

논문 2006-43TC-7-7

무선 단말기의 계산 효율성을 고려한 유·무선 통합 네트워크 환경에서의 안전한 그룹 통신

(Secure Group Communications Considering Computational Efficiency of Mobile Devices in Integrated Wired and Wireless Networks)

장우석*, 김현주*, 남정현*, 조석향*, 원동호**, 김승주*

(Woosuk Chang, Hyunjue Kim, Junghyun Nam, Seokhyang Cho, Dongho Won, and Seungjoo Kim)

요약

공개된 네트워크상에서 안전하게 그룹 통신을 하기 위해서는 그룹 구성원간에 공통의 비밀키를 안전하고 효율적으로 설정할 수 있는 방법이 필요하며, 이러한 목적으로 설계되는 프로토콜을 그룹 키 동의 프로토콜이라고 한다. 그룹 키 동의 프로토콜에 관한 연구는 그동안 많은 연구자들에 의해 다양한 관점에서 진행되어 왔으며, 최근 들어 유·무선 통합 네트워크 환경에서의 안전한 그룹 통신을 위한 그룹 키 동의 프로토콜에 대한 연구가 진행되고 있다.

유·무선 통합 네트워크 환경에 적합한 그룹 키 동의 프로토콜을 설계하기 위해서는 고성능 연산 능력을 가진 유선 단말기의 특성과 상대적으로 계산능력이 떨어지는 무선 단말기의 특성이 함께 고려되어야 한다. 특히, 시스템 자원의 제한성을 갖는 무선 단말기에서의 계산량을 최소화하는 문제는 그룹 키 동의 프로토콜 설계에 있어서 무엇보다 중요하다. 본 논문에서는 무선 단말기의 계산량을 최소화하면서 유·무선 통합 네트워크 환경에 적합한 효율적인 그룹 키 동의 프로토콜을 제안하고 그 안전성을 증명한다.

Abstract

Group key agreement protocols are designed to allow a group of parties communicating over a public network to securely and efficiently establish a common secret key. Over the years, a number of solutions to the group key agreement protocol have been proposed with varying degrees of complexity, and the research relating to group key agreement to securely communicate among a group of members in integrated wired and wireless networks has been recently proceeded.

Both features of wired computing machines with the high-performance and those of wireless devices with the low-power are considered to design a group key agreement protocol suited for integrated wired and wireless networks. Especially, it is important to reduce computational costs of mobile devices which have the limited system resources. In this paper, we present an efficient group key agreement scheme which minimizes the computational costs of mobile devices and is well suited for this network environment and prove its security.

Keywords : Group key agreement, mobile devices, integrated wired and wireless networks, CDH assumption.

I. 서 론

미래의 네트워크 환경의 특징은 한마디로 유·무선

통합이라고 할 수 있다. 유럽과 미국의 NGN (Next Generation Network), 일본의 NGmN (Next Generation mobile Network), 국내의 BcN (Broadband convergence Network)으로 대표되는 차세대 네트워크 환경은 폐깃 형태의 전송 기술을 이용하여 음성, 데이터, 인터넷, 멀티미디어 등 각종 서비스가 하나의 통합 인프라 상에서 모두 제공될 수 있는 통신망으로, 그 궁극적인 형태가 하나의 통신망에서 제공되는 것이라는 점에서 차세대 네트워크 환경의 필수 조건은 유·무선 통합이라고 할 수 있다.

* 정희원, ** 평생회원, 성균관대학교 정보통신공학부
정보보호연구소
(Information Security Group, School of Information and Communication Engineering, Sungkyunkwan University)

※ 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 육성·지원 사업의 연구결과로서 수행되었음.

접수일자: 2006년6월15일, 수정완료일: 2006년7월14일

그룹 키 동의 프로토콜(group key agreement protocol)은 일련의 그룹을 형성하는 다수의 통신 참여자들이 공개된 통신망 상에서 세션키(session key)라 불리는 그룹의 공통 비밀키를 공유함으로써 그룹 내에서의 안전한 통신을 가능하게 하는 프로토콜이다. 다수의 사용자가 참여하는 다양한 응용프로그램(유료 영상 서비스, 원격 사이버 강의, 다중 사용자 게임, 커뮤니티 채팅 등)에서 이 세션키를 공유함으로써 인증(Authentication), 기밀성(Confidentiality), 그리고 메시지의 무결성(Message Integrity) 등과 같은 보안 서비스를 효과적으로 제공할 수 있다. 이와 같은 그룹 기반의 응용 프로그램들이 현대 컴퓨팅 환경에서 급증하고 있기 때문에, 효율적인 그룹 키 동의 프로토콜에 대한 연구가 많은 주목을 받고 있다. 그룹 키 동의 프로토콜에 관한 연구는 1982년 I. Ingemarsson, D. Tang과 C. Won에 의해서 처음으로 제안되었다^[1]. 이후, 많은 그룹 키 동의 프로토콜^[4,5,6,7,8]이 발표되었으며, 모바일 단말기의 사용이 대중화되면서 무선 통신에 적합한 그룹 키 동의 프로토콜^[9,10,11,12]에 대한 연구도 활발히 진행되고 있다.

한편, 유·무선 통합 네트워크 기술이 발전하고 있는데 반하여 이와 같은 새로운 네트워크 환경에서의 안전한 그룹 통신을 위한 그룹 키 동의 프로토콜에 대한 연구는 현재 시작 단계에 불과하다. 최근, Nam 등은 유·무선 통합 네트워크 환경에서 효율적이면서도 안전한 그룹 키 동의 프로토콜을 제안하였다^[3]. 유·무선 통합 네트워크 환경에 적합한 그룹 키 동의 프로토콜을 설계하기 위해서는 무선 단말기 고유의 특성인 이동성, 시스템 자원의 제한성 등과 유선 단말기 고유의 특성인 비 이동성, 고성능 연산 능력을 함께 고려해야 한다. 특히, 무선 단말기 사용자들은 자체적인 이동성으로 인해 정적인 네트워크 환경에 국한되지 않고 원격의 네트워크로 이동하여 통신의 전송 경로가 변경되고, 모바일 사용자들은 이동성에 귀결되는 단말기의 소형화 경향으로 인해 제한된 시스템 자원을 보유하게 된다. 이러한 이동성과 시스템 자원의 제한성 등으로 인하여 유·무선 통합 네트워크 환경에서의 그룹 키 동의 프로토콜은 무선 단말기에서의 계산량을 줄이는 데에 보다 초점을 맞추어 설계되어야 한다.

따라서, 본 논문에서는 무선 단말기에서의 계산량을 최소화하면서 유·무선 통합 네트워크 환경에 적합한 효율적인 그룹 키 동의 프로토콜을 제안하고 그 안전성을 증명한다. 제안한 스킴은 Nam 등의 스킴과 비교하

여 무선 단말기에서의 계산 효율성이 훨씬 뛰어나다. Nam 등이 제안한 방식은 무선 단말기에서 그룹의 세션 키를 계산하기 위해 3번의 모듈러 멱승 연산과 2번의 모듈러 곱셈 연산을 해야 하지만, 본 논문에서 제안한 방식은 2번의 모듈러 멱승 연산만을 필요로 하며 모듈러 곱셈 연산 대신 해쉬함수와 XOR 연산을 이용하여 계산 효율성을 높였다.

본 논문의 구성은 다음과 같다. II장에서는 그룹 키 동의 프로토콜의 보안 요구사항과 네트워크 환경에 따른 기준의 contributory 그룹 키 동의 프로토콜에 대해 살펴보고, III장에서는 트리구조의 유·무선 통합 네트워크 구성에 대해서 알아본다. 그리고 IV장에서는 무선 단말기의 계산 효율성을 고려한 유·무선 통합 네트워크 환경에 적합한 그룹 키 동의 프로토콜을 제안하고, V장에서는 제안한 스킴의 효율성과 안전성을 각각 분석하며, 마지막으로 VI장에서는 결론을 맺는다.

II. 관련 연구

키 설정 프로토콜(key establishment protocol)은 세션키 생성 관점에 의해 키 전송 프로토콜(key transport protocol)과 키 동의 프로토콜(key agreement protocol)로 나눌 수 있다. 키 전송 프로토콜은 참가자 한 명이 세션키를 생성하여 안전하게 다른 참가자들에게 전송하는 방식이며, 키 동의 프로토콜은 한 명 이상의 참가자가 공통의 세션키를 생성하는데 자신의 정보를 제공하는 방식이다. 본 논문에서는 모든 참가자가 세션키 설정에 자신의 정보를 제공하는 contributory 키 동의 프로토콜에 바탕을 두고 있다.

본 장에서는 그룹 키 동의 프로토콜의 보안 요구사항과 이제까지 연구되었던 contributory 그룹 키 동의 프로토콜에 대해서 살펴보기로 한다.

1. 그룹 키 동의 프로토콜 보안 요구사항

그룹 키 동의 프로토콜의 보안 요구사항에는 그룹 키 비밀성, 전방향 안전성, 역방향 안전성, 그룹 키 독립성, 완전한 전방향 안전성이 있다. 그룹 키 비밀성과 전방향 안전성, 그리고 역방향 안전성은 모든 그룹 키 동의 프로토콜들이 제공해야 하는 필수적인 요소이며 그룹 키 독립성과 완전한 전방향 안전성은 효율성의 이유로 선택적으로 제공된다. 대부분의 contributory 그룹 키 동의 프로토콜들은 위의 다섯 가지 보안 요구사항 모두를 만족한다.

· 그룹 키 비밀성

도청자가 그룹 키를 알아내는 것은 계산상 불가능해야 한다. 이것은 합법적인 멤버만이 그룹 키를 소유하고 이 키를 소유한 개체만이 통신 내용을 수신할 수 있도록 하기 위한 것이다.

· 전방향 안전성

일정 기간 동안 생성된 그룹 키들을 안다고 하더라도, 그 이후에 생성되는 그룹 키를 유도할 수 없어야 한다. 이것은 합법적으로 통신에 참가하던 멤버가 탈퇴했을 때, 탈퇴한 이후의 통신에 대해서는 수신할 수 없도록 하기 위한 조건이다.

· 역방향 안전성

일정 기간 동안 생성된 그룹 키들을 안다고 하더라도, 그 이전에 생성된 그룹 키를 유도할 수 없어야 한다. 이것은 합법적으로 가입하여 통신에 참가한 멤버라도 가입 이전의 통신에 대해서는 수신할 수 없도록 하기 위한 조건이다.

· 그룹 키 독립성

현재 사용되는 그룹 키는 과거나 미래의 어떠한 그룹 키와도 관계없이 랜덤하게 선택되어야 한다. 즉, 과거 그룹 키들을 알더라도 이후의 그룹 키를 알아낼 수 없어야 하고, 또한 나중에 사용된 그룹 키들을 알더라도 그 이전에 사용된 그룹 키를 알아낼 수 없어야 한다.

· 완전한 전방향 안전성

일반적으로 각 그룹 멤버는 자신만이 알고 있는 비밀 키를 소유하고 있으며 그룹 키를 생성하는 과정에 이 비밀 키를 사용하게 된다. 공격자가 그룹 멤버의 개인 키를 알더라도 과거에 사용된 그룹 키를 알아낼 수 없다면 그룹 키 동의 프로토콜은 완전한 전방향 안전성을 제공한다고 한다.

2. Contributory 그룹 키 동의 프로토콜 분석

이제까지 연구되었던 contributory 그룹 키 동의 프로토콜을 유선 네트워크 환경, 무선 네트워크 환경, 유 · 무선 통합 네트워크 환경에 따라 살펴보기로 한다.

가. 유선 네트워크 환경

유선 네트워크 환경에 적합한 가장 대표적인 그룹 키 동의 프로토콜로는 1994년 Burmester와 Desmedt^[4]에 의해 제안된 BD 프로토콜과 1996년 Steiner, Tsudik와 Waidner^[5]에 의해 제안된 GDH.2 프로토콜이 있다. BD 프로토콜은 완전한 전방향 안전성을 만족하며, 2003년 Katz와 Yung^[6]에 의해 프로토콜의 안전성도 증명되

었다. 그러나 GDH.2 프로토콜은 $O(n)$ 번의 모듈러 역승 연산과 통신 라운드를 요구하는 단점이 있으며, BD 프로토콜은 그룹 크기에 따라 브로드캐스트 되는 메시지의 수가 선형적으로 변한다는 단점이 있다. 따라서 [4,5]는 그룹 사이즈가 커짐에 따라 그룹의 통신량과 연산량도 함께 증가되기 때문에, 무선 단말기와 같이 제한된 시스템 자원을 보유하고 있는 무선 네트워크 환경에는 적합하지 않다.

이 밖에도 1998년 Becker와 Wille^[7]에 의해서 제안된 Hypercube/Octopus 프로토콜과 2001년 Kim, Perrig와 Tsudik^[8]에 의해서 제안된 STR 프로토콜이 있다. Hypercube 프로토콜은 작은 라운드 수를 요구하고, Octopus 프로토콜은 최소한의 메시지 수를 요구하는 프로토콜이지만, 두 프로토콜은 특정한 네트워크 구조에 의존한다는 단점이 있다. 그리고 경사트리를 이용하는 STR 프로토콜은 각각의 그룹 멤버들이 서브키들과 그룹 키를 연산해야 하는 부담을 가지며, 그룹 후원자(sponsor)를 두어 키를 효율적으로 생성할 수는 있지만, 그룹의 크기가 커짐에 따라 그 연산량도 함께 증가하는 단점을 가지고 있다.

나. 무선 네트워크 환경

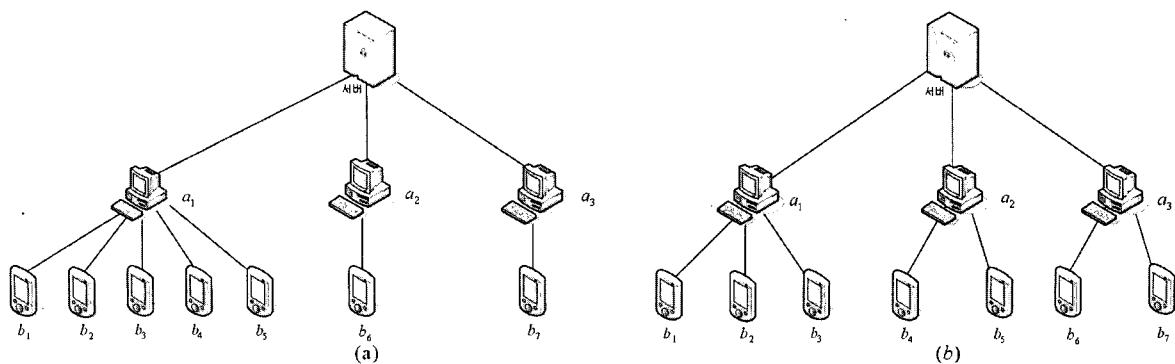
무선 네트워크 환경에 적합한 가장 대표적인 그룹 키 동의 프로토콜로는 2003년도에 Bresson 등^[9]이 제안한 프로토콜 있다. [9]은 저전력 모바일 단말기와 게이트웨이 사이에서의 효율적인 그룹 키 동의에 관한 방법을 제안하였으나 이후 Nam 등에 의해 전방향 안전성의 보안 요구사항을 만족하지 못함이 지적되었다^[10].

최근, 2005년도에 Nam 등^[11]과 Cho 등^[12]은 모바일 환경에 적합한 그룹 키 동의 프로토콜을 제안하였다. 그러나 [11,12]는 [9]과 마찬가지로 고성능 연산 능력을 가진 한 명의 사용자(서비스 제공자)가 그룹의 세션 키를 계산하기 위해서 $O(n)$ 의 연산을 수행하는데 비해 그룹에 참여하는 나머지 사용자들(모바일 사용자들)은 단지 $O(1)$ 의 연산만을 수행하는 비대칭적 구조의 문제점을 안고 있다.

따라서, 이전에 나왔던 contributory 그룹 키 동의 프로토콜들^[4-12]을 차세대 네트워크 환경인 유 · 무선 통합 네트워크 환경에 적용하기는 어렵다.

다. 유·무선 통합 네트워크 환경

최근 Nam 등은 유 · 무선 통합 네트워크 환경에서의 효율적이고도 안전한 그룹 키 동의 프로토콜을 제안하

그림 1. $m \geq 2$ 일 때, 유·무선 통합 네트워크의 구성Fig. 1. $m \geq 2$, structure of integrated wired and wireless networks.

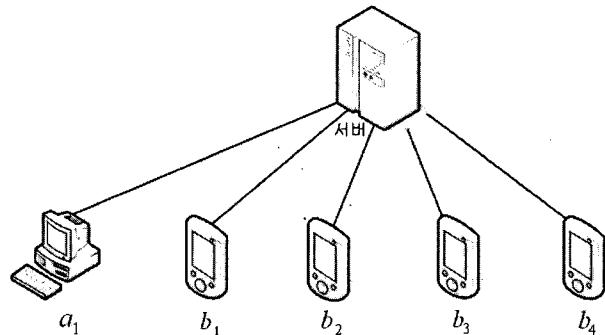
였다^[3]. [3]에서는 유선 사용자 그룹과 무선 사용자 그룹을 높이가 2인 트리구조를 이용하여 네트워크를 구성하였으며, DDH (Decisional Diffie–Hellman) 문제에 기반하여 수동적 공격자에 대한 안전함을 증명하였다. 하지만, 실질적인 네트워크 구성에 있어서 유선 사용자 그룹 멤버와 무선 사용자 그룹 멤버들 간의 네트워크 구성에 대한 방법은 제시되어 있지 않다. 또한, 제안된 프로토콜은 무선 사용자 그룹에서 3번의 모듈러 곱셈 연산과 2번의 모듈러 곱셈 연산을 수행해야 하므로 제한된 시스템 자원을 보유한 무선 단말기에서의 계산량을 최소화할 필요성이 있다.

III. 트리구조의 유무선 통합 네트워크 구성

본 논문의 시나리오는 다음과 같다. 충분한 연산 능력을 가진 유선 사용자 그룹 $S = \{a_1, \dots, a_m\}$ 과 상대적으로 낮은 계산 능력을 가진 무선 단말기 사용자 그룹 $R = \{b_1, \dots, b_n\}$ 이 같은 그룹에 참여하여 공통의 세션키를 공유함으로써 서버로부터 다양한 멀티캐스트 서비스를 제공받는다고 가정한다. 이때, 네트워크의 모든 사용자 그룹 U 는 $S \cup R$ 이다.

$m \geq 2$ 일 때, 그룹 통신에 참여하는 유·무선 사용자들은 그림 1과 같이 높이가 2인 트리 구조를 갖도록 네트워크를 구성한다. 즉, 고성능 연산능력을 가진 서버는 항상 트리의 최상위 노드에 위치하며, S 에 속한 그룹 멤버들은 레벨1상의 노드에 위치하고, R 에 속한 그룹 멤버들은 리프 노드에 위치한다.

이때, 유선 사용자 그룹 멤버와 무선 사용자 그룹 멤버들 간의 네트워크 구성은 대단히 중요하다. 만약, 그림 1(a)와 같이 R 의 그룹 멤버들이 S 의 한 멤버에게 몰려 있거나 균등하게 구성되어 있지 않을 경우, 그룹

그림 2. $m = 1$ 일 때, 유·무선 통합 네트워크의 구성Fig. 2. $m = 1$, structure of integrated wired and wireless networks.

키 동의 프로토콜을 수행하는데 있어서 네트워크의 지연과 밀집 같은 병목현상이 발생할 수 있다. 하지만, R 의 그룹 멤버들을 그림 1(b)와 같이 균등하게 나누어 S 의 그룹 멤버들과 네트워크를 구성한다면 연산 능력이 충분한 유선 사용자 그룹 멤버들 간에 계산량이 균등히 분배되므로 그룹 키 동의 프로토콜을 수행하는데 있어서의 잠재적인 병목 현상을 피할 수 있다.

그림 2의 경우는 그룹 S 의 멤버가 1명(즉, $m = 1$)일 때, 서버를 제외한 모든 그룹 멤버들은 리프 노드에 위치하게 된다.

IV. 제안하는 그룹 키 동의 프로토콜

본 장에서는 무선 단말기에서의 계산량을 최소화하면서 유·무선 통합 네트워크 환경에 적합한 효율적인 새로운 contributory 그룹 키 동의 프로토콜을 제안한다. 제안한 프로토콜은 유·무선 통합 네트워크의 구성에 따라서 기본 프로토콜과 확장 프로토콜로 구분하여 설계한다.

본 논문에서 제안하는 그룹 키 동의 프로토콜에서 사용될 시스템 파라미터의 정의는 다음과 같다.

- L_0 : 트리 구조의 최상위 레벨에 속한 서버
- L_1 : 트리 구조의 레벨1에 속한 그룹 멤버들의 집합
- L_2 : 트리 구조의 레벨2에 속한 그룹 멤버들의 집합
- I_{a_j} : 그룹 멤버 a_j 의 자식 그룹 멤버들 index 집합
- $p = k \cdot q + 1$ (k 는 정수, q 는 소수) : 큰소수
- G : 모듈러 p 상에서 위수 q 를 갖는 순환 부분군
- g : 모듈러 p 상에서 위수 q 를 갖는 순환 부분군의 원시 원소
- sk_s : 서버의 개인키
- pk_s : 서버의 공개키
- sk_{a_j} : 유선그룹 멤버 a_j 의 개인키
- pk_{a_j} : 유선그룹 멤버 a_j 의 공개키
- sk_{b_i} : 무선그룹 멤버 b_i 의 개인키
- pk_{b_i} : 무선그룹 멤버 b_i 의 공개키
- $sign$: 서명 알고리즘
- $verify$: 검증 알고리즘
- E : 암호화 알고리즘
- D : 복호화 알고리즘
- $H()$: 일방향 해쉬 함수
- K_j : 그룹 멤버 a_j 와 그 자식 그룹 멤버들 I_{a_j} 간의 서브그룹 키
- SK : 전체 그룹의 세션 키

1. 기본 프로토콜

전체 네트워크는 $L_0 = \{\text{서버}\}$, $L_1 = \{a_1, b_1, \dots, b_n\}$, $L_2 = \{\emptyset\}$ 으로 구성되어 있다고 가정한다. 다음은 제안한 프로토콜의 자세한 실행 과정을 나타낸다.

(라운드 1.) 각각의 그룹 멤버 $a_1, b_i \in L_1 (i \in [1, n])$

는 임의의 $r_{a_1}, r_{b_i} \in Z_q$ 를 선택하여 $z_{a_1} = g^{r_{a_1}}$, $z_{b_i} = g^{r_{b_i}}$ 를 계산한 다음, 각각의 개인키 sk_{a_1}, sk_{b_i} 로 z_{a_1}, z_{b_i} 를 서명하여 $\sigma_{a_1} = sign_{sk_{a_1}}(z_{a_1})$, $\sigma_{b_i} = sign_{sk_{b_i}}(z_{b_i})$ 를 얻는다. 그런 다음, $(z_{a_1}, \sigma_{a_1}), (z_{b_i}, \sigma_{b_i})$ 를 트리상의 부모 노드인 서버에게 전송한다. 한편, 서버는 임의의 $s_s, r_s \in Z_q$ 를 선택하여 $w = g^{s_s}$ 와 $x_s = w^{r_s} (= g^{s_s r_s})$ 를 계산한다.

(라운드 2.) 서버는 $(z_{a_1}, \sigma_{a_1}), (z_{b_i}, \sigma_{b_i})$ 를 수신하여 각각의 자식 그룹 멤버 a_1, b_i 의 공개키 pk_{a_1}, pk_{b_i} 를 이용하여 서명값 $\sigma_{a_1}, \sigma_{b_i}$ 를 검증한 다음, 서명값이 모두 옳다면 x_{a_1} 와 x_{b_i} 를 각각 (1), (2)와 같이 계산한다.

$$x_{a_1} = (z_{a_1})^{s_s} = g^{s_s r_{a_1}} \quad (1)$$

$$x_{b_i} = (z_{b_i})^{s_s} = g^{s_s r_{b_i}} \quad (2)$$

또한, 서버는 안전성 파라미터로 일회용의 l 비트, $\delta \in \{0, 1\}^l$ 를 선택하여 (3)과 같이 X 를 계산하고,

$$X = \bigoplus_{i=1}^n H(\delta \| x_{b_i}) \oplus H(\delta \| x_{a_1}) \oplus H(\delta \| x_s) \quad (3)$$

Y 를 (4)과 같이 계산한다.

$$Y = \{y_{a_1}, y_{b_i} | i \in [1, n]\} \quad (4)$$

이때, y_{a_1} 와 y_{b_i} 는 각각 (5), (6)과 같이 계산된다.

$$y_{a_1} = X \oplus H(\delta \| x_{a_1}) \quad (5)$$

$$y_{b_i} = X \oplus H(\delta \| x_{b_i}) \quad (6)$$

그런 다음, 서버의 개인키 sk_s 를 이용하여 메시지 $\delta \| w \| Y$ 에 대해서 (7)과 같이 서명을 생성하고,

$$\sigma_s = sign_{sk_s}(\delta \| w \| Y) \quad (7)$$

$(\delta \| w \| Y \| \sigma_s)$ 를 그룹의 모든 멤버들에게 브로드캐스트 한다.

(키 계산.) 각각의 그룹 멤버 $a_1, b_i \in L_1$ 는 서버로부터 수신한 브로드캐스트 메시지에 대해 서버의 공개키 pk_s 를 이용하여 서명값 σ_s 를 검증한 뒤 서명값이 옳다면, 그룹의 공통 비밀값 X 를 (8), (9)와 같이 계산한다.

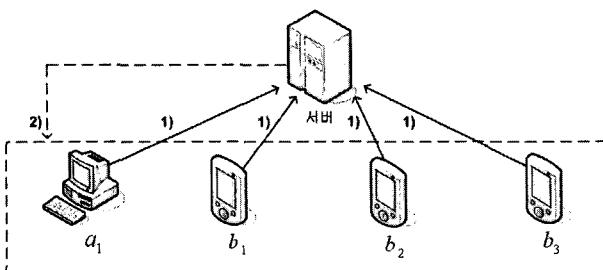
$$X = y_{a_1} \oplus H(\delta \| w^{r_{a_1}}) = y_{a_1} \oplus H(\delta \| g^{s_s r_{a_1}}) \quad (8)$$

$$X = y_{b_i} \oplus H(\delta \| w^{r_{b_i}}) = y_{b_i} \oplus H(\delta \| g^{s_s r_{b_i}}) \quad (9)$$

마지막으로, 서버를 포함한 모든 멤버들은 X 로부터 그룹의 공통 세션 키 SK 를 (10)과 같이 계산한다.

$$SK = H(Y \| X) \quad (10)$$

기본 프로토콜의 동작과정을 간단히 그림 3에 나타내었다. 그림 3에서 보듯이 이 프로토콜은 $n+1$ 번의 유



- (1)라운드 1: $(g^{r_1}, \sigma_{a_1}), (g^{r_1}, \sigma_{b_1}), (g^{r_2}, \sigma_{b_2}), (g^{r_3}, \sigma_{b_3})$.
(2)라운드 2: $(\delta, g^{s_1}, \{y_{a_1}, y_{b_1}, y_{b_2}, y_{b_3}\}, \sigma_s)$.

그림 3. 기본 프로토콜의 동작 과정

Fig. 3. An execution of the basic protocol.

니캐스트와 1번의 브로드캐스트 통신을 필요로 하고, 2 라운드 만에 그룹 통신에 사용될 세션키를 나눠 갖게 된다.

2. 확장 프로토콜

확장 프로토콜은 본 논문에서 핵심이 되는 프로토콜로서, 무선 단말기에서의 계산량을 최소화하면서 $m \geq 2$ 일 때 트리 구조를 갖는 유·무선 통합 네트워크에서 사용되는 프로토콜이다. 확장 프로토콜은 사용자 그룹을 m 개의 서브그룹으로 나누며, 각각의 서브그룹에 대해서 기본 프로토콜을 수행하여 공통의 서브그룹키를 생성한다. 또한, 그룹멤버 $a_j \in L_1$ 는 기본 프로토콜을 수행하여 서버와 a_j 간의 공통의 비밀키를 생성한다. 마지막으로, 전체 그룹의 세션키를 생성하기 위해서 서브그룹의 a_j 가 하나의 멤버로서 다시 그룹에 참여

할 때 서버와 a_j 간에 생성된 비밀키로 서브그룹키를 암호화하여 서버에게 전달해준다. 서버는 a_j 와의 비밀키 값을 계산해서 암호화된 서브그룹키를 복호화한 뒤, 복호화 된 서브그룹키들과 안전성 파라미터를 사용하여 전체 그룹의 세션키를 생성한다. 그림 4는 서버와 a_j 간의 비밀키 생성 및 a_j 와 b_i 간의 서브그룹키 생성에 대해 보여주고 있다.

제안한 프로토콜의 핵심 아이디어는 전체 그룹의 세션키를 생성하기 위해서 서브그룹의 a_j 가 하나의 멤버로서 다시 그룹에 참여할 때, 변형된 기본 프로토콜을 이용하는데 있다. 즉, 서버에서 그룹 전체의 세션키를 생성할 때, 기본 프로토콜에서 생성된 서브그룹키의 모듈러 연산값을 이용하는 대신 서브그룹키 값 자체를 이용한다. 이렇게 함으로써 유·무선 사용자 그룹에서는 공동의 세션키를 계산하기 위한 모듈러 연산을 각각 1 회 줄일 수 있게 된다.

전체 네트워크는 $L_0 = \{\text{서버}\}$, $L_1 = \{a_1, \dots, a_m\}$, $L_2 = \{b_1, \dots, b_n\}$ 으로 구성되어 있다고 가정한다. 다음은 제안한 프로토콜의 자세한 실행 과정을 나타낸다.

(라운드 1.) 각각의 그룹 멤버 $b_i \in L_2$ 는 임의의 $r_{b_i} \in Z_q$ 를 선택하여 $z_{b_i} = g^{r_{b_i}}$ 를 계산한 다음, 각각의 개인키 sk_{b_i} 로 z_{b_i} 를 서명하여 $\sigma_{b_i} = sign_{sk_{b_i}}(z_{b_i})$ 를 얻는다. 그런 다음, (z_{b_i}, σ_{b_i}) 를 트리상의 부모 노드인 그룹 멤버 $a_j \in L_1$ 에게 전송한다. 그리고, 서버는 임의의

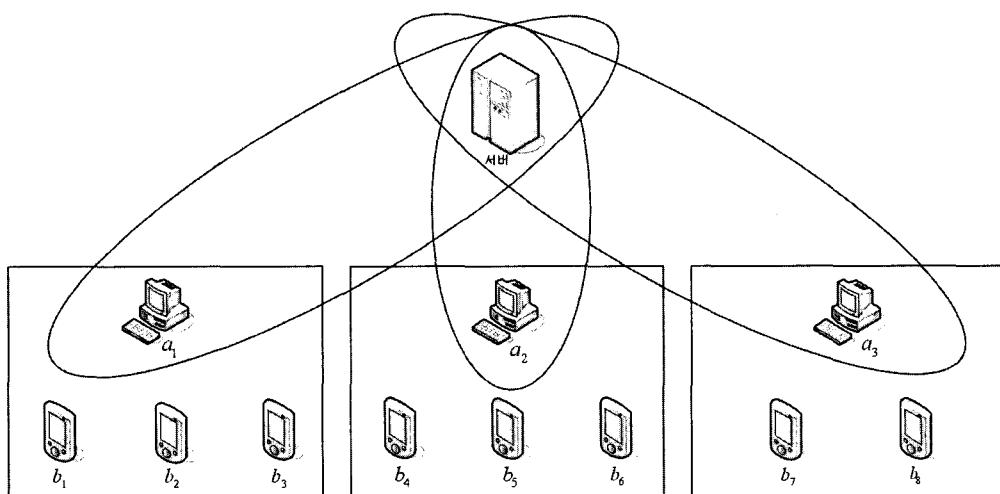


그림 4. 서버와 a_j 간의 비밀키 생성 및 a_j 와 그 자식 멤버 b_i 간의 서브그룹간 세션키 생성
Fig. 4. Secret key between sever and a_j , subgroup key between a_j and his children b_i .

$r_s \in Z_q$ 를 선택하여 $z_s = g^{r_s}$ 를 계산한 다음, 서버의 개인키 sk_s 로 z_s 를 서명하여 $\sigma_s = sign_{sk_s}(z_s)$ 를 얻는다. 그런 다음, (z_s, σ_s) 를 트리상의 자식 노드인 그룹 멤버 $a_j \in L_1$ 에게 브로드캐스트 한다. 한편, $a_j \in L_1$ 는 임의의 $s_j, r_{a_j} \in Z_q$ 를 선택하여 $w_j = g^{s_j}$ 와 $x_{a_j} = (w_j)^{r_{a_j}} = g^{s_j r_{a_j}}$ 를 계산한다.

(라운드 2.) $a_j \in L_1$ 는 각각의 자식 그룹멤버 b_i 로부터 (z_{b_i}, σ_{b_i}) 를 수신한 뒤 b_i 의 공개키 pk_{b_i} 를 이용하여 서명값 σ_{b_i} 를 검증한 다음, 서명값이 모두 옳다면 (11)과 같이 x_{b_i} 를 계산한다.

$$x_{b_i} = (z_{b_i})^{s_j} = g^{s_j r_{b_i}} \quad (11)$$

또한, $a_j \in L_1$ 는 서버로부터 (z_s, σ_s) 를 수신한 뒤 서버의 공개키 pk_s 를 이용하여 서명값 σ_s 를 검증한 다음, 서명값이 옳다면 (12)과 같이 x_s 를 계산한다.

$$x_s = (z_s)^{s_j} = g^{s_j r_s} \quad (12)$$

그리고, a_j 는 안전성 파라미터로 일회용의 l 비트, $\delta_{a_j} \in \{0,1\}^l$ 를 선택하여 (13), (14)와 같이 X_j, X_{js} 를 계산하고,

$$X_j = \bigoplus_{i \in I_{a_j}} H(\delta_{a_j} \| x_{b_i}) \oplus H(\delta_{a_j} \| x_{a_j}) \quad (13)$$

$$X_{js} = H(\delta_{a_j} \| x_{a_j}) \oplus H(\delta_{a_j} \| x_s) \quad (14)$$

(15), (16)와 같이 Y_j, Y_{js} 를 계산한다.

$$Y_j = \{y_{b_i} | i \in I_{a_j}\} \quad (15)$$

$$Y_{js} = \{y_{js} | j \in [1, m]\} \quad (16)$$

이때, y_{b_i}, y_{js} 는 각각 (17), (18)과 같이 계산된다.

$$y_{b_i} = X_j \oplus H(\delta_{a_j} \| x_{b_i}) \quad (17)$$

$$y_{js} = X_{js} \oplus H(\delta_{a_j} \| x_s) \quad (18)$$

그런 다음, 각각의 $a_j \in L_1$ 와 그 자식 그룹 멤버들간의 서브그룹키를 (19)와 같이 계산하고,

$$K_j = H(Y_j \| X_j) \quad (19)$$

서버와 각각의 $a_j \in L_1$ 간의 비밀키를 (20)과 같이 계산한 뒤,

$$K_{js} = H(Y_{js} \| X_{js}) \quad (20)$$

K_j 를 (21)과 같이 암호화 한다.

$$\hat{z}_{a_j} = E_{K_{js}}(K_j) \quad (21)$$

마지막으로, $a_j \in L_1$ 는 자신의 개인키 sk_{a_j} 를 이용하여 메시지 $\delta_{a_j} \| w_j \| \hat{z}_{a_j} \| Y_j \| Y_{js}$ 에 대해서 (22)와 같이 서명을 생성하고,

$$\sigma_{a_j} = sign_{sk_{a_j}}(\delta_{a_j} \| w_j \| \hat{z}_{a_j} \| Y_j \| Y_{js}) \quad (22)$$

$(\delta_{a_j}, w_j, \hat{z}_{a_j}, Y_j, Y_{js}, \sigma_{a_j})$ 를 자신의 자식 그룹 멤버들과 서버에게 브로드캐스트 한다.

(라운드 3.) 서버는 각 자식 그룹멤버 a_j 로부터 $(\delta_{a_j}, w_j, \hat{z}_{a_j}, Y_j, Y_{js}, \sigma_{a_j})$ 를 수신한 뒤 a_j 의 공개키 pk_{a_j} 를 이용하여 서명값 σ_{a_j} 를 검증하여 서명값이 옳다면, 서버와 $a_j \in L_1$ 간의 공통 비밀값 X_{js} 와 비밀키 K_{js} 를 각각 (23), (24)와 같이 계산한다.

$$X_{js} = y_{js} \oplus H(\delta_{a_j} \| (w_j)^{r_s}) = y_{js} \oplus H(\delta_{a_j} \| g^{s_j r_s}) \quad (23)$$

$$K_{js} = H(Y_{js} \| X_{js}) \quad (24)$$

그리고, (24)의 K_{js} 를 이용하여 \hat{z}_{a_j} 를 (25)와 같이 복호화 한다.

$$K_j = D_{K_{js}}(E_{K_{js}}(K_j)) \quad (25)$$

그런 다음, 서버는 안전성 파라미터로 일회용의 l 비트, $\delta_s, K_{sr} \in \{0,1\}^l$ 을 선택하여 X 를 (26)과 같이 계산하고,

$$X = \bigoplus_{j=1}^m H(\delta_s \| K_j) \oplus H(\delta_s \| K_{sr}) \quad (26)$$

Y 를 (27)과 같이 계산한다.

$$Y = \{\hat{y}_j | j \in [1, m]\} \quad (27)$$

이 때, \hat{y}_j 는 (28)과 같이 계산된다.

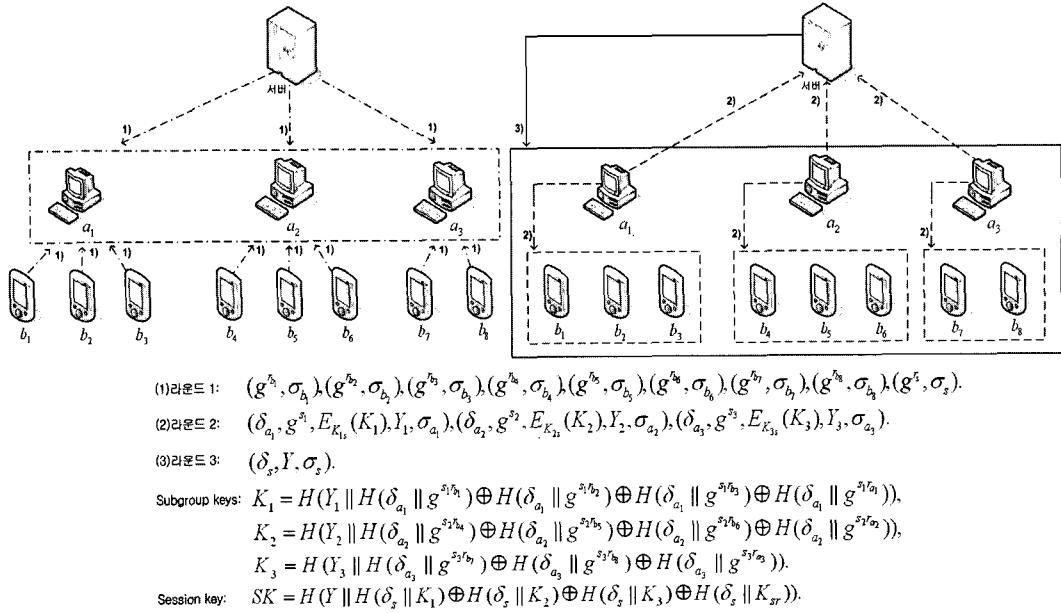


그림 5. 확장 프로토콜의 동작 과정
Fig. 5. An execution of the generalized protocol.

$$\hat{y}_j = X \oplus H(\delta_s \parallel K_j) \quad (28)$$

$$X = \hat{y}_j \oplus H(\delta_s \parallel K_j) \quad (32)$$

마지막으로, 서버의 개인키 sk_s 를 이용하여 메시지 $\delta_s \parallel Y$ 에 대해서 (29)와 같이 서명을 생성하고,

$$\sigma_s = sign_{pk_s}(\delta_s \parallel Y) \quad (29)$$

$$SK = H(Y \parallel X) \quad (33)$$

$(\delta_s \parallel Y \parallel \sigma_s)$ 를 그룹의 모든 멤버들에게 브로드캐스트 한다.

제안하는 확장 프로토콜의 실행 과정을 간단히 그림 5에 나타내었다. 그림 5에서 보듯이 이 프로토콜은 n 번의 유니캐스트와 $m+2$ 번의 브로드캐스트 통신을 필요로 하고, 3라운드 만에 그룹 통신에 사용될 세션키를 나눠 갖게 된다.

(키 계산.) 모든 $a_j (j \in [1, m])$ 과 그 자식 멤버인 $b_i (i \in I_{a_j})$ 에 대하여, $b_i \in L_2$ 는 $a_j \in L_1$ 로부터 받은 브로드캐스트 메시지에 대해 $a_j \in L_1$ 의 공개키 pk_{a_j} 를 이용하여 서명값 σ_{a_j} 를 검증한 뒤 서명값이 옳다면, 서브 그룹 공통 비밀값 X_j 와 서브그룹키 K_j 를 각각 (30), (31)과 같이 계산한다.

$$X_j = y_{b_i} \oplus H(\delta_{a_j} \parallel (w_j)^{r_{b_i}}) = y_{b_i} \oplus H(\delta_{a_j} \parallel g^{s_{j'b_i}}) \quad (30)$$

$$K_j = H(Y_j \parallel X_j) \quad (31)$$

마지막으로, 모든 $a_j (j \in [1, m])$ 과 $b_i (i \in [1, n])$ 는 서버로부터 받은 브로드캐스트 메시지를 서버의 공개키 pk_s 를 이용하여 서명값 σ_s 를 검증한 뒤 서명값이 옳다면, 전체 그룹의 공통 비밀값 X 와 전체 그룹의 세션키 SK 를 각각 (32), (33)과 같이 계산한다.

V. 효율성 및 안전성 분석

1. 효율성 분석

현재까지, Burmester와 Desmedt가 제안한 BD 프로토콜^[4]이 전방향 안전성을 제공하는 그룹 키 동의 프로토콜 중 가장 효율적인 프로토콜이라고 알려져 있으며, 최근 Nam 등이 유·무선 통합 네트워크 환경에서 효율적인 그룹 키 동의 프로토콜^[3]을 제안하였다. 따라서, 본 논문에서 제안한 프로토콜에 대한 효율성을 BD 프로토콜과 Nam 등의 프로토콜과 비교, 분석한다.

IV장에서 제안한 프로토콜은 표 1에서와 같이, 사용 가능한 전력이 극히 제한적인 무선 단말기 사용자의 계산량 측면에 있어서 매우 효율적이다. 특히, BD 프로토콜과 Nam 등의 프로토콜은 3번의 모듈러 연산을 필요로 하는데 비해 본 논문에서 제안한 프로토콜의 경우는 2번의 모듈러 연산만을 필요로 한다. 그리고

표 1. 제안하는 프로토콜과 BD 프로토콜, Nam 등의 프로토콜 간의 복잡도 비교
Table 1. Complexity comparison with the BD protocol and the protocol of Nam et al.

비교 스킴	계산량	통신량		
	연산 능력이 낮은 무선 단말기 사용자	라운드	유니캐스트	브로드캐스트
BD 프로토콜	$3E + O(t \log t)M$	2		$2t$
Nam 등의 프로토콜	$3E + 2M + 2H$	3	$t - m$	$m + 1$
제안하는 프로토콜	$2E + 4H + 2X$	3	$t - m$	$m + 2$

E : 모듈러 역승, M : 모듈러 곱셈, H : 해쉬 함수, X : XOR

t : 그룹 전체 멤버의 수, m : 유선 사용자 그룹의 수

1라운드에서 필요로 하는 모든 연산을 오프라인상에서 사전에 수행할 수 있기 때문에, 온라인상에서는 오직 1번의 모듈러 역승 연산만을 수행하면 된다. 모듈러 역승 연산은 계산량 오버헤드에 있어서 가장 큰 비중을 차지하는 요소이므로, 제한된 시스템 자원을 갖는 무선 단말기에서의 모듈러 역승 연산을 최소화 하는 것이 필요하다. 또한, 해쉬 함수와 XOR 연산은 모듈러 곱셈 연산에 비해 계산량 오버헤드에 거의 영향을 미치지 않는 요소이므로, 본 논문에서는 BD 프로토콜과 Nam 등의 프로토콜에서 사용된 모듈러 곱셈 연산 대신 해쉬 함수와 XOR 연산을 사용하여 계산 효율성을 보다 높였다.

본 논문에서 제안한 프로토콜은 라운드 수와 메시지 전송량에 있어서도 BD 프로토콜보다 매우 효율적이며 Nam 등의 프로토콜과 같은 성능을 보이고 있다. BD 프로토콜은 $2t$ 개의 브로드캐스트 메시지 전송을 필요로 하는데 비해 본 논문에서 제안한 프로토콜의 경우는 $t - m$ 개의 유니캐스트 메시지와 $m + 2$ 개의 브로드캐스트 메시지 전송을 필요로 하게 된다.

따라서, 충분한 연산 능력을 가진 유선 단말기와 상대적으로 낮은 연산 능력을 가진 무선 단말기가 혼재되어 있는 유·무선 통합 네트워크 환경에서는 본 논문에서 제안한 프로토콜이 BD 프로토콜이나 Nam 등의 프로토콜에 비해서 훨씬 효율적이며 적합한 프로토콜이라고 할 수 있겠다.

2. 안전성 증명

본 절에서 제안한 프로토콜의 수동적 공격자에 대한 안전성을 증명하고자 한다. 확장 프로토콜은 기본 프로토콜에 기반하여 서버와 $a_j \in L_1$ 간의 비밀키 생성 및 $a_j \in L_1$ 와 그 자식 멤버인 $b_i (i \in I_{a_j})$ 간의 서브그룹키를

생성하였다. 그리고 전체 그룹의 세션키를 생성하기 위해서 서브그룹의 $a_j \in L_1$ 가 하나의 멤버로서 다시 그룹에 참여할 때 서버와 $a_j \in L_1$ 간의 비밀키로 서브그룹키를 암호화하여 서버에게 전달해 주었다. 이 때 발생할 수 있는 수동적 공격자에 대한 안전성은 대칭키 암호화 방식에 사용된 키에만 의존하므로 서버와 $a_j \in L_1$ 간의 비밀키를 생성하는 기본 프로토콜의 안전성이 증명된다면 대칭키 암호 방식에 사용된 키에 대한 안전성도 보장이 된다.

따라서, 본 절에서는 기본 프로토콜에 대한 안전성을 증명하고자 한다. 기본 프로토콜의 안전성 증명은 CDH (Computational Diffie-Hellman) 문제의 랜덤 커쳐성을 이용하여 증명할 수 있다.

먼저, $Adv_G^{CDH}(t)$ 를 모든 알고리즘 D 가 t 의 수행시간 동안에 CDH 문제를 해결할 확률값

$$\Pr[g^{ab} \leftarrow D(G, g, g^a, g^b) | g \leftarrow G, a, b \leftarrow \mathbb{Z}_q].$$

들의 최대값이라고 하고, 기본 프로토콜에 대응되는 실제 분포 Real과 랜덤한 난수로 전달된 메시지의 분포인 Fake를 다음과 같이 정의한다.

$$\text{Real} = \left(T, \text{SK}, \begin{cases} r_q, r_{h_1}, \dots, r_{h_n}, r_s, s \in_R \mathbb{Z}_q; \delta \in \{0, 1\}^l; \\ z_q = g^{r_q}, z_{h_1} = g^{r_{h_1}}, \dots, z_{h_n} = g^{r_{h_n}}, z_s = g^s; \\ x_q = g^{x_q}, x_{h_1} = g^{x_{h_1}}, \dots, x_{h_n} = g^{x_{h_n}}, x_s = g^{x_s}; \\ h_q = H(\delta|x_q), h_{h_1} = H(\delta|x_{h_1}), \dots, h_{h_n} = H(\delta|x_{h_n}), h_s = H(\delta|x_s); \\ X = \bigoplus_{i=1}^n h_i \oplus h_s; \\ y_q = X \oplus h_q, y_{h_1} = X \oplus h_{h_1}, \dots, y_{h_n} = X \oplus h_{h_n} \end{cases} \right)$$

$$\text{Fake} = \left\{ \begin{array}{l} r_{a_1}, r_{b_1}, \dots, r_{b_n}, r_s, s \in_R \mathbb{Z}_q; \\ \delta, w_{a_1}, w_{b_1}, \dots, w_{b_n}, w_s \in \{0,1\}^l; \\ z_{a_1} = g^{r_{a_1}}, z_{b_1} = g^{r_{b_1}}, \dots, z_n = g^{r_{b_n}}, z_s = g^s; \\ h_{a_1} = w_{a_1}, h_{b_1} = w_{b_1}, \dots, h_{b_n} = w_{b_n}, h_s = w_s; \\ X = \bigoplus_{i=1}^n h_{b_i} \oplus h_{a_1} \oplus h_s; \\ y_{a_1} = X \oplus h_{a_1}, y_{b_1} = X \oplus h_{b_1}, \dots, y_{b_n} = X \oplus h_{b_n} \end{array} \right\},$$

여기서 a_1, b_1, \dots, b_n 은 프로토콜에 참가하는 그룹 멤버이며, $T = (z_{a_1}, z_{b_1}, \dots, z_{b_n}, \delta, y_{a_1}, y_{b_1}, \dots, y_{b_n})$ 은 전달메시지이고 $SK = H(y_{a_1}, y_{b_1}, \dots, y_{b_n} \| X)$ 는 그룹키이다.

(보조정리 1.) Real과 Fake를 구별하는 임의의 PPT 알고리즘 D 의 능력은 CDH 문제의 어려움에 의해 다음과 같이 제한된다.

$$\begin{aligned} & \Pr[D(T, SK) = 1 | (T, SK) \leftarrow \text{Real}] - \\ & \Pr[D(T, SK) = 1 | (T, SK) \leftarrow \text{Fake}] \\ & \leq \frac{1}{q_h} Adv_G^{CDH}(t + 2(n+2)t_{\text{exp}}) \end{aligned}$$

여기서, t 는 알고리즘 D 의 수행시간이며 t_{exp} 는 순환군 G 에서 한 번의 덕승을 계산하는데 필요한 시간을 의미한다.

(증명.) CDH 문제의 랜덤 귀착성을 이용하여 증명한다.

먼저, 세 값 $(g, A = g^r, B = g^\alpha) \in G^3$ 이 주어졌을 때, $r\alpha = \beta \pmod{q}$ 인 $C = g^\beta$ 값을 출력하는 알고리즘을 구성한다. 그런 다음, 임의의 $\gamma_{a_1}, \gamma_{b_i} \in \mathbb{Z}_q$ 를 선택하여, 지수를 $r_{a_1} = \alpha + \gamma_{a_1} \pmod{q}$, $r_{b_i} = \alpha + \gamma_{b_i} \pmod{q}$ 로 정의 하면 $z_{a_1} = Bg^{\gamma_{a_1}}, z_{b_i} = Bg^{\gamma_{b_i}}$ 로 계산할 수 있고, l 비트의 랜덤한 $h_{a_1}, h_{b_i} \in \{0,1\}^l$ 로 $X = \bigoplus_{i=1}^n h_{b_i} \oplus h_{a_1} \oplus h_s$ 를 계산하여, $y_{a_1} = X \oplus h_{a_1}, y_{b_i} = X \oplus h_{b_i}$ 를 구성할 수 있다. 즉, 다음과 같은 분포를 구성할 수 있다.

$$\text{Dist} = \left\{ \begin{array}{l} \gamma_{a_1}, \gamma_{b_1}, \dots, \gamma_{b_n}, \gamma_s, x'_{a_1}, x'_{b_i} \in_R \mathbb{Z}_q; \\ \delta, h_{a_1}, h_{b_1}, \dots, h_{b_n}, h_s \in \{0,1\}^l; \\ r_{a_1} = \alpha + \gamma_{a_1}, r_{b_1} = \alpha + \gamma_{b_1}, \dots, r_{b_n} = \alpha + \gamma_{b_n}, r_s = \alpha + \gamma_s; \\ z_{a_1} = Bg^{\gamma_{a_1}}, z_{b_1} = Bg^{\gamma_{b_1}}, \dots, z_{b_n} = Bg^{\gamma_{b_n}}, z_s = Bg^{\gamma_s}; \\ X = \bigoplus_{i=1}^n h_{b_i} \oplus h_{a_1} \oplus h_s; \\ y_{a_1} = X \oplus h_{a_1}, y_{b_1} = X \oplus h_{b_1}, \dots, y_{b_n} = X \oplus h_{b_n} \end{array} \right\},$$

여기서 T 와 SK 는 Real과 Fake에서 정의된 것과 같

다. 이 구성으로부터 모든 $b_i \in [1, n]$ 와 a_1 에 대하여 $z_{b_i} = g^{r_{b_i}} (= Bg^{\gamma_{b_i}}), z_{a_1} = g^{r_{a_1}} (= Bg^{\gamma_{a_1}})$ 이므로 $\text{Disk} \equiv \text{Fake}$ 가 성립한다. 결국 Real과 Fake를 구별하는 알고리즘 D 의 능력은 CDH 문제의 어려움에 의해서 제한되어 기껏해야 $\frac{1}{q_h} Adv_G^{CDH}(t + 2(n+2)t_{\text{exp}})$ 의 성공률을 가지게 된다.

(보조정리 2.) 공격자 A 에게 임의의 값 SK_b 와 Fake로부터 선택된 전달 메시지 T 가 주어진다고 가정하자. 이 때 SK_b 가 Fake로부터 T 와 함께 선택된 값인지 또는 T 와 관련이 없는 임의의 랜덤 값인지를 구별할 확률은 모든 공격자 A 에 대하여 정확히 $1/2$ 이다. 즉,

$$\Pr[A(T, SK_b) = b | (T, SK_1) \leftarrow \text{Fake}; \\ SK_0 \leftarrow \{0,1\}^l; b \leftarrow 0, 1] = 1/2.$$

(증명.) Fake실험에서, 전달 메시지 T 로부터 $y_{a_1}, y_{b_i} (i \in [1, n])$ 를 다음과 같이 나타낼 수 있다.

$$\begin{aligned} y_{a_1} &= h_{b_1} \oplus h_{b_2} \oplus h_{b_3} \oplus \dots \oplus h_{b_n} \oplus h_s = h_{a_1} \oplus h_s \oplus y_s, \\ y_{b_1} &= h_{b_2} \oplus h_{b_3} \oplus h_{b_4} \oplus \dots \oplus h_{b_n} \oplus h_s = h_{b_1} \oplus h_s \oplus y_s, \\ &\vdots \\ y_{b_n} &= h_{b_1} \oplus h_{b_2} \oplus h_{b_3} \oplus \dots \oplus h_{n-1} \oplus h_s = h_{b_n} \oplus h_s \oplus y_s \end{aligned}$$

즉, 위의 식을 만족하는 해 $(h_{a_1}, h_{b_1}, h_{b_2}, \dots, h_{b_n})$ 의 형태는 다음과 같이 고쳐 쓸 수 있다.

$$\begin{aligned} h_{a_1} &= y_{a_1} \oplus y_s \oplus h_s \\ h_{b_1} &= y_{b_1} \oplus y_s \oplus h_s \\ &\vdots \\ h_{b_n} &= y_{b_n} \oplus y_s \oplus h_s \end{aligned}$$

따라서 해의 개수는 주어진 독립변수 h_s 값이 취할 수 있는 집합의 크기인 2^l 만큼의 해가 존재하므로 개별적인 메시지 정보로부터 공격자는 X 에 대한 어떤 정보도 얻지 못한다. 이로부터 다음의

$$\Pr[A(T, X_b) = b | (T, X_1) \leftarrow \text{Fake}; \\ X_0 \leftarrow \{0,1\}^l; b \leftarrow \{0,1\}] = 1/2,$$

을 얻을 수 있으며, H 가 랜덤 오라클이므로 보조정리 2의 식이 참임을 알 수 있다.

(정리 1.) A 를 t 의 수행시간을 갖는 수동적 공격자라고 하자. A 에게 Q 개의 프로토콜 실행 메시지가 주어진다고 할 때, 프로토콜의 안전성은 다음 식에 의해 보장된다.

$$\Pr[A(T, SK_b) = b | (T, SK_1) \leftarrow \text{Real}; \\ SK_0 \leftarrow \{0,1\}^l; b \leftarrow \{0,1\}] \leq \\ 1/2 + Adv_G^{CDH}(t'),$$

여기서 $t' = t + O((n+2)Qt_{\exp})$ 이고, t_{\exp} 는 G 에서 멱승을 계산하는데 필요로 하는 시간이다.

(증명.) 앞에서 살펴본 보조정리 1과 보조정리 2, 그리고 CDH 문제의 랜덤 귀착성에 의해서 정리 1이 성립됨을 쉽게 알 수 있다.

VI. 결 론

그룹 키 동의 프로토콜에 관한 연구는 그동안 많은 연구자들에 의해 다양한 관점에서 진행되어 왔으며, 최근 들어 유·무선 통합 네트워크 기술이 발전하면서 이와 같은 새로운 환경에서의 안전한 그룹 통신을 위한 그룹 키 동의 프로토콜에 대한 연구가 진행되고 있다.

유·무선 통합 네트워크 환경에 적합한 그룹 키 동의 프로토콜을 설계하기 위해서는 고성능 연산 능력을 가진 유선 단말기의 특성과 상대적으로 계산능력이 떨어지는 무선 단말기의 특성이 함께 고려되어야 하며 특히, 시스템 자원의 제한성을 갖는 무선 단말기에서의 계산량을 최소화하는 문제는 그룹 키 동의 프로토콜 설계에 있어서 무엇보다 중요하다. 이에 본 논문에서는 무선 단말기에서의 계산량을 최소화하면서도 유·무선 통합 네트워크 환경에 적합한 효율적이고 안전한 그룹 키 동의 프로토콜을 제안하였다.

제안하는 프로토콜은 무선 단말기에서의 계산 효율성이 뛰어나 차세대 유·무선 통합 네트워크 환경에서의 다양한 멀티미디어 서비스는 물론 여러 가지 그룹 응용서비스에 활용될 수 있을 것으로 기대된다.

참 고 문 현

- [1] I. Ingemarsson, D. Tang, and C. Wong, "A Conference Key Distribution System", IEEE Transactions on Information Theory, Vol. 28, no. 5, pp. 714-720, September, 1982.
- [2] W. Diffie and M. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, Vol. 22, no. 6, pp. 644-654, November, 1976.
- [3] J. Nam, S. Kim, and D. Won, "Secure Group Communications over Combined Wired and Wireless Networks", Proceedings of TrustBus 2005, International Conference on Trust, Privacy, and Security in Digital Business (in conjunction with DEXA 2005), Springer-Verlag, LNCS 3592, pp. 90-99, August, 2005.
- [4] M. Burmester and Y. Desmedt, "A secure and Efficient Conference Key Distribution System", Advances in Cryptology-Eurocrypt'94, Springer-Verlag, LNCS 950, pp.275-286, 1995.
- [5] M. Steiner, G. Tsudik and M. Waidner, "Diffie-Hellman Key Distribution Extended to Group Communication", Proceedings of the 3rd ACM Conference on Computer and Communications Security (CSS'96), pp.31-37, May, 1996.
- [6] J. Katze and M. Yung, "Scalable Protocols for Authenticated Group Key Exchange", Advances in Cryptology-Crypto'03, Springer-Verlag, LNCS 2729, pp. 110-125, August, 2003.
- [7] K. Becker and U. Wille, "Communication Complexity of Group key Distribution", Proceedings of the 5th ACM Conference on Computer and Communications Security (CCS'98), pp. 1-6, November, 1998.
- [8] Y. Kim, A. Perrig and G. Tsudik, "Communication-efficient Group Key Agreement", Proceedings of International Federation for Information Processing (IFIP SEC'01), Springer- Verlag, LNCS 1163, pp. 229-244, June, 2001.
- [9] E. Bresson, O. Chevassut, A. Essiari, and D. Pointcheval, "Mutual authentication and group key agreement for low-power mobile devices", Proceedings of the 5th IFIP-TC6/IEEE International Conference on Mobile and Wireless Communications Networks (MWCN'03), pp. 59-62, October, 2003.
- [10] J. Nam, S. Kim, and D. Won, "A Weakness in the Bresson-Chevassut-Essiari-Pointcheval's Group Key Agreement Scheme for Low-Power Mobile Devices", IEEE Communications Letters, Vol. 9, no. 5, pp. 429-431, May, 2005.
- [11] J. Nam, J. Lee, S. Kim, and D. Won, "DDH-based Group Key Agreement in a Mobile Environment", Journal of Systems and Software, Vol. 78, no. 1, pp. 73-83, October, 2005.
- [12] S. Cho, J. Nam, S. Kim, and D. Won, "An Efficient Dynamic Group Key Agreement for Low-Power Mobile Devices", Proceedings of ICCSA 2005, International Conference on Computational Science

- and Applications, Springer-Verlag, LNCS 3480, pp. 498–507, May, 2005.
- [13] T. Phan, L. Huang, and C. Dulan, "Challenge: Integrating Mobile Wireless Devices into the Computational Grid", Proceedings of the 8th ACM Conference on Mobile Computing and Networking (MOBICOM'02), pp.271–278, September, 2002.

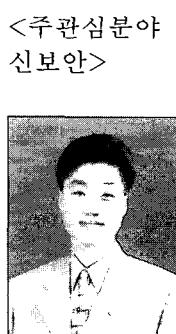
저 자 소 개



장 우석(정희원)-주저자
2005년 전국대학교 소프트웨어
공학과 학사 졸업.
2005년 ~ 현재 성균관대학교
컴퓨터공학과 석사과정.
<주관심분야 : 암호 프로토콜, 네
트워크 보안, DRM, 정보보호>



김현주(정희원)
1995년 세명대학교
수학과 학사 졸업.
1997년 서강대학교 대학원
수학과 석사 졸업.
2005년 성균관대학교 대학원 전기
전자 및 컴퓨터공학과
박사 졸업.



남정현(정희원)
1997년 성균관대학교 정보공학과
학사 졸업.
2002년 M. S., Computer Science,
University of Louisiana,
Lafayette
2006년 성균관대학교 컴퓨터
공학과 박사 졸업.



김승주(정희원)-교신저자
1990년 ~ 1999년 성균관대학교 정보공학과 학사, 석사, 박사 졸업.
1998년 ~ 2004년 한국정보보호진흥원(KISA) 팀장.
2004년 ~ 현재 성균관대학교 정보통신공학부 교수.
2001년 ~ 현재 한국정보보호학회, 한국인터넷정보학회,
한국정보과학회, 한국정보처리학회 논문지 및 학회지 편집위원.
2002년 ~ 현재 한국정보통신기술협회(TTA) IT 국제표준화 전문가.
2005년 ~ 2006년 6월 교육인적자원부 유해정보차단 자문위원.
2005년 ~ 현재 디지털콘텐츠유통협의체 보호기술워킹그룹 그룹장, 한국우주통신연구소
암호연구회 운영위원.
<주관심분야: 암호이론, 정보보호표준, 정보보호제품 및 스마트카드 보안성 평가, PET>



조석향(정희원)
1986년 이화여자대학교
수학과 학사 졸업.
1986년 ~ 1998년 (주)중앙교육진흥
연구소 근무.
2001년 서울산업대학교 전자계산
학과 석사 졸업.
2001년 ~ 현재 성균관대학교 정보통신공학부
박사과정.
<주관심분야 : 암호 프로토콜, 암호이론, 정보보
안>



원동호(정희원)
1976년 ~ 1988년 성균관대학교
전자공학과 학사, 석사,
박사 졸업.
1978년 ~ 1980년 한국전자통신
연구원 전임연구원.
1985년 ~ 1986년 일본 동경공업대
객원연구원.
1988년 ~ 2003년 성균관대학교 교학처장, 전기
전자 및 컴퓨터공학부장, 정보통신대학
원장, 정보통신기술연구소장, 연구처장.
1996년 ~ 1998년 국무총리실 정보화추진위원회
자문위원.
2002년 ~ 2003년 한국정보보호학회 회장.
현재 성균관대학교 정보통신공학부 교수,
한국정보보호학회 명예회장, (정통부지정 ITRC)
정보보호인증기술연구센터 센터장.
<주관심분야 : 암호이론, 정보이론, 정보보호>