通信情報保護學會論文誌
第 10 券 第 2 號, 2000. 6

확장 멀티캐스트에서 다중레벨 보안에 관한 연구*

박 상 철**, 서 장 원**, 이 상 철**, 전 문 석***

A Study on the Multi-Level Security for Scalable Multicasting

Sang-Chul Park**, Jang-Won Suh**, Sang-Chul Lee**, Moon-Suk Jun***

요 약

멀티캐스트 응용들이 많아지면서, 보안 멀티캐스트 통신은 점차로 중요하게 되었다. 그러나 멀티캐스트는 대부분의 네트워크 보안 프로토콜들의 점대점 유니캐스트의 개념과는 많이 다르다. 기본적으로 안전한 멀티캐스트 통신은 안전한 유니캐스트 통신과 다르다. 멀티레벨 구조의 강제적 접근 제어는 주체에 대해 의미를 부여하여 접근을 통제하는 방식인 보안 레벨에 기초한 접근 제어 보안을 제안할 것이다. 본 논문에서, 유니캐스트와 멀티캐스트 보안의 차이점을 조사하고, 멀티캐스트 상에서 멀티레벨 보안을 제안할 것이다. 본문에서 제안하는 구조에 기반 하는 프로토콜은 보안 멀티캐스트 통신이나 그룹 키 관리 서비스를 제공 등 다양한 보안 목적들을 위해 쓰일 수 있고, 멀티레벨 보안을 통한 접근제어로 등급화 된 보안 서비스를 제공할 수 있다.

ABSTRACT

As multicast applications are increase in number, Secure multicast communications is becoming more important. However, multicast is much different from point-to-point unicast concept of most network security protocols. Basically, secure multicast communications and secure unicast communications are unlike.

Using Mandatory Access Control of multilevel architecture which assigns a meaning to each subject, so we accomplish access control. In this way, access control based on secure level is proposed. A protocol based on the architecture proposed in this paper would be utilized in secure multicast communications, group key management service and levled security sevice through multilevel security policy.

keyword : *Multicast, Scalability, Multilevel security, Security Level*

Ⅰ. 서 론

멀티미디어 원격 회의, 컴퓨터를 이용한 협동 작업, 원격 컨설팅및 진료와 같이 새로이 등장하는 응용들에게는 많은 참가자들 간의 효율적인 데이터의 교환이 매우 중요하다. 멀티캐스트(Multicast)[1,2]는 한 송신자에서 여러 수신자들에게 데이터를 전송하는 효율성을 제공한다. 멀티캐스트는 송신자 전송 오버헤드, 네트워크 대역폭 요구사항, 수신자들에게의 지연시간을 줄여준다.

이런 점들이 멀티캐스트가 큰 그룹 통신에서 이상적인 기술로 인정받게 만든다. 또, 멀티캐스트에 권한의 여러 층을 둔다면, 좀더 세분화된 보안을 제공할 수 있게 된다.

* 본 연구는 한국전자통신연구원 논문연구과제 지원에 의하여 수행된 연구 결과임
** 숭실대학교 컴퓨터학과 컴퓨터통신연구실
*** 숭실대학교 컴퓨터학과

멀티캐스트가 큰 그룹에서의 효율적이고, 최선을 다하는 데이터 전송 서비스를 제공하는데 매우 성공적이라고 볼 수 있지만, 멀티캐스트에 신뢰성, 흐름 제어, 그리고 혼잡 제어 등과 같은 부문에 확장성(Scalability)을 갖도록 하는 데에는 많은 어려움이 있다고 알려져 있다. 참고문헌[4]의 S. Mitrra 가 제안한 구조에서는 이러한 확장성의 문제를 서브 그룹으로 나눔으로 해서 해결하려는 시도를 보여주고 있으므로, 본 논문에서는 이러한 점에 기반하여 다중레벨 보안을 설명하려 한다.

또, 유니캐스트(Unicast)와 비교해, 멀티캐스트는 공격에 대해 더욱 많은 허점이 있다고 볼 수 있다. 유니캐스트에서는 상대가 누구인지 정도는 알고 있다고 가정 하에서 출발하지만 멀티캐스트에서는 상대가 누구라는 것조차도 모른다. 공격이 일어날 때, 멀티캐스트는 많은 수의 주체들이 영향받게 된다. 더욱이, 멀티캐스트는 일반적으로 광고되어지고 멀티캐스트 주소는 잘 알려져 있으므로 공격자는 이러한 목표를 공격하기에 쉽게 된다.

먼저 멀티캐스트 보안과 유니캐스트 보안 사이의 차이점에 대하여 살펴볼 것이다. 또, 어떻게 이러한 차이점들이 많은 응용(Applications)에서 확장의 문제를 일으키는지 본다.

그리고 S. Mitrra의 구조상에서의 다중레벨 보안을 지원하는 확장된 멀티캐스트(Multilevel Secure Scalability Multicast)를 제안한다. 보안 분배 트리(Secure Distribution Tree)에 기반을 두고 강제적 접근(Mandatory Access)을 첨가한 확장 보안 멀티캐스트(Scalable Secure Multicast)에 대한 형태이다.

II. 유니캐스트(Unicast)와 멀티캐스트 (Multicast) 보안의 차이점

네트워크 보안 프로토콜의 기본적인 역할은 불안전한 네트워크 상에서 공격자가 원문을 읽고, 수정하거나 지울 수 없도록 해서 인증된 주체가 안전하게 통신하도록 하는 것이다. 인증(Authentication)이란 사용자나 호스트 같은 실체를 인식하는 과정을 말하며, 보안 네트워크 시스템에는 매우 중요한 부분이다. 인증의 과정은 자주 키 분배(Key Distribution)와 결부되고, 두 가지 문제가 분리되기보다는 결합되어서 다뤄져야된다고 주장되기도 한다.[3] 보안 연관(Security Association)은 인증된 주체들간에 의해서만 공유되는 키의 집합을 정의한다. 그러고 나면 인증(Authentication), 기밀성(Confidentiality), 무결성(Integrity)과 같은 다양한 보안 목적을 위해 쓰일 수 있다. 유니캐스트에서의 보안 연관의 개념은 쉽게 이해되는 반면에, 다대다(Multipoint-to-Multipoint) 멀티캐스트 모델에서는 본래부터 보안 연관의 의미가 변화된다.

유니캐스트의 경우를 살펴보자. 두 주체가 통신하기를 결정하고 유니캐스트 네트웍 보안 프로토콜로 하여금 그들 사이의 보안 연관을 설정하도록 한다. 이 연관이 쌍으로 하여금 안전하게 통신하도록 한다. 여기에서 보안 연관은 완전히 정적(Static)이다. 보안 연관은 두 주체가 통신을 시작 할 때 시작하고 그들이 그들의 통신을 끝낼 때 소멸된다.

멀티캐스트에서도 비슷한 일들이 일어난다. 그러나 두 주체가 쌍을 이루는 것이 아니라, 임의 수의 주체들이 한 그룹을 형성한다. 그리고 유니캐스트 경우의 보안 연관이 정적인 반면에, 멀티캐스트 경우에서는 그룹의 멤버쉽이 변하기 때문에 보안 연관도 반드시 동적(Dynamic)이어야 한다.

멀티캐스트 보안 프로토콜은 반드시 한 주체가 매 동적인 시기마다 인증되어 있음을 확인해야만 한다. 실제적인 멀티캐스트 동작에 맞춰보면, 이 시기간의 구분은 멤버들이 조인(Join)하고 떠나(Leave)는 것에 대응된다. 그래서 보안 연관과 키는 반드시 각 조인과 떠남마다 변화되어야 한다. 이러한 변화로 새로이 조인한 주체는 이전 멀티캐스트 데이터에 접근 할 수 없고 떠난 주체는 그룹을 떠난 후에도 계속해서 멀티캐스트 데이터를 접근 할 수 없게 된다.

매 조인과 떠남마다 키가 변해야한다는 것이 반드시 필요하다는 것은 아니다. 이는 응용에 달려 있다. 그러나 멀티캐스트 보안 프로토콜은 반드시 각 조인이나 떠남이 있을 때마다 현재 그룹의 무결성(Integrity)을 보호하기 위해서 키를 바꿀 수 있는 준비를 하고 있어야만 한다.

일반적으로, 주어진 네트웍 보안 프로토콜의 설계는 많은 요소들을 감안해야만 하는 매우 복잡한 일이다. 그러나, 동적 보안 연관과 이의 키를 관리하는 것은 유니캐스트와 멀티캐스트 보안 프로토콜간에 기본적 다르다. 즉, 유니캐스트와 멀티캐스트 보안의 기본적인 차이점은 동적 보안 연관(Dynamic Secutiry Association)과 이의 키(Key) 관련 문제이다.

Ⅲ. 다중레벨 보안(Multilevel Secutiry)-강제적 접근 통제(Mandatory Access Control)

강제적 접근 통제(Mandatory Access Control)는 주체 및 객체의 보안 레벨(Security Level)에 근거하여 주체의 객체에 대한 접근을 제어하는 방법이다. 주체 및 객체의 중요도에 따라 보안 레벨을 설정하고, 주체가 객체에 접근하고자 할 때, 주체 및 객체의 보안 레벨에 따라 접근 통제를 한다.

3.1 주체 및 객체

먼저 멀티캐스팅 환경에서의 합당한 나름대로의 주체 및 객체에 대한 정의가 되어야 한다. 다중레벨 보안에서의 주체는 전송되는 데이터를 매체(Media)를 통해 받는 응용이며, 객체는 이의 접근을 받게 되는 통신상의 데이터이다.

3.2 보안 레벨(Security Level)

보안 레벨은 주체 및 객체의 중요도를 나타내는 정보로써 여러 형태가 가능하다. 일반적인 보안레벨의 형태는 1급, 2급, 3급과 같은 계층(Hierarchical) 구조를 가지는 보안등급(Security Level)과 "정부기관", "연구기관"등과 같이 데이터의 취급 분야별로 나누는 보안범주(Security Category)로 구성되어 있다. 본문에서는 일반적인 보안등급을 통한 계층적 접근을 다룬다.

보안 레벨의 비교를 통해 접근통제(Access Control)를 하게 되는데 일반적으로 다음과 같이 표현된다.

$SL(o) \leq SL(s)$ 이면,

"주체의 보안 레벨 SL(s)는 객체의 보안 레벨 SL(o)을 지배한다."라고 한다. 그리고 접근 통제 규칙은 "주체의 보안 레벨이 객체의 보안 레벨을 지배할 때 접근 가능하다."를 적용하게 된다.

보안 레벨은 강제적 접근 통제의 근거가 되는 정보로써, 인가된 관리자에 의해 설정 및 변경이 되어야 하며, 이는 멀티캐스트에서 멤버가 조인하는 서버에 접근 통제 리스트(Access Control List)를 갖는 데이터베이스의 구축 책임이 있다.

Ⅳ. 다중레벨 보안을 지원하는 확장 멀티캐스트 (Multilevel Secure Scalable Multicast)

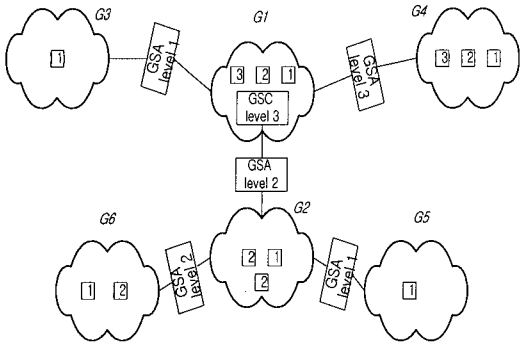
보안 레벨은 암호 키(Encryption Key)로 할당된다. 멤버는 자기 보다 높은 레벨의 키는 접근할 수 없다. 그러나 자기보다 낮은 레벨의 키에는 접근 할 수 있다. 그래서 한 멤버는 자기와 같거나 낮은 레벨의 키들을 갖고 있어야 한다.

다중레벨 보안에서 낮은 레벨의 정보는 높은 레벨 그룹 멤버들이 접근 할 수 있도록 해야 한다. 이렇게 하는 방법으로는 낮은 레벨 그룹 멤버들이 높은 레벨의 그룹에게 멀티캐스트 메시지를 보낼 수 있어야 한다. 그러나 송신자는 높은 레벨의 암호화 키를 갖을 수 없기 때문에 낮은 레벨 키들이 높은 레벨 멤버들에게 사용가능 하도록 되어있어야 된다. 또 다른 방법으로는 게이트웨이를 두어서 들어오는 메시지를 낮은 레벨 암호키로 복호화한 후 높은 레벨 키로 재암호화 하고 메시지를 전달할 수도 있다. 또는 낮은 레벨 사용자가 높은 레벨 공용키를 사용해서 전송할 수도 있다. 그러나, 게이트웨이를 두어서 복호화 하고 재암호화 하는 과정의 단점은 다음과 같다.

1) 게이트웨이로 하여금 같은 데이터의 전송을 레벨의 수만큼 반복하게 한다.
2) 게이트웨이를 거칠 때마다 시간이 소모되는 복호화와 암호화의 과정을 거쳐야만 하는 단점이 있다. 그리고 유연성이 부족하다. 왜냐면, 게이트웨이는 같은 레벨의 사용자들의 집합을 묶고 있어야 하는데 사실상 보안 레벨은 유동적이기 때문이다. 본문에서는 높은 레벨의 멤버가 낮은 레벨의 키를 접근 가능하도록 하는 방법에 대하여 논하겠다. 이 방법에서는 낮은 레벨의 정보는 그 레벨과 같거나 높은 수준의 멤버에게 디폴트로 공개된다는 특징이 있다.

확장성을 보장하기 위해서는 서브그룹(Subgroup)을 사용한다. 보안 분배 트리는 하나의 가상적 보안 멀티캐스트 그룹(Virtual Secure Multicast Group)을 계층적으로 하기 위해 많은 작은 보안 멀티캐스트 서브그룹들로 구성된다.[4](그림 1 참조)

확장성은 각 서브그룹이 상대적 독립을 유지될 때 얻을 수 있다. 보안 분배 트리 안의 각 서브그룹은 자신만의 주소로 자신만의 멀티캐스트 그룹을 갖는다.



〔그림 1〕 다중레벨 보안을 지원하는 확장 멀티캐스트의 예

또, 각 그룹은 자신의 서브그룹 키 K_{SGR}를 갖는데 전역적인 K_{GRP}는 갖지 않는다. 그래서, 한 멤버가 조인하거나 떠날 때, 단지 로컬 서브그룹에만 조인하거나 떠나는 것이 된다. 결과적으로, 오직 로컬 K_{SGR}만 바뀔 필요가 있게 되어 확장의 문제는 줄어들게 된다.

그룹 보안 제어기는 상위레벨 서브그룹을 관리하고, 서브 그룹마다 있는 GSA(Group Security Agent)들은 각 서브그룹들을 관리한다. GSC(Group Security Controller)는 보안 분배 트리(Secure Distribution Tree)의 루트에서 상위 레벨 서브그룹의 제어를 관리한다. GSC는 전체 그룹의 보안에 대한 책임을 맡는다. GSA는 GSC나 그들의 부모 GSA의 프락시 역할을 하도록 인증된 신뢰할 수 있는 서버이고 로컬 서브그룹(Local Subgroup)의 제어를 담당한다. GSA는 보안 분배 트리에서의 레벨에 따라 그룹화 되어져 있다. 특정 레벨에서의 GSA는 바로 위 레벨이나 GSC의 서브그룹에 있는 GSA의 서브그룹에 조인한다. 이때 하위 GSA는 상위에 있는 GSC나 GSA보다 높은 보안 레벨을 갖을 수 없다.

멤버는 자신의 레벨 키를 갖고 있어야 하며, 또 자신보다 낮은 레벨의 키들도 갖고 있어서 전송 데이터에 대한 접근을 허용 받을 수 있어야 한다.

이제 한 단계씩 제안된 구조의 동작을 살펴보자.

4.1 Join

보안 멀티캐스트 그룹에 조인하기 위해, 송신자나 수신자는 지정 GSA의 위치를 알아내고 JOIN 요청을 보안 유니캐스트 채널을 통해서 보낸다. 여기에서 보안 유니캐스트 채널이란 상호 인증을 제공하는 유니캐스트 보안 프로토콜중의 어떤 것이라도 좋다.

HD	{KSGR1'}KSGR1	{KSGR2'}KSGR2

〔그림 2〕 그림 1의 G2에서 보안레벨 2인 멤버의 조인으로 인한 GRP_KEY_UPDATE의 예

JOIN 요구를 받은 GSA는 데이터베이스를 조사해서 이 요구를 허용할 것인지 거부할 것인지를 결정한다. 요구가 허용된다면 (1) 새로운 멤버와만 공유되는 K_{GSA-MB}을 생성하고 (2) 개별적인 데이터베이스안에 새로운 멤버에 관련되는 다른 연관 정보를 이 키와 함께 저장하고 난 다음 (3) K_{GSA-M3}을 안전한 채널을 통해 새 멤버에게 전해 준다.

2장에서 기술한 바와 같이, GSA는 K_{SGR}를 바꾸고 K_{SGR}'를 현재의 멤버들과 조인한 멤버에게 알려야 한다. 이를 위해, GSA는 K_{SGR}로 암호화된 K_{SGR}'를 현재의 멀티캐스트 서브그룹에게 GRP_KEY_UPDATE 안에 포함해 멀티캐스트 한다. 이때 각 레벨마다 다른 키를 사용하므로, 레벨 2의 멤버가 조인했다면 그림 2와 같은 메시지가 멀티캐스트 되어 같거나 낮은 레벨의 키를 갱신하게 된다(그림 2 참조). 그런 다음 K_{SGR}'를 다른 유니캐스트 보안 채널(Unicast Secure Channel)을 통해서 조인한 멤버에게 전해준다.

GSA는 ACL(Access Control List)이나 JOIN을 처리하는데 사용되는 다른 데이터베이스를 제공받는다.

```
i=1
WHILE i <= NEW_MEMBER'S_LEVEL
  ADD {KSGRi'}KSGRi TO PACKET
```

4.2 Leave

떠남은 두 가지 조건에서 일어난다: (1) 멤버가 자율적으로 서브그룹을 떠나려고 LEAVE 요구를 GSA에게 보내거나 (2) GSA가 멤버를 서브그룹에서 쫓아내려고 멤버에게 통보를 하는 경우가 있다. 어느 경우든, K_{SGR}는 변경되어서 떠나는 멤버의 참여를 더 이상 허용하지 않도록 해야 한다. 또, 떠난 멤버가 갖고 있는 키들 모두를 바꿔야 하므로, GSA는 떠나는 멤버의 레벨이하의 키들을 생성해야만 한다.

K_{SGR}'의 복사본을 각 멤버에게 그 멤버의 K_{GSA-MB}로 암호화해서 보내는 방법이 있다. GSA는 하나의 메시지 안에 K_{SGR}'의 복사본을 각각 다른 멤버의

HD	{KSGR1'}KGSA-MB1	{KSGR1'}KGSA-MB2	{KSGR2'}KGSA-MB2

(그림 3) 그림 1의 G2에서 보안레벨 2인 멤버가 떠났을 경우 GRP_KEY_UPDATE의 예

K_{GSA-MB}로 암호화한다. 여기에서 K_{SGR}'는 해당 멤버 레벨이하의 키들을 포함한다(그림 3 참조). 이렇게 하면 하나의 메시지에 모든 멤버의 키를 보낼 수 있게 된다.

그룹 키를 분배하는 방법은 많은 연구의 대상 이였다. 예로, Diffie-Hellman 그룹 확장 키 교환,[5] 중국인 나머지 정리[6]나 polynomial interpolation[7]에 기초하는 보안 잠금 등이 여러 문헌에 기술된다.

본문에서는 암호화와 복호화를 사용한 키 분배를 사용하는데, 이는 위의 여러 방법들과 비교해 성능이 떨어지지 않는다. 왜냐면 위의 방법들은 O(n)의 계산을 요하는 방법들이기 때문이다. 또 하나의 메시지를 이용함으로써 네트워크 상에서의 부하도 덜 차지하게 된다.

```
i=1
WHILE I <=NUM_OF_MEMBERS
 FOR(j=1; j<=MEMBER_i's_LEVEL; j++)
 ADD { K_SGRj' } K_GSA-MBi TO PACKET
```

Join과 Leave 시에 인증정보를 포함하지 않았는데, 이는 실제적인 키의 분배의 경우를 본 것이기 때문이다. 물론 GSA와 멤버와의 인증을 포함 할 수 있지만, 그렇게 하지 않는다고 해서 치명적인 데이터의 누출은 일어나지 않고 단지 데이터 수신자가 수신하지 못하는 경우만 발생하게 된다. 재생공격으로 멤버를 속인다고 한다면, 재생 공격자는 현재의 그룹키를 알고 있어야 하므로, 재생공격으로 인해서 데이터가 낮은 레벨로의 누출은 없게 된다. 또 멤버는 정상적인 데이터를 받을 수 없게 되어 즉각 키의 재분배를 요구하게 된다.

4.3 Join 과 Leave시의 키 분배에 관한 Scalability 고찰

어느 멤버의 참여와 떠남이 그 멤버가 속한 서브그룹에서만 키를 다시 분배하도록 하는 구조이다. 만약 서브그룹에 없다면 키의 재분배에 전체 멤버들이 관련되어야만 하게 된다. 이 경우를 살펴보자.

c_{sh} : 가장 먼 서브그룹까지의 hop 수.
c_{sn} : 전체 서브그룹의 수.
T_{KU} : 키가 업데이트되는데 걸리는 시간.
T_{RK} : 어느 멤버에서 GSA로 키 생성 요구 메시지의 전달 시간.
T_{GK} : GSA의 키 생성 시간.
T_{SK} : GSA가 서브그룹 내에 키 분배 메시지를 전달하는 시간.

하나의 전체 그룹인 경우,

$$T_{KU} = T_{RK} + T_{GK} + c_{sh} \cdot T_{SK}$$

서브그룹에 키의 분배가 제한되는 경우,

$$T_{KU} = T_{RK} + T_{GK} + T_{SK}$$

업데이트 시간에 있어서 서브그룹에 키의 분배가 제한되는 경우에는 (c_{sh}-1) T_{SK}만큼의 시간이 덜 걸리게 된다. 멀티캐스트 서브그룹들이 점점 늘어나는 추세를 기대하고 있다면 전체 그룹에 키 분배를 한다는 것은 Scalability 문제에 봉착하게 됨을 알 수 있다.

고려될 수 있는 또 다른 관점은 GSA의 부하이다. GSA가 서브그룹에 속하지 않은 멤버의 키 생성 요구에 의해서 키를 생성하게 되면 전체 GSA로는 (c_{sn}-1) T_{GK}만큼의 시간를 더 소모하게 된다.

4.4 Data Transmission

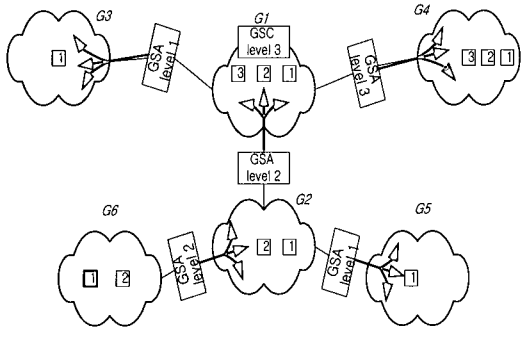
제안된 구조에서 멀티캐스트 전송은 단지 로컬 서브그룹(Local Subgroup)에만 도달하게 된다. 멀티캐스트의 계층구조가 고려되어서 전송을 받기 위해서는 전체적 보안 멀티캐스트(Entire Secure Multicast Group)그룹에 대한 어떠한 메카니즘이 있어야만 한다.

송신자가 직접 그룹에 멀티캐스팅하지 않고, 송신자는 GSA에게 K_{GSA-MB}로 암호화된 데이터를 유니캐스트한다. 그러면 GSA는 데이터를 복호화 하고 K_{SGR}로 재암호화 하고 서명한 다음 그의 부모 서브그룹뿐만 아니라 자신의 그룹에게 이를 멀티캐스트한다.

좀더 효율적인 방법으로는, 송신자가 데이터를 K_{SGR}로 직접적으로 암호화하지 않고, 송신자는 전송마다 임의 키 K_{RD}를 생성해서 이 키를 사용해 데이터를 암호화한다. 그리고 이 키를 K_{SGR}로 암호화하여 데이터에 포함시킨다.

HD	{DATA, SGSA}KRD1, {KRD1}KSGR1

〔그림 4〕 K_{RD}를 이용한 간접 암호화 패킷



〔그림 5〕 G6에서 레벨 1인 송신자의 멀티캐스트 전송

이러한 방법으로, 패킷의 복호화와 재암호화는 간단하게 임의 키 K_{RD}의 복호화와 재암호화로 줄어들게 된다. 수신자들은 이 메시지가 유효한 소스에서 왔는지를 확인하기 위해 GSA의 서명을 확인해야만 한다(그림 4 참조). 서명은 RAS나 MD5를 사용하여 DATA의 내용을 가지고 서명값을 얻을 수 있다. 서명은 DATA와 함께 암호화 키에 의해 기밀성을 보장받게 된다.

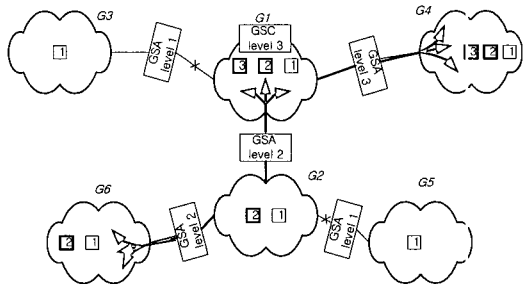
부모 GSA는 멀티캐스트 전송을 받아서, 이를 복호화 하고 그 서브그룹의 K_{SGR}로 암호화해서 다시 멀티캐스트 한다. 비슷한 방법으로 서브그룹의 자식 GSA는 멀티캐스트 전송을 받아서 복호화 하고 이들을 자식 서브그룹의 K_{SGR}로 암호화해서 자식 서브그룹에 다시 멀티캐스트 한다. 이 처리는 데이터가 재 멀티캐스트 되는 서브그룹에서도 반복할 것이므로, 그 데이터는 결국 모든 서브그룹에 도착하게 된다(그림 5 참조).

하지만 보안레벨이 높은 송신자가 보낸 데이터는 그 데이터의 보안레벨보다 낮은 레벨을 갖는 GSA와 멤버에게는 판독을 할 수 없게 된다. 그리고 같거나 높은 보안레벨의 GSA와 멤버는 판독할 수 있다(그림 6 참조).

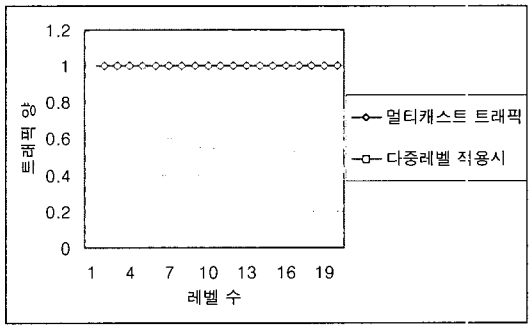
level 3 GSA의 처리 Traffic=level 1 Traffic + level 2 Traffic+ level 3 Traffic

level 2 GSA의 처리 Traffic=level 1 Traffic +level 2 Traffic.

level 1 GSA의 처리 Traffic=level 1 Traffic



〔그림 6〕 G2에서 레벨 2인 송신자의 멀티캐스트 전송



〔그림 7〕 다중레벨 적용 시 레벨 수에 따른 트래픽 양의 감소

위와 같이 되어, 데이터패킷이 자기보다 낮은 보안 레벨의 GSA는 통과하지 못하게 되므로, GSA는 패킷을 필터링하여 보안 레벨에 맞게 전체 네트워크의 부하를 줄이는 역할까지 담당하고 있다.

$$TotalTraffic = \frac{1}{n}\sum_{i=1}^{n}\frac{i}{n} = \frac{1}{n^2}\sum_{i=1}^{n} i$$
$$= \frac{n+1}{2n}$$

여기에서 n은 레벨의 수를 의미한다. 데이터 전송의 레벨, 보안레벨의 분포가 균등하고 같은 레벨의 네트워크 규모가 비슷하다는 가정 하에서, 위와 같은 결과를 얻었다.

4.5 Join 과 Leave시의 키 분배에 역할을 담당하는 GSA의 문제점과 대책

GSA는 session leader 와 인증 서버의 기능을 모두 가졌다. 멤버가 등록이 되면 session leader는 키를 보관하게 된다. 등록하기 전에 GSA는 session 정책을 검사하여 session을 열 것 인가를 결정한다. 새로운 멤버가 세션에 받아들여지면, 그 멤버는

GSA로부터 그룹키를 받는다. GSA를 그룹 리더로 볼 수 있다. 시스템의 안전도가 GSA에 의존하여, 공격의 대상이 되거나 내부 범죄에 취약하여 만일의 사태시 피해가 올 수 있다. GSA가 다운 된다면 다른 서버가 동작할 수 있도록 예비 프로토콜이 정의되어야 할 것이다. GSA 백업 서버를 두어서 신뢰성을 높일 수 있다. GSA 백업 서버는 GSA 주 서버와 일정간격으로 신호를 주고 받으며 다운되었는지 상태를 점검할 수 있다.

GSA 주 서버가 만약 다운 된다면, 백업 서버는 자신이 주 서버의 IP 주소를 인계 받고 ARP 테이블의 내용을 새로이 갱신해서 주 서버의 역할을 이어나갈 수 있다.

4.6 내부 공격자에 대한 대응책

멤버 중에 악의를 가진 자가 있을 수 있다. 모든 멤버는 그룹키를 가지고 있으므로 이의 오용을 차단할 수 있는 메카니즘이 포함되어야 한다. 특히, 재생 공격과 위장 공격에 주의하여야 한다. 왜냐면 이 두 공격은 멀티캐스트에서 키를 알고 있으면 쉽게 시도 될 수 있기 때문이다.

1) 위장 공격에 대해 살펴 보면, 그룹키 만으로는 메시지의 발신처를 알아내지 못한다. 그래서 이 문제는 각 멤버가 그의 메시지에 디지털 서명 기술을 사용해 서명이 요구되도록 해서 해결할 수 있다. 물론 디지털 서명 기술을 포함하기 위해선 이미 서로의 공개키를 가지고 있다고 보는데, 여기에 PKI를 사용한다고 가정한다. 인증서버는 모두의 공개키를 보관하고 있고 필요한 호스트에게 상대의 공개키를 제공한다고 가정한다.
2) 멀티캐스트에서는 참여한 어느 멤버든지 간에 송신자의 메시지를 받았다가 나중에 이를 똑같이 다시 전송할 수 있다. 수신자는 이전의 메시지들과 키들을 보관하고 있지 않는 한 이러한 재생을 탐지해 낼 수 없다. 만약 수신자가 이러한 기록을 유지하지 않는다고 한다면, 메시지의 freshness를 확보하는 것은 꼭 필요하다. 이를 위해 먼저 클럭이 안전하게 동기화 되었다고 가정하면, 가장 일반적인 방법으로는 메시지 m 에 타임스탬프 t를 붙이는 것이다.

여기에서 t는 메시지의 생성 시간을 가리킨다. 그래서, m 대신에 (m, t)로 대체하는 것이다. 또 다르게 freshness를 얻기 위한 방법으로는 challenge and response 방법이 쓰일 수 있다.

그 외 외부 공격자는 그룹 키를 모르기 때문에 트래픽의 양에 따라 추측하는 수동적인 공격만이 가능하다. 이마저도 차단하고자 한다면, GSA가 주기적으로 아무런 의미 없는 패킷을 전송함으로써 피할 수 있다.

V. 결 론

위에서 본 내용은 S. Mitrra가 제안한 구조의 멀티캐스트 확장성(Scalability)에 다중레벨 보안성(Multilevel Security)을 이루는 방법을 제시하고 있다. 여러 서브그룹들로 나누어서 각 서브그룹에게 멤버들의 키 관리를 위임하면서 전체적인 가상 멀티캐스트 망을 유지한다. 서브그룹에서 각 멤버의 인증 및 참여, 떠남, 데이터전송, 키 관리 등은 GSA가 맡아서 하도록 한다. GSA가 위임을 받아서 하는 만큼 위험성도 안게 되는데, 그 안정도에 따라서 GSA의 보안 레벨이 주어지도록 보안 정책을 세워야 한다. 높은 보안 레벨을 얻기 위해서는 얼마나 안전한 서버인가를 먼저 공인 받는 일련의 기준과 절차가 있어야 된다고 본다. 위협이 될 수 있는 보안 공격에 대한 대응책을 준비하는 일도 빠뜨려서는 안될 부분이다. 또 각 서브그룹과 멤버는 보안 레벨을 갖고 있어서 차별화 된 서비스를 제공할 수 있다.

참 고 문 헌

[1] T. Ballardie, P. Francis, and J. Crowcroft. Core Based Trees-An Architecture for Scalable Inter-Domain Multicast Routing. In Proceedings of ACM SIGCOMM '93, San Francisco, California, September 1993.

[2] S. Deering. *Host Extensions for IP Multicasting*, Request for Comments 1112, Internet Network Working Group, August 1989.

[3] M.Burrows, M. Abadi, and R.M. Needham. A Logic for Authentication. *ACM Transactions on Computer Systems*, February 1990.

[4] Suvo Mittra. Iolus: A Framework for Scalable Secure Multicasting. *ACM SIGCOMM*, September 1997.

[5] M. Steiner, G. Tsudik, and M. Waidner. Diff-Hellman Key Distribution Extended to Group Communication. In *Proceedings of the 3rd ACM Conference on Computer and Communications Secutiry*, New Delhi, March 1996.

[6] G.H. Chiou and W.T. Chen. Secure Broadcasting Using the Secure Lock. *IEEE Transactions on Software Engineering*, August 1989.

[7] L. Gong and N. Shacham. Multicast Security and its extension to a mobile environment. *ACM-Baltzer Journal of Wireless Networks*, 1(3):281-295, October 1995.

〈著者紹介〉

박 상 철 (Sang-chul Park) 학생회원
1999년 2월 : 단국대학교 전자계산학과 학사
1999년 3월~현재 : 숭실대학교 대학원, 컴퓨터학과 석사과정
〈관심분야〉 네트워크 보안, 정보보호, 시뮬레이션

서 장 원 (Jang-won Suh)
1992년 2월 : 서울산업대학교 전산과 학사
1996년 2월 : 숭실대학교 대학원 전산과 석사
2000년 6월 : 숭실대학교 대학원 컴퓨터학과 박사
〈관심분야〉 암호학, 네트워크 이론, 전자지불 시스템

이 상 철 (Sang-chul Lee)
1998년 8월 : 숭실대학교 전자계산학과 학사
1999년 9월~현재 : 숭실대학교 컴퓨터학과 석사과정
〈관심분야〉 PKI, 네트워크 보안, 정보보호

전 문 석 (Moon-seog Jun)
1980년 2월 : 숭실대학교 전자계산학과 학사
1986년 2월 : University of Marlyland, Computer Science 석사
1989년 2월 : University of Marlyland, Computer Science 박사
1989년 3월~현재 : 숭실대학교 컴퓨터학과 부교수
〈관심분야〉 정보 보안, 인터넷 보안, 침입 탐지, 방화벽, 암호화 알고리즘