제33회 한국정보처리학회 춘계학술발표대회 논문집 제17권 제1호 (2010. 4)

상향식 해시 트리를 이용한 동적 그룹 키 관리 기법*

강용구,[1†] 오희국,[1] 김상진[2‡]
[1]한양대학교, [2]한국기술교육대학교

Dynamic Group Key Management Using Bottom-up Hash Tree*

Yong-goo Kang,[1†] Hee-kuck Oh,[1] Sang-jin Kim[2‡]
[1]Hanyang University, [2]Korea University of Technology and Education

요 약

사용자 그룹 서비스는 IPTV를 비롯한 다양한 분야에 걸쳐 응용되고 있으며, 안전한 그룹 통신을 위해 그룹 키를 사용한다. 그룹 키 관리를 보다 효율적으로 하기 위해 최근 많은 연구에서 트리를 이용한 기법을 제시하였다. 트리의 루트 노드로부터 하향식 방식으로 노드 값을 구성하고, 특히 이진트리를 이용하여 그룹 멤버의 가입과 탈퇴에 따라 그룹 키를 갱신하는데 소요되는 비용을 줄였다. 대부분의 연구에서 그룹 키를 갱신하는데 필요한 메시지 전송량이 lg(N) 수준이다. 본 논문에서는 단말 노드로부터 루트 노드 방향으로 노드 값을 구성한 상향식 해시 트리를 기반으로 그룹 키를 갱신하는데 필요한 메시지 전송량이 lg(1) 수준인 기법을 제안한다. 이 기법은 가입 또는 탈퇴가 발생했을 때 즉시 키를 갱신하여 동적이고, 기존의 기법들에 비해 서비스 제공자와 네트워크 대역폭의 부담이 감소하여 효율적이다.

1. 서론

실시간 응용 서비스에서는 그룹의 어떤 변화가 다른 멤버들에게 영향을 주지 않도록 신속한 키 갱신이 요구된다. 대표적인 응용으로 IPTV와 같은 오디오, 비디오 방송이 있다. 가입된 사용자가 많아 그룹의 크기가 크고, 사용자의 서비스 가입과 탈퇴가 잦은 동적인 환경에서 서비스 권한을 효과적으로 관리하기 위해 그룹 키를 이용한다.

동적으로 변화하는 거대한 그룹에 대해 효과적으로 키를 관리하는 것은 어려운 문제이다. 그룹에서 멤버가 탈퇴하거나, 새로운 멤버가 그룹에 가입하는 경우 그룹 키는 갱신되어야 한다. 그룹의 멤버들은 갱신된 키를 효과적으로 계산할 수 있어야 하고, 탈퇴한 멤버는 그것을 획득할 수 없어야 한다. 효율적이고 안전한 그룹 키 관리를 위해서는 두 가지 요구사항을 만족해야 한다. 먼저, 거대한 그룹의 모든 멤버가 빠르게 키 갱신을 하기 위해 효율적인 방법으로 각 멤버에게 갱신에 필요한 메시지를 전달해야 한다. 그리고 이전에 가지고 있거나 사용되었던 키 갱신 정보 등을 이용하여 다음 키 갱신을 예측할 수 없도록 키의 독립성을 만족하여야 한다.

* 이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임(No. 2010-0000438).
† 주저자, suhostar@gmail.com
‡ 교신저자, sangjin@kut.ac.kr

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구로 기존에 제안된 방법에 대해 살펴보고, 3장에서 효율적이고 안전한 그룹 키 관리 기법을 제안한다. 4장에서 효율성과 안전성 분석을 보이고 5장에서 결론을 맺는다.

2. 관련 연구

2000년 C.K. Wong 등이 제안한 LKH(Logical Key Hierarchy)는 KEK(Key Encryption Key)s로 구성된 트리를 이용하여 그룹 키를 관리하는 기법이다[1]. 그룹의 멤버들은 하나의 단말 노드에 할당되고, 서비스 제공자와 공유하는 키를 사전에 수립한다. 중간 노드들에 해당하는 KEK들은 서로 무관하고, 그룹 키 갱신 메시지를 위해 사용되며, 루트 노드에 있는 KEK가 그룹 키에 해당한다. 각 멤버는 자신의 노드로부터 루트까지의 경로에 있는 노드들의 KEK값들을 유지한다. 트리의 가짓수가 d일 때를 예로 들어, 멤버 M_1이 탈퇴 했을 때 $d\log_d N-1$ 의 통신비용이 발생하고, M_1이 가입할 경우 발생하는 통신비용은 $2\log_d N$ 이다.

2003년 A.T. Sherman 등이 제안한 OFC(One-way function Chain)는 LKH로부터 통신비용을 줄이고자 제안된 방법이다[2]. LKH와 마찬가지로 루트 노드의 키가 그룹 키이다. $G(x)=L(x)\|R(x)$, $|L(x)|=|R(x)|=|x|$ 인 수도랜덤함수 $G(x)$를 사용한다. 멤버 탈퇴 시, 서비스 제공자가 부분트리별로 적절한 값을 전송하여 멤버 자체

적으로 그룹 키를 갱신한다. 멤버가 탈퇴하는 경우 발생하는 통신비용은 $\log_2 N$ 이고, LKH에 비해 효율적이다.

2005년 W.T. Zhu 등이 제안한 IHC(Iterated Hash Chain)은 OFC가 이진트리를 통해서만 가능하다는 점을 보완한 기법이다[3]. LKH, OFC와 마찬가지로 루트 노드의 키가 그룹 키이다. $|H(x)| = |x|$ 인 해시함수를 이용하며, 서비스 제공자가 키 갱신에 필요한 적절한 값을 부분트리별 멤버에게 전달하여 자체적으로 갱신한다. 멤버 탈퇴 시 $(d-1)\log_d N$ 의, 멤버 가입 시 $1+\log_d N$ 의 통신비용이 발생한다. IHC와 같은 논문에서 제안된 SD-LKH(Syncrho-difference LKH)는 이전의 그룹 키 값에 XOR연산을 적용하여 새로운 키를 생성하는 기법이다[3]. 이는 기존에 해시함수를 이용하던 기법들에 비해 연산량 측면에서 효율적이다. 하지만 XOR 연산의 특성 때문에 보안 위험 요소를 내포하고 있다. IHC와 마찬가지로 멤버 탈퇴와 가입 시 필요한 통신비용은 $(d-1)\log_d N$, $1+\log_d N$ 이며, 멤버 자체적으로 그룹 키를 갱신한다.

2006년 Y. Mao 등은 Join 트리와 Exit 트리를 유지하는 JET 기법을 제안하였다[4]. 이 기법은 Diffie-Helman 키 동의 방식에 기반하여 두 형제노드의 정보를 이용하여 부모노드의 값을 구성하고, 마찬가지로 루트 노드의 키가 그룹 키에 해당한다. 이 기법은 가입과 탈퇴에 따라 키 갱신에 소요되는 평균 비용을 감소시켰다. 그러나 평균 비용 분석을 시나리오를 단순화 시켰다.

본 논문에서는 멤버의 그룹 가입과 탈퇴에 따라 동적으로 그룹 키를 갱신하고, 이때 필요한 메시지 전송 비용이 lg(1) 인 효율적인 그룹 키 관리 기법을 제안한다.

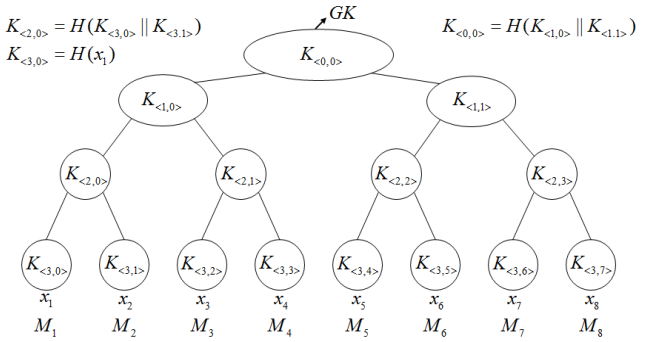
3. 제안하는 방법

본 논문은 키 갱신을 할 때, 서비스 제공자와 네트워크 대역폭의 부담을 줄이는 그룹 키 관리 기법을 제안하는 것이 목적이다. 이를 위해 <표 1>과 같은 표기법을 사용하며, 다음과 같은 보안 요구사항을 만족하여야 한다.

- 그룹 키 안전성: 그룹에 속하지 않은 멤버가 그룹 키를 알 수 없어야 한다.
- 키 독립성: 이전의 그룹 키로 차후의 그룹 키를 알아내거나, 현재 그룹 키로 이전의 그룹 키를 알아낼 수 없어야 한다.

<표 1> 표기법

표기법	내용
N	그룹 멤버 수
M_i	i번째 그룹 멤버
$<l,v>$	레벨 l의 v번째 노드
$K_{<l,v>}$	노드 $<l,v>$의 키
$K_{<0,0>}$	그룹 키 (GK)
r	랜덤 값
x_i	M_i가 할당된 노드의 대응 값



(그림 4) 제안하는 그룹 키 트리 구조

3.1 그룹 키 트리 구조

그룹의 멤버는 트리의 단말 노드에 할당된다. 단말 노드 각각에는 대응 값이 존재하고, 이 값을 해시한 값이 그 단말 노드의 키이다. 중간 노드의 키는 두 자식 노드의 키 값을 해시한 값이고, 최종적으로 루트 노드의 키가 그룹 키이다. 이때, 각 멤버는 자신의 단말 노드의 대응 값을 제외하고, 다른 멤버에 할당된 대응 값들과 자신의 노드 키 값을 서비스 제공자로부터 획득한다. 이를 통해 트리 전체 노드의 키 값을 계산하여 유지한다. 어떤 멤버가 탈퇴 한 경우 그 멤버에게 할당된 대응 값을 이용하여 그룹 키를 갱신한다. 결국 탈퇴한 멤버는 자신의 대응 값을 모르기 때문에 갱신된 그룹 키를 알 수 없다. (그림 4)에서 M_1은 노드 $<3,0>$에 할당되고, $K_{<3,0>}$은 $H(x_1)$ 이다. $K_{<2,0>}$은 두 자식노드의 키 값을 해시한 $H(K_{<3,0>} \| K_{<3,1>})$ 이고, 그룹 키인 루트 노드의 키 $K_{<0,0>}$는 $H(K_{<1,0>} \| K_{<1,1>})$ 이다.

3.2 그룹 멤버 탈퇴

그룹에서 멤버 M_i가 탈퇴하면, 서비스 제공자는 $<LEAVE,\ M_i,\ \{r\}_{GK}>$ 메시지를 방송한다. 각 멤버는 M_i가 할당됐던 노드의 대응 값 x_i를 자체적으로 갱신한다. 이때 갱신된 값은 $x_i' = H(x_i + r)$ 이다. 그리고 그 노드로부터 루트까지의 모든 노드 키를 해시 함수를 이용하여 갱신한다. (그림 4)에서 M_3이 탈퇴한 경우, $<LEAVE,\ M_3,\ \{r\}_{GK}>$ 메시지를 수신한 각 멤버는 자체적으로 $x_3' = H(x_3 + r)$을 계산하고, $K_{<3,2>}$, $K_{<2,1>}$, $K_{<1,0>}$, $K_{<0,0>}$을 차례로 계산하여 그룹 키를 갱신한다. 멤버 탈퇴 후 대응 값을 변경한 노드는 빈 노드로 계속 유지하여 새 멤버가 가입하는 경우 우선적으로 할당한다.

3.3 그룹 멤버 가입

그룹에 새 멤버 M_i가 가입하면, 그룹 키 트리상에 빈칸의 단말 노드가 있는지 여부에 따라 두 가지 경우로 나누어 삽입 노드를 할당한다.

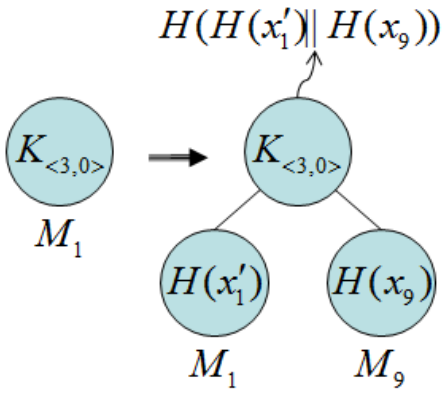
(1) 빈칸의 단말 노드가 있는 경우

그룹 멤버의 탈퇴 등으로 빈칸의 단말 노드가 있는 경

우에는 그 중 최상위 레벨의 가장 좌측의 노드를 삽입 노드로 할당한다. M_i가 할당된 노드의 대응 값이 x_i 이었다면, 서비스제공자는 $<JOIN,\ M_i,\ \{x_i'\}_{GK}>$ 메시지를 방송한다. 각 멤버는 x_i를 x_i'로 교체하고, 해당 노드로부터 루트 노드까지의 모든 노드 키를 갱신하고 GK'를 획득한다. 가입자 M_i는 서비스 제공자로부터 자신의 노드를 제외한 모든 단말 노드의 x 값들과, 자신의 노드의 노드 키 값 $H(x_i')$을 수신하여, 트리를 구성하고 갱신된 그룹 키 GK'를 획득한다.

(2) 빈칸의 단말 노드가 없는 경우

트리상에 빈칸의 단말 노드가 없는 경우에는 삽입 노드를 선정하여 확장하는 절차가 우선되어야 한다. 삽입 노드는 위와 마찬가지로 단말 노드 중 최상위 레벨의 가장 좌측 노드로 선정한다. 그 노드의 대응 값이 x_k일 경우 서비스 제공자는 $<JOIN,\ M_i,\ \{x_i\}_{GK},\ \{r\}_{GK},\ H(x_k')>$ 메시지를 방송한다. 이때, $x_k' = H(x_k + r)$ 이다. 각 멤버는 삽입 노드에 두 자식 노드를 확장하고, 좌측 자식 노드에 기존 멤버를, 우측 자식 노드에 새 멤버를 할당한다. 두 자식 노드의 대응 값은 x_k', x_i 이다. 기존 멤버는 $H(x_k')$를 통해 자기 노드의 키 값을 획득하며, 그 외 멤버들은 x_k'를 자체 갱신하고, $\{x_i\}_{GK}$로부터 x_i를 획득하여 그룹 키를 갱신한다. (그림 4)의 상태에서 M_9가 새로 가입하면 (그림 5)와 같이 확장하게 된다. 삽입 노드는 M_1의 노드로 선정되고, M_1이 좌측 자식 노드로 M_9가 우측 자식 노드로 할당된다. 각 노드의 대응 값은 x_1', x_9가 되고, 기존 삽입 노드의 노드 키 값은 $H(H(x_1')\|H(x_9))$가 된다. 이를



(그림 5) 가입에 따른 노드 확장

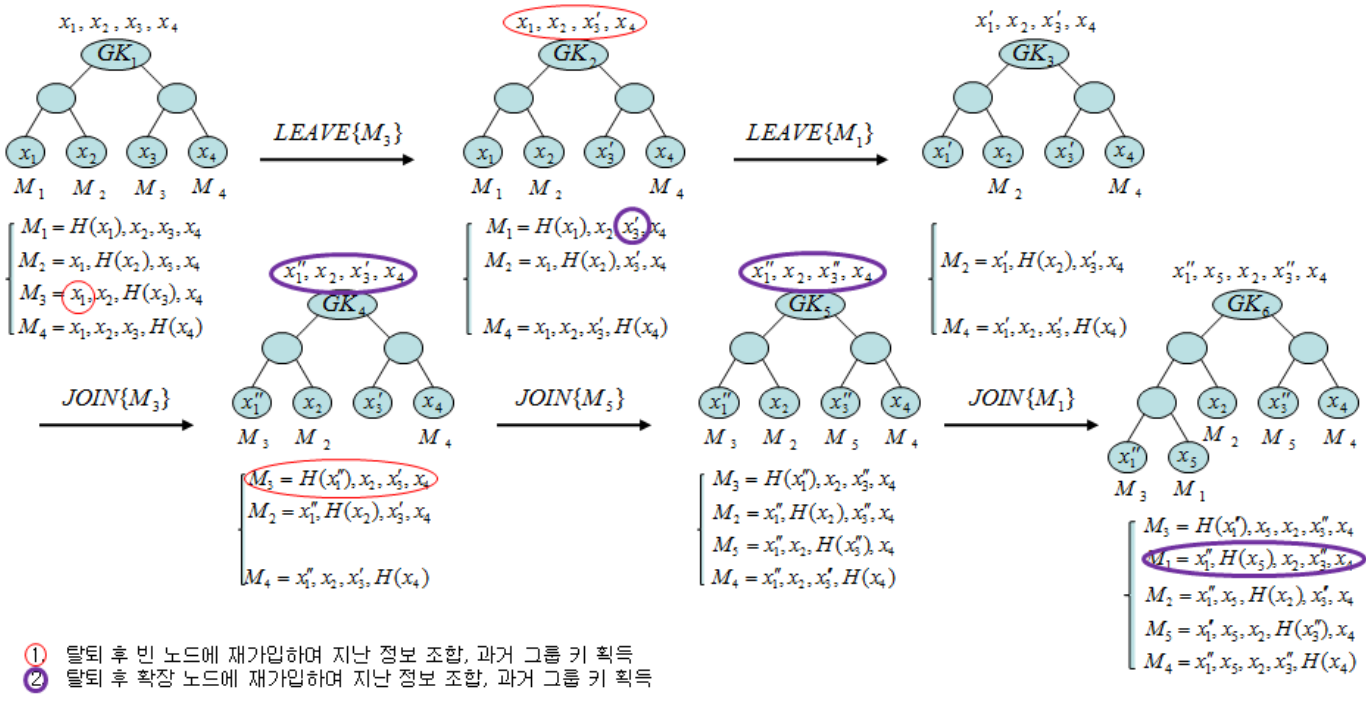
통해 최종적으로 그룹 키가 GK'로 갱신된다. 가입자 M_9는 서비스 제공자로부터 $H(x_9)$와 다른 멤버 단말 노드의 대응 값들을 수신하여 그룹 키를 획득한다.

3.4 안전성 보강 확장 프로토콜

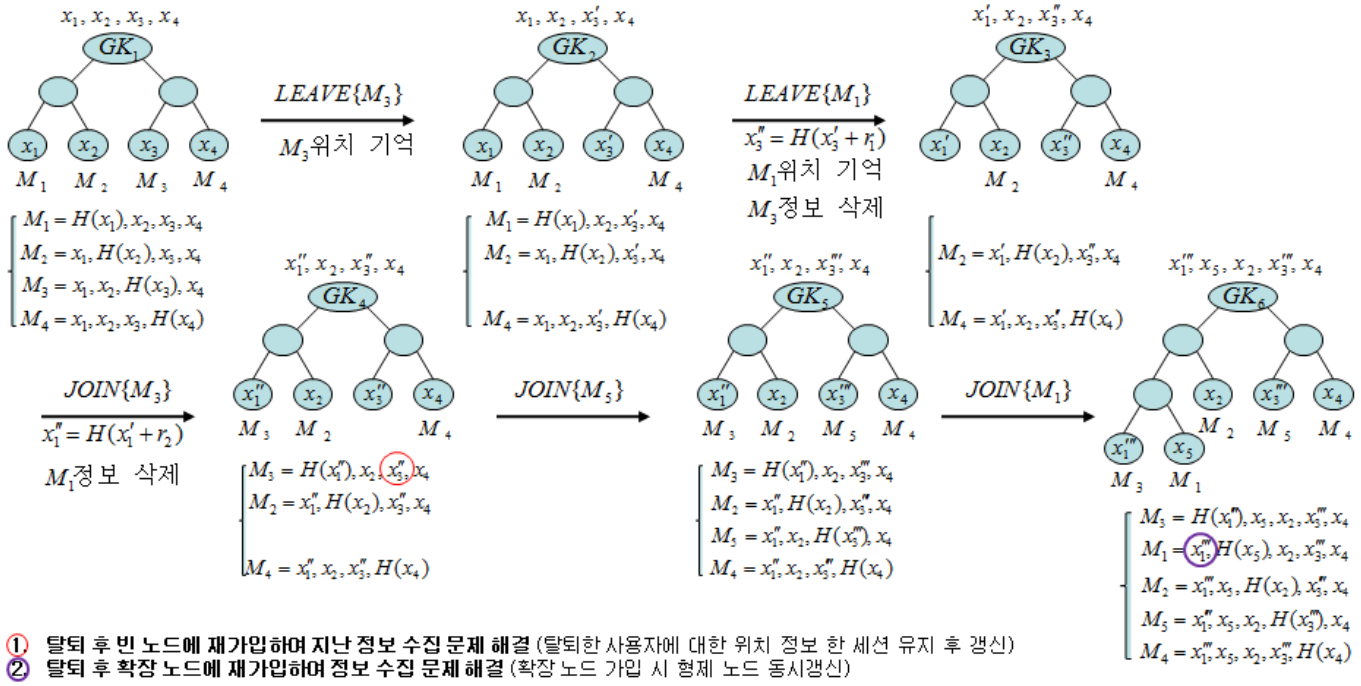
지금까지 기술한 방법만으로는 (그림 6)과 같이 보안상 취약점이 두 가지 존재한다. 먼저 탈퇴 후 빈 노드에 재가입 하여 지난 정보를 조합하면, M_3과 같이 과거의 그룹 키를 획득 할 수 있다. 또한, 탈퇴 후 확장 노드에 재가입하여 지난 정보를 조합하면, M_1과 같이 과거의 그룹 키를 획득 할 수 있다. 첫 번째 문제는 탈퇴 시 다음 세션에 해당 위치를 갱신함으로써, 두 번째 문제는 확장 재가입 시 형제노드를 동시 갱신함으로써 (그림 7)과 같이 해결할 수 있다.

4. 분석

본 장에서는 제안하는 기법의 효율성과 안전성을 분석



(그림 6) 기본 프로토콜에서의 두 가지 취약점



(그림 7) 안전성 보강을 위한 확장 프로토콜

한다. 효율성은 통신, 연산, 저장 비용 측면으로 분석하고 안전성은 키의 독립성 측면에서 분석한다.

4.1 효율성 분석

멤버의 가입 및 탈퇴가 발생하면 단 한 번의 고정크기의 메시지 전송이 요구된다. 가입자에게는 N 크기의 대응 값을 전송해야 한다. 그리고 각 멤버는 가입 및 탈퇴 시 $\lg N$의 해시 연산을 통해 그룹 키를 갱신한다. 이는 관련 연구의 기법들과 비슷한 수준이다. 또한 서버와 각 멤버가 트리와 노드 키 값을 유지하기 위해 $2N$ 만큼의 저장 비용이 요구된다. 이는 관련 연구의 기법보다 많은 비용이지만, 저장 공간의 문제는 현재 기술로써 크게 문제 되지 않는다.

4.2 안전성 분석

탈퇴한 멤버 M_i는 자신의 대응 값을 모르기 때문에 새 대응 값 $x_i' = H(x_i + r)$을 구할 수 없고, 따라서 갱신된 그룹 키를 계산해낼 수 없다. 새로 가입한 멤버가 할당되는 노드의 대응 값도 항상 갱신되고, 대응 값 x_i가 아닌 $H(x_i)$ 값을 제공받기 때문에 기존의 그룹 키를 알 수 없다. 특히 확장 프로토콜을 적용함으로써 여러 가지 상황에 대한 취약점을 보완하였다.

5. 결론

본 논문은 상향식 해시 트리를 이용하여 멤버의 가입 및 탈퇴 발생 시 효율적인 키 갱신이 가능한 그룹 키 관리 기법을 제안하였다. 제안하는 기법은 키 갱신에 필요한 메시지 전송 수를 $\lg(1)$ 수준으로 감소시켜, 서비스 제공자와 대역폭의 부담을 줄였다. 또한 멤버의 가입 및 탈퇴를 바로 적용하여 동적인 사용자 관리가 가능하다. 이러한 그룹 키 관리 기법은 현재 다양한 방면으로 제공되는 그룹 서비스에 적용할 수 있다. 특히 가입자 수가 많은 IPTV 서비스의 제한수신시스템에 적용하면 효율적인 사용자 관리가 가능하다.

참고문헌

[1] C.K. Wong, M. Gouda, and S.S. Lam, “Secure group communications using Key graphs,” IEEE/ACM Trans. Networking. vol. 8, pp. 16-30, 2000.

[2] A.T. Sherman and D.A. McGrew, “Key establishment in large dynamic groups using one-way function trees,” IEEE Trans. Software Eng., vol. 29, pp. 444-458, May 2003.

[3] W.T. Zhu, “Optimizing the tree structure in secure multicast key management,” IEEE Communications Letters, vol. 9, no. 5, pp. 477-479, May 2005.

[4] Y. Mao, Y. Sun, M. Wu, and K. J. R. Liu, “JET: Dynamic Join-Exit-Tree Amortization and Scheduling for Contributory Key Management,” IEEE/ACM Transactions on Networking, Vol. 14, No. 5, pp. 1128-1140, Oct. 2006.

[5] M.J. Mihaljevic, “Reconfigurable key management for broadcast encryption,” IEEE Communication Letters, vol. 8, pp. 440-442, July 2004.

[6] Q. Kang, X. Meng, and J. Wang, “An optimized LKH scheme based on one-way hash function for secure group communications,” IEEE ICCT, Nov. 2006.