안전한 인터넷 멀티캐스트를 위한 그룹키 관리 기법

이진호, 김태윤
고려대학교 컴퓨터학과

e-mail : jhlee@netlab.korea.ac.kr

Key Management Scheme for Secure Internet Multicast with Dynamic Scalability

Jean-Ho Lee, Tai-Yun Kim
Dept. of Computer Science, Korea University

요 약

본 논문에서는, 기존의 멀티캐스트 그룹 키 관리 기법들을 고찰하여 멀티캐스트의 보안성의 필수 요건들을 살펴보고, 이를 기준으로, 안전한 IP 멀티캐스트 구조의 구성 요소들과 단방향 함수를 사용하는 상향식 키 트리를 결합한 안전한 인터넷 멀티캐스트 그룹키 관리 기법을 제안한다. 기존 IPSEC 인터넷 프로토콜의 표준안을 그대로 따르면서 그룹 인증 및 회원 개인 인증이 가능하며, 그룹 구성의 유동성에 대해 확장성이 보장되고, 효율적인 키 재구성 비용과 전방(forward) 및 후방(backward) 보안성이 지원되는 것이 특징이다. 그리고, 새로운 인터넷 멀티캐스트 기법의 성능을 분석하고, 다른 멀티캐스트 기법들과 성능상의 차이점을 비교해 본다.

1. 서론

오늘날 대부분의 네트워크 응용 프로그램들은 클라이언트-서버 환경에 기반하여 유니캐스트 패킷 전송(unicast packet delivery)을 하고 있으며, 나아가 원격회의, 실시간 정보 서비스, 분산 환경의 시뮬레이션 등의 그룹 통신 모델을 기반으로 하여 일대다(one-to-many) 통신이 필수적인 서비스 요구 사항이 되었다. 인터넷 프로토콜에서는 멀티캐스트를 사용하여 하나의 패킷으로 다수의 수신자가 수신이 가능하고, 이것은 그룹간 통신에 효율적으로 이용되고 있다.[2]

클라이언트-서버 환경의 유니캐스트 통신 보안 문제는 매우 잘 정의되고 다양한 보안대책들이 활발히 논의되고 있지만, 이에 비해 그룹간의 멀티캐스트 통신의 경우 그렇지 못하다[7]. 직관적으로 볼 때, 단순한 point-to-multipoint 통신은 point-to-point 통신들의 집합으로 생각할 수 있고, unicast 통신 보안 기법을 확장시켜 multicast 통신에 적용시킬수 있지만, 이런 경우, 동적인 특성을 갖는 그룹에는 확장성이 제공되지 않는다.

본 연구에서는 그룹의 크기와 규모가 유동적인 인터넷 상의 그룹 통신의 보안성을 지원하는 키 관리 기법을 제시하고 분석한다.

본 연구의 구성은 다음과 같다. 2 장에서는 멀티캐스트 보안성의 필수조건과 기존의 기법들을 살펴보고, 이를 기준으로 인터넷 환경에 알맞은 멀티캐스트 기법을 3 장에서 서술하며, 4 장에서는 제안한 멀티캐스트 기법의 성능을 평가하고, 다른 멀티캐스트 기법과 비교,분석하고, 5 장에서 본 연구의 결론 및 향후 과제를 제시한다.

2. 안전한 멀티캐스트를 위한 요구 조건

멀티캐스트 통신의 안전성을 지원하기 위해 요구되는 사항들을 살펴 보고, 지금까지 연구되고 있는 기법들을 고찰한다.

2.1. 보안 요구 사항

(1)회원권(group membership) 제어와 기밀 유지
그룹 통신은 반드시 합당한 그룹 회원에게만 접근가능해야 하며, 그룹 통신 내용은 비그룹회원에게는 공개되지 않아야 한다. 이를 위해, 회원 가입/탈퇴시마다 그룹회원 관리를 해야 하고, 그룹 통신 메시지의 암호화를 통해 기밀성을 제공해야 한다. 그룹통신에 대한 접근 통제를 하려면 그룹 회원들에 대한 인증이 가능해야 하고 이를 위해 개인키 암호화가 필요하다.

(2)그룹 데이터 인증
그룹 회원은 그룹 통신 메시지가 그룹내 회원으로부터 송신되었다는 것을 확인할수 있어야 한다. 그룹 데이터 인증은 모든 그룹 회원 사이에서 공유되는 공통키와 MAC(Message Authentication Code)을 사용하여 이루어진다.

(3)개인 전송자 인증
그룹 회원은 그룹 데이터 전송자의 신원을 식별할 수 있어야 한다.

(4)그룹 관리와 소유권
그룹 소유자는 그룹 키, 로그, 오류 및 예외 상황 관리를 해야 한다.

2.2. 멀티캐스트 그룹 키 관리 프로토콜

(1)GKMP(Group Key Management Protocol)
GMKP 프로토콜은 대칭키(symmetric-key)를 사용하여 그룹 회원들을 관리한다. 각 멀티캐스트 그룹마다 하나의 그룹 제어노드(group-controller)가 존재하여, 그룹키를 생성하고, 분배하고, 재구성(re-keying)하는 역할을 한다. 새로운 회원이 그룹에 가입하거나 기존 회원이 그룹에서 탈퇴할 때 그룹키를 재구성하게 된다. 이 기법은, 매번 그룹키가 재구성될 때마다 모든 그룹 회원들 각각에게 직접 배분해야 하기 때문에 확장성 문제가 존재한다.[2]

(2)SMKD(Scalable Multicast Key Distribution)
CBT(Core-Based Tree) 라우팅 프로토콜기반으로 하나의 그룹에 대해 하나의 공유 멀티캐스트 전송(shared multicast delivery tree)트리를 사용하며, 멀티캐스트 전송 트리는 여러 개의 핵심 라우터(core router)들로 구성된다. CBT 트리가 초기화될 때, 핵심 라우터는 그룹 제어노드처럼 그룹 세션키(session-key)와 키분배키(key-distribution key)를 생성한다. 이 기법은, 확장성이 높지만 특정 라우팅 프로토콜에 종속적이고 따라서 보안 메커니즘도 라우팅 프로토콜에 영향을 받는다.[5]

(3)Iolus
안전한 배분 트리(secure distribution tree)를 사용하여, 멀티캐스트 그룹들을 계층적으로 배열된 서브그룹들로 나눈다. GSC(Group Security Controller)가 존재하여 최상위 레벨의 그룹을 관리하고, GSI(Group Security Intermediary)가 여러 개의 서브그룹들을 관리한다. 각 서브그룹마다 자신의 상위 관리자가 지정한 서브키(sub-key)를 가지며, 자신의 서브그룹과 상위 레벨의 서브그룹의 키들을 알고 있기 때문에 상/하위 레벨로의 메시지 “암호/복호회”가 가능하다. 이 기법의 단점은, GSI 가 각각의 데이터 패킷들을 복호화/재암호화하는 시간이 오버헤드가 되며, GSI 를 제거하는 과정이 너무 복잡하다.[1]

(4)MKMP(Multicast Key Management Protocol)
초기의 그룹키 관리자가 다른 노드에게 동적인 방법으로 키분배 권한을 위임할 수 있다. 초기 그룹키 관리자가 우선 그룹키를 생성한 다음, 선택한 노드들에 대해 그룹 가입을 권유하기 위해 그룹키와 그룹 접근 리스트를 메시지로 보고, 이때 메시지는 선택받은 노드들에 의해서만 복호화될 수 있다. 선택받은 노드들이 메시지를 받고 나면 그룹키 관리자처럼 동작할 수 있게 된다. 이 기법은 그룹 전체에 대해 하나의 키만을 사용하기 때문에, 경로를 지날 때(hop-by-hop)마다 복호화/재암호화 처리를 할 필요가 없어진다.[1]

(5)HFGK(Hierarchical Framework for Group Key Management)
Iolus 와 유사한 그룹키 관리를 위한 키 계층적 구조를 사용한다. 네트워크를 영역들로 분할하고, 각 영역에는 종단 영역들끼리 연결하만 회원 호스트는 포함하지 않는 하나의 “트렁크 영역”과 다수의 “종단 영역”이 존재한다. 각 영역마다 서로 다른 키관리 프로토콜을 사용하고, 서로 다른 종단 영역은 각각 다른 내부 영역 그룹키 관리 프로토콜(intra-region group key management protocol)을 사용할 수 있다.[6]

(6)LKH(Logical Key Hierarchy)
키 계층 구조를 생성하고, 키 계층구조의 맨 바닥에 있는 키부터 차례대로 각각의 그룹 회원에게 할당한다. 각 내부 노드의 키는 자신의 모든 자식 키들로 암호화되어, 그룹 전체에 브로드캐스트된다. 각 회원은 자신의 종단 위치에서 루트까지의 경로를 따라 키들을 복호화할수 있고, 루트 키가 그룹키로 사용된다. 내부 노드의 키들은 논리적인 보안 도메인에 연계된다. 이 기법은, 키 재구성 작업에 약 2log n 개의 키가 소요된다.[4]

3. 안전한 인터넷 멀티캐스트 기법

인터넷 상의 안전한 멀티캐스트를 지원하기 위해, 호스트 구조로서 [1]에서 제안되었던 안전한 멀티캐스트 프레임워크와 구성요소들을 사용하고 그룹키 관리 기법으로 [3]에서 제안된 상향식 단방향 함수 트리(bottom-up one-way function tree)를 사용하는 안전한 인터넷 멀티캐스트 기법을 제안한다.

3.1 멀티캐스트 그룹 회원 노드의 구조

(1)MIKE(Multicast Internet Key Exchange) module

키관리와 사용자의 멀티캐스트 그룹 가입 및 탈퇴를 책임지는 역할을 하며, 운영체제 밖의 응용프로그램 단계에 존재하고, 그룹 제어자(group controller) 내부의 mike 모듈과 통신하여 MSA(Multicast Security Association)를 생성, 관리한다. MSA 에는 그룹 키, 서명/인증 키, 연결 정보등을 포함한다.

(2)IPSec Module(AH/ESP)

데이터 패킷의 암호화/복호화, 인증 작업을 처리하며, 운영체제 내부에 존재한다. ESP(Encapsulating Security Payload) 헤더 앞부분의 프로토콜 헤더에는, IPv4 의 경우 50 이, IPv6 의 경우 다음 헤더 필드가 들어가고, 목적지 IP 주소에는 IP 멀티캐스트 그룹 주소가 들어간다.

멀티캐스트 데이터 인증을 위해서는, 키 관리자가 관리하고 모든 회원들이 공통의 대칭(symmetric) 키를 공유하기 때문에, IP AH(Authentication Header)와 ESP 인증 옵션 필드에 SPI(Security Parameter Index)값을 사용하는 것만으로 충분하다.

(3)SAM(Source Authentication Module)

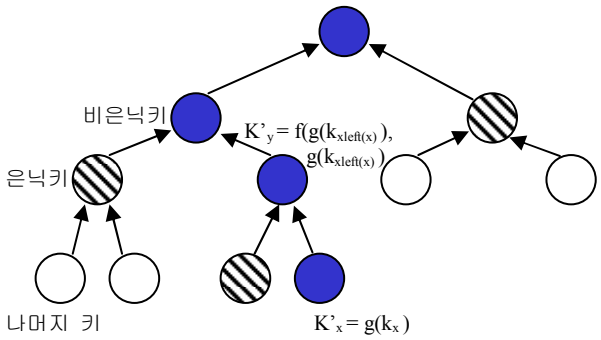
수신 데이터의 송신자 인증 변환과 그룹 메시지 재사용 방지 역할을 하며, 확장성있는 송신자 인증을 위해서는 여러 개의 패킷이 필요하므로 UDP 프레임 단위 이상의 응용프로그램 단계에 존재하게 된다. 송신자 인증을 위해서, 2 가지 메커니즘이 사용된다 : 공개키와 대칭키 방식.

(4)MKMM(Multicast Key Management Module)

그룹 키 관리를 목적으로, IPSEC 또는 SSL 을 사용하여 회원과 그룹 관리자 사이의 안전한 일대일 통신 채널을 설정한다. 그룹키와 부과 정보는 안전한 채널을 통해 전달된다. 키 갱신 메시지는 그룹 관리자로부터 회원들에게 RMS(Reliable Multicast Shim)을 통해 전달된다. 키 갱신 메시지는 공개키 서명을 통해 인증된다. RMS 는 신뢰성있는 멀티캐스트 방식이나 신뢰성있는 일대일 통신 방식으로 구현한다.

3.2 상향식 단방향 함수 트리(bottom-up one-way function tree)

그룹키를 생성하기 위해 단방향 함수를 사용하여 키 트리를 형성한다. 단방향 함수는, 함수 계산 결과인 그룹 키가 계산하기는 쉬우나, 입력 계산 인자를 역으로 계산해내기는 매우 어려운 특징이 있다. 키트리는 이진 트리로써 구성되며, 트리의 종단은 그룹 회원에게 할당되며, 각 내부 노드 는 자신의 2 개의 자식의 키로부터 생성되고 종단에서 루트까지 트리를 따라 계산된다. 루트 노드의 키가 그룹 키로 사용된다. 그룹 관리자는 이진 트리를 관리하며, 임의로 선택한 키를 그룹 회원에게 할당한다.



(1)단방향 함수 구조

내부 노드 x 의 키 $k_x = f(g(k_{left(x)}), g(k_{right(x)}))$

(left(x), right(x) : 노드 x 의 왼쪽과 오른쪽 자식

f : 혼합 함수

g : 단방향 함수)

각 회원은 자기로부터 루트까지 경로상의 비은닉 노드의 키들과, 루트까지 자신의 경로상의 사촌(sibling)인 은닉 노드 키를 알고, 나머지 키들은 알지 못한다. 각 그룹 회원은 자신과 연계된 종단의 비은닉 키와 자신의 루트까지 경로상의 노드들의 모든 사촌들의 은닉 노드 키 목록을 관리한다.

(2)회원 가입 및 탈퇴

①키 재구성(re-keying) : 만약 은닉 키 k'_x 값이 변경되면, 키 관리자가 키 k_s 로 새로운 k'_x 값을 암호화해서, 노드 x 의 사촌 노드 s 의 후손들에게 브로드캐스트한다.

②신규 가입 : 기존 종단 노드 x 가 분할되어 left(x)가 되고, 신규 노드는 right(x)가 된다. 신규 회원은 자신의 은닉 노드 키 집합을 키 관리자와 일대일(point-to-point)유니캐스트 전송을 통해 받는다. 변경된 은닉 노드 키값은 키 재구성 방식을 통해 해당 회원들에게 전달된다. 전송되는 은닉 키의 개수는 노드 x 의 높이(h)+2 이다.

③탈퇴 : 노드 y 가 탈퇴하는 경우, 노드 y 의 사촌에게 할당된 회원은 노드 y 의 부모 p 로 재할당되며, 새로운 종단 키값을 받는다. 만약 노드 y 의 사촌 s 가 부분 트리의 루트라면, 부분트리를 루트에 더욱 가까이 붙이고, 부분 트리 중 하나의 종단에 새로운 키를 부여한다. 전송되는 키의 개수는 노드 y 의 거리(distance)에 해당한다.

3.3 멀티캐스트 프로토콜

회원은 MIKE 를 통해 그룹을 선택하고, 그룹 제어자와 일대일 통신하여 상호 인증을 거쳐 그룹에 등록하고, MSA 를 설정하는 “가입” 초기화 작업을 수행한

다. 회원은, 초기화 작업 후에, MSA 를 가지고 멀티캐스트 통신에 사용할 수 있다.

키 갱신 메시지는, 상위 계층 부분이 아닌 하위 계층의 MIKE 메시지로서 MIKE 내부에서 처리된다.

회원이 그룹을 탈퇴하는 것은, MIKE 를 호출하여 그룹 관리자에 있는 등록 목록에서 자신을 삭제시키고 자신의 MSA 를 무효화시킨다.

데이터 전송은 2 가지 모드가 있다. 송신자 인증이 필요한 경우, 송신 데이터를 SAM 에 전달한 다음, MSA 로부터 그룹 키를 받아 암호화시키고, 운영체제 내부의 AP/ESP 변환을 거쳐, 데이터 패킷을 채널 상에 송신한다. 송신자 인증이 필요하지 않은 경우, 단순히 데이터는 UDP 계층을 거쳐 IP 레벨의 IPSEC 계층에 전달되고 목적 그룹 주소로 전송된다.

수신 데이터는, 우선, 커널의 IPSEC 의 AP/ESP 변환을 거친 후에 그룹키로 복호화 과정을 통해 그룹 인증이 되고 나서, SAM 계층에서 송신자 인증 과정을 거쳐 최종 데이터를 해당 응용 프로그램에 전달된다.

4. 성능 분석

멀티캐스트 그룹 키관리 방식에 대한 성능 평가 기준은 확장성, 그룹/개인 송신자 인증, 그룹키 보안성 등 여러가지가 있다[8]. 본 절에서는 그룹 키 관리 방식이 가지는 계산 회수와 통신량을 기준으로 복잡도를 계산하여, 기존의 멀티캐스트 그룹 키 관리 기법과 비교, 평가해보면 <표 1~3>과 같다.

<표 1> 그룹 초기화 비용

기법 / 측정 인자	SKDC	LKH	OFT (제안 기법)
키 전송량	n K	2nK + h	2nK + h
관리자 계산 회수	n (E+R)	2n (E+R)	2n(E+G)+nR

<표 2> 그룹 가입 비용

기법 / 측정 인자	SKDC	LKH	OFT
키 전송량	NK+log n	2nK + h	h K + h
관리자 계산 회수	n E + R	h (2E+R)	h(E+2G)+R

<표 3> 그룹 탈퇴 비용

기법 / 측정 인자	SKDC	LKH	OFT
키 전송량	NK+log n	2nK + h	hK + h
관리자 계산 회수	NE	h(2E+R)	R+h(E+2G)

(n : 그룹내 회원수, K : 키의 비트 크기, h : 트리의 높이, E : 암호화 함수 계산 비용, R : 임의의 숫자에서 키 생성하는 비용, G : 단방향 함수 g(x)의 계산 비용)

LKH, OFT 기법에서는, 회원은 키 트리의 변화에 대해 반드시 다른 회원들에게 알려 주어야 하고, 수행 성능은 키 트리의 높이에 달려 있다. 따라서 키 트리의 높이를 가능한한 줄일수 있도록 항상 키 트리의 균형을 유지해야만 한다.

5. 결론 및 향후 과제

본 연구에서는 기존의 멀티캐스트 그룹 키 관리 기법들의 고찰을 통해, 멀티캐스트 보안성의 요구사항들을 살펴보고, 이것을 근거로, 인터넷 상에서 안전한 멀티캐스트 기법을 제시하고, 이에 대한 성능을 기존의 멀티캐스트 기법과 비교해 보았다. 그룹 키 관리를 위해 키트리를 형성하여 관리함으로써 그룹의 크기에 대수적으로 증가하며, 유동적인 그룹의 확장성을 지원하고, 인터넷 상에서 신뢰성있는 멀티캐스트 통신을 지원할 수 있다.

향후 과제로는, 대규모의 그룹 회원들이 동시에 메시지를 전송하고자 하는 경우에 발생할 수 있는 송신자 인증 문제에 대한 연구가 필요하다.

참고문헌

[1] R. Canetti, P-C. Cheng, D.Pendarakis, J.R.Rao, P.Rohatgi, D.Saha, “An Architecture for Secure Internet Multicast”, Internet Draft draft-irtf-smug-sec-mcast-arch-00.txt, Feb. 1999.

[2] Thomas A. Maufer, “Developing IP Multicast in the Enterprise”, Prentice-Hall Inc., 1998.

[3] David A. McGrew, Alan T. Sherman, “Key Establishment in Large Dynamic Groups Using One-Way Function Trees”, TIS Report No.0755, TIS Labs at Network Associates, Inc., Glenwood, MD (May 1998).

[4] D. Wallner, E. Harder, R.Agee, “Key Management for Multicast : Issues and Architectures”, RFC 2627, June 1999.

[5] A.Ballardie, “Scalable Multicast Key Distribution”, RFC1949, May 1996.

[6] Chung Kei Wong, Mohamed Gouda, Simon S. Lam, “Secure Group Communication Using Key Graphs”, SIGCOMM’98, 1998.

[7] R.Canetti, B.Pinkas, “A Taxonomy of Multicast Security Issues”, Internet Draft draft-irtf-smug-taxonomy-01.txt, April 1999.

[8] Ran Canetti, Juan Garay, Gene Itkis, Daniel Micciancio, Moni Naor, Benny Pinkas, “Multicast Security : A Taxonomy and some Efficient Constructions”, INFOCOM’99, 1999.