[5C-106]

의사 임의 함수와 부울함수의 최소화 방법을 사용한 그룹 키관리 기법

**차선민, *조수영, *정종인
공주대학교
maingho@kongju.ac.kr

Group Key Management Scheme using Pseudo Random Function and Boolean Function Minimization Method

**SunMin Cha, *SuYoung Cho, *JongIn Chung
Kongju National University

요약

그룹의 한 멤버가 제거되면 새로운 그룹키를 생성하여 그룹의 나머지 모든 멤버들에게 전달되어야 한다. 새로운 키를 생성하여 분배하는 것은 많은 연산을 요구하므로 rekeying하기 위하여 제어기와 멤버가 저장하는 키의 수, rekeying할 때마다 제어기가 전달하는 메시지의 수, 초기단계에서 제어기에 의해 전달되는 키의 수, 일괄 rekeying시 전달하는 메시지의 수는 그룹 키 관리기법을 평가하는 중요한 기준이다.

일괄 rekeying은 순차적으로 개별 rekeying하는 것보다 rekeying에 대한 메시지의 수와 연산비용을 줄일 수 있다. 의사 임의 함수를 사용하여 rekeying을 위하여 보내는 메시지의 수와 연산을 줄이고, 제어기에 저장된 키의 수를 최소화하여 중앙 집중된 제어기의 부하를 줄일 수 있는 새로운 그룹 키 관리 기법을 제안한다.

1. 서론

그룹 멤버쉽의 변화가 있을 때마다 멤버가 가지고 있는 키를 변경하여야 FS(Forward Secrecy)와 BS (Backward Secrecy)가 보장된다. 이와 같이 키의 변경을 rekeying이라 한다. FS는 어떤 멤버가 그룹을 떠나면 그 이후에 이루어지고 있는 그룹에 대한 정보를 얻을 수 없는 것을 의미한다. BS는 새로운 멤버가 그룹에 가입할 때 이전에 이루어진 그룹에 대한 정보를 얻을 수 없는 것을 말한다[1].

멤버의 가입과 탈퇴는 멀티캐스트 키 관리의 확장성(scalability) 문제와 밀접한 관계가 있다. 확장성을 제공하기 위하여 KEK의 논리적인 이진트리를 사용한 연구가 많이 수행되어 왔다[2-6]. KEK의 이진 키트리를 사용한 방법은 그룹키를 변경하기 위한 메시지의 수가 트리의 깊이(log N)에 비례하므로 매우 효율적이다. Chang[3]은 확장성을 제공하기 위하여 이진 트리를 사용하며, 제어기가 관리하는 키의 수가 $2\log N+1$을 갖는 효율적인 그룹키 관리기법을 제안하였다.

그룹의 크기가 크고 탈퇴가 빈번할 경우, 각 멤버를 제거할 때마다 새로운 그룹키를 변경하고 분배하는 것은 많은 연산을 요구한다. 대부분의 응용에서는 멤버탈퇴 요구가 있을 때 즉시 처리할 필요가 없이 주기적으로 탈퇴할 멤버를 모아서 동시에 제거한다[7-9]. [1]

Rekeying을 수행할 때 고려하여야 할 가장 중요한 요소는 rekeying하기 위하여 제어기와 멤버가 저장하는 키의 수, rekeying할 때마다 제어기가 전달하는 메시지의 수, 초기단계에 제어기에 의해 전달되는 키의 수, 일괄 rekeying시 전달하는 메시지의 수 등이다.

II. 그룹키 관리기법

그룹 제어가 저장하여야 하는 키의 수를 감소하기 위하여 LKH를 변형하여 단지 제어기만이 알고 있는 의사 임의(pseudo random) 함수에 의해 노드의 키를 만듦으로서 제어기가 저장할 키의 수를 줄인다. Rekeying이 필요할 때 제어기는 변경된 키를 보내는 것이 아니라 키를 변경하기 위하여 필요한 정보를 보낸다[10,11].

제어기는 이진트리의 각 노드의 위치를 (레벨 번호, 각 레벨에서의 위치)로 정한다. 예를 들면, 레벨 0의 루트노드는 (0,0), 레벨 1의 노드는 (1,0)과 (1,1), 레벨 2의 노드는 (2,0), (2,1), (2,2)와 (2,3)이다. 노드 (i,j)의 키는 j가 짝수 일때 식 (1), j가 홀수일때 식(2)에 따라 생성하여 이진트리를 구성하면 그림 1과 같다.

$$\overline{k}_{n-i}=f_{r1}(2^{n-i}+0)\oplus r \quad (1)$$

$$k_{n-i}=f_{r1}(2^{n-i}+1)\oplus r \quad (2)$$

f_{r1}은 random seed r1을 갖는 의사 임의함수이며, r은

1 본 연구는 과학기술부 목적기초연구(과제번호: R05-2004-000-11027-0) 지원으로 수행되었음.