情報保護學會論文誌
第12券 第6號, 2002. 12

동적 멀티캐스트 서비스상의 다단계 접근통제 기법

신 동 명*, 박 희 운*, 최 용 락**

A Multi-Level Access Control Scheme on Dynamic Multicast Services

Dong-Myung Shin*, Hee-Un Park*, Yong-Rak Choi**

요 약

안전한 멀티캐스트 서비스와 관련하여 아키텍처, 키분배, 송신자 인증 등에 대한 연구가 활발히 이루어지고 있지만 서비스 거부 공격이나 권한 없는 멤버에 대한 멀티캐스트 서비스 접근을 통제할 수 있는 접근통제 기술에 대한 연구는 매우 미진한 상태이다.

멀티캐스트에서의 다단계 접근통제는 비밀 원격회의나 다양한 등급을 갖는 고객에 대한 차별된 멀티미디어 서비스를 제공하는데 응용할 수 있다. 실제 멀티캐스트 네트워크를 구성할 경우, 각각의 보안등급에 따라 서로 다른 가상 네트워크를 구성하게 된다. 그러나 기존 방식은 다중 접속 네트워크 환경에서의 불법접근을 효율적으로 막지 못하고 있고 다단계 접근통제 메커니즘을 제공하고 있지 않다.

따라서, 본 논문에서는 기존 멀티캐스트 접근통제 방식을 확장하여 네트워크 계층에서의 효율적인 계층형 접근통제 방식을 제안한다. 또한 어플리케이션 계층에서의 계층형 접근통제를 위한 계층키(hierarchical key) 분배 방식과 가입 및 탈퇴가 자유로운 동적 멀티캐스트 환경에서의 효율적인 계층키 갱신 방식을 제안한다.

ABSTRACT

The access control techniques, which can control unauthorized members to access to multicast service, have not been studied very often while there are a lot of on-going study on secure multicast architecture, multicast key distribution and sender authentication scheme have been studied.

Multi level access control scheme in multicast can be used in a remote secure conference or to provide graduated multimedia services to each customers. In fact, multicast network has its own virtual networks according to different security levels. However, Early schemes are not effective when it protects unauthorized access in multi-access network environment. Furthermore this scheme does not provide us with hierarchical access control mechanism.

This paper, therefore, proposes hierarchical access control scheme to provide the effectiveness in network layer by security level comparison. And we also suggests hierarchical key distribution scheme for multi level access control in application layer and effective hierarchical key renewal scheme in dynamic multicast environment which is easy to join and leaving the multicast group.

Keyword : *multicast, access control, hierarchical key, key management*

* 한국정보보호진흥원(dmshin@kisa.or.kr)
** 대전대학교

Ⅰ. 서 론

멀티캐스트에서의 다단계 접근통제는 원격 비밀회의나 다양한 등급을 갖는 고객에 대한 차별된 멀티미디어 서비스를 제공하는데 응용할 수 있다. 예를 들어, 멀티캐스트를 이용한 활용분야로 원격회의가 있다. 멀티캐스트를 사용하지 않을 때의 시스템은 회의에 참여한 사람들에게 서로 메시지를 전달해 주는 관리서버가 되고 이 관리서버에 모든 참여 멤버가 접속하고 관리서버가 각각의 멤버와 1:1로 연결하여 메시지를 주고받는 형태를 갖는다. 그러나, 회의에 참여한 멤버들이 각기 다른 접근권한을 갖고 참여할 수 있다. 멀티캐스트 네트워크에 메시지를 전송하는 것을 쓰기(write) 오퍼레이션이라 하고 메시지 수신을 읽기(read) 오퍼레이션이라 하면, 멀티캐스트 데이터 메시지를 읽기만 가능한 멤버, 읽고 쓸 수 있는 멤버, 쓰기만 가능한 멤버 등의 구성에서부터 국방부와 같이 좀 더 복잡한 계층구조에서의 멀티캐스트 응용을 생각해 볼 수 있다.

또다른 다중 레벨의 멀티캐스트 접근통제 서비스 예로, 멀티캐스트를 이용한 실시간 멀티미디어 서비스를 들 수 있다. 멀티미디어 서비스에서는 서비스 가입자의 요금체계에 따라 전송 메시지에 대한 열람이 제한을 받을 수 있다. 이들의 특징은 멀티캐스트 서비스에 가입한 멤버라 할지라도 상황에 따라 서로 다른 가상 멀티캐스트 네트워크가 형성된다는 점이다. 가상 네트워크 환경에서는 여러 멀티캐스트 그룹이 혼재하는 형태를 갖기 때문에, 좀 더 많은 고려사항과 다수의 암호키를 관리해야 하는 부담이 있다.

현재 멀티캐스트 데이터가 권한없는 호스트 또는 사용자들에 의해 접근되는 것을 막는 방법에 대해 많은 연구가 진행되어 왔으나 해법들의 대부분은 응용레벨의 암·복호화에 기초하고 있다. 그러나, 응용레벨 메커니즘은 플러딩 공격과 같은 서비스 거부 공격에 대해 라우팅 인프라를 보호할 수 없다. 멀티캐스트 데이터가 멀티캐스트 라우터들에게 계속 복제될 수 있기 때문에 이러한 공격들은 멀티캐스트 서비스에 치명적인 영향을 줄 수 있다. 따라서 서비스 거부 공격을 막기 위한 메커니즘은 응용계층 보다는 네트워크 계층에서 제공되어야 한다.

본 논문에서는 이미 대중화되어 있는 CBT[1]구조를 기반으로 멀티캐스트 접근통제의 효율적 적용을 위해 네트워크 계층과 어플리케이션 계층으로 나누어 제시하였다. 기존의 권한있는 사용자와 권한없는 사용자에 대한 멀티캐스트 접근통제를 확장하여 상기 서비스에 대한 네트워크 계층에서의 효율적인 계층형 접근통제 방식을 제안하고 어플리케이션 계층에서의 계층형 접근통제를 위한 계층키(hierarchical key) 분배 방식과 가입 및 탈퇴가 자유로운 동적 멀티캐스트 환경에서의 효율적인 계층키 갱신 방식을 제안한다. 기존방식에서는 다중 레벨의 멀티캐스트 접근통제에 대한 연구가 없었다.

Ⅱ. 고려사항 분석

본 논문에서는 CBT구조를 기반으로 함으로 CBT 구조에서의 보안성은 논외로 하고 계층구조를 갖는 멀티캐스트에서 다중레벨 접근통제 서비스 제공시 필수적으로 고려되어야 할 사항과 효율성을 극대화하기 위해 제공되어야 하는 요구사항을 제시한다.

1) 효율적인 멀티캐스트 접근통제 서비스 제공
   - 다중 레벨의 접근통제 서비스가 제공될 때, 권한없는 메시지에 대해 사전 차단할 수 있어야 함.
2) 서비스 거부 공격에 대한 면역성 확보
   - 불법적인 멀티캐스트 데이터에 의한 전체 멀티캐스트 서비스의 폭주를 방지할 수 있는 메커니즘이 존재해야 함.
3) 키 분배·갱신의 효율성 :
   - 다중 레벨의 접근통제를 위한 다수의 계층키를 분배하거나 갱신시 최소의 메시지 교환을 요구
4) 동적환경에서 그룹키 비밀성, 전방보호(Forward Secrecy), 후방보호(Backward Secrecy)[4]만족
   - 일정기간 생성된 그룹키를 알아도 이로부터 이후에 생성된 그룹키를 유도할 수 없는 전방보호와 이전에 생성된 그룹키를 유도할 수 없는 후방보호가 제공되어야 함
   - 멀티캐스트 그룹에 가입 및 탈퇴시에도 그룹키의 비밀성, 전방보호, 후방보호를 제공해야 함
5) 메시지 전송의 효율성
   - 다중 레벨의 접근통제 서비스에 따른 다중 암호화 등의 비효율성이 없어야 함.

Ⅲ. 관련 기반 연구

멀티캐스트 서비스상에서의 계층형 접근통제 응용분야가 많이 존재하고 중요성이 강조됨에도 불구하고 이에 대한 연구는 미흡하였다. 본 절에서는 네트

워크 계층에서의 접근통제 연구와 계층키 관련 연구에 대해 분석하였다.

3.1 네트워크 계층 멀티캐스트 접근통제 기술

멀티캐스트 데이터가 권한 없는 호스트 또는 사용자들에 의해 접근되는 것을 막는 2 레벨 접근통제에 대해 연구가 진행되어 왔으나 해법들의 대부분은 어플리케이션 계층의 암·복호화에 기초하고 있다. 그러나, 어플리케이션 계층의 메커니즘은 플러딩 공격과 같은 서비스 거부 공격에 대해 라우팅 인프라를 보호할 수 없다. 따라서 서비스 거부 공격을 막기 위한 메커니즘은 어플리케이션 계층보다는 네트워크 계층에서 제공되어야 한다.

CBT[1]와 같이 양방향성을 지원하면서, 중앙집중화된 그룹 멤버관리 형태는 서비스 거부 공격에 대해 특히 취약한 구조를 갖게된다. 악의적인 호스트가 서비스 거부 공격을 수행하고자 한다면 양방향 멀티캐스트 트리의 어떤 위치에서도 임의의 데이터로 폭주시키는 것이 가능하다. 이러한 취약성을 해결하기 위한 라우터 기반의 접근통제 기법이 제안되었다.[2]

특히, 네트워크 기반 접근통제 서비스를 제공하는 DSAC[2]방식에서는 멤버를 송수신 가능 멤버, 송신 전용 멤버, 수신 전용 멤버, 비멤버 송신자로 나누어 접근권한을 분류하고 있다. DSAC 방식에서는 라우터의 인터페이스 하나에 하나의 호스트 또는 사용자가 연결된 경우를 가정하고 있으며, 하나의 서브넷에 서로 다른 접근권한을 갖는 멤버가 존재하는 경우에는 적용되지 않는다. 또한 허브와 같은 네트워크 연결장치를 이용하여 랜환경에서 다중 접속이 허용되는 일반적인 네트워크환경에서의 불법접근을 막지 못하는 단점이 있다.

업스트림 인터페이스로부터 오는 모든 패킷은 모두 전달을 허용하기 때문에, 다중 접속 랜 환경에서 신뢰된 라우터 사이에 불법접속하는 경우를 원천적으로 막지 못한다. 그러나, 일반적인 네트워크 환경에서는 하나의 네트워크 인터페이스에 하나의 서브넷이 연결되어 있는 경우가 대부분이고, 하나의 서브넷에는 다수의 멀티캐스트 멤버들이 연결될 수 있다.

DSAC방식은 서브넷 내에 다수의 멤버가 존재하는 경우에는 적합하지 않다. 또한 DSAC방식에서는 동일한 서브넷에 있는 멤버들은 동일한 접근통제 규칙을 적용받는다. 따라서, 네트워크 세그먼트내에 동일한 그룹에 가입한 멤버가 여럿 있는 경우에 대한 방안이 마련되어야 한다.

3.2 계층 구조에서의 접근통제 암호키 기술

계층 구조 내에서 접근통제는 군사기관, 정부 기관뿐만 아니라 일반 민간 회사에서도 사용하고 있다. 이러한 서비스를 제공하기 위해서는 높은 보안 클래스(SC : Security Class)의 사용자들이 낮은 보안 클래스에 있는 사용자의 비밀키를 구할 수 있는 메커니즘이 필요하다. 하나의 보안 클래스 SC에 하나의 비밀키 SK가 맵핑된다고 할 때 이를 위한 가장 쉬운 방법은 사용자가 하위레벨의 키를 모두 갖고 있는 것이다. 특정 보안 클래스 SC_i에 속한 사용자가 하위 사용자의 모든 키를 알기 위해서는 비밀키 집합 $\{SK_i, SK_{(i-1)}, \ldots, SK_1\}$을 가져야 한다. 또한 계층이 무한히 커지면 상위 사용자는 많은 키를 가져야함으로 불편함과 동시에 많은 키를 안전하게 관리하기 힘들어진다. 따라서 사용자가 접근 가능한 모든 키를 구할 수 있는 하나의 계층키를 갖게 하는 방법이 필요하다.

계층구조를 갖는 환경에서의 키 분배를 위한 계층키 생성 및 하위키(lower key) 유도에 대한 연구가 계속되어왔다.[5~15] 그러나, 상위 키(upper key)가 하위 키를 유도할 수 있는 계층키의 특성상, 계층간의 키는 선형적으로 연결되어 있으며, 임의의 계층의 키 갱신은 전체 계층키의 갱신을 요구한다. 가입 및 탈퇴가 자유로운 동적 멀티캐스트 환경에서, 후방보호와 전방보호를 보장하기 위해서는 멤버의 가입 및 탈퇴가 일어날 때마다 멤버가 소속한 그룹의 그룹키를 갱신해주어야 한다.

따라서, 그룹키가 여러 단계의 계층구조를 이루는 경우, 위에서와 같이 멤버의 변경은 임의의 그룹의 계층키를 갱신하고 이것으로 인해 전체 계층키를 갱신해야 하는 연쇄적인 키갱신 문제가 발생한다.

현재까지의 계층키 분야 연구는 보안 클래스(Security Class)내에서 사용자의 키를 갱신하는 데에는 무리가 없지만, 보안 클래스의 키를 갱신하는 경우에는 모든 보안 클래스의 키와 소속된 사용자의 모든 비밀키도 갱신해 주어야 한다.[5~15] 이것은 보안 클래스에 소속된 사용자들이 탈퇴하거나 새로운 사용자가 가입하는 동적인 환경을 고려하지 못하고 있다. 다만, 소속된 사용자들의 비밀키를 오랜 기간 사용하는 경우, 보안성을 위해 사용자의 비밀키를 정기적으로 갱신할 필요가 있는 경우에 적용될 수 있으며

다른 보안 클래스에 속한 멤버의 키에 영향을 주지 않고 효율적으로 키갱신이 이루어진다.

KSCL,[11] Chang-Pan[15] 방식에서 사용자가 전방보호 보장을 위해 CA(Central Authority)에게 CA의 비밀키를 갱신할 것을 요구할 때 CA는 반드시 모든 사용자의 비밀 키를 다시 유도해야 한다. 다만, 보안 클래스내에서는 마음대로 자신의 비밀키를 바꿀 수 있고 CA는 단지 보안 클래스의 공개정보 C만 갱신하면 된다. 예를 들어, 보안 클래스 SC_i의 SK_i가 SK'_i로 바뀐다면, 상위 보안 클래스의 사용자는 바뀐 SK'_i를 다시 계산하는데 필요한 공개정보 C_i를 단지 $C'_i=(SK'_i \,||\, ID_i)((SK'_i \,||\, ID_i)+b_i) \bmod m$로 갱신만 하면 되고 다른 키나 정보는 바꾸지 않아도 된다. 여기에서 $(b, m=p\cdot q)$은 Rabin 공개키 시스템에서 암호화를 위한 공개키 쌍이며, ID는 4개의 평문 후보 중 정확한 평문을 찾기 위한 식별정보이다.

그러나, 탈퇴한 멤버가 자신보다 낮은 멤버의 키를 계속 유도할 수 있으므로 전방보호 보장을 위해 전체 키갱신이 반드시 필요하다. KSCL, Chang-Pan 방식에서는 권한 없는 외부 사용자에 대한 안전성만을 고려하고 있으며, 탈퇴한 사용자는 물리적으로 격리된다는 가정하에서는 유효하다. 그러나 계층형 멀티캐스트 접근통제와 같이 동적으로 멤버의 가입 및 탈퇴가 자유롭고 상위 보안 등급을 가진 사용자가 하위 보안 등급으로 내려간 경우, 이전의 키에 의해 접근될 수 있었던 정보를 차단하기 위하여 해당 보안 클래스의 모든 하위 클래스에 대한 비밀키를 갱신해야 하며 이는 CA의 비밀키를 갱신함으로써 가능하다. 따라서 전방보호와 후방보호를 보장하기 위해서는 멤버가 가입 또는 탈퇴할 때마다 CA의 비밀키를 갱신하고 모든 사용자의 비밀키를 다시 유도해야 하는 한계가 있다.

Ⅳ. 제안 방식

기존의 멀티캐스트 방식은 다중 레벨의 접근통제를 고려하지 않았다. 본 방식에서는 4.1절에서는 네트워크 계층에서의 접근통제 방식을 제시하고, 4.2절에서는 4.1절과 연계하여 어플리케이션 계층에서의 접근통제 방식을 제시한다.

4.1 네트워크 계층에서의 멀티캐스트 접근통제

네트워크 계층에서의 다중레벨 접근통제는 멤버가 코어에 등록하는 과정에서 자신이 속한 서브넷의 최대 접근레벨과 하위 노드 각각에 대한 최대 접근레벨을 등록함으로써, 접근권한이 높은 메시지의 불필요한 전달을 사전에 차단하여 전체적인 네트워크 효율성을 제공한다. 가입요청에 따른 인증과 접근통제 권한부여는 DSAC에서와 마찬가지로 코어에서 담당한다.

4.1.1 시스템 계수 정의

- Sx : 멤버 x의 보안 레벨(Security Level)
- $node\_id$: $b_1b_2....b_{(h-1)}b_h$, $b_i=\{0, 1\}$, $1\le i\le h$, h는 트리의 높이
- $EmaxR_{node\_id}$: $node_id$의 오른쪽 자식 노드들의 최대 보안 레벨, i는 트리의 레벨, i=1, 2, ..., n
- $EmaxL_{node\_id}$: $node_id$의 왼쪽 자식 노드들의 최대 보안 레벨, i는 트리의 레벨, i=1, 2, ..., n
- $Imax_{node\_id}$: $node\_id$ 노드에 소속된 멤버들의 최대 보안 레벨
- G : 가입하고자 하는 그룹 식별자
- I : 네트워크 인터페이스 주소
- $Sign\_x()$: x의 전자서명 메시지(메시지와 서명값)
- $nonce$: 재전송 방지를 위한 임시 비표
- k_{eq} : 코어 라우터와 지정 라우터간의 공유키
- SC : 보안 클래스
- sc_id : 보안 클래스 ID
- GK : 계층키 SK를 교환할 때 사용하는 키 암호화키(KEK)
- SK : 보안 클래스의 계층키
- UK : 집합 U에 속한 사용자들의 비밀키

4.1.2 시스템 개요

본 논문에서는 트리의 차수(degree)가 2이하인 양방향 완전이진트리를 가정한다.

$EmaxR$과 $EmaxL$을 통칭하여 $Emax$라 하면 $Emax$는 자신의 하위 노드 전체에 대한 최대값이고 $Imax$는 자신의 노드 안쪽에 대해서만 최대값을 나타낸다. $Emax \ge$ (하위노드 $Imax$와 하위노드 $Emax$)가 성립한다. $Emax$는 하위노드의 모든 $Emax$와 $Imax$의 최대값을 가져야 한다. 또한 $Imax$는 자신노드의 최대값을 가져야 한다. 단, 자신의 $Emax$와 자신의 $Imax$와는 상관관계가 없다. 임의의 호스트 또는 멤버는 자신의 접근통제 레벨에 상응하는 암호화된 메시지를 생성한다. 접근통제를 위한 계층형 키구조에서 각 멤버들은 해당 접근권한에 해당하는 키목록을 라

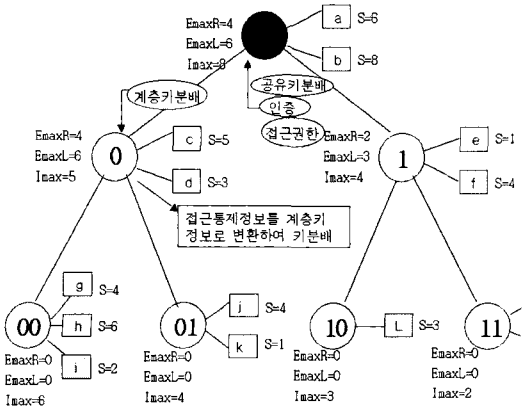
우터와 공유했다고 가정한다. 암호화된 메시지는 멀티캐스트 라우터에서 상위노드 인터페이스와 우측, 좌측 하위 인터페이스로 전달할지를 결정한다. 이때, 상위노드로의 전달은 항상 이루어지고, 하위노드에 대한 전달은 각각의 최대값과 비교하여 결정한다.

4.1.3 멤버 가입 요청

사용자 x는 아래의 멤버 가입 요청 메시지를 전송하고 코어 라우터로부터의 승인 메시지를 기다린다.

$x \rightarrow core$:
$\{join\_request||Sign_x(G||x\_id||node\_id||I)||User\_AC\_level||(EmaxR_{node\_id}||EmaxL_{node\_id}||Imax_{node\_id})||nonce_x\}$

사용자 x는 가입하고자 하는 그룹과 자신의 ID, 소속 노드의 ID, 네트워크 인터페이스 주소를 설정하고 ($EmaxR_{node\_id}$, $EmaxL_{node\_id}$, $Imax_{node\_id}$)값은 설정하지 않는다. 가입 요청 메시지는 먼저 지정 라우터(Designated Router)에 전송된다. 지정 라우터에서는 보내온 *User_AC_level* 정보를 이용하여 $Imax_{node_id}$의 값을 설정하고 현재 *node_id*의 $EmaxR_{node\_id}$, $EmaxL_{node_id}$값을 적재한다. 단, 지정 라우터에서는 $Imax_{node_id}$의 값을 저장하되, 활성화시키지는 않는다. $EmaxR_{node\_id}$, $EmaxL_{node\_id}$, $Imax_{node_id}$값은 코어 라우터로부터 승인 메시지를 수신할 때 활성화된다. 사용자 x의 가입 요청 메시지가 코어 라우터에 다다르기까지 지나가는 경유 라우터에서는 $Imax_{node_id}$값을 이용하여 자신의 $EmaxR_{node\_id}$ 또는 $EmaxL_{node\_id}$ 값을 갱신하고 가입 요청 메시지의 정보를 갱신한다.



〔그림 1〕 보안레벨을 갖는 멀티캐스트 접근통제 예

마찬가지로 승인 메시지를 받기 전까지 $EmaxR_{node\_id}$ 또는 $EmaxL_{node_id}$값은 활성화되지 않는다. 갱신할 $EmaxR_{node_id}$와 $EmaxL_{node\_id}$ 값의 선택은 *node_id*와 네트워크 인터페이스 주소를 보고 결정한다. 〔그림 1〕에서와 같이 상위노드와 하위노드는 *node_id*의 길이를 보고 결정할 수 있으며, *node_id*의 끝에 붙는 1과 0값으로 오른쪽 자식노드와 왼쪽 자식노드의 최대값을 구분한다.

$EmaxRb_1b_2...b_{h-1} =$
$Max(EmaxRb_1b_2...b_{h-1}1, EmaxLb_1b_2...b_{h-1}0, Imaxb_1b_2...b_{h-1}1)$
$EmaxLb_1b_2...b_{h-1} =$
$Max(EmaxRb_1b_2...b_{h-1}1, EmaxLb_1b_2...b_{h-1}0, Imaxb_1b_2...b_{h-1}0)$
$Imaxb_1b_2...b_{h-1} =$
$Max(Internal\ members : Sx)$

4.1.4 멤버 가입 승인

코어 라우터는 사용자 x가 보낸 가입 요청 메시지를 수신하고, 서명값을 검사하고 데이터베이스 내의 사용자 엔트리 정보와 비교하여 정상 사용자인지와 접근권한이 일치하는지를 확인한다. 그리고, $EmaxR_{core}$, $EmaxL_{core}$값을 갱신한 후 승인 메시지로써 *join_activate* 메시지를 전송한다.

$core \rightarrow x$:
$\{join\_activate||Sign_{core}(x\_id||node\_id||User\_AC\_level)||nonce_{core}\}$

승인 메시지는 가입 요청 메시지가 경유한 경로를 따라 반대방향으로 전송된다. 이때 중간의 경유 라우터에서는 승인 메시지 수신시 사용자 x의 가입 요청에 따른 $EmaxR_{node\_id}$, $EmaxL_{node\_id}$, $Imax_{node\_id}$ 계산값을 활성화시킨다.

4.1.5 멀티캐스트 메시지 전송

메시지 전송은 코어 라우터와 지정 라우터간의 공유키 k_{eq}로 암호화하여 전송한다. *User_AC_level*은 빠른 접근통제 수행을 위해 암호화하지 않고, hash-MAC(Message Authentication Code)을 사용하여 접근통제 정보의 무결성을 보장한다.

*Security_Classification_level*은 멤버가 메시지에 접근할 수 있는 허용등급을 의미하며, *User_AC level*

은 멤버의 접근권한을 의미한다.

*Security_Classification_level*은 *User_AC_level* ≤ *Security_Classification_level*을 만족하도록 송신자의 보안 레벨보다 같거나 높은 보안 레벨로 설정해야 한다. 네트워크 접근통제에서는 라우터가 *Security_Classification_level*과 $EmaxR_{node\_id}$, $EmaxL_{node\_id}$, $Imax_{node_id}$값을 비교하여 라우터간 또는 라우터 안쪽에 메시지 전달(Forward) 여부를 결정한다.

$$\{msg\_Forward||Ek_{eq}(message)||User\_AC\_level||Security\_Classification\_level||MAC_{eq}(User\_AC\_level||Security\_Classification\_level)\}$$

지정 라우터(Designated Router)에서는 서브넷내로 메시지를 전달하기로 결정된 경우, 4.2절의 $SK_{Security\_Classification\_level}$ 계층키로 메시지를 암호화 하여 브로드캐스트 한다. 암호화된 메시지를 수신한 각 멤버들은 자신이 메시지를 복호할 수 있는지 *Security_Classification_level*을 통해 확인하고, 복호가 가능한 경우, 자신이 알고 있는 계층키로 $SK_{Security\_Classification\_level}$ 계층키를 유도하여 메시지를 복호화한다.

$$\{msg\_send||Eksk_{Security\_Classification\_level}(message)||User\_AC\_level||Security\_Classification\_level||MACsk_{Security\_Classification\_level}(User\_AC\_level||Security\_Classification\_level)\}$$

본 방식에서는 멀티캐스트 트리상에서 하위 레벨로 내려가면서 사전에 하위 노드에 대한 접근통제 레벨을 파악하여 불필요한 접근통제 연산과 전체 네트워크 트래픽을 줄일 수 있다. 접근통제 레벨에 따른 연결노드의 최적화가 이루어지면, 각 노드당 메시지 전달 확률은 더욱 낮아지며, 최악의 경우에도 서브넷내에서의 접근통제에 의해 1이하의 확률을 갖는다. 일반적인 환경에서는 높은 접근권한을 갖는 멤버가 낮은 권한을 갖는 멤버보다 적기 때문에, 트리의 깊이가 커질수록 메시지 전달 확률은 낮아진다.

4.2 어플리케이션 계층의 계층형 암복호화

계층구조 내에서 사용자와 사용자의 정보는 보안 클래스의 집합으로 구성된다. 사용자가 U_1, U_2..., U_n과 같은 집합으로 나뉜다고 가정할 때, 보안 클래스 SC_i는 U_i 각각을 지정하는데 쓰인다. 따라서, 사용자들은 접근권한을 나타내는 보안 클래스를 할당받는다. SC_1, SC_2,....., SC_n에서 SC_n을 n번째 보안클래스라 하자. 그리고 ≤은 집합 $SC=\{SC_1, SC_2, ..., SC_n\}$로 완전 순서화된 관계라 정의하면 완전 순서화된 집합관계 $(SC, \leq)$, $SC_j \leq SC_i$는 SC_i에서의 사용자가 SC_j의 사용자보다 접근권한이 같거나 높다는 것을 의미한다. 즉, SC_i 보안클래스에 해당하는 사용자가 SC_j 보안클래스 사용자의 정보를 쓰거나 읽을 수 있다. 반대로 SC_j의 사용자는 SC_i사용자의 정보를 쓰거나 볼 수 없다.

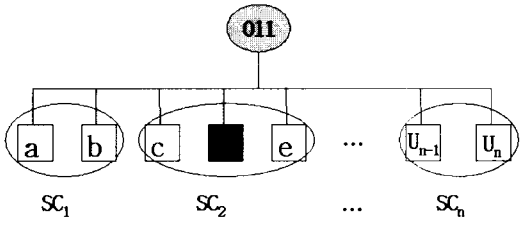
본 논문에서는 SC_i에 해당하는 계층키 SK_i값을 해쉬체인을 통해 계산한다. 라우터는 임의의 비밀정수 A를 생성하고 $SK_1=H(A)$, $SK_2=H(SK_1)$, $SK_3=H(SK_2)$, ..., $SK_n=H(SK_{n-1})$을 생성한다.

SC_i 보안 클래스의 사용자가 평문 M을 데이터베이스에 저장하거나 네트워크에 전송하려할 때 M을 암호화하기 위해서 비밀키 SK_i를 사용하고 암호문 $C=Esk_i(M)$를 계산하여 저장하거나 전송한다. 이때 오직 SK_i의 사용자만이 $M=Dsk_i(C)$를 계산함으로써 평문 M을 얻을 수 있다. $SC_j \leq SC_i$ 인 경우, SC_i는 자신의 비밀키 SK_i와 SC_j의 공개정보를 이용하여 SC_j의 비밀키 SK_j를 구할 수 있고 SC_j가 갖는 정보를 읽을 수 있다.

4.2.1 비밀키 갱신

보안 클래스를 다음과 같이 $SC=\{SC_1, SC_2, SC_3, ..., SC_n\}$로 정의하였을 때, 완전 순서화된 집합의 경우, $SC_1 \geq SC_2 \geq SC_3 \geq ... \geq SC_n$가 된다. 또한 사용자 그룹을 $U=\{U_1, U_2, U_3, ..., U_n\}$라 하면 SC_i와 U_i는 각각 일대일 대응된다고 가정한다.

- $SC=\{SC_1, SC_2, SC_3, ..., SC_n\}$,
- SC의 그룹ID=$\{IDsc_1, IDsc_2, IDsc_3, ..., IDsc_n\}$
- $U=\{U_1, U_2, U_3, ..., U_n\}$



〔그림 2〕 서브넷내에서의 보안 클래스와 멤버

[그림 2]에서와 같이 사용자 집합의 멤버 구성을 $U_1=\{a, b\}$, $U_2=\{c, d, e\}$, $U_3=\{f, g\}$.... 라 하면 각 멤버들은 고유의 비밀키 a_k, b_k, c_k.... 를 ID가 '011'인 라우터와 공유했다고 가정할 때 $UK_1=\{a_k, b_k\}$, $UK_2=\{c_k, d_k, e_k\}$, $UK_3=\{f_k, g_k\}$,...가 된다.

멤버 a, b 와 멤버 c, d, e는 각각 SC_1의 계층키 SK_1과 SC_2의 계층키 SK_2를 공유하게 된다.

[그림 2]에서 SC_2에 속하는 멤버 d가 탈퇴했을 경우, 전방보호를 만족시키기 위하여 모든 멤버의 계층키 SK_n를 갱신해야 한다. 제안 방식에서는 비밀키를 갱신하기 위해 먼저, 탈퇴한 멤버가 소속되었던 보안 그룹에서 탈퇴한 멤버를 제외한 나머지 멤버에 대해 그룹키 GK_i'를 분배함으로써 탈퇴한 멤버를 그룹에서 제거한다. 새로 분배된 GK_i'과 다른 그룹키를 이용하여 계층키 SK_n'를 분배한다.

1단계 : 멀티캐스트라우터는 탈퇴하려는 멤버 d로부터 탈퇴 메시지를 수신

2단계 : 라우터는 탈퇴 멤버 d 가 소속된 그룹의 식별 ID와 $H(d_k)$값을 멤버들에게 브로드캐스트 한다. 여기서 $H()$는 해쉬함수이다. d_k값이 아닌 $H(d_k)$값을 전송하는 이유는 멤버 d가 알고있는 GK_2와 SK_2를 노출시키지 않으면서 GK_2'을 효율적으로 재분배하기 위해서이다.

Group-ID	Value
$IDsc_2$	$H(d_k)$

3단계 : 라우터가 브로드캐스트한 Group-ID가 $IDsc_2$인 멤버들은 라우터가 보낸 $H(d_k)$값을 이용하여 다음식을 계산한다. α, β, ... 는 탈퇴한 멤버의 비밀키에 대한 해쉬값이고 g와 n은 공개된 임의의 큰 소수이다. $(x_k-\alpha)(x_k-\beta)\cdots$의 값은 음수이어도 곱셈의 역원이 항상 존재하기 때문에 상관없다.

$$x_{k'}=g^{(x_k-\alpha)(x_k-\beta)\cdots} \bmod n$$

예제에서는 멤버 d가 탈퇴했으므로, $x_k=H(d_k)$가 된다. 따라서

$$c_{k'}=g^{H(c_k)-H(d_k)} \bmod n$$
$$d_{k'}=g^{H(d_k)-H(d_k)} \bmod n=1$$
$$e_{k'}=g^{H(e_k)-H(d_k)} \bmod n$$

d_k'은 계산결과가 1이 되므로, 새로운 그룹키 GK_2'를 계산할 수 없다.

4단계 : 라우터는 새로운 그룹키 GK_2'를 c_k'과 e_k'으로 암호화하여 전송한다.

$$\{IDsk2||Ec_k'[GK_2]||Ee_k'[GK_2']\}$$

5단계 : 기존의 그룹키와 새로 분배된 그룹키를 이용하여 계층키를 분배한다. 이때 분배해야 하는 계층키의 수는 멤버수에 관계없이 그룹의 수와 같다.

또한, 갱신된 그룹키 GK_2'를 제외한 나머지 그룹키는 이전의 그룹키를 그대로 사용한다.

$$\{SK\_Update\_msg||E_{GK_1}[SK_1']||$$
$$E_{GK_2'}[SK_2']||\cdots||E_{GK_n}[SK_n']\}$$

4.2.2 그룹키 분배의 효율성 증대 방안

위의 3단계에서 분배된 c_k'과 e_k'을 이용하여 4단계에서 새로운 그룹키 GK_2'를 c_k'과 e_k'으로 각각 암호화하여 분배하였다. 본 절에서는 각각 암호화하여 분배하는 부분을 공개정수 t를 이용하여 효율적으로 분배하는 방법을 제시한다.

4단계 : 라우터는 다음의 공개정수 t를 계산하여 멤버들에게 브로드캐스트한다.

$$t=g^{C_i'+e_i'} \bmod n$$

공개정수 t는 c_k'과 e_k'을 아는 멤버만이 계산할 수 있다. 따라서, 멤버 c와 e는 다음을 계산하여 새로운 그룹키를 유도한다.

$$GK'=(t\cdot g^{-x_k'})^{x_k'} \bmod n$$

멤버 c :

$$GK_2'=(t\cdot g^{-c_k'})^{c_k'} \bmod n$$
$$=(g^{c_k'+e_k'}\cdot g^{-C_k'})^{c_i'} \bmod n$$
$$=g^{c_k'e_k'} \bmod n$$

멤버 e :

$$GK_2'=(t\cdot g^{-e_k'})^{e_k'} \bmod n$$

$$= (g^{c_k' + e_k'} \cdot g^{-e_k'})^{e_k'} \bmod n$$
$$= g^{c_k' e_k'} \bmod n$$

따라서, 멤버 c와 e는 동일한 그룹키 $g^{c_k' e_k'} \bmod n$을 갖게 된다.

그러나, 위의 식은 사용자 그룹에서 탈퇴한 멤버들을 제외한 나머지 멤버 수가 2일 때 적용 가능하다. 멤버가 탈퇴할 때, 해당 그룹에서 탈퇴한 멤버를 제외한 멤버에 대해 최대 멤버수가 2를 갖는 그룹으로 분할하여 위의 방식을 적용할 수 있다. 한 그룹의 멤버수를 n이라 할 때 $\lfloor \frac{n}{2} \rfloor$ 개의 공개 정수 t를 분배해야 하며, 전체 그룹의 수도 증가하게 된다.

4.2.3 그룹키 분배 방식의 확장

위의 식을 확장하기 위해 공개 정수 t를 다음과 같이 설정하였다.

$$t(x) = g^{f(x)} \bmod n \quad (1)$$

$$f(x) = (a_k + b_k - x)x \quad (2)$$

$$f(x) = (a_k b_k + b_k c_k + c_k a_k + x^2 - a_k x - b_k x - c_k x)x \quad (3)$$

수식 (2)에서의 $f(x)$ 함수는 그룹멤버의 수가 2인 경우이다. 예를 들어 그룹 멤버가 {a, b}인 경우, $f(a_k) = f(b_k) = a_k \cdot b_k$가 된다.

수식 (3)에서의 $f(x)$ 함수는 그룹멤버의 수가 3인 경우이다. 예를 들어 그룹 멤버가 {a, b, c}인 경우 $f(a_k) = f(b_k) = f(c_k) = a_k \cdot b_k \cdot c_k$가 된다.

Diffie-Hellman 방식을 사용하여 그룹키를 분배하는 경우에는 지정라우터와 멤버들간의 n 번의 키교환이 요구되며, 수식 (2)의 공개정보 t를 이용한 방식은 $\lfloor \frac{n}{2} \rfloor$번이, 수식 (3)과 (2)를 이용하는 경우 $\lfloor \frac{n}{3} \rfloor$번이 요구된다. 그러나, 4자 이상의 다자간 키교환 방식은 $f(x)$ 함수의 계산이 복잡해지므로, trade-off를 고려하여 $t(x)$ 계산을 위한 멤버수를 선택해야 한다.

V. 제안 방식 평가

5.1 전송 효율성 분석

제안된 방식은 완전전달(Full Forwarding) 방식에 비해 네트워크 트래픽에서 많은 이득을 준다. 완전전달 방식의 멀티캐스트 라우터는 입력된 모든 메시지를 말단 노드의 멤버들에게까지 항상 전달한다. 따라서 전달 확률은 항상 1 이다. 그러나 제안된 방식은 *Emax*와 *Imax*에 따라 하위 노드 및 서브넷 내로의 전달여부를 결정한다. 먼저, 멤버들로 구성된 트리에서 임의의 노드를 잡아 어느 정도 전달되는지 살펴보자. 각 노드를 멀티캐스트 라우터라고 볼 때 라우터가 결정하는 것은 그 노드 내의 멤버들에게 전달을 하는지 여부와 자식 노드에게 전달을 하는지 여부이다. 노드에 입력되는 메시지의 보안등급이 *1* ~L_0 사이에 난수로 구성되어 있고 각 등급의 출현 빈도가 $1/L_0$ 로 균일하다고 가정한다.

L_0 : 보안등급 수
l : 입력된 메시지의 보안등급
n : 각 노드에 딸린 멤버 수

우선 멤버 수가 1인 경우를 살펴보자. 라우터가 받은 임의로 메시지의 보안레벨을 x1이라고 하고 전달여부를 결정할 멤버의 보안레벨을 x2라고 하자. 그러면 라우터는 $x1 \le x2$ 인 경우만 전달해야 한다. 계산을 간편하게 위해 우선 각 멤버들은 1에서 L_0 사이에 고르게 분포한다고 가정한다. 그러면 보안 등급 l을 가질 확률은 $1/L_0$ 이다.

$$P(x_1 \le x_2) = \sum_{r=1}^{L_0} \frac{1}{L_0} \frac{L_0 - (r-1)}{L_0}$$
$$= \frac{1}{L_0^2}\left(L_0^2 + L_0 - \frac{L_0(L_0+1)}{2}\right) = \frac{L_0+1}{2L_0} \quad (1)$$

다음은 멤버의 수가 n개인 내부 노드에 전달하게 되는 확률을 구해보자. 전달이 일어나는 경우는 입력된 메시지의 보안레벨보다 큰 보안레벨을 가진 멤버가 하나 이상 존재할 때이다.

$$P(x_1 \le Max(x_2 \in I))$$

멤버들 중 r개만 l보다 크거나 같고 나머지는 작은 경우,

$$\frac{{}_nC_r (L_0 - l + 1)^r (l-1)^{n-r}}{L_0^n} \quad (2)$$

구하고자 하는 식은 모든 경우에서의 식이므로 각각

의 (2)를 합산한다.

$$P(x_1 \le Max(x_2 \in I)) = \sum_{r=1}^{n} \frac{{}_nC_r(L_0-l+1)^r(l-1)^{n-r}}{L_0{}^n} \quad (3)$$

식 (3)은 노드의 내부 멤버들에 대해 브로드캐스트 할 확률이다.

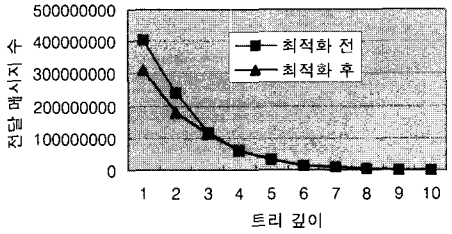
다음으로 자식 노드들에게 브로드캐스트할 확률을 구해보자. 자식 노드에게 브로드캐스트할 확률은 결국 자식 노드들의 모든 멤버들 중 입력받은 메시지의 보안레벨보다 큰 보안레벨을 갖는 멤버가 존재하는 경우이다. 따라서 식 (3)에서 n에 전체 멤버수를 대입하면 된다.

트리의 높이가 H이고 깊이가 d 인 노드는 $h'=H-d+1$ 의 높이를 갖는다. 한편, 우리가 관심을 갖고 있는 노드는 그 노드의 왼쪽이나 오른쪽 노드이기 때문에 높이가 하나 만큼 낮아 $h=H-d+1-1=H-d$ 의 높이를 갖는다. 높이가 h인 트리의 자손 노드 수는 2^h-1 이다. 따라서 각 노드의 멤버 수를 N_0 라고 한다면, 트리에서 깊이가 d 인 노드의 왼쪽이나 오른쪽 자손에 포함된 멤버 수는 다음과 같다.

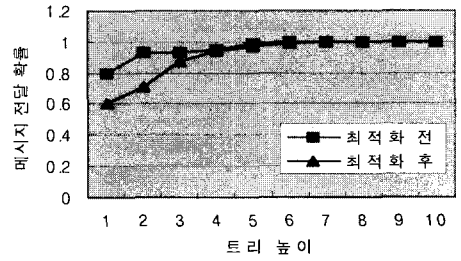
$$N_0(2^h-1) \quad (4)$$

식 (4)를 식 (3)에 대입하면 왼쪽이나 오른쪽 자손에 대해 브로드캐스트할 확률이 된다. 최악의 경우는 모든 멤버들이 같은 보안레벨을 갖거나 부모보다 자손의 보안레벨이 항상 클 경우인데, 이 경우는 이전의 방법처럼 전달할 확률이 무조건 1이된다. 최상의 경우는 부모 노드의 멤버들이 자손 노드의 멤버들보다 항상 클 경우인데 이 경우는 메시지가 위로만 전달되고 아래로는 전달되지 않는다.

결국, 노드의 수 2^h-1 이 증가할수록 루트노드에 가까운 노드의 Emax가 증가할 가능성이 커지고 최대전달 확률은 1에 가까워진다. 그러나, 하단의 노드로 갈수록 전달할 확률은 점점 낮아진다. 그림3과 그림4에서는 최적화의 수행전과 수행후의 전달메시지 수와 전달 확률의 변화를 나타내었다. 가로축은 트리의 높이가 h에 해당하는 최하단의 노드이고 세로축은 최하단의 노드에 메시지가 전달되는 수를 가리킨다. 전달 메시지로는 1,000,000개를 $1/L_0$ 확률의 보안 등급을 갖도록 무작위로 생성하였다. [그림 3]과 [그림 4]는 트리의 깊이가 커질수록 전달 메시지



[그림 3] 트리 깊이에 따른 전달 메시지 수



[그림 4] 트리깊이에 따른 메시지 전달 확률

수가 감소하고 높이가 커질수록 전달확률이 증가하나 완전 전달 방식의 확률 1 보다 낮게 나옴을 보여준다.

좀 더 높은 효율을 얻기 위해서는 *Imax*가 큰 노드를 위쪽으로 보내고 낮은 노드들은 아래로 보내는 최적화가 수행될 필요가 있다. 최적화를 통해 자식 노드에서 루트노드까지의 완만한 *Emax* 값 상승을 유도할 수 있고, 메시지 송신 횟수를 줄일 수 있게 된다.

5.1.1 트리노드의 최적화

각 노드의 최대 보안 레벨에 따라 전달 여부를 결정하므로, 트리를 최대 효율이 되도록 하기 위해, 보안 레벨이 높은 노드를 상위로 보내고 낮은 노드들을 하위로 보내도록 트리를 재조정한다.

노드 정렬 시 고려해야 할 값은 한 노드의 최대 보안 레벨을 나타내는 *Imax* 이다. *Imax*에 따라 노드들을 순차적으로 배열하면 되므로 일반 정렬 알고리즘을 그대로 사용할 수 있다.

5.2 키 분배 및 키갱신 효율성 분석

어플리케이션 계층(layer)의 계층형(hierarchical) 암복호화는 서브넷 내의 멤버의 접근권한에 따라 다

른 암호키를 분배하는 방식이다. 또한 상위 권한을 갖는 키는 하위 권한을 갖는 키를 즉시 유도해낼 수 있으나 그 역은 계산상의 어려움을 갖는다. 이러한 계층형 암호키에 대한 연구는 꾸준히 진행되어 왔으나, 멀티캐스트의 동적환경에 따른 전방보호와 후방보호를 모두 만족시키지 못하고 있다. 따라서, 본 논문에서는 계층형 키생성은 해쉬함수를 재귀적으로 이용함으로써 경량화된 계층형 암호키를 생성하고, 접근권한 레벨에 따른 다수의 암호키를 효과적으로 갱신할 수 있는 방법을 제시하였다.

어플리케이션 계층에서의 계층키 분배 및 갱신에서 키갱신을 위한 준비단계 과정이 간단하며, 공개정보의 분배만으로 양쪽 엔티티에서 키분배 키를 계산하여 유도할 수 있다. 서브넷 내의 멤버가 탈퇴한 경우 키 갱신의 범위는 서브넷 내로 한정된다. 서브넷 내에서의 네트워크 대역폭은 충분하기 때문에 키 갱신 및 키교환에 소모되는 과부하는 상대적으로 매우 낮다. 또한 제안 방식은 네트워크 속도 보다 CPU 연산속도가 훨씬 빠름에 착안하여 통신횟수와 통신량을 줄이는 방향으로 설계하였고, 이를 위해 공개정보를 이용한 키유도 계산방식을 사용하였다.

또한 그룹키 비밀성, 전방보호, 후방보호를 제공하기 위해 계층키의 갱신이 필수적으로 요구되고 있고 동적인 환경에 적합하도록 가장 단순하고 빠른 해쉬 함수를 재귀적으로 사용하는 방법을 제안하였다. 해쉬 함수의 특성으로 인해 하나의 마스터 키로부터 유도된 키들은 일방향으로만 계산이 용이하고 반대방향으로의 키유도는 계산상 어렵다는 특징을 갖는다. 본 논문에서는 계층키의 생성 방법 보다 계층키를 효율적으로 분배하는 방법에 초점을 맞추었다.

5.3 고려사항에 따른 제안 방식 분석

1) 효율적인 멀티캐스트 접근통제 서비스 제공

5.1 절의 전송 효율성 분석을 통하여 완전전달 방식에 비하여 제안 방식이 네트워크 트래픽에 이득을 주며, Imax값에 기반한 노드의 최적화 수행시 더 좋은 네트워크 효율성을 보여준다.

2) 서비스 거부 공격에 대한 면역성 확보

제안 방식은 각각의 라우터에서 다중 레벨의 네트워크 접근통제 서비스를 제공함으로써 임의의 라우터에서도 불법접근 및 서비스 거부 공격에 대해 즉시 대처할 수 있다.

3) 키 분배·갱신의 효율성

다수의 계층키를 분배하거나 갱신시 키정보를 1:1로 연결하여 교환하지 않고 공개정보 t를 브로드캐스트함으로써 다수의 접속으로 인한 네트워크 연결 과부하를 줄일 수 있고 라우터와 호스트 각각에서 공유 비밀키를 생성하므로써 키분배를 위한 메시지 교환 단계를 줄였다.

4) 동적환경에서 그룹키 비밀성, 전방보호, 후방보호 만족

일방향 해쉬체인의 사용과 효율적인 키갱신 방식을 제시함으로써 그룹키의 비밀성, 전방보호, 후방보호를 제공하였다.

5) 메시지 전송의 효율성

제안 방식에서는 다수의 계층키에 관계없이 임의의 하나의 계층키로 메시지를 암호화하여 전송하고 수신자가 하위 계층키를 유도하여 메시지를 복호할 수 있게 함으로써 다중 레벨의 접근통제 서비스에 따른 다중 메시지 암호화 등의 비효율성을 최소화하였다.

Ⅵ. 결 론

본 논문에서는 멀티캐스트에서의 계층형 접근통제를 네트워크 계층과 어플리케이션 계층으로 나누어 제시하였다. 서브넷 내에 다수의 멤버가 존재하는 경우의 문제점과 계층형 접근통제를 어플리케이션 레벨의 계층형 암호키를 이용한 해결방안을 제시하였다.

제안방식에서는 지정된 라우터간의 데이터 전달은 네트워크 레벨의 접근통제를 수행하고, 동일한 세그먼트내에서의 멤버별 접근통제는 어플리케이션 계층의 암·복호화 기법을 사용하여 수행한다. 먼저 네트워크 레벨의 계층형 접근통제를 수행하기 위하여 접근과 거부 2가지의 접근요소에서 확장하여 다중 레벨의 보안성을 고려한 접근통제 기법을 제안하였다.

현재, 멀티캐스트상에서의 접근통제에 대한 전문적인 연구는 매우 미진한 상태이며, 향후 멀티캐스트 서비스의 활성화 및 활용범위 확대와 함께 활발한 연구가 진행되리라 예상된다.

참 고 문 헌

[1] Ballardie, "Core Based trees(CBT) Multicast

Routing Architecture", IETF RFC 2201, 1997.

[2] Ning Wang & George Pavlou, "Towards Dynamic Sender Access Control for Bi-directional Multicast Trees", GLOBECOM 2001.

[3] Thomas Hardjono, "Router-Assistance for Receiver Access Control in PIM-SM", Proceedings. ISCC 2000.

[4] A. Perrig, D. Song and J. D. Tygar, "ELK, a New Protocol for Efficient Large-Group Key Distribution, 2001 IEEE Symposium on Security and Privacy, 2001.

[5] Feng-ho Kuo, Victor R. L. Shen and F. Lai, "Cryptographic key assignment scheme for dynamic access control in a user hierarchy," IEE Proceedings-E: Computers and Digital Techniques, 1999.

[6] Selim G. Akl and Peter D. Taylor. Cryptographic solution to a problem of access control in a hierarchy. ACM Transactions on Computer Systems, 239-248, August 1983.

[7] Ravinderpal S. Sandhu. Cryptographic implementation of a tree hierarchy for access control. Information Processing Letters, 27(2):95-98, 29 February 1988.

[8] G. C. Chick and S. E. Tavares. Flexible Access Control With Master Keys. In Advances in Cryptology Proceedings of CRYPTO'89, G. Brassard, Ed., pages 316-322. Springer-Verlag, 1990.

[9] MS Hwang, WP Yang, A New Dynamic Cryptographic Key Generation Scheme for a Hierarchy, 1994 IEEE Region 10's Ninth Annual International Conference, 1994.

[10] Min-Shiang Hwang. A Dynamic Key Generation Scheme for Access Control in a Hierarchy. Nordic Journal of Computing, 6(4):363-371, Winter 1999.

[11] F. H. Kuo, V. R. L. Shen, T. S. Chen and F.Lai, Cryptographic key assignment scheme for dynamic access control in a user hierarchy, IEE Proceedings. Computers&Digital Techniques, Vol. 146, No. 5, September 1999.

[12] Wong C. K., Gouda M., Lam S., "Secure Group Communications Using Key Graphs", IEEE/ACM Transactions on Networking. Vol. 8, No. 1, 2000.

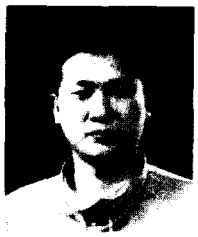
[13] Xukai Zou, Byrav Ramamurthy and Spyros Magliveras, Chinese Remainder Theorem based hierarchical access control for secure group communication. Appeared in ICICS 2001.

[14] J. C. Birget, X. Zou, G. Noubir, B. Ramamurthy, "Secure hierarchy-based access control in distributed environments", IEEE International Conference on Communications(ICC), 2002.

[15] Chang, C. C., Pan, Y. P., "Some Flaws in a Cryptographic Key Assignment Scheme for Dynamic Access Control in a User Hierarchy," Proceedings of the Second International Conference on Information Security (InfoSecu'02), July 2002.

〈著者紹介〉

신 동 명 (Dong-Myung Shin)
1997년 2월 : 대전대학교 컴퓨터 공학과 학사
2000년 2월 : 대전대학교 대학원 컴퓨터 공학과 석사
2000년~현재 : 대전대학교 대학원 컴퓨터 공학과 박사과정
2001년 7월~현재 : 한국정보보호진흥원 연구원
〈관심분야〉 컴퓨터·네트워크 보안, 보안 API, PKI, IPsec



박 희 운 (Hee-Un Park)
1997년 2월 : 순천향대학교 컴퓨터공학부 학사
1999년 2월 : 순천향대학교 전산학전공 석사
2002년 2월 : 순천향대학교 전산학전공 박사
2002년 1월~현재 : 한국정보보호진흥원 선임연구원
〈관심분야〉 암호이론, 컴퓨터 보안

최 용 락 (Yong-Rak Choi)
1982년~1986년 : 한국전자통신연구원 선임연구원
1986년~현재 : 대전대학교 컴퓨터공학부 교수
2000년~현재 : 대전대학교 공과대 학장
1997년~1999년 : 한국정보보호학회 충청지부 지부장
학회활동 : 한국통신정보보호학회, 한국정보과학회, 한국정보처리학회, 한국인터넷정보학회 종신회원
〈관심분야〉 컴퓨터통신보안