2001년 한국정보처리학회 추계 학술발표논문집 제8권 제2호

일 방향 함수를 이용한 멀티캐스트에서의 키 관리 스킴에 관한 연구

정현기*, 송주석*
*연세대학교 컴퓨터과학과
e-mail : jhk@emerald.yonsei.ac.kr

A Study on Key Management Scheme using One-Way Function in Multicast

Hyun-Ki Jung*, Joo-Seok Song*
*Dept. of Computer Science, Yonsei University

요약

멀티캐스트는 그룹에 속한 사용자들이 공유한 그룹 키를 이용하여 데이터를 송수신한다. 그래서 그룹 멤버의 수가 많고 멤버쉽이 동적일 경우에, 키 분배 및 관리에 있어서 심각한 확장성 문제를 야기한다. 이러한 확장성 문제를 해결하기 위하여 그룹/보조/개별 키로 구성된 키 그래프를 이용하는 데, 그룹 멤버의 수가 n명일 경우에 그룹 키를 업데이트 하는 데 전송되는 메시지의 양은 O(n)에서 O(log n)으로 감소한다. 본 논문에서는 키 그래프를 업데이트 하는 데 있어서, 키 서버가 모든 키를 생성 및 분배하는 것이 아니라, 그룹 키만 생성 및 분배하고, 보조 키는 수신한 새로운 그룹 키와 이전의 보조 키를 일 방향 함수를 이용하여 사용자가 직접 업데이트 하는 것이다. 이 스킴은 그룹에 한 멤버 가입 시 키 서버가 전송해야 할 메시지 수를 O(1)로 줄이는 등 키 서버와 사용자의 메시지 처리 시간 및 전송되는 네트웍 양을 감소시켜, 더욱 효율적인 멀티캐스트에서의 키 관리 및 분배를 가능하게 한다.

1. 서론

다양한 인터넷 서비스가 증가함에 따라 멀티미디어 원격회의, 각종 정보 배포, 분산 대화형 모의 실험 등 한 송신자가 다수의 수신자에게 데이터를 전송하는 멀티캐스트가 등장하였다. 멀티캐스트는 한 송신자가 네트웍 상에 널리 퍼져있는 다수의 수신자를 대상으로 데이터를 전송하므로 많은 통신 링크를 경유하게 되어 부당한 공격자들로부터 신분위장, 서비스 거부, 트래픽 관찰 등 다양한 공격을 받게 된다[1]. 이러한 보안 취약점들을 해결하기 위하여 멀티캐스트는 모든 그룹 멤버가 공유하는 그룹 키의 개념을 사용하여 데이터를 전송한다. 멀티캐스트에서는 멤버의 가입/탈퇴 시마다 그룹 키를 지속적으로 갱신해야 하기 때문에 그룹 키의 관리 및 분배가 매우 중요하다. 특히, 그룹 멤버의 수가 매우 많고, 멤버쉽이 동적일 때 그룹 키를 생성 및 분배하는 키 서버의 키/메시지 생성 시간 및 전송 메시지의 트래픽 양은 매우 크게 된다.

본 논문에서는 키 그래프와 일 방향 함수를 이용하여 키 서버와 사용자의 메시지 처리 시간 및 전송되는 메시지의 트래픽 양을 감소시킬 수 있는 멀티캐스트 키 관리 스킴을 제안하고, 그 성능을 검증하고자 한다.

2. 연구 배경

멀티캐스트는 하나의 IP(Internet Protocol) 목적지 주소에 의하여 식별되는 그룹의 멤버들에게 하나의 메시지를 전송함으로서, 모든 그룹 멤버가 동일한 메시지를 수신하는 통신 메카니즘이다[2]. 본 논문은 이러한 멀티캐스트 환경에서 기존의 키 관리 스킴들이 제공하지 못한 확장성을 제공하는 키의 계층을 이용한 키 그래프 스킴을 통하여 좀 더 효율적인 키 관리 스킴을 제안하고자 한다[3]. 이 스킴에서는 그룹 접근 통제 및 키 관리를 수행하는 신뢰할만한 서

버인 키 서버가 있다고 가정한다. 키 서버는 사용자가 그룹에 가입할 때 소유한 그룹 멤버쉽 정보를 이용하여 상호 인증을 수행하고, 차후의 키 분배를 위한 개별 키를 분배한다. 또, 그룹 멤버 변동 시마다 새로운 키를 생성하여 분배하고, 사용자-키 관계(user-key relation)를 유지한다. 이때, 키 그래프에서의 모든 키 노드들은 완전히 꽉 차고 균형적인(full and balanced) 트리를 구성한다고 가정한다.

2.1 요구 사항

멀티캐스트 환경에서 전송되는 메시지의 안전성을 보장하기 위해서는 다음과 같은 요구 사항을 만족해야 한다.

1) 현재의 멀티캐스트 그룹 멤버 이외에는 전송되는 메시지의 내용을 확인할 수 없어야 한다.

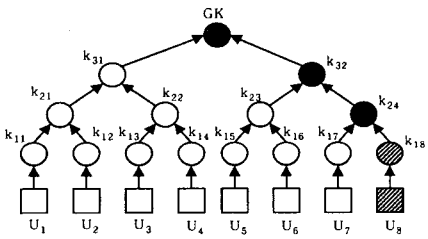
2) 새롭게 그룹에 가입한 멤버는 가입 이전에 전송된 메시지의 내용을 확인할 수 없어야 한다.

3) 그룹에서 탈퇴한 멤버는 탈퇴 이후에 전송되는 메시지의 내용을 확인할 수 없어야 한다.

4) 탈퇴 멤버들은 자신들이 가지고 있는 키 정보를 상호 공유하는 공모 공격을 통해서 현재 그룹 내에서 전송되는 메시지의 내용을 확인할 수 없어야 한다.

2.2 키 그래프

키 그래프 스킴은 사용자에게 그룹 키, 보조 키, 개별 키를 제공함으로서, 그룹 멤버의 수가 n명일 경우에 멤버의 가입/탈퇴 시 키 서버는 사용자에게 O(log n)개의 메시지를 전송하면 된다.



(그림 1) 멤버 U_8 가입/탈퇴 시 키 그래프

1) 키 그래프 : (그림 1)과 같이 노드의 2 유형을 가지는 유향 비순환 그래프(directed acyclic graph)이다.

가) k 노드 : 멤버들이 소유한 그룹/보조/개별 키

- 그룹 키 : {GK}
- 보조 키 : {k_{31}, k_{32}, k_{21}, k_{22}, k_{23}, k_{24}}
- 개별 키 : {k_{11}, k_{12}, k_{13}, k_{14}, k_{15}, k_{16}, k_{17}, k_{18}}

나) U 노드 : 그룹에 속한 각각의 멤버, {U_1~U_8}

여기서, 사용자인 U 노드에 직접적으로 연결된 k 노드들 즉, 트리의 루트인 그룹 키로부터 개별 키까지의 모든 키는 사용자가 소유한 키를 의미한다.

2) $R \subset U \times K$: 사용자 집합 U와 키 집합 K 사이의 관계로서, 사용자-키 관계라고 불린다. 사용자 u가 키 k를 가지면 (u, k)가 R에 있다고 하고, 이 관계가 성립 시 그룹은 안전하다. 예를 들면, 그림 1에서 키 그래프는 다음과 같이 안전한 그룹을 명시한다.

$$U = \{U_1 \sim U_8\}$$
$$K = \{k_{11} \sim GK\}$$
$$R = \{(U_1,k_{11}) \sim (U_8,GK)\}$$

안전한 그룹 {U, K, R}과 관련하여 다음과 같은 2개의 함수가 정의된다.

가) keyset(u) = {k | (u, k) ∈ R} : U에 속한 사용자 u에 의하여 소유된 키들의 집합

나) userset(k) = {u | (u, k) ∈ R} : K에 속한 키 k를 소유하고 있는 사용자들의 집합

3) X → Y : $\{M\}_K$: 송신자 X가 수신자 Y에게 대칭키 K를 가지고 메시지 M를 암호화하여 전송한다는 의미이다.

3. 키 그래프를 이용한 키 관리 스킴[3]

키 그래프를 이용한 키 관리 스킴은 Chung Kei Wong, Mohamed Gouda 그리고 Simon S. Lam이 [3]에서 제안하였다.

3.1 가입

그룹에 가입하기를 원하는 멤버가 키 서버에게 가입 요청을 보내면, 키 서버는 요청 멤버와 상호 인증을 수행한다. 인증 성립 시 요청 멤버에게 차후 메시지 전송을 위해 사용될 개별 키를 전송하고, 개별 키를 이용하여 그룹/보조 키를 제공한다. 이때, 키 서버는 다른 멤버와 함께 공유하게 될 그룹/보조 키를 새롭게 생성하여 멤버들에게 전송한다. (그림 1)에서, 멤버 U_8이 가입 시 키 서버는 새로운 {GK_{new}, k_{32new}, k_{24new}}를 생성하여 다음과 같이 4개의 rekey 메시지를 전송한다.

키 서버 → {U_1, U_2, U_3, U_4} : $\{GK_{new}\}_{GK}$

키 서버 → {U_5, U_6} : $\{GK_{new}, k_{32new}\}_{k32}$

키 서버 → {U_7} : $\{GK_{new}, k_{32new}, k_{24new}\}_{k24}$

키 서버 → {U_8} : $\{GK_{new}, k_{32new}, k_{24new}\}_{k18}$

이 스킴에서 키 서버는 한 멤버 가입 시 h개의 rekey 메시지를 전송한다.(단, h는 키 그래프의 높이로서, 키 그래프에 있는 가장 긴 패스의 길이를 말한다. 여기서는 4이다) 그리고, 키 서버가 rekey 메

시지를 전송하기 위하여 암호화해야 하는 키들의 수는 $h(h+1)/2 - 1$개이다.

3.2 탈퇴

탈퇴를 원하는 멤버는 키 서버에게 탈퇴 요청을 보내고, 그 탈퇴 요청이 허가되면 요청 멤버는 그룹을 떠나고, 키 서버는 탈퇴 멤버가 소유한 키 중에서 다른 멤버와 공유했던 그룹/보조 키를 갱신하여, 남아있는 멤버들에게 전송해야 한다. (그림 1)에서, 멤버 U_8이 탈퇴 시 키 서버는 새로운 $\{GK_{new}, k_{32new}, k_{24new}\}$를 생성하여 다음과 같이 3개의 rekey 메시지를 전송한다.

키 서버 → $\{U_1, U_2, U_3, U_4\}$: $\{GK_{new}\}_{k31}$

키 서버 → $\{U_5, U_6\}$: $\{GK_{new}, k_{32new}\}_{k23}$

키 서버 → $\{U_7\}$: $\{GK_{new}, k_{32new}, k_{24new}\}_{k17}$

이 스킴에서 키 서버는 한 멤버 탈퇴 시 $(d-1)(h-1)$개의 rekey 메시지를 전송해야 한다. (단, d는 키 그래프의 차수(degree)로서, 노드로 들어오는 간선(edge)의 최대 수를 의미한다. 여기서는 2이다) 그리고, 키 서버가 rekey 메시지를 전송하기 위하여 암호화해야 하는 키들의 수는 $(d-1)h(h-1)/2$개이다.

4. 일 방향 함수를 이용한 키 관리 스킴

기존의 키 그래프를 이용한 키 관리 방식은 그룹 접근 통제 및 키 생성을 담당하는 키 서버가 멤버 변동 시마다 새로운 키를 모두 생성 및 분배하므로, 키 서버와 사용자의 메시지 처리 및 전송되는 네트웍 트래픽 양에 있어서 비효율적이다. 따라서, 키 생성 및 분배를 그룹 키에 제한하고, 보조 키는 각각의 멤버가 새로운 그룹 키와 이전의 보조 키를 일 방향 함수를 이용하여 생성함으로서, 키 서버와 사용자의 메시지 처리 및 전송되는 네트웍 트래픽 양을 감소시킬 수 있다.

4.1 가입

기존의 키 그래프 스킴과 동일하나, 키 서버는 기존 멤버들에게 새로운 키를 생성 및 분배 시, 그룹 키만 생성하여 분배한다. (그림 1)에서, 멤버 U_8이 가입 시 키 서버는 기존의 그룹 멤버들과 가입 멤버 각각에게 새로운 $\{GK_{new}\}$와 $\{GK_{new}, k_{32new}, k_{24new}\}$를 생성하여 다음과 같이 2 개의 rekey 메시지를 전송한다.

키 서버 → $\{U_1 \sim U_7\}$: $\{GK_{new}\}_{GK}$

키 서버 → $\{U_8\}$: $\{GK_{new}, k_{32new}, k_{24new}\}_{k18}$

키 서버와 멤버들은 새로운 그룹 키 $\{GK_{new}\}$와 이전의 보조 키 $\{k_{32}, k_{24}\}$를 일 방향 함수 H()를 이용하여 다음과 같이 새로운 보조 키를 계산한다.

1) 키 서버, 멤버 $\{U_7\}$: $\{k_{24new}\} = H(GK_{new}, k_{24})$

$\{k_{32new}\} = H(GK_{new}, k_{32})$

2) 멤버 $\{U_5, U_6\}$: $\{k_{32new}\} = H(GK_{new}, k_{32})$

이때, 키 서버와 각 멤버들은 (h-2)회의 일 방향 함수를 수행해야 한다.

이 스킴에서 키 서버는 한 멤버 가입 시 2개의 rekey 메시지를 전송한다. 이때, 키 서버가 rekey 메시지를 전송하기 위하여 암호화해야 하는 키들의 수는 h개이다.

4.2 탈퇴

기존 키 그래프 스킴과 동일하나, 키 서버는 탈퇴 멤버가 다른 멤버와 공유했던 모든 키를 생성 및 분배하는 것이 아니라, 그룹 키만 생성하여 남아있는 멤버들에게 분배하고, 보조 키는 위에서 언급한 것처럼 일 방향 함수 H()를 이용하여 생성한다. (그림 1)에서, 멤버 U_8이 탈퇴 시, 키 서버는 새로운 $\{GK_{new}\}$를 생성하여 다음과 같이 3개의 rekey 메시지를 전송한다.

키 서버 → $\{U_1, U_2, U_3, U_4\}$: $\{GK_{new}\}_{k31}$

키 서버 → $\{U_5, U_6\}$: $\{GK_{new}\}_{k23}$

키 서버 → $\{U_7\}$: $\{GK_{new}\}_{k17}$

키 서버와 멤버들은 새로운 보조 키를 다음과 같이 계산한다.

1) 키 서버, 멤버 $\{U_7\}$: $\{k_{24new}\} = H(GK_{new}, k_{24})$

$\{k_{32new}\} = H(GK_{new}, k_{32})$

2) 멤버 $\{U_5, U_6\}$: $\{k_{32new}\} = H(GK_{new}, k_{32})$

이때, 키 서버와 각 멤버들은 (h-2)회의 일 방향 함수를 수행해야 한다.

이 스킴에서 키 서버는 한 멤버 탈퇴시 $(d-1)(h-1)$개의 rekey 메시지를 전송한다. 이때, 키 서버가 rekey 메시지를 전송하기 위하여 암호화해야 하는 키들의 수는 $(d-1)(h-1)$개이다.

5. 검증

5.1 성능

1) 통신량 : 한 명의 그룹 멤버가 가입/탈퇴 시, 키 서버가 사용자들에게 전송해야할 메시지의 수와 데이터의 양이 감소한다. 키 서버는 모든 그룹/보조 키를 생성/분배하는 대신에 그룹 키만 생성/분배하기 때문에, 전송해야 할 rekey 메시지의 수 및 데이터(rekey, 헤더)의 양은 감소하게 된다. 예를 들어, h=10, d=4일 때, 한 멤버 가입 시 기존의 스킴은 10개의 rekey 메시지와 54개의 rekey가 암호화되어야 하는 반면에, 제안하는 스킴은 2개의 rekey 메시지와 10개의 rekey가 암호화된다. <표 1>은 한 명의 그룹 멤버가 가입/탈퇴 시 키 서버가 전송해

야 할 메시지의 수와 전송 메시지에 포함되어야 할 키의 수를 나타낸다.

<표 1> 한 멤버 변동시 rekey 메시지 수 및 rekey 수 비교

구 분	전송 rekey 메시지 수		전송 메시지에 포함될 rekey의 수	
	가 입	탈 퇴	가 입	탈 퇴
키그래프 스 킴	h	(d-1)(h-1)	h(h+1)/2 - 1	(d-1)h(h-1)/2
제 안 스 킴	2	(d-1)(h-1)	h	(d-1)(h-1)

2) 프로세싱 타임 : 키 서버와 사용자들의 프로세싱 타임이 감소한다. 키 서버는 새롭게 생성된 그룹/보조 키를 전송하기 위하여, 적절한 키-암호화 키와 대칭키 암호화 알고리즘인 DES(Data Encryption Standard)등을 이용하여 생성된 키를 암호화하고, 그 메시지에 전자 서명을 하여 전송한다. 이때, 키 서버는 사용자에게 <표 1>과 같이 적은 메시지와 데이터를 전송하기 때문에, 매우 많은 시간을 소비하는 동작인 키 서버와 사용자의 암/복호화 및 전자 서명 생성/해독 시간이 감소하게 되어 전체적인 프로세싱 타임이 감소한다[4]. 반면에, 키 서버와 사용자는 보조 키 생성 수 (h-2)회 만큼의 일 방향 함수 동작을 실시해야 한다.

3) 저장 공간 : 기존의 키 그래프 스킴과 동일하게 키 서버는 2n개, 사용자는 그래프의 높이인 h개 만큼의 키를 저장할 필요가 있다.

5.2 안전성

제안하는 스킴은 다음과 같이 요구 사항을 만족한다.

1) 현재의 멀티캐스트 그룹 멤버 집합 U에 속하는 사용자 이외에는 키 집합 K에 관한 정보를 가지고 있지 않다. 즉, 멤버 이외의 사용자는 적절한 keyset(u) = {k | (u, k) ∈ R}을 가지고 있지 않으므로, 사용자-키 관계 R을 만족하지 않는다. 따라서, 그룹 멤버외에는 전송되는 메시지의 내용을 확인할 수 없다.

2) 그룹에서 멤버가 가입할 때, 가입 멤버 u가 소유하게 될 모든 그룹/보조 키는 변경된다. 이때, 기존 멤버들에게는 사전에 공유했던 그룹 키를 이용하여 새로운 그룹 키가 분배된다. 가입 멤버 u는 이전의 keyset(u)={k | (u, k) ∈ R}을 알지 못하므로, 사용자-키 관계 R을 만족하지 않는다. 따라서, 가입 멤버는 가입 이전에 전송된 메시지의 내용을 확인할 수 없다.

3) 그룹에서 멤버가 탈퇴할 때, 탈퇴 멤버 u가 남아 있는 멤버들과 공유한 모든 그룹/보조 키는 변경된다. 이때, 남아있는 멤버들에게는 탈퇴 멤버 u가 소유하지 않은 userset(k') = userset(k) - {u}에 속한 키를 이용하여 새로운 그룹 키가 분배된다. 탈퇴 멤버 u는 이후의 keyset(u) = {k | (u, k) ∈ R}을 알지 못하므로, 사용자-키 관계 R을 만족하지 않는다. 따라서, 탈퇴 멤버는 탈퇴 이후에 전송된 메시지의 내용을 확인할 수 없다.

4) 탈퇴 멤버들은 자신들이 가지고 있는 키 정보를 상호 공유하는 공모 공격을 실행할 수 있다. 하지만, 제안하는 스킴은 멤버가 탈퇴할 때마다 새로운 키 집합 K를 생성함으로, 이전의 키 정보를 가지고 상호 공모하는 공모 공격은 사용자-키 관계 R을 만족하지 않는다. 따라서, 탈퇴 멤버들은 공모 공격을 통해서 현재 그룹 내 전송되는 메시지의 내용을 확인할 수 없다.

5. 결론

멀티캐스트 환경에서 그룹의 확장성을 고려한 키 관리는 필수적이다. 본 논문에서는 멀티캐스트 그룹의 확장성을 고려한 키 관리 스킴인 키 그래프 스킴에 일 방향 함수를 적용함으로서 키 서버와 사용자 간의 통신량 및 프로세싱 타임을 감소시킬 수 있는 스킴을 제안하였다. 제안된 스킴은 일 방향 함수의 안전성을 근간으로 하여 멀티캐스트 메시지의 안전성을 보장할 수 있는 4가지 요구 사항들을 모두 만족한다.

향후에는 본 논문을 기반으로 한 시스템 구현 및 다수의 사용자들의 가입/탈퇴에 관한 연구를 수행할 것이다.

참고문헌

[1] T. Ballardie and J. Crowcroft, "Multicast -Specific Security Threats an Counter-Measures", In Proceedings of the Symposium on Network and Distributed System Security, San Diego, California, Feb. 1995.

[2] S. E. Deering, "Host Extensions for IP Multicasting", RFC 1112, Aug. 1989.

[3] Chung Kei Wong, Mohamed Gouda and Simon S. Lam, "Secure Group Communications using Key Graphs", In Proceedings of ACM SIGCOMM '98, Vancouver, B.C., Sep. 1998.

[4] Bruce Schneier, Applied Cryptography: Protocols, Algorithms and Source Code in C, 2nd Ed., John Wiley & Sons, Inc., 1996.