CBT(Core Based Tree)를 기반으로 한 멀티캐스트 키 분배 프로토콜 설계

김 봉 한† · 이 재 광††

요 약

특정 사용자 그룹에게만 음성과 영상 데이터를 전송할 수 있는 통신 메커니즘을 가진 멀티캐스트는 유니캐스트와 비교해서 통신 링크의 수가 상당히 많으므로 부당한 공격자로부터 신분 위장 서비스 부인 공격과 재전송 공격, 부인, 트래픽 관찰 공격을 받기가 쉽다 멀티캐스트-특정 정보보호 위협은 해당 사용자에게만 영향을 미치는 것이 아니라 잠재적으로 대부분의 네트워크에 연결된 사용자에게 영향을 미친다. 그러므로 본 논문에서는 차세대 멀티캐스트 라우팅으로 주목받고 있는 코어 기반 트리(CBT)를 모델로 하여 인증 서버 역할을 하는 코어를 이용한 초기 인증 절차와 효율적 리우티에서 TEK(트래픽 암호화 키)를 KEK(키 암호화 키)로 전환하는 복호키 전환 시스템을 제안함으로서 탈퇴와 재 가입 시 빈번한 그룹 키의 분배 없이 사용자 정보의 비밀성과 인증을 제공할 수 있는 멀티캐스트용 키 분배 프로토콜을 설계하였다.

The Design of Multicast Key Distribution Protocol based CBT(Core Based Tree)

Bong-Han Kim† · Jae-Kwang Lee††

ABSTRACT

Multicast has communication mechanism that is able to transfer voice, video for only the specific user group. As compared to unicast, multicast is more susceptive to attack such as masquerading, malicious replay, denial of service, repudiation and traffic observation, because of the multicast has much more communication links than unicast communication. Multicast-specific security threats can affect not only a group's receivers, but a potentially large proportion of the internet. In this paper, we proposed the multicast security model that is able to secure multi-group communication in CBT (Core Based Tree), which is multicast routing. And designed the multicast key distribution protocol that can offer authentication, user privacy using core (be does as Authentication Server) in the proposed model

1. 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 전송 기술인 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 [1, 8].

그러나, 우리가 사용하고 있는 인터넷은 모든 정보

† 준 회 원 한남대학교 강사
†† 종신회원 한남대학교 컴퓨터공학과 교수
논문접수 1999년 10월 15일, 심사완료 2000년 3월 21일

가 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 효과적인 그룹 접근 제어의 결여와 멀티캐스트 트래픽이 단일 유니캐스트 통신보다, 좀 더 많은 통신 링크로 연결되기 때문에 유니캐스트 통신이나 브로드캐스트 통신의 위협과 비교하여, 일반적인 정보보호 위협은 물론이고 멀티캐스트-특정 정보보호 위험에 대한 위험이 증가하고 있다[7, 12].

그러므로, 현재 국외에서는 이러한 정보보호 위협을 해결하기 위해서, 멀티캐스트 그룹 접근 제어를 통한 그룹의 감염 가능성을 감소시키는 방법과 비 인가된 멀티캐스트 트래픽을 검색하는 방법, 진송중인 멀티캐스트 트래픽에서 사용되는 제어를 이용하여 광대역 통신망의 붕괴를 막는 방법에 대한 연구와, 여러 가지 멀티캐스트 라우팅 프로토콜에서 정보보호 모델을 설계하고 브로드캐스트에서 적용되었던 암호화 키 분배 방식을 멀티캐스트에 적용하는 방안에 대한 연구가 진행되고 있다. 그러나 국내에서는 보다 효율적인 멀티캐스트 라우팅 프로토콜에 대한 연구만 진행되고 있고 멀티캐스트 정보보호 모델이나 안전한 키 분배 프로토콜에 대한 연구는 전무한 실정이다[2-4, 9-11].

따라서 본 논문에서는 멀티캐스트에서 발생할 수 있는 특정한 공격 위협의 형태와 여러 가지 멀티캐스트 라우팅 중에서 확장성이 가장 우수한 코어 기반 트리(CBT)를 이용하여 안전한 다중 그룹 통신을 가능하게 할 수 있는 멀티캐스트 키 분배 프로토콜을 제안하였다. 본 논문의 구성은 2장에서는 멀티캐스트에서 더욱 심각한 멀티캐스트 특정 공격 형태를 분석하였다. 3장에서는 차세대 멀티캐스트 라우팅인 CBT(코어 기반 트리)의 가입 절차를 고찰하고 멀티캐스트용 정보보호 모델을 제시하였다. 4장에서는 제안된 정보보호 모델을 기반으로 하는 멀티캐스트용 키 분배 프로토콜을 설계하였다 그리고 5장에서 결론을 맺었다.

2. 멀티캐스트 특정 공격 형태

정보보호 공격은 적극적(능동적) 또는 소극적(수동적)으로 분류된다. 전송되는 정보를 알아내려고 하는 공격은 소극적이고 메시지를 수정 또는 송수신 부인은 적극적인 공격이다. 특히, 다음 공격 형태는 일반적인 브로드캐스트나 유니캐스트 통신보다는 멀티캐스트 통신에서 더욱 심각한 위험을 가지고 있다[7, 12].

2.1 적극적 공격 형태

● 서비스의 부인(Denial of Service)

어떤 멀티캐스트 응용은 대역폭 같은 네트워크 자원을 요구한다. 멀티캐스트 데이터의 어떤 비 인가된 송신이 서비스의 부인 공격을 구성할 수 있는지에 대해 고려해야 한다. 공격은 모든 인터넷 통신에 심각한 위협을 취하지만 그룹에 데이터를 제한 없이 멀티캐스트하기 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 새 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 당사자 간의 정보의 가로채기와 관련이 있다. 그래서 트래픽 형태, 내용, 빈도, 주파수, 존재/부재, 통신량과 같은 정보 누출이 발생된다.

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

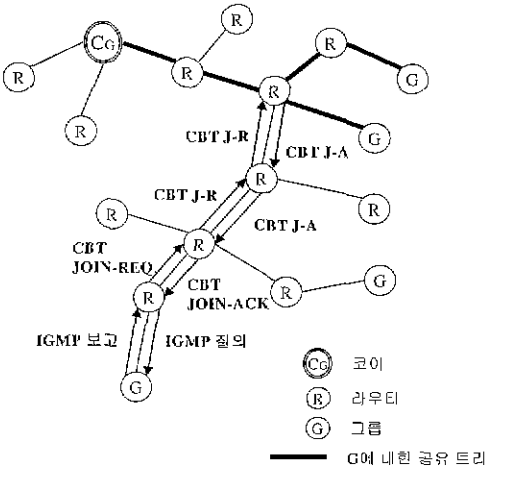
3. 멀티캐스트 정보보호 모델

3.1 CBT(코어 기반 트리)에서의 그룹 가입

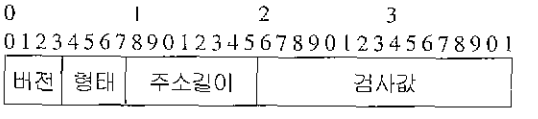
현재 연구되고 있는 여러 가지 멀티캐스트 라우팅 프로토콜 중에서 차세대 멀티캐스트 라우팅 프로토콜로 연구되고 있는 코어 기반 트리(CBT)는 공유 배달 트리에 기반을 둔 멀티캐스트 구조이다.

일반적으로, 멀티캐스트 그룹에 가입하도록 원하는 호스트는 IGMP 호스트 멤버쉽 보고를 발행한다 이 메시지는 멀티캐스트 그룹으로 전송되는 트래픽을 수신하는 로컬 CBT 라우터에게 알린다. 새로운 그룹에 대한 IGMP 호스트 멤버쉽 보고의 수신에서, 로컬 CBT 라우터는 (그림 1)처럼 그룹의 코어쪽으로 JOIN-REQUEST을 hop-by-hop 형태로 전송한다. (그림 2)은 CBT 공통 제어 패킷 헤더 형식이고 (그림 3)는 JOIN-REQUEST 패킷의 형식이다[5, 6].

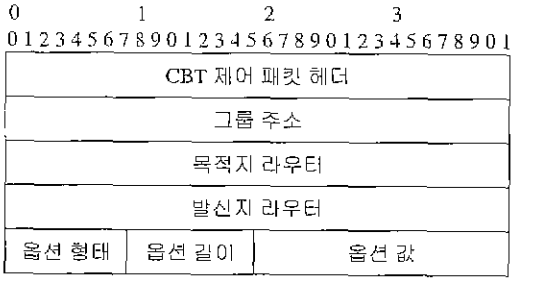
JOIN-REQUEST가 코어 라우터에 도착하기 전에, JOIN-REQUEST가 이미 그룹의 공유 트리에 있는 라우터를 만난다면, 라우터는 송신 라우터 쪽으로 JOIN-ACK를 hop-by-hop 형태로 전송한다. JOIN-REQUEST가 코어쪽으로 이 경로를 따라서 전송 중에, 공유 트리에 있는 CBT 라우터를 만나지 않는다면 코어 라우터가 JOIN-ACK를 응답한다.



(그림 1) CBT 공통 제어 패킷 헤더 형식



(그림 2) CBT 공통 제어 패킷 헤더 형식



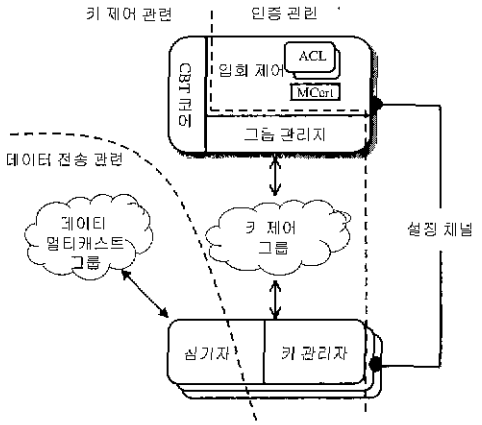
(그림 3) JOIN-REQUEST 패킷 형식

JOIN-ACK가 (그림 1)처럼, 근원지 CBT 라우터 쪽으로 반환될 때, 각 중계 라우터는 이 그룹에 대한 새로운 활성 상태(active state)를 생성한다. 새로운 가지는 인터페이스가 하위 스트림(코어부터 멀어진)인 것을 기억하는 중계 라우터를 가짐으로서 확립된다.

3.2 CBT에 적용한 정보보호 모델

(그림 4)는 제안된 키 분배 프로토콜을 위한 송신자와 수신자가 확실하게 구별되지 않는 다중 그룹 통신에서의 멀티캐스트 정보보호 모델이다. 제안된 정보보

호 구조의 구성요소는 3개의 그룹으로 구성된다. 하나는 그룹 통신에 참가하고자하는 각 참가자가 코어로부터 인증을 받는 인증 관련 부분이고 두 번째는 참가자가 데이터 전송을 위해 코어 기반 트리에 가입하는데 관련되는 키 제어 관련 부분, 그리고 세 번째는 안전한 멀티캐스트 데이터를 전송하는데 관련된 데이터 전송 관련 부분으로 나누어진다[7, 11].



(그림 4) 다중 그룹 통신 환경에서의 멀티캐스트 정보 보호 모델

● 참가자(Participant)

멀티캐스트 통신을 하는 주체로서, 로컬 키 관리자가 생성한 트래픽 암호화 키(TEK : Traffic Encryption Key)와 그룹 관리자로부터 주어진 키 암호화 키(KEK : Key Encryption Key)를 이용하여 전송하고자하는 패킷을 암호화하여 데이터 멀티캐스트 그룹으로 데이터를 전송하고 전송되어온 메시지를 로컬 키 관리자로부터 주어진 키를 이용하여 복호화 한다.

● 데이터 멀티캐스트 그룹(Data Multicast Group)

멀티캐스트, 브로드캐스트, 또는 유니캐스트 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)

그룹 통신에 가입하기를 원하는 참가자에 대해 접근 제어 목록(ACL : Access Control List)을 통해서 허용과 거부를 검증하는 기능을 수행한다.

● 키 관리자(Key Manager)

수신자에게 TEK를 전달하는 그룹 관리자로부터 재키잉 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 부트스트랩하도록 요구된다.

● 키 제어 그룹(Key Control Group)

멀티캐스트, 브로드캐스트 또는 유니캐스트 채널은 그룹 관리자로부터 의도된 수신자에게 패킷을 전달한다. 트래픽은 참가자의 키 관리자에게 분배되는 새로운 키잉 재료로 구성된다. 이 채널을 통한 전송은 모든 참가자들에게 수신되어지야 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.

● ACL(Access Control List)

그룹 접근 제어 목록으로서, 해당 그룹에 대한 입회 제어가 가능하도록 하는 기능을 수행하며, 그룹 초기자에 의해 생성되고 입회제어에서 관리한다

● MCert(Multicast Certificate)

멀티캐스트 인증서는 코어의 입회제어에 의해 생성되어 가입을 요구하는 다른 AS(Core)에게 전달된다. 멀티캐스트 인증서의 구성요소는 다음과 같다.

- 버전 번호(Version Number)
- 일련 번호(Serial Number)
- 발행자(AS) 이름(Issuer(AS) Name)
- 유효 기간(Validity Period)
- 멀티캐스트 그룹 식별자(Multicast Group Identifier)
- 멀티캐스트 그룹 초기자 구별 이름(Multicast Group Initiator Distinguished Name)
- 그룹 허용/거부 목록(Group Inclusion/Exclusion

List)
- 송신자 목록(Sender List)
- 전자 서명(Digital Signature)

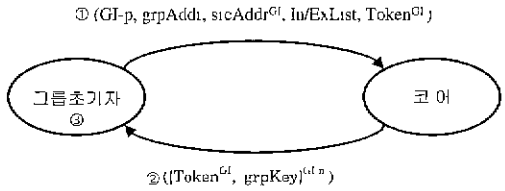
4. 멀티캐스트 키 분배 프로토콜 설계

본 논문에서 제안된 멀티캐스트 키 분배 프로토콜은 사용자 정보의 비밀성과 안전성 그리고 인증을 위하여 다음과 같이 각 참가자를 인증하는 코어에서의 인증 절차, 각 참가자가 CBT 공유 트리에 가입하기 위한 가입 절차 그리고 각 참가자가 안전하게 데이터를 전송하기 위한 데이터 전송 절차로 구분하여 키 분배 프로토콜을 설계하였다.

4.1 인증 절차에서의 키 분배 프로토콜

4.1.1 그룹 초기자의 인증 절차

① 그룹 초기자(GI)는 (그림 5)와 같은 인증 절차를 수행한다. 먼저 자신의 공개키와 비밀키 쌍을 생성한다 그리고 코어에게 그룹 개설을 위해 자신의 공개키, 그룹 주소, 발신지 주소, 허용/거부 목록과 랜덤 넘버, 타임 스탬프로 구성된 토큰을 포함한 그룹 개설 요청(Group-Open-Request)을 설정 채널을 통해서 유니캐스트한다.



GI-p 그룹초기자의 공개키 — grpAddr 그룹 주소,
srcAddr^GI 그룹 초기자의 발신지 주소 — In/ExList, 허용/거부 목록
Token^GI 그룹 초기자의 토큰 — grpKey 그룹키

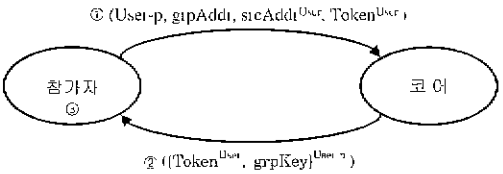
(그림 5) 그룹 초기자 인증 절차

② 코어는 입회제어를 통해서 해당 그룹의 개설을 검증한다. 입회 제어의 ACL에 해당 그룹의 허용/거부 목록을 등록하고 멀티캐스트 인증서, 그룹 키를 생성한다. 그리고 그룹 초기자의 토큰, 그룹 키를 그룹 초기자의 공개키로 암호화한 후 그룹 개설 승인(Group-Open-Ack)에 포함하여 그룹 초기자에게 전송한다. 만약 그룹이 이미 존재하면 그룹 개설 거부(Group-Open-Reject)를 통지한다

③ 그룹 초기자는 자신의 비밀키(GI-s)를 이용해 전송된 메시지를 복호화한 후 토큰에 포함된 랜덤 번호와 타임스탬프를 검증한다. 검증이 완료되면 그룹 키를 획득한다

4.1.2 참가자의 인증 절차

① 참가자는 (그림 6)과 같은 인증 절차를 수행한다 이 절차는 그룹 초기자의 인증 절차와 동일하다.



User-p 참가자의 공개키 — grpAddr 그룹 주소
srcAddr^User 참가자의 발신지 주소 — Token^User 참가자의 토큰
grpKey 그룹키

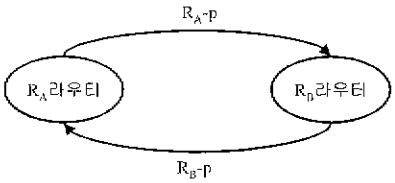
(그림 6) 참가자의 인증 절차

② 코어는 입회 제어의 ACL에 의해 해당 그룹 주소를 검색하고 허용/거부 목록을 이용해 가입 여부를 결정한다 그리고 그룹 키, 랜덤 넘버, 타임 스탬프를 참가자의 공개키로 암호화한 후 참가자 승인(Participant-Ack)에 포함하여 참가자에게 전송한다. 만약 그룹이 존재하지 않거나 거부 목록에 포함되면 참가자 거부(Participant-Reject)를 통지한다

③ 그룹 초기자와 동일한 복호화 절차를 수행한다.

4.1.3 중계 라우터의 키 분배 절차

각 CBT 중계 라우터들은 (그림 7)과 같이, 자신의 공개키와 비밀키를 생성하여 인접한 다른 중계 라우터에게 자신들의 공개키를 상호 교환한다.



(그림 7) 중계 라우터의 키 분배 절차

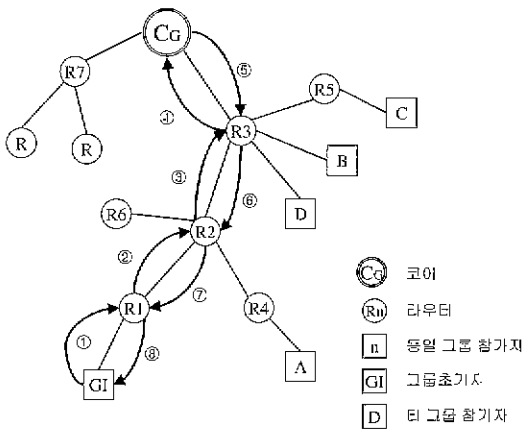
4.2 가입(Join)절차에서의 그룹 접근 제어 프로토콜

4.2.1 그룹 초기자의 가입 절차

① 그룹 초기자는 (그림 8)과 같은 키 분배 프로토콜을 수행한다. 우선 자신의 새로운 토큰을 생성한다 생성된 토큰과 그룹 주소를 그룹키로 암호화한다. 암호화된 토큰을 R1의 공개키로 암호화한 후 IGMP 그룹 멤버쉽 보고(Group-Membership-Report) 메시지에 포함시켜 R1(DR)로 전송한다.

프로토콜 1 그룹 초기자를 위한 키 분배 프로토콜

1 GI→R1 Group-Membership-Report({ {Token^{GI}, grpAddr}^{grpKey} }$^{R1\ p}$)
2 R1→R2 CBT-Join-Request({Token^{R1}, {Token^{GI}, grpAddr}^{grpKey}}$^{R2\ p}$)
3 R2→R3 CBT-Join-Request({Token^{R2}, {Token^{GI}, grpAddr}^{grpKey}}$^{R3\ p}$)
4 R3→Core CBT-Join-Request({Token^{R3}, {Token^{GI}, grpAddr}^{grpKey}}$^{Core\ p}$)
5 Core→R3 CBT-Join-Ack({Token^{R3}, Token^{GI}, grpKey, KEK}$^{R3\ p}$)
6 R3→R2 CBT-Join-Ack({Token^{R2}, Token^{GI}, grpKey, KEK}$^{R2\ p}$)
7 R2→R1 CBT-Join-Ack({Token^{R1}, Token^{GI}, grpKey, KEK}$^{R1\ p}$)
8 R1→GI Group-Membership-Query({Token^{GI}, grpKey, KEK}$^{GI\ p}$)



(그림 8) 가입 절차에서 그룹 초기자 키 분배 프로토콜

② R1은 수신된 메시지를 자신의 비밀키로 복호화한다. 그리고 자신의 토큰을 생성한 후 그룹 초기자로부터 전송된 데이터에 자신의 토큰을 추가한다. 추가된 데이터는 R2의 공개키로 암호화하여 CBT Join-Request 메시지에 포함하여 전송한다

③ R2는 수신된 메시지를 자신의 비밀키로 복호화하고 R1의 토큰을 저장한다. 그리고 자신의 토큰을 생성한 후, R1로부터 온 데이터중 R1의 토큰을 제외한 나머지 데이터와 함께 R3의 공개키로 암호화한다. 암호화된 데이터를 CBT Join-Request 메시지에 포함하여 전송한다.

④ R3는 수신된 메시지를 자신의 비밀키로 복호화하고 R2의 토큰을 저장한다 그리고 자신의 토큰을 생성한 후, R2로부터 온 데이터중 R2의 토큰을 제외한 나머지 데이터와 함께 코어의 공개키로 암호화한다. 암호화된 데이터를 CBT Join-Request 메시지에 포함하여 전송한다.

⑤ 코어는 수신된 메시지를 자신의 비밀키로 복호화하여 Token^{R3}, {Token^{GI},}^{grpKey} 를 획득한다. 또한 그룹키를 이용하여 {Token^{GI},}^{grpKey}를 복호화한다. 복호화 절차가 완료되면 코어는 KEK를 생성한다. 생성된 KEK와 그룹키, 그룹 초기자가 포함시킨 그룹초기자의 토큰, R3의 토큰을 R3의 공개키로 암호화한 후 CBT Join Ack에 포함시켜 R3에 전송한다.

⑥ R3는 자신의 비밀키를 이용해 전송된 메시지를 복호화한 후, 자신이 전송한 토큰임을 검증한다. 검증이 완료되면 grpKey, KEK를 복사하여 복호용 키 저장소에 저장한다. 저장된 Token^{R2}를 코어로부터 온 메시지에 추가하여 R2의 공개키로 암호화한 후 R2에게 전송한다

⑦ R2는 자신의 비밀키를 이용해 전송된 메시지를 복호화한 후, 자신이 전송한 토큰임을 검증한다. 검증이 완료되면 grpKey, KEK를 복사하여 복호용 키 저장소에 저장한다. 저장된 Token^{R1}을 R3로부터 온 메시지에 추가하여 R1의 공개키로 암호화한 후 R1에게 전송한다.

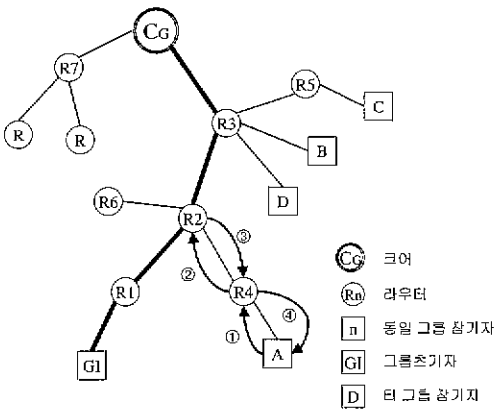
⑧ R1은 자신의 비밀키를 이용해 전송된 메시지를 복호화한 후, 자신이 전송한 토큰임을 검증한다 검증이 완료되면 grpKey, KEK를 복사하여 복호용 키 저장소에 저장한다. R2로부터 온 메시지를 그룹 초기자의 공개키로 암호화한 후 그룹 멤버쉽 질의에 포함하여 그룹 초기자에게 전송한다. 그룹 초기자는 자신의 비밀키를 이용해 전송된 메시지를 복호화한 후, Token^{GI}, grpKey, KEK 중에서 Token^{GI}이 자신이 전송한 토큰임을 검증한다. 검증이 완료되면 그룹키(grpKey)는 차후 가입을 위해 보관하고 KEK를 획득한다.

4.2.2 참가자의 가입 절차(A, B, C 동일)

참가자들은 (그림 9)와 같은 키 분배 프로토콜을 수행한다.

프로토콜 2 참가자 A를 위한 키 분배 프로토콜

1. A → R4 Group-Membership-Report({ {Token^{A}, grpAddr}^{grpKey} }$^{R4-pub}$)
2. R4 → R2 CBT-Join-Request({Token^{R4}, {Token^{A}, grpAddr}^{grpKey}}$^{R2-pub}$)
3. R2 → R4 CBT-Join-Ack({Token^{R1}, Token^{A}, grpKey, KEK}$^{R4-pub}$)
4. R4 → A Group-Membership-Query({Token^{A}, grpKey, KEK}$^{User-pub}$)



(그림 9) 가입 절차에서 참가자 키 분배 프로토콜

① 참가자 A는 자신의 새로운 토큰을 생성한다. 생성된 토큰과 그룹 주소를 그룹키로 암호화한다. 암호화된 토큰을 R4의 공개키로 암호화한 후 IGMP 그룹 멤버쉽 보고(Group-Membership-Report) 메시지에 포함시켜 R4로 전송한다

② R4는 수신된 메시지를 자신의 비밀키로 복호화한다 그리고 자신의 토큰을 생성한 후 참가자 A로부터 전송된 데이터에 자신의 토큰을 추가한다. 추가된 데이터는 R2의 공개키로 암호화하여 CBT Join Request 메시지에 포함하여 전송한다.

③ R2는 수신된 메시지를 자신의 비밀키로 복호화한다. 그리고 복호용 키 저장소에 저장된 그룹키를 이용해 다시 한번 복호화를 한 후, R4의 토큰, 그룹키, KEK를 R4의 공개키로 암호화하여 R4로 전송한다.

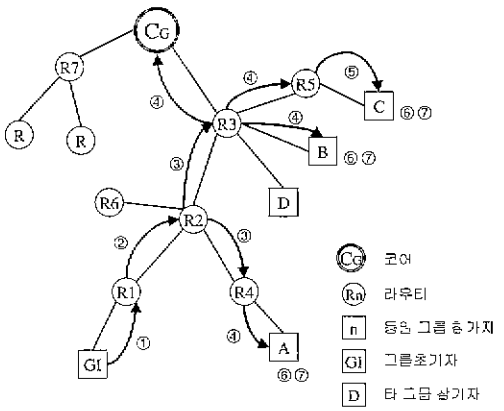
④ R4는 자신의 비밀키를 이용해 전송된 메시지를 복호화한 후, 자신이 전송한 토큰임을 검증한다. 검증이 완료되면 grpKey, KEK를 복사하여 복호용 키 저장소에 저장한다 R2로부터 온 메시지를 참가자 A의 공개키로 암호화한 후 참가자 A에게 전송한다. 참가자 A는 자신의 비밀키를 이용해 전송된 메시지를 복호화한 후, 자신이 전송한 토큰임을 검증한다. 검증이 완료되면 그룹키는 차후 가입을 위해 저장하고 KEK를 획득한다.

4.3 데이터 전송 절차에서의 키 분배 프로토콜

그룹 초기자를 포함한 모든 참가자는 (그림 10)과 같은 방법으로 데이터를 암호화하여 전송한다.

프로토콜 3. 데이터 전송을 위한 키 분배 프로토콜

1 GI -> R1 ({M}^{TEK}, {TEK}^{KEK})
2 R1 -> R2 ({M}^{TEK}, {TEK}^{KEK})
3 R2 -> R4 R2 -> R3 ({M}^{TEK}, {TEK}^{KEK})
4 R4 -> A, R3 -> R5, R3 -> B, R3 -> Core ({M}^{TEK}, {TEK}^{KEK})
5 R5 -> C ({M}^{TEK} {TEK}^{KEK})

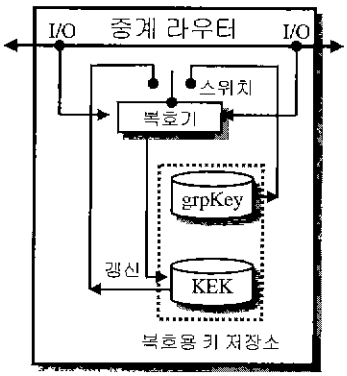


(그림 10) 데이터 전송 절차에서 키 분배 프로토콜

① 그룹 초기자를 송신지로 가정한다. 송신자는 데이터 암호화 키(TEK)를 생성하여, 전송하고자 하는 데이터(M)를 TEK로 암호화한다 그리고 암호화된 메시지와 TEK를 키 암호화 키(KEK)로 다시 암호화하여 R1으로 전송한다.

② R1은 (그림 11)과 같이 수신된 메시지를 복사하여 원본은 R2에게 전송하고 사본은 KEK로 복호화한 후 TEK를 새로운 KEK로 전환하여 복호용 키 저장소에 저장한다 암호화된 메시지 부분은 제거한다

③ R2는 수신된 메시지를 복사하여 원본은 R3에게 전송하고 사본은 KEK로 복호화한 후 TEK를 새



(그림 11) 중계 라우터의 복호키 전환 시스템

로운 KEK로 전환하여 복호용 키 저장소에 저장한다. 암호화된 메시지는 제거한다.

④ R4는 수신된 메시지를 복사하여 원본은 참가자 A에게 전송하고 사본은 KEK로 복호화한 후 TEK를 새로운 KEK로 전환하여 복호용 키 저장소에 저장한다. R3도 수신된 메시지를 복사하여 원본은 R5, 참가자 B, 코어에게 전송하고 사본은 KEK로 복호화한 후 TEK를 새로운 KEK로 전환하여 복호용 키 저장소에 저장한다. 암호화된 메시지는 제거한다.

⑤ R5는 수신된 메시지를 복사하여 원본은 참가자 C에게 전송하고 사본은 KEK로 복호화한 후 TEK를 새로운 KEK로 전환하여 복호용 키 저장소에 저장한다. 암호화된 메시지는 제거한다.

⑥ 참가자 A, B, C는 자신이 알고 있는 KEK를 이용해 $\{M\}^{TEK}$, $\{TEK\}^{KEK}$ 를 복호화하여 TEK를 획득하고, TEK를 이용하여 $\{M\}^{TEK}$를 복호화한 후 M(메시지)를 확인할 수 있다.

⑦ 각 참가자 A, B, C는 수신된 TEK를 KEK로 전환하고 새로운 TEK를 생성하여 송신자와 동일한 방법으로 메시지를 $\{Mnew\}^{TEKnew}$, $\{TEKnew\}^{TEKold}$ 처럼 암호화하여 전송한다.

4.4 기존 방식과의 비교

본 절에서는 제안된 방식, 기존에 발표된 RFC 1949 방식, Caronni의 중앙집중 트리방식을 <표 1>과 같이 비교하였다. 주요 비교 항목은 참가자 탈퇴와 재가입 시의 보안성, 키잉 발생 여부와 중계 라우터에서 보관해야하는 암호화에 관련된 키 양의 증가 여부이다. 제안된 방식은 공개키 1쌍과 비밀키 3개를, 인증 절차에서 공개키 방식을 이용하여 명확히 참가자를 인증함으로서 그룹키를 획득하고, 가입절차에서 그룹키를 이용하여 TEK를 암호화 할 수 있는 KEK를 획득하고, 멀티캐스트 데이터 전송 절차에서 데이터를 암호화 할 수 있는 TEK를 KEK를 통해서 획득할 수 있다. 모든 암호화 절차에서 공개키를 이용하여 좀 더 명확히 암호화를 시도 할 수 있지만 복잡한 키 분배와 방대한 양의 키 데이터베이스를 구축하여야 하기 때문에 초기 인증 절차에서만 공개키 방식을 사용하였다.

또한 TEK를 새로운 KEK로 전환하는 복호키 전환 시스템을 설계하여 탈퇴한 참가자로부터 기존의 멀티캐스트 데이터를 보호하기 위해서 새로운 그룹키를 분배할 필요가 없게 되었다. 그러므로 데이터 전송 중에 탈퇴지로 인한 새로운 키를 분배해야 하는 트래픽 노드를 줄일 수가 있다.

〈표 1〉 기존 방식과의 비교

항목 \ 비교대상		제안된 방식	RFC 1949 방식	caronni 방식
암호 방식	공개키	O	O	
	비밀키	O	O	O
암호키의 수		5개	5개	N-1개
참가자의 증가에 따른 키의 증가 여부		없음	없음	증가
탈퇴자에 대한 참가자의 보안성		있음 (KEK 변환)	없음	있음
새로운 참가자에 대한 이전 트래픽의 보안성		있음 (TEK 변환)	없음	있음
참가자의 재 가입시 키잉 여부		필요 없음	그룹키 재전송	암호키 재전송
참가지 수에 따른 중계 라우터에서 키의 양		변화 없음	증가	변화 없음

5. 결 론

특정 사용자 그룹에게만 음성과 영상 데이터를 전송할 수 있는 통신 메커니즘을 가진 멀티캐스트는 유니캐스트와 비교해서 통신 링크의 수가 매우 많으므로 유니캐스트에서 발생하는 정보보호 위협 뿐만 아니라 멀티캐스트 구조로 인해 발생하는 특정 정보보호 위협에도 많은 위험이 노출되어 있다 이러한 멀티캐스트-특정 위협에 의해서 부당한 공격자로부터 신분 위장, 서비스 부인 공격과 재전송 공격, 부인, 트래픽 관찰 공격을 받기가 쉽다. 멀티캐스트-특정 위협에 의한 피해는 해당 사용자에게만 영향을 미치는 것이 아니라 잠재적으로 대부분의 네트워크에 인결된 사용자에게 영향을 미친다. 따라서 본 논문에서는 현재 국내외에서 진행되고 있는 여러 가지 멀티캐스트 라우팅 중에서 차세대 멀티캐스트 라우팅으로 주목받고 있는 공유

트리를 기반으로 하는 코어 기반 트리(CBT)를 모델로 하여 안전한 다중 그룹 통신을 가능하게 할 수 있는 멀티캐스트 키 분배 프로토콜을 제안하였다.

본 정보보호 모델에서 인증 서버 역할을 하는 코어를 이용한 초기 인증 절차를 적용하고 중계 라우터의 복호키 전환 시스템을 둠으로서 기존에 제안된 키 분배 프로토콜[2, 7]보다도 좀 더 적은 수의 백터만을 분배하여 그룹 가입절차에서 참가자의 인증과 데이터 전송 중에서 참가자 정보의 비밀성을 제공할 수 있고 특히 특정 참가자가 탈퇴한 후에도 통신에 참가하고 있는 기존 참가자에게 아무런 영향을 주지 않고 탈퇴한 참가자로부터 비밀성을 유지할 수 있는 멀티캐스트용 키 분배 프로토콜을 제안하였다. 향후 연구과제로는 검증 도구를 이용하여 제안된 키 분배 프로토콜에 대한 검증과 코어 기반 트리에서의 인증 서버로서 동작하는 코어를 안전하게 보호할 수 있는 정보보호 문제에 대한 연구가 좀 더 진행되어야 한다.

참 고 문 헌

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

[2] A. Ballardic, "Scalable Multicast Key Distribution," Request for Comments 1949, Internet Activities Board, April 1996.

[3] H. Harney, C Muckenhirn, "Group Key Management Protocol(GKMP) Specification," Request for Comments 2093, Internet Activities Board, July 1997.

[4] H. Harney, C Muckenhirn, "Group Key Management Protocol(GKMP) Architecture," Request for Comments 2094, Internet Activities Board, July 1997.

[5] A Ballardie, "Core Based Tree(CBT) Mulicast Routing Architecture." Request for Comments 2201, Internet Activities Board, Sept 1997.

[6] A. Ballardie, "Core Based Tree(CBT version 2) Multicast Routing-Protocol Specification," Request for Comments 2189, Internet Activities Board, Sept 1997.

[7] 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.

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

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

[10] 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

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

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

김 봉 한

e-mail : bhkim@netwk.hannam.ac.kr

1994년 청주대학교 전자계산학과(학사)

1996년 한남대학교 대학원 전자계산공학과(공학석사)

2000년 한남대학교 대학원 컴퓨터공학과(공학박사)

현재 한남대학교 강사

관심분야 : 컴퓨터네트워크, 멀티캐스트, 정보보호

이 재 광

e-mail : jklee@netwk.hannam.ac.kr

1984년 광운대학교 전자계산학과(학사)

1986년 광운대학교 대학원 전자계산학과(이학석사)

1993년 광운대학교 대학원 전자계산학과(이학박사)

1986년~1993년 군산전문대학 전자계산학과 부교수

1997년~1998년 University of Alabama 객원교수

1993년~현재 한남대학교 컴퓨터공학과 부교수

관심분야 : 컴퓨터 네트워크, 정보통신 정보보호