■ 2008년도 학생논문 경진대회 수상작

무선 메쉬 네트워크에서의 아이디 기반 프록시 암호화를 이용한 안전한 다대다 멀티캐스트 기법

(Identity-Based Secure Many-to-Many Multicast in Wireless Mesh Networks)

허 준 범 † 윤 현 수 ††
(Junbeom Hur) (Hyunsoo Yoon)

요 약 무선 메쉬 네트워크 환경에서 그룹통신은 동적으로 변화하는 중계 메쉬 노드, 서로 다른 도메인의 그룹 간 통신에 대한 접근 제어, 그리고 네트워크를 관리하는 중앙화된 관리서버의 부재 등의 문제로 인해 관리가 어려워진다. 그룹의 멤버 뿐 아니라 위상이 동적으로 변화하는 무선 메쉬 네트워크 환경에서의 다대다(many-to-many) 멀티캐스트는 각 그룹 관리자가 자신의 그룹 멤버를 독립적으로 관리하며 그룹간 통신을 제어하는 다수의 하위 그룹으로 이루어진 비중앙화된 구조에 기반해서 구성될 수 있다. 본 논문에서는 네트워크의 위상을 고려한 비중앙화된 그룹키 관리 기법을 제안한다. 제안하는 프로토콜에서 각 멀티캐스트 송신자는 아이디 기반 암호화 알고리즘을 이용해서 분산화된 방법으로 각 그룹키를 그룹 멤버에게 전달하게 된다. 아이디 기반 암호화 기법은 그룹 멤버 뿐 아니라 메쉬 노드의 동적인 변화에도 효율적인 키관리를 가능케 하기 때문에 다대다 멀티캐스트 환경에서 키 갱신에 필요한 통신 회수 및 저장해야 할 키의 크기가 줄어드는 장점이 있다. 따라서 제안한 기법은 중앙화된 네트워크 관리자가 없고, 다수의 서비스 제공자가 그들의 그룹 통신을 독립적으로 관리하는 대규모의 동적인 메쉬 네트워크에서의 다대다 그룹통신 환경에 가장 적합하다.

키워드 : 아이디 기반 암호화, 다대다 멀티캐스트, 안전한 그룹키 관리, 메쉬 네트워크

Abstract Group communication in a wireless mesh network is complicated due to dynamic intermediate mesh points, access control for communications between different administrative domains, and the absence of a centralized network controller. Especially, many-to-many multicasting in a dynamic mesh network can be modeled by a decentralized framework where several subgroup managers control their members independently and coordinate the inter-subgroup communication. In this study, we propose a topology-matching decentralized group key management scheme that allows service providers to update and deliver their group keys to valid members even if the members are located in other network domains. The group keys of multicast services are delivered in a distributed manner using the identity-based encryption scheme. Identity-based encryption facilitates the dynamic changes of the intermediate relaying nodes as well as the group members efficiently. The analysis

· This research is supported by the Ubiquitous Computing and Network (UCN) Project, Knowledge and Economy Frontier R&D Program of the Ministry of Knowledge Economy(MKE) in Korea as a result of UCN's subproject 09C1-T1-20S, and the Korea Science and Engineering Foundation (KOSEF) grant funded by the Korea government(MEST)(No. R01-2007- 000-20865-0).

† 학생회원 : 한국과학기술원 전산학과
jbhur@nslab.kaist.ac.kr
†† 종신회원 : 한국과학기술원 전산학과 교수
hyoon@nslab.kaist.ac.kr

논문접수 : 2009년 8월 28일
심사완료 : 2009년 10월 12일

정보과학회논문지: 정보통신 제37권 제1호(2010.2)

result indicates that the proposed scheme has the advantages of low rekeying cost and storage overhead for a member and a data relaying node in many-to-many multicast environment. The proposed scheme is best suited to the settings of a large-scale dynamic mesh network where there is no central network controller and lots of service providers control the access to their group communications independently.

Key words : many-to-many multicast, Identity-based proxy encryption, Mesh network, secure group key management

1. 서 론

무선 메쉬 네트워크는 기존의 WiFi 네트워크와 같은 전통적인 네트워크를 이용하는 것 보다 보다 저렴한 비용으로 네트워크를 구성할 수 있기 때문에 네트워크의 서비스 제공자에게 유용한 선택이 될 수 있다[1]. 무선 메쉬 네트워크는 다수의 동적 메쉬 노드(mesh point)로 구성되는데, 메쉬 노드는 네트워크의 트래픽을 다른 지역으로 중계해 줌으로써 네트워크의 서비스 영역을 넓혀 주게 된다. 무선 메쉬 네트워크는 네트워크의 그룹 멤버들이 서비스 영역 밖에 있는 경우라도 가입한 멀티캐스트 서비스에 접근할 수 있는 유용한 해결책을 제안한다. 최근, IEEE 802.16 그리고 IEEE 802.11s Working Group 등의 네트워크 설계 그룹에서 WiMAX[2]와 무선랜 네트워크 환경에서 메쉬 네트워크를 구성할 수 있도록 하는 표준안을 연구 및 제안하고 있다. 앞으로의 대규모 무선 메쉬 네트워크는 각기 서로 다른 네트워크 그룹이 독립적으로 관리하는 다수의 도메인으로 구성될 것으로 예상된다[3]. 그러나 이러한 이기종 메쉬 네트워크 환경에서의 멀티캐스트 서비스가 각기 다양한 독립적 네트워크의 협력으로 확장됨으로써 중계 메쉬 노드에 대한 데이터 비밀성 제공, 그룹멤버 및 메쉬 노드의 가입 및 탈퇴 시 역방향/순방향 통신 안전성(backward/forward secrecy)[4] 보장을 위한 효율적인 그룹키 갱신, 그리고 신뢰할 수 있는 중앙화된 키 분배 센터(key distribution center)가 없는 환경에서의 비중앙화 그룹키 관리 등의 다양한 네트워크 보안 이슈들이 생기게 된다.

대규모의 동적 메쉬 네트워크 환경에서는 서로 다른 관리 도메인의 동적인 그룹들과 전체 네트워크를 관리하는 신뢰할 수 있는 중앙 서버가 없는 등의 인프라가 구축되지 않은(infrastructure-less)[1] 특성으로 인해 키 분배가 복잡해지게 된다. 이러한 메쉬 네트워크 환경에서는 그룹 멤버 뿐 아니라 데이터를 중계해 주는 중간 메쉬 노드들 또한 언제든지 네트워크에 참여 또는 탈퇴할 수 있다. 게다가 각 멀티캐스트 서비스를 제공하는 제공자의 수가 증가할 수록, 중계 메쉬 노드가 관리해야하는 그룹 내(inter-group) 그리고 그룹 간(inter- group) 통신은 훨씬 복잡해지게 되고, 메쉬 노드가 관리해야 할 키의 양 또한 크게 증가할 수 있게 된다(proxy space problem)[5]. 비밀성이 보장되어야 하는 그룹 회의 및 다수의 전송자에 의한 비디오 스트리밍 서비스와 같이 WiMAX 포럼[6]에서 언급하고 있는 다대다(many-to-many) 그룹 통신을 사용하는 많은 애플리케이션들은 각 멤버가 잠재적으로 전송자 뿐 아니라 수신자도 될 수 있기 때문에[7], 각 멤버 및 메쉬 노드에게 다수의 그룹키 관리를 위한 더 많은 자원을 요구하게 된다.

그룹키 관리 기법은 크게 중앙화(centralized), 비중앙화(decentralized) 알고리즘으로 나뉠 수 있다[4]. 중앙화 알고리즘으로는 키 트리를 이용한 LKH(logical key hierarchy)[8]와 단방향 해수 함수를 이용한 OFT(one-way function tree)[9] 등이 제안되었는데, 이러한 중앙화 알고리즘에서는 신뢰성 있는 하나의 그룹 관리자가 전체 그룹 멤버를 관리하기 위해 논리적인 키 트리를 유지하여 합법적인 그룹 멤버들에게 그룹키를 분배하게 된다. 그러나 이러한 중앙화된 그룹키 알고리즘은 그룹 관리자가 전체 네트워크의 신뢰성에 직결되기 때문에 "a single point of failure" 문제를 가지고 있으며 인프라가 갖추어있지 않은 동적인 메쉬 네트워크의 특성에 적합하지 않다. 또한 한 멤버의 가입 또는 탈퇴가 전체 그룹의 그룹키에 영향을 미치기 때문에 "1-affects-n" 확장성 문제를 가지고 있다[10]. 반면에, Iolus[10]와 같은 비중앙화 알고리즘은 전체 그룹을 다수의 독립적인 하위 그룹으로 나누고 각 그룹의 관리자가 자신의 그룹을 독립적으로 관리하게 함으로써 그룹 멤버의 변화를 해당 그룹으로만 한정시킬 수 있기 때문에 확장성 측면에서의 장점을 갖게 된다. 이러한 특성은 중앙화 그룹키 관리 기법에서의 문제점인 신뢰성 및 확장성 문제를 완화시키게 되며, 각각 독립적으로 관리되는 다수의 이기종 도메인으로 구성된 메쉬 네트워크를 설계하는데에 적합한 모델을 제공한다.

중간에서 데이터를 중계해 주는 메쉬 노드들이 서로 다른 도메인에서 관리되는 경우, 각 도메인 간 신뢰성 통합이 결여될 수 있다. 특히 이기종 메쉬 네트워크 환경에서는 멀티캐스트 서비스 영역이 동적인 메쉬 노드에 의해 빈번하게 변화될 수 있기 때문에 이러한 문제는 쉽게 발생할 수 있다. 또한, 메쉬 네트워크에서는 전체 네트워크에 대한 인프라가 갖추어지기 어렵기 때문

에 신뢰할 수 있는 중앙의 키 분배 센터를 기대하기 어렵다. 본 논문에서는 아이디 기반 암호화(Identity-based encryption)를 이용한 다대다 그룹 통신을 위한 그룹키 관리 기법을 제안하는데, 제안하는 기법은 다음과 같은 특성을 가지고 있다: (1) 중앙 키 분배 센터가 불필요한 분산화된 방식의 그룹키 분배, (2) 그룹 멤버의 변화를 지역적인 하위 그룹으로 한정시키는 비중앙화 그룹키 관리, (3) 신뢰할 수 없는 중계 메쉬 노드에 대한 데이터 비밀성 제공, (4) 그룹 멤버 또는 메쉬 노드의 가입 및 탈퇴 시 안전한 다대다 그룹 통신을 위한 확장성 있는 그룹키 갱신. 제안한 기법은 그룹 통신의 역방향 안전성 및 순방향 안전성을 보장한다. 또한 전송자가 많은 네트워크 환경일 지라도 아이디 기반의 암호화 알고리즘을 사용함으로써 중계 노드가 관리해야하는 키의 양을 줄일 수 있는 특징이 있다[5]. 아이디 기반 암호화 알고리즘은 각 메쉬 노드가 다른 메쉬 노드 또는 그룹의 많은 키를 저장하지 않고도 공개된 아이디를 이용해 그들의 공개키를 생성해 낼 수 있게 한다. 본 논문의 분석 결과에 따르면 제안한 기법은 동적인 메쉬 네트워크 환경에서 다대다 멀티캐스트를 위한 그룹키 관리 통신 비용 및 메모리 비용이 적게 드는 장점이 있다.

본 논문은 다음과 같이 구성된다. 2절에서는 기존에 제안된 안전한 그룹통신을 위한 그룹키 관리 기법을 분석한다. 3절에서는 다대다 멀티캐스트를 위한 네트워크 구조를 설명한다. 4절에서는 아이디 기반의 프록시 암호화를 이용한 비중앙화 그룹키 관리 기법을 제안한다. 5절에서는 제안한 알고리즘의 성능을 기존의 알고리즘과 비교 분석하고 안전성을 증명한다. 6절에서 본 논문의 결론을 맺는다.

2. 관련 연구

중앙화 그룹키 관리기법에서는 키 분배 센터가 논리 키 트리(logical key tree)를 유지하고 관리하게 된다. LKH[8] 기법에서 키 트리의 말단(leaf) 노드에는 각 그룹 멤버가 할당되고, 트리의 중간 노드들에는 각각 키암호화키(key encryption key)가 할당된다. 그룹의 멤버는 자신의 말단 노드로 부터 트리의 최상위 노드(root)에 이르는 통로 상의 모든 패스키(path key)를 알고 있다. 만약 그룹에 멤버가 가입 또는 탈퇴할 경우, 키 분배 센터는 그룹 통신의 역방향 또는 순방향 안전성을 위해 해당 패스키를 갱신하고 그 갱신된 패스키를 이용해서 새로운 그룹키를 유효한 그룹 멤버들에게 안전하게 전송한다. 역방향 안전성은 새로 가입한 멤버가 그룹에 가입하기 이전에 전송된 그룹 통신을 알 수 없어야 함을 의미하고, 순방향 안전성은 탈퇴한 멤버가 그 이후의 그룹 통신에 접근할 수 없어야 함을 의미한다[4]. 그러면 해당 키암호화키를 알고 있는 멤버는 그룹키 갱신 메시지를 복호화하고 새로운 그룹키를 얻게 된다. 그룹키 갱신에 필요한 통신 비용을 줄이기 위해 LKH 알고리즘에 기반한 다양한 기법들이 제안되었다[9,11]. 그러나 전체 네트워크의 모든 멤버가 하나의 키 분배 센터에 의해서 관리되기 때문에 센터의 "a single point of failure" 문제가 존재한다. 또한 한 멤버의 변화가 전체 네트워크의 그룹키에 영향을 미치기 때문에 "1-affects-n" 문제[10] 또한 중앙화 그룹키 관리 알고리즘에서는 해결되기 어려운 문제점이다.

비중앙화 알고리즘은 이러한 중앙화 알고리즘의 확장성 및 안정성 문제를 해결하는데 유용한 특성을 가지고 있다. Iolus[10]와 같은 비중앙화 그룹키 관리 기법에서는 하나의 멀티캐스트 그룹을 다수의 그룹으로 나누고 서로 다른 관리자가 각 그룹을 관리한다. 각 그룹의 관리자는 그룹 간 통신을 조정하고 각 그룹의 멤버의 변화에 따른 자신의 그룹키를 독립적으로 관리한다. 따라서 멤버의 변화는 해당 그룹 안에서만 지역적으로 영향을 미치게 되기 때문에 확장성 문제가 해결될 수 있다. 그러나 그룹 간의 안전한 통신을 위해서는 각 그룹의 관리자가 다른 그룹으로 부터 전송된 암호화된 메시지를 복호화 할 수 있기 때문에 메시지의 평문 또는 그룹의 비밀키가 각 그룹의 관리자에게 노출되게 된다. 이러한 특성은 그룹 통신의 비밀성이 각 그룹의 관리자에 대한 신뢰성에 완전하게 의존하게 되는 "trusting third party" 문제를 발생시킨다[10].

Dondeti[15]는 "trusting third party" 문제를 해결하기 위해 DEP(dual encryption protocol) 알고리즘을 제안했다. DEP 알고리즘에서 그룹 멤버들은 몇개의 하위 그룹으로 나뉘고, 각 하위 그룹은 하위 그룹 관리자(SGM)가 관리하게 된다. 이 기법에서는 데이터 암호화키(DEK)를 전달하기 위해 세 가지의 키암호화키(KEK)를 사용하는데 어떠한 그룹 관리자도 동시에 모든 키를 알지 못하게 함으로써 위의 문제를 해결하고 있다. 그러나 DEP 기법은 주기적인 키갱신 알고리즘을 사용하기 때문에 탈퇴한 멤버가 데이터 암호화 키가 갱신되기 전까지는 여전히 그룹 통신에 접근할 수 있다. 따라서 역방향 및 순방향 그룹 통신 안전성을 보장하지 못한다.

Chiu[13]는 기존의 ElGamal 프록시 암호[5]를 송신자 기반의 멀티캐스트 트리로 확장시킴으로써 비중앙화 그룹키 알고리즘을 제안했다. 프록시 암호는 비밀키를 가지고 있는 중간의 노드가 한 사람의 비밀키로 암호화되어 있는 암호문을 다른 사람의 암호문으로 변형시키는 암호화 기법을 의미하는데, 원자성(atomicity property)으로 인해 그 변형 과정에서 평문이나 비밀키의 어떠한 정보도 중간 노드에게 노출되지 않는다는 특징

이 있다. 이러한 프록시 암호 알고리즘의 특성은 송신자와 수신자 사이에 다수의 신뢰할 수 없는 노드가 존재하는 네트워크 환경에서 안전한 멀티캐스트를 구현하는 데에 사용될 수 있다. 신뢰할 수 있는 키 분배 센터는 송신자와 수신자들에게 비밀키를 분배하고, 멀티캐스트 트리의 위상에 따라 비밀 키를 계산해서 각 중계 노드에게 전송한다. 멤버가 가입 또는 탈퇴 할 경우, 키센터는 그 멤버의 해당 노드의 비밀키를 갱신한다. 이러한 기법은 메시지 전달 과정에서 비밀성을 만족시켜 주지만 여전히 전체 네트워크의 위상을 이해하고 각 멀티캐스트 트리의 비밀키를 관리하기 위해 중앙화된 키 관리 센터가 필요하다는 특징이 있다.

Huang[14]은 [13]의 기법을 확장시켜 송시자로부터 새로 가입한 수신 노드에 이르는 중간 노드의 비밀키들의 통합 값을 수신자에게 전달함으로써 수신자가 키를 계산해 낼 수 있게 함으로써 중앙화된 키 분배 센터를 제거 시킬 수 있게 하였다. 이 기법에서 프록시 암호는 그룹키 갱신 메시지를 전달하는 과정에서 사용되고, 그룹 통신은 새롭게 갱신된 그룹키를 이용해서 암호화되게 된다. Huang의 방식은 중간 노드의 비밀키 분배 과정에서 중앙화된 키 분배 센터가 불필요하다는 특성이 있다. 그러나, 키 결합과정에 필요한 계산량의 증가 및 그룹 통신의 안전성 저하 등의 문제가 발생한다. 이 알고리즘에서 그룹키는 주기적인 갱신(periodic rekeying) 방식에 따라 이루어지기 때문에, 기존의 DEP[15] 알고리즘과 같이 그룹키가 얼마나 자주 갱신되는지에 따라 그룹 통신의 순방향 안전성 및 역방향 안전성이 영향을 받게 되는 단점이 존재한다. 게다가, [13]과 [14]의 방식에서는 중계 노드들이 모든 송신 및 수신 그룹에 해당하는 수, 혹은 이웃 노드의 수에 비례하는 키를 저장해야 하는 문제가 있다. 따라서 네트워크에서 송신 노드 혹은 이웃하는 노드 등이 증가할수록 메모리 비용 및 네트워크의 위상 변화에 다른 키 갱신 비용이 증가하게 된다. 이러한 문제는 멤버의 수가 많고 자원이 한정되어 있는 단말 노드가 중계 메쉬 노드의 역할을 수행하게 되는 환경에서는 매우 중요한 문제가 될 수 있다. 중간 노드의 메모리 부담 문제는 기존의 RSA 기반의 프록시 암호화를 이용한 키 분배 방식에서도 필연적으로 생기게 된다[5].

3. 다대다 그룹 통신

본 논문에서는 [7]의 연구와 같이 다대다 그룹 통신을 다수의 일대다(one-to-many) 그룹 통신으로 구성되어 있다고 가정한다. 메쉬 네트워크에서의 다대다 멀티캐스트는 다수의 송신자 기반의 멀티캐스트 트리로 구조화될 수 있다. 트리는 네트워크의 위상에 따라 구성되며 각 루트 노드는 멀티캐스트 송신자가 할당된다. 트리의 중간 노드는 멀티캐스트 데이터를 중계해 주는 메쉬 노드가 할당되게 되는데, 각 노드는 독립적으로 하위 그룹을 형성함으로써 하위 그룹 멤버를 관리할 수 있다. 송신자는 자신의 멀티캐스트 그룹의 그룹키 및 세션을 독립적으로 관리하기 때문에, 각 멀티캐스트 서비스의 세션은 동기화 될 필요가 없으며 한 멀티캐스트 그룹의 송신자는 다른 그룹의 수신자가 될 수도 있다. 메쉬 노드는 자신의 하위 그룹 멤버쉽 및 하위 그룹키를 관리하고 각 멀티캐스트 그룹의 송신자로 부터 전송된 그룹키 갱신 메시지를 자신의 하위 그룹 멤버들에게 전송하는 역할을 한다.

이러한 메쉬 노드는 일반적인 AP(access point)와 같은 고정된 메쉬 라우터, 또는 이동하는 차량이나 보행자가 사용하는 통신장비와 같이 이동성이 있는 동적인 노드들이 될 수 있다. 따라서 본 논문에서는 각 사용자 뿐 아니라 메쉬 노드 또한 네트워크에 동적으로 가입 또는 탈퇴할 수 있다고 가정한다.

제안하는 다대다 그룹 통신을 위한 네트워크 시스템은 다수의 멀티캐스트 서비스의 송신자 및 수신자, 그리고 다수의 하위 그룹으로 이루어진다. 각 구성 요소는 다음과 같은 기호로 나타내어진다. $G=\{G_1,\ldots,G_s\}$는 네트워크에서 멀티캐스트 그룹의 집합 또는 멀티캐스트 서비스를 나타낸다. $U=\{u_1,\ldots,u_n\}$는 사용자의 전체 집합을 나타낸다. $P=\{P_1,\ldots,P_m\}$는 메쉬 노드의 집합, 그리고 $SG=\{SG_1,\ldots,SG_m\}$는 하위 그룹의 집합을 나타낸다. s_j는 $G_j \in G$의 송신자, 그리고 $r_j \subseteq U$는 $s_j (1 \le j \le s)$로부터 전송되는 멀티캐스트 서비스 G_j에 접근할 수 있는 사용자의 집합을 나타낸다.

4. 그룹키 관리 기법

이번 절에서는 다대다 멀티캐스트를 위한 다중 그룹키 관리 기법을 제안한다. 그룹키 갱신 과정은 메쉬 노드로부터의 하위 그룹키 갱신 및 멀티캐스트 송신자로 부터의 그룹키 전달 과정으로 구성된다. 그룹키 갱신 메시지는 아이디 기반의 암호화 기법을 이용해서 분산화된 방식으로 멀티캐스트 트리를 따라 재암호화되며 전달된다.

4.1 기호 및 가정

제안하는 기법에서 모든 사용자 및 메쉬 노드, 그리고 모든 그룹은 유일한 아이디를 가지고 있으며, 각 멤버는 자신의 아이디와 자신이 속해 있는 그룹의 아이디를 알고 있다고 가정한다. 메쉬 노드는 전송받은 암호문을 아이디 기반 암호화 알고리즘을 이용해 올바르게 변형시켜서 하위 그룹 멤버 및 자식 메쉬 노드에게 재전송해 준다고 가정한다.

제안하는 그룹키 관리 기법에서 사용하는 기호는 다

음과 같다.

- ID_x: 하위 그룹 또는 메쉬 노드 x의 아이디. 예를 들어, ID_{SG_j}와 ID_{p_j}는 각각 하위 그룹 SG_j와 메쉬 노드 p_j의 아이디를 가리킨다.
- GK_j^i: 멀티캐스트 서비스 G_j의 i번 째 세션에서 사용되는 그룹키. GK_j^i는 서비스 G_j에 i번째 세션에 가입되어 있는 그룹 멤버 사이에서 안전한 그룹 통신을 위해 사용된다. GK_j^i는 멀티캐스트 서비스 G_j의 송신자 s_j와 그룹 멤버 집합 r_j 사이에 공유된다. i 세션에서의 $p_l(\notin r_j)$에 대해서, GK_j^i는 p_l이 s_j로 부터 전송된 키갱신 메시지를 재암호화할 때 메시지의 평문을 복호화하지 못하도록 한다.
- PK_j^l: 하위 그룹 SG_l의 메쉬 노드 p_j가 관리하는 하위 그룹키. PK_j^l는 메쉬 노드 p_j와 SG_l의 하위 그룹 멤버들 간에 공유되는 비밀키이다. 하위 그룹키는 멤버의 변화를 해당 하위 그룹으로 한정시키는데에 사용된다.
- $H(k,m)$: k와 메시지 m을 입력으로 받아 해쉬값을 출력하는 암호학적으로 안전한 단방향 키해쉬(keyed-hash) 함수.
- $PRF(m)$: m을 입력으로 받아 의사 난수를 생성하는 의사 난수 생성 함수.

4.2 페어링(pairing) 및 이중선형(bilinear form)

메쉬 노드는 아이디 기반 암호화 알고리즘을 이용해서 그룹키 갱신 메시지를 변형하는 역할을 담당하는데, 이 과정에서 효과적으로 계산 가능한 이중선형 사상(map)을 사용하게 된다.

$\mathbb{G}_1$과 $\mathbb{G}_2$를 차수가 q(q는 임의의 큰 소수)인 두 개의 순환 그룹 (cyclic group)이라고 하자. 사상 $e:\mathbb{G}_1\times\mathbb{G}_2\rightarrow\mathbb{G}_2$는 모든 $P,Q\in\mathbb{G}_1$과 $a,b\in Z_q^*$에 대해서 $e(aP,bQ)=e(P,Q)^{ab}$를 만족할 경우 이중선형(bilinear)이라고 정의되고, $\mathbb{G}_1$의 생성자 P에 대해서 $e(P,P)\neq 1$을 만족할 경우 비축중(non-degenerate) 성질을 만족한다고 할 수 있다.

아이디 기반 암호화 알고리즘은 두 그룹 $\mathbb{G}_1$과 $\mathbb{G}_2$ 사이에서 $\mathbb{G}_1$에서의 선택적 Bilinear Diffie-Hellman 문제의 어려움에 그 안전성을 기반으로 하며, 효과적으로 계산가능한 비축중 이중선형 사상 $e:\mathbb{G}_1\times\mathbb{G}_2\rightarrow\mathbb{G}_2$를 이용해서 구현된다. 타원곡선 상에서의 Weil 페어링[16]이나 Tate 페어링[17] 등이 효과적으로 계산 가능한 이중선형 맵으로 사용될 수 있다. 이러한 효율적이고 실용적인 맵을 찾는 것은 [18-20]에서 찾아볼 수 있다.

4.3 아이디 기반 암호화를 이용한 키분배 기법

제안하는 아이디 기반 암호화 기법은 [16]에서 처음 제안된 FullIdent 기법에 기반을 두고 설계되었다. [16]의 기법은 선택적 평문 공격(chosen plaintext attack, CPA)에 안전한 알고리즘을 Fujisaki-Okamoto 변환[21]을 통해 변형함으로써 선택적 암호문 공격(chosen ciphertext attack, CCA)에 대한 안전성을 보장하였다. 그러나 CPA 안전성은 많은 실제적인 키관리 기법에서 요구하는 단계의 안전성이다[5,13,14]. 따라서 우리는 CPA에 안전한 아이디 기반의 암호화 기법을 제안한다.

초기 셋업 단계에서 신뢰할 수 있는 키서버는 마스터 비밀키 $s\in Z_q^*$, 마스터 공개키 sP를 생성하고 각 사용자 x에게 비밀키 sID_x를 발급한다. (여기서는 $ID\in\mathbb{G}_1$라고 가정한다.) 이 초기 셋업 단계 이후 모든 키분배 알고리즘은 키서버 없이 비중앙화된 방식으로 이루어지게 된다. 제안하는 아이디 기반 암호화 기법은 다음과 같은 Encrypt, Decrypt 알고리즘으로 구성된다.

1. Encrypt: Encrypt 알고리즘은 송신자가 메시지를 암호화하거나, 메쉬 노두가 전달받은 비밀문을 변환할 때 사용된다. 이 알고리즘은 두개의 알고리즘으로 구성된다.

- Encrypt$_S$: 이 알고리즘은 멀티캐스트 데이터 전송자에 의해 수행된다. i 세션에 해당 하위 그룹의 메쉬 노드가 p_n인 송신자 s_l에 대해서, Encrypt$_S$ 알고리즘은 난수 $r\in Z_q^*$과 $\sigma\in\mathbb{G}_2$를 선택한다. 그리고 메시지 m, 아이디 $ID_{p_n}\in\mathbb{G}_1$, 그리고 G_l의 현재 그룹키 GK_l^i를 입력으로 받아들여 암호문 $\langle U,V,W\rangle=\left\langle rP,\sigma\cdot e(ID_{p_n},sP)^r,m\cdot H(GK_l^i,\sigma)\right\rangle$을 출력한다. m은 $W=m\cdot H(GK_l^i,\sigma)$의 형태로 암호화 되는데 이것은 $W=E_{H(GK_l^i,\sigma)}(m)$로 대체될 수 있다(여기서 E는 안전한 대칭 암호 기법을 나타낸다[21]).
- Encrypt$_P$: 이 알고리즘은 메쉬 노드에 의해 수행된다. 하위 그룹키가 $PK_n^l\in Z_q^*$인 하위 그룹 SG_l의 메쉬 노드 p_n에 대해서 알고리즘은 난수 $r'\in Z_q^*$을 선택하고 암호문 $\langle U,V,W\rangle$을 입력으로 받아 다음의 두 암호문을 출력한다: (1) 멀티캐스트 트리 상에서 p_n의 자식 메쉬 노드 p_j를 위한 $\langle U',V',W\rangle=\left\langle r'P,V\cdot\frac{e(ID_{p_j},sP)^{r'}}{e(U,sID_{p_n})},W\right\rangle$, (2) SG_l의 하위 그룹 멤버를 위한 $\langle U,V',W\rangle=\left\langle U,V\cdot\frac{e(U,PK_n^i\cdot ID_{SG_l})}{e(U,sID_{p_n})},W\right\rangle$. p_n이 말단 메쉬 노드이거나 또는 하위 그룹 멤버가 없을 경우 암호문을 재생성하지 않는다.

2. Decrypt: 이 알고리즘은 그룹 멤버들에 의해 수행된다. Decrypt 알고리즘은 수신한 암호문 $\langle U'', V'', W\rangle$을 하위 그룹키와 현재 그룹키를 이용해 복호화한다. 세션 i에 그 메쉬 노드가 p_j인 SG_n에 위치한 $u_t \in r_l$가 암호문을 복호화하기 위해서 Decrypt 알고리즘은 다음을 수행한다: (1) $V''/e(U'', PK_j^n \cdot ID_{SG_n}) = \sigma$, (2) $W/H(GK_l^i, \sigma) = m$, (3) 암호문 $\langle U'', V'', W\rangle$의 복호화 결과로 m 출력.

그림 1은 송신자 s_1과 s_2가 그룹 멤버 $u_1, u_3 \in r_1$가 $u_2 \in r_2$에게 그룹키 갱신 메시지를 전달하는 일부분의 과정을 보여주고 있다. 여기서 m_1과 m_2는 각각 G_1과 G_2의 새로운 그룹키를 포함하고 있다. SG_D의 u_2는 하위 그룹키 PK_4^D와 그룹키 GK_2^i를 알기 때문에 수신한 암호문을 $W_2/H(GK_2^i, V_2''/e(U_2', PK_4^D \cdot ID_{SG_D})) = m_2$의 연산을 통해 복호화하고, $m_2 (= GK_2^{i+1})$를 알아낼 수 있다. 송신자가 멀티캐스트 데이터를 전송할 때는 새로운 그룹키로 암호화된 후 전송된다.

Encrypt$_S$ 알고리즘에서 송신자는 $e(ID, sP)$의 페어링 연산을 수행해야 한다. 이 연산은 메시지와 독립적으로 실행될 수 있기 때문에 한번 계산된 결과를 반복 사용할 수 있다. 따라서 $e(ID, sP)$ 연산을 한번 수행하게 되면, Encrypt$_S$를 계산하는데 필요한 계산량은 ElGamal 암호화 알고리즘과 거의 같게 된다. Encrypt$_P$ 알고리즘에서 메쉬 노드는 Encrypt$_S$ 보다 최대 두 번의 페어링 연산 $e(U, PK \cdot ID)$와 $e(U, sID)$의 연산을 수행하게 된다. 멀티캐스트 트리의 자식 메쉬 노드의 수가 늘어날수록 메쉬 노드가 계산해야하는 Encrypt$_P$의 연산량은 [13]과 [14]의 기법에서와 마찬가지로 자식 노드의 수에 비례해서 증가하게 된다. Decrypt 알고리즘은 단순한 페어링 연산으로 이루어진다. [17]과 [22]는 supersingular 타원 곡선 상에서 Tate 페어링 연산이 1 GHz 펜티엄 III 프로세서와 156Mb RAM의 시스템에서 구현될 경우 30ms 정도 소요됨을 보여준다. 최근 PDA(personal digital assistant)와 같은 개인 장비들이 500MHz 이상의 프로세서와 충분히 확장 가능한 외부 기억장치를 장비하고 있음을 고려할 때, 이러한 연산량은 보다 가용자원이 큰 이동 장치 기반의 애플리케이션 등에 충분히 실용적이라고 볼 수 있다.

4.4 그룹키 갱신

멤버가 그룹에 가입 또는 탈퇴할 경우, 현재 사용하는 그룹키는 역방향 및 순방향 그룹 통신 안전성을 위해 갱신되어야 한다. 제안한 기법에서는 매 멤버 가입 또는 탈퇴 시 세션이 변화하며 그룹키 갱신이 이루어진다.

4.4.1 멤버 가입

가입하는 사용자는 먼저 가장 가까운 메쉬 노드에 가입 요청을 한다. 그 메쉬 노드는 그 멤버의 부모 메쉬 노드가 되고, 가입 요청 메시지를 멀티캐스트 트리의 패스를 따라 송신자에게 전달한다. 만일 송신자가 사용자

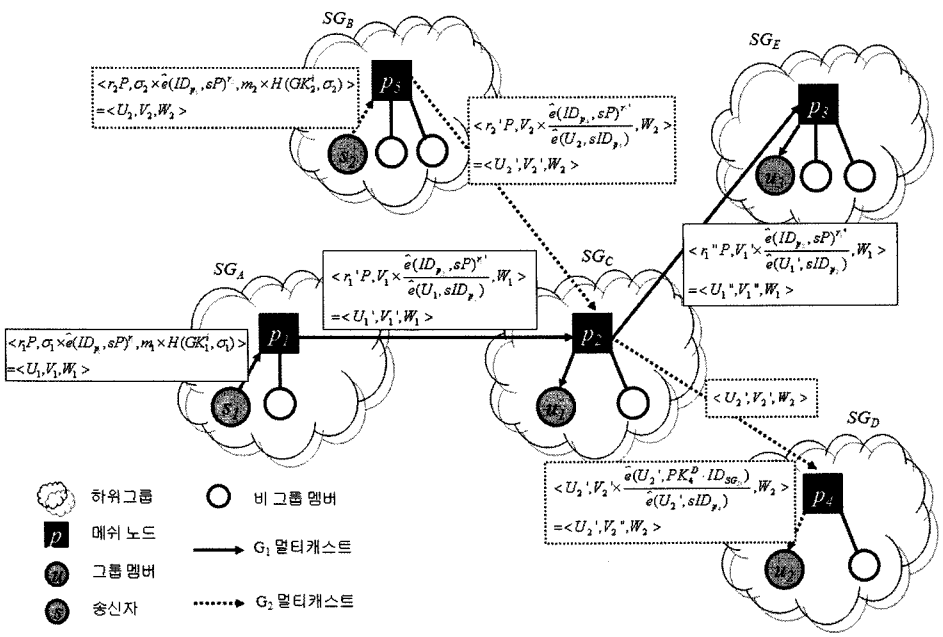


그림 1 아이디 기반 프록시 암호를 이용한 다대다 멀티캐스트 메시지 전송 과정

를 인증하게 되면, 세션은 변화하고 그룹키는 키 갱신 과정을 통해 갱신된다. 멤버가 $i-1$ 번째 세션에 하위 그룹 SG_y의 메쉬 노드 p_j를 통해 멀티캐스트 서비스 G_x에 가입할 경우, 그룹키 갱신 과정은 다음과 같다.

1. 그룹키 GK_x^{i-1}는 $GK_x^i = PRF(GK_x^{i-1})$ 연산을 통해 GK_x^i로 갱신된다.
2. 송신자 s_x는 새로운 그룹키 GK_x^i를 새로 가입한 멤버에게 안전하게 전송한다.
3. 부모 메쉬 노드 p_j는 자신의 하위 그룹키 PK_j^y를 새로 가입한 멤버에게 안전하게 전송한다.
4. GK_x^{i-1}를 알고있는 기존의 합법적인 멤버들은 의사 난수 생성 함수를 이용해서 새로운 그룹키 GK_x^i를 계산해 낸다.

만일 사용자가 하나 이상의 멀티캐스트 그룹에 가입하고자 할 경우, 모든 그룹에 성공적으로 가입할 때까지 그룹키 갱신 과정을 독립적으로 수행하게 된다.

멤버 가입시 그룹키를 갱신하는 데 요구되는 통신량은 두번의 단일전송(unicast)이다. 그림 2의 예에서 u_1이 G_1에 가입할 경우 GK_1^i와 하위 그룹키 PK_4^D를 각각 송신자 s_1과 부모 메쉬 노드 p_4로부터 전송받게 된다. 이전키를 가지고 있는 모든 멤버들은 새로운 그룹키를 자체적으로 계산하게 된다. 따라서, 두번의 단일전송 이외의 어떠한 추가적인 통신비용은 필요없다. 여기서 송신자와 새로 가입한 사용자 사이의 안전한 통신은 가입한 사용자의 아이디로 암호화함으로써 이루어지게 된다.

4.4.2 멤버 탈퇴

멤버 탈퇴 시 키 갱신 과정은 지역적 하위 그룹키 갱신 후 새로운 그룹키 전달 과정으로 이루어 진다. 멤버가 특정 멀티캐스트 그룹을 탈퇴할 경우, 그 멀티캐스트 그룹의 세션은 변화되고 그 멤버의 부모 메쉬 노드는 하위 그룹키를 갱신하게 된다. 멤버가 i 세션에 하위 그룹 SG_y의 메쉬 노드 p_j로 부터 멀티캐스트 서비스 G_x를 탈퇴할 경우, 그룹키 갱신 과정은 다음과 같다.

1. SG_y의 메쉬 노드 p_j는 새로운 하위 그룹키 $PK_j^{y\prime}$를 이전의 PK_j^y와 독립적인 임의의 값으로 생성한다.
2. 메쉬 노드 p_j는 $PK_j^{y\prime}$를 자신에게 직접 연결된 r_x에 속한 모든 하위 그룹 멤버들에게 안전하게 전송한다.
3. 송신자 s_x는 새로운 그룹키 GK_x^{i+1}를 GK_x^i와 독립적으로 생성하고 Encrypt_S 알고리즘으로 암호화 한 후 멀티캐스트 트리를 따라 전송한다. 그리고 p_j는 수신한 메시지를 Encrypt_P 알고리즘을 이용해 새로 갱신된 하위 그룹키 $PK_j^{y\prime}$를 가지고 재암호화한 후 하위 그룹 멤버들에게 전송한다.

그림 2는 멤버 u_2가 그룹 G_2를 탈퇴할 경우의 지역적 키 갱신 과정의 예를 보여주고 있다. u_2를 제외한 모든 하위 그룹 멤버들은 새로운 하위 그룹키 $PK_2^{B\prime}$를 p_2로부터 전송 받는다. 그러면 s_2는 새로운 그룹키 GK_2^{i+1}를 멀티캐스트 트리를 따라 전송하게 된다. 하위 그룹 멤버의 수를 n으로 나타낼 때, 하위 그룹키를 하위 그룹 멤버들에게 단일 전송을 전달하는 데 필요한 통신 비용은 $O(n)$이다. 이러한 확장성 문제를 향상시키기 위해서 기존의 LKH[8] 혹은 OFT[9]와 같은 중앙화

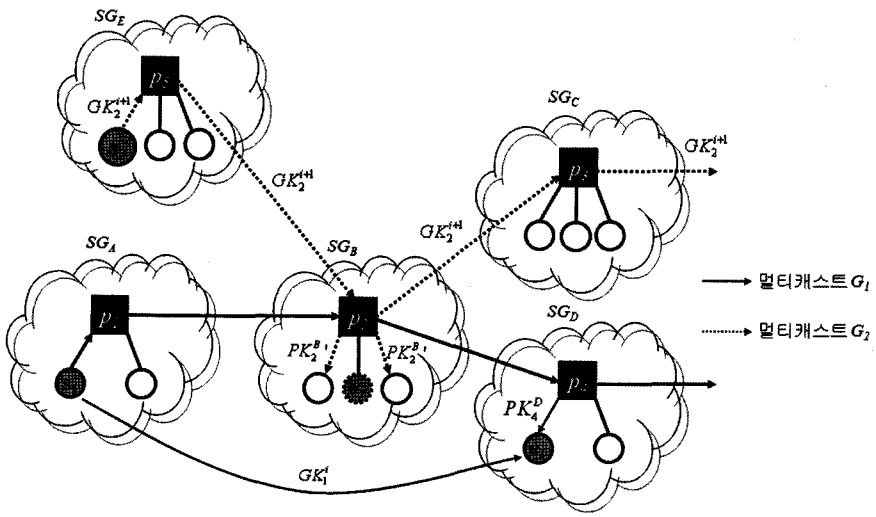


그림 2 멀티캐스트 그룹에서의 멤버 변화

그룹키 관리 알고리즘을 적용시킬 수 있는데, 제안하는 기법에서 LKH를 하위 그룹에서의 키 전달에 적용함으로써 멤버 당 $O(\log n)$ 만큼의 키 저장을 위한 공간을 추가로 요구하면서 키 갱신에 필요한 통신 비용을 $O(n)$로 부터 $O(\log n)$로 줄일 수 있다.

4.5 위상 제어

메쉬 네트워크 환경에서 메쉬 노드는 세션에 따라 동적으로 네트워크에 가입 또는 탈퇴할 수 있기 때문에 사용자들은 변화하는 위상으로 인해 멀티캐스트 서비스 접근에 영향을 받는다. 메쉬 노드의 변화는 멀티캐스트 트리의 위상에 변화를 주며 트리의 패스상으로 연계된 하위 그룹 키들의 관계에 영향을 주게 된다. 특히, 다대다 멀티캐스트 환경에서는 각 하위 그룹이 보다 많은 이웃한 하위 그룹과 연관이 되므로 일대다 그룹 통신에 비해 그룹키 관리가 훨씬 어렵게 된다[5,13,14]. 그러나 이 문제는 제안한 프로토콜에서 해결 될 수 있다.

4.5.1 메쉬 노드 가입

새로운 메쉬 노드가 네트워크에 가입할 때, 기존의 서로 연결된 두 개의 메쉬 노드를 선택한 후 자신을 그 노드 간의 패스 상으로 연결시키거나, 또는 멀티캐스트 트리의 말단 노드로 네트워크에 가입하게 된다. 새로 가입한 노드는 자신의 아이디와 하위 그룹의 아이디를 네트워크에 알리게 되고 다른 메쉬 노드들의 아이디를 전달 받는다.

가입한 메쉬 노드에 멤버가 없을 경우, 혹은 그룹 통신과 관계 없는 사용자들만 멤버로 가지고 있는 경우, 그 노드는 멀티캐스트 트리 상의 부모 노드로 부터 받은 메시지를 자식 노드들에게 해당 ID의 노드에 이를 때 까지 변환 연산 없이 전달만 하게 된다. 예를 들어, 그림 1에서 메쉬 노드 p_2는 자신의 하위 그룹에 G_2에 가입된 그룹 멤버가 없기 때문에 자신의 부모 노드 p_5로부터 전송받은 암호문 $\langle U_2', V_2', W_2 \rangle$를 자식 노드인 p_4에게 변환 없이 중계만 해준다. 이러한 노드들을 비가담(nonpartisan) 노드라고 명명한다. 그 후 멀티캐스트 서비스에 가입한 멤버가 그러한 비가담 노드에 들어올 경우, 그 노드는 자신의 역할을 가담(partisan) 노드로 변경하고 키 갱신 과정을 수행하게 된다. 다대다 멀티캐스트 트리 네트워크에서는 메쉬 노드가 각 멀티캐스트 서비스 마다 독립적인 프로토콜을 수행할 수 있다.

4.5.2 메쉬 노드 탈퇴

메쉬 노드가 네트워크를 탈퇴할 때, 그 노드와 이웃 노드들 간의 연결이 끊어지게 된다. 메쉬 노드가 탈퇴하면 해당 하위 그룹의 멤버 중 한 멤버는 새로운 메쉬 노드로 선택되어 그 탈퇴 노드를 대체하게 되고 자신의 아이디를 네트워크에 알리게 된다. 만일 하위 그룹에 멤버가 없을 경우 그 하위 그룹은 네트워크에서 제거 되고 탈퇴한 노드의 부모 노드 중 한 노드는 탈퇴한 노드의 자식 노드 중 한 노드로 탈퇴한 노드를 대체하고 멀티캐스트 트리의 위상을 재구조화 한다. 제안한 기법에서는 메쉬 노드 탈퇴 시 이전의 ElGamal 기반 혹은 RSA 기반의 프록시 암호화 기법[5,13,14]들과 달리 아이디를 알리는 것 이외의 어떠한 키 갱신 비용도 들지 않게된다. 기존의 기법들은 중간의 노드가 다른 모든 노드 혹은 다른 하위 그룹의 키를 저장해야 하기 때문에 위상 변화로 인한 키 갱신 메시지는 이웃 노드 혹은 송신자의 수가 증가할수록 그에 비례하게 증가하게 된다.

5. 프로토콜 분석

5.1 성능 분석

표 1은 각 알고리즘의 데이터 비밀성 제공, 중앙의 키 분배 센터 필요 여부 등을 나타내며, 각 사용자와 메쉬 노드에 요구되는 메모리 비용 및 그룹키 갱신에 필요한 통신 비용을 보여준다. 또한 표 1은 안전한 데이터 전송을 위해 중간의 메쉬 노드에 대해 요구되는 신뢰 정도를 보여준다.

표 1에서 기호 N과 M은 각각 전체 네트워크 그룹의 멤버 수 및 하위 그룹 멤버의 평균 수를 가리킨다. 네트워크의 멀티캐스트 서비스의 개수는 S, 멀티캐스트 트리에서 각 메쉬 노드의 평균 이웃 메쉬 노드의 수는 P로 나타내어진다. 송신자로부터 수신자에 이르는 패스 상의 평균 노드의 개수는 $L(=\log_P \lceil N/M \rceil)$로 나타낸다. 명확하고 공정한 비교를 위해 네트워크의 모든 멤버는 모든 S 서비스에 가입되어 있다고 가정한다. 따라서 모든 메쉬 노드들은 가담 노드가 된다. 또한 Chiu, Huang, 그리고 본 논문에서 제안한 프로토콜에서 하위 그룹 안에서의 키 갱신 기법은 LKH를 사용한다. Table 1은 비교 결과를 보여준다.

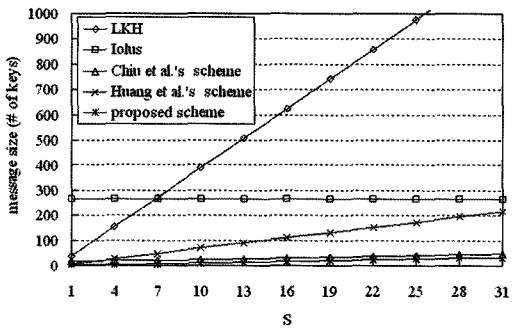
제안한 아이디 기반의 암호화 기법은 분산된 방식으로 그룹키 갱신 메시지를 전달하고 멀티캐스트 트리의 위상을 관리한다. 따라서 제안한 프로토콜에서는 그룹간 하위 그룹키 조정을 위한 중앙화된 키 분배 센터는 필요없게 된다. 이것은 "single point of failure" 문제를 해결한다. 또한 멀티캐스트 패스 상의 메쉬 노드들에 대한 데이터 비밀성은 프록시 암호 함수의 원자성(atomicity property)[5]으로 인해 보장되기 때문에 "trusting third party" 문제 역시 제안한 기법에서 해결될 수 있다.

멤버가 그룹에 가입하는 경우, 제안한 프로토콜은 한 번의 하위 그룹키 전송 및 S 개의 그룹키 전송을 위한 총 $1+S$ 번의 통신이 필요하다. 제안하는 프로토콜은 Huang의 기법에서 처럼 새로 가입하는 멤버에게 El-

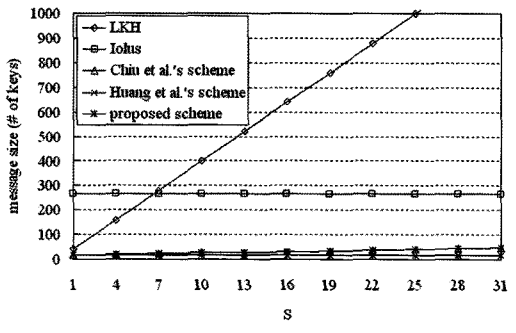
표 1 다대다 멀티캐스트 환경에서 그룹키 관리 프로토콜 비교

	LKH [8]	Iolus [10]	Chiu [13]	Huang [14]	제안 기법
데이터 비밀성	-	no	yes	yes	yes
메쉬 노드 신뢰도	-	total	partial	partial	partial
키분배 센터	yes	no	yes	no	no
키갱신 통신비용 (멤버 가입, 탈퇴)	$S(2\log N-1)$, $2S\log N$	$M+P$, $M+P$	$2\log M-1+S$, $2\log M+S$	$S(L+3)$, $2\log M$	$1+S$, $2\log M+S$
키갱신 통신 비용 (메쉬 노드 가입, 탈퇴)	$S(\log N+1)$, -	P, $M+P$	$S(P+1)$, $S(P+1)$	P, $2P$	0, 0
키 저장 크기 (멤버, 메쉬 노드)	$S(\log N+1)$, -	1, $M+P$	$\log M+1$, $S(P+1)+2M-1$	$\log M+S+1$, $P+2M+1$	$\log M+1$, $2M+1$
역방향/순방향 안전성	yes	yes	yes	no	yes

Gamal 프록시 암호화를 위한 복호화 키를 계산하고 전달하는 과정이 불필요하다. 멤버가 그룹을 탈퇴하는 경우, 그 멤버의 해당 하위 그룹의 키는 갱신된 후 LKH 프로토콜을 이용하여 하위 그룹의 유효한 그룹 멤버에게 전달된다. 따라서 제안하는 프로토콜에서 멤버 탈퇴 시 하위 그룹키 갱신을 위한 $2\log M+S$의 통신과 그룹키 전달을 위한 S의 통신이 요구되기 때문에 $O(\log N)$과 비교할 때 "1-affects-n" 문제를 완화시키게 된다. $N \gg M \gg S$의 조건에서 $O(\log M+S)$의 키 갱신 비용은 $O(\log N)$보다 훨씬 적게되고 $O(\log M)$의 비용과 거의



(a) 멤버 가입 시 키 갱신 비용



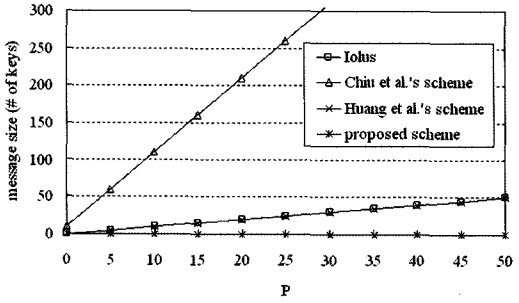
(b) 멤버 탈퇴 시 키 갱신 비용

그림 3 멤버 변화시 키 갱신 비용($N=2^{20}, M=2^8, P=2^3$)

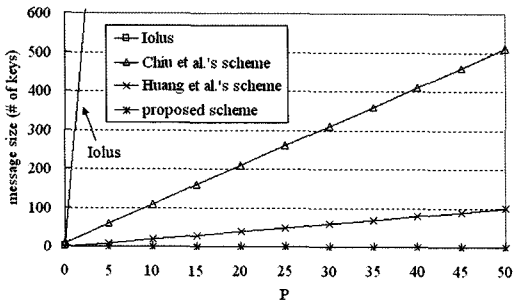
같게 된다. Huang의 기법은 주기적 키 갱신 방법을 이용하고 있지만 공정하고 명백한 비교를 위해 ElGamal 기반의 프록시 암호화를 이용한 그룹키 전달 비용이 분석 결과에 포함되었다. 그림 3(a)와 (b)는 각각 멤버의 가입과 탈퇴 시 요구되는 키 갱신 비용에 대한 실험 결과를 나타낸다.

메쉬 노드 가입 및 탈퇴 시 요구되는 키 갱신 비용은 멀티캐스트 트리 재구조화를 위한 키 갱신 비용을 나타낸다. 다른 기법들과 달리 제안한 알고리즘은 메쉬 노드 변화시 멀티캐스트 트리 재구조화를 위한 어떠한 통신도 필요로 하지 않는다. 메쉬 노드는 목표 메쉬 노드들의 공개 아이디만을 이용해 아이디 기반의 프록시 암호화 기법을 사용해 키 갱신 메시지를 변환하기 때문에 비밀키들이 그룹 간 통신을 하는 과정에서 노드들 간에 공유될 필요가 없다. 따라서, 제안하는 기법은 네트워크의 동적인 위상 변화에 효과적으로 대응할 수 있다. 메쉬 노드 가입 및 탈퇴에 따른 키 갱신 비용에 대한 실험은 그림 4에서 보여진다. 멀티캐스트 트리에서 송신자와 자식 메쉬 노드의 수가 늘어날수록, 제안하는 기법의 장점은 더욱 두드러진다.

제안한 프로토콜에서 각 멤버는 LKH 알고리즘을 이용한 하위 그룹 내 하위 그룹키 분배에 사용되는 $\log M$ 키암호화키를 저장해야 하며, 부모 노드로 부터 받은 하위 그룹키 키를 저장한다. 그룹키는 모든 프로토콜에서 공통으로 사용되기 때문에 분석 결과에 포함되지 않았다. 메쉬노드는 송신자 혹은 이웃 노드의 수와 관계없이 하위 그룹 내 키 갱신을 위한 $2M-1$ 키암호화키를 저장하고 sID와 자신의 하위 그룹만을 저장한다. 따라서 다대다 그룹 통신 환경에서 메쉬 노드가 저장해야할 키의 양을 $2M+1$로 줄임으로써 저장공간 문제를 해결할 수 있다. 특정 환경에서 각 멤버 및 메쉬 노드에 요구되는 메모리 비용에 대한 실험 결과는 그림 5에서 볼 수 있다. Iolus와 다른 프로토콜 사이에서 요구되는 하위 그룹키의 비용 차이는 지역적인 키 갱신 프로토콜의 차이로부터 기인된다. Iolus는 지역적인 키 갱신을 하는

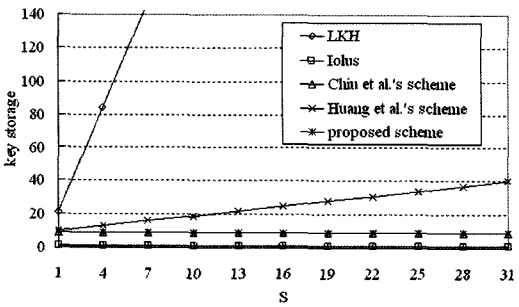


(a) 메쉬 노드 가입 시 키 갱신 비용

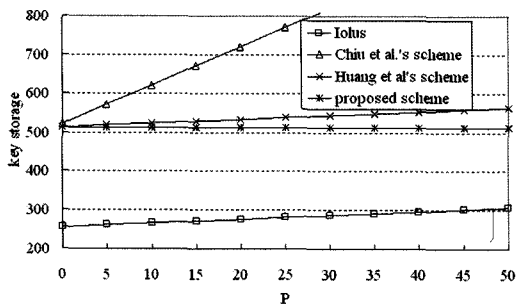


(b) 메쉬 노드 탈퇴 시 키 갱신 비용

그림 4 메쉬 노드 변화시 키 갱신 비용 ($N=2^{20}, M=2^8, S=10$)



(a) 멤버의 키 저장 요구량



(b) 메쉬 노드의 키 저장 요구량

그림 5 키 저장 요구량($N=2^{20}, M=2^8, S=10$)

과정에서 단일전송을 이용하기 때문에 메쉬 노드가 M 멤버 키를 저장하는 반면, 다른 프로토콜은 LKH를 이용하기 때문에 메쉬 노드가 $2M-1$ 키암호화키를 저장하게 된다. 따라서 키 갱신을 위해 요구되는 통신과 메모리 비용 사이에는 트레이드오프(trade-off) 관계가 존재한다.

제안하는 알고리즘은 그룹 멤버의 변화에 따른 그룹키 갱신으로 그룹 통신의 역방향 및 순방향 안전성을 보장한다. 반면에 Huang의 기법에서는 탈퇴한 멤버가 메쉬 노드로 부터 새로운 키암호화키를 받지 못하더라도 그룹키가 주기적 키 갱신 알고리즘에 의해 갱신될 때 까지 그룹 통신에 참여할 수 있다. 마찬가지로 새로 가입한 멤버는 그룹키가 갱신될 때까지 가입 이전의 그룹 통신을 복호화 할 수 있다. 이러한 특성으로 인해 그룹 통신의 순방향 및 역방향 안전성이 보장되지 못한다. 제안하는 기법의 안전성 분석은 다음절에서 보다 자세히 다루어진다.

5.2 안전성 분석

이 절에서는 제안하는 기법이 멤버 가입 시 그룹 통신의 역방향 안전성을 보장하고, 멤버 탈퇴 시 그룹 통신의 순방향 안전성을 보장함을 증명한다. 또한 제안하는 아이디 기반의 암호화를 이용한 키 전달 기법이 외부의 확률적 다항 시간(probabilistic polynomial-time) 공격자에 대해서 안전함을 보인다.

정리 1 (역방향 안전성): i 세션에 G_i에 새로 가입한 u_t는 i 세션 이전의 G_i의 그룹키를 알아낼 수 없다.

증명. 사용자 u_t가 G_i에 i번째 세션에 가입했을 때, 이전 세션의 그룹키는 $GK_i^i = PRF(GK_i^{i-1})$로 갱신된다. 새로 가입한 u_t가 현재 그룹키 GK_i^i를 전달받고 i번째 세션 이전의 암호화된 그룹 통신 데이터를 저장해 두었다 할지라도, 그 이전 세션의 그룹키를 알지 못하고는 그 데이터를 복호화할 수 없다. 현재 세션의 GK_i^i를 가지고 이전 세션의 그룹키를 알아내기 위해서는 u_t는 $GK_i^i = PRF(x)$를 만족하는 x를 찾아낼 수 있어야 한다. 그러나 의사 난수 생성 함수의 단방향성을 깨뜨리기는 계산적으로 매우 어렵다(computationally infeasible). 따라서 공격자는 현재 세션의 그룹키 GK_i^i를 가지고 이전 세션의 그룹키 GK_i^{i-1}를 얻어낼 수 없다.

공격자가 이전 세션의 그룹키 GK_i^{i-1}을 알아내기 위한 또 다른 방법은 송신자 혹은 메쉬 노드가 전송한 GK_i^{i-1}를 포함하는 이전의 그룹키 갱신 메시지 $\langle U, V, W\rangle$를 획득하고 그 메시지를 공격하는 것이다. 따라서 키 갱신 메시지에서 GK_i^{i-1}를 얻어내기 위해서는 u_t가 비록 PK를 이용해 같은 하위 그룹 멤버들에게 전달되는 키 갱신

메시지로부터 σ를 계산할 수 있더라도, GK_l^{i-2} 없이 프로토콜을 공격해야 한다. 그러나 GK_l^{i-2} 없이 $W=GK_l^{i-1}\times H(GK_l^{i-2},\sigma)$를 복호화하는 것은 계산적으로 불가능하다. 따라서, 멤버 u_t는 가입하기 이전의 G_l의 그룹키를 알아낼 수 없다. □

정리 2 (순방향 안전성): i 세션에 G_l에서 탈퇴한 u_t는 i 세션 이후의 G_l의 그룹키를 알아낼 수 없다.

증명. 사용자 u_t가 하위 그룹 SG_m의 메쉬 노드 p_j로부터 그룹을 탈퇴할 경우, p_j는 새로운 하위 그룹키 $PK_j^{m'}$를 생성하고 합법적인 하위 그룹 멤버들에게 안전하게 전송한다. 그리고 새로 갱신된 그룹키 GK_l^{i+1}는 새로운 하위 그룹키를 이용해 아이디 기반의 프록시 암호화 알고리즘으로 암호화 된 후 각 멤버들에게 전송된다. p_j의 그룹 멤버들에게 수신된 키 갱신 메시지는 $\langle U, V, W\rangle = \langle rP, \sigma\cdot e(rP, PK_j^{m'}\cdot ID_{SG_m}), GK_l^{i+1}\cdot H(GK_l^i,\sigma)\rangle$의 형태가 된다. 탈퇴한 사용자 u_t가 GK_l^i와 이전의 하위 그룹키 PK_j^m을 가지고 있더라도 새로운 하위 그룹키 $PK_j^{m'}$을 모르고 그룹키 갱신 메시지를 복호화 하는 것은 계산적으로 불가능하기 때문에 새로운 그룹키를 얻어낼 수 없다.

W와 GK_l^i가 주어졌을 때, GK_l^{i+1}은 비밀값 σ에 의해 결정된다. U, V, 그리고 ID_{SG_m}이 주어졌을 때, $PK_j^{m'}$을 얻고 다시 σ를 알아내기 위해서 사용자 u_t는 다음을 만족하는 x를 찾아야 한다.

$$V=\sigma\times e(U, x\cdot ID_{SG_m}).$$

U, V, 그리고 ID_{SG_m}는 상수 값이기 때문에 이 식은 σ에 대해서 유일한 해를 가지고 있다. 다시 말해, u_t에게 알려져 있는 정보는 키 $PK_j^{m'}$의 가능한 값 $x\in Z_q^*$에 대해서 일정하다. 따라서 σ는 유일하게 결정될 수 없고, 다시 GK_l^{i+1} 또한 결정될 수 없다. 그러므로 제안된 암호화 시스템은 GK_l^i를 알고 있는 탈퇴한 멤버에 대해서 무조건적 안전(unconditionally secure)하다[25]. 탈퇴한 멤버 u_t가 그룹키 갱신 메시지를 복호화 할 수 없기 때문에 탈퇴한 이후의 G_l의 그룹키를 알아낼 수 없다. □

정리 3 (그룹키 안정성 및 데이터 비밀성): 제안한 아이디 기반 암호화 키 전달 구조는 외부의 확률적 다항시간 공격자들에 대해서 그룹키 안전성 및 데이터 기밀성을 보장한다.

증명. 멀티캐스트 그룹 G_l에서, Encrypt_S 알고리즘은 송신자의 현재 세션의 그룹키 GK_l^i와 난수 σ를 이용해서 목표로 하는 메쉬 노드의 아이디로 키갱신 메시지 $\langle U, V, W\rangle = \langle rP, \sigma\cdot e(ID, sP)^r, GK_l^{i+1}\cdot H(GK_l^i,\sigma)\rangle$를 생성한다. 키 갱신 메시지로부터 GK_l^{i+1}를 얻기 위해서 외부 공격자는 메쉬 노드의 sID 없이 σ를 먼저 알아내야 한다. 그러나 $\langle U, V\rangle$는 단방향 아이디기반 암호화로 알려져 있고[16], 선택적 Bilinear Diffie-Hellman 문제가 풀기 어려운 한 CPA 공격에 안전하다고 알려져 있다[5]. 또한 외부 공격자는 송신자 s_l의 현재의 그룹키 GK_l^i를 알 수 없다. 그러므로 외부 공격자는 Encrypt_S 알고리즘의 키갱신 메시지를 복호화하는 데에 필요한 어떠한 정보도 알 수 없다.

Encrypt_P 알고리즘은 수신한 암호문을 자식 메쉬 노드 또는 하위그룹 멤버들을 위한 암호문으로 변형시킨다. 메쉬 노드가 재암호화하는 과정에서 σ는 메쉬 노드의 비밀키 sID로 복호화되고 자신의 하위 그룹키 또는 자식 노드의 ID로 재암호화된다. 이 과정에서 암호문의 $\langle W\rangle = \langle GK_l^{i+1}\times H(GK_l^i,\sigma)\rangle$가 메쉬 노드에 의해서 복호화되거나 변형되지 않기 때문에 제안한 프로토콜의 안전성에는 영향을 주지 않는다. 외부 공격자가 메쉬 노드를 공격해 하위 그룹키 또는 σ를 알아낸다 할지라도 현재 세션의 그룹키 GK_l^i는 노출되지 않기 때문에 그룹키 안전성은 보장된다. 이것은 또한 멀티캐스트 데이터를 중계해 주는 메쉬 노드에 대해서 메시지의 비밀성을 보장한다는 것을 의미한다. □

6. 결 론

본 논문에서는 동적인 메쉬 네트워크에서 다대다 그룹 통신을 위한 아이디 기반 암호화를 이용한 비중앙화 그룹키 관리 기법을 제안하였다. 제안한 기법은 중간의 메쉬 노드에 대해서 데이터 비밀성을 보장하기 때문에 "trusting third party" 문제를 해결할 수 있었다. 기존 기법들의 다량의 키 저장으로 인한 메모리 문제 또한 아이디 기반 암호화 알고리즘을 이용함으로써 완화 되었다. 그룹키는 분산화된 방식으로 암호화되고 전송되기 때문에 중앙화된 키 분배 센터 혹은 추가적인 하위 그룹키 계산 과정도 불필요하게 되었다. 또한 제안한 그룹키 관리 기법은 그룹 통신의 역방향 및 순방향 안전성을 보장한다. 게다가 하위 그룹키 갱신 과정이 멤버가 변한 지역적 하위 그룹으로 한정되기 때문에 네트워크의 확장성 또한 향상될 수 있다. 제안한 기법은 동적인 멤버의 변화 뿐 아니라 동적인 네트워크 위상 변화 또한 효과적으로 다룰 수 있다. 따라서 제안한 기법은 다수의 송신자가 존재하고, 중앙의 네트워크 관리자가 없으며, 중간의 중계 메쉬 노드를 완전히 신뢰할 수 없는 동적인 메쉬 네트워크 환경에 가장 적합하다.

참 고 문 헌

[1] I. F. Akyildiz, X. Wang, W. Wang, Wireless Mesh Networks: A Survey, Computer Networks 47 (March 2005), pp.445-487.

[2] IEEE Std 802.16-2004, Air Interface for Broadband Wireless Access Systems, October 2004.

[3] Y. Zhang, Y. Fang, A Secure Authentication and Billing Architecture for Wireless Mesh Networks, Wireless Networks 13 (2007), pp.663-678.

[4] S. Rafaeli, D. Hutchison, A Survey of Key Management for Secure Group Communication, ACM Computing Surveys 35 (September 2003), pp.309-329.

[5] A. Ivan, Y. Dodis, Proxy Cryptography Revisited, in: Proceedings Network and Distributed System Security Symposium (February 2003).

[6] WiMAX Forum, "Mobile WiMAX - Part I: A Technical Overview and Performance Evaluation," February 2006.

[7] D. Huang, D. Medhi, A Key-chain Based Keying Scheme For Many-to-Many Secure Group Communication, ACM Transactions on Information and System Security 7 (November 2004), pp.1-30.

[8] C. K. Wong, M. G. Gouda, and S. S. Lam, Secure Group Communications Using Key Graphs, in: *Proceedings ACM SIGCOMM (September 1998),* pp.68-79.

[9] D. A. McGrew and A. T. Sherman, Key Establishment in Large Dynamic Groups Using One-way Function Trees, Tech. Rep. No. 0755, TIS Labs at Network Associates, Inc., Glenwood, Md.

[10] S. Mittra, Iolus: A Framework for Scalable Secure Multicasting, in: *Proceeding ACM SIGCOMM (September 1997),* pp.277-288.

[11] A. N. Pour, K. Kumekawa, T. Kato, S. Itoh, A Hierarchical Group Key Management Scheme for Secure Multicast increasing Efficiency of Key Distribution in Leave Operation, Computer Networks 51 (August 2007), pp.4727-4743.

[12] M. Steiner, G. Tsudik, M. Waidner, Diffie-Hellman Key Distribution Extended to Group Communication, in: *Proceedings ACM CCS (March 1996),* pp.31-37.

[13] Y. Chiu, C. Lei, C. Huang, Secure Multicast Using Proxy Encryption, in: *Proceedings International Conference on Information and Communications Security, Lecture Notes in Computer Science 3783 (December 2005),* pp.280-290.

[14] C.-Y. Huang, Y.-P. Chiu, K.-T. Chen, C.-L. Lei, Secure Multicast in Dynamic Environments, Computer Networks 51 (July 2007), pp.2805-2817.

[15] L. Dondeti, S. Mukherjee, A. Samal, Scalable Secure One-to-many Group Communication Using Dual Encryption, Computer Communication 23 (July 1999) pp.1681-1701.

[16] D. Boneh, M. Franklin, Identity-Based Encryption from the Weil Pairing, in: *Proceedings Crypto 2001, Lecture Notes in Computer Science 2139 (August 2001),* pp.213-229.

[17] S. D. Galbraith, K. Harrison, D. Soldera, Implementing the Tate Pairing, in: *Proceedings 5th International Symposium on Algorithmic Number Theory, Lecture Notes in Computer Science 2369 (2002),* pp.324-337.

[18] V. S. Miller, The Weil Pairing and Its Efficient Calculation, *J. Cryptol. 17 (2004),* pp.235-261.

[19] Y. J. Choie, E. Lee, Implementation of Tate Pairing on Hyperelliptic Curves of Genus 2, in: *Proceedings ICISC 2003, Lecture Notes in Computer Science 2971 (2004),* pp.97-111.

[20] J. Hwu, R. Chen, Y. Lin, An Efficient Identity-based Cryptosystem for End-to-end Mobile Security, IEEE Trans. on Wireless Communications 5 (September 2006), pp.2586-2593.

[21] E. Fujisaki, T. Okamoto, Secure Integration of Asymmetric and Symmetric Encryption Schemes, in: *Proceedings Crypto 1999,* pp.537-554.

[22] G. M. Bertoni, L. Chen, P. Fragneto, K. A. Harrison, G. Pelosi, Computing Tate Pairing on Smartcards (2005). http://www.st.com/stonline/products/families/smartcard/ches2005_v4.pdf.

[23] M. Bellare, A. Desai, D. Pointcheval, P. Rogaway, Relations among notions of security for public-key encryption schemes, in: Proceedings Crypto'98 (1998) pp.26-45.

[24] Y. Tsiounis, M. Yung, On the Security of ElGamal Based Encryption, in: Proceedings International Workshop on Practice and Theory in Public Key Cryptography, Lecture Notes in Computer Science 1431 (February 1998), pp.117-134.

[25] D. R. Stinson. Cryptography Theory and Practice (3rd ed.) (Chapman & Hall/CRC, 2006).

허 준 범

2001년 고려대학교 컴퓨터교육과 학사 2005년 한국과학기술원 전산학과 석사 2005년~현재 한국과학기술원 전산학과 박사과정. 관심분야는 네트워크 보안, 정보보안, 암호학

윤 현 수

1979년 서울대학교 전자공학과 학사. 1981년 한국과학기술원 전산학과 석사. 1988년 미국 오하이오 주립대학 전산학과 박사. 1989년~현재 한국과학기술원 교수 관심분야는 병렬 컴퓨터 구조, 무선 이동통신, 애드혹 및 센서 네트워크, 정보보안