□특집□

멀티캐스트의 정보보호

한 근 희†

◈ 목 차 ◈

1. 개 요

멀티캐스트의 정보보호는 현재 다른 인터넷 관련 기술들의 정보보호 연구에 비하여 다소 뒤쳐져있는 상황이며 IETF (Internet Engineering Task Force) 내에 본분야의 연구 및 표준화를 담당하는 Working Group도 아직 구성되지 않은 상태이다. 본 분야를 연구하는 표준그룹은 IRTF에 SMuG라는 그룹으로 1998년 중반에 구성이 되었지만 IRTF는 장기적으로 필요한 인터넷 기술들의 표준을 연구하는 그룹으로서 추후에 구성될 IETF Working Group에 필요한 자료를 제공하는 목적을 가지고 있는만큼 본 분야는 아직 표준화를 논의하기 이전인 연구의 단계에 있다고 보여진다.

본 분야의 연구가 부진한 이유는 멀티캐스트 자체가 인터넷에서 왕성하게 사용되지 못하는데서 기인된다고 보여진다. 현재 인터넷에서 데이타들을 운반하는 router들은 멀티캐스트를 이해하지 못하기 때문에 멀티캐스트 통신을 위해서는 기존의 router들을 보완하거나 또는 새로운 router들로 교체하여야 하는데 router vendor및 ISP들로서는 멀티캐스트 시장이 확실히 예견되지 못하는 상황에서의 투자가 어려운 상황이다. 그러나, 이러한 상황은 멀티캐스트에 대한 시장의 요구가 커짐에 따라 변할 것으로 판단된다. 또는 현재 진행되고 있는 MPLS 표준화가 빠른 속도로 진척되고 그에 따라 멀티캐스트를 이해하는 MPLS router들이 널리 보급되는 상황도 기대할 수 있다.

현재 멀티캐스트를 이용한 통신은 MBone이라는 가상 멀티캐스트 통신망을 통해서 이루어지고 있다. 여기서 가상(virtual)이라는 용어가 사용된 이유는 멀티캐스트를 이해하는 router들 사이에 tunneling 기술을 이용하여 멀티캐스트를 이해하지 못하는 router들과 함께 멀티캐스트 packet들을 전송하기 때문이다. 이러한 전송 과정에서 멀티캐스트 packet은 멀티캐스트를 이해하지 못하는 router들에게 일반 unicast packet과 동일하게 처리할 수 있도록 설계 되어있다.

본 논문에서는 멀티캐스트에서 요구되는 대표적인 정보보호 요구사항들을 소개한다.

2. 멀티캐스트의 정보보호

다른 응용분야들과 마찬가지로 멀티캐스트에서 요구되는 정보보호는 타 분야의 정보보호에 비하여 다소 독특한 면을 제시하고 있다. 멀티캐스트는 화상회의 등 실시간 응용소프트웨어 들에 의하여 주로 사용되므로 정보보호 기능이 실시간이라는 개념을 해칠 수 있는 overhead를 부여할 수 없다는 점과 또한 매우 많은 수의 사용자들이 메

† 정회원 : 한국전자통신연구원 연구원

세지를 암복호화하기 위하여 항상 한개의 비밀키를 공유해야 한다는 점도 있다. 여기에서 의미하는 비밀키는 대칭 키 암호화 알고리즘의 비밀키를 의미한다. RSA와 같은 비대칭 키 암호화 알고리즘의 키는 그 자체의 특성 (느린 처리 속도) 때문에 멀티캐스트의 packet들을 암복화하는 그룹키로 사용될 수는 없다. 그룹내에서 공유되고 있는 비밀키는 새로운 사용자들이 그룹에 참가(join operation) 하고 또한 기존의 사용자가 그룹을 벗어남(leave operation)에 따라 계속 새로운 그룹키로 변경되어야 하는데 이는 다음과 같은 Backward and Forward Secrecy를 만족시키기 위함이다.

1) 멀티캐스트 그룹을 떠나는 사용자는 그룹을 떠난 이후의 메시지를 복호화할 수 없어야 한다.
2) 멀티캐스트 그룹에 새로 가입한 사용자는 가입하기 이전의 메시지를 복호화할 수 없어야 한다.

상기한 조건을 만족시킬 수 있는 방법은 매 join 또는 leave operation 마다 현재 사용되고 있는 그룹 키를 새로운 그룹 키로 대체하는 방법 외에는 없다 (이러한 과정을 rekey operation 라고 불리운다). 새로 생성된 그룹 키는 모든 사용자들에게 다시 전달이 되어야 하는데 그룹 크기가 가령 100,000명이라면 결코 간단한 문제가 아니며 internet-draft [10] 에서도 모든 그룹 키 관리 알고리즘들은 최소한 100,000명의 사용자들을 효율적으로 관리할 수 있어야만 한다는 지적이 있다. 멀티캐스트 메시지는 특별한 인증 메카니즘이 적용되지 않는 한 이를 원하는 사용자들은 해당 멀티캐스트의 주소(IP address)만 입력하면 곧바로 수신할 수 있으므로 상기한 Backward and Forward Secrecy는 화상회의와 같은 멀티캐스트 응용 소프트웨어들에게는 중요한 정보보호 요구 사항이다. 멀티캐스트의 그룹 키 관리는 다음 장에서 좀더 상세히 다루어진다.

멀티캐스트 메시지의 인증은 Group Authentication 및 Individual Authentication으로 구분되며 Group Authentication은 메시지가 동일한 그룹 내에서 전송되었다는 것을 인증하는 반면 Individual Authentication은 특정한 사용자가 해당 메시지를 전송하였다는 것을 인증하는 것이다. Group Authentication은 그룹 키를 이용하여 메시지를 암호화하는 것으로 충분하지만 Individual Authentication은 화상회의와 같은 실시간 응용 소프트웨어에서 RSA와 같은 전통적인 전자서명의 방법을 사용하기가 어렵다. 이는 공개키 암호화 알고리즘들의 느린 처리속도 때문이다. 이러한 제한점을 극복하기 위하여 [1] 에서는 서명되어야 할 메시지의 내용을 알기 이전에 미리 특정 계산을 off-line으로 수행한 후 실제로 메시지를 받았을 때에는 on-line으로 매우 적은 양의 계산만을 수행하도록 하는 기법이 제안되었다. Individual Authentication을 위한 알고리즘들은 [1] 및 [2], [3], [4] 등을 참고하도록 한다. 상기한 알고리즘 외에도 계산속도 및 생성되는 검증자료의 양적인 면에서 매우 효율적인elliptic curve를 이용한 전자서명 방법도 사용될 수 있다.

멀티캐스트의 응용분야 중 가장 규모가 큰 분야는 Cable-TV (Pay-TV) 라고 예상할 수 있는데 본 분야는 상기한 정보보호서비스 이외에 또다른 요구사항을 지니고 있다. Cable-TV의 메시지 내용은 공개되지 못할 성질을 가진 것은 아니다. 따라서, 이 경우에는 메시지 암호화가 실제로는 사용자 인증의 방법으로 사용이 되며 메시지 전체를 암호화할 필요는 없이 비데오 파일의 특정 부분만을 암호화하는 것으로 충분하다. 그러나 Cable-TV가 요구하는 정보보호는 Piracy에 대한 대책이 필요하다. 즉, Cable-TV의 정당한 사용자(고객)가 자신의 지니고있는 그룹 키를 의도적으로 그룹 외의 타인들에게 배포 함으로서 정당하지 않은

사용자들이 해당 Cable-TV 메시지를 복호화하게 하는 행위에 대한 대책이 필요하다. 또는 그룹 키를 배포하지는 않는 대신 자신이 복호화된 메시지를 타인에게 배포하는 행위에 대한 대책도 필요하다. 그룹 키 배포를 막는 방법으로는 스마트 카드, 그리고 복호화한 메시지를 배포하는 행위를 막는 방법으로는 Watermark 기술의 사용이 제안되고 있다.

3. 멀티캐스트의 그룹키 관리

지금까지 개발된 그룹 키 관리 알고리즘들은 중앙집중 방식(Centralized Group Key Management) 및 분산환경 방식(Distributed Group Key Management)으로 나뉘어질 수 있지만 상기한 2가지가 복합적으로 사용되는 방식도 있다. 중앙집중 방식은 한 개의 유일한 키 서버가 그룹 키를 관리하는 방식이며 분산환경 방식은 복수개의 키 서버들을 사용하는 방식이다. 중앙집중 방식은 매우 효율적이지만 사용자들의 수가 늘어남에 따르는 확장성의 문제가 있으며, 분산환경 방식은 키 서버들을 위한 별도의 그룹 키들이 필요하게 되는 등 중앙집중 방식에 비하여 복잡하지만 상대적으로 뛰어난 확장성을 지니고 있다. 그러나 보안의 관점에서는 한개의 키 서버가 그룹 키를 관리하는 중앙집중 방식이 훨씬 유리하다. 다음은 지금까지 제안된 그룹 키 관리 프로토콜들 중 몇몇을 요약한 것이다.

GKMP[5] (Group Key Management Protocol) 프로토콜은 중앙집중 방식으로서 GC (Group Controller)를 이용하여 메시지 암호화에 사용될 대칭 키를 사용자들에게 분배하는데 그룹 키의 생성은 GC가 사용자들 중 몇몇을 대표로 선택하여 공동으로 생성한다. 그룹 키가 생성된 후 GC는 나머지 사용자들에게 자신의 신원을 전자보증서 등을 이용하여 검증토록 한 후 그룹 키를 분배한다. 본 프로토콜은 GC 가 단독으로 키를 관리하고 또한 rekey 메커니즘에 대한 특별한 제안이 없기 때문에 확장성에 문제가 있다.

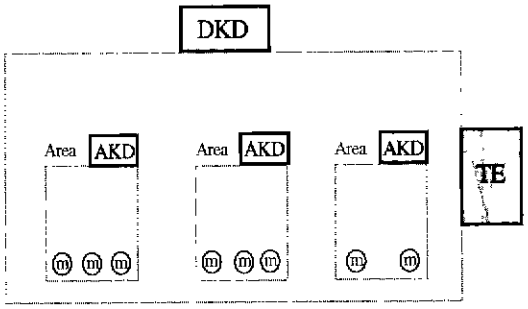
SMKD[6] (Scalable Multicast Key Distribution) 프로토콜 (RFC 1949, 1996)은 분산환경 방식으로서 뛰어난 확장성을 지니고 있지만 Core-based Tree (CBT) Routing 프로토콜에만 사용이 될 수 있고 또한 Router들을 신뢰해야 하는 보안상 취약점이 있다.

MKMP[7] 프로토콜은 Group Key Manager가 그룹 키를 생성한 후 그룹 키를 동적으로 선택된 몇몇의 사용자들에게 전달하여 그들로 하여금 사용자들에게 그룹 키를 전달하도록 하는 프로토콜이다. 그룹 키를 전달하도록 위임 받은 선택된 사용자들은 실제적으로 Sub-Group Key Manager의 역할을 하게 된다. 본 프로토콜은 분산환경 방식처럼 인식되지만 단 한 개의 그룹 키를 사용한다. 그러나 확장성에 문제가 있다.

Lolus [8]는 Secure Distribution Tree라는 계층구조를 이용하였다. 본 메카니즘은 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. 본 메카니즘은 이러한 복호/암호화(translation)에 따르는 overhead가 크다.

Intra-Domain GKMP (Group Key Management Protocol) [9]는 최근에 internet-draft로 제안된 그룹 키 관리 프로토콜로서 (그림 1)과 같은 구조를 가지고있다. DKD (Domain Key Distributor)가 관리하는 한 개의 도메인은 여러 개의 Area로 나뉘어져 있으며 각각의 Area에는 AKD (Area Key Distributor)가 할당되어있다. 멀티캐스트 사용자들(그림에서 m으로 표현됨)은 각 Area내에 분산되어있다. DKD는 도메인내의 모든 멀티캐스트 메시지의 암 복화에 사용되는 유일한 그룹 키인

MKey를 생성하고 또한 AKD들에게 안전하게 전송하는 역할을 수행한다. DKD 및 모든 AKD 들은 그들만으로 구성된 All-KD-Group이라는 그룹에 속해 있으며 본 그룹 내에서만 사용되는 All-KD-Key 라는 비밀 키가 있다.



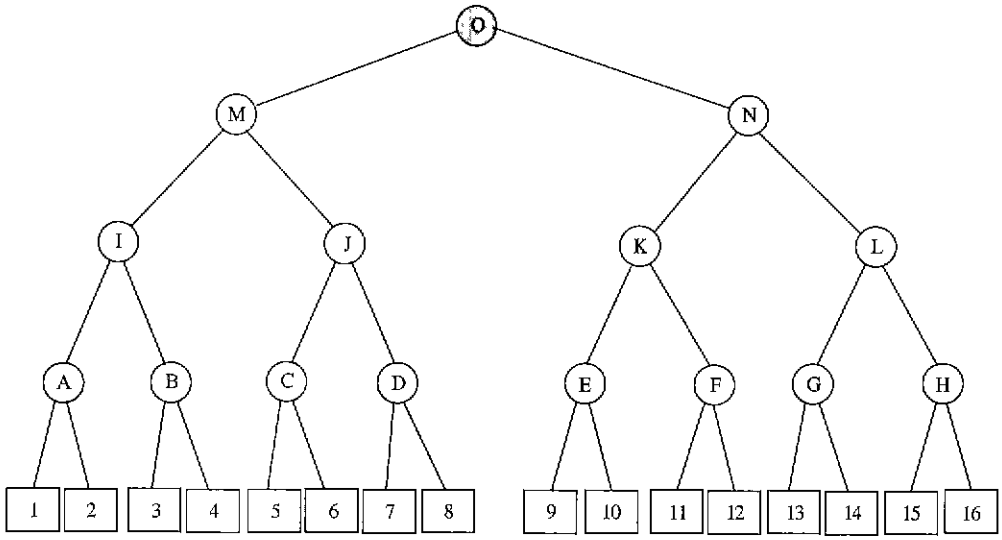
(그림 1) Intra-Domain GKMP 구조

DKD는 All-KD-Key를 이용하여 멀티캐스트의 형식으로 모든 AKD들에게 MKey를 전송할 수도 있으며 또는 DKD와 개개 의 AKD들 사이에 설정된 AKD-Private-Key들을 이용하여 unicast의 형식으로 MKey를 개별적으로 전송할 수도 있다. 이러한 선택사항을 부여한 이유는 요구되는 보안 요구 사항에 따라 적절한 전송방법을 선택할 수 있게 하기 위함이다. AKD와 그에 속한 사용자들은 Area-Group-Key라는 비밀 키를 공유하게 되며 본 키는 해당 Area 외부에는 알려져 있지 않다. DKD로부터 MKey를 전달 받은 AKD는 사용자(m)들에게 MKey를 연속하여 전달하는데 이때 상기한 Area-Group-Key 를 이용하여 멀티캐스트 형식으로 전송할 수도 있고 또는 AKD와 개개 의 사용자들 사이에 설정된 Member-Private-Key를 통하여 uncast형식으로 전달될 수도 있다. 이러한 선택사항을 부여한 이유는 이전의 경우와 동일하다. 즉, 일정한 시간이 지나서 단순히 MKey를 rekey하는 경우라면 Area-Group-Key를 이용한 멀티캐스트의 방식이 충분하지만 leave/join operation의 경우라면 개개 의 사용자들과의 사이에 설정된 Member-Private-Key를 이용하여 Backward and Forward Secrecy를 보장하여야 한다. 타 도매인과의 멀티캐스트 통신은 TE (Translating Entity)를 통하여 이루어지는데 다른 도매인으로부터 메시지가 들어오는 경우 TE는 해당 메시지를 복 호화한 후 다시 본 도매인의 MKey로 암호화하여 전달하게 된다. 따라서 TE는 다른 도매인의 MKey도 저장하고 있어야 한다.

Intra-Domain GKMP는 분산환경의 그룹 키 관리 방식으로서 뛰어난 확장성이 있으며 또한 한개의 Mkey를 사용하여 멀티캐스트의 메시지를 암복호화하기 때문에 도매인 내에서는 translation에 따르는 overhead가 없다. 그러나 AKD들이 MKey를 알고있는데 따르는 보안상의 취약점이 따른다.

분산환경의 그룹 키 관리 방식은 상기한 Intra-Domain GKMP 처럼 보안상의 취약점을 포함하지만 Cable-TV(Pay-TV) 와 같은 응용 소프트웨어들에게는 이러한 취약점이 적용되지 않을 것으로 판단된다. Cable-TV의 메시지 내용은 비밀을 요구하는 사항이 아니고 또한 Cable-TV 회사는 나름대로 자체적인 통신 기반을 소유하고 있을 것이므로 상기한 구조에서 AKD들을 직접 소유 및 운용하게 되면 이들을 신뢰하는 것 또한 문제가 없을 것이다. 또한 본 응용분야는 leave/join operation에 민감하게 대응할 필요없이 rekey는 하루에 한번 또는 1시간에 한번 정도만 이루어져도 충분할 것이다. 따라서, 분산환경의 그룹 키 관리 방식은 Cable-TV에 가장 알맞은 구조라 판단된다.

중앙집중 방식의 그룹 키 관리는 Tree 구조를 바탕으로 이루어진다. 현재까지 LKH (Logical Key Hierarchy)[10] 및 OFT(One-way Function Tree) [11] 등 2개의 알고리즘이 internet-draft로 제안되고 있다. LKH와는 독립적으로 Key Graph[12]를 이용한 알고리즘이 제안되어있지만 기반을 이루는 메커니즘은 LKH와 동일하다. 그러나 [12]는 LKH 모델을 포함하고 있는 internet-draft에 비하여 모델



(그림 2) LKH 모델

분석에 대한 매우 상세한 내용을 담고있다. LKH 모델은 예제를 통하여 가장 쉽게 이해될 수 있다.

LKH모델은 Binary Tree를 기초로 정의되었으며 그림 3.2에서 node O는 그룹 키 서버를 의미한다. Tree의 모든 내부 node들 (node *A* ~ *N*)은 실제로 존재하는 physical entity가 아니며 그룹 키를 관리하기 위한 sub-group key들로서 모두 그룹 키 서버 내에 저장된다. Tree의 leaf node들은 사용자들을 대표하며 모든 사용자들은 그룹키 서버와 one-to-one으로 대응되는 비밀 키를 소유하게 된다. 사용자들은 또한 자신의 node로부터 Tree의 root까지의 path에 있는 모든 sub-group key및 그룹 키 서버의 키를 저장하고 있다. 그룹 키 서버는 모든 sub-group key들을 생성 및 저장하며 이러한 sub-group key 및 Tree구조를 이용하여 매우 효율적인 rekey를 수행할 수 있게 된다. 예를 들어, 사용자 11이 그룹을 떠난다고 가정하자. 그룹을 떠난 후 사용자 11 이후의 그룹 메시지를 복호화하지 못하게 하기 위해서 현재 사용중인 그룹키를 바꾸는 leave operation이 수행되는데 이를 위해서는 사용자 11이 저장하고 있던 그룹 키 *O* 및 sub-group key 들인 *N, K, F*를 새로 생성한 후 이들을 적절한 나머지 사용자 들에게 분배하여야 한다. 이 부분에서 Tree구조의 최대 장점이 나타나는데 가령 사용자 1~8까지를 고려하면 그들은 새로 생성된 키들 중 그룹 키, 즉 새로운 키 *O* 만이 필요하며 또한 사용자 1~8들이 공유하고 있는 sub-group key M은 사용자 9 ~ 16까지에게는 알려져 있지 않다. 따라서 전체 사용자의 1/2인 사용자 1~8은 새로운 그룹 키를 O로 암호화한 뒤 멀티캐스트를 통하여 이들에게 한번에 전달될 수 있게된다. 상기한 방법의 전과정이 다음 표에 소개되어있다. 여기서 k_x는 *x*의 키를 의미하며 $(k_x)k_y$는 *x*의 키가 *y*의 키로 암호화 되어있음을 의미한다. 또한 k'_x는 *x*의 새로 생성된 키를 의미한다. 암호화된 키를 수신한 사용자들은 자신과 그룹 키 서버 사이에 공유하고 있는 키 및 sub-group key들을 이용하여 복호할 수 있게 된다.

1. Server ⇐ m12: $(k'_F)k_{12}$
2. Server ⇐ m12: $(k'_K)k'_F$
3. Server ⇐ m9, m10: $(k'_K)k'_E$
4. Server ⇐ m9,m10,m12: $(k'_N)k'_K$
5. Server ⇐ m13 ~ m16: $(k'_N)k'_L$

6. Server ⇐ m9, m10, m12 ~ m16: $(k'_O)k'_N$
7. Server ⇐ m1 ~ m8: $(k'_O)k'_M$

상기한 예에서는 모두 7개의 메시지 전달이 수행되었는데 일반적인 경우 $(kd-1)$개의 메시지 전달이 필요하다. 여기서 d는 Tree의 height를 의미하며 k는 Tree에서 각node들이 지니는 children node의 갯수를 (Binary tree의 경우 2) 의미한다. LKH모델과 근본 개념은 동일하지만 [12] 에서는 그룹키 관리를 위한 tree 구조에 대한 더욱 세밀한 분석이 포함되어 있으며 rekey message를 구성함에 있어서 user-oriented mode, key-oriented mode 및 group-oriented mode등으로 구분시킨 후 각각의 mode에 대한 분석결과를 포함하고 있다.

기존의 논문들은 다루지 않았지만 tree구조를 자세히 분석하면 그룹크기가 3명 이상인 경우 join 및 leave operation 에 모두 최적화된 tree 구조가 존재할 수 없다는 것을 수학적으로 증명 할 수가 있다. 이는 join 및 leave operation 들은 서로 상반된 구조를 가지는 tree 구조에서 최적화된 성능을 보이기 때문이다.

Tree구조를 이용한 그룹 키 관리의 장점은 한 개의join 또는 leave operation 에 대하여 요구되는 rekey 메시지 수가 전체 사용자 수의 logarithm에 비례한다는 것이다. 이는 leave operation의 경우 전체 사용자 수에 정비례하는 분산 환경 방식의 그룹 키 관리에 비하여 매우 뛰어난 장점이다. 그러나 중앙집중 방식은 한개의 서버가 모든 키들의 생성 및 관리를 하기때문에 확장성에 단점을 지니고 있다.

4. 결 론

지금까지 멀티캐스트 분야는 기존의 router들이 멀티캐스트를 이해하지 못하는 점과 router vendor들이 멀티캐스트 시장의 불확실성 때문에 새로운 router들을 생산하는데 주저하여온 상충되는 이해관계 때문에 다른 분야에 비하여 발전속도가 저조하였다. 그러나 audio 및 video등을 이용한 멀티미디어 응용 소프트웨어들이 계속 개발되고 이들을 운반하는 통신 기반 기술이 발전함에 따라 향후에는 멀티캐스트 분야의 개발이 진전될 것이라 기대된다. 최근에 개발 되고있는 MPLS (Multiprotocol Label Switching) 기술이 멀티캐스트 packet을 운반할 수 있도록 설계되어있음은 주목할 사항이다. MPLS는 아직 연구 단계에 있지만 Cisco Systems 에서는 자신들이 개발한 Tag Switching 이라는 MPLS 기술을 통하여 이미 MPLS용 router들을 생산하였다. 1997년에 IETF에 MPLS의 표준화를 위한 Working Group이 생성되었으며, 또한 MPLS 기술의 수혜자는 일반 사용자들도 당연히 포함되지만 통신 내용물 또는 사전 계약에 따라 서비스의 질을 달리하여 사용자들에게 과금을 할 수 있게 되는 서비스 공급자들도 포함되기 때문에 이 분야의 개발은 빠른 속도로 진행될 것이다.

멀티캐스트 응용 소프트웨어들은 전통적인 정보보호서비스 기술에 덧붙여 그룹 키 관리 및 Individual Authentication 등 멀티캐스트 분야에서 특별히 요구되는 정보보호 기술들의 개발이 필요하다. 그룹 키 관리는 확장성을 보장하는 알고리즘이 개발되어야 하며 Individual Authentication은 계산 속도 때문에 기존의 전자서명 기술을 적용할 수 없는 등 선결되어야 할 문제들을 포함하고 있다. 또한 멀티캐스트 기술의 최대 이용분야로 예상되는 Cable-TV (Pay-TV) 는 2장에서 설명되었듯이 Piracy에 대응하기 위하여 Watermark와 같은 어려운 기술이 요구되는 등 멀티캐스트에 정보보호서비스를 제공하기 위해서는 아직 선결되어야 할 분야들이 많이 있다.

이전 장에서 밝혔듯이 tree를 이용한 그룹키 서버는 서로 상반되는 tree구조에서 최적화된 join 또는 leave operation 이 가능하다. 따라서, 적용하

고자 하는 멀티캐스트 응용프로그램의 보안 요구 사항에 따라 join 또는 leave operation 의 성능에 우선권을 부여할 수 있는 tree 구조의 개발도 향후의 연구과제로 고려될 수 있을 것이다.

참고문헌

[1] Even S., O. Goldreich, S. Micali, "On-line/off-line digital signature", Advances in Cryptology Crypto '89, Springer-Verlag LNCS 435, pp. 263 277, 1990.

[2] Gennaro R., P. rohatgi, "How to Sign Digital Streams", Advances in Cryptology Crypto'97, SpringerVerlag LNCS 1294, pp. 180 197, 1997.

[3] Wong C. K., Lan S. S., "Digital Signatures for Flows and Multicasts", IEEE ICNP98.

[4] Canetti R., J. Garray, G. Itkis, D. Micciancio, M. Naor, B. Pinkas, "Multicast Security: A Taxonomy and Efficient Authentication", INFOCOM99.

[5] H. Harney, C. Muckenhirn, "Group Key Management Protocol (GKMP) Architecture", RFC 2094, July, 1997.

[6] A. Ballardie, "Scalable Multicast Key Distribution", RFC1949, May 1996.

[7] Harkins D., N. Doraswamy, "A Secure, Scalable Multicast Key Management Protocol(MKMP)".

[8] Mittra S., "Iolus: A Framework for Scalable Secure Muticast". In Proceeding of ACM SIGCOMM97, Cannes, France, Sep. 1997.

[9] Thomas Hardjono, Brad Cain, "Intra-Domain Group Key Management Protocol", draft-ietf-ipsec-intragkm- 00.txt, Nov., 1998.

[10] Debby M. Wallner, Eric J. Harder, "Key Management for Multicast: Issues and Architectures", draft-wallner-key-arch-01.txt, Sep., 1998.

[11] D. Balenson, D. McGrew, A. Sherman, "Key Management for Large Dynamic Groups: One-Way Function Trees and Amortized Initialization", draft-balenson-groupkeymgmt-off-00.txt, Feb., 1999/10/27.

[12] Wong C. K., Gouda M., Lam S. S., "Secure Group Communication Using Key Graphs", SIGCOMM98.