서로 다른 셀의 모바일 장치간의 그룹키 동의 프로토콜

(Group Key Agreement for Mobile Devices in Different Cells)

김 지 연 † 최 연 이 †† 김 승 주 ††† 원 동 호 †††
(Jeeyeon Kim) (Yeonyi Choi) (Seungjoo Kim) (Dongho Won)

요 약 모바일 장치의 사용이 대중화되면서 무선 통신을 이용한 화상회의, 다중 사용자 게임, 인터랙티브 채팅 등의 그룹 기반의 어플리케이션에 대한 관심이 증가되고 있다. 이러한 그룹 기반의 어플리케이션이 안전하게 수행되기 위해서는 그룹 구성원간 안전한 통신을 위한 키 동의가 선행되어야 한다. 기존에 제안된 모바일 환경에서의 그룹키 동의 프로토콜에서는 하나의 셀 내의 모바일 장치들이 그룹키를 공유하는 것을 고려하였다. 본 논문에서는 기존 모델을 확장하여 최초로 서로 다른 셀에 속한 모바일 장치들 간의 그룹키 동의 프로토콜을 제안하고 안전성을 분석하도록 한다. 또한 모바일 장치의 계산 부담을 줄이기 위해 패스워드 인증 방식을 제안한 프로토콜에 적용해 보도록 한다.

키워드 : 그룹키 동의 프로토콜, 모바일 장치

Abstract Mobile communication has become more pervasive and it is considered as one of main concerns of conferencing, multi-user games and etc. in mobile environment. These applications need to secure communication in group. Most of the published protocols are based on model which consists of a stationary base station and a cluster of mobile devices. In this paper, we have focused on the extended model of which participants are several base stations and mobile devices in different cells. We present a new group key protocol among mobile devices in different cells and analyze its security. And we also look at how password authentication can be used to our group key agreement protocol. The mobile device's computing load may be reduced by using password authentication.

Key words : Group key agreement, Mobile devices

1. 서 론

IP 텔레포니(IP telephony), 화상회의, 다중 사용자 게임, 인터랙티브 채팅 등의 그룹 기반의 어플리케이션에 대한 관심이 증가하면서 그룹 기반의 보안 메커니즘 개발의 필요성이 대두되고 있다. 이러한 그룹 기반의 보안 메커니즘이 제대로 동작하기 위해서는 그룹 구성원간의 안전한 통신을 위한 키 동의가 선행되어야 한다. 그룹키 동의 프로토콜은 그룹 구성원에게 공개된 네트워크를 통해 그룹키(또는 세션키)를 공유하게 함으로써 그룹 내에서의 안전한 멀티캐스트 통신을 가능하게 하는 프로토콜이다.

통신하는 객체들 사이에 공통의 키를 공유하는 프로토콜은 키 생성을 누가 하느냐에 따라 키 전송 프로토콜과 키 동의 프로토콜로 분류할 수 있다. 키 전송 프로토콜이란, 세션키를 공유하고자 하는 객체들 중 어느 한 객체가 임의로 세션키를 선택한 후 다른 객체에게 안전하게 전송하는 방식이다. 키 전송 프로토콜은 한 객체의 임의대로 키를 생성하기 때문에 키를 전송받는 객체의 입장에서는 공정하다고 할 수 없다. 반면, 키 동의 프로토콜에서는 키 생성에 참여하는 어떠한 객체도 미리 그룹키를 결정할 수 없고 모든 객체의 합의 즉, 비밀정보를 이용하여 키를 생성하는 contributory의 특성을 갖는다.

1982년에 Ingemarsson과 Tang과 Wong이 그룹키 동의 프로토콜을 최초로 제안한 이래, 많은 그룹키 동의 프로토콜이 제안되었다[1-6]. 그러한 대부분의 그룹키 동의 프로토콜은 양자간의 Diffie-Hellman(DH) 키 동

· 본 연구는 정보통신부 정보통신연구진흥원의 대학 IT연구센터 지원 사업의 연구결과로 수행되었음
† 정 회 원 : 성균관대학교 전기전자및컴퓨터공학과
jykim@kisa.or.kr
†† 정 회 원 : 신성대학 컴퓨터정보계열 교수
yychoi@shinsung.ac.kr
††† 종신회원 : 성균관대학교 정보통신공학부 정보보호연구소 교수
skim@security.re.kr
dhwon@security.re.kr
논문접수 : 2005년 3월 15일
심사완료 : 2005년 8월 10일

의 프로토콜을 그룹으로 확장한 형태를 갖는다.

최근에 모바일 장치의 사용이 대중화되면서 무선 통신에 적합한 그룹키 공유 프로토콜에 대한 연구도 활발히 진행되고 있다[4-6].

2003년에 Bresson 등은 저전력 모바일 장치에 적합한 그룹키 동의 프로토콜을 제안하고 제안한 프로토콜이 계산적 DH 가정하의 랜덤오라클 모델에서 안전함을 증명하였다[4]. 그러나 2005년 Nam 등은 BressonChevassut-Essiari-Pointcheval 프로토콜의 초기 설정(GKE.Setup) 프로토콜이 능동적 공격자에게 취약하여 키 인증(key authentication), 순방향 안전성(forward secrecy) 및 세션키 노출에의 안전성(known-key secrecy)의 보안 요구사항을 만족하지 못함을 지적하면서 개선된 방식을 제안하였다[5]. 또한 Nam 등은 모바일 환경에 적합한 그룹키 동의 프로토콜을 제안하였고, 제안한 프로토콜이 결정적 DH 가정하의 랜덤오라클 모델에서 순방향 안전성을 만족하고 능동적 공격자에 안전함을 증명하였다[6].

지금까지 제안되었던 프로토콜에서는 단일 셀 내에서의 그룹키 동의 프로토콜로 하나의 무선 게이트웨이(서버 또는 기지국)와 여러 개의 모바일 장치들 간의 그룹키를 공유하는 모델만을 고려하였다. 여기서 셀이란 모바일 장치가 기지국의 메시지를 직접적으로 수신할 수 있는 지역을 말한다.

본 논문에서는 기존 모델을 확장하여 최초로 서로 다른 셀에 속하는 모바일 장치들 간의 그룹키 동의 프로토콜을 제안하고 그 안전성을 분석하도록 한다. 제안하는 모델은 기존 모델에 비해 보다 현실적인 시나리오를 고려하였다고 할 수 있다. 그림 1은 제안하는 모델이 기존 모델의 확장된 형태임을 보여준다.

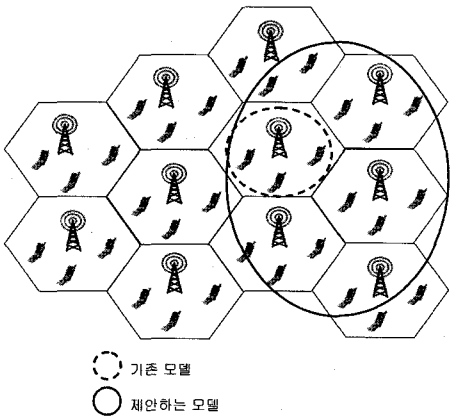

그림 1 기존 모델과 제안 모델간의 비교

다음의 시나리오를 생각해 보자.

휴대폰과 같은 모바일 장치($U_1^{(1)}$)를 가진 사용자 A가 무선통신을 이용하여 사용자 B, C, D, E, F에게 파일을 전송한다고 하자. 사용자 A, B, C, D, E, F는 동일한 회사의 직원이며, B, C, D, E, F 역시, A와 마찬가지로 모바일 장치를 이용하여 파일을 수신한다. B는 모바일 장치 $U_2^{(1)}$를 C는 모바일 장치 $U_1^{(2)}$를 D는 모바일 장치 $U_1^{(3)}$를 E는 모바일 장치 $U_1^{(4)}$를 D는 모바일 장치 $U_2^{(4)}$를 각각 가지고 있다. 여기에서 B는 A와 같은 셀 내에 존재(즉, A와 B의 모바일 장치인 $U_1^{(1)}$과 $U_2^{(1)}$는 기지국 B_1에 연결됨)하며, C와 D와 E와 F는 A와는 다른 셀 내에 존재(즉, C의 모바일 장치 $U_1^{(2)}$는 기지국 B_2에 연결되어 있고 D의 모바일 장치 $U_1^{(3)}$는 기지국 B_3에 연결되어 있고, E와 F의 모바일 장치인 $U_1^{(4)}$과 $U_2^{(4)}$는 기지국 B_4에 연결되어 있음)하고 있다고 하자. 전송되는 파일은 회사 업무와 관련된 민감한 정보를 포함할 수 있으므로 B와 C와 D와 E와 F 이외의 사용자에게 노출되지 않아야 함으로 A, B, C, D, E, F로 구성된 그룹 내에 안전한 멀티캐스트 통신 채널이 구축되어야 한다. 이러한 안전한 멀티캐스트 통신 채널을 효율적으로 구축하기 위해서는 그룹키 동의 프로토콜의 수행이 필요하다. 그림 2는 이러한 시나리오를 보여준다.

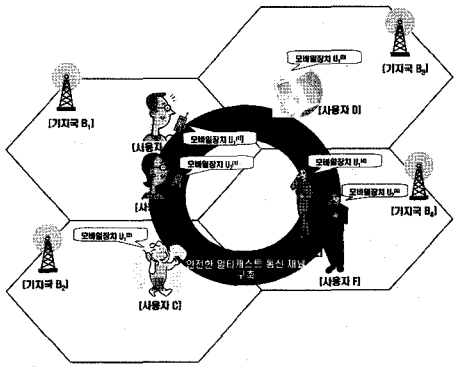

그림 2 제안하는 프로토콜에서 고려되는 시나리오

본 논문에서는 이러한 시나리오에 적합하도록 n개의 기지국($B_1, B_2, \cdots, B_n$) 각각에 연결된 m개의 모바일 장치 $[U_1^{(1)}, \cdots, U_m^{(1)}]$, $[U_1^{(2)}, \cdots, U_m^{(2)}], \cdots, [U_1^{(n)}, \cdots, U_m^{(n)}]$들 간의 그룹키 동의 프로토콜을 제안하였다. 또한 본 논문에서는 모바일 장치의 계산 부담을 줄일 수 있는 방안으로, 전자서명을 이용한 인증 방식 대신 널리 사용되고 있는 패스워드 인증 방식을 제안하는 그룹키 동의 프로토콜에 적용한 프로토콜도 제안하였다.

본 논문의 구성은 다음과 같다. 제 2장에서 서로 다른 셀의 모바일 장치간의 그룹키 동의 프로토콜의 요구조건을 설명하고 제 3장에서 기존의 단일 셀 내의 그룹키 동의 프로토콜을 제안하는 모델에 적용할 수 있는 방식

및 문제점을 간략히 살펴보고 서로 다른 셀에 속한 모바일 장치간의 그룹키 동의 프로토콜을 제안하고 그 안전성을 분석하도록 한다. 또한 제 4장에서는 패스워드 인증방식을 제안하는 그룹키 동의 프로토콜에 어떻게 적용할 수 있는 지를 간략히 살펴보도록 한다. 마지막으로 제 5장에서 결론에 대해 논의하도록 한다.

2. 서로 다른 셀의 모바일 장치간의 그룹키 동의 프로토콜의 요구조건

제안하는 프로토콜에서는 둘 이상의 기지국들과 각 기지국에 연결된 모바일 장치들 간의 그룹키 동의를 수행하는 모델을 고려한다. 프로토콜에서는 다음과 같은 통신 및 계산 능력 상의 제약 사항을 가정한다.

- **기지국을 통한 통신** : 모바일 장치는 자신이 속해진 기지국에 연결되어 있으며 자신이 속한 셀의 기지국을 통해서만 다른 셀에 속해 있는 모바일 장치와 통신할 수 있다.
- **계산능력의 비대칭성** : 모바일 컴퓨팅 기술은 프로토콜 참가자의 계산적인 능력 측면에서 비대칭적이다. 즉, 프로토콜 참가자는 충분한 계산 능력을 가진 고정된 기지국과 클라이언트라고 부르는 제한된 계산 능력과 메모리를 갖는 모바일 장치들로 구성된다. 그러므로 프로토콜 상에서의 복잡한 계산은 기지국이 수행하게 하도록 하여 모바일 장치의 계산 부담을 줄이도록 설계하여야 한다.
- **contributory 키동의** : 이렇게 제한된 계산 능력을 가진 모바일 장치에 물리적인 랜덤 소스를 제공한다는 것은 어렵기도 하지만 비용이 많이 든다. 그래서 일반적으로 모바일 장치에는 암호학적으로 안전하지 않은 랜덤 생성기가 제공되거나 제조 단계에서 임의의 랜덤 씨드가 탑재될 수도 있다[7]. 이러한 안전하지 않은 랜덤 생성기를 이용하여 암호학적으로 안전한 그룹키를 생성하기 위해, 프로토콜에 참여하는 어떠한 구성원도 미리 그룹키를 결정할 수 없도록 하고 모든 구성원의 비밀정보를 이용하여 그룹키를 생성하도록 하는 contributory 키동의 프로토콜 설계를 고려한다. 이러한 contributory 키동의 프로토콜은 n명의 구성원 중에서 최소 한명이 선택한 비밀정보의 랜덤성만 보장된다면 구성원들이 서로 공모하더라도 최종 그룹키의 값을 제어할 수 없는 특징을 갖는다.

3. 서로 다른 셀의 모바일 장치간의 그룹키 동의 프로토콜

새로운 그룹키 동의 프로토콜을 제안하기에 앞서 우선 단일 셀의 환경을 고려한 기존 그룹키 동의 프로토콜을 이용하여 서로 다른 셀의 모바일 장치간의 그룹키 동의 프로토콜을 손쉽게 설계할 수 있는 방안을 살펴보도록 한다. 이러한 방안으로 다음과 같은 두 가지가 있을 수 있다.

방식 1

각 기지국($B_j, 1 \le j \le n$)은 자신의 셀 내의 모바일 장치들과 그룹키 동의 프로토콜을 통해 셀 그룹키(K_j 임의의 한 셀 내에 공유된 그룹키)를 생성한다. 그리고 난 후, 셀 그룹키를 다른 기지국의 공개키로 암호화하여 전송한다. 암호문을 수신한 기지국은 암호문을 복호화하여 다른 셀 그룹키를 얻고, 해쉬 함수 등을 이용하여 최종적인 그룹키($K = H(K_1, \cdots, K_n)$)를 생성한다. 그리고 기지국의 자신 셀 내의 모바일 장치들에게 최종 그룹키를 자신의 셀 그룹키로 암호화한 암호문 ($E_{K_j}(K)$)을 전송한다. 모바일 장치들은 셀 그룹키를 이용하여 암호문을 복호화하여 최종 그룹키를 획득한다.

방식 1의 경우, 기지국의 공개키가 노출되면 공격자가 이전의 그룹키를 계산할 수 있으므로 순방향 안전성을 제공하지 못하는 문제가 있다. 그리고 악의 있는 기지국이 그룹키의 암호문 $E_{K_j(K)}$ 대신 임의의 랜덤값(R)의 암호문 $E_{K_j(R)}$을 전송했을 경우, 모바일 장치는 이에 대해 확인할 방법이 없으므로 묵시적 키인증을 제공하지 못한다.

방식 2

각 기지국($B_j, 1 \le j \le n$)은 자신의 셀 내의 모바일 장치들과 그룹키 동의 프로토콜을 통해 셀 그룹키(K_j)를 생성한다. 그리고 난 후, 기지국들은 그룹키 동의 프로토콜을 통해 기지국들간의 그룹키(BK)를 생성한 후, 기지국들간의 그룹키를 이용하여 셀 그룹키를 암호화한 암호문($E_{BK}(K_j)$)을 생성하여 다른 기지국들에게 전송한다. 암호문을 수신한 기지국은 암호문을 복호화하여 다른 셀 그룹키를 얻고, 해쉬 함수 등을 이용하여 최종적인 그룹키($K = H(K_1, \cdots, K_n)$)를 생성한다. 그리고 기지국의 자신 셀 내의 모바일 장치들에게 최종 그룹키를 자신의 셀 그룹키로 암호화한 암호문($E_{K_j}(K)$)을 전송한다. 모바일 장치들은 셀 그룹키를 이용하여 암호문을 복호화하여 최종 그룹키를 획득한다.

방식 2의 경우, 순방향 안전성을 제공하나 방식 1과 마찬가지로 묵시적 키인증을 제공하지 못한다. 그리고 통신이 발생되는 매 세션마다 기지국들 간의 그룹키 동의 프로토콜이 부가적으로 수행되어야 하므로 비효율적이다.

이제, 묵시적 키인증, 순방향 안전성 및 세션키 노출에의 안전성을 만족하는 contributory 그룹키 동의 프로토콜을 제안하도록 한다.

3.1 프로토콜 초기화

프로토콜 수행을 위한 준비 단계는 다음과 같다.

- 각 클라이언트(모바일 장치) $U_i^{(j)}(1 \le i \le m)$는 자신이 속한 셀의 기지국 $B_j(1 \le j \le n)$에 연결되어 있다.
- 각 모바일 장치와 기지국들은 전자서명을 위한 공개키/개인키 쌍을 가지고 있다.

- p와 q와 g는 프로토콜에 참여하는 모든 객체에게 공개되며 공통으로 사용된다. 지수에서의 연산을 제외한 모든 계산은 mod p상에 이루어진다. p와 q는 소수이며 $p=2q+1$이다. g는 위수가 q인 Z_p^*상의 부그룹 G의 생성기이다.
- 모바일 장치와 기지국은 그룹키 동의 프로토콜 수행 시 안전한 일방향 해쉬 함수 H와 안전한 대칭키 암호알고리즘 E 및 선택암호문공격에 안전한 전자서명 알고리즘을 사용한다.

3.2 프로토콜 설명

서로 다른 셀의 모바일 장치간의 그룹키 동의 프로토콜은 다음과 같이 수행된다.

1) ① 각 모바일 장치 $U_i^{(j)}(1 \le i \le m)$는 랜덤하게 $r_{U_i^{(j)}} \in Z_q$를 선택하고 $z_{U_i^{(j)}} = g^{r_{U_i^{(j)}}}$를 계산한다. 자신이 속한 셀의 기지국 B_j에게 $m_{U_i^{(j)}} = (U_i^{(j)}, z_{U_i^{(j)}})$와 $\sigma_{U_i^{(j)}}$을 전송한다. $\sigma_{U_i^{(j)}}$는 메시지 $m_{U_i^{(j)}}$에 대한 서명문이다.

   ② 다른 기지국 $B_k(\neq B_j)(1 \le k \le n)$ 또한 랜덤하게 $r_{B_k^{(j)}} \in Z_q$를 선택하고 $z_{B_k^{(j)}} = g^{r_{B_k^{(j)}}}$를 계산한다. 그리고 난 후 기지국 B_j에게 $m_{B_k^{(j)}} = (B_k, z_{B_k^{(j)}})$와 $\sigma_{B_k^{(j)}}$를 전송한다. $\sigma_{B_k^{(j)}}$는 메시지 $m_{B_k^{(j)}}$에 대한 서명문이다.

2) 기지국 B_j는 자신이 수신한 서명 $\sigma_{U_i^{(j)}}$와 $\sigma_{B_k^{(j)}}$을 검증한 후 랜덤하게 $r_j, r_{Bj^{(j)}} \in Z_q$를 선택하고 $z_j = g^{r_j}$와 $K=j=(\prod_{i=1}^{m} z_{U_i^{(j)}} \times \prod_{k=1}^{n} z_{B_k^{(j)}})^{r_j} = g^{r_j(\Sigma_{i=1}^{m} r_{U_i^{(j)}} + \Sigma_{k=1}^{n} r_{B_k^{(j)}})}$를 계산한다. 그리고 난 후, B_j는 (m_{Bj}, σ_{Bj})를 자신에게 연결된 모바일 장치와 다른 기지국에게 브로드캐스트한다. σ_{Bj}는 (B_j, K_j)의 서명문이다.

$$m_{Bj} = (B_j, z_j, X^{(j)}, Y^{(j)})$$

$$X^{(j)} = x_l^{(j)} | 1 \le l \le m,\ Y^{(j)} = y_l^{(j)} | 1 \le l \le n$$

$$x_l^{(j)} = \left(\frac{\prod_{i=1}^{m} g^{r_{U_i^{(j)}}} \times \prod_{k=1}^{n} g^{r_{B_k^{(j)}}}}{g^{r_{U_l^{(j)}}}}\right)^{r_j},\ y_l^{(j)} = \left(\frac{\prod_{i=1}^{m} g^{r_{U_i^{(j)}}} \times \prod_{k=1}^{n} g^{r_{B_k^{(j)}}}}{g^{r_{B_l^{(j)}}}}\right)^{r_j}$$

3) ① 브로드캐스트 된 메시지를 수신한 각 모바일 장치 $U_i^{(j)}(1 \le i \le m)$는 $K=j=x_i^{(j)} \times z_j^{r_{U_i^{(j)}}}$를 계산한 후, 서명 σ_{Bj}을 검증한다.

   ② 다른 기지국 $B_k(\neq B_j)(1 \le k \le n)$도 마찬가지로 $K=j=y_k^{(j)} \times z_j^{r_{B_k^{(j)}}}$를 계산한 후, 서명 σ_{Bj}을 검증한다. 그리고 자신에게 연결된 모바일 장치 $U_i^{(k)}(1 \le i \le m')$에게 $E_{K_k(K_j | 1 \le j \ne k \le n)}$와 서명 σ_{Bj}를 브로드캐스트 한다.

4) 최종적으로 각 셀의 모든 모바일 장치들은 $E_{K_k(K_j | 1 \le j \ne k \le n)}$를 복호화하여 K_j를 획득한다. 그리고 서명 σ_{Bj}의 검증을 통해 K_j의 무결성을 확인한 후, 그룹키 $K=H(K_1, K_2, \cdots, K_n)$를 계산한다.

그림 2는 기지국 B_1에 속해있는 모바일 장치 $U_1^{(1)}$과 $U_2^{(1)}$와 기지국 B_2에 속해있는 모바일 장치 $U_1^{(2)}$과 $U_2^{(2)}$들 간의 그룹키 공유 프로토콜의 예를 보여준다. 그림 2에서 실선은 기지국 B_1이 셀 그룹키 K_1을 생성할 때의 메시지 흐름이며, 점선은 기지국 B_2가 셀 그룹키 K_2을 생성할 때의 메시지 흐름이다.

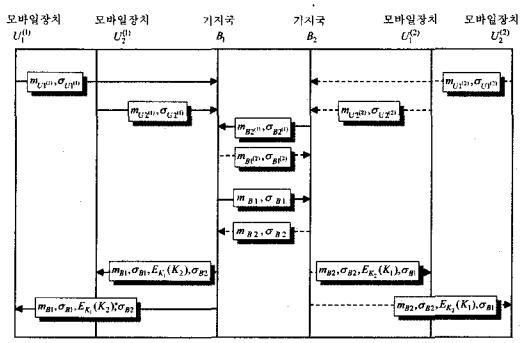

그림 3 서로 다른 두 기지국 B_1과 B_2에 속해있는 모바일 장치들 $U_1^{(1)}, U_2^{(1)}, U_1^{(2)}, U_2^{(2)}$ 간의 그룹키 동의 프로토콜의 예

3.3 안전성 분석

본 절에서는 제안한 프로토콜이 묵시적 키인증과 순방향 안전성 및 세션키 노출에의 안전성을 만족함을 보이도록 한다.

제안하는 프로토콜의 안전성은 사용된 대칭키 암호알고리즘의 안전성과 전자서명알고리즘의 안전성과 CDH (Computational Diffie-Hellman) 문제의 어려움에 근거한다. CDH 문제란, g^a와 g^b가 주어졌을 때 g^{ab}를 계산하는 문제이다.

- 제안한 프로토콜은 contributory 그룹키 동의 프로토콜이다.
  - 프로토콜 수행 후 생성된 그룹키 $K=H(K_1, K_2, \cdots, K_n)$ $(K_j = g^{r_j(\Sigma_{i=1}^{m} r_{U_i^{(j)}} + \Sigma_{k=1}^{n} r_{B_k^{(j)}})})$의 형태를 살펴보면, 프로토콜의 모든 구성원이 선택한 랜덤값 $r_{U_i^{(j)}}$와 $r_{B_k^{(j)}}$와 r_j이 이용되고 있으므로 제안한 프로토콜이 contributory 그룹키 동의 프로토콜임을 쉽게 알 수 있다.
- 제안한 프로토콜은 묵시적 키인증을 제공한다. 묵시적 키인증이란, 프로토콜에 참여한 자만이 해당 그룹키 값을 알고 있음을 보장한다.
  - 프로토콜 수행후 수동적 공격자는 $[(U_i^{(j)}, g^{r_{U_i^{(j)}}}, \sigma_{U_i^{(j)}}), (B_k, g^{r_{B_k^{(j)}}}, \sigma_{B_k^{(j)}}), (B_j, g^{r_j}, X^{(j)}, Y^{(j)}, \sigma_{Bj}), (1 \le i \le m, 1 \le j \ne k \le n)$ 및 $E_{K_k}(K_j | 1 \le j \ne k \le n)]$의 정보를 얻을

수 있다. 공격자가 자신이 획득한 정보로부터 그룹키 K를 계산하기 위해서는, ① $g^{r_i U^{(j)}}$와 $g^{r_B B^{(j)}}$와 g^{r_j}로부터 K_j를계산하거나 ② $E_{K_k}(K_{j1 \le j \ne k \le n})$를 복호화 하여야 한다. ①의 경우, $g^{(\Sigma_{i=1}^{m} r_i U_i^{(j)} + \Sigma_{k=1}^{n} r_B B^{(j)})}$와 g^{r_j}가 주어졌을 때 $K_j = g^{r_j(\Sigma_{i=1}^{m} r_i U_i^{(j)} + \Sigma_{k=1}^{n} r_B B^{(j)})}$를 계산하는 것은 CDH 문제이므로 공격자가 키 K_j를 계산하는 것은 암호학적으로 불가능하다. ②의 경우는 기존의 안전한 대칭키 암호알고리즘의 사용을 가정하였기 때문에 공격자가 $E_{K_k}(K_{j1 \le j \ne k \le n})$를 복호화하는 것 역시 암호학적으로 불가능하다.

- 전송되는 메시지를 변조하거나 새로운 메시지를 삽입할 수 있는 능동적 공격자는 모바일 장치 또는 기지국인척 하고 프로토콜에 참여할 수 있다. 그러나 이렇게 하기 위해서 공격자는 자신이 그룹 구성원임을 증명할 수 있는 정당한 전자서명을 생성하여야 한다. 그러나, 선택암호문공격에 안전한 전자서명 알고리즘의 사용을 가정했으므로 이 공격은 암호학적으로 불가능하다.
- 악의 있는 기지국 $B_k (1 \le j \ne k \le n)$이 $E_{K_i}(K_{j1 \le j \ne k \le n})$의 K_j를 임의의 랜덤값으로 바꾸기 위해서는 랜덤값에 대한 정당한 서명을 생성하여야 한다. 그러나 선택암호문공격에 안전한 전자서명 알고리즘의 사용을 가정했으므로 이 공격은 암호학적으로 불가능하다.

• 제안한 프로토콜은 순방향 안전성을 제공한다. 순방향 안전성이란, 공격자가 프로토콜의 긴 주기(long-term) 키를 알더라도 이전의 그룹키를 알아내는 것이 암호학적으로 불가능해야 한다.

- 모바일 장치 또는 기지국의 서명생성키가 노출되었다고 가정하자. 이 경우, 공격자는 모바일 장치 또는 기지국인척 하고 프로토콜에 참여하여 새로운 그룹키를 생성하는 것은 가능하다. 그러나 공격자가 서명생성키를 알고 있다 할지라도 이전 프로토콜의 정보 $[(U_i^{(j)}, g^{r_{U_i^{(j)}}}, \sigma_{U_i^{(j)}}), (B_k, g^{r_{B^{(j)}}}, \sigma_{B_k^{(j)}}), (B_j, g^{r_j}, X^{(j)}, Y^{(j)}, \sigma_{Bj}), (1 \le i \le m, 1 \le k \le n)$와 $E_{K_k}(K_{j1 \le j \ne k \le n})$]로부터 이전 그룹키 K를 계산하는 문제는 묵시적 키인증에서 분석한 것과 같이 CDH 문제의 어려움과 기존 대칭키 암호알고리즘의 안전성에 기반을 둔다. 그러므로 서명생성키를 알고 있는 공격자가 이전의 그룹키를 계산하는 것은 암호학적으로 불가능하다.

• 제안한 프로토콜은 세션키 노출에의 안전성을 제공한다. 세션키 노출에의 안전성이란, 임의의 그룹키가 노출되더라도 수동적 공격자가 다른 그룹키를 알아내는 것이 계산적으로 불가능해야 하고 능동적 공격자가 프로토콜의 다른 참여자를 흉내 내는 것이 불가능해야 한다.

- 프로토콜의 기지국들과 모바일 장치들은 매 세션마다 다른 랜덤값을 이용하여 그룹키 K를 생성하기 때문에 각각의 그룹키들은 세션마다 독립성을 갖는다. 그러므로 노출된 그룹키 정보는 다른 그룹키를 계산하고자 하는 공격자에게는 아무런 도움이 되질 않는다.
- 능동적 공격자가 프로토콜의 다른 참여자를 흉내내기 위해서는 다른 구성원의 정당한 전자서명을 생성해야 한다. 노출된 그룹키는 전자서명키에 대한 정보를 포함하지 않으므로 그룹키 정보는 공격자가 프로토콜 구성원인척 하는 데에는 도움이 되질 않는다.

3.4 효율성 분석

제안하는 프로토콜에서 모바일 장치는 그룹키를 생성하기 위해 지수승 계산 2번, 서명생성 1번, 서명검증 n번의 계산량을 갖는다. 반면, 기지국은 지수승 계산 $(m+2(n+1))$번, 서명생성 2번, 서명검증 $(m+2(n-1))$번의 계산량을 갖는다. 즉, 그룹키를 생성하기 위해 모바일 장치보다 기지국이 더 많은 계산을 수행하도록 설계하였다.

모바일 장치로 가장 많이 사용될 수 있는 것으로는 휴대폰과 PDA 등이 있다. 휴대폰 안에는 PC의 CPU의 역할을 수행하는 MSM 칩내에 ARM 코어가 내장되어 있는데, 현재 일반적인 핸드폰에는 ARM7 이상의 CPU가 탑재되어 있다. ARM7의 CPU를 탑재한 정도의 핸드폰에서는 지수승 계산이 가능하며 최근에 출시되고 있는 ARM11의 경우 최대 1GHz까지의 속도가 나오고 있으므로 일반적인 핸드폰 정도에서도 제안하는 프로토콜의 지수승 연산 등의 암호 연산을 수행하는 데는 무리가 없을 것으로 생각된다.

모바일 환경에 적합한 그룹키 동의 프로토콜은 2003년에 제안된 Bresson 등의 프로토콜과 2005년에 제안된 Nam 등의 프로토콜이 있다. 앞에서 언급하였듯이 Bresson 등의 프로토콜은 순방향 안전성을 제공하지 못하는 등의 취약성을 갖는다[5].

이에 능동적 공격자를 고려한 Nam 등의 3-라운드 그룹키 프로토콜과 제안하는 프로토콜의 모바일 장치의 계산량을 비교하면, 지수승 계산측면에서의 계산량은 동일하다. 게다가 기지국이 다른 셀의 키를 올바르게 전송한다고 가정한다면 모바일 장치는 자신이 생성하는 셀의 키에 대한 서명검증(1번)만 수행하여도 된다. 표 1은 제안하는 프로토콜과 Nam 등의 3-라운드 그룹키 프로토콜에서의 기지국과 모바일 장치들의 계산량을 비교한 것이다.

표에서도 알 수 있듯이, 다중 셀로 확장되면서 기지국

표 1 Nam 등의 3-라운드 그룹키 프로토콜과의 효율성 비교

계산량 / 프로토콜	기지국			모바일 장치			비고
	지수승	서명생성	서명검증	지수승	서명생성	서명검증	
Nam 등의 3-라운드 그룹키 프로토콜	m+2	1	m	2	1	1	단일 셀 내에서의 그룹키 동의 프로토콜
제안 프로토콜	m+2(n+1)	2	m+2(n-1)	2	1	1(n)	다중 셀 내에서의 그룹키 동의 프로토콜

m : 셀 내의 모바일 장치들의 개수, n: 기지국의 개수

의 계산량은 증가하는 반면, 모바일 장치의 계산량은 자신의 셀의 모바일 장치들과 그룹키를 공유하는 정도의 양이므로 효율적이라 할 수 있다.

4. 패스워드 인증 방식을 이용한 서로 다른 셀의 모바일 장치간의 그룹키 동의 프로토콜

본 장에서는 일반적으로 사용되는 패스워드 인증방식이 제안한 그룹키 동의 프로토콜에 어떻게 적용할 수 있는 지를 살펴보도록 한다.

패스워드는 사람들이 쉽게 외울 수 있다는 장점 때문에 사용자 인증 방식으로 많이 사용되고 있으며, 이러한 패스워드를 이용한 키교환 프로토콜에 대한 연구도 활발히 진행되고 있다[8-13]. 또한 멀티캐스트 통신을 위한 패스워드 인증 방식을 위한 그룹키 동의 프로토콜에 대한 연구도 진행되고 있다[14-16]. Keung 등의 프로토콜은 키전송 형태의 그룹키 동의 프로토콜이다. 앞에서도 언급하였지만 키 전송은 서버를 제외한 그룹 구성원 입장에서는 공정하지 못하다. Asokan과 Bresson 등이 제안한 패스워드 인증방식의 그룹키 동의 프로토콜에서는 프로토콜에 참여하는 모든 구성원들이 사전에 패스워드를 공유하는 것을 가정하므로 현실적이지 못하다고 할 수 있다.

본 장에서는 모바일 장치와 자신이 속한 셀의 기지국 간에만 모바일 장치의 패스워드를 공유하는 것을 가정한 키동의 프로토콜을 제안하도록 한다. 각 클라이언트 $U_i^{(j)}(1 \le i \le m)$는 자신이 연결되어 있는 기지국 $B_j(1 \le j \le n)$과 패스워드 $pwd_{U_i^{(j)}}$를 공유하고 있고 각 기지국 B_j은 전자서명을 위한 공개키/개인키 쌍을 가지고 있다. 패스워드 인증방식으로 Bellovin과 Merrit의 EKE 스킴을 이용한다[8].

1) ① 각 클라이언트(모바일 장치) $U_i^{(j)}(1 \le i \le m)$는 랜덤하게 $r_{U_i^{(j)}} \in Z_q$를 선택하고 $z_{U_i^{(j)}} = g^{r_{U_i^{(j)}}}$를 계산한다. 자신이 연결된 기지국 B_j에게 $m_{U_i^{(j)}} = (U_i^{(j)}, E_{pwd_{U_i^{(j)}}}(z_{U_i^{(j)}}))$를 전송한다.

② 다른 기지국 $B_k(\neq B_j)(1 \le k \le n)$ 또한 랜덤하게 $r_{B_k^{(j)}} \in Z_q$를 선택하고 $z_{B_k^{(j)}} = g^{r_{B_k^{(j)}}}$를 계산한다. 그리고 난 후 기지국 B_j에게 $m_{B_k^{(j)}} = (B_k, z_{B_k^{(j)}})$와 $\sigma_{B_k^{(j)}}$를 전송한다.

2) 기지국 B_j는 $E_{pwd_{U_i^{(j)}}}(z_{U_i^{(j)}})$를 복호화하여 $z_{U_i^{(j)}}$를 알아낸다.

이 후의 과정은 3장에서 제안한 그룹키 동의 프로토콜 2) ~ 4)의 과정과 동일하다.

패스워드 인증방식을 이용한 프로토콜에서는 패스워드에 대한 오프라인 사전공격(dictionary attack)에 필요한 정보($z_{U_i^{(j)}}$)가 네트워크상에서 평문의 형태로 존재하지 않고 모바일 장치가 랜덤하게 선택한 비밀정보이기 때문에 프로토콜이 패스워드에 대한 오프라인 사전공격에 안전함을 알 수 있다. 또한 3장에서 제안한 그룹키 동의 프로토콜과 마찬가지로 묵시적 키인증과 순방향 안전성과 세션키 노출에의 안전성을 만족한다. 패스워드 인증방식의 프로토콜은 모바일 장치의 인증을 위해 패스워드 인증방식을 사용함으로써 서명 알고리즘을 사용했을 때보다 모바일 장치의 계산 부담을 줄일 수 있다는 장점을 갖는다.

5. 결 론

본 논문에서는 모바일 환경에서의 안전한 그룹 통신이 가능하도록 하는 그룹키 동의 프로토콜을 제안하였다. 기존에 제안되었던 프로토콜에서는 기지국이 하나 있는 단일 셀에서의 모바일 장치들 간의 그룹키 동의만을 고려하였으나, 본 논문에서는 이를 좀 더 확장한 실용적인 모델을 고려하였다. 즉, 서로 다른 셀에 속해 있는 모바일 장치들 간의 안전한 그룹 통신을 위한 그룹키 동의 프로토콜을 제안하였다. 그리고 제안한 프로토콜이 CDH 문제의 어려움과 사용된 암호화 알고리즘과 전자서명 알고리즘의 안전성의 가정 하에 일반적인 키동의 프로토콜이 만족해야 할 묵시적 키인증과 순방향 안전성과 세션키 노출에의 안전성을 만족함을 보였다. 또한 사용자 인증 방식으로 널리 사용되고 있는 패스워드 인증방식을 제안한 프로토콜에 적용함으로써 모바일 장치의 계산 부담을 좀 더 줄일 수도 있다는 것도 보였다.

제안하는 프로토콜은 먼 거리에 위치에 있는 사용자들이 자신들의 모바일 장치를 이용하여 안전한 화상회의, 그룹 채팅 등의 응용에 효과적으로 적용될 수 있을 것으로 생각된다.

참 고 문 헌

[1] I. Ingemarsson, D. T. Tang, C.K. Wong, "A conference key distribution system," *IEEE Transactions on Information Theory*, IT-28(5), pp. 714-720, September 1982.

[2] M. Burmester, Y. Desmedt, "A secure and efficient conference key distribution system," In *Advances in Cryptology-Eurocrypt'94*, Springer-Verlag, pp. 275-286, 1995.

[3] M. Steiner, G. Tsudik, M. Waidner, "Diffie-Hellman Key Distribution Extended to Group Communication," *Proc. of the 3rd ACM Conference on Computer and Communication Security(CCS'96)*, pp. 31-37, March 1996.

[4] E. Bresson, O. Chevassut, A. Essiari, D. Pointcheval, "Mutual Authentication and Group Key Agreement for Low-Power Mobile Devices," *International Conference on Mobile and Wireless Communications Networks*, Springer-Verlag,, Lecture Notes in Computer Science, LNCS 1514, pp. 59-62, 2003.

[5] J. Nam, S. Kim, D. Won, "A Weakness in the Bresson-Chevassut-Essiari-Pointcheval's Group Key Agreement Scheme for Low-Power Mobile Devices," *In Cryptology ePrint Archive, Report 2004/251, to appear, IEEE Communications Letters*, 2005.

[6] J. Nam, J. Lee, S. Kim, D. Won, "DDH-based Group Key Agreement in a Mobile Environment," *In Cryptology ePrint Archive, Report 2004/127, to appear, Journal of Systems and Software(JSS)*, 2005.

[7] C. Carroll, Y. Frankel, Y. Tsiounis, "Efficient key distribution for slow computing devices : Achieving fast over-the-air activation for wireless systems," *In IEEE Symposium on Security and Privacy (S&P '98)*, May 1998.

[8] S. Bellovin, M. Merrit, "Encrypted key exchange: password based protocols secure against dictionary attacks," In Proc. of the Symposium on Security and Privacy, pp. 72-84, 1992.

[9] M. Bellare, D. Pointcheval, P. Rogaway, "Authenticated key exchange secure against dictionary attacks," In *Advances in Cryptology - Eurocrypt 2000*, Springer-Verlag, pp. 139-155, 2000.

[10] J. Katz, R. Ostrovsky, M. Yung, "Efficient Password-Authenticated key exchange Using human-Memorable Passwords," In *Advances in Cryptology-Eurocrypt 2001*, Springer-Verlag, pp. 475-494, 2001.

[11] M. Steiner, G. Tsudik, M. Waidner, "Refinement and extension of Encrypted Key Exchange," *ACM Operating Systems Review*, vol. 29, no. 3, pp. 22-30, 1995.

[12] J. W. Byun, I. R. Jeong, D. H. Lee, C. S. Park, "Password-Authenticated Key Exchange between Clients with Different Passwords," *4th International Conference on Information and Communication Security(ICICS)*, pp. 134-146, 2002.

[13] J. Kim, S. Kim, J. Kwak, D. Won, "Cryptanalysis and improvement of password authenticated key exchange scheme between clients with different passwords," *2nd Computational Science and Its Applications(ICCSA)*, pp. 895-902, May 2004.

[14] N. Asokan, P. Ginzboorg, "Key Agreement in Ad-hoc Networks," *Expanded version of a talk given at the Nordsec'99 workshop*, Februry 2000.

[15] E. Bresson, O. Chevassut, D. Pointcheval, "Group Diffie-Hellman Key Exchange Secure Against Dictionary Attacks," *Advances in Cryptology Asiacrypt'02*, LNCS vol. 2501, Springer-Verlag. pp. 497-514, 2002.

[16] S. Keung, K. Siu, "Efficient Protocols Secure Against Guessing and Replay Attacks," *Proceedings of the Fourth International Conference on Computer Communications and Networks*, pp. 105-112, 1995.

김 지 연

1995년 2월 성균관대학교 정보공학과(공학사). 1997년 2월 성균관대학교 대학원 정보공학과(공학석사). 2003년 2월 성균관대학교 대학원 전기전자및컴퓨터공학과 박사과정 수료. 1996년 12월~현재 한국정보보호진흥원(KISA) 선임연구원. 관심분야는 암호프로토콜, 키관리, 개인정보보호기술

최 연 이

1993년 2월 한림대학교 화학과. 1995년 8월 성균관대학교 산업과학대학원 정보공학과(공학석사). 1999년 2월 성균관대학교 대학원 정보공학과 박사과정 수료 1997년 3월~현재 신성대학 컴퓨터정보계열 조교수. 관심 분야는 암호이론, 키관리 센서네트워크 보안

김 승 주

1994년 2월~1999년 2월 성균관대학교 정보공학과(학사, 석사, 박사). 1998년 12월~2004년 2월 한국정보보호진흥원(KISA) 팀장. 2004년 3월~현재 성균관대학교 정보통신공학부 정보보호연구소 교수. 2001년 1월~현재 한국정보보호학회, 한국인터넷정보학회, 한국정보과학회, 한국정보처리학회 논문지 및 학회지 편집위원 2002년 4월~현재 한국정보통신기술협회(TTA) IT 국제표준화 전문가. 2005년 6월~현재 교육인적자원부 유해정보차단 자문위원. 관심분야는 암호이론, 정보보호표준, 정보보호제품 및 스마트카드 보안성 평가, PET

원 동 호

1976년~1988년 성균관대학교 전자공학과(학사, 석사, 박사). 1978년~1980년 한국전자통신연구원 전임연구원. 1985년~1986년 일본 동경공업대 객원연구원 1988년~2003년 성균관대학교 교학처장, 전기전자및컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장. 1996년~1998년 국무총리실 정보화추진위원회 자문위원. 2002년~2003년 한국정보보호학회장. 현재 성균관대학교 정보통신공학부 정보보호연구소 교수, 한국정보보호학회 명예회장, (정통부지정 ITRC) 정보보호인증기술연구센터 센터장. 관심분야는 암호이론, 정보이론, 정보보호