대규모 동적 그룹에서 안전한 멀티캐스트를 위한 키 분배 프로토콜

김 태 연[†] · 김 영 균[††]

요 약

멀티캐스트 통신에서 그룹에 새로운 멤버가 가입하거나 기존의 멤버가 탈퇴하는 경우 멤버들이 사용중인 그룹 키는 갱신되어야 한다. 이러한 절차는 완전 전방향과 후방향 비밀성을 보장하기 의해 필요하다[8]. 불행하게도, 빈번한 멤버쉽이 변경되는 대규모 그룹에서의 키 갱신은 그룹을 확장하는데 커다란 장애가 된다. 본 논문에서는 대규모 동적 그룹에서 그룹 키를 효율적으로 분배할 수 있는 새로운 방식을 제안한다. 기존의 안전한 멀티캐스트 프로토콜과는 달리, 제안된 프로토콜은 키 갱신의 빈도와 계산에 따른 오버헤드가 전체 그룹의 크기가 아닌 서브그룹의 크기에 따라 영향을 받기 때문에 대규모 그룹으로 확장이 가능하며, 그룹 접근 제어를 수행하는 서브그룹 관리자가 송신자에 의해 전송된 멀티캐스트 데이터에 접근할 수 없도록 하는 메카니즘을 제공한다. 또한 무선 컴퓨팅 환경에서 프라이버시를 보장할 수 있는 보안 서비스를 제공한다.

A Key Distribution Protocol for Secure Multicasting in Large Dynamic Groups

Tae Yeon Kim[†] · Young Kyoon Kim[††]

ABSTRACT

Changing group key is necessary for the remaining members when a new member joins or a member leaves the group in multicast communications. It is required to guarantee perfect forward and backward confidentiality. Unfortunately, in large groups with frequent membership changes, key changes become the primary bottleneck for scalable group. In this paper, we propose a novel approach for providing efficient group key distribution in large and dynamic groups. Unlike existing secure multicast protocols, our protocol is scalable to large groups because both the frequency and computational overhead of re-keying is determined by the size of a subgroup instead of the size of the whole group, and offers mechanism to prevent the subgroup managers with group access control from having any access to the multicast data that are transfered by sender. It also provides security service for preserving privacy in wireless computing environments.

키워드 : 세션키(Session Key), 멀티캐스트(Multicast), 키 분배(Key Distribution), 보안(Security), 서브그룹(Subgroup)

1. 서 론

인터넷의 상업성과 광대역망 기술이 발전함에 따라 다양한 장비 및 서비스 개발에 대한 관심이 고조되고 있다. 특히, 유·무선이 결합된 초고속망의 구조와 실시간 멀티미디어 중심의 서비스를 위한 기반 환경을 조성할 수 있는 멀티캐스트 기술에 대한 연구가 활발히 진행 중에 있다. 멀티캐스트는 원격 교육과 원격 회의, 주요 스포츠 이벤트의 방송, 분산 데이터베이스 접근 등에 적용될 수 있다. 최근 들어 인터넷을 기반으로 한 이러한 유형의 응용 서비스에 대한 요구가 급증하고 있으나 아직은 소수의 멀티캐스트 통신 시스템이 운용되고 있는 실정이다. 게다가 이들 중 몇몇 시스템만이 실제 응용에서 인증과 접근제어 등과 같은 간단한 보안 서비스만이 적용되고 있어 다른 보안 서비스도 지원되는 안전한 멀티캐스트 시스템이 필요하다.

안전한 멀티캐스트 시스템을 설계하고 구현하는데 있어서 고려되어야 할 보안 서비스는 인증과 접근제어, 비밀성, 무결성, 부인봉쇄 등이 있다. 멀티캐스트 그룹 멤버 가입을 통제하기 위한 인증과 접근제어, 데이터의 비밀성과 무결성, 부인봉쇄의 보장을 위한 처리 절차는 기존의 유니캐스트 구조에서의 처리 과정보다도 훨씬 더 복잡하다. 또한 무선 컴퓨팅 환경에서는 송·수신자의 신원이나 데이터 내용, 위치의 노출 등으로 인한 사용자의 프라이버시 침해를 방지하는 서비스가 필요하다. 멀티캐스트 환경에서 이러한 보안 서비스를 기반으로 하여 멤버들간에 안전하게 데이터를 교환하기 위해서는 그룹내의 모든 단말(또는 멤버)들만이 알고 있는 그룹 세션키를 사용하여 데이터를 암호화하여 전송해

† 종신회원 : 서남대학교 컴퓨터정보통신학과 교수
†† 정 회 원 : 한국전자통신연구원 컴퓨터소프트웨어연구소 컨텐츠기술연구부 선임연구원
논문접수 : 2001년 12월 11일, 심사완료 : 2002년 5월 15일

야 한다. 본 논문에서 송신자 그룹을 포함한 두 개 이상의 그룹에서 사용되는 키를 그룹 세션키(TEK : Traffic Encryption Key)라고 정의하고, 서브그룹내의 단말간에만 사용되는 키를 지역 세션키(LTK : Local Traffic encryption Key)라고 정의한다.

그룹의 유형은 그룹에 가입(join)하거나 그룹으로부터 탈퇴(leave)하는 멤버의 수나 그룹의 크기에 따라 두 가지로 나눌 수 있다. 첫째는 간헐적으로 한 멤버의 가입이나 탈퇴로 인한 그룹 크기의 변동이 적은 형태이다. 둘째는 다수의 멤버가 일시에 가입하거나 탈퇴되는 경우와 하나의 그룹이 두 개의 서브그룹으로 분리(fission)되거나 서브그룹들이 하나의 그룹으로 통합(fusion)되는 경우처럼 그룹 크기의 변동이 큰 형태이다. 또한 그룹의 유형은 그룹 통신에 가입하는 시간이나 사용자의 습관, 날씨, 계절 등에 많은 영향을 받게 된다. 예를 들어, 늦은 밤이나 한 낮에는 멀티캐스트를 사용하는 멤버가 적어 그룹 크기의 변동이 적지만, 일과가 시작되는 시간이나 업무가 끝나는 늦은 오후에는 멤버의 이동이 많기 때문에 그룹 크기가 심하게 변한다.

이와 같이 멤버의 이동이 빈번한 대규모 동적 그룹 환경에서 안전한 멀티캐스트 데이터가 효율적으로 전송될 수 있도록 하기 위해서는 세션키를 효율적으로 관리해야 한다. 키 관리자는 멤버가 그룹 가입 시에 새로운 세션키를 기존의 멤버와 새로 가입한 멤버에게 안전하게 분배해야하고, 그룹내의 특정 멤버가 그룹으로부터 강제 탈퇴되거나 자의적인 탈퇴 요청이 있는 경우에도 새로운 세션키를 생성하여 나머지 멤버에게만 안전하게 전송해야한다[7, 9]. 그룹 멤버의 가입과 탈퇴에 따라 세션키를 갱신하는 이유는 단말이 가입 전(탈퇴 후)에 수신한 데이터에 접근할 수 없도록 하는 것이다[8]. 그룹에 새로운 멤버의 가입에 대해서 인증 과정을 수행하여 정당한 사용자인 경우에는 멀티캐스트 데이터베이스를 갱신하고 새로운 세션키를 분배하는 절차가 있어야 하고, 기존 멤버 탈퇴 시에도 멀티캐스트 데이터베이스를 갱신한 다음 새로운 세션키를 생성하여 분배하는 과정이 필요하다. 이러한 매카니즘을 사용하는 멀티캐스트 통신은 멤버의 가입(또는 탈퇴)이 빈번하게 이루어지거나 그룹의 크기가 매우 큰 환경에서는 그룹 통신 시스템의 오버헤드를 증가시켜 잠재적인 효율이 제한 받게 된다. 최악의 경우에는 단말의 인증 과정과 세션키의 갱신을 처리하는데 많은 시간을 소비하게 되어 멀티캐스트 데이터를 전송할 수 없는 상황이 발생한다. 결국 안전한 멀티캐스트 시스템에서 가장 중요하게 고려되어야 할 사항은 키 분배와 관리라고 할 수 있다.

본 논문에서는 멤버의 이동이 빈번한 대규모 동적 그룹 환경에서 아래와 같은 보안 기능이 지원될 수 있는 키 분배 트리와 알고리즘을 제안하고, 기존의 방식들과 그룹 확장성과 멤버 가입과 탈퇴에 따른 전체 시스템의 오버헤드, 멤버의 프라이버시 등의 측면에서 비교 분석한다.

(1) 기존의 멀티캐스트 전송 프로토콜에 보안 기능의 첨가로 인한 시스템의 오버헤드가 최소화되어야 한다.
(2) 그룹의 확장이 전체 시스템의 성능에 큰 영향을 주어서는 안 된다.
(3) 빈번한 그룹 멤버의 이동에 대해서 시스템은 완전 전방향과 후방향 비밀성(perfect forward and backward secrecy)을 보장하여야 한다[8].
(4) 서비스의 사용자가 아닌 서브그룹 관리자로의 데이터 노출을 막을 수 있어야 한다.
(5) 사용자의 프라이버시를 보장하기 위한 익명성이 제공될 수 있어야 하며 불법 추적이 불가능하여야 한다.

본 논문에서는 이동 통신을 위한 Hand-Off를 지원하는 프로토콜에 대해서는 언급하지 않았으며, 논문의 구성은 다음과 같다. 2장에서는 관련 연구를 기술하고, 3장과 4장에서는 키 그룹 트리의 개념과 구조, 세션키 분배 프로토콜에 대해서 기술한다. 5장과 6장에서는 기존에 연구된 다른 방식과 본 논문에서 제안한 방식을 비교분석하고, 결론과 향후 연구 방향을 제시한다.

2. 관련 연구

안전한 멀티캐스트 통신에서 그룹 키는 키의 사용 관점에 따라 정적 그룹 키(static group key)와 동적인 그룹 키(dynamic group key)로 나눌 수 있고, 키 생성 방법에 따라 출자 그룹 키(CGK : Contributory Group Key)와 중앙집중 그룹 키(IGK : Integrated Group Key), 분산 독립된 그룹 키(DGK : Distributed and independent Group Key)로 구분할 수 있다[3, 4, 6].

정적 그룹 키는 멤버가 그룹 가입 시에 키를 할당받아서 그룹을 탈퇴할 때까지 사용할 수 있는 키로서 사용자는 그룹에 가입하기 전에 수신된 송신자의 멀티캐스트 데이터에 접근할 수 있을 뿐만 아니라 탈퇴 후에 수신한 데이터에도 접근할 수 있게 되는 취약점을 갖고 있다. 그러나 동적 그룹 키는 그룹 멤버쉽이 바뀔 때마다 새로운 키를 사용하여 데이터를 전송하기 때문에 정적 그룹 키를 사용하는데서 발생할 수 있는 문제점을 해결할 수 있다.

CGK는 그룹내의 모든 멤버들이 출자한 키 정보를 수집하여 생성한 키이고, IGK는 키 분배 센터에서 독자적으로 생성한 키로서 키 분배 센터의 성능과 신뢰도에 따라 서비스의 질이 좌우된다. 그러나 IGK가 적용되는 환경에서는 중앙 키 분배 센터에 장애가 발생하거나 병목 현상이 발생할 수 있다. 전자의 경우에는 IGK의 백업을 관리함으로써 해결될 수 있고, 후자의 경우에는 여러 곳에서 키를 생성되어 분배되는 DGK를 사용함으로써 해결할 수 있다. 다음은 지금까지 제안된 안전한 멀티캐스트 전송을 위한 연구들을 기술한다.

Burmester[2]는 그룹 멤버들에 의해서 생성한 스패닝 트

리를 통해서 세션 키를 분배하는 방식을 제안했지만, 모든 멤버는 데이터를 수정하지 않고 다른 멤버에게 전달한다는 가정을 두고 있을 뿐만 아니라 멤버의 이동에 대해 효율적으로 멤버쉽을 조정할 수 있는 방식이 아니다.

Steiner[6]은 Diffie-Hellman 키 교환 프로토콜을 사용하여 동적 그룹에 세션 키를 분배하는 출자 그룹 키 생성(CGG) 방식을 제안하였다. 최근에 가입한 멤버는 모든 멤버들의 키 정보를 수집하여 세션키를 생성해서 그룹내의 모든 멤버에게 분배하는 그룹 관리자 역할을 수행한다. 이 구조는 동적인 소 그룹환경에서 세션키를 효율적으로 분배할 수 있는 방식이지만 동적인 대규모 그룹 환경에서 특정 노드의 처리 부담이 가중되기 때문에 그룹 확장에 제한을 받게 된다.

Iolus에서는 대규모 그룹을 여러 개의 소규모 그룹으로 분할하고, 각 서브그룹은 서로 다른 지역 세션키를 사용하도록 하여 그룹의 확장성을 지원하는 방식을 제안하였다[4]. 그룹 멤버의 이동이 전체 그룹에 영향을 주지 않고 해당 서브그룹만에 영향을 주는 방식으로 각 서브그룹 관리자는 세션키를 생성하고 분배하는 기능과 수신한 멀티캐스트 데이터를 재암호화(re-encrypting)하여 중계하는 역할을 담당한다. 이 구조는 중간 서브그룹 관리자를 전적으로 신뢰해야 하고, 재암호화에 따른 데이터의 지연 문제가 발생한다.

Wong[9]이 제안한 방식은 Iolus방식에서 서브그룹간에 전송되는 데이터를 재암호화하는 과정에서 생기는 지연 문제를 해결하기 위한 방법으로 모든 멤버들이 하나의 세션키를 사용하도록 한 것이다. 이 방식은 멤버의 빈번한 이동이 있는 환경에서는 자주 세션키를 갱신해야 하는 문제점을 안고 있다.

Kronos에서는 Iolus 방식의 재암호화를 수행해야 하는 문제와 Wong[9]이 제안한 방식에서 발생하는 빈번한 세션키의 갱신을 줄이기 위해서 멤버의 이동에 관계없이 일정한 기간 동안 모든 그룹 멤버들은 하나의 정적 세션 키를 사용하도록 하는 메카니즘을 제안하였다[7]. 이 방식은 일정기간 동안 그룹을 이동 (가입/탈퇴)한 멤버에 의한 데이터의 접근을 허용하는 문제가 발생한다.

Molva[5]는 중간 노드를 신뢰한다는 가정 하에서 대규모 동적 그룹으로의 확장성과 그룹 분할에 따른 보안 노출을 봉쇄하는 메카니즘을 제안하였다. 이 방식은 특정 멤버의 이동이 다른 서브그룹의 멤버에 영향을 주지 않지만 중간 노드와 서비스 사용자인 단말은 많은 계산 처리로 인한 오버헤드가 증가하게 된다.

Dondeti[3]는 대규모 그룹에서 빈번한 멤버의 이동이 전체 시스템에 끼치는 영향을 최소화하고 중간 노드에게 데이터가 노출되는 것을 방지하기 위해 그룹 세션키를 각 서브그룹 관리자의 비밀키로 암호화하여 전송하는 이중 프로토콜을 제안하였다. 이 방식은 송신자가 관리해야 하는 비밀키의 수와 데이터를 암호화하는 횟수가 서브그룹의 수와 비례하게 되어 송신자의 처리 오버헤드가 가중된다.

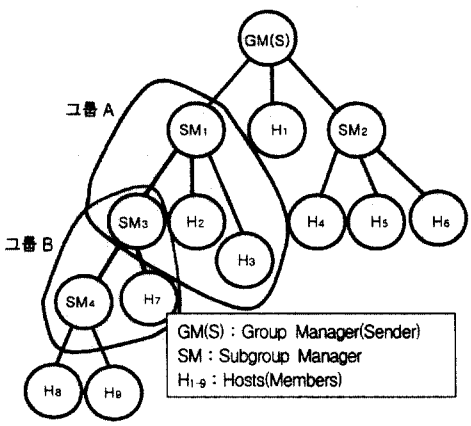
3. 키 그룹 트리

3.1 그룹 구성 트리

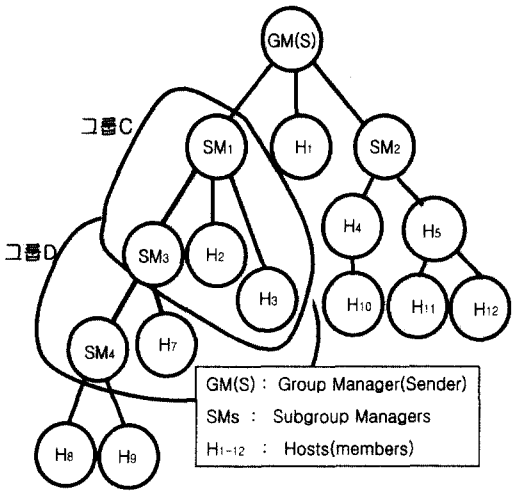
그룹은 데이터를 분배하는 방식에 따라 동등 그룹(peer groups), 확산 그룹(diffusion groups), 클라이언트/서버 그룹, 트리 형태인 계층 그룹(hierarchical groups)으로 구분할 수 있다[1]. 동등 그룹은 하나의 그룹으로 구성된 형태로서 모든 멤버는 동등한 권한을 가지며, 다른 멤버를 감시하고, 태스크(tasks)를 분담 처리할 수 있는 구조이다. 따라서 그룹 관리자는 고정되어 있지 않고 임의의 멤버가 관리자 역할을 수행한다. 확산 그룹은 그룹 내에 하나의 서브그룹을 멤버로 가지며, 서브그룹은 다시 자신의 멤버로 하나의 서브그룹을 가지는 형태로서 특정 멤버는 여러 개의 그룹에 중복되게 된다. 가장 작은 서브그룹의 임의의 멤버가 그룹의 관리자 역할을 수행한다. 클라이언트/서버 그룹은 모든 멤버가 여러 개의 서브그룹으로 분할되어 각 그룹은 독립적인 영역을 차지하는 구조이다. 이 유형에서 모든 그룹의 멤버는 고정된 한 멤버에 의해서 관리된다. 계층 그룹은 클라이언트/서버 그룹과 유사한 구조로서 그룹의 한 멤버가 모든 멤버를 관리하는 것이 아니라 각 서브그룹내의 멤버가 독자적으로 자신의 그룹을 관리하는 트리 구조이다.

본 논문에서 기술한 그룹 구성 트리는 계층 그룹의 형태로서 각 서브그룹 관리자는 다양한 수의 가지(degree)를 가질 수 있으며, 전체 그룹을 관리하는 근(root)노드, 서브그룹 멤버를 관리하는 중간 노드, 서비스를 사용하는 단 노드로 구성된다. 그룹의 초기 단계에는 그룹 관리자(GM : Group Manager)만이 있게 된다. 따라서 단 노드가 서브그룹 관리자(SM : Subgroup Manager)가 되는 경우는 그룹 내에 멤버가 없는 상태이다.

그룹은 그룹의 멤버가 너무 많아 그룹 관리자가 멤버들을 관리하는데 부담이 큰 경우에 논리적인 서브그룹으로 분할되어 관리되고, 역으로 그룹의 멤버가 너무 적은 그룹들은 하나의 그룹으로 통합되어 관리된다.



(그림 1) 그룹 구성 트리(비중복)



(그림 2) 그룹 구성 트리(중복)

(그림 1)은 그룹 구성 트리를 나타낸 것으로 노드 GM은 그룹 관리자, 노드 $SM_i(i = 1, \cdots, 4)$는 그룹의 연결장치로서 서브그룹의 멤버를 관리하는 관리자, 나머지 노드 $H_i(i = 1, \cdots, 9)$는 그룹 멤버인 단말이다. (그림 1)의 트리는 5개({GM, SM_1, SM_2, H_1}, {SM_1, SM_3, H_2, H_3}, {SM_2, H_4, H_5, H_6}, {SM_3, SM_4, H_7}, {SM_4, H_8, H_9})의 서브그룹으로 구성되어 있다. 그룹 관리자 GM은 서브그룹 관리자 SM_1과 SM_2, 단말 H_1를 관리하고, SM_1은 다른 서브그룹 관리자 SM_3과 단말 H_2, H_3를 관리한다. (그림 1)에서 단말 H_2과 H_3은 서브그룹 SM_1의 멤버이지만, (그림 2)에서 단말 H_2과 H_3는 서브그룹 SM_1의 멤버이면서 SM_3의 멤버이므로 두 서브그룹 관리자에 의해서 관리되는 형태이다.

3.2 키 그룹 트리

본 논문에서는 키 관리를 간단하고 엄격하게 제어하기 위해서 변형된 트리 기반 구조를 사용한다[9]. 키 그룹 트리는 키의 적용 범위에 따라 GM이 생성한 그룹 세션키(TEK)와 그룹 세션키를 암호화(생성)하는 알고리즘($E^{GM}{}_K()$)을 관리하는 키 노드(G-node), 독립적인 서브그룹 내에서 생성한 지역 세션키(LTK)와 지역 세션키 암호화(생성) 알고리즘($E^{lg}{}_K()$)을 관리하는 키 노드(L-node)로 구성된 비순환 그래프이다. (그림 3)에서 그룹 관리자인 노드 GM와 노드 $A_i(i = 1, \cdots, 4)$는 G-node이며, 노드 $A_i(i = 1, \cdots, 4)$와 최하위 레벨에 있는 노드 $H_i(i = 0, \cdots, 9)$는 L-node이다. 노드 $A_i(i = 1, \cdots, 4)$는 G-node이면서 L-node이다.

(그림 3)은 그룹 관리자와 서브그룹 관리자, 그룹 단말 ($A_i(i = 1, \cdots, 4), 0, \cdots, 9$)로 구성된 논리적인 키 그룹 트리로서 모든 단말은 서브그룹 $SG_3 = \{A_1, 0, 1\}$, $SG_4 = \{A_2, A_3, 2, 3, 4, 5\}$, $SG_5 = \{A_4, 6, 7\}$, $SG_6 = \{A_4, 8, 9\}$으로 분할되어 있다. 여기에서 노드 $A_i(i = 1, \cdots, 4)$는 서브그룹 보안 에이전트(sub-group security agent)로 정의한다.

〈표 1〉 논문에서 사용되는 기호

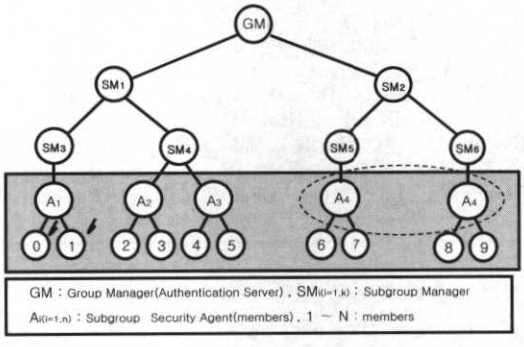
기 호	의 미
GM	그룹 관리자
SM(i = 1, …, g)	서브그룹 관리자로서 상위 그룹의 멤버이거나 라우터
$A_k(k = 1, \cdots, s)$	전체 그룹내의 보안 에이전트 권한을 단말들
$H_{ki}(i = 1, \cdots, n)$	보안 에이전트 A_k와 같은 세션키를 사용하는 단말들
P_{id}	Pseudo ID
RC_{Hjoin}	단말(Host)의 가입 요청 증명서(Request Certificate)
AC_H/AC_A	단말(Host/Agent)의 권한 증명서(Authorization Certificate)
R_{new1}/R_{new2}	그룹 세션키와 지역 세션키의 생성을 위한 키 정보
$H_{join}/(H_{id}=H_{leave})$	이동 중(가입/탈퇴)인 보안 에이전트 역할을 하지 않은 단말(H_i)
$A_{join}/(A_{id}=A_{leave})$	이동 중(가입/탈퇴)인 보안 에이전트(A_k)
A_{old}/A_{new}	SM의 멤버인 기존의 보안에이전트와 새로운 보안 에이전트
K^S_H, K^P_H	단말의 Secret Key와 Public Key
K^S_A, K^P_A	에이전트의 Secret Key와 Public Key
TEK	Traffic Encryption Key
$LTK_i(i = 1, \cdots, k)$	Local-Traffic encryption Key
[m]TEK	데이터 m을 그룹 세션키로 암호화
[m]LTK	데이터 m을 지역 세션키로 암호화
$E^{GM}{}_K$	TEK Encryption(generation) algorithm
$E^{lg}{}_{Ki}()(i = 1, \cdots, k)$	LTK Encryption(generation) algorithm

앞으로 논문에서 사용되는 기호들은 <표 1>과 같다. H_{ki} ($i = 1, \cdots, n$)와 $A_k(k = 1, \cdots, s)$는 SM_i의 멤버로서 서비스를 사용하는 단말이다. RC_{Hjoin}와 AC_H/AC_A, P_{id}는 각각 단말의 가입 요청 증명서(RC : Request Certificate)와 권한 증명서(AC : Authorization Certificate), 가명 ID이다. 요청 증명서는 각 단말이 소유하는 것으로서 보안 센터가 단말을 인증하는데 필요한 정보가 들어 있다. 권한 증명서는 보안 센터가 발급하는 것으로 단말의 가명과 키 그룹 ID, 보안 에이전트 지정, 단말의 공개키, 사용 가능 기간 등이 들어 있다. 그룹 세션키 TEK(또는 지역 세션키 LTK)는 아래와 같이 비밀 키 암호화 알고리즘 $E^{GM}{}_K()$(또는 $E^{lg}{}_{Ki}()$)와 GM과 SM에 의해서 생성된 임의의 키 정보(keying material) R을 이용하여 생성한다. GM이 생성한 R_{new1}은 새로운 TEK를 생성하는데 사용되는 키 정보이고, SM이 생성한 R_{new2}는 새로운 LTK를 생성하는데 사용되는 키 정보이다.

$$TEK = E^{GM}{}_K(R_{new1}) \text{ 또는 } LTK_i = E^{lg}{}_{Ki}(R_{new2}),$$
$$i = 1, \cdots, k, k : \text{ 에이전트의 수} \quad (1)$$

비밀키 암호화 알고리즘($E^{GM}{}_K()$ 또는 $E^{lg}{}_{Ki}()$)은 그룹 관리자에 의해서 생성되어 모든 멤버에게 분배되지만 알고리즘 $E^{GM}{}_K()$는 그룹 관리자 GM과 보안 에이전트 $A_k(k = 1, \cdots, s)$만이 소유할 수 있고, 알고리즘 $E^{lg}{}_{Ki}()$는 SM_i의 멤버만이 소유할 수 있다. 따라서 (그림 3)에서 노드 GM과 단말 $A_k(k = 1, \cdots, 4)$만이 알고리즘 $E^{GM}{}_K()$를 사용하여 그룹 세션키 TEK를 생성할 수 있으며, 단말 A_1과 $H_i(i = 0, 1)$은 $E^{lg}{}_{K1}()$을 사용하여 지역 세션키 LTK_1를 생성하고 단말 A_2과 $H_i(i = 2, 3)$은 $E^{lg}{}_{K2}()$을 사용하여 지역 세션키 LTK_2를 생성할 수 있다.

이와 같이 비밀키 암호화 알고리즘을 사용하는 이유는 전체 시스템에 영향을 주지 않고 세션키를 갱신할 수 있기 때문이다. 다시 말해서 단말의 가입이나 탈퇴가 있는 경우에 모든 멤버들이 사용중인 그룹 세션키를 갱신해야하는 오버헤드를 줄이기 위해 단말의 이동에 따라 다른 서브그룹의 지역 세션키를 갱신하지 않고 해당 지역 세션키만 변경할 수 있는 메커니즘이다. 예를 들면, 가입을 요청하는 단말이 서브그룹 내에 멤버가 없어 보안 에이전트의 역할을 해야하는 경우에는 그룹 세션키 TEK만 갱신하면 되며, 보안 에이전트가 아닌 단말이 가입하거나 탈퇴하는 경우에는 다른 지역 세션키를 변경하지 않고 해당 지역 세션키만 갱신하면 된다.



(그림 3) 키 그룹 트리

GM은 모든 그룹 단말을 관리하고 보안에 대한 책임을 맡고 있는 노드로서 정보에 대한 불법적인 사용자 접근을 막기 위해 접근제어 리스트(ACL)를 관리한다. 단말의 가입 요청에 대한 인증과 가입을 허가하는 권한 증명서(AC) 배부, 그룹 세션키(TEK)와 알고리즘 $E^{GM}{}_K()$및 $E^{lg}{}_K()$의 분배, 그룹 탈퇴 처리, 정당하지 않는 단말의 강제 탈퇴 등의 권한을 갖은 보안 서버이다. 또한 GM은 실제 멀티캐스트 데이터를 전송하는 송신자에게 키 정보와 암호화 알고리즘 $E^{GM}{}_K()$, 보안 에이전트 A의 ID를 보내 데이터를 안전하게 전송할 수 있도록 한다. 본 논문에서는 편의상 GM을 멀티캐스트 데이터를 암호화하여 분배하는 송신자로 가정한다.

SM_i(i = 1, …, g)은 서비스 사용에 관련이 없는 서브그룹 관리자이거나 라우터로서 서브그룹 멤버의 가입과 탈퇴 요청을 처리하고, 상위 관리자로부터 수신한 암호화된 멀티캐스트 데이터와 필요에 따라 지역 세션키를 생성하는데 사용되는 키 정보(R)를 멤버들에게 분배하고, 자신의 서브그룹 멤버에 대한 ACL을 관리하는 관리자 역할을 수행한다. 그러나 SM은 TEK로 암호화된 멀티캐스트 데이터를 복호화할 수 없다. 그룹 관리자 GM과 보안 에이전트들이 공유하는 알고리즘 $E^{GM}{}_K()$및 $E^{lg}{}_{Ki}()$은 안전한 채널을 통해서 전송되기 때문에 현재 사용중인 그룹 세션키 TEK와 지역 세션키 LTK를 생성할 수 없기 때문이다. 다시 말해서, 서브그룹 관리자는 송신자가 그룹 단말에게 전송한 데이터에 접근할 수 없는 중계(relay) 역할만을 담당한다.

노드 A_k(k = 1, …, s)는 그룹의 형성 시 GM에 의해서 서브그룹의 임시 관리자의 역할을 수행하는 멤버이다. 이와 같이 SM과 에이전트 A를 분리하는 이유는 직접적인 서비스의 사용자가 아닌 서브그룹 관리자나 라우터에게 멀티캐스트 데이터가 노출되는 것을 막기 위함이다. 보안 에이전트는 서브그룹내의 다른 단말과는 달리 TEK를 공유할 수 있으며, 자신의 서브그룹 내에서만 사용할 수 있는 지역 세션키인 LTK를 생성할 수 있는 알고리즘 $E^{lgi}{}_{Ki}()$를 멤버들에게 안전한 채널을 통해 분배하는 역할을 수행한다. 노드 A_i(i = 1, …, 4)는 송신자로부터 도착한 멀티캐스트 데이터를 지역 세션키 LTK로 재암호화하여 분배하는 역할을 담당한다. 이러한 환경에서 서브그룹내의 보안 에이전트가 그룹을 탈퇴하게 되면 나머지 단말 중에서 가장 최근에 가입한 단말이 GM으로부터 권한 증명서와 키 정보(R_{new1}), 알고리즘 $E^{GM}{}_K()$및 $E^{lg}{}_{Ki}()$를 수신 받아 보안 에이전트 역할을 수행한다. 이 과정에서 그룹 세션키와 지역 세션키를 갱신하여 그룹 탈퇴를 한 에이전트가 더 이상 데이터에 접근할 수 없도록 한다.

보안 에이전트는 그룹의 크기나 단말의 가입 형태에 따라 그 수가 증가하거나 두 개 이상의 서브그룹을 관리하게 된다. (그림 3)는 하나(SM_4)의 서브그룹 내에 두 개(A_2와 A_3)의 보안 에이전트가 있고, 하나(A_4)의 보안 에이전트가 두 개(SM_5와 SM_6)의 서브그룹에 포함된 경우를 보여주고 있다. 전자는 그룹을 효율적으로 관리하기 위해서 하나의 그룹을 두 개의 서브그룹으로 분할되고, 후자는 단말이 두 서브그룹에 중복 가입된 것이다. 따라서 그룹 SM_4내에는 두 개의 지역 세션키가 사용되고, SM_5와 SM_6내에서 하나의 지역 세션키가 사용된다. 보안 에이전트는 GM과 A_k간에 사용하는 $E^{GM}{}_K()$와 노드 A_k와 H_{ki}간에 사용하는 $E^{lg}{}_{Ki}()$를 관리해야 한다.

최하위 서브그룹내의 단 노드는 서비스를 사용하는 그룹 단말로서 LTK와 $E^{lg}{}_{Ki}()$를 관리한다. 다른 단말이 그룹에 가입하거나 탈퇴되는 경우에 멤버들은 SM_i로부터 수신한 키 정보(R_{new2})와 식 (1)를 이용하여 서브그룹에서 사용 중인 LTK를 갱신한다.

4. 키 분배 프로토콜

키 그룹 트리의 초기 상태는 그룹 관리자 GM와 라우터와 같은 서브그룹 관리자 SM들로 구성되며, GM은 그룹 단말들에 대한 각종 보안 정책을 수행하는 역할을 담당한다. 그룹에 가입을 원하는 단말은 모든 SM에게 가입 요청 증명서를 보내 그 응답에 따라 자신의 SM이 선택되어 해당 서브그룹의 멤버가 된다. 가입을 희망하는 단말의 서브그룹 내에 다른 멤버가 없는 경우에 자신은 보안 에이전트 A이면서 멤버가 되지만 보안 에이전트 A가 존재하는 경우에는 멤버가 된다. 멤버들을 관리하는 GM과 SM은 ACL을 저장하는 데이터베이스를 가지고 있어 접근제어 정책을 수행한다. 단말간의 부정과 SM의 악의 있는 방해는 없는 것으로 가정한다.

4.1 단일 멤버 연산(single member operation)

4.1.1 가입(join)

(1) 보안 에이전트가 없는 서브그룹

그룹 가입을 원하는 단말(H_{join})는 자기가 속해 있는 SM_i에게 요청 증명서 RC_{Hjoin}을 보내면, 다시 SM_i는 GM에게 필요한 정보를 보내 가입 허용 여부를 결정하도록 한다. 그룹 관리자 GM은 정당한 사용자인지를 검사하여 정당한 사용자인 경우에는 SM_i를 경유해서 권한 증명서 AC_A와 R_{new1}, $E^{GM}{}_K()$, $E^{lg}{}_{Ki}()$를 단말에게 전달한다. 단말에게 전송되는 정보는 다른 노드(SM, 서브그룹 에이전트 권한이 없는 단말, 불법 사용자)에게 노출되지 않도록 비밀키로 암호화되어 전달된다. 그리고 기존에 사용중인 세션키를 갱신하기 위해 기존의 에이전트들에게 새로운 키 정보(R_{new1})를 안전한 채널을 통해 전송한다. 권한 증명서 내에는 서브그룹 에이전트의 권한이 부여되어 있기 때문에 가입 단말은 세션키 TEK로 암호화한 모든 멀티캐스트 데이터를 직접 수신할 수 있게 된다.

① $H_{join} \rightarrow SM_i : P_{id}, [RC_{Hjoin}]K^P{}_{GM}$
② $SM_i \rightarrow GM : P_{id}, [RC_{Hjoin}]K^P{}_{GM}, [SM_i]K^P{}_{GM}$
③ $GM \rightarrow A_1, A_2, \cdots, A_s : [R_{new1}]TEK$, s는 보안 에이전트의 수
④ $GM \rightarrow SM_i : [AC_A]K^P{}_{SM}, [AC_A, R_{new1}, E^{GM}{}_K, E^{lg}{}_{Ki}]K^P{}_{Hjoin}$
⑤ $SM_i \rightarrow H_{join}(A) : [AC_A, R_{new2}]K^P{}_{Hjoin}, [AC_A, R_{new1}, E^{GM}{}_K, E^{lg}{}_{Ki}]K^P{}_{Hjoin}$

(2) 보안 에이전트가 존재하는 서브그룹

멤버가 없는 서브그룹에서와 같이 가입을 원하는 단말(H_{join})은 SM_i를 통해서 GM에게 가입 요청을 한다. GM은 권한 증명서 AC_H를 SM_i과 에이전트 A_k에게 전달하여 가입 단말로 하여금 권한 증명서와 지역 $E^{lg}{}_{Ki}()$, 새로운 키 정보(R_{new2})를 안전한 채널을 통해 수신하도록 한다.

① $H_{join} \rightarrow SM_i : P_{id}, [RC_{Hjoin}]K^P{}_{GM}$
② $SM_i \rightarrow GM : P_{id}, [RC_{Hjoin}]K^P{}_{GM}, [SM_i]K^P{}_{GM}$
③ $GM \rightarrow SM_i : [AC_H]K^P SM_i$
④ $SM_i \rightarrow A_k : [P_{id}, K^P{}_{Hjoin}, R_{new2}]K^P{}_{Ak}$
⑤ $A_k \rightarrow H_{join} : [A_k, R_{new2}, E^{lg}{}_{Ki}]K^P{}_{Hjoin}$
⑥ $A_k \rightarrow H_{k1}, H_{k2}, \cdots, H_{kn} : [P_{id}, R_{new2}]LTK$

4.1.2 탈퇴(leave)

(1) 보안 에이전트(A)가 아닌 단말

단말(H_d)이 보안 에이전트가 있는 서브그룹을 탈퇴하는 경우에 SM_i는 GM에게 탈퇴를 통보하고 앞으로 단말이 멀티캐스트 데이터에 접근할 수 없도록 지역 세션키 LTK를 갱신하는데 사용되는 새로운 키 정보(R_{new2})를 단말(H_d)을 제외한 나머지 단말들에게 안전한 채널을 통해 분배한다.

① $H_d \rightarrow SM_i : P_{id}$
② $SM_i \rightarrow GM : P_{id}$
③ $SM_i \rightarrow A_k, H_{k1}, H_{k2}, \cdots, H_{kn} : P_{id}, [R_{new2}]K^P{}_{Ak}, [R_{new2}]K^P{}_{Hk1}, [R_{new2}]K^P{}_{Hk2}, \cdots, [R_{new2}]K^P{}_{Hd-1}, [R_{new2}]K^P{}_{Hd+1}, \cdots, [R_{new2}]K^P{}_{Hkn}$

(2) 서브그룹 내에 다른 단말을 관리하는 보안 에이전트

서브그룹 내에 다른 단말이 있는 보안 에이전트가 그룹을 탈퇴하는 경우는 새로운 단말이 보안 에이전트가 되어야 한다. 먼저 SM_i는 GM에게 보안 에이전트의 탈퇴를 통보하면, GM은 해당 서브그룹내의 다른 단말에게 권한 증명서 AC_A를 전송하여 에이전트의 역할을 수행할 수 있도록 새로운 키 정보(R_{new1})와 $E^{GM}{}_K()$를 전송한다. 그리고 SM_i는 사용중인 지역 세션키를 갱신하기 위해 새로운 키 정보(R_{new2})를 탈퇴하는 단말(A_d)을 제외한 나머지 멤버에게 전송한다. ④에서 암호화 알고리즘 $E^{lg}{}_{Ki}()$은 전송하지 않고 기존의 알고리즘을 그대로 사용한다.

① $A_d \rightarrow SM_i : (A_d)P_{id}$
② $SM_i \rightarrow GM : (A_d)P_{id}$
③ $GM \rightarrow A_1, A_2, \cdots, A_s : (A)P_{id}, [R_{new1}]K^P{}_{A1}, [R_{new1}]K^P{}_{A2}, \cdots, [R_{new1}]K^P{}_{Ad-1}, [R_{new1}]K^P{}_{Ad+1}, \cdots, [R_{new1}]K^P{}_{As}$
④ $GM \rightarrow SM_i : [AC_A, H_{ki}]K^P{}_{SM}, [R_{new1}, E^{GM}{}_K]K^P{}_{Hki}$
⑤ $SM_i \rightarrow H_{ki} : [AC_A, R_{new2}]K^P{}_{Hki}, [R_{new1}, E^{GM}{}_K]K^P{}_{Hki}$
⑥ $SM_i \rightarrow H_{k1}, H_{k2}, \cdots, H_{kn} : (A)P_{id}, [R_{new1}]K^P{}_{Hk1}, [R_{new1}]K^P{}_{Hk2}, \cdots, [R_{new1}]K^P{}_{Hkn}$

(3) 서브그룹내에 다른 멤버가 없는 에이전트

SM_i는 GM에게 보안 에이전트의 탈퇴를 통보하면 GM는 새로운 키 정보(R_{new1})와 $E^{GM}{}_K()$를 생성하여 탈퇴되는 에이전트를 제외한 다른 에이전트에게 전송한다.

① $A_d \rightarrow SM_i : (A_d)P_{id}$
② $SM_i \rightarrow GM : (A_d)P_{id}$
③ $GM \rightarrow A_1, A_2, \cdots, A_s : (A)P_{id}, [R_{new1}]K^P{}_{A1}, [R_{new1}]K^P{}_{A2}, \cdots, [R_{new1}]K^P{}_{Ad-1}, [R_{new1}]K^P{}_{Ad+1}, \cdots, [R_{new1}]K^P{}_{Ak}$

4.2 서브그룹 연산(subgroup operation)

그룹을 소그룹으로 분할(division)하고자 하는 경우에는 아래와 같이 SM_i는 그룹내의 특정 멤버를 에이전트로 GM에게 통보하면 지정된 단말($H_{ki}(A_{new})$)은 GM으로부터 AC_A와 새로운 키 정보(R_{new1}), $E^{GM}{}_K()$, $E^{lg}{}_{Ki}()$를 수신한다. 분할된 그룹내의 소그룹은 서로 다른 지역 세션키를 사용하며 각 멤버들은 자신의 에이전트를 통해서 송신자의 데이터를 수신한다. 서브그룹을 통합(fusion)하는 경우에는 위에서 기술한 서브그룹 내에 다른 멤버가 있는 에이전트 탈퇴 절차와 같다.

① $SM_i \rightarrow GM : H_{ki}(A_{new})P_{id}$
② $GM \rightarrow SM_i : [AC_A, H_{ki}(A_{new})]K^P{}_{SM}, [AC_A, R_{new1}, E^{GM}{}_K, E^{lg}{}_{Ki-1}]K^P{}_{Hki}$
③ $SM_i \rightarrow H_{ki} : [AC_A]H^P{}_{ki}, [AC_A, R_{new1}, E^{GM}{}_K, E^{lg}{}_{Ki+1}]H^P{}_{ki}, [R_{new2}, H_{i+1}, H_{i+2}, \cdots, H_n]H^P{}_{ki}$
④ $H_{ki} \rightarrow H_{i+1}, H_{i+2}, \cdots, H_n : [R_{new2}, E^{gi}{}_{Ki+1}]K^P{}_{Hi+1}, [R_{new1}, E^{gi}{}_{Ki+1}]K^P{}_{Hi+2}, \cdots, [R_{new1}, E^{gi}{}_{Ki+1}]K^P{}_{Hn}$

4.3 데이터 전송(data transmission)

송신자는 멀티캐스트 데이터를 그룹 세션키 TEK로 암호

화하여 SM에게 분배한다. SM은 수신한 데이터를 자신의 멤버(서브그룹 SM, 에이전트를 포함한 단말)에게 다시 재분배하는데 보안 에이전트만이 송신자가 분배한 데이터를 복호화할 수 있다. 보안 에이전트는 수신한 데이터를 지역 세션키로 재암호화하여 자신의 멤버들에게 분배하고 나머지 단말은 지역 세션키를 사용하여 송신자가 보낸 데이터에 접근한다.

4.4 정기적 키 갱신(periodic re-keying)

멀티캐스트 데이터가 안전하게 전송되기 위해서는 데이터의 암호화와 세션키의 갱신 절차가 필요하다. 암호화 과정은 데이터의 노출을 방지하기 위함이고, 세션키의 갱신은 키 분석가로부터 키 추적과 그룹을 가입하거나 탈퇴되는 단말들이 데이터에 접근하는 것을 막기 위함이다. 앞에서 기술한 것처럼 그룹에 단말의 가입하거나 탈퇴로 인한 세션키의 갱신은 일시적 키 갱신(temporary re-keying)이라 정의하고, 키 갱신 시기에 의한 갱신은 정기적인 키 갱신(periodic re-keying)이라고 정의한다. 하나의 세션키가 장기간 사용되거나 많은 양의 데이터를 암호화하는데 사용되면 키 분석가에게 쉽게 해독되게 된다. 따라서 세션키가 사용된 기간이나 암호화된 데이터 량 등에 따라 정기적인 키 갱신 시기를 결정하는 정책이 필요하다. 또한 안전한 데이터 교환을 위하여 정기적으로 비밀키 암호화 알고리즘을 갱신한다.

5. 분 석

5.1 보안 위협 분석

본 논문에서 제안한 키 분배 프로토콜에 대한 보안 위협은 그룹 세션키와 지역 세션키, 단말 신원과 위치 정보의 노출 등이 있다. 전송중인 세션키의 노출 문제는 키를 안전한 채널을 통해 전달하므로 안전하며, 지역 세션키의 문제는 불법 사용자가 다른 서브그룹 노드(보안 에이전트 제외)와의 타협을 통해 지역 세션키를 알게 되더라도 서브그룹 간에는 서로 다른 키를 사용하기 때문에 안전하다. 또한 지역 세션키를 생성하는 알고리즘을 알고 있는 가입(또는 탈퇴) 단말이 가입 전(또는 후)에 수신한 데이터에 접근하기 위해서는 키 정보(R)가 있어야 한다. 그러나 R은 안전한 채널을 통해 전달되기 때문에 세션키를 추적하는 것은 쉬운 일이 아니다. 또한 단말의 그룹 가입 시 실제 ID가 들어있는 요청 증명서 RC를 가명 P_{id}를 사용하여 인증 센터에 보내고, 각종 정보나 데이터를 가명으로 수신하기 때문에 모든 단말의 신원과 위치정보를 알아내는 것이 쉽지 않다.

5.2 기존 모델과의 비교분석

안전한 멀티캐스트 프로토콜을 위한 키 분배 방식을 제안한 Wong[9]와 Iolus[4], Dondeti[3]과 본 논문에서 제안된 키 분배 방식을 <표 2>과 같이 서로 비교 분석하였다. Wong과 Dondeti의 방식에서 모든 단말은 중앙 키 분배 센터에서 분배한 하나의 세션키를 사용하기 때문에 빈번한 일시적인 키 갱신을 수행해야 하는 환경에서는 전체 시스템의 성능에 많은 영향을 주게 된다. Iolus가 제안된 방식은 서브그룹간에 서로 다른 지역 세션키를 사용하기 때문에 단말의 이동에 따른 오버헤드는 적지만 송신자와 수신자 사이에 여러 개의 서브그룹 관리자가 존재하는 경우에 서브그룹의 수만큼 재암호화와 재분배로 인한 데이터의 전송 지연이 발생하게 되어 그룹을 확장하는데 한계가 있다. 그러나 본 논문에서 제안된 방식은 Iolus의 방식과 유사하지만 송신자와 모든 수신자간에 재암호화 절차를 한 번만 수행하고, 각 서브그룹별로 자치적인 지역 세션키를 사용하는 방식이다. 따라서 제안된 방식은 Iolus 방식의 문제점인 반복되는 재암호화와 재분배 과정을 줄일 수 있고, Wong과 Dondeti의 방식에서 야기될 수 있는 빈번한 키 갱신 문제를 완화할 수 있어 기존 방식에 비해 더 유리한 대규모 그룹 확장성을 가진 메커니즘이다.

그리고 Wong와 Iolus 방식에서는 데이터가 중간 노드(서브그룹 관리자)에게 노출되는 문제를 고려하지 않았지만 서브그룹 멤버인 보안 에이전트의 개념을 사용하여 이러한 노출 문제를 해결하였으며, Wong와 Iolus, Dondeti 방식에서는 단말에 대한 프라이버시 침해 문제를 고려하지 않았지만 본 논문에서는 가명(P_{id})와 RC를 사용하여 단말의 프라이버시 문제를 해결하였다.

〈표 2〉 기존의 프로토콜과의 비교

구 분	Wong	Iolus	Dondeti	제안된 모델
그룹 세션 키의 수	1	ℓ	1	ℓ
전체 키의 수	$\frac{dn-1}{d-1}$	$n+\ell+1$	$n+\ell+1+c$	$n+2\ell+1$
GM이 관리하는 키의 수	$\frac{dn-1}{d-1}$	2	$c+2$	2
SM이 관리하는 키의 수	-	$\ell+1$	2	3
멤버가 관리하는 키의 수	$\log_d n$	2	3	2
가입시 메시지의 전송 수	$\log_d n$	2	2	2
탈퇴시 메시지의 전송 수	$d\log_d n$	$\underline{\ell}$	$\underline{\ell}$	$\underline{\ell}$
SM의 세션키 암호화 횟수	1	1	c	1
세션키 분배시 전체 암호화 횟수	1	$\underline{\ell}$	$\ell+c$	ℓ
송·수신자간의 최대 재암호화 횟수	0	D	0	1
서브그룹의 자치성	없음	있음	중간	있음
그룹의 확장성	가능	가능	가능	가능
멤버의 프라이버시	-	-	-	보장
빈번한 멤버 가입/탈퇴에 따른 전체 시스템의 오버헤드	많음	적음	많음	중간
데이터 전송 지연의 주원인	키 분배	재암호화	키 분배	재암호화
세션키 생성의 주체	중앙 센터	중앙 센터, 서브그룹 관리자	중앙 센터	중앙 센터, 보안 에이전트
중간 노드의 신뢰성 조건	필요	필요	불필요	불필요

n : 전체 그룹의 멤버(그룹 관리자의 수 + 서브그룹 관리자의 수 + 전체 단말의 수(H, A)), a : 보안 에이전트의 수($0<h$, $0<a\le h$) ℓ : 서브그룹의 수 ($0\le\ell<h$), $\underline{\ell}$: 한 서브그룹의 평균 크기, D : 키 분배 트리의 깊이, d : 가지 수, c : 송신자 서브그룹의 크기(키 그룹의 수), - : 언급되어 있지 않음

6. 결 론

본 논문에서는 멤버의 이동(가입/탈퇴)이 빈번한 대규모 동적 그룹 환경에서 효율적으로 세션키를 분배하는 프로토콜에 관하여 기술하였다.

기존에 개발된 안전한 멀티캐스트 프로토콜들과는 달리, 본 논문에서 제안된 프로토콜은 시스템의 오버헤드를 최소화하면서 대규모 그룹으로의 확장성을 지원할 뿐만 아니라 전송중인 데이터에 중간 노드인 서브그룹 관리자가 접근할 수 없도록 하였다. 또한 무선 컴퓨팅 환경에서는 송·수신자의 신원이나 데이터 내용, 위치의 노출 등으로 인한 사용자의 프라이버시 침해를 방지할 수 있는 장점을 갖는다. 기존의 시스템과 여러 가지 측면에서 <표 2>과 같이 비교 분석해 본 결과 제안된 프로토콜이 더 우수하다. 그러나 서비스를 사용하는 그룹 단말들은 보안 에이전트의 신뢰성에 의존하게 되고, 보안 에이전트에서의 키 관리와 재암호화에 따른 오버헤드가 발생하는 문제가 있다.

향후 과제는 제안된 프로토콜을 구현하고, 실제 통신망 환경에서의 시뮬레이션을 통하여 기존의 프로토콜들과 비교 분석하는 연구를 수행할 예정이다.

참 고 문 헌

[1] A. Schiper, K. Birman, P. Stephenson, "Lightweight Causal and Atomic Group Multicast," ACM Trans. on Computer Systems, Vol.9, No.3, August, 1991.

[2] M. Burmester and Y. G. Desmedt, "Efficient and secure conference-key distribution," In Security Protocols Workshop, 1996.

[3] Lakshminath R. Dondeti, Sarit Mukherjee, "A Dual Encryption Protocol for Scalable Secure Multicasting," Proceedings of IEEE International Symposium on Computer Communication, June, 1999.

[4] Suvo Mittra, "Iolus : A Framework for Scalable Secure Multicasting," In Proceedings of ACM SIGCOMM '97, Sept., 1997.

[5] Alain Pannetrat, Refik Molva, "Scalable Multicast Security with Dynamic Recipient Groups," ACM transactions on Information and System security, Vol.3, No.3, pp.136-160, August, 2000.

[6] Gene Tsudik, Michael Steiner, Michael Waidner, "CLIQUES : A New Approach to Group Key Agreement," In Proceedings of ICDCS '98, May, 1998.

[7] Eric Harder, Samir Koussih, Sanjeev Setia, Sushil Jajodia, "Kronos : A Scalable Group Re-keying Approach for Secure Multicast," Proceeding of 2000 IEEE Symposium on Security & Privacy, 2000.

[8] D. M. Wallner, E. G. Harder and R. C. Agee. "Key Management for Multicast : Issues and Architecture," Internet Draft, draft-wallner-key-arch-01.txt September, 1998.

[9] Chung Kei Wong, Mohamed Gouda, Simon S. Lam, "Secure Group Communications Using Key Graphs," In Proceedings of ACM SIGCOMM '98, Sept., 1998.

김 태 연

e-mail : tykim@tiger.seonam.ac.kr

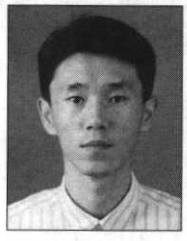
1986년 전남대학교 계산통계학과(이학사)

1988년 전남대학교 대학원 전산통계학과 (이학석사)

1996년 전남대학교 대학원 전산통계학과 (이학박사)

1996년~현재 서남대학교 컴퓨터정보통신학과 조교수

관심분야 : 정보 보안, 통신망 관리, 이동 통신 등



김 영 균

e-mail : kimyoung@etri.re.kr

1991년 전남대학교 전산통계학과(이학사)

1993년 전남대학교 대학원 전산통계학과 (이학석사)

1995년 전남대학교 대학원 전산통계학과 (이학박사)

1995년~현재 한국전자통신연구원 컴퓨터소프트웨어연구소 컨텐츠기술연구부 선임연구원

관심분야 : 데이터베이스 시스템, 멀티미디어 정보 검색, 데이터베이스 통합, 데이터베이스 보안 등