情報保護學會論文誌
第12券 第2號, 2002. 4

이동네트워크 환경에서의 그룹키 관리구조*

박 영 호**, 이 경 현***

A Group Key Management Architecture in Mobile Network Environments

Young-Ho Park**, Kyung-Hyune Rhee***

요 약

본 논문에서는 안전한 그룹통신을 위한 그룹키 관리 기법을 기반으로 이동네트워크 환경에서의 그룹키 관리 구조와 멤버의 인증과 키 설정을 위한 프로토콜을 제안한다. 기존의 대부분의 그룹키 관리기법들이 초기의 키 서버와 멤버간의 안전한 공유키 설정을 위해 공개키 기반의 인증서 교환을 이용하였으나, 본 논문에서는 인증서의 교환과 검증으로 인한 대역폭 소모의 효율성을 위해 ICPK를 이용해서 그룹 내에서의 멤버의 인증과 키 교환에 이용하도록 한다. 또한, 전체 그룹을 이동호스트들에 대한 셀 그룹과 셀 그룹 관리자들에 대한 제어그룹으로 구분하여 셀 그룹마다 셀 그룹 관리자가 관리함으로써 멤버십의 변경으로 인한 영향을 지역적으로 한정시킨다.

ABSTRACT

In this paper, we propose a group key management architecture for the secure group communications in mobile networks and authenticated key agreement protocol for this system. Most of existing group key management schemes use certificates based on the public key for the purpose of user authentication and key agreement in secure fashion, however, we use the ICPK(Implicitly Certified Public key) to reduce the bandwidth for a certificate exchanging and to improve a computational efficiency. In this architecture, we use two-tier approach to deal with key management where the whole group is divided into two parts; the first is a cell groups consisted of mobile hosts and another is a control group consisted of cell group managers. This approach can provide flexibility of key management such that the affection for a membership change is locally restricted to the cell group which is an autonomous area of the CGM(Cell Group Manager).

keyword : *Key management, Group key, Secure group communication, Scalability, Efficiency*

Ⅰ. 서 론

인터넷의 활용 영역이 다양한 분야로 확대되면서 여러 명의 사용자들에게 동일한 서비스를 제공해주기 위한 그룹 통신에 대한 요구가 증가하고 있다. 따라서 안전한 그룹 통신을 위해 그룹 사용자들에게 전송되는 정보에 대한 기밀성(confidentiality)과 무결성(integrity) 그리고 그룹 사용자에 대한 인증과 같은 보안 요구사항이 만족되어야 한다.

안전한 그룹 통신 프로토콜은 효율적이며 안전한 그룹키 관리기능과 그룹 멤버십 제어기능을 제공해야 한다. 일대일 통신이 하나의 통신 세션동안 정적인데 반해 그룹 통신은 한 세션동안 사용자들의 그룹 참여(join)와 탈퇴(leave)가 발생하는 동적인 특성

* 본 논문은 2001년 한국학술진흥재단의 지원에 의하여 연구되었음(KRF-2001-13-E00064)
** 부경대학교 정보보호과정(pyhoya@mail1.pknu.ac.kr)
*** 부경대학교 전자컴퓨터정보통신공학부(khrhee@pknu.ac.kr)

을 고려해야 하며, 탈퇴하는 멤버에 대한 forward secrecy와 새로 참여하는 멤버에 대한 backward secrecy를 제공해야 한다. 그리고 그룹키 관리의 효율성(efficiency)과 확장성(scalability)을 고려할 때, 그룹키의 갱신과 키의 전송 및 암호화와 관련된 오버헤드는 그룹의 크기에 독립적이어야 하며 그룹에서의 호스트의 추가와 삭제로 인한 그룹키 갱신의 영향이 그룹의 모든 멤버에게 끼치지 않도록 해야한다.

본 논문에서는 이동네트워크 환경에서 안전한 그룹통신을 위한 그룹키 관리구조를 제안한다. 이동네트워크 환경에서의 그룹 관리 구조를 이동 호스트들로 구성되는 셀 그룹(cell group) 영역의 하부계층과 그룹 관리서버(Group manager, GM)와 각 셀 그룹 관리서버(Cell group manager, CGM)들의 관리개체들로 구성되는 상부계층으로 구분함으로써 2-계층 형태의 그룹키 관리구조를 적용하도록 한다.

이동네트워크의 주된 특징은 호스트의 이동성이며, 호스트의 빈번한 이동으로 인한 셀 그룹의 참여와 탈퇴는 그룹의 동적인 특성을 더욱 증대시킨다. 그러므로 이동네트워크 환경에서는 그룹의 동적인 특성을 고려한 그룹키 관리가 이루어져야 한다.

본 논문에서는 하부의 셀 그룹의 그룹키 관리는 키 관리 서버가 담당함으로써 멤버들의 그룹키 관리에 대한 부담을 줄이고, 상부의 제어그룹에 대한 키 관리는 분산형(decentralized) 방식을 사용함으로써 특정 키 관리 개체의 오류로 인한 'one-point failure'[8]를 방지하도록 한다. 또한 각 셀 그룹은 자신들만의 자치영역을 구성함으로써 해당 그룹의 멤버십 변경에 대한 영향을 지역적으로 한정시키고 다른 셀 그룹에 영향을 주지 않도록 한다. 즉, 어떤 호스트의 이동으로 인해 전체 그룹에 대한 멤버십의 변경은 발생하지 않고 단지 호스트의 관리를 위한 셀 그룹의 서비스 영역만 변경된다. 그러므로 호스트의 관리 영역이 변경되더라도 이동한 호스트는 계속적으로 그룹 통신에 참여할 수 있어야 하고, 이전의 셀 그룹에 대해서는 멤버의 셀 그룹 탈퇴와 이전한 셀 그룹에 대해서는 멤버의 셀 그룹 참여로 인한 셀 그룹키 갱신이 수행되어야 한다.

본 논문의 구성은 다음과 같다. 2장에서는 그룹키 관리시의 고려사항과 그룹키 관리기법들의 유형에 대해서 설명하고, 3장과 4장에서는 제안시스템의 구조와 그룹키 운영방식에 대해서 각각 설명한다. 5장에서는 제안시스템에 대해 성능 및 안전성을 분석하며 6장에서 결론을 맺는다.

II. 그룹키관리 관련연구 및 고려사항

2.1 그룹키 관리의 고려사항

안전한 그룹통신의 핵심은 그룹키의 관리이며, 그룹키를 관리함에 있어서 고려해야 하는 사항으로 그룹키에 대한 안전성과 관리 시스템의 효율성을 고려해야 한다.

- 그룹키의 비밀성(Group Key Secrecy)

가장 기본적인 성질로서, 어떤 악의적인 공격자가 그룹키를 도출해 내는 것이 계산상 불가능하여야 한다.

- Forward Secrecy

악의적인 공격자가 이전 세션의 그룹키들에 대한 정보를 알고있더라도 이후의 그룹키를 계산하지 못하게 함으로써 데이터에 접근할 수 없어야 한다.

- Backward Secrecy

악의적인 공격자가 이후에 알려진 그룹키에 대한 정보를 가지고서 이전 세션의 그룹키를 계산하지 못함으로써 데이터에 접근할 수 없어야 한다.

- 키 독립성(*Key Independency*)

그룹키 집합 K의 적당한 부분집합 K'을 알고있는 공격자가 그룹키의 다른 부분집합 $\overline{K} \in (K-K')$를 계산할 수 없어야 한다.

위 네 가지 성질들은 서로 연관성을 가지고 고려되어야 한다. 그룹 멤버의 탈퇴시 이후의 데이터에 대한 forward secrecy를 제공해야 하며 새로운 멤버의 참여시 이전의 데이터에 대한 backward secrecy를 제공해야 한다. 그리고 여러 멤버들의 공모로 인해 그룹키가 노출되는 것을 막기 위해 키의 독립성도 제공해야 한다.

이러한 암호학적인 성질들과 함께 그룹키 관리 메커니즘을 구현함에 있어 시스템의 성능에 대해서도 다음과 같은 사항을 고려해야 한다.

- 시스템 구조 : one point failure의 해결

즉 한 개체의 오류가 전체 시스템의 오류로 확산

되어서는 안 된다.

- 시스템의 확장성(Scalability)

다수의 멤버들이 광범위한 지역으로 분포되어 있는 그룹을 관리할 수 있도록 확장성을 제공해야하고, 동적인 멤버십을 가지는 그룹의 빈번한 키 갱신을 효율적으로 처리할 수 있어야 한다.

- 그룹 관리자와 멤버들이 관리하는 키의 개수
- 키 갱신을 위해 필요한 메시지의 개수
- 키 관리를 위한 processing time

2.2 이동 네트워크 환경에서의 고려사항

이동네트워크 환경에서의 이동호스트들은 기존의 유선 환경의 호스트들에 비해 다음과 같은 제약사항을 가진다.

- 계산 능력과 저장공간의 제약
- 낮은 대역폭의 무선 채널
- 호스트의 이동

이동호스트는 일반적이 유선환경에서의 호스트인 PC에 비해 충분한 계산능력과 저장공간을 가지지 못하며, 무선 통신 채널의 낮은 대역폭에 대한 제약사항도 고려되어야 한다. 이동호스트의 이러한 제약사항은 이동호스트들이 피어(peer)로서 안전한 그룹통신에 참여하는 것을 제한하게 되며, 이동호스트를 위한 효율적인 그룹키 관리가 수행되어야 한다. 그리고 이동네트워크의 주된 특징은 호스트의 이동성이며 이동호스트가 다른 영역으로 이동하는 경우 해당 영역에서의 새로운 세션키를 통해 계속적인 그룹통신을 안전하게 수행할 수 있어야 한다.

2.3 그룹키 관리기법

안전한 그룹통신을 위한 대부분의 연구들이 그룹키의 관리에 초점을 맞추어 연구되어 왔으며, 이들은 시스템 관리 유형에 따라 크게 중앙집중형 방식과 분산형 방식 그리고 계층적 관리구조로 구분할 수 있다. 중앙집중형 방식은 하나의 신뢰되는 개체(trusted entity)인 키 관리 서버가 모든 그룹의 멤버들에게 암호화키의 분배를 담당하는 방식으로, 그룹의 멤버십이 변경될 때마다 그룹 관리자가 갱신된 그룹키를 모든 그룹 멤버들에게 안전하게 전달하는 방식이다. 이 방식은 그룹의 모든 멤버들을 하나의 관리 개체가 직접관리 하므로 한 멤버의 멤버십 변경이 전체 그룹 멤버들이 그룹키를 갱신해야 하는 'one effects all'의 성질과 중앙 키 관리 서버의 오류로 인해 전체 그룹키 관리가 수행되지 못하는 'one-point failure'의 문제를 가진다.[8]

분산형 방식은 그룹의 모든 멤버들이 피어(peer)로서 그룹에 참여하며 동등하게 신뢰되는 방식으로 그룹키 생성과 분배에 대한 책임을 여러 멤버들에게 분담하는 방식이다. 그러나 키의 분배를 멤버들에게 분담함으로 인해 내부 공모에 대한 보안상의 취약성을 가질 수 있다.

계층적 그룹키 관리 방식은 중앙집중형 시스템의 확장성을 제공하기 위한 방법으로, 이 방식은 다시 두 가지로 구분된다. 첫 번째 방식은 키 트리(Key tree)라는 키들간의 계층구조[2,11,12]를 사용하는 방식이고 두 번째는 확장성을 위해 네트워크 노드들간의 계층구조[8]를 사용하는 방식이다. 키 트리를 사용하는 대부분의 방식이 중앙집중형의 키 서버의 확장성을 위해 제안되었으며 키 관리서버의 관리비용을 $O(n)$에서 $O(\log n)$으로 감소시킬 수 있고, [7][9]에서는 키 트리를 이용한 분산형 키 관리 방안을 제안하였다.

본 논문의 제안구조에서는 OFT(One way function tree)[2]와 TGDH(Tree-based group Diffie-Hellman)[7]를 그룹키 관리 기법으로 가정하므로 이 두 기법의 그룹키 계산과정만을 본 절에서 설명하도록 한다.

2.3.1 OFT 그룹키 관리 기법

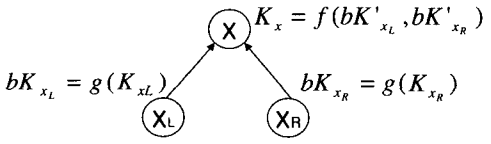
OFT[2]는 멤버의 참여나 탈퇴시 키 갱신을 위한 키 관리서버의 계산량을 줄이기 위해 키 트리 기법의 변형된 방법을 제안하였다. 이 방법은 키 트리에서 새로운 그룹키를 계산하기 위해 일방향함수(one-way function)를 키 트리에 상향식(bottom-up)으로 적용하였다. 키 관리서버는 일반적인 키 트리 기법처럼 사용자의 비밀키를 단말노드로 가지고 루트노드가 그룹키가 되며 중간 노드의 키들이 키 암호화키(Key encryption key)로 사용되는 이진 키 트리(binary key tree)를 관리한다.

키 트리에서 각 노드 x는 노드 키(node key) K_x와 블라인드 노드 키(Blinded node key)라는 bK_x 두 개의 키와 연관되어 진다. 이때 블라인드 노드 키 $bK_x = g(K_x)$이며, 함수 $g()$는 일방향함수

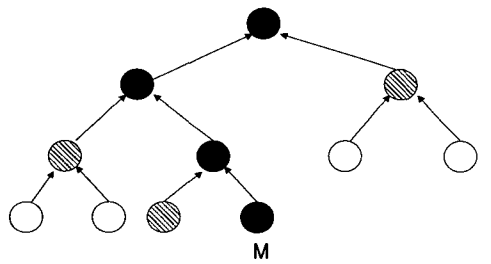
이다. 즉, 블라인드 키는 실제 키의 값을 직접 드러내지 않도록 숨기는 역할을 하게되고 키 갱신 정보는 노드키로 암호화되어 전달된다. 함수 g가 일방향 함수이므로 bK_x로부터 노드 키 K_x를 구하는 것은 계산상 불가능하다는 성질을 가지게 된다. 키 트리의 구조에서 중간 노드들은 모두 두개의 자식 노드를 가지며 단말노드는 각각의 멤버와 그룹 관리자간에 공유되는 비밀키로 할당된다. 키 트리상의 중간노드 x의 노드키 K_x는 x의 두 자식 노드의 블라인드 키들에 의해 계산되며 이를 도식화하면 [그림 1]과 같다. 여기서 x_L과 x_R은 노드 x의 왼쪽과 오른쪽 자식노드를 나타낸다. 함수 f는 혼합함수(mixing function)로써 일방향함수일 필요는 없으며, [2]에서는 혼합함수로서 bit-XOR 연산을 사용하였다.

그룹 멤버는 자신에 해당하는 단말노드의 키와 루트노드까지의 경로상의 형제 노드들(sibling nodes)의 블라인드 키들을 관리하고, 함수 g와 f를 사용해서 경로상의 노드키와 루트키인 그룹키를 계산해낼 수 있다. [그림 2]는 OFT 트리의 예제이다. M으로 표기된 단말노드에 해당하는 멤버는 빗금으로 표시된 노드의 블라인드 키들만 알고 있고 자신의 비밀키와 트리 경로상의 형제 노드들의 블라인드 키들을 함수 $g()$와 $f()$를 이용해서 경로상의 노드들의 키를 계산하고 최종적으로 루트노드인 그룹키를 계산할 수 있다.

어떤 멤버가 그룹에 참여하거나 탈퇴할 때, 해당 멤버에 대한 트리의 경로상의 모든 키들이 갱신되어야 한다. 하지만 내부 노드의 키들은 하위 노드의 키들에 의해 계산될 수 있으므로 그룹서버는 해당멤버에 의해 영향 받는 단말노드의 키 하나만 새로



[그림 1] OFT의 노드키 계산 과정



[그림 2] OFT 트리의 구성

갱신하면 된다. 그리고 그룹서버는 변경된 키를 이용해서 내부 노드들의 키를 계산하고 그룹내의 멤버들이 멤버십의 변화로 인해 변경된 키들을 다시 계산할 수 있도록 새롭게 계산된 키들에 대한 정보를 안전하게 멀티캐스트 해야 한다. 그룹 멤버의 수가 n명이라 할 때, 그룹서버는 키 갱신을 위해 $O(\log_2 n)$의 연산을 필요로 하며, 실제로 전송되는 메시지는 멤버십이 변경되는 해당 멤버에서 루트 노드까지의 경로상의 모든 형제 노드들에 대한 블라인드 키들이다.

2.3.2 TGDH 그룹키 관리 기법

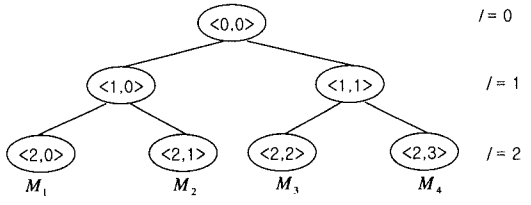
TGDH[7]는 피어들 간의 안전한 그룹 통신을 위한 분산형 그룹키 관리 방법으로서, 그룹키의 생성과 분배를 위해 Diffie-Hellman key exchange 프로토콜을 키 트리 구조에 적용하였다. 그룹키 관리를 위해 중앙 키 관리 서버를 두지 않고 있으며, 멤버의 참여와 탈퇴로 인해 그룹 멤버십의 변경이 발생하는 경우 스폰서(sponsor)로 지정되는 특정 그룹 멤버가 그룹키의 생성과 분배의 역할을 담당한다.

키 트리에서 각 l-레벨의 노드들은 $\langle l, v\rangle$로 표시되며 v는 $0 \le v \le 2^l - 1$ 범위의 값을 가지고 루트노드의 키가 모든 그룹멤버들간에 공유되는 그룹키로 사용된다. 각 노드 $\langle l, v\rangle$는 노드키 $K_{\langle l, v\rangle}$와 블라인드 노드키 $BK_{\langle l, v\rangle}$와 연관되며, $BK_{\langle l, v\rangle} = f(K_{\langle l, v\rangle})$로 계산되며, 이때 함수 $f()$는 임의의 큰 소수 p에 대한 법-지수(modulo exponentiation) 연산 즉, $f(k) = \alpha^k \bmod p$이다.

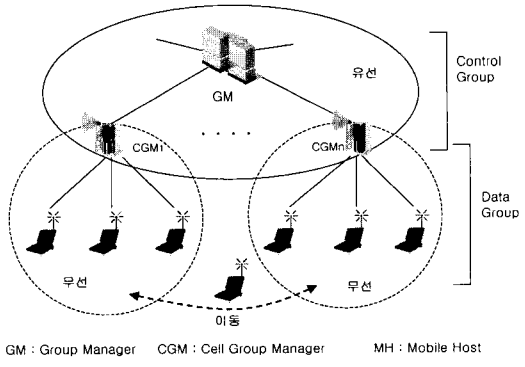
키 트리에서 단말 노드의 키는 해당 멤버 M_i 만이 알고있는 비밀값 r_i가 되며 단말 노드의 블라인드 노드키는 $\alpha^{r_i} \bmod p$가 된다. M_i는 자신의 비밀값과 키 트리상의 다른 노드들의 블라인드 노드키를 이용해서 단말노드에서 루트 노드인 $\langle 0, 0\rangle$까지의 경로상의 모든 노드키를 계산할 수 있다. 예를 들어, [그림 4]에서 멤버 M_2는 경로상의 노드키 집합 $\{K_{\langle 2,1\rangle}, K_{\langle 1,0\rangle}, K_{\langle 0,0\rangle}\}$와 모든 블라인드 노드키를 알고 있다.

모든 키 $K_{\langle l, v\rangle}$는 다음과 같은 반복적인 계산과정을 통해 계산될 수 있다.

$$
\begin{aligned}
K_{\langle l, v\rangle} &= (BK_{\langle l+1, 2v+1\rangle})^{K_{\langle l+1, 2v\rangle}} \bmod p \\
&= (BK_{\langle l+1, 2v\rangle})^{K_{\langle l+1, 2v+1\rangle}} \bmod p \\
&= \alpha^{K_{\langle l+1, 2v\rangle} \cdot K_{\langle l+1, 2v+1\rangle}} \bmod p \\
&= f(K_{\langle l+1, 2v\rangle} \cdot K_{\langle l+1, 2v+1\rangle})
\end{aligned}
$$



〔그림 3〕 TGDH의 키 트리 구성



〔그림 4〕 제안 모델의 그룹 관리 구조

$\langle l, v\rangle$노드의 키를 계산하기 위해서는 두 개의 자식 노드 중의 하나의 노드키와 다른 자식노드의 블라인드 키를 알고 있어야 한다. 키 트리에서 루트 노드의 키 $K_{\langle 0,0\rangle}$는 모든 그룹 멤버들간에 공유되는 그룹키로 사용된다.

그러므로 〔그림 3〕에서 각 멤버 M_i의 단말 노드에 대한 비밀값을 각각 r_i라고 할 때, 그룹키 $K_{\langle 0,0\rangle}$는 다음과 같이 계산된다.

$$K_{\langle 1,0\rangle} = \alpha^{r_1 \cdot r_2} \pmod{p}$$
$$BK_{\langle 1,0\rangle} = \alpha^{\alpha^{r_1 \cdot r_2}} \pmod{p}$$
$$K_{\langle 1,1\rangle} = \alpha^{r_3 \cdot r_4} \pmod{p}$$
$$BK_{\langle 1,1\rangle} = \alpha^{\alpha^{r_3 \cdot r_4}} \pmod{p}$$
$$K_{\langle 0,0\rangle} = \alpha^{\alpha^{r_1 \cdot r_2 \cdot r_3 \cdot r_4}} \pmod{p}$$

TGDH의 키 트리 갱신은 스폰서로 지정되는 특정 멤버가 담당하며, 스폰서는 멤버의 추가와 삭제로 인해 갱신되는 단말 노드에 대한 서브-트리(sub-tree)에서 제일 오른쪽의 단말 노드에 할당된 멤버가 된다. 스폰서는 변경되어야 하는 키 트리 상의 노드들의 블라인드 키들을 새로이 갱신하여 멤버들에게 전송하고, 새로운 블라인드 키들을 수신한 멤버들은 그룹키를 갱신하게 된다.

Ⅲ. 제안 모델의 그룹키 관리구조

3.1 시스템 구성

본 논문의 제안 모델은 그룹 멤버인 이동호스트 *MH*(Mobile host)와 전체 그룹관리자 *GM*(Group manager) 그리고 각 셀 영역의 그룹을 관리하는 셀 그룹 관리자 *CGM*(Cell group managers)로 구성된다. 그룹관리 구조는 2-계층(2-tier) 형태로 적용할 수 있으며, 첫 번째 계층(1st-tier)은 *GM*과 각 셀 그룹의 *CGM*들로 구성되는 제어그룹이 되며 *GM*과 *CGM*은 유선네트워크를 통해 통신하는 고정된 호스트들이 담당한다. 두 번째 계층(2nd-tier)은 각 *CGM*과 이동호스트들로 구성되는 셀 수준의 데이터 그룹으로 볼 수 있으며, *CGM*은 무선 통신을 위한 인터페이스를 가지고 있고 이동 호스트와 셀 그룹간의 데이터 전송을 담당한다. 이동호스트의 데이터 전송은 현재 자신이 속한 셀 영역의 *CGM*을 통해 수행된다. 〔그림 4〕는 제안모델의 그룹 관리 구조를 나타낸다.

1) 그룹 관리자(Group manager)

그룹 관리자 *GM*은 모든 멤버들에게 신뢰되는 개체로서, 이동호스트의 그룹 참여에 대한 초기인증과 이동호스트와 *CGM* 간의 인증과 키 설정을 위한 ICPK (Implicitly certified public key)를 제공하고 그룹의 전반적인 정책 관리만을 담당하며 이동호스트의 멤버십 변경에 대한 직접적인 키 관리는 수행하지 않는다.

2) 셀 그룹 관리자(Cell group manager)

셀 그룹 관리자 *CGM*은 유선과 무선 통신을 위한 인터페이스를 가지고 있으며 그룹키 관리를 위한 충분한 컴퓨팅 환경을 갖춘 호스트이다. 셀 그룹 관리자는 자신의 해당 셀 영역에 존재하는 그룹 멤버들에 대한 셀 그룹키를 생성하고 관리하며, 이동호스트의 데이터 트래픽을 다른 셀 그룹으로 전송을 중재(relay)하는 역할을 담당한다. 셀 그룹 관리자는 상부계층인 제어그룹의 구성원이 되며 제어그룹키를 사용해서 셀 그룹 관리자들과 제어그룹의 통신을 수행한다.

3) 이동호스트

이동호스트는 그룹통신의 주체가 되는 멤버로서

여러 셀들을 이동하게 된다. 이동호스트는 현재 자신이 속한 셀 그룹의 셀 그룹관리자와 다른 이동호스트들과 셀 그룹키를 공유하며 암호화된 통신을 수행한다.

3.2 그룹키 관리 전략

본 논문에서 제안하는 그룹키 관리 구조는 2-계층(2-tier)형태로서, 이동호스트들로 구성되는 셀 영역의 데이터 그룹과 관리개체들로 구성되는 제어그룹으로 형성된다. 각 셀 그룹은 셀 그룹 관리자와 해당 셀 그룹내의 이동호스트들과 공유하는 셀 그룹키를 사용해서 암호화된 통신을 수행하며, 각 셀 그룹 관리자들로 구성되는 제어그룹은 제어그룹키를 사용해서 암호화된 통신을 수행한다.

제어그룹키 관리와 셀 그룹키 관리는 독립적으로 수행되며, 이동호스트는 상대적으로 제약된 컴퓨팅 환경으로 인해 피어로서 그룹키 관리에 참여하는 것이 불가능하므로 셀 그룹키 관리는 해당 셀 그룹관리자가 담당하는 중앙집중형 방식을 적용하고 제어그룹키 관리는 각 셀 그룹관리자들이 피어로서 참여하는 분산형 방식을 적용한다.

만일 전체 그룹을 셀 그룹으로 분할하지 않고 모든 이동호스트들을 하나의 그룹키로 관리하는 경우, 호스트들이 다른 셀 영역으로 이동하더라도 그룹키를 변경하지 않아도 되므로 효율성을 가질 수 있다. 그러나 이러한 경우 이동호스트들의 컴퓨팅 능력의 제약으로 인해 그룹키 관리가 멤버들에게 분산되는 분산형 방식의 그룹키 관리는 수행될 수 없으며, 키 관리 서버가 그룹키 관리를 담당하는 중앙집중형 방식이 사용되어야 한다. 그리고 중앙집중형 방식은 'one-point failure'에 대한 문제가 발생할 수 있고 한 멤버의 멤버십 변경으로 인해 모든 멤버들이 새롭게 그룹키를 계산해야 하는 'one effects all'의 성질을 가지므로, 본 논문에서는 전체 그룹을 셀 그룹으로 분할하여 셀 그룹별로 독립적인 그룹키를 관리함으로써 멤버십의 변경으로 인한 영향이 셀 그룹으로 한정되도록 한다.

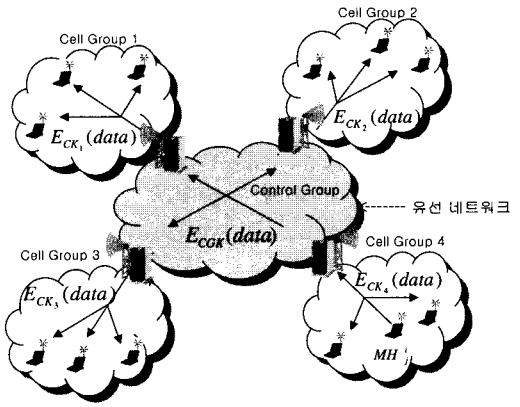
그룹키 관리에 관한 많은 기법들이 연구되어 왔으며, 본 논문에서는 제어그룹의 그룹키 관리 기법으로 피어간의 분산형 그룹키 계산 방법인 TGDH를 가정하고 셀 그룹키 관리는 OFT를 가정한다.

OFT는 새로운 멤버가 그룹에 참여시 새로운 멤버의 인증과 멤버와 관리자간에 공유되는 키 트리의 단말 노드키(Leaf node key)를 설정하기 위해 IKE (Internet key exchange)[5] 프로토콜을 가정하였다. 그러나 IKE의 경우 멤버의 인증을 위해 공개키 기반의 인증서(Certificate)의 교환을 통해 안전하게 키를 설정한다. 키 설정을 위한 인증서의 교환과 검증은 대역폭을 소모하고 많은 계산을 필요로 하며, 이동네트워크 환경에서 무선 통신 채널의 대역폭의 제한과 이동단말기의 계산능력으로 인해 인증서를 사용한 서명의 사용은 이동호스트에게 많은 계산상의 부담을 주게 된다. 그러므로 본 논문에서는 이동호스트의 인증과 OFT상에서 멤버에게 할당되는 단말노드의 비밀키를 설정하기 위해 그룹 내에서 인증과 키 설정을 위한 ICPK(Implicitly certified public key)를 사용한다. 4장에서 ICPK의 생성과 ICPK를 이용한 인증 및 키 설정 과정을 설명하도록 한다.

ICPK의 개념은 Günther가 [4]에서 제안하였으며 ElGamal 전자서명 기법을 기반으로 하고 있다. 본 논문에서는 계산상의 효율성을 고려해서 SDSS[14] 서명기법을 변형하여 이동호스트가 셀 그룹에 참여시 셀 그룹 관리자와의 인증과 키 설정을 위한 ICPK를 생성하도록 한다. ICPK는 그룹 관리자 GM이 생성하며 그룹에 가입하기를 원하는 이동호스트의 초기인증(Pre-authentication)을 수행한 후 그룹 내에서 사용되는 ICPK를 제공하고, 이동호스트는 이후의 셀 그룹에 참여시 셀 그룹 관리자와 ICPK의 교환을 통해 키를 설정하게 된다.

3.3 셀 그룹간의 암호화키 변환

이동호스트는 현재 자신이 위치한 셀 그룹의 *CGM*과 통신을 하며 다른 셀 그룹으로의 데이터 전송은 각 셀 그룹의 *CGM*들의 중재로 이루어진다. 즉, 셀 그룹 관리자 CGM_j의 셀 그룹에 위치한 이동호스트 MH_u^j가 현재 자신이 속한 셀 그룹의 셀 그룹키 CK_j로 데이터를 암호화한 후 CGM_j에게 전송한다. 암호화된 데이터 트래픽을 수신한 CGM_j는 자신의 셀 그룹내에 있는 멤버들에게는 수신한 데이터 트래픽을 다시 멀티캐스트하고, 다른 셀 그룹으로 전송하기 위해 암호화된 데이터 트래픽을 복호화 하여 현재 제어그룹키 *CGK*로 암호화하여 셀 그룹 관리자들에게 유선 네트워크를 통해 멀티캐스트 한다. 각 셀 그룹 관리자 CGM_k ($k \neq i$)는 제어그룹을 통해 수신된 데이터 트래픽을 현재 제어그룹키 *CGK*로 복호화



〔그림 5〕 그룹 데이터 전송을 위한 키 변환 과정

하고 자신의 셀 그룹키 CK_k로 암호화하여 셀 그룹으로 멀티캐스트 한다. 각 셀 그룹의 이동호스트 MH_u^k들은 자신들이 소유한 셀 그룹키 CK_k로 데이터에 접근할 수 있다. 그러므로 이동호스트들은 현재 자신이 위치한 셀 그룹의 그룹키만 관리하고 다른 셀 그룹으로의 데이터 전송은 각각의 셀 그룹 관리자들이 담당하게 된다. 〔그림 5〕는 이러한 과정을 도식화하여 나타내고 있다.

Ⅳ. 그룹 운용

4.1 그룹 초기화

*GM*은 그룹 초기화 단계에서 멤버들의 인증과 키 설정에 필요한 ICPK를 위한 파라미터들을 생성하고 공개하며, 각 CGM_i에 대한 ICPK를 제공한다. 각 CGM_i의 ICPK는 새로운 멤버가 자신의 셀 그룹에 참여할 때 멤버의 키 설정을 위해 사용된다. Procedure-1은 *GM*의 제어그룹을 구성하는 *CGM*들에 대한 ICPK 생성과 분배를 나타낸다. *GM*과 *CGM* 간의 통신은 유선 네트워크를 통해 이루어지며 초기의 ICPK의 분배는 안전한 통신 채널을 통해 각각 전송된다고 가정한다.

〔9〕에서는 멤버의 인증과 키 설정을 위해 〔4〕의 ElGamal 서명기법을 기반으로 하는 키 교환 프로토콜을 변형하여 ICPK를 생성함으로써 인증과 키 설정에 사용하였다. 〔14〕에서는 ElGamal 서명보다 효율성을 개선한 SDSS(Shortened DSS)를 제안하였다. 본 논문에서 사용하는 ICPK는 SDSS 서명기법을 변형하여 생성하였으며 키 설정과정에서 〔4〕의 법-역원(modulo-inverse) 연산을 제거하였다.

그룹 관리자 GM

1. 임의의 소수 p와 원시근 $\alpha(\alpha \in Z_p^*)$를 선택
   p : $512 \le p \le 1024$ bit
2. GM의 비밀값 $x \in Z_p^*$를 선택
   $y = \alpha^x \bmod p$를 계산,
   p, α, y 를 그룹 멤버들에게 공개
3. 각각의 셀 그룹 관리자 CGM_i에게 ICPK 분배
   3.1 각 CGM_i에 대한 ID_i를 선택
   3.2 각 CGM_i에 대한 K_i를 선택, K_i^{-1}를 계산
   : 이때, $\gcd(K_i, p-1)=1$이고,
   $K_i \cdot K_i^{-1} \equiv 1 \pmod{p-1}$
   3.3 CGM_i의 공개키를 계산
   $\gcd(K_i, p-1)=1$계산
   3.4 CGM_i의 비밀키를 계산
   $S_i = K_i^{-1} \cdot (H(P_i, ID_i) + x) \pmod{p-1}$
   3.5 ID_i, S_i, P_i를 제공

S_i : 개체 i의 비밀키,
P_i : 개체 i의 공개키
ID_i : 개체 i의 식별자
$H()$: hash function

Procedure-1 GM의 각 CGM의 ICPK 생성 및 분배

$MH_u \rightarrow GM$: *join_request*
GM이 MH_u의 인증을 수행하고 ICPK를 제공
$GM \rightarrow MH_u$: ID_u, P_u, S_u
; MH_u에 대한 Procedure-1 수행

Protocol-1 이동호스트 MH_u에 대한 ICPK 분배

$CGM_i \rightarrow MH_u$: ID_i, P_i,
$MH_u \rightarrow CGM_i$: ID_u, P_u, $(P_i)^{r_u} \bmod p$
$CGM_i \rightarrow MH_u$: $(P_u)^{r_i} \bmod p$
MH_u와 CGM_i는 키를 계산
$K_{MH_u} = \alpha^{K_u \cdot S_u \cdot r_i + K_i \cdot S_i \cdot r_u} \bmod p$

Protocol-2 MH_u와 CGM_i간의 인증 및 키 설정

4.2 그룹 참여

어떤 이동호스트 MH_u가 그룹에 참여하고자 하는 경우 MH_u는 *GM*의 초기 인증을 통해 ICPK를 부여받고, 자신이 소속되는 셀 그룹의 셀 그룹 관리자와 인증 키 설정을 통해 그룹에 참여한다. 이 때 멤버의 가입시 초기의 안전한 키 설정을 위해 *GM*과의 초

기인증을 통한 ICPK의 분배는 안전한 통신 채널을 사용하도록 하며, 셀 그룹 관리자와 protocol-1과 protocol-2에 따라 ICPK의 교환으로 키를 설정한다. *GM*과의 초기인증은 호스트가 처음 그룹에 멤버로 가입하는 경우에 한 번만 수행되며, 이 후의 이동호스트가 새로운 셀 그룹에 참여하는 경우에는 *GM*의 인증을 수행할 필요가 없다.

*GM*과의 인증을 통해 ICPK를 수신한 MH_u는 자신의 공개키 P_u와 식별자 ID_u를 자신이 소속하게 되는 셀 그룹의 관리자 CGM_i에게 전달하며, CGM_i는 MH_u에 대한 ICPK의 교환과 인증을 수행하고 CGM_i의 셀 그룹 멤버로 참여시킨다.

이 과정에서 만일 CGM_i가 자신의 셀 영역임을 알리기 위해 브로드캐스트 되는 공지 메시지(Advertisement message)에 자신의 ID_i와 P_i를 포함시킨다면 메시지 교환을 한번 정도 줄일 수도 있다. 한편 MH_u와 CGM_i의 키 K_{MH_u}의 계산은 procedure-2에 따라 계산할 수 있다. 이동호스트 MH_u는 CGM_i와 공유키를 계산하기 위해 한번의 해쉬연산과 두 번의 법-지수(modulo-exponentiation) 연산을 필요로 한다.

CGM_i는 MH_u를 멤버로 참여시키고, 새로운 멤버 MH_u에 대한 노드의 키를 K_{MH_u}로 할당하고 앞서 2장에서 설명된 OFT 프로토콜에 의해 자신의 셀 그룹의 키 트리를 갱신하고 갱신된 그룹키를 암호화해서 분배한다. 이 때 새로운 멤버의 OFT 트리 경로상의 형제 노드(sibling node)의 블라인드 키들은 K_{MH_u}로 암호화해서 MH_u에게 전달한다.

만일 해당 이동호스트가 위치한 셀 그룹의 CGM_i가 상위 제어그룹에 참여하고 있지 않은 경우 CGM_i의 제어그룹의 참여가 이루어져야 하며, 제어그룹의 그룹키는 앞서 2장에서 설명된 TGDH 프로토콜에 따라 갱신된다.

$$K_{MH_u} = \alpha^{K_u \cdot S_u \cdot r_i + K_i \cdot S_i \cdot r_u} = \alpha^{K_u \cdot S_u \cdot r_i} \cdot \alpha^{K_i \cdot S_i \cdot r_u} \pmod{p}$$

1) $\alpha^{K_u \cdot S_u \cdot r_i}$는 CGM_i로부터 수신한 $(P_u)^{r_i}$에 S_u를 지수승 함으로써 계산

$\therefore \alpha^{K_u \cdot S_u \cdot r_i} = ((P_u)^{r_i})^{S_u} \pmod{p}$

2) $\alpha^{K_i \cdot S_i \cdot r_u} = \alpha^{(H(ID_i, P_i)+x) \cdot r_u}$

$\therefore \alpha^{K_i \cdot S_i \cdot r_u} = (\alpha^{H(ID_i, P_i)} \cdot y)^{r_u} \pmod{p}$

Procedure-2 ICPK 교환 후의 키 계산

4.3 그룹 탈퇴

어떤 멤버 MH_u가 그룹에서 탈퇴하는 경우 forward secrecy를 위해 MH_u가 알고있는 모든 키의 정보를 갱신해야 한다. 따라서 MH_u가 속한 셀 그룹의 관리자 CGM_i는 OFT의 그룹 탈퇴 프로토콜에 따라 키를 갱신하고 남아있는 모든 멤버들에게 안전하게 전달한다.

만일 CGM_i의 셀 그룹내의 이동호스트 MH_u의 그룹 탈퇴로 인해 셀 그룹에 더 이상 멤버가 존재하지 않게 되는 경우 CGM_i 는 제어그룹에 참여할 필요가 없으며, 따라서 CGM_i는 상부 제어그룹에 대한 탈퇴를 수행한다. 이 때, 제어그룹은 TGDH의 멤버 탈퇴 프로토콜에 의해 제어그룹키를 갱신한다.

4.4 Hand-over시 키 설정

이동네트워크의 주된 특징은 호스트의 이동성(mobility)이며, 어느 셀 에서 다른 셀로의 호스트의 이동은 셀 수준(Cell level)에서, 이전의 셀 그룹에 대해서는 해당 셀 그룹의 탈퇴이며 새로 이전한 셀 그룹에 대해서는 새로운 셀 그룹의 참여가 수행되어야 한다. 현재 $Cell_i$에 속한 이동호스트 MH_u가 $Cell_j$로 이동하는 경우 CGM_i와 CGM_j간에 hand-over가 발생하며, $Cell_j$에서 안전한 그룹 통신을 위해 MH_u는 CGM_j와 공유되는 비밀키를 설정해야 한다.

이동호스트 MH_u는 다른 셀 그룹으로 이동하는 경우, 이전한 셀의 셀 그룹 관리자 CGM_j와 비밀키 K'_{MH_u}를 설정하게 된다. 기존의 그룹 멤버의 셀 그룹 변경으로 인하여 서비스 영역이 바뀌더라도 전체 그룹에 대한 멤버십의 변경은 발생하지 않으므로 인증과정은 생략될 수 있다. 대신에 새로운 키를 계산함에 있어서 이전의 셀 그룹에 대한 정보를 사용하도록 함으로써 이전의 셀 그룹으로부터 이동하는 정당한 멤버임을 확인하도록 한다. Protocol-3은 이러한 과정을 나타낸다. 이전해온 호스트 MH_u가 이전의 셀에서 인증된 멤버임을 확인하기 위해 이전의 셀 그룹에서의 키 정보를 이용한다. CGM_j가 CGM_i로부터 받은 h_i와 MH_u의 h_u가 일치하는 경우 MH_u와 CGM_j는 동일한 키 K'_{MH_u}를 계산할 수 있다.

CGM_j는 이 과정을 통해 계산된 키 K'_{MH_u}를 MH_u와 공유되는 비밀키로 하여 새로이 $Cell_j$의 셀 그룹키를 OFT 방식으로 갱신한다.

MH_u		CGM_j		CGM_i
임의의 난수값 r_u 선택 $h_u = hash(K_{MH_u} \| CK_i)$ $v_u = \alpha^{r_u} \bmod p$ $r_u \cdot h_u \bmod (p-1)$ 계산 $K'_{MH_u} = v_j^{r_u \cdot h_u}$ $= \alpha^{h_j \cdot r_u \cdot h_u} \pmod p$	v_u =====〉 v_j 〈=====	$h_j = hash(CK_j \| h_i)$ $v_j = \alpha^{h_j} \bmod p$ $K'_{MH_u} = v_u^{h_i \cdot h_j}$ $= \alpha^{r_u \cdot h_i \cdot h_j} \pmod p$	h_i 〈=====	$h_i = hash(K_{MH_i} \| CK_i)$

Protocol-3 Hand-over 과정에서 키 교환

V. 제안 구조의 분석

5.1 제안시스템의 성능 분석

본 논문에서 제안하는 그룹키 관리 구조는 그룹 멤버에 대한 관리를 각 셀 그룹으로 분할하여 전체 멤버의 관리에 대한 그룹 관리자의 작업을 각 셀 그룹 관리자들에게 분담함으로써 그룹 관리의 확장성을 제공하도록 한다.

셀 그룹 관리자 CGM의 수를 n_c, 각 셀 그룹에 속한 멤버의 수를 n_{h_i} 그리고 $N(N = n_c \times n_{h_i})$을 전체 그룹 멤버의 수라고 할 때, 만일 GM이 트리 기반의 중앙집중형 그룹키 관리 기법을 사용하여 모든 멤버를 직접 관리하는 경우, GM의 그룹키 갱신에 대한 비용은 $O(\log N)$이 되며 각 멤버의 키 갱신 비용도 $O(\log N)$이 되고 이동호스트의 이동으로 인해 셀 영역이 변경되더라도 그룹키의 갱신은 수행되지 않아도 된다. 그러나 GM의 시스템 오류로 인한 one-point failure가 문제가 발생할 수 있다.

만일 그룹키 계산을 모든 멤버들에게 분담하는 분산형 그룹키 관리기법을 적용할 경우 GM에 대한 one-point failure 문제는 해결할 수 있으나 이동 호스트들이 그룹키 갱신을 담당하기에는 계산상의 부담이 많이 든다. 그러므로 제어그룹의 키 관리를 분산형 키 관리 방식을 사용함으로써 키 관리 서버의 시스템 오류로 인한 "one-point failure" 문제를 지하도록 하고, 셀 그룹의 키 관리는 중앙 관리서버가 수행하도록 하여 이동호스트의 키 관리 부담을 줄이도록 한다. 본 논문에서는 분산형 그룹키 관리 기법으로 TGDH기법을 가정하였고 셀 그룹의 관리기법으로 중앙집중형 그룹키 관리 기법인 OFT기법을 가정하였다.

〔표 1〕은 제안 시스템의 그룹키 관리에 대한 계산

〔표 1〕 제안 구조의 키 관리비용

키 저장 공간	
관리개체	멤버
$2n_{h_i} \cdot \|K_O\| + \log n_c \cdot \|K_T\|$	$2\log_2 n_{h_i} \cdot \|K_O\|$
키 갱신 계산량	
관리개체	멤버(min, max)
$O(\log n_{h_i})_{OFT} + (O(\log n_c)_{TGDH})$	$1, (\log n_{h_i})_{OFT}$

상의 비용과 키 저장 공간에 대한 비용을 보여준다. $|K_O|$는 셀 그룹의 OFT의 키 크기이며 $|K_T|$는 제어그룹의 TGDH의 키 크기이다. 키 갱신과 관련된 계산은 OFT의 일방향함수로 MD5나 SHA-1과 같은 암호학적인 해쉬함수를 사용할 수 있으며, TGDH의 경우 큰 소수 p에 대한 법-지수(modulo-exponentiation) 연산으로 인해 계산량이 많을 수 있으나, TGDH는 제어그룹의 키 관리 기법이며 셀 그룹 관리자의 수는 전체 멤버의 수에 비해 상대적으로 적으며 제어그룹의 갱신은 셀 그룹에 더 이상 멤버가 존재하지 않을 때 발생하므로 빈번하게 발생하지 않을 것이다.

그리고 이동호스트들의 관리는 셀 그룹에서 이루어지므로 이동호스트들이 셀 그룹키 갱신을 위해 필요한 연산은 OFT에 대한 해시함수의 연산만 수행하게 된다.

모든 멤버들이 각각의 셀 그룹에 균일하게 분포되어 있는 경우, 즉 $n_{h_i} \approx N/n_c$이라면, 각 CGM_i의 관리상의 부담이 동등할 것이다. 그러나 특정 셀 그룹으로 멤버들이 편중되어 있는 경우 해당 CGM_i의 다른 CGM_j에 비해 그룹관리에 대한 부담이 더 많이 들 것이다.

TGDH는 비슷한 유형의 그룹키 관리 기법들 중에서[1] 계산상의 효율성(computation efficiency)을 증대시킨 기법이며, 만일 통신상의 효율성(com-

〔표 2〕 제안 구조와 B·R 구조의 비교

	B·R의 구조		제안 구조	
키 관리	제어그룹	셀 그룹	제어그룹	셀 그룹
	키 서버	키 서버	분산형	키 서버
인증/키교환	공개키 기반 전자서명		ICPK 사용	
one-point failure	전체 발생가능		셀 그룹에서 발생가능	
멤버십 변경	셀 그룹만 영향		셀 그룹만 영향	

munication efficiency)을 중요시한다면 제어그룹의 그룹키 관리기법으로 〔6〕에서 제안한 그룹키 관리기법을 채택할 수 있을 것이다.

본 논문에서 제안된 ICPK를 사용한 멤버의 인증은 PKI기반의 인증서의 교환과 검증에 대한 계산과 대역폭을 줄일 수 있다. 그룹 관리자와의 초기인증을 통한 ICPK의 안전한 분배를 위해 전자서명에 대한 인증서의 교환이 발생할 수 있으나, 그룹관리자와의 인증은 멤버의 참여시 단 한번만 수행되며 이후의 셀 그룹의 참여로 인한 이동호스트의 셀 그룹관리자에 대한 인증과 키 설정에서는 ICPK를 사용하므로 인증서의 교환이나 별도의 안전한 통신 채널을 가정하지 않는다.

그룹 내에서의 인증과 키 설정을 위한 ICPK의 개념은 기본적으로 ElGamal 서명기법을 근간으로 하고 있으며, 키 설정시 연산을 줄이기 위해 SDSS 서명기법을 변형하여 기존의 ICPK를 사용한 키 계산에서 법-역원(modulo-inverse) 연산을 제거하였다.

유사한 연구 결과로써 Bruschi와 Rosti는 무선 이동네트워크 환경에서의 안전한 그룹통신에 대한 연구를 수행하였다.[3] 〔표 2〕에서는 실제 운영방안에서의 B·R의 구조와 제안구조를 비교 요약하여 나타내었다. B·R의 구조에서는 멤버의 인증과 키 교환을 공개키 기반의 인증서의 교환과 전자서명을 사용하였으며, 제어그룹과 셀 그룹의 키 관리를 〔11〕에서 제안한 그룹키 관리 방식을 채택하였다. B·R의 구조와 제안구조는 전체 그룹을 셀 그룹으로 분할함으로써 그룹키 관리에 대한 확장성을 고려하였다.

5.2 제안시스템의 안전성 분석

그룹키 관리에서 주요 보안 요구사항은 멤버의 가입과 탈퇴에 대한 forward secrecy와 backward secrecy이며, 제안 시스템에 대한 forward secrecy와 backward secrecy는 제어그룹과 셀 그룹에서 사용하는 TGDH와 OFT에서 사용되는 블라인드 키의 특성을 따르게 되며 각각의 기법에 대한 안전성은 〔7〕과 〔2〕에서 상세히 분석되어있다. 실제 TGDH 방식의 안전성의 근간은 Decision Diffie-Hellman 알고리즘에 의존하며 OFT 방식은 키 일치를 위해 사용되는 일방향 함수의 안전성에 의존한다.

〔2〕에서 OFT 단말 노드에 대한 멤버의 비밀키는 IKE를 통해 안전하게 설정되었으나 본 논문에서는 인증서의 교환으로 인한 대역폭의 소모와 전자서명 검증에 대한 이동호스트의 계산을 줄이기 위해 ICPK의 교환을 통해 멤버의 인증과 키 설정을 수행한다. 각 멤버의 ICPK의 생성은 GM이 담당하며 GM은 신뢰되는 개체로 간주한다. 멤버 가입시 초기의 안전한 키 설정을 위해 ICPK의 분배는 멤버의 초기 인증시에만 인증서를 사용한 안전한 통신 채널을 통해 이루어진다. 또한 본 논문에서 사용된 ICPK는 변형된 SDSS 서명기법을 근간으로 하고 있으며, 사용된 SDSS의 안전성은 이산대수 문제[10]와 해쉬함수의 안전성에 의존하게 된다.

악의적인 공격자가 셀 그룹키를 계산하기 위해서는 OFT 키 트리상에서 사용되는 블라인드 키를 알아야 하며, 블라인드 키들은 멤버 참여시 사용자와 셀 그룹 관리자간에 설정된 비밀키로 암호화되어 전달된다. 멤버의 셀 그룹 참여시 키 설정을 통해 생성된 셀 그룹 관리자와 사용자간의 비밀키에서, $\alpha^{K_u \cdot S_u \cdot r_i} = ((P_u)^{r_i})^{S_u} \pmod{p}$와 $\alpha^{K_i \cdot S_i \cdot r_u} = (\alpha^{KH(ID_i, P_i)} \cdot y)^{r_u} \pmod{p}$를 계산하기 위해 악의적인 공격자는 멤버의 비밀 난수값 r_u와 비밀값 $S_u = K_u^{-1} \cdot (KH(ID_u, P_u) + x) \pmod{p-1}$를 계산할 수 있어야 한다. 악의적인 공격자가 r_u를 계산하는 것은 Diffie-Hellman 문제와 이산대수 문제에 의해 계산상 어려우므로, 그룹 관리자 GM의 비밀값 x를 계산하는 것도 역시 이산대수 문제로 인해 계산상 어려우며 x값을 모르면서 S_u를 계산할 수 없고 x값을 임의적으로 선택해야 할 것이며, 이 값을 임의로 선택할 확률은 $1/2^{|p|}$이 된다.

Hand-over과정에서, 호스트가 다른 셀 그룹으로 이동하더라도 전체 그룹에 대한 멤버십은 변경되지 않으므로 이전한 새로운 셀 그룹 관리자와 인증과정을 수행하는 대신에 공유키를 계산함에 있어서 이전의 셀 그룹에 대한 키 정보를 이용한다. 즉, MH_u가 이전에 속해있던 셀 그룹의 키 정보를 이용

함으로써 부당한 사용자가 새로운 셀 그룹에 참여하지 못하도록 한다. 그러나 새로운 키를 계산함에 있어서 이전의 셀 그룹키의 정보를 이용하더라도 셀 그룹키 자체가 알려져서는 안된다. Protocol-3에서 암호학적 해쉬함수의 성질에 의해 셀 그룹 관리자 CGM_i가 CGM_j 에게 제공하는 정보를 통해 $Cell_i$의 셀 그룹키를 계산하는 것은 어려우므로 셀 그룹키의 누출을 방지할 수 있다. 그리고 이전의 셀 그룹 관리자 CGM_i는 이동호스트 MH_u와 CGM_j간에 계산된 키를 계산할 수 없다.

Ⅵ. 결론 및 향후과제

본 논문에서는 이동네트워크 환경에서 안전한 그룹통신을 위한 그룹키 관리구조를 제안하였다. 이동호스트의 이동성은 그룹의 동적인 특성을 증대시키므로 호스트의 이동성에 대해 효율적이며 확장성을 제공하는 그룹키 관리가 이루어져야 한다. 본 논문에서 제안하는 그룹키 관리구조는 이동호스트들로 구성되는 셀 그룹과 셀 그룹관리 개체들로 구성되는 제어그룹으로 구분하며, 각 셀 그룹을 셀 그룹관리자들이 독자적으로 관리함으로써 멤버십의 변경으로 인한 그룹키 관리의 영향을 지역적으로 한정시킨다. 제어그룹의 키 관리는 분산형 방식을 사용함으로써 특정 관리개체의 오류로 인한 one-point failure 문제를 해결하고자 하였으며, 분산형 그룹키 관리기법인 TGDH를 가정하였다. 그리고 멤버의 인증을 위해 ICPK를 사용하여 이동호스트의 인증과 키 설정 프로토콜을 수행하므로 인증서 기반의 프로토콜보다 효율적으로 인증과 키 교환을 수행할 수 있다.

본 논문에서는 호스트가 이동할 때마다 각 셀 그룹의 수준에서 멤버의 탈퇴와 가입에 대한 키 갱신을 가정한다. 그러나 이동네트워크에서 호스트들은 계속적으로 이동하며 호스트가 이동할 때마다 셀 그룹의 키 갱신이 매우 빈번하게 발생할 수 있다. 이러한 경우 어떤 멤버의 멤버십이 변경될 때마다 그룹키를 갱신하지 않고 일정한 키 갱신 주기(rekeying period) 동안 변경되는 멤버십에 대해 한꺼번에 처리하는 일괄적인 키 갱신(Batch rekeying)[15]을 사용함으로써 효율성을 증대시킬 수 있다. 그러나 일괄적 키 갱신의 경우 키 갱신 주기가 길어질 경우 시스템의 효율성은 증대하지만 탈퇴한 멤버가 키 갱신 주기가 만료되기 전까지는 계속적으로 그룹 데이터에 접근할 수 있는 backward secrecy의 취약성이 발생하므로 안전성과 효율성 관점의 trade-off에 대한 연구가 계속되어야 할 것이다. 한편 제안구조에서는 다른 셀 그룹으로의 데이터 전송을 위해 셀 그룹 관리자의 데이터 트래픽에 대한 복호화와 재암호화 과정으로 인한 데이터 전송에 복잡성이 발생하므로 이에 대한 방안에 대해서도 추후 보완되어야 할 것으로 판단된다.

참 고 문 헌

[1] G. Ateniese, M. Steiner, G. Tsudik, Authenticated group key agreement and friends. In ACM CCS 98′, pp. 17~26, November, 1998.

[2] D. Balenson, D. McGrew, A. Sherman. Key management for large dynamic groups: One-way function trees and amortized initialization. Internet-Draft: draft-balen-songroupkeymgmt-oft-00.txt, Febrary, 1999.

[3] D. Bruschi, E. Rosti, Secure multicast in wireless networks of mobile hosts: protocols and issues, to appear in ACM-Balzer MONET Journal, Special issue on Multipoint Communication in Wireless Mobile Networks, 2000.

[4] C. G. Günther, An identity-based Key Exchange Protocol. Lecture Notes in Computer Science 434, Advances in Cryptology, EUROCRYPT89, pp. 29~37, 1989.

[5] D. Harkins, D. Carrel, The Internet Key Exchange(IKE), IETF, RFC 2409, November, 1998.

[6] Y. Kim. A. Perrig and G. Tsudik Communication-Efficient Group Key Agreement, International Federation for Information Processing, IFIP-SEC 2001, June 2001.

[7] Y. Kim, A. Perrig, G. Tsudik. Simple and fault-tolerant key agreement for dynamic collaborative groups. Proceedings of the 7th ACM conference on Computer and communications security, pp. 235~244, November, 2000.

[8] S. Mittra, Iolus: A Framework for Scalable

Secure Multicasting, Proceedings ACM SIGCOM, pp. 277~288, 1997.
[9] A. Perrig. Efficient collaborative key management protocols for secure autonomous group communication. International Workshop on Cryptographic Techniques and E-Commerce CrypTEC '99. pp. 192~202, 1999.
[10] A. J. Menezes, P. C.van Oorschot, S. A. Vanstone, Handbook of applied cryptography, CRC press, 1997.
[11] M. Waldvogel, G. Caronni, D. Sun, N. Weiler, and B. Plattner, The VersaKey Framework: Versatile Group Key Management. Selected Areas in Communications, IEEE Journal on, Volume: 17 Issue: 9, pp. 1614~1631, Sept. 1999.
[12] D. Wallner, E. Harder, R. Agee, Key management for multicast: issues and architecture, RFC2627, June, 1999.
[13] C. K. Wong, M. Gouda, S. S Lam. Secure group communications using key graphs. In Proceedings of ACM SIGCOMM '98, pp. 68~79, September 1998.
[14] Y. Zheng. Shortened Digital Signature, Signcryption and Compact and Unforgeable Key Agreement Schemes, Submission to IEEE P1363a: Standard Specifications for Public-Key Cryptography, August 1998.
[15] Xiaozhou Steve Li, Yang Richard Yang, Mohamed G. Gouda, Simon S. Lam, Batch rekeying for secure group communications, The tenth international World Wide Web conference on World Wide Web, ACM, pp. 525~534, April 2001.

〈著者紹介〉

박 영 호 (Young-Ho Park) 학생회원
2000년 2월 : 부경대학교 전자계산학과 졸업
2002년 2월 : 부경대학교 전자계산학과 석사
2002년 3월~현재 : 부경대학교 정보보호 박사과정
〈관심분야〉 네트워크보안, 그룹키 관리, 이동네트워크

이 경 현 (Kyung-Hyune Rhee) 정회원
1982년 2월 : 경북대학교 수학교육과 졸업
1985년 2월 : 한국과학기술원 응용수학과 석사
1992년 8월 : 한국과학기술원 수학과 박사
1985년 2월~1993년 2월 : 한국전자통신연구소 연구원, 선임연구원
1993년 3월~현재 : 부경대학교 전자컴퓨터정보통신공학부 전임, 조교수, 부교수
〈관심분야〉 암호이론, 암호프로토콜, 네트워크보안, 이동네트워크, 그룹키 관리