主題

멀티캐스트 보안 서비스와 보안 구조

한남대학교 김봉한, 이희규, 조한진, 이재광

차 례

요 약

데이터(Data), 영상(Video) 그리고 음성(Audio)을 특정 사용자 그룹에게만 전송하는 데이터 전송기술인 멀티캐스트(Multicast)는 효과적인 그룹 접근 제어의 결여와 단일 유니캐스트 통신보다 많은 통신 링크 때문에, 부당한 공격자에게 많은 공격 기회를 제공하고 있다. 이것은 그룹의 수신자에게만 영향을 미치는 것이 아니라 잠재적으로 대부분의 네트워크에 연결된 사용자에게 영향을 미친다. 특히 참가자의 가입과 탈퇴 시에 신분위장, 재전송, 부인공격에 노출되어있기 때문에 이러한 부당한 공격 위협에 대한 보안대책이 필요하다. 본 논문에서는 안전한 멀티캐스트 트래픽 전송을 위한 보안 메커니즘 설계를 위한 기반 기술로서 멀티캐스트에서 보안의 필요성과 멀티캐스트에서 고려해야할 보안 서비스를 분석하고 단일 송신자와 다중 그룹에서 구성될 수 있는 보안 구조 및 보안 구성요소를 연구하였다.

Ⅰ. 서 론

정보통신 기술과 정보매체의 발전으로, 현재 전세계적으로 사용하고 있는 인터넷의 사용 영역은 그 범위가 점차 넓어지고 있다. 이러한 다양한 인터넷 서비스 중에서도 데이터(Data), 영상(Video) 그리고 음성(Audio)을 특정 사용자 그룹에게만 전송하는 데이터 전송기술인 멀티캐스트(Multicast)는 음성 및 영상회의, 중복된 데이터베이스 검색 및 수정, 소프트웨어 수정본의 배포, 음성 및 영상 배포, CSCW(Computer Supported Co-operative Work), 주기적인 정보(주식, 스포츠 경기 기록, 잡지, 신문) 배포, 분산 대화형 모의실험 등 여러 분야에서 사용되는 중요한 통신 메커니즘이다[2 6 9 10]

그러나, 우리가 사용하고 있는 인터넷은 모든 정보가 디지털로 전송되고 통신망 자체가 개방성을 갖기 때문에 중요한 정보 자원에 대한 위협이 날로 증가하고 있다. 그러므로 불법적인 침입자에 의해 우연 또는 의도적인 침입 위협에 대한 대책이 절실히 요구되는 실정이다. 특히, 멀티캐스트 통신은 유니캐스트 통신이나 브로드캐스트 통신에서 발생되는 위협은 물론이고 멀티캐스트-특정 보안 위협에 대한 위험이 증가하고 있다. 이것은 효과적인 그룹 접근 제어의 결여와 멀티캐스트 트래픽이 단일 유니캐스트 통신보다, 좀 더 많은 통신 링크를 통한다는 사실에서 발생한다. 이 때문에, 링크 공격에 대한 상당히 많은 공격 기회를 제공하고 있다[1 4 8].

그러므로, 현재 국외에서는 이러한 보안 위협을 해결하기 위해서, 멀티캐스트 그룹 접근 제어에 의한 그룹의 감염 가능성을 감소시키는 방법과 비인가된 멀티캐스트 트래픽을 검색하고 전송중인 멀티캐스트 트래픽을 채택된 제어를 이용하여 광대역 통신망의 붕괴를 막는 방법에 대한 연구가 진행되고 있다. 하지만 아직 국내에서는 멀티캐스트 라우팅 방식에 대한 연구만 진행되고있고 안전한 멀티캐스트 통신을 보장할 수 있는 보안에 대해서는 전무한 실정이다[11].

따라서 본 논문에서는 멀티캐스트 통신에서의 보안의 필요성, 발생할 수 있는 보안 위협 그리고 고려해야할 보안 서비스를 분석·정리하고, 또한 안전한 트래픽을 전달할 수 있는 멀티캐스트 보안 구조에 대하여 연구하고자 한다.

Ⅱ. 멀티캐스트 개요

멀티캐스팅은 최선의 노력(best-effort)으로 그룹 구성원들에게 신뢰성을 제공한다. 따라서 멀티캐스트 데이터 그램이 그룹의 모든 구성원에게 도착한다는 보장이 없고, 전송과 같은 순서로 도착한다는 보장도 없다. 멀티캐스트 IP 패킷과 유니캐스트 IP 패킷간의 차이점은 IP 헤더의 목적지 주소 필드에 멀티캐스트 D 클래스 그룹 주소(224.0.0.0-239.255.255.255)를 지정한다는 것이다.

멀티캐스트 그룹(multicast group) 구성원(member)인 각 호스트는 언제든지 멀티캐스트 그룹에 가입(join) 또는 탈퇴(leave)할 수 있다. 또,

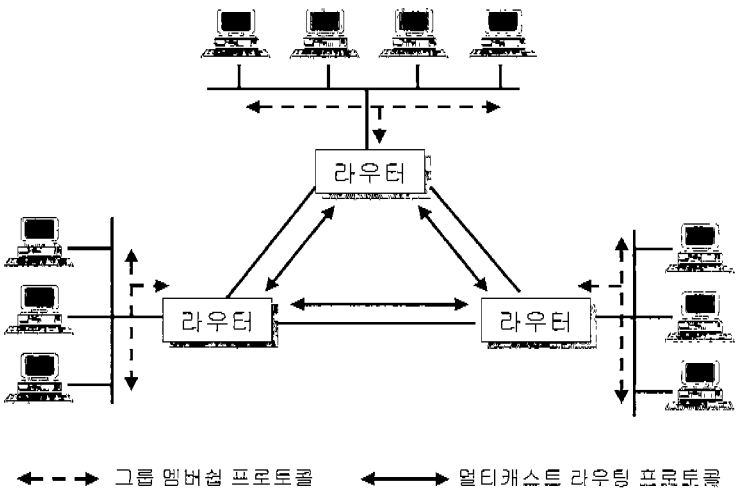

그림 1. 그룹 멤버쉽 프로토콜과 멀티캐스트 라우팅 프로토콜

물리적인 위치와 그룹 구성원 수에 대한 제한도 없다. 따라서, 호스트는 여러 개의 멀티캐스트 그룹에 속하는 구성원이 될 수 있고, 그룹에 속하지 않아도 그룹 구성원에게 메시지를 전송할 수 있다.

라우터는 그룹 멤버쉽 프로토콜(group membership protocol)을 이용하여 자신이 연결된 서브넷에 그룹 구성원이 있는지를 파악한다. 호스트가 멀티캐스트 그룹에 가입할 때, 수신하고자 하는 그룹(들)에 대한 그룹 멤버쉽 프로토콜 메시지를 전송하고, 멀티캐스트 그룹으로 주소 지정된 프레임을 수신하기 위해 자신의 IP 프로세스와 네트워크 카드 인터페이스를 설정한다[2, 6, 9].

멀티캐스트 라우터는 인터네트워크에서 멀티캐스트 데이터 그램을 전송(forwarding)하는 전달 경로(delivery path)를 지정하는 멀티캐스트 라우팅 프로토콜을 실행하게 된다. 이 프로토콜에는 2가지가 있는데, DVMRP(Distance Vector Multicast Routing Protocol)는 거리-벡터 라우팅 프로토콜이고, MOSPF(Multicast Open Shortest Path First)는 OSPF 링크-상태 프로토콜의 확장판이다. 멀티캐스트 라우팅 프로토콜과 그룹 멤버쉽 프로토콜의 관계는 (그림 1)과 같다.

멀티캐스트 주소는 멀티캐스트 그룹에 속하는 수신자를 지정하게 된다. 그래서, 송신자는 모든 그룹 구성원들에게 전달되도록 멀티캐스트 주소를 패킷의 목적지 IP 주소로 사용한다. IP 멀티캐스트 그룹은 D 클래스 주소를 사용하는데, 이의 형식은 (그림 2)와 같다.

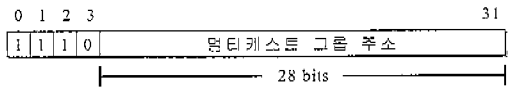

그림 2. D 클래스 멀티캐스트 주소 형식

D 클래스 주소는 상위 4 비트가 1110로 설정되고, 그 다음 28 비트는 멀티캐스트 그룹 ID로 사용된다. IANA(인터넷 주소 할당 기관)는 등록된 IP 멀티캐스트 그룹의 목록을 관리한다. 표준 점-십진 주소로 표현된 멀티캐스트 그룹 주소의 범위는 224.0.0.0부터 239.255.255.255까지 이다. 이 중에서 기본 주소 224.0.0.0은 예비용이기 때문에 그룹에 할당할 수 없다. 224.0.0.1부터 224.0.0.255 범위에 있는 멀티캐스트 주소는 라우팅 프로토콜과 하위-레벨 토폴로지 식별이나 유지관리 프로토콜용으로 예약되어 있다. 이외에 224.0.1.0에서 239.255.255.255는 여러 가지 멀티캐스트 응용을 지정하거나 아직 지정되지 않은 것도 있다. 특히 239.0.0.0에서 239.255.255.255는 인터넷 응용이 아닌 사이트 관리 응용용으로 예약되어 있다.

Ⅲ. 멀티캐스트-특정 공격 형태

1. 멀티캐스트 보안의 필요성

멀티캐스트 통신의 당사자는 그들의 대응되는 그룹 멤버쉽을 특정 사용자/호스트/서브넷으로(예를 들어, 오디오, 비디오 회의) 제한되기를 필요로 한다. 그래서 최근에는 점-대-점 암호화 방식을 사용하기보다는 그룹 제한을 수행할 수 있는 메커니즘을 사용한다. 점-대-점 암호화 방식을 사용하지 않고 그룹의 접근성을 억제하는 방법이 멀티캐스트 그룹 접근 제어(group access control)이다. 그러나 그룹 접근 제어는 링크 공격에 대한 보호를 제공하지 않는다.

그룹 접근 제어 없이, 네트워크에 연결되어 있는 사용자는 단순히 그룹 멤버가 되는 시점에 멀티캐스트 그룹으로부터 데이터를 수신할 수 있다. 이때에 공격자는 고의로 또는 다른 것을 통해 서비스 부인 공격을 수행하기가 쉽다는 것이다. 이것은 그룹의 수신자에게만 영향을 미치는 것이 아니라 잠재적으

로는 대부분의 네트워크에 연결된 사용자에게 영향을 미친다. 더욱이, 광역 멀티캐스트에 의해 전달되는 통신 링크의 수는 통신경로가 단지 하나의 발신지와 목적지 사이에서의 링크와 노드의 모음인 단일 유니캐스트와 비교해서 상당히 많다. 그러므로, 멀티캐스트는 공격자에게 본질적으로 트래픽 가로채기에 대해서 상당히 많은 기회를 제공하고 있다. 다음은 멀티캐스트 통신에서 보안의 필요성을 기술한 것이다[1 4].

- 멀티캐스트 통신의 참가자는 그룹 멤버쉽 제한을 받기 때문에, 현재에 그들 마음대로 사용할 수 있는 메커니즘을 가지고 있지 않다. 그래서, 표현된 그룹에 쉽게 접근할 수 있다. 따라서 공격자(attacker)가 합법적인 그룹 멤버처럼 동작하는 수단을 제공한다.

- IP 멀티캐스트 주소 공간은 공격자가 위치하기 쉬운 이미 잘 알려진 IP 주소 공간을 가진다.

- 그룹으로 멀티캐스트 데이터를 송신하는 것에서 그룹 멤버들 또는 비-그룹 멤버들중 하나를 막을 수 있는 메커니즘이 존재하지 않는다. 이것은 광대역 통신망에서 서비스 부인(항상 밀집하기 때문에) 결과를 가진다.

- IP 멀티캐스트의 전송 프로토콜인 UDP의 사용은 멀티캐스트 송신자에 의해서 발생할 수 있는 밀집을 예방하기 위한 내장 프로토콜 메커니즘이 없음을 의미한다.

- 멀티캐스트는 근본적으로 멀티캐스트 트래픽의 비 인가된 가로채기에 대해서 상당히 많은 기회를 발생시킨다.

트래픽 가로채기에 의한 공격을 멀티캐스트 알고리즘에 의해서 구축된 배달 트리의 형태인 발신지-기반(source-based) 또는 공유 트리(shared tree)에 따라 자세히 살펴보면, 발신지-기반(source-based) 트리에 대해서는 모든 수신자들이 특정 그룹이 활동하는 시점에서의 활성 송신자라면, 완전하게 상호 연결된 통신망에서 그룹의 생존기간동안, 공격자는 잠재적으로 매우 많은 통신 경로의 공격 기회를 가진다. 반면에, 그룹 당 하나의 공유(shared) 배달 트리로 구축된 멀티캐스트 알고리즘은 비교적 공격에 대해 적은 기회를 제공한다. 그래서 공격자는 공격이 수행하고자 하는 곳에서의 통신 경로의 수에 제한을 받는다

2. 멀티캐스트-특정 공격 형태

보안 공격은 적극적(능동적) 또는 소극적(수동적)으로 분류된다. 정보를 노출하는 공격은 수동적이고 메시지 수정 또는 부인은 능동적인 공격이다. 특별히, 멀티캐스트는 다음과 같은 공격 형태에 대해서 상당한 위험을 가지고 있다[1].

2.1 적극적 공격 형태

- 서비스의 부인(Denial of Service)

어떤 멀티캐스트 응용은 대역폭 같은 네트워크 자원의 요구를 강요한다. 멀티캐스트 데이터의 어떤 비 인가된 송신이 서비스의 부인 공격을 구성할 수 있는지에 주목하여야 한다. 이 공격은 모든 인터넷 통신에 심각한 위협을 취하지만 그룹에 데이터를 제한 없이 멀티캐스트 하기 위한 멤버 또는 비-그룹 멤버 능력뿐만 아니라 어떠한 멤버쉽 정책 없이도 멀티캐스트 그룹에 연결하는 능력을 가진 개방된 멀티캐스트 형태에서도 그 영향이 심각하다.

- 신분위장(Masquerading)

종종 스푸핑(spoofing)이라고 불리는 신분위장은 자기 자신이 아닌 다른 식별자를 이용한 주체에

의해 정보의 발행, 정보의 수신 또는 접근 권한의 획득에 관여한다. 이것은 사용자를 위한 IP 패킷의 네트워크층 헤더에 가짜 발신지 주소를 삽입하기가 상대적으로 쉽기 때문에 침입자는 어떤 다른 합법적인 멀티캐스트 그룹 멤버처럼 위장하는 능력을 가질 수 있다.

역 경로 전송(reverse-path forwarding)에 기반을 둔 멀티캐스트 알고리즘은 발신지에 도착하는 것보다 인터페이스에 도착하는 멀티캐스트 패킷을 버리기 때문에, 신분위장에 대해서 함축적인 안전장치(safeguard)를 구성한다. 그러므로 공격자는 공격의 성공을 위해서 멀티캐스트 라우터의 관점에서 인증된 발신지를 위한 최단 역-경로에 존재해야 한다.

• 부당한 재전송(Malicious Replay)

재전송 공격은 공격자가 가로챈 정보를 가지고 나중에 이것을 재 전송하는 것을 말한다. 그러므로 서비스 부인을 할 수 있다. 서비스 부인은 멀티캐스트 패킷 분배의 "곱수 효과(multiplier effect)" 때문에 유니캐스트에서만 발생하는 것보다 대부분의 인터네트워크에 영향을 준다.

• 부인(Repudiation)

부인은 특정한 통신의 일부분 또는 참가하고 있는 모든 주체에 의해 부인된다. 이것은 신분위장에 의해 직접적으로 발생할 수 있다. 유니캐스트에서는 단지 하나의 수신자만 영향을 받지만 멀티캐스트에서는 영향받는 수신자의 수가 그룹 수신자들의 수와 비례한다.

2.2 소극적 공격 형태

• 트래픽 관찰(Traffic Observation)

종종 도청이라고 불리는 트래픽 관찰은 통신 당사자간의 정보의 가로채기와 관련이 있다. 그래서 트래픽 형태, 내용, 빈도, 주파수, 존재/부재, 통신량과 같은 정보 누출이 발생된다.

이러한 보안 위협에 대해서, 그룹 접근을 제어하는 능력을 가지는 것은 필수적이고, 그룹 수신자들은 그들이 수신한 데이터의 무결성(integrity), 인증(authenticity)과 선명성(freshness)을 확신해야 한다. 동시에, 음성과 같은 실시간 트래픽을 전송하는데 부과되는 필수적이지 않은 지연이 없도록 하는 응용의 중요성이 증가하고 있다.

Ⅳ. 멀티캐스트 보안 서비스

멀티캐스트 보안 구조 설계는 네트워크 프로토콜과 네트워크 사이트, 그리고 네트워크 사이트와 호스트간(멀티캐스트관리 센터로서 기능을 하는)의 믿을 수 있는 관계에 많은 제어 기능을 배치하도록 고려해야 한다.

바람직한 보안 설계는 기존의 네트워크 프로토콜과 호환되고 광역 인터넷의 범위로 확장할 수 있으며, 투명성을 가져야한다. 그래서 상위 레벨 응용과 서비스가 인증, 자격, 정책의 검사와 같은 세부항목에 대해서 자유로워야 한다. 특히, 세션과 표현 층에 존재하는 보안 메커니즘은 근원적인 네트워킹 메커니즘에 제한을 받지 않는다. 그러므로, 네트워크에서 전송과 교환 요소의 수정을 요구하지 않을 것이다. 또한, 보안 구조는 상위 레벨 응용에 의해 요구되는 것과 같이, 높은 다양한 세션 제어의 정책을 지원하는데 유연해야 한다. 이들 특징들은 인터넷과 같은 기존의 환경에 믿을 수 있는 멀티캐스트를 쉽게 통합시킬 수 있게 한다[4, 5, 7].

1. 인증

인증은 기존의 세션에 가입하도록 요구하는 멀티

캐스트 주소와 스크린 호스트의 등록을 제어하기 위한 신뢰받는 멀티캐스트에서 필수적인 메커니즘이다. 때때로, 가입을 요구하는 참가자와 기존의 세션 멤버는 상호 인증을 요구한다. 경우에 따라, 한 참가자는 다른 참가자에게 인증을 위임하기도 한다.

멀티캐스트 인증에서는 두 가지의 고려해야할 사항이 있다. 하나는 그룹의 멤버쉽을 누가 제어하는가 그리고 어떻게 그러한 멤버쉽 정책을 집행하는가이다. 다른 하나는 존재하고 있는 그룹에 허가되기 위해서 무엇을 구성해야 하는가 이다.

익명성을 가진 세션의 경우를 제외하고, 그룹에 속하기 위한 최소한의 요구사항은 새로운 참가자가 모든 또는 몇몇의 기존 멤버에게 소개되어야 한다는 것이다. 이 소개는 새로운 참가자의 이름 같은 식별 사항을 공지하고 이 소개는 어떤 멤버에 의해서 특히 그룹 리더에 의해서 수행될 수 있다. 좀 더 강한 요구 사항은 각각의 기존 멤버와 새로운 참가자가 초기 소개 절차 후에, 성공적으로 상호 인증해야 된다는 것이다. 더욱 강한 요구는 모든 다른 멤버가 새로운 참가자에 대해 안다는 것을 다른 모든 멤버가 또한 알아야 한다는 것이다.

인증을 요구하기 위해서는, 비록 인증 수행이 새로운 참가자가 그룹을 가입함으로서 가입 절차가 증가하더라도, 크기 n의 그룹에 대한 인증 프로토콜의 $O(n^2)$에 수행되기를 요구한다. 그러나 이것은 인증 절차에 상당한 분담을 가지게 한다. 그래서 좀 더 효과적인 방법은 새로운 멤버를 확실히 인증하기 위해서 다른 그룹 멤버에 의해 신뢰받는 그룹 리더를 선택하는 것이다. 이 경우에서, 그룹 리더는 사실상 그룹 멤버쉽 정책을 제어한다. 자연적인 그룹 리더 선택은 세션 초기자를 그룹 리더로 하는 것이다. 세션 초기자가 세션을 등록할 때, 이것은 그룹 리더가 되고 입회 정책을 명시한다. 만약 그룹 리더가 고장나고 임기 만료되면, 새로운 리더가 세션 정책에 의해, 안전한 프로토콜을 통해서 선택되어야 한다. 몇 몇 멤버는 정책과 일치하는지를 검사하기 위해 그룹 리더의 행동을 모니터할 수도 있다.

멤버가 자진해서 또는 다른 이유로 세션을 탈퇴할 때, 멤버는 정확히 종료(sign off)하여야 한다. 이를테면 그룹키와 같은 세션과 관계된 민감한 정보를 반드시 제거하여야 한다. 그렇게 하지 않으면, 이 멤버는 그룹에 가입하지 않고 나중에 도청을 할 수 있다. 또한 탈퇴한 멤버의 잔류 정보가 잠재적인 공격자에 의해 부당하게 이용될 수 있다. 정상적인 멤버가 잔류 정보의 제거를 잃어버릴 수 있기 때문에, 이점에서 그룹키를 갱신하도록 하여야 하고 그룹은 향후의 토론에 대해 탈퇴한 참가자가 참가할 수 없도록 만들기 위해서 그를 종료시킬 것이다. 멤버의 상태는 "heart-beat" 메시지를 교환하는 것과 같은 다수의 방법에 의해 모니터될 수 있다.

2. 안전한 세션

그룹 지향 분배 시스템에서는 안전한 세션을 위해서 다음과 같은 몇 가지 사항을 고려해야한다.

2.1 세션 멤버쉽 정책

세션은 다양한 형태의 멤버쉽 정책을 가지고 다양한 목적을 위해서 설정될 수 있다. 멀티캐스트 관리를 위해서 몇 가지 일반적인 정책이 존재한다. 첫 번째는, 참가자가 허가 없이 자유롭게 참가할 수 있는 USENET 뉴스그룹과 같은 개방 세션이고, 두 번째는 도시의 특정 건물처럼, 참가자가 자유롭게 참가할 수 있는 개방된 세션이지만 참가자는 안전 검사를 통과해야 하고, 세션 중개자가 있어야 하는 반-개방 세션이다. 마지막으로, 의회의원들만이 참가할 수 있는 의회회의와 같은 제한된 세션이다. 때때로 비-멤버가 참가하지만 대부분의 기존 멤버가 동의할 때만 참가할 수 있다. 이처럼, 구조는 다양한 정책을 조정하는데 충분히 유연해야 한다. 그래서 각 개별적인 응용 또는 각 세션은 하나의 정책 또는 기본 정책들의 집합을 구현하도록 선택할 수 있다.

2.2 등록과 등록 취소

호스트 또는 사용자가 멀티캐스팅 세션을 확립하기 위해서 네트워크 주소를 요구할 때, 멀티캐스팅 관리 센터(MMC: Multicasting Management Center)는 요청자의 식별을 검증하고 세션을 등록할 수 있는 자가 요구하는 세션 정책을 검사한다. 요청자는 세션이 정확하게 등록되도록 MMC의 식별을 검증하기를 바랄 것이다. 멤버쉽 정책, 사용자 증명서, 등록된 세션의 기록 같은 정보는 접근 제어 목록형태의 MMC에 저장된다.

MMC는 중앙집중 서비스 또는 분산 서비스가 될 수 있다. 네트워크에 하나 이상의 MMC가 있을 때, 멀티캐스트 주소의 일관성 및 유일성을 보증하기 위해 각각의 MMC는 조화롭게 구성되어야 한다. 각각의 MMC는 동일한 입회 정책을 채택할 수 도 있고 채택하지 않을 수도 있다.

MMC에서 세션이 도착하는 것을 등록 취소하도록 요청할 때는 요청자를 인증해야 하고 만약 이러한 요구에 대해 인증이 되면 종료한다. 일반적으로 세션 리더 또는 이것의 대리인만이 세션을 등록 해제할 수 있다. 세션 리더가 고장나거나 등록 해제하는 것을 잃어버릴 때에는 주기적으로 모든 등록된 세션의 활동을 검사하는 MMC를 가짐으로서 죽은 세션(dead session)을 쓰레기로 수집할 수 있다. 만약 멀티캐스트 세션이 바람직하지 못하면 세션은 종료된다.

2.3 세션 가입과 탈퇴

세션 멤버사이의 통신은 공개적으로 또는 개인적으로 할 수 있다. 이러한 사항은 등록 시간에 명시하고 나중에 변경할 수도 있다. 이것은 개별적인 멤버의 재량에 따라 속성을 가짐으로서, 몇 몇 통신은 공개적인 통신을 하면서 동시에 개인적인 통신을 할 수 있다. 대부분의 네트워크는 네트워크 트래픽 도청에 의해 공개되기 때문에, 멀티캐스트에서 개인적인 세션을 위해서는 충분한 프라이버시 준비가 요구된다. 가입과 탈퇴가 요청될 때, 인증된 자만이 메시지를 정확히 복호화할 수 있도록 보증하기 위해서 메시지 내용을 암호화 필요가 있다.

2.4 안전한 세션 통신

안전한 세션을 통신을 위해서는 다음과 같은 방법이 사용된다. 모든 세션 멤버에 의해서 공유된 공통 암호화키의 분배를 사용하고 이 그룹 키를 이용해 브로드캐스트 메시지를 암호화하는 것이다. 이 접근을 이용하여, 초기 키 분배는 세션이 등록될 때 발생해야 한다. 이 키는 세션 리더 또는 인증 서버에 의해 선택될 수 있다. 이 키는 세션 리더에 의해 유지되거나 세션이 등록되는 MMC에 저장된다. 누군가가 세션에 가입될 때, 그룹 리더 또는 MMC는 세션 정책을 검사한다. 새로운 멤버가 세션으로 받아들여질 때, 이것은 MMC 또는 그룹 리더로부터 그룹 키를 수신한다. 그룹 리더가 고장나면, 기존에 많이 알려진 선택 프로토콜을 이용하여 새로운 리더가 선택된다.

이 방법의 중요한 단점은 만약 세션 멤버가 부당한 사용자라면, 그룹키는 메시지의 발신지를 식별하지 않는다는 것과 트래픽이 많은 세션일 경우, 그룹 멤버들 사이의 동기화를 위한 빈번한 키 변경은 수행 성능을 위해서 매우 바람직하지 않다는 것이다. 따라서 아래의 안전한 브로드캐스트 알고리즘은 이 두 개의 문제점을 완화시킬 수 있다.

2.5 안전하고 효과적인 브로드캐스트

멤버는 새로운 멤버쉽을 위해서 메시지 당 새로운 암호화키를 선택할 수 있다. 그러므로 탈퇴하는 멤버에 의한 키 누출의 위험은 상당히 감소되고 새로운 그룹 키를 할당할 필요가 없다.

각 멤버는 공개키와 개인키를 지원하는 RSA 암호화 시스템을 사용할 수 있다. 멤버는 적어도 모든 다른 멤버들의 공개키와 같은 기본적인 그룹 멤버쉽에 대한 지식을 가져야한다. 메시지를 브로드캐스트

하기 위해서, 멤버는 랜덤하게 암호화 키(DES에서 사용하기 위해)를 선택하고 메시지를 암호화한다. 멤버는 이때에 개인키를 이용하여, 타임스탬프(재전송 공격을 방어하도록), DES 키, 원 메시지의 단방향 해쉬 함수(무결성 체크섬을 제공하기 위해)를 서명한다. 멤버는 이때에 서로 멤버의 공개키를 이용하여 이 서명을 암호화한다. 마지막으로, 암호화된 서명과 암호화된 메시지를 n-1 번 브로드캐스트(또는 멀티캐스트)한다. 분명한 것은 그룹 멤버가 아닌 다른 사람은 메시지를 수신할 수 없다. 이 간단한 알고리즘은 다음과 같은 특징을 가진다.

- 암호화키는 모든 메시지에 대해 변경된다. 그러므로 멤버쉽은 그룹 키를 변경하는 것처럼 추가적인 보안 대책을 요구하지 않는다
- 메시지 몸체가 아닌 메시지 헤더(암호화된 서명을 포함하는)는 목적지 숫자만큼 산술적으로 증가한다. 더욱이, 단방향 해쉬 함수의 연산은 매우 효과적일 수 있고 체크섬은 적은 여분의 바이트만을 추가한다.

이 브로드캐스트 프리미티브를 사용하기 위해서, 세션 멤버는 다른 공개키와 다른 관련된 데이터를 수신하고 캐쉬한다. 세션 멤버쉽 변경을 통고할 때, 멤버는 탈퇴자를 포함한 세션의 외부에 있는 사람이 판독할 수 없도록, 간단히 그들의 로컬 멤버쉽 목록을 갱신하고 미래의 멀티캐스트를 위해서 새로운 DES 키를 선택한다.

2.6 암호화 모드

Electronic Code Book(ECB) 모드를 사용하는 것은 일반적으로 바람직하지 않다. ECB 모드는 각 블록이 독립적으로 암호화되기 때문에, 슬라이싱 공격과 해독에 대해서 공격받기가 쉽다. 평문-피드백 모드에서 블록의 암호화는 이전 블록의 평문에 의존한다. 이것은 만약 이전 의 모든 블록이 정확히 복호화되지 않는다면 현재의 블록도 정확히 복호화할 수 없다. 따라서 네트워크 또는 스트림이 신뢰할 수 없을 때에는 과도한 재전송이 필요하다. 암호문-피드백 모드는 제한적이지만 제어할 수 에러 전달을 가진다. 2개의 연속적인 암호문이 수신되는 동안, 복호화는 계속되고 재 동기화는 자동적으로 수행된다. 더욱이 오디오와 비디오 처리에 관련이 있는 응용에서는 이 모드를 선택하는 것이 유리하다.

멀티캐스트는 응용 환경에 따라, 다중 암호화 모드들 사이와 블록 암호화와 스트림 암호를 이용하는 사이에서 요구될 수 있다. 예를 들어, ECB 모드는 메시지의 개별적인 블록에서 랜덤 접근을 허가한다. 또한 스트림의 사전연산이 가능한 스트림 암호화는 일반적으로 블록 암호보다 빠르지만, 데이터 손실이 발생할 때 재 동기화의 비용 때문에, 높은 신뢰를 가지는 환경에서 더 적당하다.

마지막으로, 스트림의 일부분만 암호화하는 경우를 고려해야 한다. 전체 스트림을 암호화하는 것은 효율성 때문이다. 반면에, 부분 암호화는 스트림의 암호화 시간과 복호화 시간을 줄여준다. 따라서 여분의 시간을 화상의 해상도나 오디오 음향 처리에 사용할 수 있다. 예를 들어, 그림의 배경은 공개적이지만 가운데의 사람 이미지는 특별한 처리를 요구하는 경우에 유용하다.

2.7 세션 통지

많은 서비스는 통지되어질 필요가 있다. 등록된 세션은 게시판 서비스와 같은 것에 의해서 고유의 증명서와 신원 정보를 제공하여야 한다. 그래서 이들은 통지의 인증을 검증할 수가 있다. 경우에 따라서는 서비스 정보의 통지를 제한할 필요도 있다. 이런 경우에는 게시판을 안전한 다중레벨 형태로 만들어야 한다.

3. 트리 접근의 제어

인증은 단지 공인된 사용자가 합법적인 참가자가

되는 것을 보증한다. 그리고 그룹-지향 암호화는 단지 이 참가자가 전송되어온 데이터를 복호화하도록 할 수 있도록 하는 것이다. 아직까지는 네트워크 레벨 멀티캐스트 라우팅과 전송 메커니즘이 사용자가 마음대로 트래픽에 삽입하고 트리로의 경로를 확립할 수 있도록 허가한다. 그래서 분배된 트리로 물리적 접근을 제한하는 네트워크 레벨 메커니즘을 채택하도록 하여야 한다.

네트워크 교환에 대한 종단 사용자의 인증 처리는 대등 호스트사이에서의 인증과는 다르다. 먼저, 저장과 처리 제한 때문에, 교환은 네트워크에 연결된 모든 호스트를 위한 공개키 또는 개인키들을 유지할 수 있다고 예상되지 않는다. 더욱이, 동시에 연결이 초기화되면, 교환하는 것을 알지 못하는 호스트는 이것의 요청을 지원하도록 그들의 라우팅 테이블을 실제로 변경할 것이다.

각 네트워크 교환은 하나 또는 그 이상의 인증 서버에 소유되는 개인키와 대응하는 공개키를 유지한다. 새로운 연결이나 기존 연결의 수정을 위한 요청을 초기화하기 전에, 호스트는 먼저 인증 서버에 요청 메시지를 전송한다. 호스트를 인증한 후에, 서버는 서명이 첨부된 메시지를 반환 전송한다. 메시지는 네트워크 경로를 따라서 전송되고 경로의 모든 교환은 서명에 대하여 지역 서버의 공개키를 이용하여 검사한다. 또한, 트래픽에 삽입되기를 원하는 노드는 서버로부터 서명을 먼저 획득해야 한다. 네트워크 노드는 이러한 서명 없이 발신지로부터 트래픽을 받아들일 수 없다.

수신자의 인증은 상대적으로 드물게 수행됨으로 교환에서 큰 처리 부담을 가지지 않는다. 반면에, 비인가된 발신지를 막기 위해서, 패킷에 서명을 전송하는 것은 교환에서 부담을 가중시킨다. 특히, 화상과 같은 스트림 트래픽에서 더욱 심각하다. 스트림 트래픽 교환을 위해서는 단지 패킷의 일부분이 서명을 운송하고 교환은 이들 서명을 운송하지 않는 패킷의 전송을 위해서 서명을 캐쉬 해야 한다. 캐쉬는 가끔 갱신되어야 한다.

정크 패킷을 이용하여 멀티캐스트 주소를 플르딩하거나 가짜 멀티캐스트 세션을 설정함으로서 악의있는 참가자는 네트워크 자원을 공격할 수 있다. 따라서 가능하면 멀티캐스트 발신지의 근처에서 이러한 정크 패킷을 식별하여 막도록 하여야 한다. 그렇지 않고 목적지에서 정크 패킷을 식별하면 그것이 목적지에 도착할 때까지 귀중한 네트워크 자원이 소비되어진다.

4. 확장성과 최적안

사용자 또는 호스트 인증을 위해서 할당되는 초기의 암호화키의 과제는 안전한 멀티캐스트에 참가하고자 하는 사용자 또는 호스트의 숫자가 산술적으로 커진다는 것이다. 세션을 확립하기 위해서, 세션 멤버쉽을 교환하기 위한 메시지의 숫자는 세션 크기에 따라 커진다. 안전한 브로드캐스트 알고리즘은 메시지 기반에서 동적인 암호화 키 변경을 허가한다. 그러므로 그룹 멤버쉽 변경에서 새로운 그룹 키를 요구하는 것을 제거할 수 있다. 그러나 가입과 탈퇴가 더 이상이 발생하지 않는 상태가 되면 그룹 멤버쉽이 적당히 안정되어 메시지를 기반으로 하는 암호화 방식보다 그룹 키를 사용하는 것이 좀 더 효과적이다.

때때로, 세션의 멤버는 많은 양의 그룹을 형성한다. 예를 들어, 원격회의 응용에서, 비록 모든 멤버들의 음성이 모든 목적지에 브로드캐스트 되더라도, 멤버는 단지 자신의 근처에 있는 멤버에게만 물리적 위치 정보(자신의 좌표)를 브로드캐스트 하기를 원할 것이다. 이 같은 그룹을 구성하기 위해서, 데이터 암호화키는 메시지 당 키를 동적으로 선택할 수 있기 때문에, 멤버는 다수의 그룹의 키를 저장할 필요가 없다. 물론 멤버는 멤버쉽 변경이 발생할 때까지 데이터 암호화키를 저장하고, 서명된 메시지 헤더를 대응시키고, 그들을 재 사용함으로서 최적화될 수 있다.

5. 다중레벨의 안전한 멀티캐스트

그룹들과 멤버들은 서로 다른 레벨로 분류될 수 있다. 그리고 참가자는 자기 자신보다 높은 보안 레벨을 가진 그룹의 멤버가 될 수 없다. 또한 레벨은 암호화키를 할당받고 레벨이 좀 더 높은 곳의 키에 대해서는 접근할 수 없다. 암호화를 위해서, 키의 레벨은 평문의 레벨보다 동등하거나 높아야한다. 암호문의 레벨은 이때의 키의 레벨이다. 이러한 할당은 가상 네트워크로 멀티캐스트 네트워크를 효과적으로 분리한다.

다중 레벨 보안은 높은 레벨 그룹 멤버가 낮은 레벨 정보를 접속할 수 있음을 요구할 것이다. 이것을 확립하는 하나의 방법은 낮은 레벨 그룹 멤버가 멀티캐스트 메시지를 높은 레벨의 그룹에게 전송할 수 있도록 하는 것이다. 그런데, 송신자가 일반적으로 적당한 높은 레벨의 암호화키를 가질 수 없기 때문에, 높은 레벨 멤버가 낮은 레벨 키를 사용할 수 있도록 하거나 낮은 레벨 키를 이용해서 전입 메시지를 복호화하고, 메시지를 중계하기 전에 높은 레벨 키를 이용해서 메시지를 재 암호화하는 게이트웨이를 다중 레벨 네트워크 구성요소에 포함시키는 것이다.

V. 멀티캐스트 보안 구조

1. 멀티캐스트 보안 구성 요소

(그림 3)은 단일 송신자와 다중 수신자 환경에서의 멀티캐스트 구성요소이다. 일반적으로, 구성요소는 두 개의 그룹으로 구성된다. 하나는 이들 현재의 불안전한 멀티캐스트 또는 브로드캐스트 통신 구조와 매우 비슷한 구성요소를 다루는 데이터 관련 그룹으로서, 이들은 송신자, 수신자 그리고 하나 또는 더 많은 데이터 멀티캐스트 그룹으로 구성된다. 다른 하나는 키 협정과 교환 처리에 연루된 모든 구성요소를 포함하는 제어 관련 그룹(키 관리)이다[4].

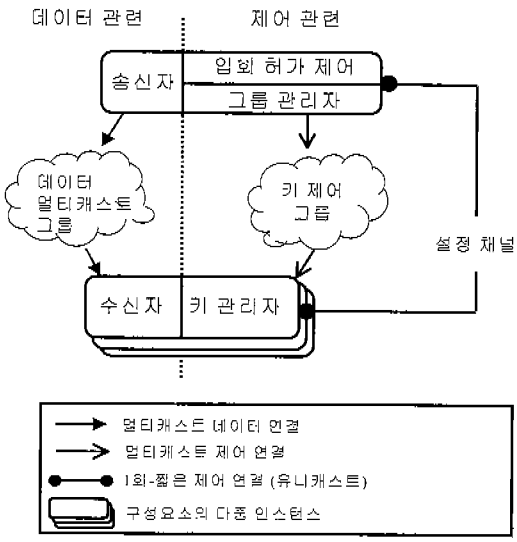

그림 3. 단일 송신자, 다중 수신자 환경에서의 멀티캐스트 보안 구조

• 송신자(Sender)

응용은 불안전한 전송에 대해서 동작하는 데이터를 준비한다. 이때에, 그룹 관리자로부터 수신된 현재의 트래픽 암호화 키(TEK: Traffic Encryption Key))를 이용하여 패킷을 암호화한다.

• 수신자(Recipient)

데이터 멀티캐스트 그룹으로부터 데이터를 수신하고 로컬 키 관리자로부터 주어진 TEK를 이용하여 이것을 복호화한다.

• 데이터 멀티캐스트 그룹(Data Multicast Group)

멀티캐스트, 브로드캐스트, 또는 애니캐스트 채널은 적어도 의도된 수신자에게 송신자로부터 안전한 패킷을 전달한다. 이것은 대부분의 응용 데이터를 전송하는데 사용된다.

• 그룹 관리자(Group Manager)

참가자로부터 가입과 탈퇴 요청을 수신하고 허가하고 처리한다. 그리고 필수적인 키 교환을 수행하기 위해 키 관리자에게 메시지를 송신한다.

• 입회 제어(Admission Control)

누가 허가되는지를 찾기 위하여 그룹 관리자에 의해서 질의된다. 이 기능은 예를 들면 회의에서의 의장과 같은 사람에게 위임될 수 있다.

• 키 관리자(Key Manager)

수신자에게 TEK를 전달하는 그룹 관리자로부터 재 키잉 요청을 수신하고 복호화한다

• 설정 채널(Setup Channel)

새로운 멤버로부터의 가입 요청은 항상 이 유니캐스트 연결 또는 다른 out-of-band 메커니즘을 통해 수신된다. 이 채널은 새로운 참가자와 그룹 관리자 사이에서 인증을 수행하기 위해서 가입 요청을 부트스트랩 하도록 요구된다.

• 키 제어 그룹(Key Control Group)

멀티캐스트, 브로드캐스트 또는 애니캐스트 채널은 그룹 관리자로부터 의도된 수신자에게 패킷을 전달한다. 트래픽은 참가자의 키 관리자에게 분배되는

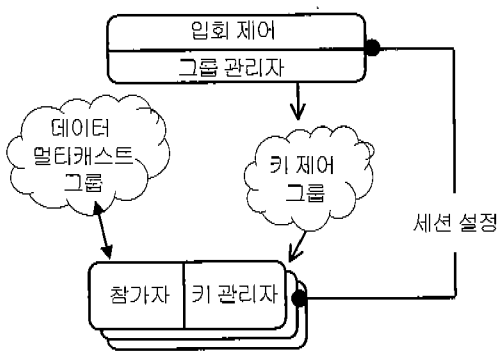

그림 4. 다중 그룹 통신 환경에서의 멀티캐스트 보안 구조

새로운 키잉 재료로 구성된다. 이 채널을 통한 전송은 모든 참가자들에게 수신되어져야 한다. 어떤 이유에 의해서 수신자가 정당한 시간에 패킷을 수신할 수 없다면, 그룹 관리자와 다시 접속한다. 이것은 또한 반환 채널이 없을 때, out-of-band를 이용하여 수행할 수 있다.

때에 따라서, 하나 이상의 송신자와, 송신자들과 수신자가 구별되지 않는 그룹 통신이 존재 할 수 있다. (그림 4)에서 보여주는 상황과 같은 그룹 환경에서 모든 그룹의 멤버는 송신과 수신을 할 수 있다. 이것은 송신자와 수신자가 통합되고 그룹 관리자가 분리되는 (그림 3)의 변형이다. 송신자와 수신자가 동등하게 다루어진다면, 송신자와 수신자를 구별하지 않고 "참가자(participant)"라는 용어를 사용한다.

2. 멀티캐스트 그룹에서의 기본 동작

트래픽 암호화키를 안전하게 전송하기 위하여, 다수의 키 암호화 키(KEK: Key Encryption Key)는 TEK를 포함하는 제어 트래픽을 암호화하도록 사용된다. 키들을 구별하기 위하여, 각 키는 유일한 ID, 버전(Version), 개정(Revision), 그리고 적당한 키잉 재료로 구성된다. 위에서 말한 구성요소와 키는 다음과 같은 동작을 수행할 때 사용된다.

• 그룹 생성(Group Creation)

그룹 관리자는 그룹과 접근 제어 정보를 가지고 구성된다. 추가적으로, 그룹 파라미터는 디렉토리 서비스를 이용하여 발행된다.

• 단일 가입(Single Join)

새로운 참가자의 키 관리자는 이 참가자의 가입이 허가되는지를 검사하는 그룹 관리자에게 새로운 참가자의 요청을 전송한다. 허가된다면, 그룹 관리자

는 그에게 유일한 ID를 할당한다. 그리고 새로운 참가자에게 전송될 KEK의 시리즈를 선택한다. KEK의 선택은 각각의 키 관리 스킴에 따라 선택된다.

그룹 관리자는 단방향 함수(암호화적으로 안전한 해쉬)를 통해 키잉 재료를 통과시킴으로서 참가자에게 전송되어지는 모든 키(TEK와 KEK)의 개정을 증가시킨 후, 새로운 참가자에게 키를 전송한다. 이것은 또한 새로운 TEK를 사용하도록 송신자에게 통지한다. 다른 참가자는 일상적인 데이터 패킷을 통해 개정 변경을 통지할 것이다. 그리고 단방향 함수를 통해 그들의 TEK를 또한 통과시킨다. 함수는 역 방향이 가능하지 않기 때문에, 새로운 참가자는 이전에 사용된 키를 알 수가 없다.

• 단일 탈퇴(Single Leave)

그룹을 탈퇴하는 방법에는 3가지가 있다

① 조용한 탈퇴: 어느 참가자에게도 통지하지 않고 수신자가 그룹에 참가하는 것을 정지한다. 별도의 필요한 동작은 없다.

② 자발적인 탈퇴: 수신자가 정책에 따라 탈퇴를 알린다. 이것의 키잉 재료는 아래에 설명된 것처럼, 탈퇴 메시지를 통해 쓸 수 없게 할 수 있다. 탈퇴 메시지는 다른 탈퇴가 수행될 때까지 또는 동작하는 작업이 없을 때까지 지연될 것이다. 탈퇴 메시지가 지연된다면, 탈퇴하고자 하는 수신자는 수신을 계속하도록 허가된다.

③ 강제 탈퇴: 만약 입회 제어가 참가자를 강제적으로 차단할 필요가 있다면, 탈퇴 메시지가 전송된다. 또한, 참가자는 멤버를 차단하도록 입회 제어를 물을 것이다. 이러한 요청을 다루는 방법인 입회 정책이 존재한다. 멤버를 차단하기 위해서, 알려진 모든 키는 완전히 새로운 키잉 재료로 대체되어야 한다. 모든 잔류하는 참가자에게 이 변경을 인식하게 하기 위해, 키의 버전 번호는 증가한다.

그룹 관리자는 모든 잔류하는 참가자의 키 관리자들에 의해 복호화될 수 있는 새로운 키잉 재료를 가진 메시지를 전송한다. 그러나 탈퇴한 멤버에게는 전송하지 않는다. 추가로, 다른 새로운 참가자가 사용할 수 있도록, 탈퇴하는 참가자에 의해서 이전에 사용된 슬롯을 자유롭게 한다. 모든 참가자가 이전의 키잉 재료를 버리면, 지나간 트래픽에 대한 완전한 전송 비밀성은 보증된다.

• 다중 가입, 다중 탈퇴, 그룹 합병, 그룹 분리 (Multiple Join, Multiple Leave, Group Merge, Group Split)

이들 기능은 매우 복잡하기 때문에 선택되는 스킴에 따라 수행된다. 그리고 수행의 상세한 기술은 해당 스킴에서 설명된다.

• 그룹 해제(Group Destruction)

그룹 관리자는 모든 잔류하는 참가자에게 해제를 통지하고, 모든 네트워크 연결을 종료하고, 모든 키잉 재료를 폐기하여 모든 메모리를 자유롭게 한다. 그래서 모든 당사자가 그들의 키잉 재료를 버리면, 제 3의 사용자에 대해서 완전한 전송 비밀성은 보증된다.

Ⅵ. 결 론

음성 및 영상회의, 중복된 데이터베이스 검색 및 수정, 소프트웨어 수정본의 배포, 음성 및 영상 배포, CSCW(Computer Supported Co-operative Work), 주기적인 정보(주식, 스포츠 경기 기록, 잡지, 신문) 배포, 분산 대화형 모의실험 등 여러 분야에서 사용되는 중요한 통신 메커니즘으로 자리잡고 있는 멀티캐스트는 부당한 공격자에 의해 서비스 부인 공격을 수행하기가 쉽다. 이것은 그룹의 수신자에게만 영향을 미치는 것이 아니라 잠재적으로 대부분의 네트워크에 연결된 사용자에게 영향을

미친다. 특히 멀티캐스트는 유니캐스트와 비교해서 통신 링크의 수가 상당히 많으므로 트래픽 가로채기에 대해서 상당히 많은 기회를 제공하고 있고 노드의 가입과 탈퇴과정 중에 신분위장, 재전송, 부인공격에 노출되어 있다. 그렇지만 아직까지 이러한 부당한 공격 위협에 대한 보안대책은 미비한 실정이다.

따라서 본 논문에서는 멀티캐스트 트래픽 전송을 안전하게 하도록 하는 보안 메커니즘 설계를 위한 기반 기술로서 멀티캐스트에서 보안의 필요성과 멀티캐스트에서 고려해야할 보안 서비스를 5부분으로 나누어 분석하였고 단일 송신자와 다중 수신자, 다중 그룹에서 구성될 수 있는 보안 구조 및 보안 구성 요소 그리고 멀티캐스트 그룹에서의 기본 동작을 연구하였다. 향후 연구과제로, 실제 통신망에서의 보안 구조 적용과 각 참가자에 대한 최적의 암호키 분배 프로토콜 연구, 그리고 중계 라우터에서의 키 관리에 대한 연구가 필요하다.

※ 참고문헌

[1] T. Ballardie, J. Crowcroft, "Multicast-specific security threats and counter-measure" Proceedings of the Symposium on Network and Distributed System Security, San Diego, California, February 1995.

[2] Thomas A. Maufer "Deploying IP Multicast in the Enterprise," Prentice Hall, 1997

[3] suvo mittra. "A Framework for Scalable Secure Multicasting" In proceedings of ACM SIGCOMM'97, pp 277-288, Sept 1997.

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

[5] L. Gong, N. Shacham, "Multicast Security and its extension to a mobile environment," ACM-Baltzer Journalof Wireless Networks, October 1994.

[6] Christian Huitema, "Routing in the Internet," Prentice Hall, 1995

[7] L. Gong, N. Shacham, "Elements of Trusted Multicasting," Technical Report SRI-CSL-94-03, Computer Science Laboratory, SRI International, Menlo Park, California, March 1994.

[8] A. Ballardie, "Scalable Multicast Key Distribution," Request for Comments 1949, Internet Activities Board, April 1992.

[9] C. Semeria T. Maufer, "Introduction to IP Multicast Routing," <draft-ietf-mboned -intro-multicast-00.txt>, January 1997

[10] 강신규, 심영철, "대형 네트워크에서의 멀티캐스트 라우팅 알고리즘의 비교," 한국정보처리학회 추계학술발표논문집, 제5권, 제2호, pp.1120-1123, 1998

[11] 심영철, "Secure Multicasting in Internet," 차세대정보통신기술(ICAT'98), pp173-180, 1998

김 봉 한

1994년 청주대학교 전자계산학과(학사)
1996년 한남대학교 대학원 전자계산공학과(석사)
2000년 한남대학교 대학원 컴퓨터공학과(박사)
현재 한남대학교 강사
관심분야 : 컴퓨터네트워크, 멀티캐스트, 정보보호

이 희 규

1998년 우송대학교 컴퓨터과학과(학사)
2000년 한남대학교 대학원 컴퓨터공학과(석사)
현재 한남대학교 대학원 컴퓨터공학과 박사과정
관심분야 : 컴퓨터네트워크, 자바 보안, 전자상거래 보안

조 한 진

1997년 한남대학교 컴퓨터공학과(학사)
1999년 한남대학교 대학원 컴퓨터공학과(석사)
현재 한남대학교 대학원 컴퓨터공학과 박사과정
관심분야 : 컴퓨터네트워크, 자바 보안, 전자상거래 보안

이 재 광

1984년 광운대학교 전자계산학과(학사)
1986년 광운대학교 대학원 전자계산학과(석사)
1993년 광운대학교 대학원 전자계산학과(박사)
1986년~1993년 군산전문대학 전자계산학과 부교수
1997년~1998년 University of Alabama 객원교수
1993년~현재 한남대학교 컴퓨터공학과 부교수
관심분야 : 컴퓨터 네트워크, 정보통신 정보보호