http://dx.doi.org/10.14400/JDC.2014.12.3.237

# 클라우드 컴퓨팅 환경에 적합한 그룹 키 관리 프로토콜

김용태*, 박길철**
한남대학교 멀티미디어학부*, **

# Group key management protocol adopt to cloud computing environment

**Yong-Tae Kim*, Gil-Cheol Park****
**Department of Multimedia Engineering, Hannam University*, ****

요 약 IT 서비스 및 컴퓨팅 자원을 기반으로 인터넷 서비스를 제공하는 클라우드 컴퓨팅이 최근 큰 관심을 받고 있다. 그러나 클라우드 컴퓨팅 시스템에 저장되는 데이터는 암호화한 후 저장되어도 기밀 정보가 유출되는 문제점이 있다. 본 논문에서는 사용자가 클라우드 컴퓨팅 시스템에서 제공되는 데이터를 제 3자가 임의로 악용하는 것을 예방하기 위한 그룹 키 관리 프로토콜을 제안한다. 제안된 프로토콜은 임의의 사용자가 원격에서 클라우드 컴퓨팅 서버에 접근할 경우 서버에 존재하는 사용자 인증 데이터베이스내 사용자 정보를 일방향 해쉬 함수와 XOR 연산을 사용하여 사용자 인증을 제공받는다. 도한 사용자의 신분확인 및 권한을 연동하여 클라우드 컴퓨팅 시스템에 불법적으로 접근하는 사용자를 탐색함으로써 클라우드 컴퓨팅의 사용자 보안 문제를 해결하고 있다.

주제어 : IMD, 키 분배, 프로토콜, RSA

**Abstract** Recently, wind energy is expanding to combination of computing to forecast of wind power generation as well as intelligent of wind powerturbine. Wind power is rise and fall depending on weather conditions and difficult to predict the output for efficient power production. Wind power is need to reliably linked technology in order to efficient power generation. In this paper, distributed power generation forecasts to enhance the predicted and actual power generation in order to minimize the difference between the power of distributed power short-term prediction model is designed. The proposed model for prediction of short-term combining the physical models and statistical models were produced in a physical model of the predicted value predicted by the lattice points within the branch prediction to extract the value of a physical model by applying the estimated value of a statistical model for estimating power generation final gas phase produces a predicted value . Also, the proposed model in real-time National Weather Service forecast for medium-term and real-time observations used as input data to perform the short-term prediction models.

**Key Words :** IMD, Key Distribution, Protocol, RSA

## 1. 서론

클라우드 컴퓨팅은 최근 IT 서비스와 컴퓨터 자원을 인터넷 기반으로 서비스를 제공하면서 많은 관심을 받고 있다[1]. 클 라우드 컴퓨팅이 널리 관심을 받은 이유는 컴퓨터 기술의 발달이 글로벌 기업들의 전략적 투자 전략

Received 6 January 2014, Revised 17 February 2014
Accepted 20 March 2014
Corresponding Author: Gil-Cheol Park (Department of Multimedia Engineering, Hannam University)
Email: gcpark@hnu..kr

ISSN: 1738-1916

과 맞물려 급속하게 파산되면서 서로 다른 물리적인 위치에 존재하는 무형의 형태로 존재하는 하드웨어, 소프트웨어 등의 컴퓨팅 자원을 가상화 기술을 통해 통합할 수 있기 때문이다[2].

클라우드 컴퓨팅은 기존 시스템에 잠재되어 있던 보안 위협과 새로운 형태의 보안 위협에 노출되어 있어 서버가 해킹당할 경우 개인정보가 유출될 수 있고 서버 장애가 발생하면 자료 이용이 불가능하다.

최근 모바일 클라우드가 다양한 분야로 확산되면서 다양한 디바이스 플랫폼 및 운영체제에서는 기존에 사용되던 패스워드 인증 방식대신 2-factor 인증방식을 사용한다. 그 이유는 기존 방식이 낮은 보안성, 비사용, 재사용, 공유, 망각, 도난, 입력 어려움, 키 로깅, 중간자 공격 취약점 등 다양한 보안 문제점이 존재하기 때문이다[3].

현재까지 클라우드 컴퓨팅 환경에서 사용되고 있는 가상 및 클라우드 플랫폼의 보안 공격은 매우 용이하지만 보호는 매우 어려운 상황이다. 기업이 이를 위한 보안 기술을 수용하게 되면서 기업의 중요한 데이터를 보호해야 하는 IT 관리자는 더 큰 부담을 안고 있다. 엄청난 규모의 가상화 서버에 대한 패칭 작업은 결코 쉬운 일이 아니며 해커들이 서버를 탈취하고 트래픽을 방해하고 취약한 시스템에서 데이터를 훔칠 수 있는 여지를 제공할 수 있다.

대부분의 클라우드 서비스는 PC에 국한돼 제공되고 있으며 모바일 단말기를 지원할 경우 특정 단말에 한정되어 있어 클라우드 서비스가 원활하게 지원되고 있지 않다. 따라서 기존 클라우드 서비스를 모바일로 서비스를 제공받으려면 각각 별도로 개발해야 하는 어려움이 있다. 향후 모바일 클라우드 시대가 되면 다양한 단말 기기에서 공통으로 서비스해야 할 수요가 커질 것이며 이를 위해 단말기의 독립적인 서비스가 요구된다[5,6].

이 논문에서는 클라우드 컴퓨팅 환경에서 주로 사용하고 있는 사전키 분배 방식에서의 확률적 키에 의존하는 문제를 키 재사용/추가에 유연성을 갖는 ID 기반 대칭키 기법을 확장한 키 관리 프로토콜을 제안한다. 제안 프로토콜은 클라우드 환경에 적합하도록 키 사전 배치 전 공유키를 사용하여 사용자의 키 전송/수용 과정을 제거하여 키 관리 측면에서 효율성을 높이고 있다. 또한 네트워크상에 존재하는 타협된 노드들을 탐지하기 위해 lightweight 침입 탐지 메커니즘 기능을 적용함으로써 안전성 문제를 해결한다. 특히, 제안 프로토콜은 서버의 효율성 뿐만 아니라 비용 절감을 위해서 내부 사용자의 인증을 분산 처리하며 외부 사용자는 클라우드 플랫폼이 제공하는 통합 인증 시스템을 이용하여 서버내의 시스템에 접근한다. 또한 제안 프로토콜은 클라우드 컴퓨팅에서 분산 처리된 개인 정보를 모두 중앙에 위치한 서버에 중앙 집중하여 클라우드 컴퓨팅의 사용자 보안 문제를 해결하고 있다.

이 논문의 구성은 다음과 같다. 2장에서는 클라우드 컴퓨팅과 클라우드 환경의 키 관리 프로토콜에 대해서 알아본다. 3장에서는 클라우드 컴퓨팅 환경을 위한 키 관리 프로토콜을 제안한다. 4장에서는 제안 기법의 보안성을 분석하고 마지막으로 5장에서 결론을 맺는다.

## 2. 관련연구

### 2.1 클라우드 컴퓨팅

클라우드 컴퓨팅은 언제, 어디서나 컴퓨팅 자원을 필요에 따라 차용하여 네트워크를 통해 다양한 방식으로 접근하는 서비스를 의미한다[1,2].

클라우드 컴퓨팅은 소프트웨어, 스토리지, 네트워크 등 사용 가능한 대부분의 컴퓨팅 자원들을 필요한 만큼 제공받아 사용하고 서비스 종류에 따라 SaaS(Software as a Service), PaaS(Platform as a Service), IaaS (Infrastructure as a Service) 등으로 사용한다.

최근까지 IT 기술의 꾸준한 발달로 인하여 클라우드 컴퓨팅을 위한 인증 연구 또한 꾸준히 연구되고 있다[7]. Shoup-Rubin[8]은 3개의 키 분배 프로토콜에 기반한 Bellare-Rogaway 모델[9]을 확장한 기법이다. 이 기법은 스마트카드에서 사용되는 비밀키가 길어 제 3자로부터 스마트카드가 타협(compromised)되지 않는 장점은 있지만 두 객체 중 하나의 객체가 타협되면 안전하지 않은 단점이 있다. Liao et. al. [7] 은 패스워드의 수와 속성에 기반한 스마트카드를 통합하여 인증을 수행하는 기법을 제안하였다. 이 같은 이유는 클라우드 컴퓨팅에서 클라이언트-서버 구조가 다양하여 기존 클라이언트-서버의 인터 네트워크 시스템보다 강한 인증이 필요하기 때문이다. Lee et. al.[10]은 클라우드 컴퓨팅에서 인증을 위한 공개키와 이동 대역폭을 제안하였다. 그러나 이 기법은 인식

자(identifier), 패스워드 그리고 PKI 등의 데이터를 평문으로 전달하여 공격자가 데이터를 쉽게 가로챌 수 있는 단점이 있어 실시간 클라우드 컴퓨팅 환경에 부적합하다. Li et. al.[11]는 클라우드 컴퓨팅 시스템이 서비스를 지원하기 위한 신뢰된 플랫폼(trusted platform)과 조합된 이론적 프로토타입 시스템을 제안하였다.

### 2.2 클라우드 키 관리 기법

Eschenauer-Gigor기법을 기반으로 [12]은 이들 방법에 q-composite 랜덤 키 사전 분배 방법을 적용하여 키 셋업에 대한 보안성을 강화하였다. 그러나 이 기법은 센서 네트워크 특성을 고려하지 않고, 확률적으로 랜덤하게 키를 분배하므로 센서 노드간의 공유키가 존재하지 않을 가능성이 매우 높다. 또한 공유키가 존재하더라도 공유키를 발견하는데 소용되는 시간과 에너지가 많아 에너지 사용이 효율적이지 못하다.

Blundo는 노드 사이의 충돌에 대해서 안전하도록 공통키를 계산하기 위해서 $t$ 파티 그룹으로 여러 기법들을 제안하였다[13]. 이 기법들은 메모리 소비가 그룹 멤버에 있지 않도록 통신 비용을 줄이는데 초점을 가진다.

[14]에서는 두 통신 주체 사이에 키를 공유하기 전에 클러스터 헤드가 자신의 멤버 호스트들을 대신하여 인증을 수행하는 방법이 제안되었다. 이 방법에서는 임의의 두 클러스터 헤드가 각자 상대편 클러스터 헤드의 공개키를 이용하여 상호인증을 수행한다. 따라서 클러스터 헤드의 공개키가 먼저 모든 클러스터 헤드에 분배되어 있어야 한다. 클러스터 헤드 간 인증 후에 대칭키 기반의 세션키가 분배되고, 이는 다시 통신 주체인 멤버 호스트에게 분배된다. 이 방법은 클러스터 헤드들이 자신의 공개키를 모든 클러스터 헤드에게 분배해야 하므로 통신 오버헤드가 크다. 또한 두 멤버 호스트간 비밀키인 세션키 분배 시 헤드의 개인키로 암호화되어 해당 노드에 분배함으로써 세션키가 클러스터 내의 모든 호스트들에게 노출 될 수 있다.

Khalili[15]는 ID 기반 암호화 기법의 편리성과 효율성, 임계치 암호화 기법의 유연성 및 안전성의 이점을 결합하여 Ad Hoc 네트워크에서 각 노드의 공개키와 개인키를 생성하는 기법을 제안하였다. 이 방식은 노드가 네트워크에 참여할 때 공통적으로 분배받는 마스터 공개키와 공개되어 있는 호스트의 ID로 해당 노드의 공개키를 유도하고 임계 개수만큼 주변 노드들로부터 ID에 해당하는 부분 개인키를 얻어내어 완전한 개인키를 획득한다. 그러나 이 방식은 비밀키를 요청하는 주체를 분명히 인증하지 못하므로 중간자 공격에 매우 취약하다.

## 3. 클러스터 기반의 키 관리

이 논문에서 제안하는 클라우드 환경의 키 관리 프로토콜은 클러스터 기반의 대칭키를 사용하며, 사용자와 서버 사이에 안전한 통신을 위해 사전에 설정된 키들을 이용하여 프로토콜을 제공한다.

### 3.1 가정

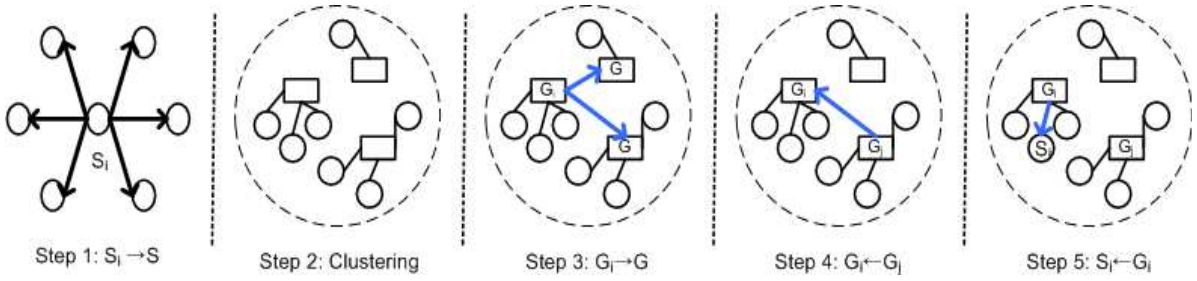
제안 프로토콜에서 사용자와 서버 사이의 동작에 대한 가정은 다음과 같다. 사용자는 신뢰성이 있다거나 악의적으로 사용할 수 있다는 가정을 만들지 않는다. 네트워크상에 존재하는 모든 자료들은 직접 통신을 통해 접근가능하다. 또한 네트워크 사이에는 안전한 그룹통신을 한다고 가정한다. 통신에 사용되는 클러스터링 알고리즘[10]은 안전한 통신 설정을 할 수 있도록 쉽게 확장할 수 있다. 제안 프로토콜은 그룹 키 동의 프로토콜을 사용하여 그룹키를 설치할 수 있다. 서버는 클라우드 컴퓨팅 환경의 모든 사용자들에 대해서 안전하고 신뢰적이라고 가정한다. 침입탐지 메커니즘은 서버에서 완벽하게 동작하고, 약속된(타협된) 사용자의 제거는 침입탐지 메커니즘에 따른다.

### 3.2 클러스터링 과정

클라우드 서버에 저장되어 있는 데이터를 사용자가 요청하게 되면 접속시간과 종료시간이 체크되도록 타이머가 동작되어 모든 사용자들은 타이머가 만기되기 전에 데이터를 수신하게 된다. 만약 그렇지 않은 경우에는 클라우드 서버는 자동으로 사용자의 데이터 수신을 종료한다.

### 3.3 키 관리 프로토콜

클라우드 컴퓨팅 환경에서 데이터를 사용자가 안전하게 수신받기 위한 방법으로 제안 프로토콜에서는 키 분배/추가/폐기/갱신 등의 4개 하부 프로토콜이 수행된다.




[Fig. 1] Initial Protocol Operation Process

3.3.1 키 분배

클라우드 서버에서 사용자에게 키를 분배하기 위해서는 우선 사전분배 방식을 통해 사전에 2개의 키를 사용자가 보유한다. 사용자가 보유한 키 중 하나는 사용자 그룹과 공유하고 다른 하나는 클라우드 서버와 공유한다. 사용자 개인은 신뢰적이지만 적은수의 키만을 가지고 있는데 반해 그룹내 사용자들은 많은 수의 키를 보유하지만 신뢰적인 못한다. 클라우드 서버는 안전하다고 가정하고 사용자들과의 모든 비밀키를 보유한다.

클라우드 서버에서 키를 분배하기 위한 초기 구문의 동작 과정은 [그림 1]과 같다.

- 단계 1 : 모든 사용자는 클라우드 서버로부터 공유키를 얻기 위해 그룹관리자의 식별번호를 사전에 전달받는다.
- 단계 2 : 클라우드 서버로부터 동일한 데이터를 전달받는 사용자들을 클러스터링 하는 과정으로써, 사용자들은 클러스터링 메커니즘을 사용하여 클러스터한다.
- 단계 3 : 클러스터 형성이 끝나면 클러스터 내에 존재하는 사용자들은 비밀키와 인식자를 가지고 이웃 클러스터 그룹에게 알린다.
- 단계 4 : 클러스터가 형성된 타 그룹을 인식하기 위해서 티켓(ticket)을 부여하여 전송한다. 이때, 티켓을 이용하는 것은 네트워크에 존재하는 타협된 노드들을 안전하게 탐지할 수 있는 역할을 수행하기 위해서이다.
- 단계 5 : 그룹내 사용자들은 서버로부터 데이터를 정상적으로 수신을 받는다.

3.3.2 키 추가

클라우드 컴퓨팅 환경에서 사용자들은 인위적으로 클라우드 서버에 접속하여 데이터를 수신한다. 이 때, 사용자들은 클러스터에 참여하는 다른 사용자들과 동일하게 두 개의 키를 할당받는다. 클라우드 서버는 새로 클러스터에 추가된 사용자의 키를 클러스터내 사용자들과 공유할 수 있도록 (인식자, 키) 쌍을 전송한다.

- 단계 1 : 사용자는 클러스터 그룹에 참여하기 위한 'hello' 메시지를 브로드캐스트한다.
- 단계 2 : 사용자들은 클러스터링 메커니즘을 통해 클라우드 서버로부터 동일 데이터를 전달받은 사용자들을 클러스터한다. 이 과정에서 클러스터링 메커니즘은 클러스터 재구성에 의해서만 적용된다.
- 단계 3 : 각각의 클러스터는 클러스터 범위내에 있는 사용자들에게 그룹 키를 브로드캐스트한다.
- 단계 4 : 사용자는 새로운 그룹키를 할당받아 그룹내 사용자가 공유한다.

3.3.3 키 폐기(철회)

클라우드 컴퓨팅 환경에서 서비스를 중지하기 위해서는 키 폐기 과정을 수행한다. 이 과정은 타협 사용자를 탐지한 후에 수행되며 침입탐지 메커니즘은 타협 사용자의 명령 노드에게 통보한다. 클러스터 그룹이 타협(compromised)된다면 모든 사용자의 리스트를 제거한다.

- 단계 1 : 클라우드 컴퓨팅 환경에서 탈퇴하는 사용자가 발생할 경우 사용자는 클라우드 서버에게 탈퇴 요청 메시지를 전달한다.
- 단계 2 : 클라우드 서버는 탈퇴하는 사용자가 속한 클러스터의 그룹키를 새로 갱신하여 클러스터 그

룹내 사용자에게 그룹키를 전달한다.

- 단계 3 : 클러스터내 속한 사용자는 클라우드 서버에게 전달받은 그룹키를 수신하여 새로운 클러스터링 과정을 수행한다.
- 단계 4 : 클러스터링 과정이 끝난 후 새로운 그룹키가 만들어지면 새로 생성된 그룹키를 클라우드 서버에게 전달한다.

3.3.4 키 갱신

클라우드 환경에서 사용자가 서비스를 요구하고 취소하는 과정이 수시로 이루어지기 때문에 해당 서비스에 따라 키를 수시로 갱신한다. 경우에 따라서는 클러스터 그룹을 위해 암호키를 새로 만들 필요가 있다. 클러스터내 사용자의 키를 갱신하기 위해서는 클라우드 서버가 키 갱신과 철회와 같은 경우가 발생할 경우 키를 클라우드 그룹내 사용자에게 전달한다. 연속적인 갱신이 발생할 경우 시간 간격을 두어 키를 갱신하도록 한다.

## 4. 평가

클라우드 컴퓨팅 환경에서 사용자가 데이터를 안전하게 전달받도록 키를 관리하는 측면에서의 안전성을 평가한다. 제안 프로토콜에서는 (IP address, key) 묶음 정보의 안전성을 보장받도록 비밀키 암호 알고리즘과 해쉬함수의 두 번째 사전 이미지 저항 속성에 의존한다. 비밀키 암호시스템은 제안 프로토콜의 보안 요구사항에 효과적이다. 더욱이 MD5나 SHA-1이 판독되는 두 번째 사전 이미지 저항과 64비트의 출력을 가지는 해쉬함수는 (만일 우리가 64비트중 하나를 보관하고 있다면) 공격자가 주어진 IP 지역의 두 번째 비밀키를 찾기 위해 평균 $2^{62}$ 번 시도한다. 제안 프로토콜은 공격자가 빠른 작업처리를 하지 못하게 할 뿐만 아니라 공격자가 시도한 비밀키에 대해 인위적인 추측이 불가능하다. 만약 공격자가 해쉬함수 입력에 대한 추측을 한다면 두 번째 pre-image resistant 해쉬 함수를 빠르게 처리하여 실제 공격자가 사용하지 못하도록 한다. 해쉬 함수에 대한 생일공격이 제안 프로토콜의 함수 사이에서 발생하더라도 제안 프로토콜은 입력이 $2^{32}$ 시도만큼 유일 분포로 나타나고, 임의 두 노드 사이에서 충돌할 노드의 수는 $10^9$ 노드 순서에 의해서만 존재하기 때문에 제안 프로토콜은 해쉬함수에 대한 생일공격에 안전하다.

## 5. 결론

최근 클라우드 컴퓨팅 환경의 보안성을 확보하기 위하여, 클라우드 서버와 사용자 간에 데이터를 암호화하고 인증하는 것이 중요시되고 있다. 이 논문에서는 클라우드 컴퓨팅 환경에서 사용자간 클러스터링을 통해 그룹 공유키 분배 문제를 확률적 키에 의존하지 않는 새로운 키 관리 프로토콜을 제안하였다. 제안 프로토콜은 클러스터내 사용자간 공유된 공유키를 이용하여 사용자의 데이터 수신시 키 전송/수용 과정을 제거하였기 때문에 키 관리 측면에서 효율적이다. 또한 네트워크상에 존재하는 타협된 사용자들을 탐지하기 위해 lightweight 침입탐지 메커니즘 기능을 프로토콜에 적용하여 노드의 안전성 문제를 해결하였다. 앞으로 제안 프로토콜에 키 중복 비용 부분을 함께 접목시키는 방안과 재클러스터링을 통하여 클라우드 서버내 저장된 사용자 정보의 동기화 문제를 개선에 대한 연구를 수행할 계획이다.

## REFERENCES

[1] D. W. Kim, J. W. Han, and K. I. Chung(2009), "Trend of Home Device Authentication/ Authorization Technology", Weekly IT BRIEF, No. 1329, pp. 1-11.

[2] S.Y. Lee, K.B. Yim, K.J. Bae, Taeyoung Jeong, and Jong-Wook Han(2009), "Counterplan of Ubiquitous Home Network Privacy based on Device Authentication and Authorization," Korea Institute of Information Security & Cryptology, Review of KIISC, 18(5), pp.125-131.

[3] D. Halperin, T. S. Heydt-Benjamin, B. Ransford et al.(2009), "Pacemakers and implantable cardiac defibrillators: software radio attacks and zero-power defenses", in Proc. of SP'08, pp. 129-142.

[4] W. Jansen, and T. Grance(2011), “Guidelines on Security and Privacy in Public Cloud Computing”.
[5] M. Mannan, B. H. Kim, A. Ganjali, and D. Lie(2011), “Unicorn: Two-factor Attestation for data Security”, Proc. of the 18th ACM conference on Computer and Communications Security.
[6] F. Zhang, J. Chen, H. Chen, and B. Zang(2011), “CloudVisor: Retrofitting Protection of Virtual Machines in Multitenant Cloud with Nested Virtualization”, Proc. of 23rd ACM Symposium on Operating Systems Principles.
[7] L. Eschenauer and V. D. Gligor(2002), “A key-management scheme for distributed sensor networks,” in Proceedings of the 9th ACM conference on Computer and communications security, Washington, DC, USA, pp. 41 - 47.
[8] Gupta G, Younis M(2003), "Performance Evaluation of Load-Balanced Clustering in Wireless Sensor Networks" In the proc. of 10th International Conference on Telecommunications (ICT 2003), Tahiti, French Polynesia.
[9] M. Tatebayashi, N. Matsuzaki, and D. B. Newman(1999), "Key distribution protocol for digital mobile communication systems," Advances in Cryptology-CRYPTO'89, pp. 324-334, INCS Volume 435, Springer-verlag.
[10] C. Park, K. Kurosawa, T. Okamoto, and S. Tsujii(1993), "On key distrubution and authentication in mobile radio networks," Advances in Cryptology - euroCrypt'93, pp. 461-465, INCS Volume 765, Springer-verlag.
[11] S. Basagni, K. Herrin, D. Bruschi, and E. Rosti(2001). “Secure pebblenets," In Proceedings of the 2001 ACM International Symposium on Mobile ad hoc networking & computing, ACM Press, pp. 156-163.
[12] L. Echenauer and V. D. Gligor(2002), "A Key-Management scheme for Distributed sensor networks," In Proceedings of the 9th Computer Communication Security, pp.41-47.
[13] H. Chan, A. Perrig, and D. Song(2003), "Random key predistribution schemes for Sensor networks," In IEEE Symposium on Research in Security and Privacy, pp.197-213
[14] S. Zhu, S. Setia, and S. Jajodia(2002), "A distributed group key managemet protocol for ad hoc networks," Unpublished manuscript, George Mason University.
[15] A. Khalili, et al.(2003), "Toward Secure key Distribution in Truly Ad-Hoc Networks," IEEE SAINT'03, pp. 342-346.

김 용 태(Kim, Yong Tae)

・1984년 2월 : 한남대학교 계산통계학과 학사
・1988년 2월 : 숭실대학교 전자계산학과 석사
・2008년 2월 : 충북대학교 전자계산학과 박사
・2002년 12월 ~ 2006년 2월 : (주)가림정보기술 이사
・2010년 10월 ~ 현재 : 한남대학교 멀티미디어학부 교수
・관심분야 : 모바일 웹서비스, 정보 보호, 센서 웹, 모바일 통신보안
・E-Mail : ky7762@hnu..kr

박 길 철(Park, Gil Cheol)

・1983년 2월 : 한남대학교 계산통계학과 학사.
・1986년 2월 : 숭실대학교 전자계산학과 석사.
・1998년 2월 : 성균관대학교 전자계산학과 박사.
・2006년 : UTAS, Australia 교환교수
・1998년 8월 ~ 현재 : 한남대학교 멀티미디어학부 교수
・2005년 2월 : 한국정보기술학회 이사 멀티미디어 분과 위원장
・관심분야 : Multimedia And Mobile Communication, Network Security
・E-Mail : gcpark@hnu..kr