2차원 배열을 이용한 그룹키 생성에 관한 연구

이병길, 전문석
숭실대학교 컴퓨터학과
e-mail : lbksuper@nate.com, mjun@ssu.ac.kr

Study for generating group key mechanism used two-dimension array

Byoung-Kil Lee, Moon-Seog Jun
Dept of Computer Science, Soongsil University

요 약

단말간의 안전한 그룹 통신의 핵심은 그룹 키의 관리에 있는데, 그룹 키를 관리함에 있어서는 그룹 키에 대한 안전성과 관리 메커니즘의 효율성을 중요시 해야한다. 키 교환 프로토콜은 이미 많은 연구가 진행되어 왔지만 나날이 발전하는 새로운 위험이나 통신환경의 변화 때문에 안전하고 효율적인 키 교환 프로토콜이 필요하게 되었다.

본 논문에서는 2차원 배열로 된 keyset 선 분배를 통한 간단한 연산으로 그룹 키 생성의 효율성을 높이는 동시에 각 단말의 정보를 보호함으로써 안전성 또한 향상 되었다.

1. 서론

멀티 캐스트 전송 방식은 하나 이상의 송신자들이 특정한 하나 이상의 수신자들에게 데이터를 전송하는 방식이다. 기존의 유니캐스트 전송 방식은 동일한 패킷을 각각의 수신자에게 중복으로 전송하게 되고 늘어나는 패킷 양에 따라 네트워크의 효율이 급감한다. 반면에 멀티 캐스트 방식은 메시지 송신자 입장에서 여러 수신자에게 한 번에 메시지를 전송할 수 있고, 통신 효율을 증가시킬 수 있다. 멀티캐스트 전송 방식은 패킷의 헤더에 수신자의 주소대신 수신자가 참여하고 있는 그룹의 주소를 표시하여 패킷을 전송하고 멀티캐스트 패킷을 전송받은 수신자는 자신이 그 그룹에 속해 있는지 판단하여 패킷의 수용 여부를 결정하게 된다.

그룹 키 교환(group key agreement) 프로토콜은 두 명 혹은 그 이상의 사용자들이 안전하지 않은 공개된 통신망에서 안전하게 공통된 키를 생성하는 기법이다. 키 교환 프로토콜을 수행하여 생성된 공통된 키를 세션 키라고 하고 이렇게 생성된 세션키는 암호화/복호화, MAC, 인증과 디지털 서명등의 키로 사용되어 진다.

안전한 그룹 통신이란, 어떤 목적 아래 모인 특정한 그룹이 있을 때, 그 그룹에 속한 멤버들만이 그룹의 정보를 송 수신할 수 있도록 비밀스런 통신을 보장하는 것이다. 즉, 정보를 공유하고자 형성된 그룹이 있을 때, 이때 형성된 그룹의 멤버만이 그룹의 비밀 정보를 얻을 수 있어야 하며 그룹 내에서 공유되고 있는 비밀키는 Backward secrecy와 Forward secrecy를 만족시키기 위해 새로운 사용자들이 그룹에 참여하고 또한 기존의 사용자가 그룹을 탈퇴함에 따라 계속 새로운 그룹 키로 변경되어야 한다. 즉, 그룹에 새로 가입한 사용자는 가입하기 이전에 메시지를 복호화 할 수 없어야 하고, 그룹을 떠나는 사용자가 그룹을 떠난 이후의 메시지를 복호화 할 수 없어야 한다.

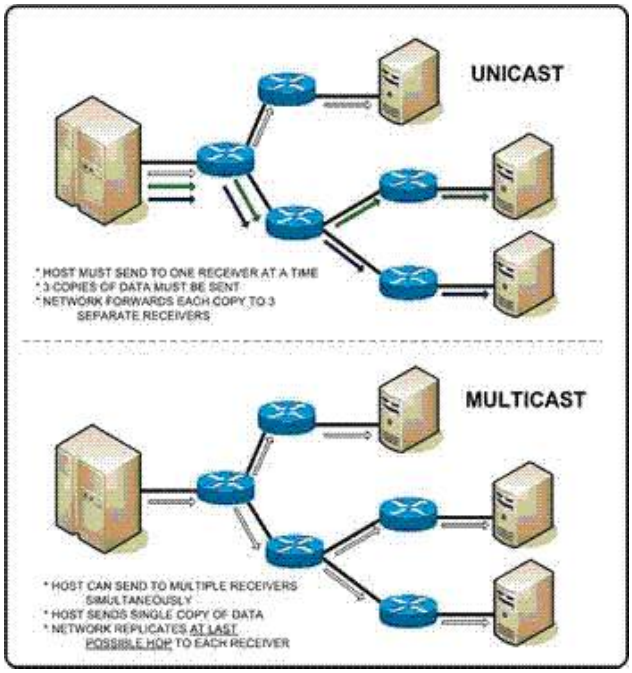
본 논문에서는 2차원 배열을 가지고 할 수 있는 연산을 이용해 그룹 키와 식별 키를 생성해서 연산량이 적으면서 보안과 실시간성 두 가지 측면이 고려된 그룹 키 생성 방법에 대해 서술하고 있다.

2. 관련 연구

2.1 멀티캐스트

유니캐스트는 전송 대상자의 수가 늘어나게 되면

송신자의 전송 부담은 더욱 커진다. 이로 인한 효율 저하가 전송 자체의 성능에 큰 영향을 미친다. 멀티캐스트의 가장 큰 특징은 메시지 송신자 입장에서 여러 수신자에게 한 번에 메시지를 전송 할 수 있다.



[그림 1] Unicast와 multicast 시스템의 구조

2.2 쿼럼 시스템

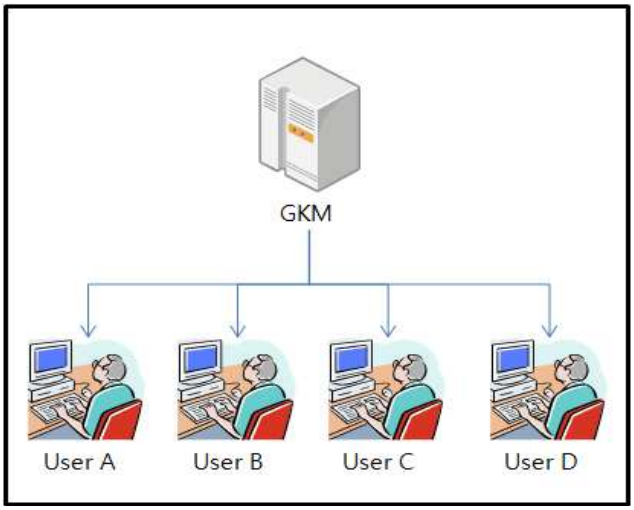
쿼럼(Quorum)이라는 것은 두 개의 교집합 원소가 무조건 하나 이상 존재하는 것을 말한다. 즉, 임의의 두 집합을 교집합 연산을 했을 때, 공집합이 되지 않는 집합들의 모임을 쿼럼 시스템(Quorum System)이라 한다. 예를 들어 {1,2,3,4,}, {2,5,6,8}, {3,8,9,0}은 쿼럼 시스템 이다. {1,2,3,4}∩{2,5,6,8}={2}, {2,5,6,8}∩{3,8,9,0}={8}, {1,2,3,4}∩{3,8,9,0}={3}으로 어떤 집합 셋끼리 교집합 연산을 하여도 공집합이 나오지 않기 때문에 쿼럼 시스템이 된다. 만약에 집합이 {1,2,3,4,}, {2,5,6,7}, {3,8,9,0} 이라면 {2,5,6,7}과 {3,8,9,0}의 교집합은 공집합이기 때문에 쿼럼 시스템이 되지 않는다.[1]

2.2.1 그리드(Grid)쿼럼 시스템

그리드 쿼럼 시스템에서 원소들은 2차원 평면 상에 줄지어서 위치해 있다. 쿼럼 시스템을 구성하기 위해서 각각의 집합은 행과 열을 각각 하나씩 고르게 된다. 선택한 행에 속한 원소들과, 선택한 열에 속한 원소들을 합쳐서 자기의 원소로 정하면 이 시스템 내에서 임의의 집합 두 개를 선택 하더라도 서로 겹치는 부분이 항상 최소 2개 이상 나오게 된다.

이 쿼럼 시스템은 전체 원소 n개 중에서 $2\sqrt{n}-1$ 개의 원소를 뽑음으로 2개 이상의 공통 원소를 보장할 수 있는 특징이 있다.

3. 2차원 배열을 이용한 그룹 키 생성

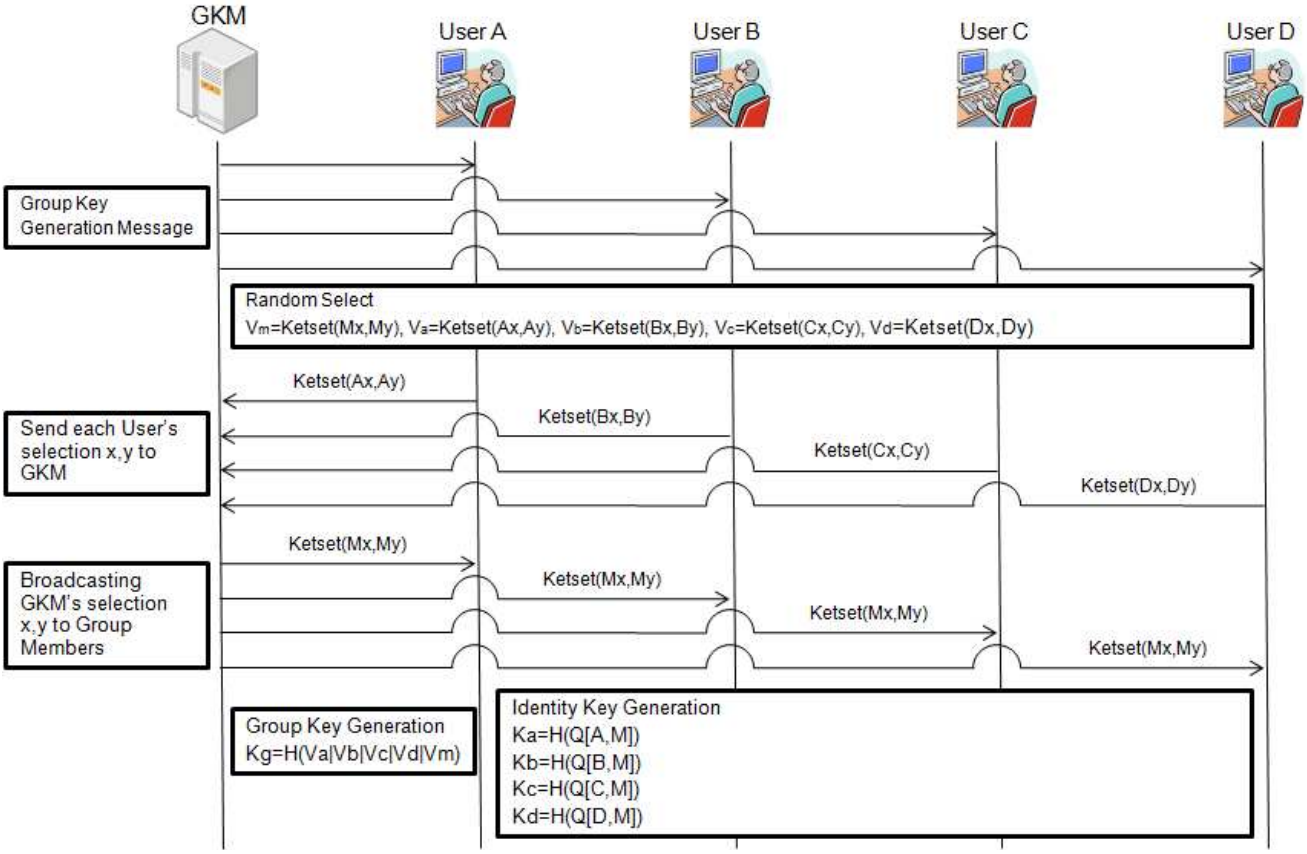


[그림 2] 그룹 구성도

그룹 키 생성을 위한 그룹 형태는 [그림 2]과 같이 중앙에서 GKM(Group Key Management)가 통제를 하고 GKM은 각각의 유저에게 그룹 키를 생성해서 분배 해 주고 그룹을 관리하는 역할을 한다. 여기서 GKM과 각 인증된 User에게는 [그림 3]와 같은 형태의 2차원 배열로 된 Keyset을 받게 되는데, 각각 전달되는 Keyset은 10x10의 값을 넣을 수 있게 되어있고 각 cell에는 대문자 A-Z, 소문자 a-z, 숫자 0-9까지의 값을 넣을 수 있고 cell은 랜덤함수로 채우게 된다.

A	B	C	D	E	F	G	H	I	J
K	L	M	N	O	P	Q	R	S	T
U	V	W	X	Y	Z	a	b	c	d
e	f	g	h	i	j	k	l	m	n
o	p	q	r	s	t	u	v	w	x
y	z	1	2	3	4	5	6	7	8
9	0	L	k	i	e	m	h	E	y
o	B	j	Y	I	n	O	F	U	o
r	N	G	E	K	v	e	I	r	L
I	O	4	9	V	8	0	2	1	6

[그림 3] Keyset의 예



[그림 4] 키 생성을 위한 프로토콜

GKM과 각 User는 Keyset을 가지고 그룹 키 생성과 식별 키를 생성하기 위한 연산을 하게 된다.

3.1 그룹 키 생성 알고리즘

그룹 키 생성을 위한 프로토콜은 [그림 4]와 같다.

① GKM에서 그룹 키 생성메시지를 각 User에게 전달 한다.

② GKM과 각 User는 가지고 있는 Keyset에서 행과 열을 랜덤 선택하여 Vm, Va, Vb, Vc, Vd 값을 추출한다.

③ User는 Keyset에서 선택한 행과 열의 값을 GKM에게 보내준다.

④ GKM도 Keyset에서 선택한 행과 열 값을 각 그룹 Member에게 보낸다.

⑤ GKM은 각 User가 보내준 행,열 값을 자신의 Keyset에 적용해 Va, Vb, Vc, Vd 값을 추출, 해쉬 함수를 돌려서 그룹 키 (Kg=H(Va|Vb|Vc|Vd|Vm)를 만들고 각 User는 자신의 행,열 값과 GKM의 행, 열값을 쿼럼 연산후 해쉬 함수를 적용해 식별 키를 만든다.

위 프로세스를 거치면 GKM은 그룹 키 Kg값을 얻게 되고 각 User는 식별 키를 갖게 되는데, Kg를 각 유저의 식별 키로 암호화 해서 보내주면 그룹 키 분배가 완료 된다.

4. 성능 평가

[표 1] 제안 시스템과 ID 기반 시스템의 비교

	제안 시스템	ID기반 시스템
정보 노출	적음	보통
연산량	낮음	보통
연산 속도	보통	보통

ID 기반의 그룹 키 교환 기법에도 여러 가지 방법이 있지만, 그룹 키를 사용하는데 있어서 ID를 기반으로 하기 때문에 각 단말의 정보 노출의 문제점을 피할 수 없는 반면에 제안 시스템 에서는 개인정보와는 전혀 무관한 사전 분배 된 2차원 배열을 키 생성에 사용함으로써 개인 정보 노출의 문제점을 해결하였고, 연산량은 ID기반에도 여러 가지 방법이 있지만, 환경과 프로토콜에 따라 차이가 심하다.

5. 결론

일반 네트워크 환경에서 그룹 키 분배의 중요성은 나날이 증가 하고 있지만, 그룹 키 생성/분배의 방법에서 여러 가지 좋은 기법들이 많이 연구되고 있다. 하지만, 효율성만을 중시하는 방법이 있는가 하면, 효율성과 안정성을 가졌지만 정보노출을 피할 수 없는 방법도 있다. 제안 시스템 에서는 2차원 행렬을 이용해서 개인 정보의 노출을 최대한 없애고 그룹 키 생성시에 키의 다양성과 효율성을 만족시키는 방법을 제시하고 있다. 단, 2차원 배열이 만약 10x10 이라고 가정 하고 들어갈 수 있는 인자가 0-9, A-Z, a-z 라고 한다면 랜덤으로 키 셋을 만들 때 중복되는 값이 생기는데, 키 셋이 노출 되었을 경우 낮은 확률로 같은 키가 생성될 수 있다.

참고문헌

[1] 강지명 “센서 네트워크에서의 쿼럼 시스템을 이용한 키 사전 분배” 정보과학회 논문지 : 정보통신 제 33권 제 3호(2006.6)