한국산학기술학회논문지
Vol. 11, No. 9 pp. 3495-3501, 2010

멀티캐스트 전송을 위한 키 체인 기반의 안전한 그룹 키 관리방안 연구

김보승[1*], 김정재[1], 이기영[2], 신용태[1]
[1]숭실대학교 컴퓨터학과, [2]에스넷시스템(주)

A Study of Secure Group Key Management Based on Key-Chain for Multicast Data Transmission

Bo-Seung Kim[1*], Jeong-Jai Kim[1], Ki-Young Lee[2] and Yong-Tae Shin[1]
[1]**Dept of computer Science, Soongsil University**
[2]**S.Net Systems Inc.**

요 약 최근 화상회의, 인터넷방송, 온라인 게임등 대규모의 데이터를 여러사용자에게 동시에 전송하는 애플리케이션이 증가함으로 인해 그룹 통신의 중요성 및 활용도가 높아지게 됨에 따라 그에 대한 보안이 중요한 문제로 인식되게 되었다. 멀티캐스트 환경에서 보안성을 제공하기 위해 기존의 하나의 그룹 관리 서버를 통해 키 트리 기반의 프로토콜을 이용한 연구가 많지만, 제안하는 논문에서는 상대적으로 오버헤드가 적은 안전한 그룹키 관리 기법을 제안하고자 한다. 따라서 제안하는 논문에서는 기존의 그룹키 관리기법과의 차별성 및 효율성을 비교하여 우수성을 입증한다.

Abstract Because the application simultaneously to transmit large amounts of data (Video conferencing, Internet broadcasting, Online games etc.) to multiple users increases, the importance and utilization of group communication was greater. So the security was recognized as a important issue. To provide security in multicast environment, A study of single group management server using protocol based on Key Tree Scheme was proposed. But the paper proposes secure group key management scheme to be a relatively low-overhead. Therefore proposed paper is demonstrated to be excellent by comparing the effectiveness of existing and proposed group key management scheme.

Key Words : Group-Key, Multicast, Security, Key-Chain

1. 서론

인터넷의 급속한 발전에 따라 그룹 통신을 기반으로 하는 새로운 종류의 통신 응용 서비스들이 등장하고 있다. 이러한 그룹 통신은 일대다 혹은 다대다 통신 형태로 구성되며 멀티캐스트는 이러한 그룹 통신에 적합한 프로토콜이다[8,9]. 멀티캐스트 환경에서는 메시지에 대한 하나의 복사본만을 전송함으로써 멀티캐스트 그룹의 모든 멤버가 수신할 수 있고 단 하나의 그룹 키로 멀티캐스트 통신을 보호받을 수 있다. 멀티캐스트 그룹 키는 그룹의 멤버들을 관리하고 데이터를 암·복호화하기 위하여 사용된다.

멀티캐스트 그룹 키는 멤버들의 그룹 가입/탈퇴로 인하여 그룹 키 생성 및 재분배가 필요하다. 또 안전한 그룹 키 관리를 위해서는 주기적으로 키 갱신이 이루어져야 한다[3]. 그러나 그룹의 규모가 큰 경우 모든 멤버에게 그룹 키를 재분배해야 하기에 네트워크 지연을 발생시키는 단점을 가진다. 본 논문에서는 이를 고려하여 키 체인

*교신저자 : 김보승(kdwon2002@ssu.ac.kr)
접수일 10년 06월 29일 수정일 (1차 10년 08월 20일, 2차 10년 09월 03일) 게재확정일 10년 09월 08일

방식을 이용한 그룹 키 관리 기법을 제안한다. 그룹에 속하는 멤버들은 공통의 키 체인 방식을 통해 그룹 키를 생성한다. 이 방식은 통신 중간 단계에서의 그룹 키 교환을 배제하여 키의 노출을 방지면서 동시에 키 생성 및 재분배를 위한 지연을 감소시킨다. 특히 복잡하고 규모가 큰 그룹이나 실시간으로 발생되는 데이터 처리에 대해 좋은 성능을 가질 수 있다.

본 논문의 구성은 다음과 같다. 2장은 관련연구부분으로서 안전한 그룹 키 관리 구조와 요구사항을 파악하고 키 체인을 이용한 기존 기법을 분석한다. 3장은 새로운 키 관리기법을 제안하는 부분으로 키 관리기법의 플로우, 송•수신자 측에서의 키 체인 생성 및 그룹 키 관리에 대하여 기술하고, 4장에서 성능평가를 한 후 마지막으로 5장에서 결혼을 맺고 향후 연구 방향을 살펴본다.

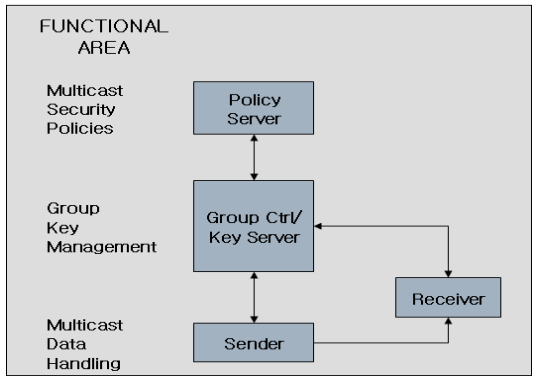
2. 관련 연구

2.1 안전한 그룹 키 관리 구조

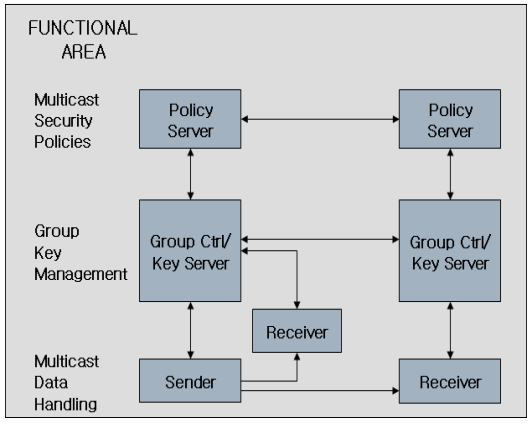
안전한 그룹 키 관리 구조[1,2,7]의 요소에는 Policy Server, GCKS(Group Controller and Key Server), Sender /Receiver 가 있다. Policy Server는 Entity가 사용할 Security policy를 생성하고 관리한다. GCKS는 암호화 키 분배와 관리 및 사용자 인증 기능을 수행한다. Sender/Receiver는 사용자와 device인증 및 key material을 통한 새로운 키를 획득한다.

현재 정의 되어 있는 그룹 키 관리 구조는 두 가지가 있다. 즉 하나의 GCKS가 존재하는 중앙집중형 (Centralized Reference Framework) 키 관리 구조와 여러 개의 서브그룹으로 나누어 관리하는 분산형(Distributed Reference Framework) 키 관리 구조이다. 중앙집중형 키 관리 구조는 Policy Server와 GCKS를 하나씩 두어 관리하고 있지만 분산형 키 관리 구조는 Policy Server와 GCKS를 분산시켜 여러 개를 두어 네트워크의 부하를 줄인다.

아래 그림 1과 그림 2는 각각 중앙집중형 키 관리 구조도와 분산형 키 관리 구조도를 나타내고 있다.



[그림 1] 중앙집중형 키 관리 구조



[그림 2] 분산형 키 관리 구조

2.2 안전한 그룹 키 관리 요구사항

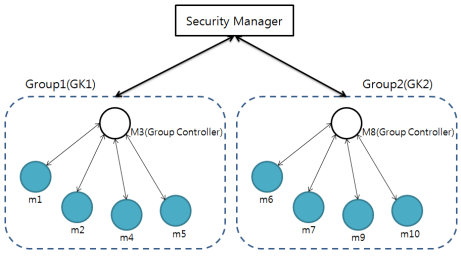
안전한 그룹 키 관리를 위한 요구사항은 다음과 같다. 첫째: 그룹 키의 유효시간을 정의하여 정기적인 키 갱신을 수행해야 한다. 키 갱신은 Backward Secrecy와 Forward Secrecy를 보장하기 위해 필요하다. Backward Secrecy는 새로 가입한 멤버가 이전의 멀티캐스트 데이터에 접근 권한을 제한하는 것이고 Forward Secrecy는 기존 멤버의 탈퇴 후 멀티캐스트 데이터에 접근 권한을 제한하는 것이다. 둘째: 멤버에 대한 접근제어를 위해 그룹에 가입 시 인증이 필요하다. 셋째: 키 관리자와 멤버 사이에 유니캐스트 채널을 통한 통신이외의 방법으로 그룹 키의 재분배가 가능해야 한다.

2.3 기존의 그룹키 관리 기법

2.3.1 GKMP(Group Key Management Protocol)

GKMP는 SM(Security Manager)으로부터 키 관리에 대한 권한을 위임받아 키 생성, 키 분배, 그룹키 재구성,

진행과정에 대한 보고를 담당하는 GC(Group Controller)와 GC의 키 생성 작업을 도우며, GC 인증수행에 따른 확인 과정, GC로부터의 키 수선/요청, 로컬(CRL(Compromise Recovery List)를 유지, 로컬 키 관리 등을 수행하는 그룹 멤버로 구성된다[5]. GC에 의하여 생성되는 키는 데이터의 암호화 전송을 위해 필요한 GTEK(Group Rtaffic Encryption Key)와 갱신한 그룹키의 암호화 전송을 위해 필요한 GKEK(Group Key Encryption Key), GC로부터 키를 맴버에게 전송하기 위해 SKEK(Session Key Encryption Key)이다. GC는 각 사용자의 신원을 확인하기 위해 인증작업을 하고, 유효한 멤버에게는 SKEK를 보낸 후, GTEK와 GKEK 키를 전송한다. 새로운 사용자가 가입하는 경우에도 GC에 가입 요청이 전달되면, 위와 같은 단계를 거쳐서 키를 전송하게 된다.

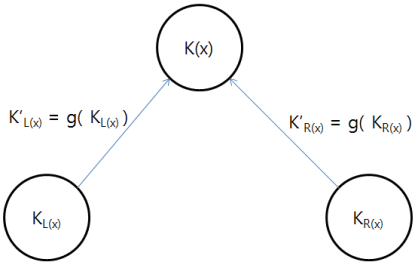


[그림 3] GKMP의 구조

2.3.2 OFT(One-way Function Tree)

OFT를 이용한 그룹키 관리 기법은 키 갱신 작업 시 메시지의 수를 줄이기 위한 기법으로 그룹·보조·개별키 개념을 이용한 키 트리를 사용하지만, 기존의 키 트리 기법과는 달리 그룹 서버와 멤버들이 Blind 노드키·개별키·단방향 해쉬함수 그리고 혼합함수를 이용하여 직접 그룹·보조키를 생성한다[6].

OFT에서의 키 트리는 이진트리 구조로 이루어지며, OFT에서 그룹·보조키는 각각의 노드에 해당하는 두 개의 하위 노드 키를 단방향 함수와 혼합함수에 입력하여 생성된다.



[그림 4] OFT의 노드키 계산

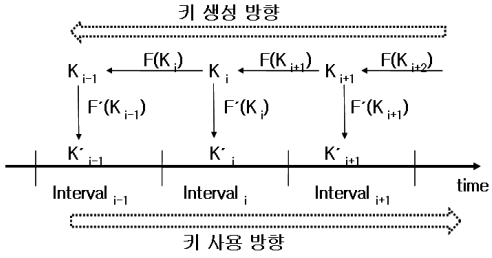
그림 4와 같이 은닉키 K'(x)는 K(x) 노드 키를 단방향 함수에 대한 입력으로 얻게 되며, 그룹·보조키는 두 개의 자식 노드 키에 대한 은닉키를 혼합함수를 이용하여 얻을 수 있다.

따라 그룹·보조키의 생성 방법은 다음과 같이 계산된다.

$$k(x) = f(g(k_{L(x)}), g(k_{R(x)})) \quad (1)$$

2.4 키 체인을 이용한 기존의 기법

이 절에서는 키 체인을 이용한 기존의 기법 중에서 TESLA에 대해 살펴보도록 한다. TESLA는 소스 인증을 기반으로 하며 MAC(Message Authentication Code) 알고리즘을 사용한다. 또한 대칭암호화를 사용하고 필요한 비대칭 속성을 만족하기 위해 키 사용에 대한 송신자와 수신자간의 느슨한 시간 동기화를 필요로 한다. TESLA는 인증정보의 생성과 검증을 위한 부하가 적고 DoS 공격으로부터 수신자를 보호한다.



[그림 5] TESLA의 one-way key chain 구조

그림 5는 TESLA의 one-way key chain 구조를 나타낸다. TESLA의 키 생성은 역방향으로 이루어지기 때문에 사전에 데이터의 크기를 알고 있어야 한다. 즉 TESLA는 제한된 크기의 데이터를 처리함으로 이것은 지속적으로 발생하는 실시간 데이터 처리에 부적합하다. 또한 TESLA는 RTT를 기반으로 송신자와 수신자간에 시간동기화를 하기 때문에 지연에 민감한 문제가 있다.

3. 제안하는 키 관리 기법

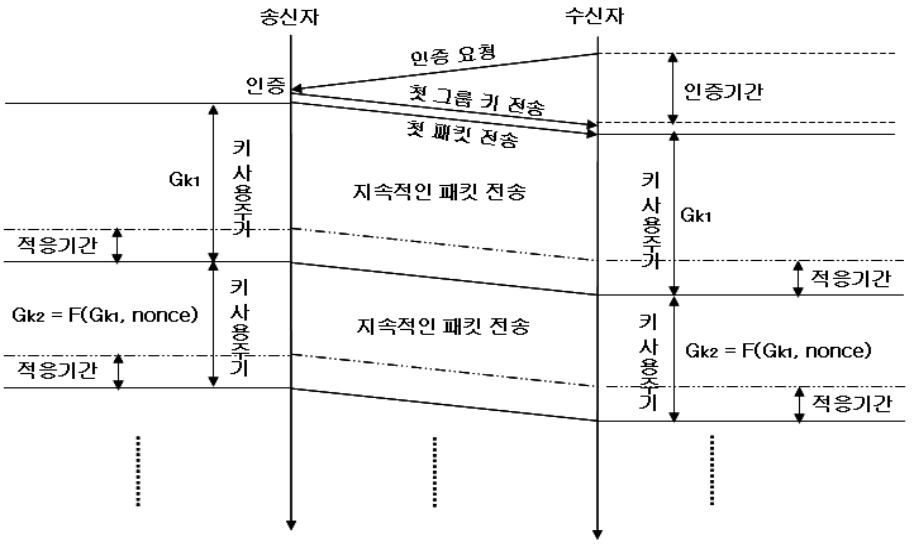
본 논문에서 사용하는 용어는 다음과 같이 정의한다.

G_{k_i} : i 주기 동안 사용되는 그룹 키

F : 해쉬 함수

P_{sqn}: 패킷의 일련번호

T : 한 그룹 키가 사용될 유효 시간을 측정하기 위한 timer값



[그림 6] 제안하는 그룹 키 관리 기법의 플로우

3.1 제안하는 키 관리 기법을 위한 가정

본 논문에서 제안하는 키 관리기법은 보안성을 제공하기 위해 다음과 같이 가정한다.

- 송신자는 수신자를 기존의 인증시스템을 통해 인증한다.
- 키 체인을 구성하기 위한 함수는 일 방향 해쉬 함수를 사용한다.
- 세션 셋업과 멤버의 가입 시 송신자와 수신자는 안전한 채널을 통해 첫 번째 그룹 키를 공유한다.

3.2 키 관리 기법의 플로우

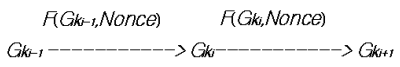
송신자와 수신자간에 안전한 채널을 통하여 첫 번째 그룹 키를 공유한다. 송신자는 다음 키 생성을 위하여 해쉬 함수에 그룹 키와 임시변수 nonce값을 사용한다. 그리고 생성된 그룹 키로 데이터를 암호화하여 수신자에게 전달한다. 수신자는 전달 받은 패킷에서 nonce값과 이전 그룹 키로 다음 그룹 키를 생성하고 그 그룹 키로 암호화된 데이터를 복호화 한다. 제안하는 그룹 키 관리 기법의 전체 플로우는 그림 6과 같다.

3.2.1 키 체인 생성

키 체인은 해쉬 함수 F를 통하여 생성한다.

$$G_{k_i} = F(G_{k_{i-1}}, Nonce) \quad (2)$$

해쉬 함수 F는 다음 주기에 사용될 그룹 키를 생성하기 위하여 현재의 그룹 키와 nonce값을 key material로 사용한다. 키 체인을 이용한 그룹 키 생성과정은 아래 그림 7과 같다.



[그림 7] 그룹 키 생성 과정

여기서 nonce값은 해쉬 함수를 통해 생성되는 그룹 키의 안정성을 높이기 위해 사용된다. nonce값은 매번 패킷 전달이 될 때 송신자로부터 수신자로 전달이 되지만 실제로 그룹 키 생성을 위한 유효 값은 그룹 키 갱신되기 직전에 전달이 된다.

가. 송신자 키 체인 생성

송신자 키 체인 생성을 살펴보면 우선 첫 번째 그룹 키는 송신자와 수신자간에 안전한 채널을 통해 공유한다고 가정한다. 그리고 해쉬 함수를 사용하여 주기적으로 그룹 키를 갱신한다. 송신자는 전체 키 체인을 생성하거나 전송할 데이터가 발생할 때 마다 새로운 그룹 키를 생성한다. 여기서 그룹 키는 사용주기에 따라 주기적으로 갱신한다.

나. 수신자 키 체인 생성

수신자 키 체인은 송신자와 동일한 해쉬 함수를 사용하여 생성되며 그룹 키 생성에 필요한 nonce값은 송신자

로부터 전달받게 된다. 수신자는 전체 키 체인을 생성하는 것이 아니라 Forward secrecy보장을 위하여 새로운 그룹 키 사용주기 직전에 다음 그룹 키를 생성한다.

3.2.2 그룹 키 관리

안전한 그룹 키 관리를 위해서는 키 갱신이 필요하다. 키 갱신은 사용 주기가 만료 되거나 그룹에 속한 멤버가 그룹을 탈퇴할 경우에 발생한다. 송신자와 수신자는 정해진 timer값 T동안 그룹 키를 사용하며 T가 일정한 값 이하로 감소하면 멤버는 새로운 그룹 키 생성을 위한 단계로 들어간다. 이런 과정은 세션이 끝날 때까지 반복이 된다. 여기서 그룹 키 생성 시간에 따른 지연을 최소화하기 위하여 적응기간을 둔다.

가. 주기적인 그룹 키 갱신

그룹 키는 주기적인 갱신을 위한 일정한 사용기간을 갖는데 이것을 그룹 키 사용주기라 한다. 여기서 그룹 키의 사용주기는 시간이 아닌 전송 될 데이터의 양으로 계산된다. 그룹 키의 사용주기 계산을 위해 송신자는 T를 설정한다. 송신자는 매번 데이터를 전송한 후 T를 감소하며 수신자는 매번 데이터를 받고 T를 감소시킨다. 초기 T설정은 송신자 측에서 일정한 값으로 정하거나 임의의 값으로 매번 다르게 할 수도 있다. T가 0이 되면 송신자는 새로운 그룹 키로 데이터를 암호화하여 전송하고 T를 다시 설정한다. 수신자는 송신자로부터 전달된 패킷을 받지 못할 경우 T와 P_{sqn}을 통해 패킷 손실 여부를 확인할 수 있다.

나. 새로운 멤버 추가

그룹에 join을 원하는 수신자는 인증 서버를 통해 사용자 인증과정을 거친 후, 첫 번째 packet을 복호화 할 수 있는 그룹 키를 전달 받는다. 이는 송신자와 수신자간에 세션이 연결될 때 안전한 채널을 통한 첫 번째 그룹 키를 공유과정과 동일하다. 멤버는 첫 번째 그룹 키를 통해 수신된 packet을 복호화 하여 데이터와 T를 획득한다.

다. 멤버의 그룹 탈퇴

그룹 탈퇴를 원하는 멤버는 탈퇴 전에 그룹 탈퇴 메시지를 송신자에게 전송한다. 송신자는 수신자의 그룹 탈퇴 메시지를 받으면 해당 멤버를 그룹에서 탈퇴시키고 전 그룹 키와 새로운 nonce값으로 다음 그룹 키를 만든다. 그리고 T를 설정하고 새로운 그룹 키 생성에 사용된 nonce값과 함께 packet에 포함하여 멤버에게 전송한다. 수신자는 전달받은 패킷에서 T를 확인한 후 수신한 nonce값과 이전 그룹 키로 새로운 키를 생성하게 된다.

4. 성능평가

본 논문에서는 성능 평가를 위해 GKMP/OFT 프로토콜과의 Storage cost, Communication cost, Computation cost의 세 가지 요소를 바탕으로 효율성을 비교 분석한다. 멀티캐스트 환경을 고려한 비교를 위해 m명의 멤버에 주기적인 인증 및 키 갱신이 일어난다고 가정하며, 또 키 갱신 주기는 Service Lifetime의 만료시점으로 가정한다.

4.1 Storage cost 분석

각 그룹키 저장 개수를 비교한 표로 GKMP는 송신자 1명과 수신자가 n명의 각각의 멤버와 비밀키를 공유하여야 함으로 n + 1개의 키가 필요하며, 수신자는 자신과 송신자와의 키만을 가지고 있으면 되기 때문에 2개만을 요구하게 된다. OFT의 경우는 차수 감소로 인해 송신자는 약 2배정도 늘어나게 되며, 수신자는 각 그룹의 키의 루트노드부터 자식노드까지 1/2배씩 감소함으로 인해 킷값이 줄어들게 된다.

하지만 제안하는 시스템은 송수신자 모두 2개의 키만 유지되고 있으면 가능하기 때문에 Storage cost가 매우 적다.

[표 1] Storage cost 비교

프로토콜	키 갯수	
	송신자	수신자
GKMP	n+1	2
OFT	2n - 1	$\log_2 n+1$
제안하는 시스템	2	2

4.2 Communication cost 분석

수신자에 대한 인증과 키 갱신을 위해 교환되는 메시지에 대한 cost로 수신자의 가입 및 탈퇴 시에 실시간적으로 적용할 수 있는 주요요소이다.

[표 2] Communication cost 비교

프로토콜	키 갱신 메시지 갯수	
	수신자 가입	수신자 탈퇴
GKMP	2	n-1
OFT	$2\log_2 n+2$	$\log_2 n+1$
제안하는 시스템	2	1

각각의 키 갱신 메시지는 같은 길이의 암호키로 구성되기 때문에 키 갱신 메시지 횟수에 비례되며, GKMP의 경우 새로운 수신자가 그룹 가입시에 2개의 메시지가 필요하지만, 그룹 탈퇴시는 n-1명의 키 갱신 메시지가 필요하기 때문에 적합하지 못하다. OFT의 경우는 가입 탈퇴시 모든 멤버에게 키 갱신 메시지를 전송하기 때문에 메시지의 양이 많다. 하지만 제안하는 시스템은 가입시 인증확인 메시지인 Auth reply 메시지와 멤버에게 첫 번째 그룹키 수신 확인 메시지인 Key received 2개의 메시지만 필요하다. 반대로 탈퇴 시에는 그룹키 갱신을 위해 timer 값과 nonce 값을 포함한 메시지만 필요하게 된다.

4.3 Computation cost 분석

[표 3] Computation cost 비교

프로토콜		GKMP	OFT	제안하는 시스템
멤버	송신자	$2T_c$	$(2\log_2 n+2)\times(T_c+T_h)$	(T_d+T_h)
	최고값	T_d	$(\log_2 n+1)\times(T_c+T_h)$	(T_d+T_h)
	평균값	T_d	$2(T_d+T_h)$	T_d

암복호화에 소비되는 시간으로, 암호화에 소비되는 시간을 T_c, 복호화에 소비되는 시간을 T_d, 단방향 해쉬함수에 수행되는 시간을 T_h로 표기한다. 암복호화에 걸리는 비용은 통신비용에 암호화 시간 또는 복호화 시간을 곱한 것과 같다.

5. 결론

본 논문에서는 키체인 기법을 활용하여 기존의 그룹키 관리 프로토콜을 개선함으로 인해 멀티캐스트 데이터 전송 효율을 향상시키고, 데이터 중에 Key가 노출 상황을 배제함으로 인해 안전성을 높일 수 있는 알고리즘을 제안하였다. 이는 송수신자와의 오버헤드를 최소화 시킴과 동시에 양방향 인증을 수행하고, 전송되는 데이터의 기밀성 또한 보장할 수 있다. 따라 대용량의 실시간스트리밍 서비스인 화상 회의, 인터넷 방송, 온라인 게임과 같은 대규모 데이터를 여러 사용자에게 동시에 안전하게 전송할 수 있다.

향후 그룹 키 사용을 위한 사용주기 설정 및 패킷 손실 처리 등에 대한 세부 알고리즘에 관한 연구가 필요하다. 또한 제안하는 키 관리 기법과 선행 연구와의 성능평가 및 비교 분석을 통해 키 체인을 이용한 그룹 키 사용의 우수성을 입증할 필요가 있다.

참고문헌

[1] Canetti, R., Garay, J., Itkis, G., Micciancio, D., Naor, M. and Pinkas, B., "Multicast security: a taxonomy and some efficient constructions," IEEE INFOCOM 99, pp. 708-716, 1999.

[2] D. Kosiur, IP Multicasting : The Completer Guide to Interactive Corporate Networks, John Wiley & Sons, Inc., 1998.

[3] Moyer MJ, Rao JR, Rohatgi P., "A Survey of Security Issues in Multicast Communications," IEEE Network, V.13 N.6, pp. 12~23, 1999.

[4] Perring, A., Song, D., Canetti, R., Tygar J. D., Briscoe, B., "Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction," RFC 4082, June 2005.

[5] H.Harney and C. Muckenhirn, "Group Key Management Protocol(GKMP) Specification,", Request for Comments 2093, July 1997.

[6] Alan T. Sherman and David A. McGrew, "Key Establishment in Large Dynamic Groups using One Way Function Trees," IEEE Trans. on Software Engineering, Vol.29, No.5, pp. 444-458, 2003.

[7] T. Hardjono, "Key Management Framework for IP Multicast Infrastructure Security," IS&N99, LNCS 1597, 1999.

[8] 임효준, 김종권, "계층 비디오 멀티캐스트를 위한 효율적인 키 분배 방법", 정보과학회 논문지, 제27권 4호, pp. 476~481, 2000.

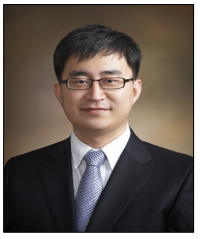
[9] 홍종준, "PIM-SM 정보 보안을 위한 멀티캐스트 그룹 키 관리 프로토콜 설계", 한국 인터넷 정보학회 논문지, 제3권 5호, pp. 87~94, 2002.

김 보 승(Bo-Seung Kim) **[정회원]**

- 2002년 2월 : 영동대학교 컴퓨터공학과 졸업 (공학사)
- 2004년 8월 : 숭실대학교 컴퓨터학과 졸업 (공학석사)
- 2005년 3월 ~ 현재 : 숭실대학교 컴퓨터학과 박사과정

<관심분야>
멀티캐스트, IPTV, 센서네트워크, IPv6, DNS, 홈네트워크

김 정 재(Jeong-Jai Kim) **[정회원]**



- 1999년 2월 : 영동대학교 컴퓨터공학 졸업 (공학사)
- 2001년 2월 : 숭실대학교 컴퓨터공학과 졸업 (공학석사)
- 2005년 8월 : 숭실대학교 컴퓨터공학과 졸업 (공학박사)

<관심분야>
암호학, DRM, RFID/USN, 네트워크 보안

이 기 영(Ki-Young Lee) **[정회원]**

- 2004년 2월 : 관동대학교 컴퓨터공학과 졸업 (공학사)
- 2008년 8월 : 숭실대학교 컴퓨터학과 졸업 (공학석사)
- 2009년 7월 ~ 현재 : 에스넷시스템(주) 연구원(과장)

<관심분야>
멀티캐스트, IPv6, RFID/USN, 네트워크 보안

신 용 태(Yong-Tae Shin) **[정회원]**

- 1985년 2월 : 한양대학교 산업공학과 졸업 (공학사)
- 1990년 12월 : Iowa대학교 전자계산학과 졸업 (공학석사)
- 1994년 5월 : Iowa대학교 전자계산학과 졸업 (공학박사)
- 1995년 3월 ~ 현재 : 숭실대학교 컴퓨터학부 교수

<관심분야>
멀티캐스트, IPv6, RFID/USN, 네트워크 보안