멀티캐스트 전송을 위한 안전한 그룹관리에 관한 연구

고훈°), 장의진, 신용태
대진대학교 컴퓨터공학과, (주) 디지캡스, 숭실대학교 컴퓨터학과
skoh21@daejin.ac.kr neon@digicaps.com shin@comp.ssu.ac.kr

A Study of Secure Group Management to Multicast Data Transmission

Hoon Ko°), Uijin Jang, Yongtae Shin
Department of Computer Science Daejin Univ. Digicaps Inc,
Department of Computer Science Soongsil Univ.

요 약

인터넷을 통해서 많은 중요한 정보들이 송수신되고 있다. 그러나 이러한 중요한 정보는 많은 위협에 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 데이터 전달을 위한 안전한 그룹 관리 방법을 제안하고자 한다.

1. 서 론

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 접근제어 그리고 비밀성, 무결성, 부인봉쇄 등을 제공하는 것이다. 논문 구성은 다음과 같다. 2장은 제안하는 방법인 안전한 그룹 관리에 대해서 설명하고, 3장은 제안한 방법의 모델을 분석한다. 마지막으로 4장에서는 결론을 맺는다.

2. 안전한 그룹관리

안전한 멀티캐스트 시스템을 설계하고 구현하는데 있어서 고려되어야 할 보안 서비스는 인증과 접근제어, 비밀성, 무결성, 부인봉쇄 등이 있다. 멀티캐스트 보안 구조의 목적은 인증 받은 그룹 멤버들이 안전하게 그룹 통신을 할 수 있도록 하는 것이다. 이를 위해서는 멤버의 가입 및 탈퇴를 처리하고 관리하는 그룹 키에 대한 생성 및 갱신 그리고 분배 함에 있어서 얼마나 안전한가에 있다[4].

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.

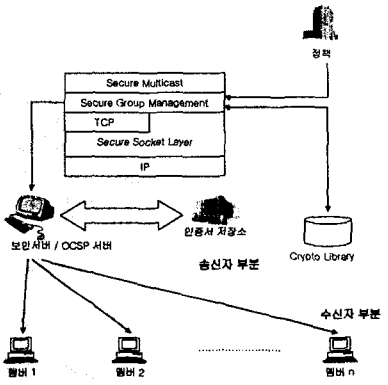

그림 1. 안전한 그룹 구조

안전한 그룹 구조의 구성요소는 다음과 같다.

- 송신자(인증서 저장소) : 멤버들에게 전송할 최신의 인증서 취소 목록을 가공한다.
- 수신자(멤버) : 송신자가 보내는 정책을 수신하고, 암호화 해서 수신된 데이터를 복호화 해서 사용자의 인증서 검증 요청에 응한다.
- 보안서버 : 그룹관리, 멤버관리 관리를 한다. 그룹 게시자로서, 세션 시작전에 보안 정책을 결정하여 그룹에게 미리 분배한다. 데이터를 암호화 해서 전송한다.
- 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.

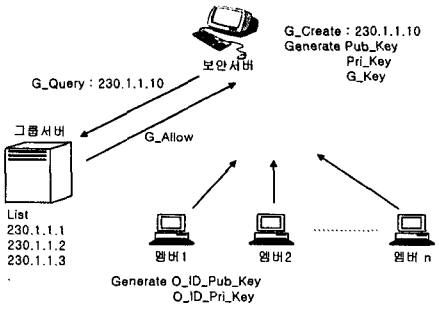

그림 2. 그룹생성

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
	O_ID_Pub_Key	OCSP 서버 공개키 생성
	O_ID_Pri_Key	OCSP 서버 개인키 생성

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

2.3 그룹 구조

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

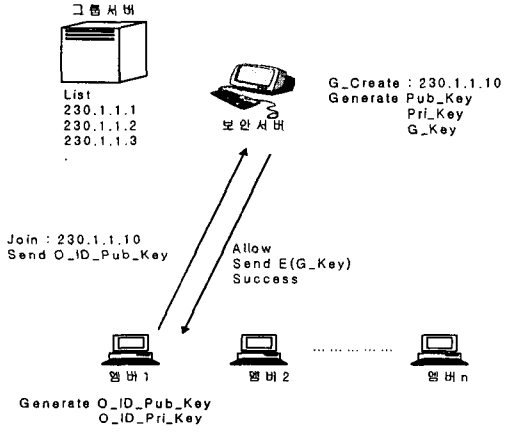

그림 3. 그룹 가입

2.4 그룹 재 가입

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

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	O_ID_Pub_Key	공개키 전송
	E(G_Key)	OCSP 서버의 공개키를 이용해서 그룹키 암호화 후 전송

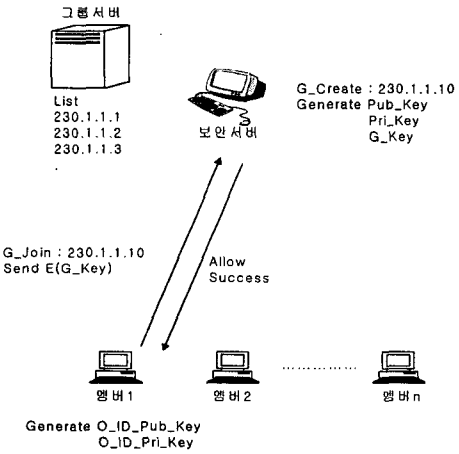

그림 4. 그룹 재가입

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	O_ID_Pub_Key	공개키 전송
	E(G_Key)	OCSP 서버의 공개키를 이용해서 그룹키 암호화 후 전송

3. 모델 분석

3.1 그룹 가입

보안서버는 특정 목적을 위한 그룹을 생성한다. 물론 그룹에 대한 인증서도 CA를 통해서 할당받고 그룹 키를 생성하게 된다.

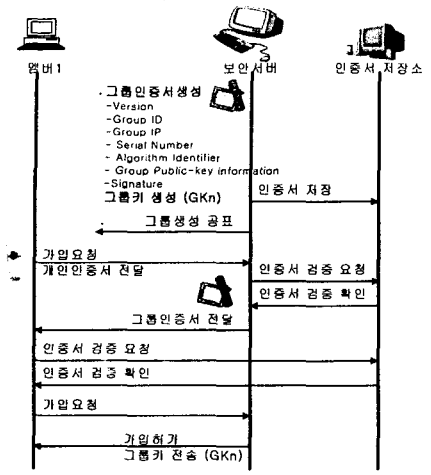

그림 5. 그룹 가입 절차

보안 서버는 그룹 생성에 대한 정보를 멤버들에게 전송한다. 그룹 가입을 희망하는 멤버는 보안 서버에 가입을 요청하고 개인 인증서를 보안 서버에 전송하게 된다. 이를 수신한 보안서버는 인증서 저장소의 CRL을 참고해서 인증서에 대한 검증을 한다.

3.2 그룹 탈퇴

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

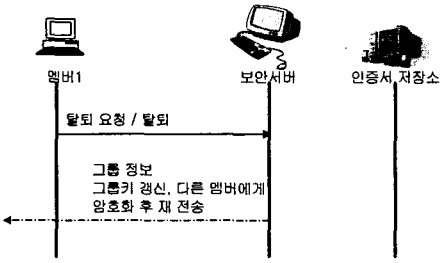

그림 6. 그룹 탈퇴

3.3 그룹 재가입

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

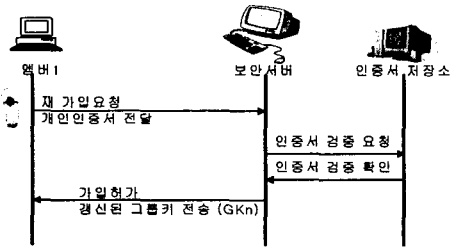

그림 7. 재가입 요청

3.4 재 가입 결과

그림 8은 탈퇴했던 그룹에 재 가입을 위한 시간을 측정한 결과이다.

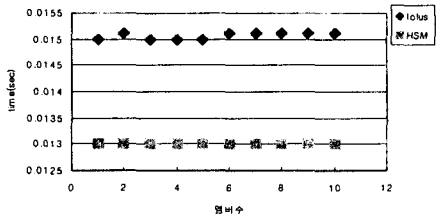

그림 8. 그룹 재 가입 시간

4. 결론

본 모델은 대규모 동적인 그룹에게 안전한 데이터 및 안전한 그룹 인증을 위한 설계를 하였다. 그룹 인증과 개인 인증으로 지연되는 시간을 최소화 하기 위한 단계로 설계하였고, 그룹 탈퇴 후 그룹에 대한 세션키 생성 및 전달 부분을 처리함으로써 탈퇴한 사용자가 그룹 키를 노출하더라도 기존 사용자의 데이터에 대한 비밀성을 보장하였다. 그러나 어느 멀티캐스트 그룹도 마찬가지겠지만 멤버의 유동이 너무 빈번하면 보안서버의 그룹 키 생성 전송에 많은 부담이 따른다. 따라서 차후 분산되어 있는 그룹들을 계층형으로 처리하여 중간 계층에 제2의 보안서버를 두어서 지역적으로 처리를 하게 하고자 한다.

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] 은상아, 조태남, 채기준, 이상호, 박원주, 나재훈 "안전한 멀티캐스트 서비스 제공을 위한 효율적인 그룹 관리 메커니즘 및 구조," *한국 정보처리학회 논문지 (C)*, 9C(4), pp. 323-330, June 2002.

[4] 장주만, 김태윤, "안전한 인터넷 멀티캐스트를 위한 확장성 있는 분산 그룹 키 분배 기법," *한국 정보과학회 논문지*, 제27권 제1호, 2000

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

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