : 멤버들에게 전송할 최신의 인증서 취소 목록을 가공한다.
- 수신자(멤버) : 송신자가 보내는 정책을 수신하고, 암호화해서 수신된 데이터를 복호화 해서 사용자의 인증서 검증 요청에 응한다.
- 보안서버 : 그룹관리, 멤버관리 관리를 한다. 그룹 게시자로서, 세션 시작 전에 보안 정책을 결정하여 그룹에게 미리 분배한다. 데이터를 암호화해서 전송한다.
- 계층서버 : 계층 구조를 이루었을 경우 그 그룹의 대표가 되어 보안서버의 역할을 대신한다. 정책 결정 암호화 생성 전송 등의 기능은 없다.
- 정책서버 : 그룹의 정책을 결정한다. 공개키 기반 구조의 정책기관과 같은 역할을 한다. 단 본 논문에서는 보안 그룹에 대한 정책 결정을 담당한다.
- Crypto Library : 본 모델에서 사용될 각종 암호화 복호화 및 각종 보안 모듈들을 저장하고 있다.

2-2. 그룹 생성

그룹 생성은 보안서버가 담당한다. 지정된 그룹 ID를 부여하고 그림 2와 같이 그룹 생성이 가능한지G_Query를 통해서 파악한 후 가능하다면 G_Create를 이용해서 생성하게 된다.

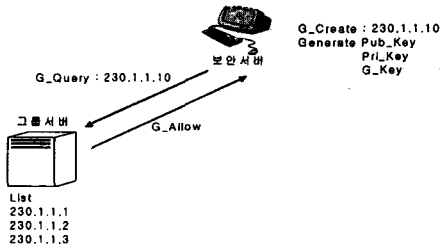

그림 2. 그룹생성

표 1. 그룹 생성시의 메시지 정의

메시지	매개변수	의미
G_Create	G_IP, G_ID	지정된 IP로 그룹을 생성
G_Query	G_IP	지정된 IP의 그룹 조사
Generate	G_IP, Pub_Key	보안서버 공개키 생성
	G_IP, Pri_Key	보안서버 개인키 생성
	G_IP, G_Key	보안서버 그룹키 생성
	HS1_Pub_Key	계층서버1 공개키 생성
	HS1_Pri_Key	계층서버1 개인키 생성

그룹을 생성한 후에 Generate를 이용해서 그룹키(G_Key)를 생성한다.

2-3. 그룹 가입

안전한 그룹 가입을 위해서 보안서버는 그룹 생성히 Generate를 이용해서 그룹 키를 생성하게 되고, 멤버들도 각각의 개인키과 공개키 쌍을 생성하게 된다[그림 3].

표 2. 그룹 관리시의 메시지 정의

메시지	매개변수	의미
G_Modify	G_IP, G_ID	지정된 IP의 그룹정보 변경
Join	G_IP, G_ID, IP	지정된 IP로 그룹 재가입
Allo	G_IP, IP	지정된 IP로부터 그룹 허용
Success	G_IP, IP	지정된 IP 구룹 가입 성공
Fail	G_IP, IP	지정된 IP 구룹 가입 실패
Send	HS1_Pub_Key	계층서버1의 공개키 전송
	E(G_Key)_HS1_Pub_Key	계층서버1의 공개키를 이용해서 그룹키 암호화 후 전송

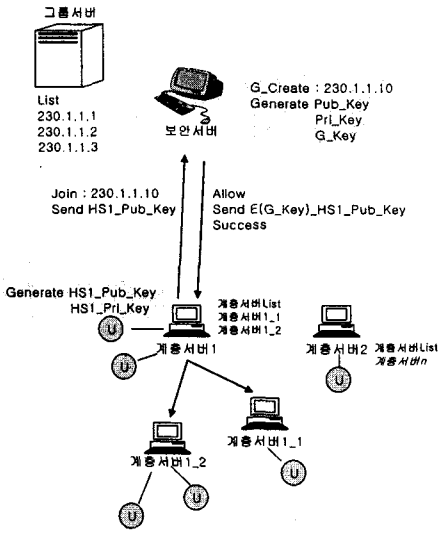

그림 3. 그룹가입

2-4. 그룹 재가입

그룹 재가입에서는 멤버의 오류 및 기타 문제로 인해서 재시작 등으로 인해서 그룹에서 탈퇴된 상태에서 재시작 완료 후 자동 가입시에 대한 설명이다. 이때 재시작된 멤버는 보안서버에 G_Join 메시지와 그룹 키를 보안서버의 공개키를 이용해서 암호화해서 보안서버에 보내게 된다. 보안서버는 그룹키를 복호화 해서 확인한 후 그룹에 재가입을 승인한다[그림 4].

표 3. 그룹 관리시의 메시지 정의

메시지	매개변수	의미
G_Modify	G_IP, G_ID	지정된 IP의 그룹정보 변경
G_Join	G_IP, G_ID	지정된 IP로 그룹 재가입
G_Leave	G_IP, G_ID	지정된 IP로부터 그룹탈퇴
Success	G_IP, G_ID	지정된 IP 구룹 가입 성공
Fail	G_IP, G_ID	지정된 IP 구룹 가입 실패
Send	HS1_Pub_Key	계층서버1의 공개키 전송
	E(G_Key)_HS1_Pub_Key	계층서버1의 공개키를 이용해서 그룹키 암호화 후 전송

3. 모델분석 및 실험

3-1. 그룹 가입

보안서버는 특정 목적을 위한 그룹을 생성한다. 물론 그룹에 대한 인증서도 CA를 통해서 할당받고 그룹 키를 생성하게 된다. 보안 서버는 그룹 생성에 대한 정보를 멤버들에게 전송한다. 그룹 가입을 희망하는 멤버는 보안서버에 가입을 요청하고 개인 인증서를 보안 서버에 전송하게 된다. 이를 수신한 보안서버는 인증서 저장소의 CRL을 참고해서 인증서에 대한 검증을 한다. 검증 후에 그룹 인증서를 멤버에게 전송한다. 그룹인증서를 받은 멤버도 마찬가지로 인증서 저장소로부터 그룹 인증서에 대한 검증을 하고 검증 확인이 되면 보안서버에 그룹 가입을 요청한다

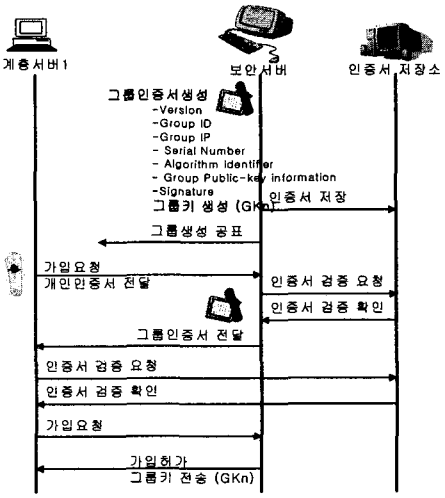

그림 4. 그룹 가입 절차

. 보안서버는 멤버에게 멤버의 공개키를 이용해서 그룹키를 암호화 후 전송한다.

3-2. 그룹 탈퇴

특정 멤버가 그룹에서 탈퇴를 할 경우, 보안 서버는 탈퇴된 멤버를 제외한 나머지 멤버들에게 그룹 인증서를 재발급하게 된다. 이렇게 함으로써 생성된 그룹은 갱신하게 된다.

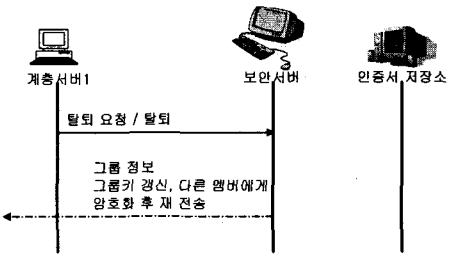

그림 5. 그룹탈퇴

3-3. 재 가입

기존 그룹에 재 가입을 요청하는 경우 보안 서버는 멤버의 인증서를 확인하고 갱신된 그룹키를 멤버의 공개키로 암호화해서 전송하게 된다.

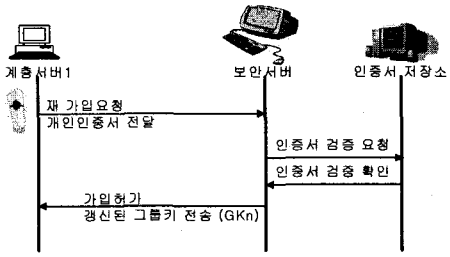

그림 6. 재가입 요청

3-4. 실험 환경

본 모델은 사이버 교육 환경에서 분산되어 있는 10에서 20명 사이의 학생이 인터넷상에서 화상을 이용한 교육을 받고 있다고 가정한다.

표 4 : 실험 환경 변수

멀티캐스트 라우팅 프로토콜	DVMRP
CBR 트래픽	0.06초
데이터 크기	64bytes-5Kbytes
암호 알고리즘	Rijndael
키 길이	56bits
해쉬 알고리즘	SHA1
서명 알고리즘	RSA
서명 / 인증 키 길이	512bits
노드 개수	4개
호스트 개수	10명 - 20명
실험시간	300초
링크지연	10ms
대역폭	1.5mb, 10mb

3-5. 실험 결과

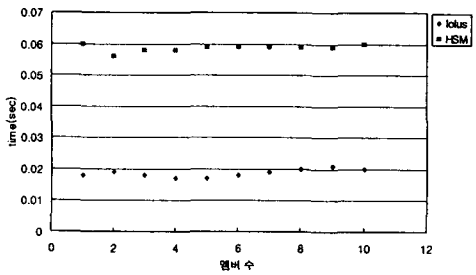

그림 7. 멤버 가입시 지연시간

그림 8은 멤버 가입시 가입을 위해서 처리해야 하는 시간을 측정한 결과이다. 제안한 방법은 서로 간에 인증서를 교환하고 검증을 받은 후에 가입이 승인되기 때문에 이를 위한 처리시간이 기존의 방법에 추가된 결과를 보여준다.

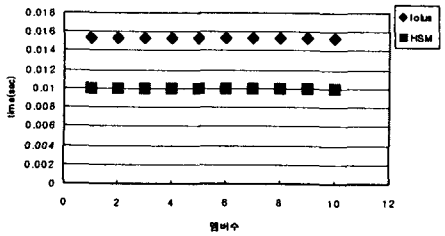

그림 8. 멤버 탈퇴 시 처리시간

그림9는 멤버 탈퇴 시 처리하는데 걸리는 시간을 측정한 결과이다. 그림 10은 탈퇴했던 그룹에 재 가입을 위한 시간이다. 제안된 모델은 계층적인 구조를 이루고 있다. 따라서 멤버 가입에 있어서 전체 그룹 구조에 어떠한 영향을 미치지 않는다. 따라서 계층의 한 부분에 접속만 시도 하면 된다. 따라서 기존 방법에 비교해 봤을 때 빠른 가입 처리를 수행 하였다.

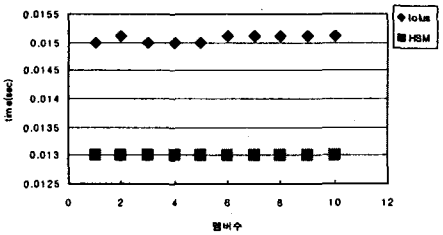

그림 9. 그룹 재 가입 시간

4. 결론 및 향후 과제

초기의 네트워크는 사용자의 소규모로 인해서 특별한 문제가 제기 되지 않았으며 보안상의 문제점도 없었다. 그러나 인터넷 사용자 증가 및 인터넷 활용도가 높아지면서 인터넷을 이용한 중요한 정보들이 흐르고 있다. 또한 데이터의 대용량성으로 인해서 멀티캐스트 기법이 제안되었지만, 많은 보안상의 문제점을 가지고 있다. 특히 실시간 데이터 전송을 요청하는 최근의 데이터의 특성상 많은 부분에서 문제점이 제기되고 있다. 향후 정부에서는 공개키 기반구조를 기반으로 한 전자 정부를 구축하겠다고 한다. 본 논문은 계층 구조를 가지고 있지만, 그 계층은 미리 정의한 구조이다. 즉 계층 구조가 동적일 경우에는 구조의 재구성을 위한 시간도 필요하다. 이러한 점을 고려하여 보다 더 안전하고 더 빠르고 효율적인 계층 구조에 대한 연구를 진행해야 할 것이다.

참고문헌

[1] 김태연, 김영균, "대규모 동적 그룹에서 안전한 멀티캐스트를 위한 키 분배 프로토콜," *한국 정보처리학회 논문지* (C), 9C(4), pp. 597-604, August 2002.

[2] 김문화, 황준 "멀티미디어 데이터 통신의 신뢰성 보장을 위한 서비스 제공자 중심의 멀티캐스트 미들웨어 설계 및 구현," *한국 인터넷 정보학회 논문지*, 3(4), pp. 11-17, August 2002.

[3] H. Liu and Magada 띠 Zarki "D띠표 and Synchronization Control Middleware to Support Real time Multimedia Services over Wireless PCS Networks," *IEEE journal Communication*, Volume 17, Number 9, pp. 1660-1672, 1999.

[4] R. Canetti and B.Pinkas, "A taxonomy of multicast security issues," draft-irtf-smug-taxonomy-01.txt, August., 2000

[5] Pekka Pessi, "secure Multicast," Proc. of Helsinki University of Technology Seminar on Network Security, 1995.