論文2003-40TC-1-2

그룹키를 이용한 보안 멀티캐스트 시스템에서 최소 비용을 위한 Rekey Interval 할당에 관한 연구

(Efficient Rekey Interval for Minimum Cost on Secure Multicast System using Group Key)

李 九 淵 *, 李 庸 **

(Goo Yeon Lee and Yong Lee)

요 약

본 논문에서는 그룹키를 이용하는 보안 멀티캐스트 환경에서 그룹키 노출로 인한 정보손실과 그룹키 재분배의 과정에 대하여 연관지어 설명한다. 또한 손실된 정보에 대한 비용과 키 갱신에 소요되는 비용의 관계를 결합하여 최소의 비용을 갖는 최적의 rekey interval을 분석한다. 본 분석의 결과를 이용하면 그룹키 재분배에 있어서 비용적인 면을 효율성의 척도로 하여, 회원수, 회원의 보안 능력 및 탈퇴율등을 반영하여 rekey interval을 구함으로서 최소비용으로 그룹을 관리할 수 있다. 이러한 효율적인 rekey interval 할당에 대한 연구는 지금까지 크게 중요시되지 않던 부분이었으나 rekey interval 할당에 대한 문제를 현재보다 개선하고 보완한다면, 보안 멀티캐스트 그룹의 확장성과 활용성을 증가시킬 수 있을 것이다.

Abstract

In this paper, we investigate a rekey mechanism for a secure multicast group communications and relate the mechanism to the loss of information from group key exposal. We also combine cost for the information loss and cost for group key updates and analyze the optimum rekey interval. Using the results of the analysis in this paper, we can manage a secure multicast group efficiently with the minimal cost on the bases of number of group members, each member's security level and withdrawal rates.

Keywords : group key, secure multicast, rekey interval

I. 서 론

최근 들어, 인터넷을 통한 그룹간 통신은 화상회의나 인터넷 공동작업과 같은 용도로 급속하게 증가하고 있다. 멀티캐스트 통신은 이러한 그룹간 통신을 효율적으로 처리하기 위해 나타난 기술로, 일대다 및 다대다 간의 통신을 지원함으로서, 유니캐스트나 브로드캐스트통신의 단점을 보완하고 있다. 멀티캐스트 통신은 많은 경우에 인터넷을 통해 이루어지고 있으며, 인터넷상에서의 멀티캐스트 그룹의 가입 및 탈퇴와 멀티캐스트 라우팅 같은 그룹관리 활동은 IGMP(Internet Group Management Protocol) 및 MOSPF(Multicast Open Shortest Path First)등의 프로토콜에 의해 이루어진다. 하지만,

* 正會員, 江原大學校 工科大學 電氣電子情報通信工學部 (Dept. of Information and Telecommunications Kangwon National University)

** 正會員, 韓國情報保護振興院 電子署名認證管理센터 (Korea Certification Authority Central Korea Information Security Agency)

接受日字:2002年4月19日, 수정완료일:2002年12月9日

이러한 멀티캐스트 통신 그룹은 회원의 가입 및 탈퇴가 자유로운 상태로 여러 가지의 측면에서 데이터 보안에 취약한 점을 보인다.

보안 멀티캐스트 환경이란, 하나의 그룹키를 사용하여 특정 멀티캐스트 그룹 회원들에게 보내어지는 메시지를 암호화함으로서, 멀티캐스트 통신을 보호받는 것으로, Iolus 나 GKMP(Group Key Management Protocol) 등의 많은 연구가 있었다[1-3].

보안 멀티캐스트 환경에서 그룹의 전체적 관리는 그룹 컨트롤러(Group Controller, 이하 GC)가 맡고 있다. 즉 GC는 그룹회원의 가입 및 탈퇴 그리고, 그룹키의 관리를 담당한다. GC는 일정시간간격(rekey interval)을 두고 그룹키로 사용될 새로운 키를 생성하여 각각의 그룹회원들에게 전달해 준다. 또한 새로운 회원의 탈퇴가 이루어지게 되면, 같은 과정을 통해 새로운 그룹키를 분배하게 된다. 새로운 그룹키의 할당은 같은 키를 장시간 사용했을 때 나타날 수 있는 키의 노출을 방지하고, 탈퇴한 회원이 악의적으로 그룹키를 노출시키는 것을 방지하기 위해서이다.

본 논문에서는 이러한 보안 멀티캐스트 환경에서 요구되는 그룹키의 rekey interval에 대하여, 그룹키를 만들고 배포하는데 걸리는 비용과 그룹의 보안성을 유지함으로서 얻을 수 있는 비용을 그룹의 회원 수와 공격에 의한 피해정도를 통해 효과적으로 할당하는 방법을 제시하고 있다.

본 논문의 구성은 다음과 같다. 서론에 이어 2장에서는 기술적 배경을 설명하고 3장에서는 rekey interval 결정시 고려사항을 기술한다. 4장에서는 최적의 rekey interval을 분석하며 5장에서는 그 결과를 분석한다. 이어 6장에서 결론을 맺는다.

Ⅱ. 기술적 배경

멀티캐스트 통신에서 멀티캐스트 통신 그룹의 보안성을 보장하는 보안 멀티캐스트 환경의 예로, 대표적인 프로토콜에 GKMP가 있다. 이 프로토콜의 기본적인 구조는, 그룹 내에 하나의 대칭 키를 생성하고, 그 키를 통신주체인 그룹 회원들에게 분배함으로서, 대칭 키를 이용한 안전한 암호화 통신을 할 수 있도록 하는 것이다. 키를 생성하는데는 RSA, Diffe-Hellman, elliptic curves 등의 다양한 알고리즘을 사용하며, 그룹 내 통신은 대등한 관계(peer-to-peer)로 이루어진다. 여기서, GC는 처음 그룹을 만드는 회원과 그룹생성과정을 거쳐 그룹을 구성하고, 키 생성, 키 분배, 회원 관리, rekey 및 그룹의 모든 상황 진행에 대한 처리를 수행한다.

Rekey interval이란, 그룹키를 생성, 배포하여 사용 후, 새로운 그룹키가 생성, 배포되기까지의 그룹키 사용 기간을 말하는 것으로, 새로운 그룹키를 생성, 배포하는 주기를 말한다. 정해진 rekey interval에 의해서 이루어지는 rekey는 그룹 회원의 가입탈퇴와 같은 특별한 사건이 발생하지 않는 한 정해진 주기에 의해 이루어진다. 한 주기가 끝나고 rekey 과정을 거쳐 새로운 그룹키를 분배하는 방법은 처음 그룹이 만들어지는 과정과 흡사하게 이루어진다. 즉, 특정 그룹회원과 GC는 새로운 그룹키를 생성하여, 그룹회원들에게 전달해주게 된다. 이 때, 새로 분배되는 그룹키와 함께 rekey interval도 전달된다.

GKMP에서 이렇게 주기를 두어 그룹키를 바꾸어주는 이유는, 대칭 키를 이용한 암호화통신방식에서 세션키를 바꾸는 것과 같은 이유다. 세션키를 이용한 암호화 통신에서 세션키를 자주 변경하여 교환할수록 더욱 더 높은 안전성을 주게 되는데, 그 이유는 주어진 하나의 세션키에 대해서 공격자가 사용할 수 있는 암호문의 수가 적어지기 때문이다[4]. 그러나 키 변경의 단점은 키 분배 작업이 정보의 교환을 지연시키고, 네트워에 부담을 준다는 것이다[4]. 따라서, 그룹키 사용기간을 정하는데 있어 그룹의 안전성과 네트워 트래픽을 고려하는 것은 중요한 문제라 하겠다.

Ⅲ. Rekey Interval 결정에서 고려사항

Rekey interval을 결정하는데, 고려해야 할 대표적 요소에는 크게 다음의 네 가지를 들 수 있으며, 이들은 서로 연관성을 갖는다.

첫 번째로, 그룹의 규모. 즉, 회원 수를 들 수 있다. 그룹에 포함된 각각의 회원들은 GC에 의해 새로운 키가 분배될 때마다 새로운 키 패킷을 받고, 복호화 하는 계산상의 오버헤드가 생긴다. 이는 회원의 컴퓨터에서 실행되는 딜레이에 민감한 응용프로그램과 제한된 자원하에 실행되는 응용프로그램에 영향을 줄 수 있는 요소로 그 중요성을 지닌다[5]. 이러한 이유로 나타나는 다양한 피해는 사용자에게 비용적인 손해를 가져올 수 있으며, 이로 인한 손실은 그룹 전체 회원으로 계산될 때, 회원 수와 정비례 관계로 늘어나게 된다. 또한 위와 같

은 계산적인 오버헤드는 회원들에서 뿐 아니라, GC가 키를 만들고, 암호화하여 전달하는 과정에도 같은 영향을 미친다. Rekey interval이 짧아져 자주 rekey가 일어나면, 위의 손실은 급속히 증가하게 된다.

두 번째로, 그룹의 다이나믹성. 즉, 그룹 회원들의 단위시간당 가입탈퇴 횟수를 들 수 있다. 이 요소는 첫 번째에서 설명한 그룹의 규모와도 정비례의 관계를 가지고 있는 것으로 회원의 수가 많아질수록 회원의 가입탈퇴 횟수도 같이 증가하게 된다. 가입과정에서 GC는 새로운 회원이 가입요청을 하면, 회원가입 과정을 거쳐 가입한 회원에게 그룹키를 분배하고, 그룹회원정보를 갱신하게 된다. 탈퇴과정의 경우, GC는 탈퇴회원의 기록을 삭제하고, 나머지 회원들에게 새로운 그룹키를 분배하여 새로운 그룹회원을 구성해야 한다. 이러한 회원 가입, 탈퇴 빈도가 rekey interval 할당에 있어 중요한 요소가 되는 이유는, 회원탈퇴에 의한 rekey의 빈도가 rekey interval에 의한 주기적인 rekey의 빈도보다 높을 경우, rekey interval을 정하는 의미 자체가 약해지기 때문이다.

셋째로, 보안강도. 즉, 그룹 내에서 다루는 정보의 가치가 얼마나 중요한가를 들 수 있다. Rekey interval이 지나치게 긴 경우, 같은 키를 장시간 사용하게 되면서 키의 노출확률은 높아지게 된다. 반대로 rekey interval을 짧게 하여 rekey를 자주 하게 되면, 그 만큼 보안강도를 높일 수 있다. 만일, 그룹에서 주고받는 데이터의 목적이 군사적인 문제와 관련된 것이라면, 그 데이터의 보안강도는 매우 높아야 할 것이다. 반대로, 데이터의 내용이 일반적인 뉴스그룹의 것과 같은 것이라면, 그만큼 보안강도는 낮게 정하여도 무방할 것이다. 보안강도가 높은 정보를 다루는 경우 대부분 그 정보를 공유하는 회원의 수는 적다. 반대로 뉴스그룹처럼 일반적인 정보를 다루는 곳은 많은 회원을 보유하고 있다.

넷째로 네트워 트래픽에 관한 문제도 rekey interval 설정에 영향을 준다. 자주 일어나는 rekey는 네트워 트래픽을 증가시키게 되는데, 이렇게 증가되는 트래픽은 네트워의 자원을 사용한다는 면에서 비용으로 간주되어진다.

Ⅳ. 최적의 rekey interval 분석

본 논문에서 제안하는 rekey interval 할당 방법은, 그룹이 가지고 있는 정보의 가치와 보안 멀티캐스트 환경에서 rekey 과정을 운영하면서 소요되는 비용을 고려하여 제안하고 있다. 즉, 그룹이 보유하고 있는 정보의 노출로 인한 손해 비용과 rekey 과정으로 인한 소요 비용의 합이 최소가 되는 rekey interval T_{rk}를 찾는 것이다.

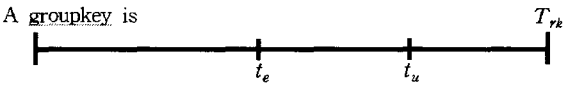


그림 1. Rekey interval 및 그룹키 노출 시점과 그룹회원의 탈퇴 시점을 나타낸 다이아그램

Fig. 1. Timing diagram of rekey interval, group key exposure time and withdrawal time of a member.

<그림 1>은 rekey interval 및 그룹키 노출 시점과 그룹회원의 탈퇴 시점을 나타낸 다이아그램이다. <그림 1>에서의 변수의 정의는 다음과 같다.

T_{rk} : rekey interval.

t_u : 하나의 그룹회원이 그룹으로부터 탈퇴한 시점을 나타내는 랜덤 변수.

t_e : rekey가 이루어진 이후로부터 그룹키가 공격 당하여 노출된 시점을 나타내는 랜덤 변수.

그룹키의 노출은 각 회원의 개인적인 이벤트로서 다른 회원과 독립적으로 발생한다고 볼 수 있으므로 t_e 시점을 지수분포를 따른다고 가정하며 t_u와 t_e의 확률밀도함수를 각각 $f_{t_u}(t)$와 $f_{t_e}(t)$로 정의한다.

다음 rekey 시점은 그룹회원의 탈퇴가 없는 경우 T_{rk}가 되며, 그룹회원의 탈퇴가 있게되면 탈퇴한 회원이 그룹키를 악용할 것이 우려되므로 그 탈퇴시점을 rekey 시점으로 한다. t_{rk} 를 다음 rekey 시점을 나타내는 랜덤 변수라고 하면 식 (1)과 같이 나타낼 수 있다.

$$t_{rk} = \min(t_u, T_{rk}) \tag{1}$$

그룹회원의 신규 가입시점은 사용중인 그룹키를 분배하여 주면 되므로 rekey 시점과는 관계가 없다.

n 을 그룹의 크기 (그룹회원의 수)를 나타내는 랜덤 변수라고 가정하고 n의 기대치를 $E(n)=N$이라 하자. 또 $n \gg 1$ 이라고 가정하고 그룹회원의 탈퇴와 가입이 독립적으로 빈번하게 이루어지고 가입률과 탈퇴율이 같은 평형상태라고 가정하면, central limit theorem[6]에 의해 n은 N의 근방에 존재하게 되므로 본 논문에서는 n을

N 으로 대치하여 분석하기로 한다. 또한 그룹에서의 각 회원의 그룹키를 노출하는 성향이 모두 같다고 가정한다. 그러면 λ와 u를 각각 다음과 같이 정의할 수 있다.

λ : 하나의 그룹회원이 그룹키를 노출하는 정도를 나타내는 노출률

u : 하나의 그룹회원이 그룹으로부터 탈퇴 또는 신규가입 하는 정도를 나타내는 탈퇴(가입)율

그룹키의 노출정도는 그룹회원의 수(N)과 그룹회원의 노출성향(λ)에 비례하므로 t_e의 확률밀도함수인 $f_{t_e}(t)$는 식 (2)와 같이 얻어진다.

$$f_{t_e}(t) = N\lambda e^{-N\lambda t} \tag{2}$$

그룹회원이 그룹으로부터 탈퇴는 다른 회원과 독립적으로 이루어진다고 생각하고, 탈퇴 시점까지의 시간은 지수함수를 따른다고 가정한다. 탈퇴빈도는 그룹회원의 수(N) 과 그룹회원의 탈퇴율(u)에 비례하므로 t_u의 확률밀도함수인 $f_{t_u}(t)$는 식 (3)과 같이 얻어진다.

$$f_{t_u}(t) = Nue^{-Nut} \tag{3}$$

그러면 아래의 식이 성립한다.

$$\begin{aligned} P[t_{rk} < t] &= 1 - e^{-Nut} \quad (t < T_{rk}) \\ P[t_{rk} = T_{rk}] &= e^{-NuT_{rk}} \quad (t = T_{rk}) \end{aligned} \tag{4}$$

A_d를 그룹키의 노출로 인한 노출된 정보량이라고 하자. 어느 시간 구간 동안 전송되는 정보량은 그룹회원의 수와 시간 구간의 크기에 비례하므로 A_d는 기본적으로 N에 비례하고 또 그룹키 노출시점 t_e와 다음 rekey 시점 t_{rk}와의 시간차에 비례하게 된다

실제적으로 그룹의 정보가 노출되는 시기는, t_e 시점 이후부터이기 때문에 <그림 1>과 같이 $t_{rk} - t_e$ 동안 교환되는 모든 메시지는 노출되며, 이 값이 커질수록 그룹의 노출정보량은 커지게 된다. 또한, t_{rk} 시간이 경과한 후에는 새로운 그룹키가 그룹회원들에게 할당되어 그룹의 정보노출은 더 이상 없는 것으로 간주하면, t_e 시점으로부터의 노출 정보량은 다음과 같은 순서로서 얻을 수 있다. 우선 $t_e = t_1, t_{rk} = t_2$ 의 조건하에 A_d 를 구하면 식 (5)와 같다.

$$A_d \mid_{(t_e = t_1,\ t_{rk} = t_2)} = (t_2 - t_1) \cdot N \tag{5}$$

위의 식에서 '|' 는 조건부 계산을 표시한다. 식 (5)를 t_1에 대하여 적분하면 식 (6)이 나온다.

$$\begin{aligned} A_d \mid_{(t_{rk} = t_2)} &= \int_0^{t_2} (t_2 - t_1) \cdot N \cdot f_{t_e}(t_1) dt_1 \\ &= \int_0^{t_2} (t_2 - t_1) \cdot N \cdot N\lambda e^{-N\lambda t_1} dt_1 \equiv K(t_2) \end{aligned} \tag{6}$$

마찬가지로 식 (6)을 t_2에 대하여 적분하면 식 (7)과 같다.

$$\begin{aligned} A_d &= \int_0^{T_{rk}} K(t_2) f_{t_{rk}}(t_2) dt_2 + K(T_{rk}) \cdot e^{-NuT_{rk}} \\ &= \int_0^{T_{rk}} K(t_2) Nue^{-Nut_2} dt_2 + K(T_{rk}) \cdot e^{-NuT_{rk}} \end{aligned} \tag{7}$$

C_G를 그룹회원이 전송하는 정보량과 정보 비용사이의 비례상수라고 하면 그룹키노출로 인한 총 정보손실 비용은 식 (8)과 같다.

그룹키노출로 인한 총 정보손실비용 = $C_G \cdot A_d$. (8)

A_{rk}를 그룹키의 갱신에 따른 네트워 자원 사용량을 나타내는 변수라고 하자. 네트워 자원 사용량은 그룹의 크기와 비례하므로 식 (9)와 같이 나타낼 수 있다.

$$A_{rk} = N \tag{9}$$

C_{rk}를 네트워 자원 사용량과 비용과의 비례상수라고 하면

한번의 그룹키 갱신에 따른 비용 = $C_{rk} \cdot A_{rk}$. (10)

$E(t_{rk})$를 평균 rekey interval 이라고 하면

$$\begin{aligned} E(t_{rk}) &= \int_0^{T_{rk}} t f_{t_{rk}}(t) dt + T_{rk} e^{-NuT_{rk}} \\ &= \int_0^{T_{rk}} t \cdot Nue^{-Nut} dt + T_{rk} e^{-NuT_{rk}} \end{aligned} \tag{11}$$

A_T를 단위시간당 소비되는 총 비용이라고 하면 식 (12)와 같은 식을 얻는다.

$$A_T = \frac{(C_G A_d + C_{rk} A_{rk})}{E(t_{rk})} \tag{12}$$

식 (12)에서 A_T가 최소값을 갖게되는 T_{rk} 값이 최적의 rekey interval 값이 된다.

V. 결과 분석

단위시간당 총 비용 (A_T)의 값은 그룹회원의 수 N, 그룹키의 노출성향 λ, 그룹회원의 탈퇴율 u 및 $\frac{C_G}{C_{rk}}$의 값에 따라 가변적인 값을 갖게 된다. 그러므로 각 요소의 변화에 따른 단위시간당 총 비용 (A_T)의 변화를 <그림 2,3,4> 그리고 <그림 5>에 보였다. 그림으로부터 우리는 단위시간당 총 비용 (A_T)를 최소로 하는 T_{rk}의 값을 구할 수가 있다.

<그림 2>는 임의로 $C_G=1000$, $C_{rk}=1$, $\lambda=10^{-10}$, $u=10^{-7}$ 일 때 N의 변화에 따른 단위시간당 총 비용 (A_T)을 그린 것이다. <그림 2>에서 최적의 rekey interval 이 N이 커짐에 따라 작아지게 되는 것은 N이 커짐에 따라 그룹키의 노출확률이 높아지기 때문이다.

<그림 3>은 임의로 $C_G=1000$, $C_{rk}=1$, $u=10^{-9}$, $N=1000$ 일 때, λ를 10^{-7} 부터 10^{-11}까지 변화시키면서 단위시간당 총 비용 (A_T)을 보인 것이다. 이 곡선에서 A_T가 최소 값일 때의 T_{rk}가 그 조건하의 최적의

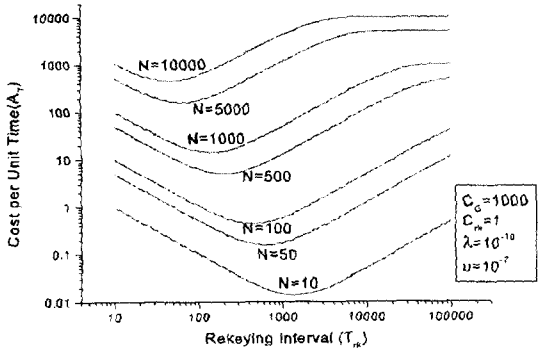


그림 2. $C_G=1000$, $C_{rk}=1$, $\lambda=10^{-10}$, $u=10^{-7}$일 때 N의 변화에 따른 단위시간당 총 비용 (A_T)

Fig. 2. Total cost per unit time A_T at $C_G=1000$, $C_{rk}=1$, $\lambda=10^{-10}$, $u=10^{-7}$ and various values of N.

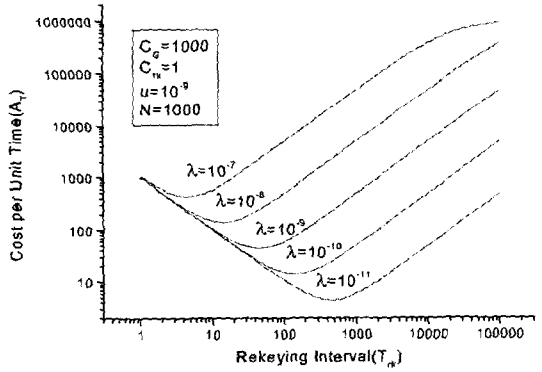


그림 3. $C_G=1000$, $C_{rk}=1$, $u=10^{-9}$, $N=1000$ 일 때 λ 의 변화에 따른 단위시간당 총 비용 (A_T)

Fig. 3. Total cost per unit time A_T at $C_G=1000$, $C_{rk}=1$, $u=10^{-9}$, $N=1000$ and various values of λ.

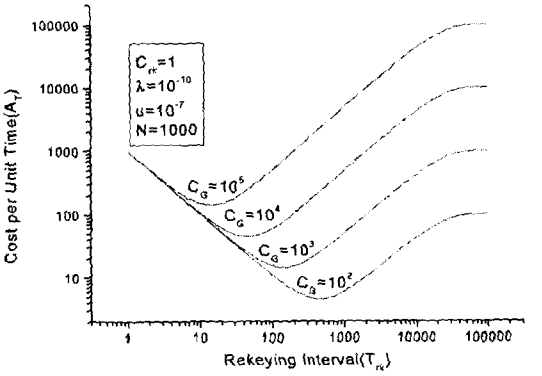


그림 4. $C_{rk}=1$, $\lambda=10^{-10}$, $u=10^{-7}$, $N=1000$ 일 때 C_G 의 변화에 따른 단위시간당 총 비용 (A_T)

Fig. 4. Total cost per unit time A_T at $C_{rk}=1$, $\lambda=10^{-10}$, $u=10^{-7}$, $N=1000$ and various values of C_G.

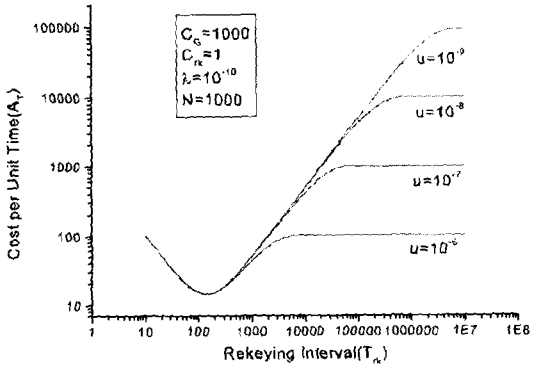


그림 5. $C_G=1000$, $C_{rk}=1$, $\lambda=10^{-10}$, $N=1000$ 일 때 u 의 변화에 따른 단위시간당 총 비용 (A_T)

Fig. 5. Total cost per unit time A_T at $C_G=1000$, $C_{rk}=1$, $\lambda=10^{-10}$, $N=1000$ and various values of u.

rekey interval을 나타내는 것이다. 그림은 λ값이 작아질수록, rekey interval 값이 커짐을 보여주고 있다. 여기서, λ는 그룹의 정보 노출 성향을 나타내는 것으로서, 그룹을 구성하고 있는 회원들의 보안능력에 따라 변화하는 값이다. 즉, 그룹 회원들의 보안능력이 강하다면, T_{rk}를 길게 하고, 그렇지 못하다면 짧게 해야함을 나타내고 있다.

<그림 4>는 임의로 $C_{rk}=1$, $\lambda=10^{-10}$, $u=10^{-7}$, $N=1000$ 일 때 C_G의 변화에 따른 단위시간당 총 비용(A_T)을 그린 것이다. <그림 4>에서 C_G의 값이 커지면 키 갱신 비용보다 노출에 의한 비용이 더 커지므로 rekey interval은 보다 짧아지는 것을 알 수 있다.

<그림 5>는 임의로 $C_G=1000$, $C_{rk}=1$, $\lambda=10^{-10}$, $N=1000$ 일 때 u 의 변화에 따른 단위시간당 총 비용(A_T)을 보인 것이다. 최적의 T_{rk}가 $\frac{1}{u}$ 보다 상대적으로 작은 값에서 결정된 결과로서 이는 그룹회원의 평균 탈퇴 시간 간격이 최적의 T_{rk} 보다 많이 크게 되므로써 최적의 T_{rk}는 주로 그룹키의 노출 성향 λ에의하여 결정이 되어진다. 그러므로 이 그림에서는 단위시간당 총 비용 (A_T)은 u의 변화 범위에 대하여 거의 변화가 없게된다.

위의 그림들에서 우리는 T_{rk}가 무한히 커지면 단위시간당 총 비용 (A_T)이 상수값으로 수렴하는 것을 볼 수 있다. 이것은 rekey intertval을 길게 하면 그룹키의 노출이 먼저 발생하게 되고 그룹키 노출이후 전송되는 모든 정보량은 노출이 되므로 단위시간당 전송하는 모든 정보량이 바로 단위시간당 총 비용이 되기 때문이다. 이것은 T_{rk}를 $\frac{1}{u}$에 비해 아주 길게하면 키 갱신은 T_{rk}에 의하여 일어나기 보다는 대부분 그룹회원의 탈퇴로 인하여 발생하게 되므로 T_{rk}의 변화에 무관하게 상수값을 갖게 됨을 의미한다.

Ⅵ. 결 론

본 논문에서는 그룹키를 이용한 보안 멀티캐스트 환경에서의 그룹키 노출로 인한 정보손실과 그룹키 재분배의 과정에 대하여 연관지어 설명하였다. 또한 손실된 정보에 대한 비용과 키 갱신에 소요되는 비용의 관계를 결합하여 최소의 비용을 갖는 최적의 rekey interval을 분석하였다. 본 분석에서는 그룹키 재분배에 있어서 비용적인 면을 효율성의 척도로 하여, 회원수, 회원의 보안 능력 및 탈퇴율등을 반영하여 rekey interval을 구함으로서 최소비용으로 그룹을 관리할 수 있도록 하였다.

이러한 효율적인 rekey interval 할당에 대한 연구는 지금까지 소홀히 되는 부분이었다. 그러나, rekey interval 할당에 대한 점을 현재보다 개선하고 보완한다면, 보안 멀티캐스트 그룹의 확장성과 활용성을 증가시킬 수 있을 것이다.

참 고 문 헌

[1] H. Harney, and C. Muckenhirn, "Group Key Management Protocol (GKMP) Specification". RFC 2093, July 1997.

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

[3] Suvo Mittra, "Iolus : A Framework for Scalable Secure multicasting", Proceedings of the ACM SIGCOMM '97, Secptember 14~18, 1997.

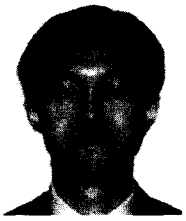
[4] William Stallings, Cryptography & Network Security : Principles & Practice 2nd edition, Prentice Hall, 1998.

[5] Sanjeev Setia, Samir Koussih, Sushil Jajodia, Eric Harder, "Kronos : A Scalable Group Re-Keying Approach for Secure Multicast", Proc. of 2000 IEEE Computer Society Symposium on Research in Security and Privacy, 2000.

[6] W. B. Davenport, Jr., Probability and Random Processes, McGraw-Hill. 1970.

[7] D. Balenson, D. McGrew, A. Sherman, "Key Management for Large Dynamic Groups : One-Way Function Trees and Amortized Initialization", Internet Draft, draft-irtf-smug-groupkeymgmt-oft-00.txt, August 2000.

저 자 소 개



李 九 淵(正會員)

1988년 : KAIST 전기및전자공학과 (석사). 1993년 : KAIST 전기및전자공학과(박사). 1993년~1996년 : 디지콤정보통신연구소. 1996년 : 삼성전자. 1997년~현재 : 강원대학교 전기및전자공학부 부교수

李 庸(正會員)

1997년 : 연세대학교 컴퓨터과학과 (석사). 2001년 : 연세대학교 컴퓨터과학과(박사). 1993년~1994년 : 디지콤 정보통신 연구소 연구원. 2001년~현재 : 한국정보보호진흥원 전자서명인증관리센터 선임연구원.