안전한 멀티캐스트 서비스 제공을 위한 효율적인 그룹 관리 메커니즘 및 구조

은 상 아[†] · 조 태 남[††] · 채 기 준[†††] · 이 상 호[†††] · 박 원 주[††††] · 나 재 훈[†††††]

요 약

멀티캐스트 서비스들이 점차 다양해지고, 서비스 사용자의 폭도 넓어지고 있다. 이에 비례하여 공격자들의 주목을 받게되고 정보의 누출 가능성도 높아진다. 따라서 멀티캐스트 서비스 활용과 동시에 그에 대한 보안 연구도 함께 이루어져야 한다. 본 논문에서는 멤버의 동적인 가입·탈퇴가 발생하는 그룹에서 효율적인 그룹 관리를 적용하여 안전한 멀티캐스트 서비스를 제공할 수 있는 구조를 제안한다. 제안한 구조는 한 명의 송신자와 다수의 수신자로 구성된 멀티캐스트 통신 상황에서, 보안 측면을 고려하여 많은 이용자들에게 안전한 멀티캐스트 서비스를 제공할 수 있다. 시뮬레이션을 통하여 기존의 구조와 성능을 비교·분석한 결과, 제안하는 구조는 멤버 관리가 효율적이고, 전송 지연을 줄이면서 보다 안전하게 데이터를 전송할 수 있다는 것을 알 수 있었다.

Efficient Group Management Mechanism and Architecture for Secure Multicast

Sang-A Eun[†] · Tae-Nam Cho[††] · Ki-joon Chae[†††]
Sang-Ho Lee[†††] · Won-Joo Park[††††] · Jae-Hoon Na[†††††]

ABSTRACT

Multicast services are gradually diversified and used widely. Proportionately, they become the center of attackers' attention and there are growing possibilities of an intelligence leak. Therefore, research related to secure multicast should be required to provide multicast service efficiently. This paper presents the architecture for secure multicast which provides efficient group management mechanism in group consists using member's dynamic join and leave. This architecture can provide secure multicast services to many users with regard to security aspects in one-to-many communication. The simulation results show that the proposed architecture achieves an efficient group management and a secure data transmission with low latency compared with the other existing secure multicast architecture.

키워드 : 안전한 멀티캐스트(secure multicast), 그룹 관리(group management), 분산형 구조(distributed architecture)

1. 서 론

멀티캐스트는 네트워크 상에서 하나의 정보를 실시간으로 그리고 선별된 특정 다수의 수신자에게 전송하는 효율적인 방식이다. 중복된 데이터 스트림으로 인한 병목현상을 없애고, 네트워크 점유율을 낮추어 효율성을 높이며 자원을 절약할 수 있다. 인터넷 기술이 급격하게 발달하면서 원격 화상·음성 회의, 주식 시세 배포, 소프트웨어 다운로드 등의 다양한 그룹 통신 서비스가 활성화되었다. 그러나 현재 효과적인 그룹 접근 제어 기술 결여로 인해 멤버의 가입·탈퇴시 신분위장, 재전송, 부인 공격 등에 노출되어 있고, 네트워크 레벨의 접근 제어가 취약하여 도청, 비인가자에 의한 데이터 생성·변경·파괴, 불법 사용 등의 위협이 존재하게 된다. 또한 멀티캐스트 본래의 광범위한 영역으로 인해 많은 잠재적인 공격의 기회를 제공한다[1]. 그러나 멀티캐스트 보안에 관련된 연구는 아직 초기 단계이고, 다른 인터넷 관련 기술들의 정보보호 연구에 비하여 뒤처져 있는 상황이다.

현재까지 연구된 안전한 멀티캐스트 구조에는 그룹 제어자 유형에 따라 중앙 집중형 구조와 분산형 구조가 있다. 중앙 집중형 구조는 신뢰하는 단일 제어자가 멤버의 가입·탈퇴 처리, 키 분배 등 모든 그룹을 관리하고, 그룹의 멤버들은 하나의 공통된 그룹키를 이용하여 멀티캐스트 통신을 한다. 구조가 단순하고 효율적이지만 그룹의 멤버 수 증가에 따른 확장성 문제와 단일 제어자 의존성 문제가 있다. 멤버의 동적인 가입·탈퇴의 영향을 최소화하고자 분산

※ 본 연구는 한국전자통신연구원 정보보호기술연구본부 네트워크보안연구부 위탁연구 과제에 의한 것임.
† 정 회 원 : 이화여자대학교 과학기술대학원 컴퓨터학과
†† 준 회 원 : 이화여자대학교 과학기술대학원 컴퓨터학과
††† 종신회원 : 이화여자대학교 컴퓨터학과 교수
†††† 준 회 원 : 한국전자통신연구원 연구원
††††† 정 회 원 : 한국전자통신연구원 책임연구원
논문접수 : 2002년 1월 10일, 심사완료 : 2002년 4월 2일

형 구조에 대한 연구가 이루어졌다. 분산형 구조는 하나의 그룹을 여러 서브 그룹으로 나누고, 각 서브 그룹을 관리하는 서브 그룹 제어자가 존재한다. 그러나 중앙 집중 방식에 비해 복잡하고, 각 서브 그룹의 서로 다른 키 사용으로 인해 데이터 전송시 중간에 암·복호화 지연이 존재한다[2, 3]. 또한 암·복호화 시 데이터가 그대로 노출된다는 위험이 있다. 국내에서는 단일 송신자와 다중 수신자로 이루어진 멀티캐스트 환경에서의 보안 구성 요소들과, 분산형 그룹 키 분배를 고려한 연구들이 이루어지고 있다[4, 5].

본 논문은 MSEC과 기타의 연구그룹에서 발행된 표준화 문서들을 바탕으로 효율적인 그룹 관리 메커니즘을 적용하여 안전하게 데이터를 전송하는 멀티캐스트 서비스 구조를 제안하고자 한다. 제안한 구조중, 그룹 관리와 데이터 전송 측면에 초점을 맞추어 통신에 참여하는 수신자의 수와 전송되는 데이터 크기를 변화시켜가면서 멤버의 가입·탈퇴 처리와 보안 메커니즘을 적용한 데이터 전송시간을 측정하고, 기존 구조와 비교·분석한다.

본 논문의 구성은 다음과 같다. 2장에서 제안하는 안전한 멀티캐스트 서비스 구조에 대해 설명한다. 3장에서는 다양한 시나리오의 시뮬레이션을 통해 기존의 구조와 성능을 비교 및 분석하고, 4장에서 결론을 맺는다.

2. 안전한 멀티캐스트 서비스

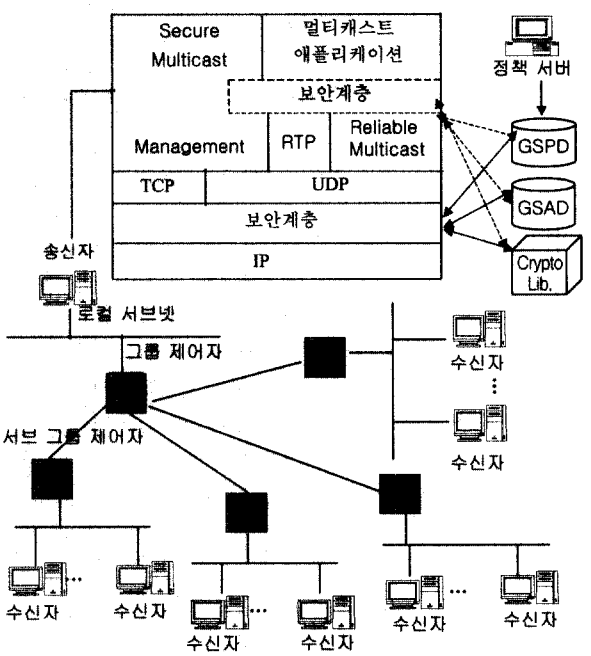
멀티캐스트 보안 구조의 목적은 정당한 그룹 멤버들이 안전하고 효율적으로 그룹 통신을 할 수 있도록 기밀성과 인증을 제공하는 것이다. 이를 위해 멤버의 가입·탈퇴를 처리·관리하는 그룹 멤버쉽 관리 기능이 가장 중요하고, 인터넷상에서 메시지를 안전하게 보내고, 수신된 패킷의 송신원이 정당함을 입증하는 보안 메커니즘들이 필요하다[6, 7]. 안전한 그룹 통신을 위한 보안 정책도 정의되어야 한다. 이러한 요소들을 갖춘 보안 구조는 멀티캐스트 그룹 크기에 영향받지 않도록 확장성과 효율성을 제공해야하고, 키 갱신, 데이터에 보안 메커니즘 적용으로 인한 오버헤드를 줄이며, 새로운 멤버의 가입이나 기존 멤버의 탈퇴로 인한 영향을 최소화해야 한다[8]. 본 장에서는 확장성과 효율성을 제공하는 분산형 그룹 관리를 통해 안전한 멀티캐스트 서비스를 제공할 수 있는 보안 구조를 제안한다.

2.1 보안 구조

단일 송신자와 다수의 수신자 그룹에서 구성될 수 있는 보안 구조 구성요소에 대해 고려하였다. 멀티캐스트 통신은 멀티캐스트 그룹 멤버쉽을 관리하고 멤버들의 접근 제어와 키 분배를 수행하는 제어 관련과 데이터에 암호, 복호, 전자서명 등 보안 메커니즘을 적용하여 전송하는 데이터 전송 두 측면으로 이루어진다[9]. 제안하는 보안 서비스 구조는 (그림 1)과 같이, 하나의 멀티캐스트 그룹을 여러 서브 그룹으로 나누어 멤버의 가입·탈퇴로 인한 새로운키 분배 오버헤드를 줄이고, 각 서브 그룹을 관리하는 서브 그룹 제어자와 전체 그룹을 관리하는 그룹 제어자 두 계층으로 구성된다. 보안 서비스 구조의 구성 요소들을 살펴보면 다음과 같다.

- 송신자 : 그룹 개시자로서, 세션 시작전에 보안 정책을 결정하여 서브 그룹 제어자들에게 미리 분배한다. 데이터에 보안 메커니즘을 적용하여 전송한다.
- 수신자 : 전송받은 데이터를 복호화 또는 인증한다.
- 그룹 제어자 : 서브 그룹 제어자들과 키(GCK : Group Controller Key)를 공유하고, 각 서브 그룹의 멤버들과 공통의 키(GKi : Group Key)를 공유함으로써 그룹을 관리한다. 송신자가 이 역할을 수행하거나 별도의 구성요소로도 존재할 수 있다.
- 서브 그룹 제어자 : 서브 그룹의 키(SGKi : Sub-Group Key)를 관리하고, 멤버의 접근 제어를 수행한다. 전송받은 데이터를 자신의 서브 그룹키로 암호화하여 수신자들에게 전송한다.
- 정책 서버 : 어플리케이션 특징에 따른 보안 요구 사항을 고려하여 그룹의 정책을 결정한다. 송신자가 이 역할을 수행하거나 별도의 구성요소로도 존재할 수 있다.
- 그룹 보안 정책/보안 협상 데이터베이스(GSPD : Group Security Policy Database/GSAD : Group Security Association Database) : 안전한 그룹 통신을 위한 보안 메커니즘과 그룹 관리 정책들에 대해 저장하고 있다.

그룹의 보안 정책, 보안 정책에 따른 제어자의 그룹 관리, 보안 메커니즘을 이용한 안전한 데이터 전송 이 세 가지 측면에 대해 좀 더 자세히 살펴본다.



(그림 1) 분산형 멀티캐스트 보안 구조

2.2 보안 정책

그룹 보안과 관련한 모든 행위, 접근 제어 파라미터, 보안 메커니즘 등을 통틀어서 멀티캐스트 보안 정책이라 정의한다. 멀티캐스트와 같이 다수의 수신자가 존재할 경우, 송신자와 수신자 사이의 통신을 통해 보안 파라미터를 협상하는 방식은 비효율적이다. 그러므로 세션을 시작하는 그룹 개시자 즉, 송신자가 안전한 세션을 위한 보안 파라미터를 정의하여 분배하고, 이를 이용해 서브 그룹 제어자들은 멤버 접근 제어와 키 생성·분배의 역할을 수행하며, 멤버들은 보안 메커니즘을 적용하여 데이터를 송·수신한다. 보안 파라미터는 SA(Security Association)형식으로 저장되고, 세션에 필요한 암호/인증 알고리즘, 암호/인증 키, 암호 초기 벡터, 키 유효기간, 보안 협상 유효기간 정보 등이 포함된다. 안전한 멀티캐스트 통신을 위해 요구되는 보안 정책은 다음과 같다.

- 세션 키 갱신 정책 : 그룹의 멤버들간 안전한 데이터 통신을 위해 이용되는 세션키가 갱신되어야 하는 시점을 정의하고 있다. 주기적 또는 멤버쉽의 변화 발생 시 변경하도록 명시할 수 있다.
- 어플리케이션 메시지 정책 : 어플리케이션 데이터의 보안 요구사항에 따라 적용되는 기밀성, 무결성, 그룹 인증, 소스 인증 등의 보안 메커니즘 유형을 정의하고 있다.
- 접근 제어 정책 : 그룹의 각 멤버들에 대한 역할을 정의하여, 멤버들이 자신의 역할에 맞는 의무와 책임을 하도록 한다.
- 멤버쉽 제어 정책 : 그룹 멤버쉽 정보의 유용성을 명시한다. 어플리케이션 특징에 따라 멤버들이 멤버쉽 정보를 필요로 할 경우, 그룹에 참여하는 멤버들 정보를 키와 같이 전송한다[10].

2.3 그룹 관리

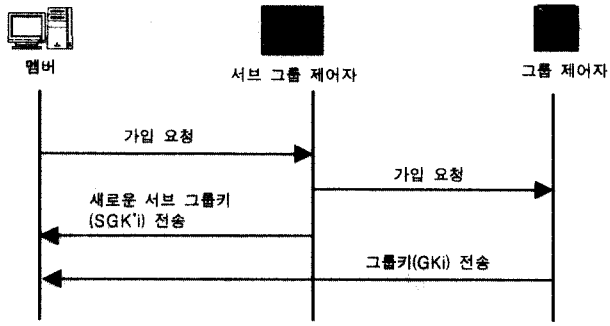
정의된 그룹의 보안 정책에 따라 그룹을 관리한다.

2.3.1 그룹 공표

그룹 개시자인 송신자가 멀티캐스트 세션의 시작을 공개적으로 알린다. SDP(Session Description Protocol), SAP(Session Advertisement Protocol), SIP(Session Initiation Protocol)를 통해 세션의 이름과 목적, 시작 시간, 세션을 이루는 미디어, 미디어를 받기 위한 정보 등을 전송하여 세션의 존재를 알리고, 참가할 수 있도록 충분한 정보를 전달한다[11-13]. 이 때, 보안 요구사항들과 보안 협상 정보도 같이 전송될 수 있다.

2.3.2 멤버 가입

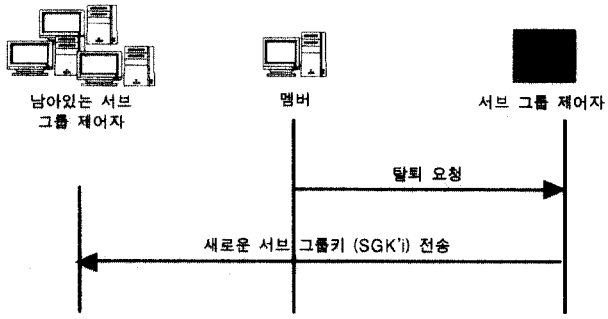
멤버의 가입 요청시, 서브 그룹 제어자는 접근 제어 리스트를 통해 정당한 멤버인지 확인하고, 새로운 서브 그룹키를 생성하여 새로운 멤버와 기존의 서브 그룹 멤버들에게 전송한다. (그림 2)와 같이 멤버는 서브 그룹 제어자로부터 SGK'i를 받고, 그룹 제어자로부터 GKi를 받은 후 멀티캐스트 통신에 참여할 수 있다.



(그림 2) 멤버 가입 과정

2.3.3 멤버 탈퇴

멤버의 탈퇴 요청 시, 서브 그룹 제어자는 새로운 SGK'i를 생성하여 남아있는 서브 그룹의 멤버들에게 전송한다((그림 3) 참조).



(그림 3) 멤버 탈퇴 과정

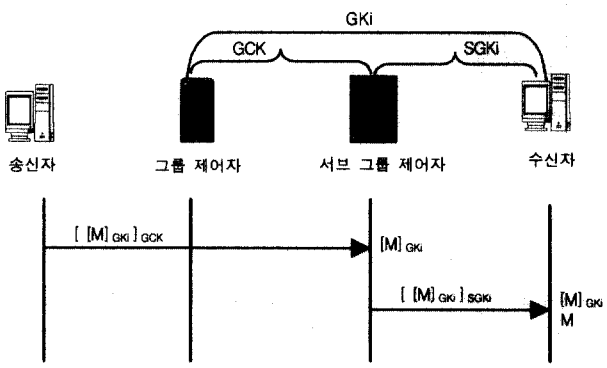
2.4 데이터 전송

2.4.1 보안 메커니즘

특정 세션에 정의된 보안 정책이나, 요구되는 보안 레벨에 따라 기밀성, 무결성, 인증 서비스를 적절히 조합하여 제공한다.

- 무결성 : 데이터의 해쉬값을 데이터와 같이 전송함으로써 전송도중 데이터가 위조·변조되지 않았음을 증명한다.
- 기밀성 : (그림 4)와 같이 대칭키 암호 기법으로 이중 암호화하여 데이터를 전송한다. 송신자가 GKi로 데이터를 암호화하고, GCK로 이중 암호화하여 전송하면, 이를 수신한 서브 그룹 제어자는 GCK로 복호화하고, SGKi로 암호화하여 서브 그룹 멤버들에게 전송한다. 수신자들은 SGKi와 GKi를 이용하여 메시지를 복호화한다.

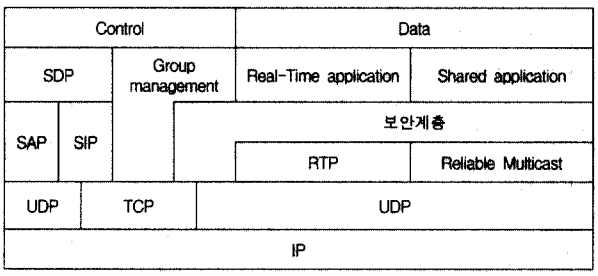
- 그룹 인증 : 데이터의 해쉬값을 GKi로 암호화하여 MAC (Message Authentication Code)을 생성한 뒤 데이터와 같이 전송한다. 수신자는 MAC을 GKi로 복호화함으로써 그룹의 정당한 멤버로부터 데이터가 전송되었음을 보장할 수 있다.
- 소스 인증 : 데이터의 해쉬값을 송신자의 비밀키로 전자 서명하여 전송하면, 수신자가 송신자의 공개키를 이용하여 서명을 검증함으로써 송신자를 인증 할 수 있다.



(그림 4) 데이터 전송 과정

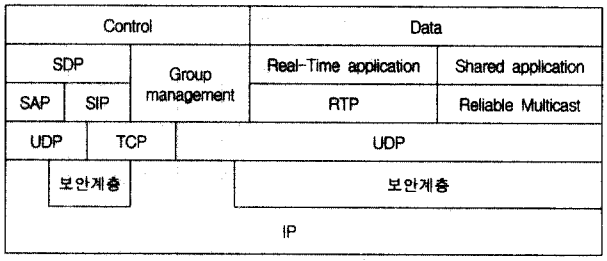
2.4.2 보안 계층

위에서 언급한 보안 서비스들은 네트워크 계층 또는 어플리케이션 계층에서 제공될 수 있다. (그림 5)의 어플리케이션 계층에서의 보안 서비스는 커널 수정을 요구하지 않고, 구현과 적용이 빠르고, 상위 계층의 프로토콜의 성능을 향상시킬 수 있다. 그러나 어플리케이션 데이터에 한정되어 보안 서비스를 제공하기 때문에 트래픽 분석(traffic analysis)과 같은 공격에 쉽게 노출되고, 네트워크 계층에서의 보안 서비스보다 보안 강도가 약하다.



(그림 5) 어플리케이션 계층의 보안 서비스

(그림 6)의 네트워크 계층에서의 IP 보안 메커니즘은 현재 IPsec에 정의되어 있는 ESP, AH를 멀티캐스트로 확장하여 기밀성과 무결성의 강력한 보안 서비스를 제공할 수 있다. 어플리케이션의 변경을 요구하지 않아, 사용자에게 투명한 상태로 처리된다. 반면, 커널 수정이 요구될 수 있고, IPsec이 적용된 곳에서만 가능하다. 신뢰성 있는 멀티캐스트 라우팅 프로토콜이 적용될 경우, 로컬 캐싱이나 제어 정보의 결합을 위해 중간 노드들이 신뢰되어야 하고, 키잉 요소들을 가지고 있어야하는 제약점으로 인해 최선책이 될 수 없다[14]. 그러나 인터넷 프로토콜의 채택시 중요하게 고려되는 확장성을 IPsec은 지원하고 있고, IPv6에서는 IPsec 구현을 의무로 규정하고 있다. IPsec 기술이 인터넷 보안의 기반 기술로 확고하게 자리잡을 것으로 전망되고 있는 시점에서, IPsec에 멀티캐스트를 도입하여 네트워크 계층에서의 안전한 보안 서비스를 제공하는 것이 바람직하다.



(그림 6) 네트워크 계층의 보안 서비스

3. 성능 평가

본 장에서는 위에서 제안한 구조중, 멀티캐스트 환경에서 동적인 멤버쉽 변화를 지원하는 효율적인 그룹 관리 측면과 안전하게 데이터를 전송하는 데이터 전송 측면에 초점을 맞추어 시뮬레이션을 수행한다. 송신자가 전송하는 데이터 크기를 변화시키면서 다양한 보안 메커니즘을 적용하였을 때의 전송 지연과, 그룹에 참여하는 멤버 크기를 변화시켜보며 멤버의 가입·탈퇴 처리 지연을 살펴본다. 시뮬레이션을 위해 UCB(University of California, Berkeley)의 LBNL(Lawrence Berkeley National Laboratory)에서 개발한 ns(network simulator)[15]와 보안 메커니즘 적용을 위한 리눅스 버전의 Crypto++ 4.1[16]을 사용하였다.

3.1 시뮬레이션 환경

멀티캐스트 라우팅 프로토콜인 DVMRP(Distance Vector Multicasting Routing Protocol)를 사용하여 멀티캐스트를 지원한다. CBR(Constant Bit Rate) 트래픽을 0.05초 간격으로 생성하고, 데이터 크기를 64bytes에서 8Kbytes까지 증가시키면서 보안 메커니즘을 적용하여 전송한다<표 1>[17]. 링크 지연은 10ms, 대역폭은 1.5MB와 10MB로 지정하였다.

<표 1> 보안 메커니즘 변수

암호 알고리즘	DES
키 길이	56bits
해쉬 알고리즘	MD5
서명 알고리즘	RSA
서명·인증 키 길이	512bits
데이터 패킷 크기	512bytes

성능 비교 모델은 <표 2>와 같다.

〈표 2〉 성능 비교 모델

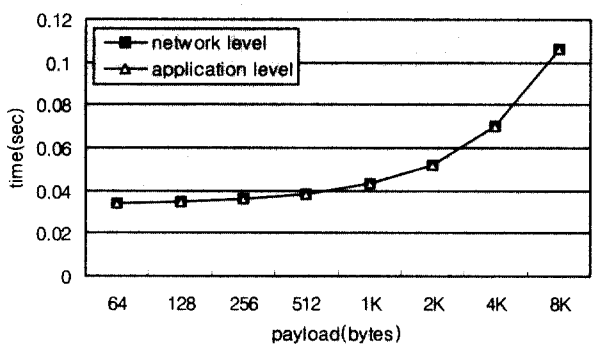
비교 항목	중앙집중형구조 (Centralized)	Iolus	제안한 구조 (DSMA)
구조 유형	중앙 집중 구조	다중 계층의 분산 구조	두 계층의 분산 구조
제어자	단일 제어자	서브 그룹 제어자	그룹 제어자, 서브 그룹 제어자
키	단일 그룹키	서브 그룹키	서브 그룹키, 그룹키

3.2 시뮬레이션 결과 및 분석

3.2.1 호스트 내의 보안 계층에 따른 데이터 지연

멀티미디어 데이터 특성상, 송신자가 중간에서 조각화되지 않을 정도의 작은 크기로 전송한다. 이로 인해 네트워크 계층과 어플리케이션 계층에서의 보안 서비스 차이는 하위 프로토콜에 대한 보안 제공 정도이다. 데이터 크기를 변화시켜가면서 네트워크와 어플리케이션 계층에서 보안 서비스를 적용했을 때, 평균 데이터 전송 지연시간 결과는 (그림 7)과 같다.

데이터 크기가 커질수록 암·복호화 시간이 많이 걸리고, 네트워크 계층에서의 보안이 어플리케이션 계층의 보안에 비해 하위 프로토콜에 대한 보안을 제공하기 때문에 좀 더 시간이 걸리지만, 큰 차이가 나지 않는다. 그러므로 좀 더 강력한 보안을 제공하는 네트워크 레벨에서의 보안 서비스가 권장된다.

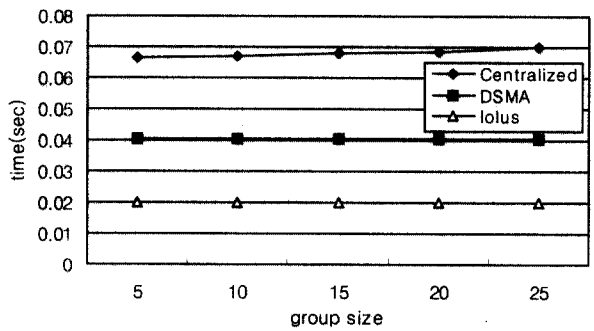


(그림 7) 보안 계층에 따른 데이터 지연

3.2.2 멤버의 가입·탈퇴 처리 지연

● 멤버 가입 처리

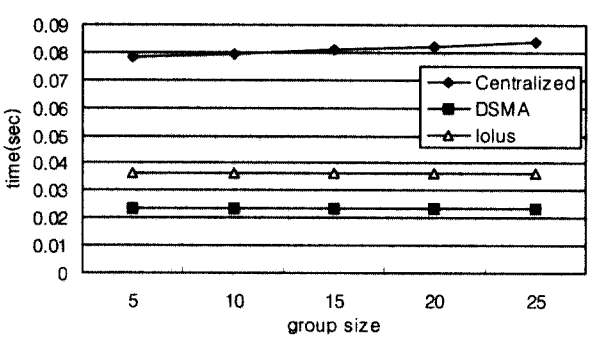
멀티캐스트 통신에 참여하는 멤버들의 수를 증가시키며 새로운 멤버의 가입 요구가 발생했을 때, 가입이 수락되어 새로운 키를 분배받을 때까지의 평균 시간을 측정하였다((그림 8) 참조). 중앙 집중형 구조는 멤버 가입요구 때마다 중앙의 제어자가 새로운 키를 생성하여 분배한다. 멤버의 위치가 단일 제어자로부터 멀리 떨어져 있을수록, 그룹의 크기가 증가할수록 지연이 증가된다. 이에 반해 Iolus는 가입 요청 멤버는 해당 서브 그룹으로부터 새로운 서브 그룹키를 전송받으면 된다. DSMA는 가입요청 멤버가 서브 그룹 제어자로부터 새로운 서브 그룹키를 받고, 그룹 제어자로부터 서브 그룹 멤버들과의 공유키를 받아야만 멀티캐스트 통신에 참여할 수 있다. DSMA는 두 계층으로 이루어져 있기 때문에 그룹 제어자로부터 키를 받아오는데 걸리는 시간은 멤버의 위치에 영향을 받지 않는다. 따라서 DSMA에서의 멤버 가입 처리는 Iolus보다는 지연이 크지만, CSMA보다는 효율적이다. Iolus와 DSMA 모두 멤버의 가입이 한 서브 그룹 내에서만 처리되기 때문에 그룹에 참여하는 멤버의 수가 증가하여도 가입 처리 시간은 일정하다.



(그림 8) 멤버 가입 처리 지연

● 멤버 탈퇴 처리

통신에 참여하던 멤버의 탈퇴 요청시, 새로운 키가 생성되어 남아있는 그룹의 멤버들이 새로운 키를 전송받는데 걸리는 평균시간을 측정하였다(그림 9). 중앙 집중형 구조는 멤버가 탈퇴하면 중앙의 제어자가 새로운 그룹키를 생성하여 남아 있는 모든 멤버들에게 전송한다. 그룹의 크기와 멤버들의 분산정도가 커질수록 탈퇴 처리 시간도 길어진다. Iolus는 탈퇴하는 멤버의 해당 서브 그룹 제어자가 새로운 서브 그룹키를 생성하여 서브 그룹 내의 남아있는 멤버들에게 전송하고, 이웃하는 서브 그룹 제어자들에게 갱신된 서브 그룹키를 알려주면 된다. DSMA 역시 Iolus와 유사한 방식으로 서브 그룹 제어자가 새로운 서브 그룹키를 생성하여 남아있는 서브 그룹의 멤버들에게 전송하면 탈퇴 처리가 완료된다. 이 때, Iolus와는 달리 이웃 서브 그

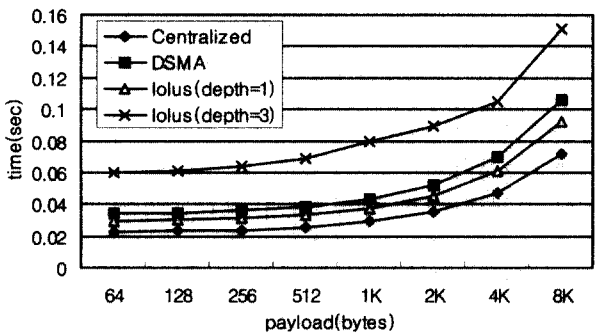


(그림 9) 멤버 탈퇴 처리 지연

룹 제어자들에게 서브 그룹키를 전송하는 지연이 없기 때문에 DSMA의 탈퇴 처리 시간이 제일 짧다.

3.2.3 데이터 전송 시간

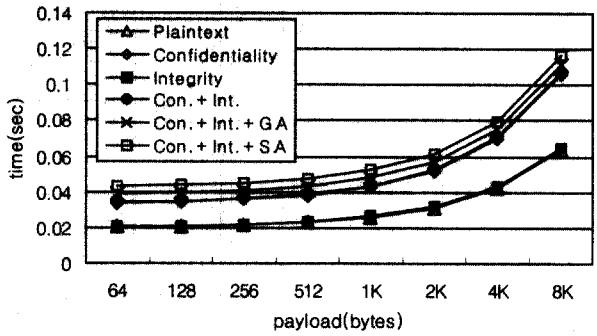
(그림 10)과 같이 512bytes 크기의 데이터를 암호화하여 전송하였을 경우, 평균 데이터 전송시간을 측정하여 비교하였다. 중앙 집중형 구조(Centralized)는 단일 그룹키를 이용하여 데이터를 암호화하여 전송하기 때문에 송신자와 수신자들 양 끝 쪽에서만 암·복호화가 수행된다. 그로인해 데이터 전송 지연시간이 제일 작다. Iolus는 각 서브 그룹마다 서로 다른 서브 그룹키를 가지고 있기 때문에 데이터 전송시 중간에 암·복호화가 수행되어야 한다. 그룹의 계층(depth)이 깊어질수록 중간의 잦은 암·복호화 과정으로 인한 데이터 전송지연이 커진다. DSMA는 이중 암·복호화 프로세싱으로 인한 오버헤드가 존재하지만, 두 계층으로 이루어져있기 때문에 중간에 암·복호화는 한 번만 일어난다. 따라서 Iolus에서 그룹의 계층(depth)이 깊은 경우보다 효율적이다.



(그림 10) 데이터 전송 지연

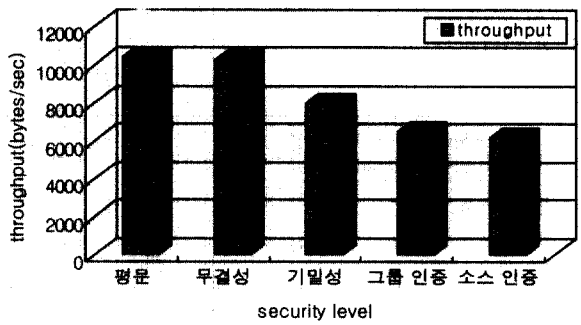
3.2.4 제안한 구조의 보안 강도에 따른 지연과 처리율

어플리케이션들의 보안 요구사항을 고려하여 제안한 분산 멀티캐스트 보안 구조(DSMA)에서 다양한 보안 메커니즘을 적용하였을 때의 평균 데이터 전송 시간을 측정하였다. 메시지의 해쉬값을 이용하여 무결성 서비스를 제공할 수 있다. 해쉬값을 계산하는 시간은 암·복호화 수행 시간에 비해 매우 작기 때문에 (그림 11)에서도 볼 수 있듯이 평문 데이터 전송시간과 별 차이 없다. 즉, 데이터 무결성 서비스는 큰 오버헤드 없이 제공할 수 있다. 기밀성 서비스는 암·복호화 프로세싱 시간으로 인해 평문 전송에 비해 평균 데이터 전송시간이 지연된다. 데이터 크기가 커질수록 암·복호화 시간도 크게 증가하므로 평문 전송시간과 많은 차이가 발생한다. 데이터 자체의 무결성과 기밀성 서비스에서 나아가 데이터가 정당한 사용자로부터 전송되었음을 증명하는 그룹 인증과 소스 인증 서비스를 통해 좀 더 강력한 보안을 제공할 수 있다. 소스 인증은 그룹 인증에 비해 보다 강력한 보안 서비스이지만, 서명과 서명값 검증으로 인한 지연이 크다. 따라서 소스 인증은 모든 데이터 전송에 기본적으로 제공하기보다는 어플리케이션 특징에 따라 정책에 명시된 특정한 경우에만 제공하는 것이 효율적이다.



(그림 11) 보안 레벨에 따른 데이터 전송 지연

보안 메커니즘에 따른 시간당 평균 데이터 처리율 측정 결과는 (그림 12)와 같다. 앞에서 언급했듯이 무결성 서비스를 제공하는 시간은 크지 않기 때문에 평문과 비슷한 데이터 처리율을 갖는다. 기밀성, 그룹 인증, 소스 인증 등 좀 더 강력한 보안 기능이 제공될수록 보안 메커니즘 프로세싱으로 인해 데이터 처리율이 낮아진다.



(그림 12) 보안 레벨에 따른 데이터 처리율

4. 결론 및 향후 연구 방향

네트워크의 혼잡을 줄이고, 멀티미디어 등의 많은 대역폭을 차지하는 애플리케이션을 효율적으로 전달하기 위한 방법으로 멀티캐스트가 등장했지만, 많은 보안상의 취약점을 갖는다.

본 논문은 한 명의 송신자와 다수의 수신자로 구성된 멀티캐스트 통신 상황을 가정하고, 보안 측면을 고려하여 효율적인 그룹 관리를 통해 인터넷 상의 많은 이용자들에게 안전한 멀티캐스트 서비스를 제공하기 위한 구조를 제안하였다. 확장성과 효율성을 고려하여, 그룹 제어자와 서브 그룹 제어자들이 두 계층으로 구성되고, 전송되는 데이터에 대해 IP 계층에서 보안 메커니즘을 적용하여 보다 강력한

보안 서비스를 제공할 수 있다.

시뮬레이션을 수행하여 기존의 보안 구조와 비교·분석한 결과, 제안 구조는 이중 암·복호화 수행으로 인해 그룹의 멤버들이 두 개의 키를 가져야 하므로 멤버 가입시 약간의 지연이 존재한다. 그러나 이중 암·복호화 수행을 통해 기존의 분산형 구조보다 좀 더 강력한 보안을 제공하고, 즉 중간의 암·복호화로 인한 데이터 노출의 위험이 줄어들고, 두 계층 구조로 인해 데이터 전송시 중간의 잦은 암·복호화 오버헤드가 존재하지 않는다. 단순한 데이터 무결성에서 강력한 소스 인증에 이르기까지 강도가 강해질수록 보안 메커니즘 적용으로 인한 지연이 커지므로 어플리케이션의 보안 요구사항에 따라 그에 맞는 정책을 설정·적용하여 안전하고 효율적으로 보안 서비스를 제공할 수 있다.

제안된 구조를 바탕으로 보다 안전하고 효율적인 방식으로 멀티캐스트 서비스를 제공하고, 효율적인 서비스 관리 구조를 이용하여 보안 지원으로 인한 네트워크 부하 및 성능 저하를 최소화하는데 유용한 정보를 제공할 수 있다. 최근 멀티캐스트가 급격한 주목을 받으며 발전하고 있는데 반하여, 멀티캐스트 보안에 대한 기술은 다른 인터넷 관련 기술들의 정보보호 연구에 비하여 뒤쳐져 있는 상황에서 의미를 갖는다.

본 논문에서는 두 계층으로 이루어진 구조로 인해 그룹의 확장성이 다소 떨어진다. 또한 서브 그룹을 관리하는 서브 그룹 제어자들을 둠으로써 보안 기능을 어느 정도 분산시켰지만, 서브 그룹 제어자들을 관리하는 중앙의 그룹 제어자로 인해 단일 노드 실패(single node failure)의 위험을 안고 있다. 이러한 점을 고려하여 좀 더 안전하고 효율적인 보안 구조에 대한 연구가 수행되어야 할 것이다.

참 고 문 헌

[1] P. Kruus and J. Macker, "Techniques and issues in multicast security," Proc. IEEE MILCOM, 1998.

[2] M. J. Moyer, J. R. Rao and P. Rohatgi, "A Survey of Security Issues in Multicast Communications," IEEE Network Magazine, November/December, 1999.

[3] S. Mittra, "Iolus : A Framework for Scalable Secure Multicasting," Proc. ACM SIGCOMM, 1997.

[4] 김봉한, 이희규, 조한진, 이재광, "멀티캐스트 보안 서비스와 보안 구조", 한국통신학회논문지, 제17권 제3호, 2000.

[5] 장주만, 김태윤, "안전한 인터넷 멀티캐스트를 위한 확장성 있는 분산 그룹 키 분배 기법", 한국정보과학회논문지, 제27권 제1호, 2000.

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

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

[8] L. R. Dondeti, S. Mukherjee and A. Samal, "Survey and Comparison of Secure Group Communication Protocols," Department of Computer Science, University of Maryland, 1999.

[9] G. Caronni, M. Waldvogel, D. Sun and B. Plattner, "Efficient Security for Large and Dynamic Multicast Groups," Proceedings of 7th Workshop on Enabling Technologies, (WETICE '98), IEEE Computer Society Press, 1998.

[10] P. McDaniel, A. Prakash and P. Honeyman, "Antigone : A Flexible Framework for Secure Group Communication," Proceedings of the 8th USENIX Security Symposium, pp.23-36, August, 1999.

[11] M. Handley and V. Jacobson, "SDP : Session Description Protocol," IETF RFC 2327, 1998.

[12] M. Handley, C. Perkins and E. Whelan, "SAP : Session Announcement Protocol," IETF RFC 2974, 2000.

[13] M. Handley, H. Schulzrinne, E. Schooler and J. Rosenberg, "SIP : Session Initiation Protocol," IETF RFC 2543, 1999.

[14] P. S. Kruus and J. P. Macker, "Techniques and Issues in Multicast Security," Proc. IEEE MILCOM, 1998.

[15] "The Network Simulator : ns-2," http : //www.isi.edu/nsnam/ns/.

[16] "Crypto++ 4.2," http : //www.eskimo.com/~weidai/cryptlib.html.

[17] "CryptoGraphy," http : //security.kaist.ac.kr/reports/cryptography.html.

은 상 아

e-mail : esa77@hanmail.net

2000년 이화여자대학교 컴퓨터학과 학사

2002년 이화여자대학교 과학기술대학원 컴퓨터학과 석사

20002~현재 삼성전자

관심분야 : 네트워크 보안, 무선이동통신, 네트워크 프로토콜

조 태 남

e-mail : tncho@ewha.ac.kr

1986년 이화여자대학교 전자계산학과 학사

1988년 이화여자대학교 대학원 전자계산학과 석사

1988년~1996년 한국전자통신연구원 선임연구원

1998년~현재 이화여자대학교 과학기술대학원 컴퓨터학과 박사과정

관심분야 : 정보보호, 암호 프로토콜, 알고리즘 설계

채 기 준

e-mail : kjchae@ewha.ac.kr

1982년 연세대학교 수학과 이학사

1984년 미국 Syracuse University 컴퓨터학과 이학석사

1990년 미국 North Carolina State University 컴퓨터공학과 공학박사

1990년~1992년 미국 해군사관학교 컴퓨터학과 조교수

1992년~현재 이화여자대학교 컴퓨터학과 교수

관심분야 : 네트워크 보안, 액티브 네트워크 보안 및 관리, 인터넷/무선통신망/고속통신망 프로토콜 설계 및 성능분석

이 상 호

e-mail : shlee@ewha.ac.kr

1979년 서울대학교 계산통계학과 학사

1981년 한국과학기술원 전산학과 석사

1987년 한국과학기술원 전산학과 박사

1983년~현재 이화여자대학교 컴퓨터학과 교수

관심분야 : 알고리즘 설계, 정보보호, 바이오인포매틱스

박 원 주

e-mail : wjpark@etri.re.kr

1998년 충남대학교 정보통신공학과 학사

2000년 충남대학교 대학원 정보통신공학과 석사

2000년~현재 한국전자통신연구원 연구원

관심분야 : IPsec, IPv6, VPN, 멀티캐스팅, 네트워크 보안

나 재 훈

e-mail : jhnah@etri.re.kr

1985년 중앙대학교 컴퓨터공학과 학사

1987년 중앙대학교 대학원 컴퓨터공학과 석사

1987년~현재 한국전자통신연구원 책임연구원

관심분야 : IPsec, Mobile IP, IPv6, 네트워크 보안