다중레벨 보안을 지원하는 확장 멀티캐스트

박상철*, 김정규, 이상철, 전문석
숭실대학교 컴퓨터학과

Multilevel Secure Scalable Multicast

Sang-Chul Park*, Jung-Gyu Kim, Sang-Chul Lee, Moon-Suk Jun
Dept. of Computing, Soongsil University

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 제어벨 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.

1. 서 론

멀티미디어 원격 회의, 컴퓨터를 이용한 협동 작업, 원격 컨설팅 및 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 보안 서비스를 제공할 수 있게 된다

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

그리고 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.

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

네트워크 보안 프로토콜의 기본적인 역할은 인증된 주체가 안전하게 통신하도록 하는 것이다. 인증(Authentication)이란 사용자나 호스트 같은 실체를 인식하는 과정을 말한다 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

유니캐스트의 경우, 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 일어나지만, 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 접근할 수 없고 떠난 주체는 그룹을 떠난 후에도 계속해서 멀티캐스트 데이터를 접근 할 수 없게 된다.

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

강제적 접근 통제(Mandatory Access Control)는 주체 및

객체의 보안 레벨(Secutry 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 보안(Multilevel Security)에서의 주체는 전송되는 데이터를 매체(Media)를 통해 받는 응용이며, 객체는 이의 접근을 받게 되는 통신상의 데이터이다

3.2 보안 레벨(Security Level)

보안 레벨(Security Level)은 주체 및 객체의 중요도를 나타내는 정보로써 여러 형태가 가능하다 일반적인 보안레벨의 형태는 1급, 2급, 3급과 같은 계층(Hierarchical)구조를 가지는 보안등급(Security Level)으로 구성되어 있다. 본문에서는 일반적인 보안등급을 통한 계층적 접근을 다룬다.

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

$SL(o) \leq SL(s)$ 이면,

"주체의 보안 레벨 SL(s)는 객체의 보안 레벨 SL(o)을 지배한다."라고 한다. 그리고 접근 통제 규칙은 "주체의 보안 레벨이 객체이 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

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

보안 레벨(Security Level)은 암호 키(Encryption Key)로 할당된다. 멤버는 자기 보다 높은 레벨의 키는 접근할 수 없으나 자기보다 낮은 레벨의 키에는 접근 할 수 있어야 하므로, 자기와 같거나 낮은 레벨의 키들을 갖고 있어야 한다.

다중레벨 보안(Multilevel Security)에서 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 암호화키를 갖을 수 없기 때문에 낮은 레벨 키들이 높은 레벨 멤버들에게 사용가능 하도록 되어있어야 된다.

확장(Scalability)을 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).

그룹은 자신의 서브그룹 키 K_{SGR}를 갖는다. 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.

GSC(Group Security Controller)는 상위레벨 서브그룹을 관리하고, 서브 그룹마다 있는 GSA(Group Security Agent)들은 각 서브그룹을 관리한다. GSC(Group Security Controller)는 보안 분배 트리(Secure Distribution Tree)의 루트에서 상위레벨 서브그룹의 제어를 관리한다. GSC는 전체 그룹의 보안에 대한 책임을 맡는다 GSA는 GSC나 그의 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 접근을 허용 받을 수 있어야 한다

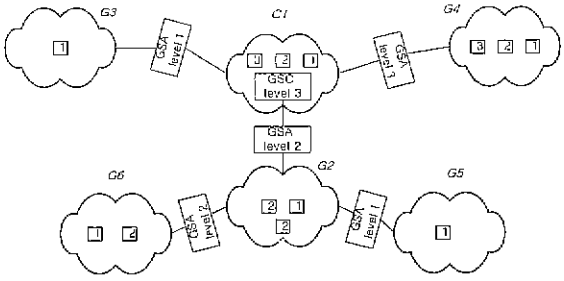

그림 1 다중레벨 보안을 지원하는 확장 멀티캐스트의 예

이제 한 단계씩 제안된 구조의 동작을 살펴보자.

4.1 Joining

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.

JOIN 요구를 받은 GSA는 데이터베이스를 조사해서 이 요구를 허용할 것인지 거부할 것인지를 결정한다. 요구가 허용된다면 (1) 새로운 멤버와만 공유되는 $K_{GSA\text{-}MB}$을 생성하고 (2) 개별적인 데이터베이스안에 새로운 멤버에 관련되는 다른 연관 정보를 이 키와 함께 저장하고 난 다음 (3) $K_{GSA\text{-}MB}$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 암화화된 K_{SGR}'를 현재의 멀티캐스트 서브그룹에게 GRP_KEY_UPDATE안에 포함해 멀티캐스트 한다. 이때 각 레벨마다 다른 키를 사용하므로, 레벨 2의 멤버가 조인했다면 그림 2와 같은 메시지가 멀티캐스트되어 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.

HD	{KSGR1'}KSGR1	{KSGR2'}KSGR2

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

4.2 Leaving

떠남은 멤버가 자율적으로 서브그룹을 떠나려고 LEAVE 요구를 GSA에게 보내거나 GSA가 멤버를 서브그룹에서 쫓

아내려고 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 보낸다. GSA는 하나의 메시지 안에 K_{SGR}'의 복사본을 각각 다른 멤버의 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, 중국인 나머지 정리나 polynomial interpolation에 기초하는 보안 잠금 등이 여러 문헌에 기술된다.

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

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

4.3 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 사인한 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. 이러한 방법으로, 패킷의 복호화와 재암호화는 간단하게 임의 키 K_{RD}의 복호화와 재암호화로 줄어들게 된다. 수신자들은 이 메시지가 유효한 소스에서 왔는지를 확인하기 위해 GSA의 사인을 확인해야만 한다(그림 4 참조)

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

그림 4 K_{RD}를 이용한 간접 암호화 패킷

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 암호화 해서 자식 서브그룹에 다시 멀티캐스트 한다. 이 처리는 데이터가 재 멀티캐스트 되는 서브그룹에서도 반복할 것이므로, 그 데이터는 결국 모든 서브그룹에 도착하게 된다(그림 5 참조)

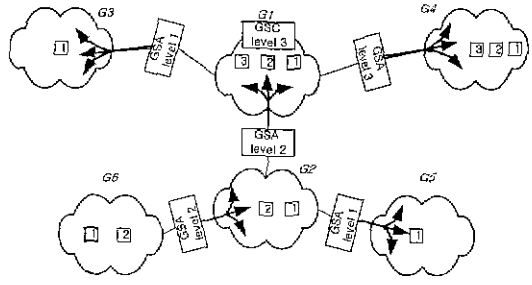

그림 5 G6에서 레벨 1인 송신자의 멀티캐스트 전송

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

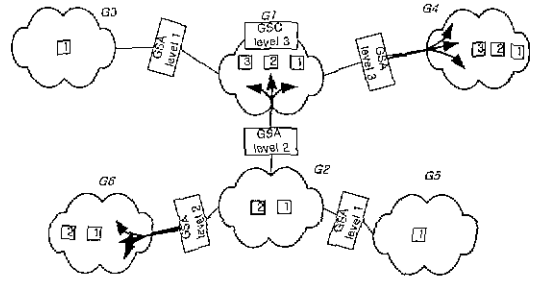

그림 6 G2에서 레벨 2인 송신자의 멀티캐스트 전송

5. 결론

위에서 본 내용은 멀티캐스트 보안의 확장(Scalability)과 다중레벨 보안(Multilevel Secutiry)을 동시에 이루는 방법을 제시하고 있다. 이러 서브그룹들로 나누어서 각 서브그룹에게 멤버들의 키 관리를 위임하면서 전체적인 가상 멀티캐스트 망을 유지한다 또 각 그룹과 멤버는 보안 레벨을 갖고 있어서 차별화 된 서비스를 제공할 수 있다. 또 이 구조는 유연한 관리 환경에 알맞다 사용자의 입장에서는 로컬 GSA를 알고 있으면 전체 그룹에 참여 할 수 있기 때문이다.

참고문헌

[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.