산업기술연구(강원대학교 산업기술연구소 논문집), 제21권 A호, 2001.
Journal of Industrial Technology, Kangwon Nat'l Univ.,Korea, No. 21 A, 2001.

보안 멀티캐스트 환경에서 최소비용을 위한 효과적인 Rekey Interval 할당에 관한 연구

The Study of Efficient Rekey Interval Allotment for Minimum Cost on Secure Multicast

박 진 영* 이 구 연** 이 용***
Baag, Jin-Young Lee, Goo-Yeon Lee, Yong

Abstract

This paper proposed for allotment of group key's rekey interval required from secure multicast environment. New group key distribution occurs in two cases: one is periodical update and the other is permitted or unpermitted withdrawal of group member. In later case, the group controller distributes new group key to member except withdrawal member because it can't predict precisely. In former case, the group member who created the group can adjust the rekey interval. Using relation between security level, overhead and cost from rekey interval, this paper suggests effective rekey interval allotment through probable performance analysis in large dynamic group.

키워드 : *보안 멀티캐스트, 그룹 키*
Keywords : *secure multicast, group key, rekey interval*

1. 서 론

최근 들어, 인터넷을 통한 그룹간 통신은 화상회의나 인터넷 공동작업과 같은 용도로 급속하게 증가하고 있다. 멀티캐스트 통신(multicast communication)은 이러한 그룹간 통신을 효율적으로 처리하기 위해 나타난 기술로, 일대다 및 다대다 간의 통신을 지원함으로서, 유니캐스트(unicast)나 브로드캐스트(broadcast) 통신의 단점을 보완하고 있다. 멀티캐스트 통신은 일반적으로 인터넷을 통해 이루어지고 있으며, 멀티캐스트 그룹의 가입 및 탈퇴와 같은 그룹관리 활동은 IGMP (Internet Group Management Protocol)에 의해 이루어진다.

하지만, 이러한 멀티캐스트 통신 그룹은 데이터를 받는 수신자가 멀티캐스트 그룹에 가입 및 탈퇴가 자유로운 상태로, 통신 데이터 보안에 취약한 점을 보인다.

보안 멀티캐스트 환경이란, 하나의 그룹 키(group key)를 사용하여 특정 멀티캐스트 그룹 회원들에게 보내어지는 메시지를 암호화함으로서, 멀티캐스트 통신을 보호받는 것으로, Iolus 나 GKMP (Group Key Management Protocol) 등 의 많은 연구가 있었다 [1][3][6].

보안 멀티캐스트 환경에서 그룹의 전체적 관리와 그룹회원의 가입 및 탈퇴 그리고, 그룹 키의 관리는 그룹 컨트롤러(Group Controller, 이하 GC)가 맡고 있으며, GC는 일정시간간격을 두고 그룹 키로 사용 될 새로운 키를 생성하여 rekey과정을 통해 각각의 그룹회원들에게 전달해 주게된다. 또한 새로운 회원의 가입 및 탈퇴가 이루어지게 되면, 같은 과정을 통해 새로운 그룹 키를 분배하게 된다. 새로운 그룹 키의 할당은 같은 키를 장시간 사용했을 때 나타날 수 있는 키의 노출을 방지하고, 탈퇴한 회원이 악의적으로 그룹 키를 노출시키는 것을 방지하기 위함으로서, 그룹 내 보안 환경을 보호하는데 그 목적이 있다.

* 강원대학교 대학원 컴퓨터정보통신공학과 석사과정
** 강원대학교 컴퓨터정보통신공학과 교수, 공학박사
*** 한국정보보호센터

본 논문에서는 이러한 보안 멀티캐스트 환경에서 요구되는 그룹 키의 rekey interval에 대하여, 그룹 키를 만들고 배포하는데 걸리는 비용과 그룹의 보안성을 유지함으로서 얻을 수 있는 비용을 그룹의 회원 수와 공격에 의한 피해정도를 통해 효과적으로 할당하는 방법을 제시하고 있다. 서론에 이어 제 2장에서는 보안 멀티캐스트 환경을 위해 연구되어진 프로토콜의 기본적인 사항을 설명하며, 제 3장에서는 rekey interval할당에 있어 고려해야 할 사항과 효과적인 할당 방법에 대해 설명한다. 그리고, 마지막으로 제 4장에서 결론을 맺는다.

2. 기술적 배경

본 장에서는 보안 멀티캐스트 환경에 대한 대략적인 설명과 보안 멀티캐스트 환경에서 rekey interval의 역할과 현재의 문제점에 대해 알아보고, 효과적인 할당 방법을 제안한다.

2.1 보안 멀티캐스트 환경

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 회원(*member*)들에게 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 회원(first member)과 그룹생성과정을 거쳐 그룹을 구성하고, 키 생성, 키 분배, 회원 관리, rekey 및 그룹의 모든 상황 진행에 대한 report를 맡아서 처리한다.

GKMP에서 *rekey interval*의 설정은 처음 그룹 생성을 요청하는 회원이 정하여, GC에게 알려주게 되는데, 아직까지 그 설정방법에 대한 정확한 규정은 되어있지 않고 있다.

2.2 Rekey Interval

Rekey interval이란, 그룹 키를 생성, 배포하여 사용 후, 새로운 그룹 키가 생성, 배포되기까지의 그룹 키 사용 기간을 말하는 것으로, 새로운 그룹 키를 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 그룹 키를 분배하는 방법은 처음 그룹이 만들어지는 과정과 흡사하게 이루어진다. 즉, 특정 그룹회원과 GC는 새로운 그룹 키를 생성하여, 그룹회원들에게 전달해주게 된다. 이때, 새로 분배되는 그룹 키와 함께 rekey interval도 전달된다.

최초 그룹을 생성하는 과정과 새로운 그룹 키를 분배하는 rekey과정은 그림 1과 그림 2에 나타나 있다[1].

GKMP에서 이렇게 주기를 두어 그룹 키를 바꾸어주는 이유는, 대칭 키를 이용한 암호화통신방식에서 세션 키(session key)를 사용하는 것과 같은 이유다.

세션 키는 자주 변경하여 교환할수록 더욱 더 높은 안전성을 주게 되는데, 그 이유는 주어진 하나의 세션 키에 대해서 공격자가 사용할 수 있는 암호문이 적어지기 때문이다 [5].

그러나, 이러한 장점 이외에 세션 키의 단점은 세션 키 분배 작업이 정보의 교환을 지연시키고, 네트워크에 부담을 준다는 것이다 [5]. 이러한 점은 세션 키에서 뿐 아니라, 그룹 키의 rekey 과정에서도 같은 결과를 가져온다. 따라서, 그룹 키 사용기간을 정하는데 있어 그룹의 안전성과 네트웍 트래픽(network traffic)을 고려하는 것은 중요한 문제라 하겠다.

3. 효과적인 ReKey Interval 할당

3.1 Rekey Interval 결정에서 고려사항

Rekey interval을 결정하는데, 고려해야 할 대표적 요소에는 크게 다음의 세 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 KP(Key Packet)를 받고, 복호화 하는 계산적인 오버헤드(computational overhead)가 생긴다. 이는 회원의 컴퓨터에서 실행되는 딜레이에 민감한 응용프로그램과 제한된 자원 하에 실행되는 응용프로그램에 영향을 줄 수 있는 요소로 그 중요성을 지닌다[2]. 이러한 이유로 나타나는 다양한 피해는 사용자에게 비용적인 손해를 가져올 수 있으며, 이로 인한 피해액은 그룹 전체 회원으로 계산될 때, 회원 수와 정비례 관계로 늘어나게 된다. 또한 위와 같은 계산적인 오버헤드는 회원들에서 뿐 아니라, GC가 키를 만들고, 암호화하여 전달하는 과정에도 같은 영향을 미친다.

Re-keying interval이 짧아져 자주 re-key가 일어나면, 위의 피해가 일어날 확률은 급속히 증가하게 된다.

두 번째로, 그룹의 다이나믹성. 즉, 그룹 회원들

의 단위시간당 가입탈퇴 횟수를 들 수 있다. 이 요소는 첫 번째에서 설명한 그룹의 규모와 정비례의 관계를 가지고 있는 것으로 회원의 수가 많아질수록 회원의 가입탈퇴 횟수도 같이 증가하게 된다.

가입과정에서 GC는 새로운 회원이 가입요청을 하면, Member join 과정을 거쳐 가입한 회원에게 그룹 키를 분배하고, 그룹회원정보를 갱신하게 된다. 탈퇴과정은 두 가지로 나눌 수 있다. 한 가지는 허가 된 탈퇴로서 회원은 GC에게 탈퇴요청을 하게되면, 그 메시지를 받은 GC는 탈퇴하는 회원의 키를 파괴하고 그룹회원정보에서 탈퇴한 회원을 삭제하게 된다. 다른 하나는 불허된 탈퇴로서 이러한 겨우, GC는 탈퇴회원의 기록을 삭제하고, 나머지 회원들에게 새로운 group key를 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.

위에서 나열한 세 가지 요소 이외에, 네트웍 트래픽에 관한 문제도 rekey interval 설정에 영향을 준다. 자주 일어나는 rekey는 네트웍 트래픽을 증가시키게 되는데, 이렇게 증가되는 트래픽은 실제로 전달되어야하는 데이터의 측면에서 본다면 오버헤드가 된다.

지금 까지 rekey interval을 결정하는데 고려해야 할 사항들에 대해 설명하였다. 위에서 설명한 요소들을 적절히 이용하여 rekey interval을 설정한다면 효과적인 rekey interval 할당이 가능하게 된다.

이러한 rekey interval 할당에 관한 문제는 GKMP와 같이 중앙의 GC가 모든 회원들을 관리하는 경우나 Iolus 와 같이 그룹을 계층적으로 나누어 서브 그룹을 두고 관리하는 경우 모두에 해당한다.

3.2 제안하는 할당방법

본 논문에서 제안하는 rekey interval 할당 방법은, 그룹이 가지고 있는 정보의 가치와 보안 멀티캐스트 환경에서 rekey 과정을 운영하면서 소요되는 비용(cost)을 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.

T_{rk} 시간동안 그룹이 정보를 노출 당할 수 있는 확률이 지수분포(exponential distribution)를 따른다고 가정하고, T_{rk} 중 공격당하는 시점을 t라 한다.

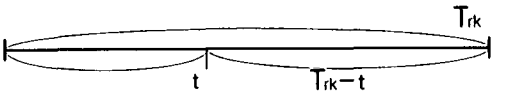

그림 1 T_{rk} 기간 중, 공격시점 t 와 공격시간 $T_{rk}-t$

그렇다면, t 라는 시점에서 확률밀도함수(Probability Density Function, PDF)는, $f_X(x)=\lambda e^{-\lambda x}$ 의 지수함수의 PDF 값에 따라 그룹의 회원 수 N과 비례함을 고려하여, (식 3.1)과 같이 나타낼 수 있다.

$$f(t)=N\lambda e^{-N\lambda t} \qquad \text{(식 3.1)}$$

실제적으로 그룹의 정보가 노출되는 시기는, t 시점 이후부터이기 때문에 그림 1과 같이 $T_{rk}-t$ 로 타나낼 수 있으며, 이 값이 커질수록 그룹의 손실은 커지게 된다. 또한, T_{rk} 시간이 경과한 후에는 새로운 그룹 키가 그룹회원들에게 할당되어 그룹의 정보손실은 더 이상 없는 것으로 전제하면, (식 3.2)와 같이 나타낼 수 있다.

$$f(t)=(T_{rk}-t)N\lambda e^{-N\lambda t} \qquad \text{(식 3.2)}$$

따라서, (식 3.2)를 0부터 T_{rk}까지 적분하여 얻은 누적분포함수(Cumulative Distribution Function, CDF) 값과 그룹의 전체 정보가치 NC_G를 곱하여 나온 값을 T_{rk}로 나누어주면, T_{rk} 당 정보노출로 생기는 그룹의 손실비용 A_d를 얻을 수 있다. 이를 식으로 나타내면, (식 3.3)과 같다. 단, 여기서 그룹의 정보는 그룹에 참가하는 회원 수와 비례한다고 보고, 각각의 회원이 전

달하는 정보가치를 C_G로 하여 전체 정보가치를 NC_G로 하였다.

$$A_d = \frac{NC_G}{T_{rk}} \int_0^{T_{rk}} (T_{rk} - t) N\lambda e^{-N\lambda t} dt \quad \text{(식 3.3)}$$

(식 3.3)을 계산하면, (식 3.4)와 같다.

$$A_d = \frac{C_G}{\lambda T_{rk}} (e^{-N\lambda T_{rk}} + N\lambda T_{rk} - 1) \quad \text{(식 3.4)}$$

이와 함께, rekey에 따른 소요비용이 회원 한 명당 C_{rk} 가 소요된다면, rekey에 따른 소요 비용 A_{rk}은 (식 3.5)로 나타낼 수 있다.

$$A_{rk} = \frac{NC_{rk}}{T_{rk}} \quad \text{(식 3.5)}$$

따라서, 위에서 나타낸 (식 3.4)와 (식 3.5)의 결과 값을 합한 값이 총 손해 비용 A_T 로, 아래의 (식 3.6)로 나타낼 수 있다.

$$A_T = A_d + A_{rk}$$

$$A_T = \frac{C_G}{\lambda T_{rk}} (e^{-N\lambda T_{rk}} + N\lambda T_{rk} - 1) + \frac{NC_{rk}}{T_{rk}} \quad \text{(식 3.6)}$$

위 (식 3.6)에서 A_T 의 최소 값을 만족하는 T_{rk} 값이 최적의 rekey interval 값이 된다.

이 공식을 통해 계산되어지는 총 소요 비용 A_T 는 T_{rk} 가 증가할수록 NC_G 로 수렴하게 되는데, 이것은 만일 보안 멀티캐스트 그룹이 rekey를 전혀 실행하지 않을 경우, 그룹의 정보는 결국 모두 노출되어 손실됨을 보여준다.

그림 2는 임의로 $C_G = 1$, $N = 10^2$, $C_{rk} = 10^{-3}$로 설정한 뒤, λ를 1 부터 10^{-12} 까지 변화시키며 시뮬레이션 한 결과 곡선이다. 이 곡선에서 A_T가 최소 값일 때의 T_{rk}가 그 조건하의 최적의 rekey interval을 나타내는 것이다. 그림은 λ값이 작아질수록, rekey interval 값이 커짐을 보여주고 있다. X는 λ가 10^{-9}일 때, T_{rk}를

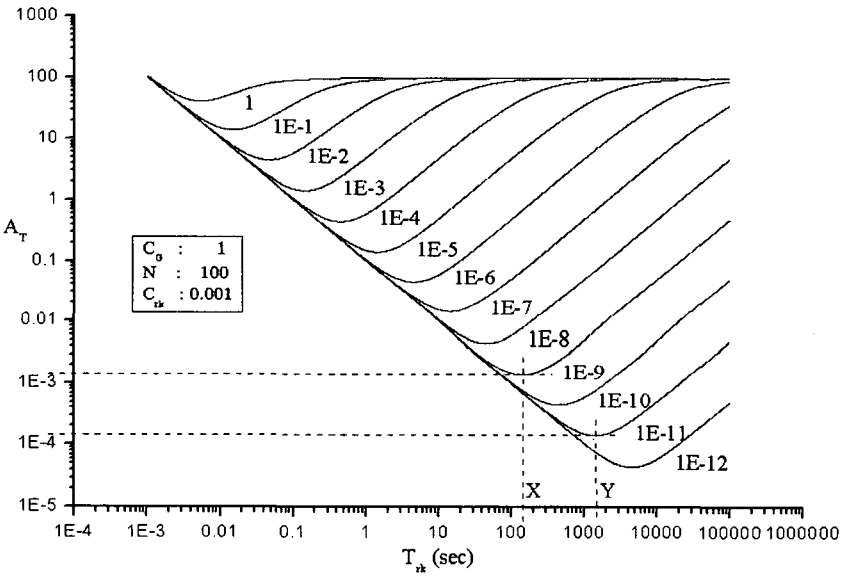

그림 2 λ 변화에 따른 T_{rk}의 변화

임의로 $C_G = 1$, $N = 10^2$, $C_{rk} = 10^{-3}$로 설정한 뒤, λ를 1 부터 10^{-12} 까지 변화시키며 시뮬레이션 한 결과 곡선이다. 이 곡선에서 A_T가 최소 값일 때의 T_{rk}가 그 조건하의 최적의 rekey interval을 나타내는 것이다. λ값이 작아질수록, rekey interval 값이 커짐을 보여주고 있다.

나타내는 것이고, Y는 λ가 10^{-11}일 때, T_{rk}를 나타내고 있으며, 두 값은 10배의 차이를 보이고 있다. 여기서, λ는 그룹의 정보 노출률을 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 3와 그림 4은 각각 그룹회원 수 N과 rekey에 따른 소요비용 C_{rk}가 변화함에 따라 변화하는 rekey interval T_{rk}를 보여주고 있다.

4. 결론

본 논문은 보안 멀티캐스트 환경을 소개하며, 그 가운데 그룹 키 재분배 과정인 rekey를 위한 효과적인 rekey interval 할당의 필요성을 설명하고, 그 방법을 제안하였다. 또한 제안한 방법을 이용하여 최적의 rekey interval 값을 찾아 낼 수 있음을 시뮬레이션을 통하여 보여주었다. 논문에서 제안하고 있는 할당방법은 그룹 키 재분배에 있어 비용적인 면을 효율성의 척도로 한 것으로, 회원 수 및 높은 보안 강도를 요구하는 그룹과 상대적으로 낮은 보안 강도를 요구하는 그룹을 차별하여, rekey interval 을 할당해 최소 비용으로 그룹을 관리할 수 있도록 하고 있다.

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

이에 본 연구는, 이 논문에서 직접적으로 고려되어지지 않았던 그룹회원의 가입탈퇴과정과 같이 불규칙적으로 일어나는 사건들에 의한 rekey의 빈도를 확률적인 방법으로 계산하여 rekey interval 공식에 포함시키는 연구를 진행하고 있다. 이 연구는 보안 멀티캐스트 환경을 위한 보다 효율적인 rekey interval 할당을 가능하게 할 것이다.

ACKNOWLEDGMENT

본 논문은 정보통신부에서 주관하는 정보통신 우수시범학교 지원사업에 의하여 수행되었음.

참 고 문 헌

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

[2] S. Setia, S. Koussih, S. Jajodia, and E. Harder, "Kronos: A Scalable Group Re-Keying Approach for Secure Multicast", *To appear in Proc. of 2000 IEEE Computer Society Symposium on Research in Security and Privacy*, pp. 215-228, 2000.

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

[4] D. Balenson, D. McGrew, and 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.

[5] W. Stallings, *Cryptography & Network Security: Principles & Practice 2nd edition*, Prentice Hall, 1998.

[6] S. Mittra, "Iolus: A Framework for Scalable Secure multicasting" , *Proceedings of the ACM SIGCOMM ' 97*, pp. 277-288, September, 1997.

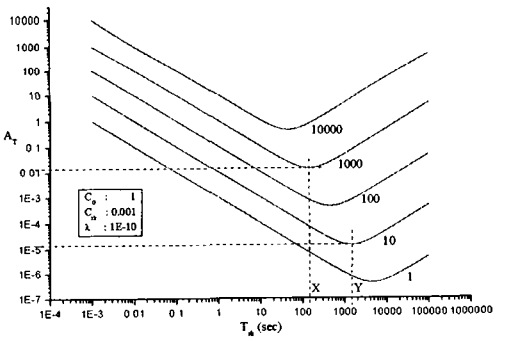

그림 3 N 변화에 따른 T_{rk}의 변화

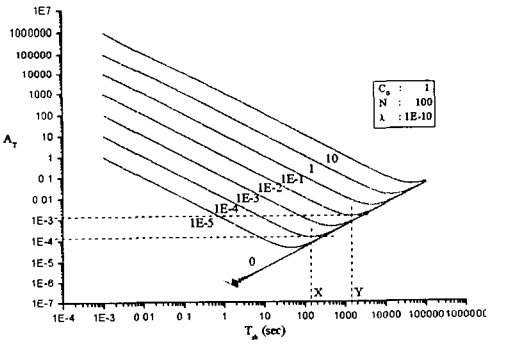

그림 4 C_{rk} 변화에 따른 T_{rk}의 변화