通信情報保護學會論文誌
第 10 券 第 2 號, 2000. 6

그룹 통신을 위한 멀티캐스트 키 분배 프로토콜 설계 및 검증

김 봉 한*, 이 재 광**

The Design and Verification of Multicast Key Distribution Protocol for Group Communication

Bong-han Kim*, Jae-kwang Lee**

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. 그러므로 본 논문에서는 현재 멀티캐스트 통신을 위해서 제안 및 사용되고 있는 여러 가지 멀티캐스트 라우팅 프로토콜 중에서 보다 효율적인 보안 체계를 구성할 수 있는 공유 트리를 기반으로 하는 코어 기반 트리(CBT: Core Based Tree)를 이용하여 3개로 구성된 그룹키, KEK, TEK을 획득함으로서 안전한 멀티캐스트 통신이 가능한 키 분배 프로토콜을 설계하였다. 그리고 패트리넷을 이용하여 안전성을 검증하였다.

ABSTRACT

As compared to unicast, multicast with communication mechanism transmitting voice data or video data to specific user group may easily have a attack of attacker because of a number of communication links. Thus, we designed the key distribution protocol enabling secure multicast communication by getting three key(group key, KEK, TEK) with Core Based Tree(CBT) configurating more effective security system in multicast routing protocols proposed or using to take multicast communication, and verified its security with Petri net in this paper.

keyword : *multicast, security, CBT, key distribution*

Ⅰ. 서 론

정보통신 기술의 발전과 다양한 정보매체의 활용이 가능해 짐에 따라 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 영상배포, CSCW(Computer Supported Co-operative Work), 주기적인 정보(주식, 스포츠 경기 기록, 잡지, 신문) 배포, 분산 대화형 모의실험 등과 같은 서비스 및 응용을 가능하게 한다. 그러나 멀티캐스트는 유니캐스트 통신이나 브로드캐스트 통신에 비해서, 효과적인 그룹 접근 제어의 결여와

* 한남대학교 강사(bhkim@netwk.hannam.ac.kr)
** 한남대학교 컴퓨터공학과 부교수(jklee@netwk.hannam.ac.kr)

트래픽이 유니캐스트 통신보다, 좀 더 많은 통신 링크를 경유하기 때문에 신분 위장, 서비스 부인 공격, 재전송 공격, 부인, 트래픽 관찰 공격에 대한 위험이 증가하고 있으며, 링크에 대한 상당히 많은 공격 기회를 제공하고 있다. 또한 이러한 보안 위협을 해결하기 위해 제안된 키 분배 방법들도 KDC(Key Distribution Center)가 모든 가입에 대한 인증과 키 분배를 혼자 처리함으로서 확장성에 대한 심각한 문제점을 발생시키고 있다.[1,4,8]

이러한 상황에서, 현재 국외에서는 확장성에 대한 문제점을 보완하면서 이러한 보안 위협을 해결하기 위한 연구가 다각도로 진행되고 있다. Ballardie,[4] Caronni,[5] Li Gong[6]은 멀티캐스트에서 제공해야 할 다양한 보안 요소를 통해서, 어떻게 광대역 통신망의 붕괴를 막을 수 있는 지에 대한 연구를 진행하고 있으나 이들 역시 많은 키 분배 횟수를 요구함으로 트래픽의 밀집 현상이 발생하고 실제 인터넷에는 적용할 수 없다는 단점을 가지고 있다.

따라서 본 논문에서는 현재 멀티캐스트 통신을 위해서 제안 및 사용되고 있는 여러 가지 멀티캐스트 라우팅 프로토콜 중에서 보다 효율적인 보안 체계를 설계할 수 있는 공유 트리를 기반으로 하는 코어 기반 트리(CBT: Core Based Tree)를 이용하여 적은 수의 키를 분배하면서도 안전한 멀티캐스트 통신을 제공할 수 있는 키 분배 프로토콜을 제안하였다. 또한 제안된 키 분배 프로토콜의 안전성을 위해서 패트리넷을 통하여 검증하였다.

논문의 구성은 2장에서 멀티캐스트 통신에서 보안의 필요성을 기술하였다. 3장에서 제안된 키 분배 프로토콜의 기반인 코어 기반 트리 구조에 대해 분석하였고, 4장에서는 인증 절차, 가입 절차 그리고 데이터 전송 절차로 구분하여 키 분배 프로토콜을 설계하였다. 5장에서는 제안된 키 분배 프로토콜의 안전성을 검증하기 위해서 패트리넷을 이용한 검증 결과를 기술하였다. 6장에서는 연구 결과에 대한 결론과 향후 연구방향에 대하여 정리하였다.

II. 멀티캐스트 보안의 필요성

멀티캐스트 통신의 당사자는 자신과 대응되는 그룹 멤버쉽이 특정 사용자/호스트/서브넷으로(예를 들어, 오디오, 비디오 회의) 제한되도록 요구한다. 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 쉽다. 이것은 그룹의 수신자에게만 영향을 미치는 것이 아니라 잠재적으로는 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.[4,7,9]

- 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 공격자가 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 비인가된 가로채기에 대해서 상당히 많은 기회를 발생시킨다.

Ⅲ. 코어 기반 트리(Core Based Tree) 구조

본 절에서는 차세대 멀티캐스트 라우팅 프로토콜로 연구되고 있는 코어 기반 트리에 대해서 분석하였다. CBT는 공유 트리에 기반을 둔 멀티캐스트 구조이다. 이것은 인터넷을 통해서 멀티캐스트 응용이 지원될 때, 확장성을 다루기 위한 목적으로 제안되었고 사설 인트라넷 내에서 사용하기에 적당하다.

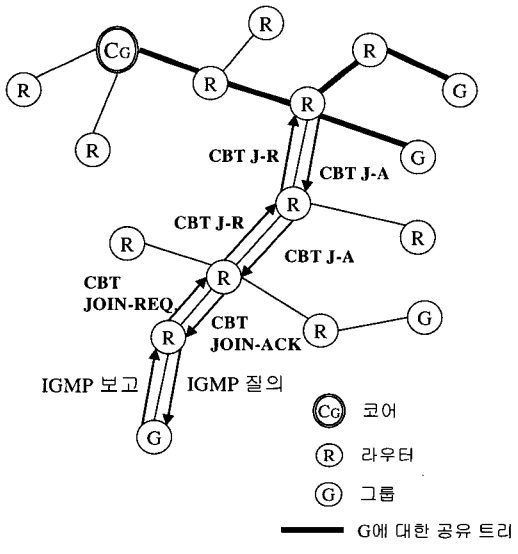
또한 CBT는 프로토콜에 대해 독립적이다. CBT는 이것의 공유 배달 트리를 구축하기 위해 유니캐스트 라우팅 테이블 내에 포함되는 정보를 사용한다. CBT는 어떻게 유니캐스트 라우팅 테이블이 배달되는지를 상관하지 않는다. 단지 유니캐스트 라우팅 테이블이 있기만 하면 된다.[2,3]

3.1 그룹의 공유 트리 가입

일반적으로, 멀티캐스트 그룹에 가입하기를 원하는 호스트는 IGMP 호스트 멤버쉽 보고를 발행한다. 이 메시지는 멀티캐스트 그룹으로 전송되는 트래픽을 수신하는 이것의 로컬 CBT 라우터에게 전송된다. 새로운 그룹에 대한 IGMP 호스트 멤버쉽 보고의 수신에서, 로컬 CBT 라우터는 그림 1처럼 그룹의 코어 쪽으로 JOIN_REQUEST을 hop-by-hop 형태로 전송한다.

만약 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. 만약 JOIN_REQUEST가 코어 쪽으로 이 경로를 따라서 전송 중에, 공유 트리에 있는 CBT 라우터를 만나지 않는다면 코어 라우터가 JOIN_ACK를 응답한다.

JOIN_ACK가 근원지 CBT 라우터 쪽으로 반환될 때, 각 중계 라우터는 이 그룹에 대한 새로운 활성 상태(active state)를 생성한다.



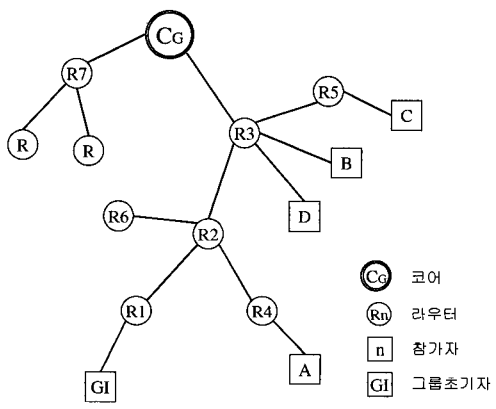
〔그림 1〕 CBT JOIN-REQUEST와 CBT JOIN-ACK

Ⅳ. 멀티캐스트 키 분배 프로토콜 설계

본 논문에서 제안된 멀티캐스트 키 분배 프로토콜은 사용자 정보의 비밀성과 안전성 그리고 인증을 위하여 다음과 같이 각 참가자를 인증하기 위한 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 설계하고자 한다.

4.1 제안된 프로토콜 설계를 위한 조건

조건은 그림 2와 같이 단일 코어에서 단일 그룹을 가진 통신망 구조를 가진 캠퍼스 LAN을 기반으로 화상회의나 화상강의가 가능한 멀티캐스트 통신 환경상에서, 단일 대학 캠퍼스에서 단일 강좌를 화상 강의하기 위한 키 분배 방식으로서 단일 강좌에 대한 강사와 학생간의 의견을 교환하는 방식이다. 조건은 단일 코어와 단일 그룹만을 가지며 각 참가자는 코어 내에 존재한다. 강사가 그룹 초기자의 역할을 수행한다.



〔그림 2〕 키 분배 프로토콜을 위한 네트워크 구성도

학생들은 참가자의 역할을 수행한다. 각 참가자는 각각 다른 라우터에 존재할 수도 있고 같은 라우터에 존재할 수도 있다. 그리고 각 참가자에 대해서 빈번한 가입과 탈퇴를 허용한다. 탈퇴한 후, 재 가입한 참가자는 탈퇴 후로부터 재 가입한 이전에 발생한 멀티캐스트 메시지를 획득할 수 없다.

4.2 인증 절차에서의 키 분배 프로토콜

본 장에서 CBT를 이용하여 키 분배 프로토콜을 설계하였다. 본 장에서 사용되는 표기법은 표 1과 같다.

4.2.1 그룹 초기자의 인증 절차

① 그룹 초기자(GI)는 프로토콜 1과 같은 인증 절차를 수행한다. 먼저 자신의 공개키와 개인키 쌍을 생성하고 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 세션 설정을 통해서 유니캐스트한다.

② 코어는 입회제어를 통해서 해당 그룹의 개설을 검증한다. 입회 제어의 ACL에 해당 그룹의 허용/거부 목록을 등록하고 멀티캐스트 인증서, 그룹키를 생성한다. 그리고 그룹 초기자의 토큰, 그룹키를 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.

〔표 1〕 표기법

기 호	의 미
n-p	해당 개체의 공개키
n-s	해당 개체의 개인키
grpAddr	그룹 주소
$srcAddr^{GI}$	그룹 초기자의 발신지 주소
$srcAddr^{User}$	참가자의 발신지 주소
$Token^{n}$	해당 개체의 토큰
In/ExList	허용/거부 목록
r^{n}	해당 토큰의 랜덤 넘버
t^{n}	해당 토큰의 타임 스탬프
grpKey	그룹 키
KEK	키 암호화 키
TEK	트래픽 암호화 키

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

프로토콜 1. 그룹 초기자에 대한 인증 절차

1. GI→Core : (GI-p, grpAddr, $srcAddr^{GI}$, In/ExList, $Token^{GI}$)
2. Core→GI : ($\{Token^{GI}, grpkey\}^{GI-P}$)

4.2.2 참가자의 인증 절차

① 참가자는 프로토콜 2와 같이, 그룹 초기자의 인증 절차와 동일한 과정을 수행한다.

② 코어는 입회 제어의 ACL에 의해 해당 그룹 주소를 검색하고 허용/거부 목록을 이용해 가입 여부를 결정하고 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.

프로토콜 2. 참가자에 대한 인증 절차

1. User→Core : (User-p, grpAddr, $srcAddr^{User}$, $Token^{User}$)
2. Core→User : ($\{Token^{User}, grpkey\}^{User-p}$)

4.2.3 각 중계 라우터의 키 분배 절차

각 CBT 중계 라우터들은 프로토콜 3과 같이, 자신의 공개키와 개인키를 생성하여 인접한 다른 중계 라우터에게 자신들의 공개키를 상호 교환한다.

프로토콜 3. 중계 라우터의 키 분배 절차

1. 라우터 A → 라우터 B : (R_A-p)
2. 라우터 B → 라우터 A : (R_B-p)

4.3 가입(Join)절차에서의 그룹 접근 제어 프로토콜

4.3.1 그룹 초기자의 가입 절차

① 그룹 초기자는 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 R1로 전송한다.

② R1은 수신된 메시지를 자신의 개인키로 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 개인키로 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 R3도 R2와 동일한 과정을 거쳐 암호화된 데이터를 CBT Join-Request 메시지에 포함하여 코어에게 전송한다.

⑤ 코어는 수신된 메시지를 자신의 개인키로 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 R3은 자신의 개인키를 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 R2도 R3와 같은 동일한 과정을 거쳐 메시지를 R1의 공개키로 암호화한 후 R1에게 전송한다.

⑧ R1은 자신의 개인키를 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 개인키를 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.

프로토콜 4. 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}$^{GI-p}$)

4.3.2 참가자의 가입 절차

참가자들의 가입 절차는 그룹 초기자의 키 분배 프로토콜과 같은 키 분배 프로토콜을 수행한다.

프로토콜 5. 참가자 A를 위한 키 분배 프로토콜

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

4.4 데이터 전송 절차에서의 키 분배 프로토콜

그룹 초기자를 포함한 모든 참가자는 다음과 같은 방법으로 데이터를 암호화하여 전송한다.

프로토콜 6. 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 : ($\{M\}^{TEK}$, $\{TEK\}^{KEK}$)
   R4 -> A, R3 -> R5, R3 -> B, R3 -> Core
   : ($\{M\}^{TEK}$, $\{TEK\}^{KEK}$)
4. R5 -> C : ($\{M\}^{TEK}$, $\{TEK\}^{KEK}$)

〔표 2〕 제안된 시스템에서 사용되는 키

키 종류	암호방식	기 능	사용되는 부분		
			인증	가입	데이터 전송
n-p	공개키	라우터와 라우터사이에서 데이터 암호용	O	O	
n-s		공개키로 암호화된 메시지 복호용	O	O	
KEK	비밀키	TEK를 획득하기 위한 키			O
TEK		메시지를 암호화하는 키			O
grpKey		KEK를 획득하기 위한 키		O	

〔표 3〕 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 증가여부		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
참가자 수에 따른 중계 라우터에서 키의 양		변화 없음	증가	변화 없음

① 그룹 초기자를 송신자로 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 수신된 메시지를 복사하여 원본은 R2에게 전송하고 사본은 KEK로 복호화한 후 TEK를 새로운 KEK로 전환하여 복호용 키 저장소에 저장한다. 암호화된 메시지 부분은 제거한다.

③ 모든 중계 라우터는 R1과 같은 키 분배 프로토콜을 수행하고 가입 절차 과정에서 상호 연결된 다른 중계 라우터에게 암호화된 메시지를 전송한다.

④ 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.

⑤ 각 참가자 A, B, C는 수신된 TEK를 KEK로 전환하고 새로운 TEK를 생성하여 송신자와 동일한 방법으로 메시지를 $\{Mnew\}^{TEKnew}$, $\{TEKnew\}^{TEKold}$ 처럼 암호화하여 전송한다.

제안된 키 분배 프로토콜에서 사용되는 키들은 표 2와 같다. 공개키 방식을 이용한 n-p, n-s 키는 인증절차와 가입절차에서 라우터와 라우터 사이의 데이터 암호용으로 사용되고, KEK, TEK, grpKey는 비밀키 방식으로 가입절차와 데이터 전송 절차에서 다른 키를 획득하기 위해서 사용된다. grpKey는 동일 그룹에 재 가입할 때 필요하므로 안전하게 보관하여야 한다. TEK는 메시지마다 다른 키로 변경됨으로 탈퇴자가 재 가입했을 때 이전에 발생된 멀티캐스트 메시지를 현재의 TEK로 복호화 할 수가 없다. 그러므로 탈퇴자로 인해서 코어가 새로운 그룹키를 발생시켜 분배할 필요가 없게 된다.

제안된 방식과 기존에 발표된 RFC 1949 방식, Caronni의 중앙집중 트리방식을 표 3에서 비교하였다. 주요 비교 항목은 참가자 탈퇴와 재가입시의 보안성, 키잉 발생 여부와 중계 라우터에서 보관해야하는 암호화에 관련된 키 양의 증가 여부이다.

V. 제안된 멀티캐스트 키 분배 프로토콜 검증

5장에서는 인증절차와 데이터 전송절차에서 제안된 키 분배 프로토콜에 대한 안전성을 패트리넷을 이용하여 검증하였다.

5.1 패트리넷을 이용한 검증 방법

5.1.1 패트리넷의 개요

① 패트리넷 구조

원으로 표시되는 플레이스의 집합, 막대로 표시되는

트랜지션의 집합, 트랜지션의 입력 함수, 트랜지션의 출력함수로 구성되며 다음과 같이 정의된다.[10]

C=(P, T, I, O)

P : 플레이스의 유한 집합, $P=\{p_1, p_2, \ldots, p_n\}$, $n \geq 0$
T : 트랜지션의 유한 집합, $T=\{t_1, t_2, \ldots, t_m\}$, $m \geq 0$
I : 트랜지션의 입력 함수, $t_j \in T \rightarrow I(t_j) \in P$
O : 트랜지션의 출력 함수, $t_j \in T \rightarrow O(t_j) \in P$
$P \cap T = \varnothing$

② 마킹(marking)
마킹 μ : P →N는 패트리넷 C 의 플레이스 집합 P에서 음수가 아닌 정수 N으로 변환하는 함수이다.
③ 마킹된 패트리넷(marked Petri net)
마킹된 패트리넷은 PN = (P, T, I, O, μ)으로 표시된다.
④ 활성(enable)
어떤 트랜지션의 입력 플레이스 모두에 토큰이 존재할 때 그 트랜지션은 활성 상태이다.
⑤ 점화(firing)
활성 상태인 트랜지션의 입력 플레이스에 있던 토큰들이 출력 플레이스로 이동한다.
⑥ 보존성(boundness) 및 안전성(safeness)
각 플레이스에 있는 토큰의 개수가 k(k: 유한 정수)이하이면 "보존적"이라고 말하고 k=1이면 "안전하다(safe)"고 한다.
⑦ 도달성(reachability)
주어진 상대(마킹)로부터 상태의 도달 가능성을 의미하며, 주어진 상태로부터 도달 가능한 상태(마킹)의 집합을 도달성 집합이라 한다. 도달성 집합을 트리 또는 그래프로 표시할 수 있는데 노드는 상태(마킹)가 되고 호선(arc)은 상태 변환을 야기한 트랜지션이 된다.
⑧ 데드락(deadlock)
더 이상 전이될 수 없는 상태(마킹)를 의미한다.

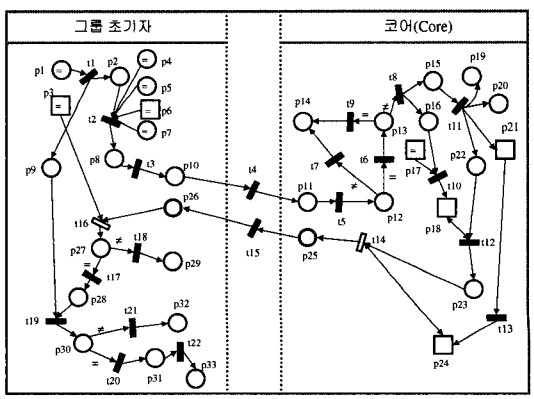
5.1.2 검증을 위한 패트리넷의 확장

암호화 키 분배 프로토콜을 모형화하기 위하여 5.1의 5.1.1에서 정의한 표준 패트리넷을 사용하며, 패트리넷의 모형화 및 분석 능력에는 영향을 미치지 않으면서 가시성을 높이기 위해 다음과 같은 표현 방법을 쓴다.

① 암호화된 메시지 플레이스
암호화가 됐음을 표시하기 위한 플레이스로 암호화된 횟수에 따라 원의 수가 증가한다.
② 암호화 키 플레이스
암호화 키를 가지고 있는 플레이스로서 사각형으로 표시한다.
③ 암호·복호화 트랜지션
암호·복호화 알고리즘을 수행하는 트랜지션을 의미하며 일반 트랜지션과 구분하여 흰색으로 표시한다.
④ 트랜지션
메시지의 송·수신, 송신할 메시지 단위 소자의 결합, 수신된 메시지의 분할, 사건의 순서를 표시한다.
⑤ 호선
토큰의 이동로를 표시한다.
⑥ 토큰
메시지, 변수 값의 활성화, 컨트롤을 의미한다.
⑦ 초기마킹
프로토콜의 초기 가정을 의미한다.
⑧ 점화 순서
프로토콜의 진행순서를 의미한다.

5.2 인증 절차에서의 검증 결과

그룹 초기자의 인증 절차를 모형화한 결과는 그림 3과 같고 표 4는 사용한 플레이스와 트랜지션의 의미이다. 그리고 도달성 그래프는 그림 4와 같다. 따라서 그룹 초기자는 인증 절차에서 오류 없이 그룹키를 획득할 수 있다. 또한 참가자도 오류 없이 그룹키를 획득할 수 있다.



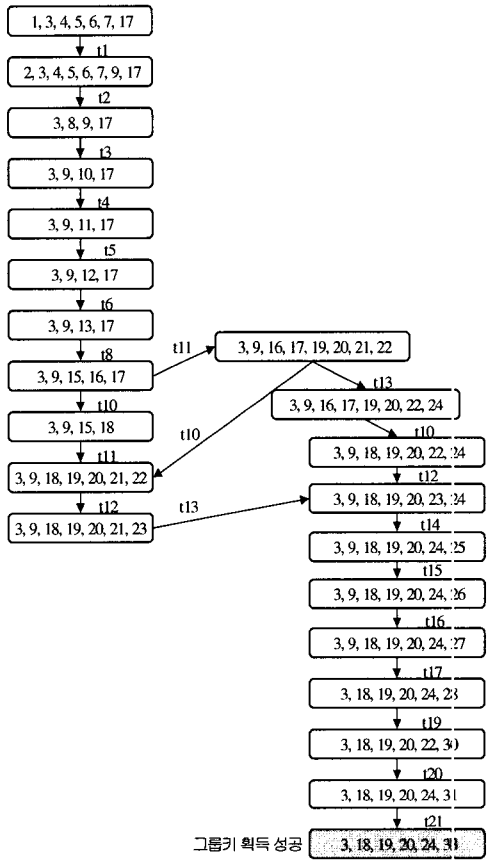
〔그림 3〕 그룹 초기자 인증 모형화

〔표 4〕 그룹 초기자의 인증 절차에서 플레이스와 트랜지션의 의미

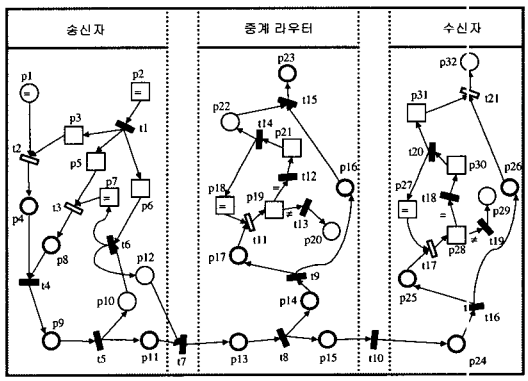
p	기능	t	기능
1	토큰(Token^{GI})생성	1	토큰(Token^{GI})복사
2	토큰(Token^{GI})대기	2	GI-p, grpAddr, srcAddr^{GI}, In/Ex, Token^{GI} 병합
3	개인키(GI-s) 생성	3	메시지 송신 처리
4	그룹 주소(grpAddr) 생성	4	메시지 전송
5	허용/거부(In/Ex) 목록 생성	5	메시지 수신 처리
6	공개키(GI-p) 생성	6	검증 성공 처리
7	발신지 주소(srcAddr) 대기	7	검증 실패 처리
8	병합 성공	8	존재 부재 처리
9	토큰(Token^{GI})대기	9	존재 확인 처리
10	메시지 송신	10	그룹키 생성 처리
11	메시지 수신	11	GI-p, Token^{GI} 분리
12	발신지 주소 검증	12	Token^{GI}, grpKey 병합
13	그룹 주소 존재 확인	13	공개키 처리
14	재전송 요구	14	암호화({Token^{GI}, grpKey}$^{GI-p}$)
15	그룹 주소 등록	15	암호 메시지 전송
16	그룹키(grpKey) 생성 신호 대기	16	복호화({Token^{GI}, grpKey}$^{GI-p}$)
17	그룹키(grpKey) 생성	17	검증 성공 처리
18	그룹키 대기	18	검증 실패 처리
19	허용/거부 목록 등록	19	토큰(Token^{GI}) 검증 처리
20	그룹 주소 등록	20	토큰 검증 성공 처리
21	공개키 대기	21	토큰 검증 실패 처리
22	토큰 대기	22	그룹키 처리
23	병합 메시지 대기		
24	공개키 대기		
25	암호 메시지 송신		
26	암호 메시지 수신		
27	복호화 검증		
28	복호화 검증 성공		
29	복호화 검증 실패		
30	토큰 검증		
31	토큰 검증 성공		
32	토큰 검증 실패		
33	그룹키 획득		

5.3 데이터 전송 절차에서의 검증 결과

각 참가자는 CBT 공유 트리 가입이 완료되었으므로 코어로부터 수신된 KEK와 자신이 생성한 TEK를 이용해 메시지를 암호화하여 전송한다. 암호 메시지 처리 절차에 대한 검증 결과는 그림 5 그림 6과 같다.



〔그림 4〕 그룹 초기자 인증의 도달성



〔그림 5〕 데이터 전송 절차의 모형화

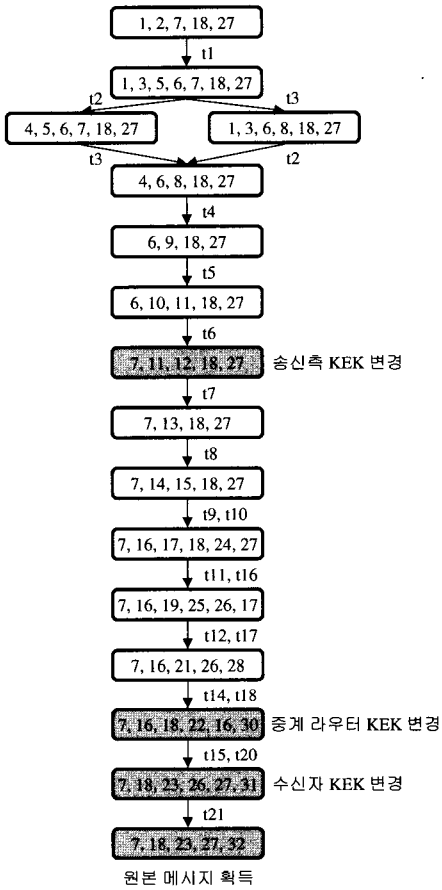
Ⅵ. 결 론

본 논문에서는 현재 멀티캐스트 통신을 위해서 제안되고 사용되고 있는 여러 가지 멀티캐스트 라우팅 프로토콜 중에서 보다 효율적인 보안 체계를 설계할 수 있는 공유 트리를 기반으로 하는 코어 기반 트리

〔표 5〕 데이터 전송 절차에서의 플레이스와 트랜지션의 의미

p	기능	t	기능
1	전송 메시지 발생(M)	1	TEK 복사
2	TEK 생성	2	암호화($\{M\}^{TEK}$)
3	TEK 대기	3	암호화($\{TEK\}^{KEK}$)
4	전송 메시지 암호화 성공	4	$\{M\}^{TEK}$, $\{TEK\}^{KEK}$병합
5	TEK 대기	5	송신 신호 처리
6	TEK 대기	6	TEK를 새로운 KEK로 변경
7	KEK 대기	7	암호 메시지 전송
8	암호화 성공	8	전송된 암호 메시지 복사
9	병합 성공	9	$\{M\}^{TEK}$, $\{TEK\}^{KEK}$ 분리
10	암호화 성공	10	암호 메시지 전송
11	암호 메시지 송신 대기	11	복호화($\{TEK\}^{KEK}$)
12	송신 허가 신호	12	복호화 검증 성공 처리
13	암호 메시지 수신	13	복호화 검증 실패 처리
14	암호 메시지 대기	14	TEK를 새로운 KEK로 변경
15	암호 메시지 송신	15	암호 메시지 제거
16	암호 메시지($\{M\}^{TEK}$) 대기	16	$\{M\}^{TEK}$, $\{TEK\}^{KEK}$ 분리
17	{TEK}KEK 대기	17	복호화($\{TEK\}^{KEK}$)
18	KEK 대기	18	복호화 검증 성공 처리
19	복호화 검증	19	복호화 검증 실패 처리
20	검증 실패	20	TEK를 새로운 KEK로 변경
21	검증 성공	21	복호화($\{M\}^{TEK}$)
22	$\{M\}^{TEK}$ 제거 신호 대기		
23	암호 메시지 제거 성공		
24	암호 메시지 수신		
25	$\{TEK\}^{KEK}$ 대기		
26	$\{M\}^{TEK}$ 대기		
27	KEK 대기		
28	복호화 검증		
29	복호화 검증 실패		
30	복호화 검증 성공		
31	TEK 대기		
32	원본 메시지 획득(M)		

(CBT: Core Based Tree)를 이용하여 3개로 구성된 그룹키, KEK, TEK만을 획득함으로서 안전한 멀티캐스트 통신이 가능한 키 분배 프로토콜을 제안하였다. 각 키들은 3가지 절차를 통하여 획득된다. 인증 절차에서 공개키 방식을 이용하여 명확히 참가자를 인증함으로서 그룹키를 획득하고, 가입절차에서 그룹키를 이용하여 TEK를 암호화 할 수 있는 KEK를 획득하고, 멀티캐스트 데이터 전송 절차에서 데이



〔그림 6〕 데이터 전송 절차의 도달성

터를 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 방식을 제안함으로서 탈퇴한 참가자로부터 기존의 멀티캐스트 데이터를 보호하기 위해 새로운 그룹키를 분배할 필요가 없게 되었다. 그러므로 데이터 전송 중에 탈퇴자로 인한 새로운 키를 분배해야 하는 트래픽 노드를 줄일 수 가 있다. 그리고 다중 코어로 확장 시에도 멀티캐스트 인증서를 분배함으로서 해당 코어에서 인증 절차를 수행할 수 있다. 설계된 키 분배 프로토콜을 검증하기 위해서 모형화 도구인 패트리넷을 이용하여 설계된 프로토콜의 안전성을 검증하였다. 향후 연구 과제로 제안된 키 분배 프로토콜을 실제 통신망에 적용하기 위

한 구현 방식에 대한 연구가 진행되어야 한다.

참 고 문 헌

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

[2] A. Ballardie, "Core Based Tree(CBT) Multicast Routing Architecture," Request for Comments 2201, Internet Activities Board, October 1997.

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

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

[5] G. Caronni, M. Waldvogel, D. Sun and 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.

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

[7] L. Gong and 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 1996.

[9] M. Burmester and Y. Desmedt, "A Secure and efficient conference key distribution system," In advances in Cryptology : Proceedings of Eurocrypt '94, pp 275-286 Berlin, 1995

[10] Gang-Soo Lee and Jin-Seok Lee, "Petri Net Based Models for Specification and Analysis of Cryptographic Protocols," Journal of System and Software U.S.A 1997

[11] Peter S. Kruus,"A Survey of multicast security issues and architectures," NISSC'98, Oct. U.S.A,

[12] Suvo mittra, *"Iolus: Framework for Scalable Secure Multicasting,"* In proceedings of ACM SIGCOMM'97, pp.277-288, Sept 1997.

〈著者紹介〉

김 봉 한 (Bong-han Kim) 정회원
1994년 2월 : 청주대학교 전자계산학과 졸업
1996년 2월 : 한남대학교 전자계산공학과 석사
2000년 2월 : 한남대학교 컴퓨터공학과 박사
현재 : 한남대학교 강사
〈관심분야〉 컴퓨터네트워크, 멀티캐스트, 정보보호

이 재 광 (Jae-kwang Lee) 정회원
1984년 2월 : 광운대학교 전자계산학과 졸업
1986년 2월 : 광운대학교 전자계산학과 석사
1993년 2월 : 광운대학교 전자계산학과 박사
1986년 3월~1993년 8월 군산전문대학 전자계산학과 부교수
1997년 7월~1998년 6월 University of Alabama 객원교수
1993년 8월~현재 : 한남대학교 컴퓨터공학과 부교수
〈관심분야〉 컴퓨터네트워크, 정보통신, 정보보호