PIM-SM을 기반으로한 멀티캐스트 보안 구조

정영목*, 노종혁*, 황교철**, 이균하*
*인하대학교 전자계산공학과
**수원여자대학 컴퓨터응용학부
e-mail:g1991280@inhavision.inha.ac.kr

Multicast Secure Architecture based on PIM-SM

Young-Mok Jung*, Jong-Huk Roh*, Kyo-Cheul Hwang**, Kyoon-Ha Lee*
*Dept. of Computer Science & Engineering, Inha University
**Division of Computer Application, Suwon Women's College

요약

기존의 멀티캐스트 보안 프로토콜은 DVMRP, CBT와 같이 비교적 규모가 큰 라우팅 프로토콜에 적합하도록 설계되어 있어서 사용자가 비교적 적고, 호스트들간의 지역적인 거리가 멀고, 최단경로 라우팅 특성을 가지는 PIM-SM(Protocol Independent Multicast-Sparse Mode)라우팅 프로토콜을 지원하는데 무리가 있다. 본 논문에서는 모든 사용자간의 가입/탈퇴시 또는 서비스 사용 중에 사용자의 정당한 서비스 보호를 위해 서브그룹을 *RP* 단위로 나누고, 송신자만의 비밀키를 따로 관리하는 보안 구조를 설계하였다. 그 결과 데이터 전송시 그룹키에 의한 데이터 변환 작업이 불필요하여 키 분배시간이 단축되고, 다른 보안 구조에 비해 구조가 보다 간단해졌다.

1. 서론

초기의 인터넷 환경은 유니캐스트를 이용한 데이터 전송이 주로 사용하였으나, 인터넷의 발달과 함께 멀티미디어의 요구가 확대되어지자 실시간 서비스를 위한 사용자의 수요는 급증하고 있다. 이러한 네트워크 환경을 위해서 송신자로부터 다수의 수신자에게 데이터를 전송하는 멀티캐스트의 요구가 증가되어가고 있다[1]. 멀티캐스트는 효과적인 데이터 전송을 위해서 다른 여러 가지 특성들을 요구하는데, 즉 확장성, 흐름 제어, 혼잡 제어 등의 요구사항들로 인해서 멀티캐스트는 유니캐스트에 비해 실시간 서비스를 필요로 하는 사용자에게 더욱 많은 서비스를 효과적으로 전송 할 수 있게 한다. 또 다른 요구사항으로 멀티캐스트는 그룹 주소가 개방되고, 그 그룹이 매우 많은 지역적인 분포를 가지고 있어서 유니캐스트보다 많은 보안에 따른 약점들을 가지고 있어 멀티캐스트의 응용에 더욱 많은 장애가 되고 있다[2].

이러한 가운데 멀티캐스트 보안 프로토콜들이 점점 연구 발표되면서 멀티캐스트 그룹통신에서 서브그룹 단위로 그룹키 등을 분배하는 계층적인 보안구조들이 설계되었다. 이러한 보안 프로토콜은 기존의 유니캐스트에서 사용한 보안 프로토콜과는 다른 1:N 구조나 혹은 N:N 구조로 서브그룹단위로 그룹키를 관리함으로써 사용자의 가입/탈퇴에 따른 키 재분배를 한다[7].

현재 발표된 보안 구조들은 CBT, DVMRP, MOSPF[6]과 같은 많은 사용자가 지역적으로 근접한 곳에 조밀하게 분포되어져 있는 멀티캐스트를 위해 만들어졌다[1]. 그러나 적은 수의 사용자를 가지고있는 Small Group Multicast에 적합한 PIM-SM (Protocol Independent Multicast Sparse Mode)라우팅 알고리즘[5,10]은 적은 사용자들이 지역적으로 분산된 가운데 유니캐스트와 멀티캐스트가 혼용된 멀티캐스트 라우팅 알고리즘으로, 이에 적합한 보안프로토콜은 없는 실정이다.

본 논문에서 제안하는 방법은 키 관리자가 송신자 등록에 있어 송신자에게 송신자 고유의 비밀키를 부여하고 인증된 수신자에게 송신자의 비밀키를 전한다. 그리하여 송신자가 데이터를 보낼 때 자신만의 비밀키로 암호화한 후 RP(Rendezvous-Point)를 거쳐 각 수신자에게 전송하여 수신자에게 전송하여 수신자는 미리 받은 송신자의 비밀키로 데이터를 복호화할 수 있다. 즉 다른 보안구조와 같은 키 변환작업이 필요 없게 된다. RP와 키 관리자를 동일한 위치에 둠으로써 보안구조를 간단히 하였고 PIM-SM 멀티캐스트 그룹통신에서의 사용자의 서비스보호를 위한 보안 구조를 제안하였다. 그 결과 PIM-SM 라우팅 알고리즘의 변형 없이 그대로 사용하여 다른 보안 프로토콜에 비해 보다 간단해진 구조가 되었고, 송신자의 경로가 변하더라도 이미 비밀키를 가지고 있으므로 복호화가 가능하며, 중간 라우터 내에서 그룹키에 의한 데이터 변환이 필요가 없어 전송시간이 단축되었다.

2. 멀티캐스트 보안구조

멀티캐스트에서 요구되는 정보보호는 타 분야의 정보보호에 비하여 다소 독특한 면을 제시하고 있다. 멀티캐스트는 화상회의 등 실시간 응용소프트웨어에서 주로 사용되므로 정보보호 기능이 실시간이라는 개념을 해칠 수 있는 오버헤드가 없어야 된다. 또한 많은 수의 사용자들이 메시지를 암호화/복호화하기 위하여 항상 한 개의 비밀키를 공유해야한다는 점이 있다[7].

그룹 내에서 공유되고 있는 비밀키는 새로운 사용자들이 그룹

에 참가(Join Operation)하고 또한 기존의 사용자가 그룹을 벗어남(Leave Operation)에 따라 계속 새로운 그룹키로 변경되어야 하는데 이는 다음과 같은 Backward Secrecy 와 Forward Secrecy를 만족시키기 위함이다[7].

- 멀티캐스트 그룹을 떠나는 사용자가 그룹을 떠난 이후에는 메시지를 복호화 할 수 없어야 한다.
- 멀티캐스트 그룹에 새로 가입한 사용자는 가입하기 이전의 메시지를 복호화 할 수 없어야 한다.

이러한 조건을 만족시킬 수 있는 방법은 매 가입 또는 그룹을 벗어날 때마다 현재 사용되고 있는 그룹 키를 새로운 그룹 키로 대체하는 방법이다(Rekey Operation).

또한 멀티캐스트 보안구조를 설계하는데 다음과 같은 중요한 조건들이 제시 되고있다.

- 시스템 구조(System Architecture): 단일 호스트의 장애가 발생할 때 전체 네트워크의 미치는 영향을 고려해야 한다.
- 확장성(Scalability): 지역적으로 넓고, 분산된 그룹에 대한 관리, 또한 빈번한 가입/탈퇴에 대한 관리를 제공해야 한다.
- 키 관리자의 성능(Processing Time for Key management): 그룹의 멤버가 가입/탈퇴시 새로운 키의 생성과 키 재분배를 위한 키 관리자의 성능과 암호화 알고리즘이 중요하다.
- 그룹 키의 수(Number of Keys with Controller and Member): 멀티캐스트 그룹을 관리하기 위해서 키 관리자와 그룹의 사용자들은 일정한 수의 키를 가지고 있어야 한다. 적은 수의 키를 가지고 그룹전체를 관리하는 것이 중요하다.

여러 가지 멀티캐스트 보안 구조와 프로토콜들이 이러한 조건을 만족시키기 하기 위하여 제안되었다. 대표적으로 Iolus[2]와 Nortel network[3,4]에서 제안한 구조가 있다. Iolus는 계층적 방법의 일종으로 멀티캐스트 어플리케이션에서 secure multicast를 위한 독립적인 그룹 키 관리 서비스와 안전 모듈(secure module)로서 유용하다.

Iolus는 여러 계층구조로 구성될 수가 있는데 중간계층은 상부 및 하부의 비밀키를 알고 있으며 이를 이용하여 계층간의 통신 메시지를 복호화한 후 다시 상대 계층의 비밀키로 암호화하여 전송하는 방법이다. 이는 각 단계별 복호화/암호화하는 과정이 반복되는 관계로 시간이 많이 소요된다[2].

그림1은 Iolus 보안 분산 트리(Secure Distribution Tree)의 예를 보여준다.

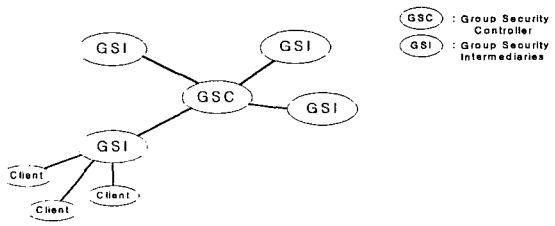

그림 1. Iolus 분산된 보안구조

Nortel 네트워크에서 제안한 Intra-Domain GKMP (Group Key Management Protocal) 구조는 분산 구조로서 키 관리를 위해 상/하 두 개의 레벨로 구성된다. 가장 높은 레벨은 트렁크 지역으로 그것은 많은 서브그룹들에 의해서 구분되어 진다[3,4]. 그림2는 Notel에서 제안된 구조이다.

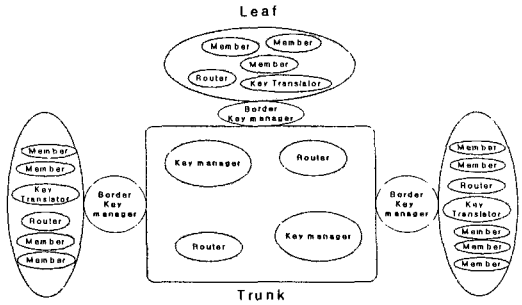

그림 2. Nortel 제안된 보안구조

이러한 분산되어진 구조는 여러 가지의 멀티캐스트의 라우팅에 대해서 독립적으로 설계되어져 있으나 데이터가 항상 특정 서브그룹에서 생성되어 트렁크를 거쳐 수신자에게 전달되어지는 고정된 라우팅 프로토콜에 적합한 구조이다. 그리하여 능동적인 라우팅 프로토콜을 지원하는 보안 구조가 필요로 하게 되는 것이다.

3. PIM-SM 보안 구조

3.1 PIM-SM 라우팅 알고리즘

PIM은 특정한 유니캐스트 라우팅 프로토콜에서 제공되는 방식과 무관하게 멀티캐스팅을 지원한다. PIM은 특정한 라우팅 테이블의 계산을 필요로 하지 않기 때문에 DVMRP보다 단순하다. 다만 유니캐스트 라우팅이 존재한다는 것만 가정하고, PIM 라우터가 멀티캐스팅을 위한 경로를 계산하지 않는다.

PIM 라우팅 알고리즘에는 두 가지 모드가 있다. 그 중에 Dense-mode는 대역폭이 충분하고 그룹 멤버들이 밀집되어 있는 환경에서 작동되는 프로토콜을 말하고, Sparse-mode는 대역폭이 충분하지 않은 환경에서 인터넷상의 여러 지역에 걸쳐서 그룹의 멤버들이 존재하는 경우를 일컫는다[5,10].

PIM-SM 라우팅 알고리즘의 수신자는 하나 이상의 RP를 가지고, 송신자와 RP사이의 공유트리를 두어 라우팅 경로를 공유함으로써 네트워크의 부하를 감소시킨다. 각 RP의 정보와 멀티캐스트의 그룹에 대한 정보를 항시 가지고 있어야 하는 DR(Designated-Router)은 송신자로부터의 멀티캐스트 그룹에 속한 첫 번째 라우터로서 RP에 대한 정보를 가지고 송신자의 Register에 대한 정보를 RP에게 송신한다. 여기서 DR은 자신이 속해져 있는 그룹내의 모든 RP의 정보를 BOOTSTRAP 프로토콜로서 정보를 수집한다. 그리하여 자신에 속해져 있는 호스트로부터 그룹의 가입을 나타내는 IGMP를 수신시 어떤 RP로 송신해야 할지 미리 알고 있어야 한다.

또한 PIM-SM은 라우팅 경로에 있어서 Shortest Path Tree또한 사용한다. 이는 원하는 질의 서비스를 얻지를 못할 때는 수신자는 각 라우터에게 최단경로에 대해 질의함으로써 송신자로부터 최단경로로 데이터를 수신할 수 있는 것을 말한다[5]. 이는 보안구조 자체가 멀티캐스트뿐만 아니라 유니캐스트도 지원해야 함을 나타낸다.

3.2 제안된 PIM-SM 보안 구조

PIM-SM에서는 SPT 때문에 기존의 보안구조로는 사용자의 보안을 확립할 수 없다. PIM-SM의 보안 구조는 그림 3과 같은 구성요소로 되어있다.

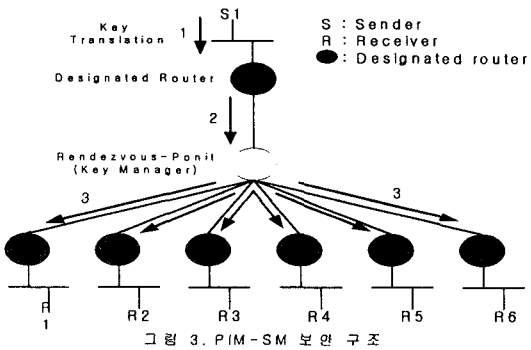

그림 3. PIM-SM 보안 구조

RP라는 수신 공용의 라우터를 둠으로서 각 수신자(R)들은 RP에 의해 통제, 키 관리, 데이터수신 등의 기능을 하며 각 RP당 하나의 Key Manager를 두어 서브그룹으로 나누는 기준이 된다. 그리고 각 송신자(S)에게는 Key Translator를 두어 데이터 전송시 각 서브그룹에 맞는 암호화 키를 가지고 암호화하여 전송한다.

그리하여 본 논문에서는 송신자별 암호화키를 키 관리자로부터 할당받아서 메시지를 송신자 자신만의 키로 가지고 암호화 한 후 RP로 송신하고 이에 따라 수신자는 RP로부터 수신한 데이터를 그룹 키를 가지고 메시지와 암호화키를 복호화 한다. 이후 SPT 라우팅 경로로 변경하여도 송신자의 암호화키는 유효하므로 데이터의 복호화가 가능하다.

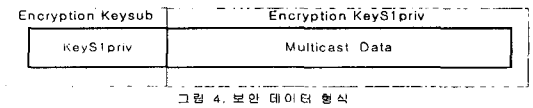

그림 4. 보안 데이터 형식

3.3 송신자가 하나와 다수의 수신자가 있을 경우

PIM-SM에서의 수신자의 그룹 가입

수신자들은 멀티캐스트 그룹가입을 희망하는 IGMP를 그룹 내에 가장 가까운 라우터(DR)를 거쳐 RP에게 송신함으로써 그룹가입을 요청한다. RP는 IGMP를 수신한 후 회의제어에 의해서 멀티캐스트 그룹에 적합한 사용자로 확인이 되면 Secure Channel을 통해 그룹키와 함께 그룹에 가입을 나타내는 응답을 보내게된다. Secure Channel은 멀티캐스트 그룹이 설정되기 이전에 공개키 알고리즘, 서신등 수신자와 RP간의 미리 정의해 놓는 방법으로서 여기서는 특별히 언급을 하지 않는다. 이때 보내는 그룹키는 RP에 따라서 다른 그룹키를 사용한다. 그러므로 각 수신자는 자신이 속한 RP 즉 서브그룹의 키를 가지고 자신의 RP에서 수신한 데이터를 복호화 시킨다.

송신자의 멀티캐스트 그룹 Register

송신자는 Register과정을 하기 위해 DR에게 Register에 대한 신호를 송신하면 DR은 자신이 미리 알고 있는 그룹의 RP에게 Register를 보낸다. RP는 자신의 회의 제어를 확인하여 허가된 송신자로 판정되면 Register에 대한 응답을 회신한다. Register에서 통과한 송신자만이 쓸 수 있는 암호화 키를 Secure Channel을 통해서 분배를 한다. 그리고 RP는 각 수신자에게 송신자의 비밀키를 그룹키로서 암호화하여 보내줌으로서 S2에게서 온 데이터를 복호화할 수 있도록 한다.

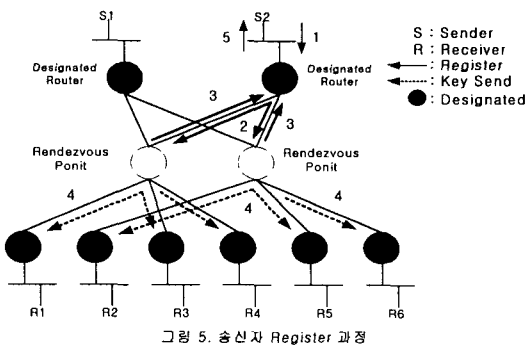

그림 5. 송신자 Register 과정

수신자 탈퇴시 그룹키 변환

그룹에서 R의 탈퇴시 각 그룹은 Rekey Operation 과정을 거쳐야 한다. RP에 존재하는 키 관리자는 새로운 호스트의 Join/Leave시에 자신에게 속해져 있는 호스트에게 새로운 그룹키를 생성/전달해야 한다. 기존의 그룹키를 Secure Channel을 통하여 새로운 그룹키로 각 호스트에게 업데이트 해야 한다. 이때 수신자뿐만 아니라 송신자에게도 새로운 암호화 키를 부여하여야 한다. 그 이유는 기존의 비밀키로 암호화한 데이터를 새로운 가입자가 저장해 놓았다가 변화되지 않은 비밀키를 얻은 후 복호화하면 규칙 2를 또는 탈퇴한 수신자가 계속 데이터를 복호화할 수 있어 규칙 1을 어긋나기 때문이다. 송신자의 탈퇴시 단지 RP는 각 R에게 탈퇴를 알리는 메시지만 전송하면 된다.

탈퇴 과정은 R이 탈퇴를 요구하는 IGMP를 송신하면 수신한 RP는 각 R, S에 대해 새로운 키를 수신하야 함을 알린다. 그럼 서브그룹내 모든 송신자, 수신자는 Secure Channel을 통해 새로운 키를 부여받는다.

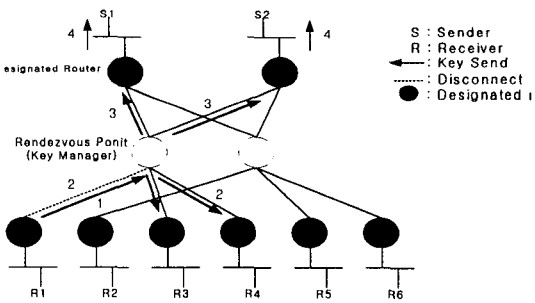

그림 6. Rekey Operation

SPT 경로 변환

송신자는 RP로부터 받은 암호화키로서 자신이 송신을 해야하는 데이터를 암호화함과 동시에 RP에게 전송을 시작한다. 송신자로부터 받은 데이터는 DR에 의해서 RP로 전송되어지고 RP는 각 수신자에게 암호화 된 메시지를 변화없이 그대로 전송함으로써 기존의 서브그룹별로 암호화/복호화 시간을 줄임으로써 전송지연을 줄일 수 있다. 수신자들은 송신자의 데이터를 해독할 수 있는 비밀키를 이미 전송 받았기 때문에 복호화할 수가 있다. 이때 SPT 라우팅경로로 변환시 각 송신자에 대한 암호화된 메시지를 수신한 후 SPT 경로로 변한다. 그렇기 때문에 다른 경로로 받은 송신자의 암호화 된 데이터도 미리 받은 해독키를 가지고 계속 해독을 하면 된다.

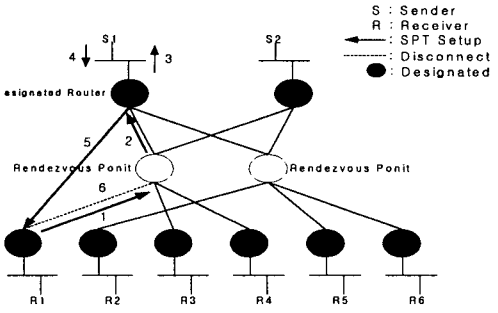

그림 7. SPT 경로 설정

RP에 따른 서브그룹관리

멀티캐스트 그룹내 한 명의 수신자만이라도 가입/탈퇴시 모든 그룹내에 있는 송신자, 수신자에게 키 재분배를 해야 하므로 오버헤드가 크고 모든 수신자는 RP에 의하여 그룹 관리를 받는 라우팅 알고리즘이기 때문에 각 RP간 서로 다른 서브그룹으로 나눈다. 그리고 키 관리자 상호간의 직접적인 정보 교환이 없는 관계로 추가적인 경로도 필요 없다.

따라서 그림7 에서 보는 바와 같이 그룹은 두 개로 그룹 1의 멤버는 (R1, R3, R4)이 속하고 그룹 2의 멤버는(R2, R5, R6)이 된다.

4. 실험 및 결과

그림 7과 같이 두 개의 송신자와 두 개의 RP, 그리고 하나의 RP당 4개의 호스트를 가지고 있는 상황을 설정한 후 네트워크에서 키 분배하는 시간은 다음과 같다.

표 1. 키 분배시간

종 류	변 수 명	시 간
키 설정시간	KTset	10 ms
키 전송시간	KTsed	10 ms
키 변환시간	KTtra	0.1sec/Kbyte
가입/탈퇴에 대한 IGMP 수신 시간	It	10 ms
10Kbyte 데이터 전송시간	Dtra	1 ms

1Kbyte의 데이터를 DES 알고리즘으로 암호화시 약 0.1초의 시간경과가 생겨난다. 그러므로 1 Megabyte 데이터를 전송시 암호화 시간은 10초정도가 소요된다.

위와 같은 구조를 각 보안 구조로 적용시키면 Iolus의 경우 3번의 키 변환이 일어나고, Nortel에서 제안한 구조로는 2번의 키 변화가 일어나므로 각 30초와 20초의 키변환 시간이 필요하다. 그러므로 3가지 보안구조로 송신자가 Register 과정을 거쳐 10Kbyte의 데이터 전송시의 총 소요 시간(T_{total})은 다음과 같다.

$$T_{total} = R_{register\ time} + D_{datasend\ time}$$

$$R = I_t + K_{set} + K_{send}$$

$$D = D_{send} + KT_{tra}$$

$$* \ KT_{tra} = Key\ Translation\ time$$

여기서 R의 시간은 모든 구조에서 동일하기 때문에 구조에 따른 데이터 전송 시간 D는 다음과 같다.

$$D_{xm-sm} = 2D_{send} + KT_{4tra}$$

$$D_{iolus} = 4D_{send} + 3KT_{tra}$$

$$D_{nortel} = 3D_{send} + 2T_{tra}$$

그리고 각 보안구조의 특징은 다음과 같다.

표 2. 보안 구조의 특징

구 분	Iolus	Nortel	PIM-SM
구 조 형 태	다중구조	분산구조	분산구조
능 동 성	high	high	Very high
그룹 확장성	Very high	High	Normal
단일 실패에 대한 결함	Yes	No	No
SPT 경로 지원	No	No	Yes

5. 결론

위와 같은 결과로 인해 본 논문에서 제안한 서브그룹을 RP 단위로 나누고, 송신자만의 비밀키를 따로 관리하는 보안 구조로 인하여 PIM-SM에서도 모든 사용자가 정당한 보호를 받으며, 서브 그룹에 따른 키 변환 작업이 불 필요하여 전송시간 또한 다른 구조에 비하여 단축되는 것을 보였다.

앞으로 연구해야 할 점으로는 RP가 증가함에 따라서 송신자가 전송시 많은 비밀키로 암호화하여 전송하여야 함으로 다른 구조와 비교하여 성능을 보장할 수 있는 RP의 개수와 SPT 경로 설정시 성능분석을 계속적으로 연구되어져야 할 점이다.

참고문헌

[1] Moyer MJ, Rao JR, Rohatgi P., "A survey of security issues in multicast communications," IEEE Network , V.13 N.6, pp.12-23, 1999.

[2] Suvo Mittra. "Iolus:A Framework for Scalable Secure Multicasting," Computer Communication Review, V.27 N.4, pp.277-288, 1997.

[3] Thomas Hardjono, Brad Cain, N. Doraswamy., "A Framework for Group Key Management for Multicast Security," draft-ietf-ipsec-gkmframework-03.txt, Aug., 2000.

[4] Thomas Hardjono, Brad Cain, "Intra-Domain Group Key Management Protocol," draft-ietf-ipsec-intragkm-02.txt, Feb., 2000.

[5] D. Estrin, "Protocol Independent Multicast Sparse Mode (PIM-SM): Protocol Specification," RFC 2362, Jun., 1998.

[6] Sahasrabuddhe L H, Mukherjee B, "Multicast Routing Algorithms and Protocol: A Tutorial", IEEE Network, V.14 N.1, pp.90-102, 2000.

[7] 한근희, "멀티캐스트의 정보보호," 정보처리학회 학회지, 제7권, 제2호, pp.34-40, Mar. 2000.

[8] 김봉한, 이재광, "CBT(Core Based Tree)를 기반으로한 멀티캐스트 키 분배 프로토콜", 한국정보처리학회 논문지, 제7권 제4호, pp.1184-1192, Apr., 2000.

[9] Boivie R, Feldman N, Metz C, "Small group multicast: A new solution for multicasting on the Internet", IEEE Internet Computing , V.4 N.3, 75 79, 2000.

[10] MBone KR, *차세대 멀티미디어 인터넷 MBone해부*, 정보시대, 1997.