커뮤니티 기반 유비쿼터스 네트워크 환경에서 사용자 테이블을 이용한 효율적인 그룹키 관리 기법

홍철화*, 김성일*, 정수환*
*숭실대학교 정보통신전자공학과
e-mail : {blmhong, skytast, souhwanj}@ssu.ac.kr

Member Table Based Efficient Group Key Management Scheme in Community Based-Ubiquitous Network

Chul-Wha Hong *, Sou-Hwan Jung *
*School of Electronic Engineering, Soong-Sil University

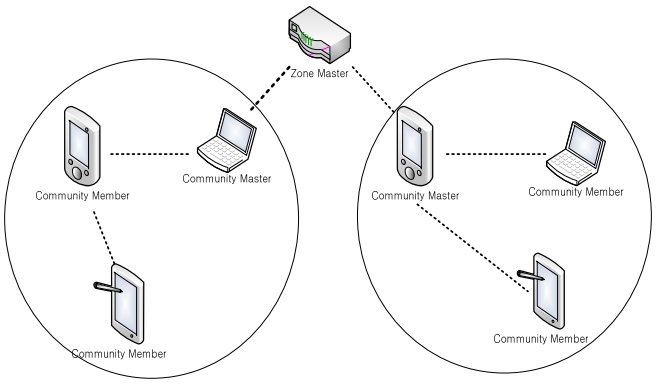
요 약

커뮤니티 기반 유비쿼터스 네트워크 환경에서 커뮤니티 사용자는 응용 서비스 및 네트워크 서비스를 제공받기 위해 자유롭게 커뮤니티에 참여하고 탈퇴할 수 있다. 이런 서비스가 안전하게 제공되기 위해서는 그룹키가 필요하다. 커뮤니티 사용자의 참여 및 탈퇴는 그룹키의 순방향, 역방향 안정성에 영향을 주고 갱신된 그룹키는 효율적인 분배가 이루어져야 한다. 기존 그룹키 관리 기법은 사용자 수에 따라 그룹키를 교환하는데 사용되는 메시지 수가 증가하는 확장서 문제를 가지고 있다. 본 논문에서는 사용자 테이블을 이용하여 커뮤니티 내에 사용자 수에 영향을 받지 않는 그룹키 관리 기법을 제안한다.

1. 서론

유비쿼터스 네트워크 환경이 도시 환경, 항만 및 유통 시스템 등 다양한 분야에 적용되고 있다. 또한 유비쿼터스 네트워크 환경은 사용자의 상황인식 정보를 바탕으로 사용자가 필요로 하는 서비스를 제공하는 지능적인 네트워크 기술 연구가 진행되고 있다. 이와 같은 기술로는 최근 연구되고 있는 커뮤니티 기반의 유비쿼터스 네트워크가 있다. [1]

커뮤니티 기반의 유비쿼터스 네트워크는 그림 1 과 같이 존 마스터 노드를 중심으로 커뮤니티를 형성하고, 커뮤니티에 따라 필요한 응용 서비스 및 네트워크 서비스를 제공한다. 사용자들은 사용자들이 원하는 서비스를 받거나 제공하기 위해 자유롭게 커뮤니티에 참여 또는 탈퇴할 수 있다.



(그림 1) 커뮤니티 기반 유비쿼터스 네트워크

안전한 커뮤니티 서비스를 제공하기 위해서는 초기 인증과정을 통해 그룹키를 알고 있는 사용자만이 암호화된 그룹 통신을 복호화 할 수 있어야 한다. 또한 사용자의 동적인 특성을 고려하여 커뮤니티 참여와 탈퇴가 발생하는 동안, 탈퇴하는 사용자에 대한 순방향 안전성(Forward Secrecy)과 새로운 사용자에 대한 역방향 안전성(Backward Secrecy)을 제공해야 한다.[2] 그리고 그룹키 분배의 효율성과 사용자 수에 따른 확장성을 고려할 때, 그룹키의 갱신과 전송 및 암호화와 관련된 오버헤드는 그룹의 크기에 독립적이어야 하며 커뮤니티에서의 사용자 변화로 인한 그룹키 갱신의 영향이 전체 네트워크에 영향을 끼치는 '1-affect-n' 문제도 고려해야 한다.[3]

본 논문에서는 커뮤니티 관리자가 커뮤니티 사용자의 키값으로 구성된 사용자 테이블을 생성하고 이를 이용한 그룹키 관리 기법을 제안한다. 제안하는 기법은 다음과 같은 특성을 가지고 있다. (1) 다항식 연산을 이용한 멀티캐스트 방식의 그룹키 분배, (2) 해쉬함수를 이용한 그룹키 갱신, (3) 커뮤니티 사용자의 변화를 커뮤니티로 한정시키는 비중앙화 그룹키 관리, 제안한 기법은 커뮤니티 사용자간 역방향 안정성 및 순방향 안전성을 제공한다.

본 논문의 구성은 다음과 같다. 2 장에서는 그룹키 관리시의 고려사항과 기존에 수행되었던 그룹키 관리 기법들에 대해 설명하고 3 장에서는 본 논문에 제안하는 사용자 테이블을 이용한 그룹키 관리 기법을 제안한다. 4 장에서는 제안 시스템에 대해 성능 및 안전성을 분석하고 5 장에서 결론을 맺는다.

2. 그룹키 관리 관련 기술

2.1. 안전한 그룹 통신을 위한 보안 요구사항

안전한 그룹통신의 핵심은 사용자의 참여 또는 탈퇴시 발생하는 그룹키의 관리이며, 그룹키는 다음과 같은 보안 요구사항을 만족시켜야 한다.

- 그룹키의 비밀성(Group Key Secrecy)
  그룹키는 그룹 사용자들만이 공유해야 하며, 어떤 악의적인 공격자에 의해 그룹키를 도출하는 것이 계산상 불가능 해야 한다.

- 순방향 안전성(Forward Secrecy)
  탈퇴한 사용자가 이전 세션의 그룹키들에 대한 정보를 알고 있더라도 이후의 그룹키를 계산하지 못하게 함으로써 그룹 통신에 접근할 수 없어야 한다.

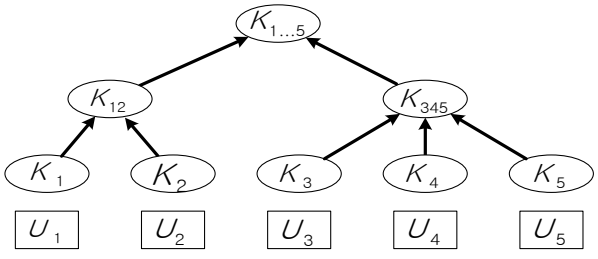
- 역방향 안전성(Backward Secrecy)
  그룹에 참여한 새로운 사용자가 새로운 그룹키에 대한 정보를 가지고서 이전 세션의 그룹키를 계산하지 못함으로써 데이터에 접근할 수 없어야 한다.

- 그룹키의 독립성(Group Key Independence)
  그룹의 전체 사용자 집합 M 의 부분 집합 M' 을 알고 있는 악의적인 공격자에 의해 다른 부분 집합 $\overline{M} \in (M - M')$ 의 그룹키를 계산 할 수 없어야 한다.

안전한 그룹 통신을 위한 연구는 시스템 관리 유형에 따라 크게 중앙 그룹키 관리 기법과 비중앙 관리 기법으로 구분할 수 있다.

2.2. 중앙 그룹키 관리 기법

중앙 그룹키 관리 기법은 키관리자가 전체 네트워크에서 사용되는 그룹키를 생성 및 분배하는 기법이다. 그 중에 동적인 네트워크 변화를 고려한 키 트리 그래프를 이용한 그룹키 관리 기법은 동적인 네트워크 변화에 신속한 그룹키 관리가 가능하다.[4][5] 트리 그래프의 각 말단 노드에 사용자가 위치하고, 트리의 중간 노드들은 키암호화키(Key Encryption Key, KEK)를 할당한다. 그리고 루트노드에는 현재 세션에 대한 그룹키가 할당된다. 사용자는 정점의 노드에 이르는 직접경로 상에 있는 키값들만 알고 있다.

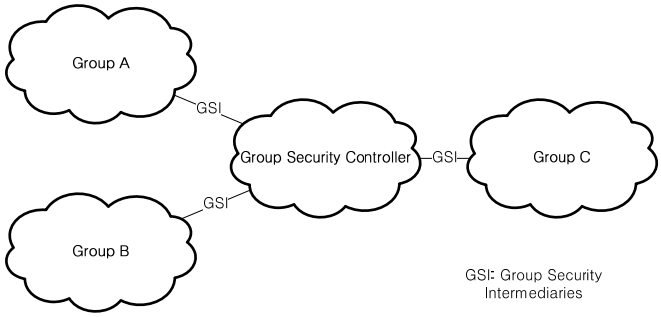


(그림 2) 트리 그래프를 이용한 키계층 구조

다른 사용자가 그룹에 참여 또는 탈퇴하는 경우, 사용자로부터 루트노드까지 경로상에 위치한 키들은 갱신되고 새로운 그룹키가 경로상에 사용자들에게 전송된다. 이러한 키 트리 그래프를 이용한 그룹키 관리 기법은 하나의 사용자 변화에도 전체 네트워크 그룹키를 갱신해야 하므로 '1-affect-n' 문제가 발생한다.

2.3. 비중앙 그룹키 관리 기법

비중앙 그룹키 관리 기법에서는 전체 그룹의 사용자를 다수의 하위 그룹으로 나누고, 각 하위 그룹은 각각의 하위 그룹 관리자에 의해 통제가 된다.[6][7] 중앙 그룹키 관리 기법과는 달리 그룹의 사용자가 참여 또는 탈퇴하는 경우, 한 사용자의 변화가 전체 네트워크에 영향을 미치는 '1-affect-n'문제가 완화된다.
비중앙 관리 기법에서 그룹간의 통신은 각 하위 그룹의 관리자를 통해서 조정이 되고 그룹의 관리자는 그룹의 사용자를 관리한다. 그룹 A 에서 그룹 B 로 데이터를 전송하는 경우, 그룹 A 관리자는 그룹 A 의 그룹키로 암호화된 메시지를 복호화 한 후, 그룹 B 의 그룹키로 데이터를 재암호화 한 후 그룹 B 에 전송하게 된다. 이 과정에서 각 그룹의 관리자는 데이터를 확인할 수 있고 전송되는 그룹의 그룹키도 노출되기 때문에 그룹 통신의 비밀성이 보장될 수 없는 문제가 발생한다.



(그림 3) 비중앙 그룹키 관리 기법

3. 제안 기술

이번 절에서는 커뮤니티 사용자 테이블을 이용한 그룹키 관리 기법을 제안한다. 그룹키 갱신 과정은 다항식 연산을 이용한 그룹키 분배 및 해쉬함수를 이용한 그룹키 갱신 과정으로 구성된다.

3.1. 기호 및 가정

제안하는 기법에서 모든 사용자, 커뮤니티는 유일한 아이디를 가지고 있으며, 각 사용자는 사용자가 속해 있는 커뮤니티의 아이디를 알고 있다. 초기 등록과정을 통해 커뮤니티 관리자와 커뮤니티 사용자간에 인증 과정을 통해 대칭키를 공유한다고 가정한다.

제안하는 그룹키 관리 기법에서 사용하는 기호는 다음과 같다.

- ID_g: 커뮤니티 g 의 아이디.
- m_n: 커뮤니티를 구성하는 사용자. n 은 커뮤니티를 구성하는 사용자의 수를 의미한다.
- K_{m_n}: 커뮤니티를 구성하는 사용자 n 에게 부여되는 키 값. 사용자 n 이 커뮤니티에 참여하는 경우 커뮤니티 관리자에 의해 유일한 임의의 값이 주어진다.
- GK_n^i: 커뮤니티에서 사용되는 그룹키. n 명의 멤버가 포함된 커뮤니티 g 에 i 세션에서 커뮤니티 사용자간에 통신을 위해 사용한다.
- $M(x)$: 그룹키를 전달하는 함수. 각 커뮤니티의 사용자에게 부여되는 키 값을 이용해 생성되는 메시지를 이용하여 GK_n^i 를 멀티캐스트한다.
- $H(ID_g \,||\, GK_n^i \,||\, K_{m_n})$: 새로운 그룹키를 생성하는 함수. 그룹키를 생성하기 위해서 커뮤니티 g 의 아이디 ID_g, i 세션에서 커뮤니티에서 사용하는 그룹키 GK_n^i, 커뮤니티를 구성하는 사용자 n 의 키 값 K_{m_n} 을 이용해 해쉬값을 출력하는 함수이다.

3.2. 커뮤니티 사용자 참여

가입하는 사용자는 먼저 주변 사용자 검색과정을 통해 커뮤니티 관리자에 가입 요청을 한다. 커뮤니티 관리자와 등록과정을 통해 사용자 m_{n+1} 에게 키 값 $K_{m_{n+1}}$ 을 커뮤니티 사용자 테이블에 등록한다. 그리고 $K_{m_{n+1}}$ 를 이용해 $i+1$세션에 그룹키 GK_{n+1}^{i+1}을 생성한다.

$$GK_{n+1}^{i+1} = H(ID_g \,||\, GK_n^i \,||\, K_{m_{n+1}}) \tag{1}$$

커뮤니티 등록과정을 통해 커뮤니티 관리자와 커뮤니티 사용자는 대칭키를 공유하게 된다. 이 대칭키를 이용하여 새로운 그룹키 GK_{n+1}^{i+1}을 m_{n+1}에게 안전하게 유니캐스트한다.

$$M = E_{GK_n^i}(GK_{n+1}^{i+1} \,||\, R) \,||\, H(E_{GK_{n+1}^{i+1}}(R)) \tag{2}$$

커뮤니티 관리자는 기존 커뮤니티 사용자들에게 이전 그룹키 GK_n^i를 이용하여 $i+1$세션 그룹키 GK_{n+1}^{i+1}를 멀티캐스트한다. 커뮤니티 사용자는 메시지에 포함된 $R(RandomValue)$을 이용하여 그룹키가 올바른 키값인지 확인할 수 있다. 새로운 사용자 m_{n+1} 은 이전 그룹키 GK_n^i을 알고 있지 않아도 커뮤니티 관리자로부터 새로운 그룹키 GK_{n+1}^{i+1}을 전송 받아 커뮤니티 통신에 참여 가능하다.

3.3. 커뮤니티 사용자 탈퇴

커뮤니티 사용자 탈퇴 시 키 갱신 과정은 커뮤니티 관리자가 새로운 그룹키 갱신 후 탈퇴한 사용자를 제외한 나머지 사용자들에게 그룹키를 멀티캐스트 하는 과정으로 이루어진다. 탈퇴한 사용자의 키값 K_{m_n} 를 이용하여 $i+1$ 세션에 그룹키 GK_{n-1}^{i+1}를 생성한다.

$$GK_{n-1}^{i+1} = H(ID_g \,||\, GK_n^i \,||\, R) \tag{3}$$

커뮤니티 관리자는 $i+1$ 세션 그룹키를 다른 사용자에게 전송하기 위해 다항식 연산을 이용하여 메시지를 생성한다. 다른 커뮤니티 사용자들에게 그룹키 전달 메시지 $M(x)$를 멀티캐스트한다.

$$M(x) = (x - K_{m_1})(x - K_{m_2})\ldots(x - K_{m_{n-1}}) + R \tag{4}$$

메시지를 받은 기존 커뮤니티 사용자들은 그룹 아이디 ID_g, i 세션 그룹키 GK_n^i, 탈퇴한 사용자 m_n 의 키값 K_{m_n} 를 이용하여 $i+1$세션 그룹키 GK_{n-1}^{i+1}를 생성한다.

$$GK_{n-1}^{i+1} = H(ID_g \,||\, GK_n^i \,||\, R) \tag{5}$$

i 세션 그룹키 GK_n^i를 가지고 있는 사용자 m_n 은 그룹키 전달 메시지 $M(x)$를 통해 $i+1$세션 그룹키 GK_{n-1}^{i+1}를 계산할 수 없다.

4. 제안 기법 분석

4.1. 안전성 분석

- 그룹키의 비밀성

i 세션에 참여한 커뮤니티 사용자 m_n 은 그룹키 GK_n^i을 이용해 그룹 통신에 참여할 수 있다. 커뮤니티 관리는 초기인증과정을 통해 사용자에게 그룹키를 전송한다. 사용자의 참여 및 탈퇴시 이전 세션의 그룹키와 다항식 연산을 이용하여 신뢰할 수 있는 사용자만이 그룹키를 이용하여 그룹 통신에 참여할 수 있다.

- 순방향 안전성

새 사용자가 커뮤니티 $i+1$ 세션에 참여하는 경우 i 세션 그룹키 GK_n^i 을 이용하여 $i+1$ 세션 그룹키 GK_{n+1}^{i+1}을 전송하기 때문에 참여한 사용자는 i 세션의 그룹키 GK_n^i에 대한 정보를 얻을 수 없다. 또한 해쉬 함수를 이용하여 생성된 GK_{n+1}^{i+1}을 통해 i 세션 그룹키 GK_n^i을 계산할 수 없다.

- 역방향 안전성

커뮤니티 사용자 m_n 커뮤니티 탈퇴 시, 커뮤니티관리자는 다항식 연산을 통해 선택적으로 그룹키 전달 메시지 $M(x)$를 전송한다. 탈퇴한 사용자 m_n 은 키값 K_{m_n} 을 이용하여 $M(x)$에서 정보를 얻을 수 없다.

- 그룹키의 독립성

그룹키 전달 메시지는 그룹에 참여한 사용자의 키값으로만 구성되기 때문에 커뮤니티를 탈퇴한 사용자의 부분 집합 M'을 알고 있는 악의적인 공격자는 그룹키 전달 메시지에서 $i+1$ 세션 그룹키 GK_n^{i+1}를 계산할 수 없다.

4.2. 효율성 분석

제안 논문을 통신량 측면에서 기존 프로토콜과 효율성 분석이다.

<표 1> 기존 프로토콜과 효율성 분석

효율성 / 프로토콜	통신량		그룹키 갱신 문제	
	참여시 메시지	탈퇴시 메시지	그룹키 확장성	그룹간 통신
중앙 키관리기법 (LKH)[8]	N	N	No	Yes
비중앙 키관리기법 (Iolus)[9]	n	n	Yes	No
제안 기법	2	1	Yes	Yes

1) N: 그룹에 포함된 사용자의 수
2) n: 하위 그룹에 포함된 사용자의 수
3) 참여시 메시지: 사용자 참여시 네트워크에 전송되는 메시지 수
4) 탈퇴시 메시지: 사용자 탈퇴시 네트워크에 전송되는 메시지 수

본 논문에서 제안한 프로토콜은 <표 1>에서 사용자 참여 및 탈퇴에 따른 그룹키의 갱신 과정에서 통신량 측면에서 효율적이고 기존 갱신 문제를 해결한 프로토콜이다.

5. 향후 연구 방향 및 결론

본 논문에서는 커뮤니티 기반의 유비쿼터스 네트워크에서 사용자 테이블을 이용해 사용자가 커뮤니티에 참여 또는 탈퇴시 효율적인 그룹키 관리기법을 제안하였다. 사용자가 참여하는 경우 해쉬함수를 이용하여 생성된 그룹키를 전송함으로써 커뮤니티 사용자는 그룹키의 신뢰성을 확보할 수 있다. 또한 사용자가 커뮤니티 탈퇴시 사용자의 키값을 다항식 연산을 이용한 멀티캐스트를 사용한다. 기존의 그룹키 관리기법은 그룹키 갱신과정에서 모든 커뮤니티 사용자별로 전송함으로써 사용자가 증가함에 따라 네트워크 내 통신 메시지가 증가하는 확장성 문제가 있다. 하지만 제안하는 기법은 커뮤니티 내 사용자 수와 상관없이 그룹키를 효과적으로 전송할 수 있다.

제안하는 기법은 사용자가 커뮤니티 참여 및 탈퇴시 제안하는 기법은 두 개의 알고리즘을 사용하고 있다. 두 개의 기법을 병행함으로써 생기는 안정성 및 효율성 등 향후 연구가 필요하다.

참고문헌

[1] K. Namhi, P. Ilkyun, and K. Younghan, “Ubiquitous Zone Networking Technologies for Multi-hop Based Wireless Communications,” IWSOS 2006, LNCS 4124, pp. 233~235, September 2006.

[2] S. Rafaeli and D. Hutchison, “A Survey of Key Management for Secure Group Communication,” ACM Computing Surveys 35, pp.309-329, September 2003.

[3] D.S. Devi and G.Padmavathi, “Performance of Cluster-Based Multicast Key Distribution Scheme for Mobile AdHoc Networks,” IJCA, VOL.1, No.23, August 2010

[4] A.Rossi, S.Pierre and S.Krishnan, “An Efficient and Secure Self-Healing Scheme for LKH,” Jounal of Network and Systems Management, VOL.18, No.3, pp.327-347, May 2010.

[5] T. Aurisch, “Using key trees for securing military multicast communication”, IEEE MILCOM 2004, October 2004.

[6] V. Hubenko, R. Raines, R. Baldwin, B. Mullins, R. Mils and M. Grinmaila, “ A Secure and Effiecient Satellite-based Multicast Architecture,” IEEE, Radio and Wireless Symposium, pp.227-230, January 2008

[7] S.shnthi, M.Aramudhan, and A.Shanmugasundaram, “Scarable Dynamic Key Based Group Key Management System,” IJCSNS, VOL.10, No.9, September 2010.

[8] C. K. Wong, M. G. Gouda, and S. S. Lam, "Secure Group Communications Using Key Graphs," IEEE, Transaction on Networking, VOL.8, NO.1, pp.16-30, February 2000.

[9] S. Mittra, "Iolus: A Framework for Scalable Secure Multicasting," Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, pp.277-288, October 1997.