情報保護學會論文誌
第 21 卷 第 4 號, 2011. 8

스마트그리드 환경에 적용 가능한 해쉬체인 기반의 그룹키 관리 메커니즘*

은 선 기,† 오 수 현‡
호서대학교

Hash chain based Group Key Management Mechanism for Smart Grid Environments*

Sun-Ki Eun,† Soo-Hyun Oh‡
Hoseo University

요 약

스마트그리드는 기존의 전력망과 정보통신 기술을 융합하여 에너지 효율을 최적화할 수 있는 차세대 지능형 전력망이다. 이는 소비자에게는 전력 요금의 실시간 확인을 통해 능동적인 전력소비를 유도하고, 공급자에게는 예상 발전량 측정을 통해 보다 안정적인 전력 시스템을 운용하도록 할 수 있다는 장점이 있다. 그러나 스마트그리드는 지능형 장치를 통한 양방향 통신 사이에서 데이터 노출, 데이터 도용, 프라이버시 침해와 같은 다양한 보안 위협들이 존재할 가능성이 있다. 따라서 이러한 스마트그리드의 보안 위협에 대응할 수 있는 안전한 환경을 구축하기 위해서는 보안 메커니즘 개발에 핵심이 되는 키 관리 기법이 필수적으로 요구된다. 본 논문에서는 해쉬 체인을 이용하여 계층적 구조를 갖는 스마트그리드 환경에 효율적으로 적용 가능한 그룹키 관리 메커니즘을 제안하고, 제안하는 그룹키 관리 메커니즘의 안전성 및 효율성을 분석한다.

ABSTRACT

Smart Grid is the next-generation intelligent power grid that maximizes energy efficiency with the convergence of IT technologies and the existing power grid. It enables consumers to check power rates in real time for active power consumption. It also enables suppliers to measure their expected power generation load, which stabilizes the operation of the power system. However, there are high possibility that various kinds of security threats such as data exposure, data theft, and privacy invasion may occur in interactive communication with intelligent devices. Therefore, to establish a secure environment for responding to such security threat with the smart grid, the key management technique, which is the core of the development of a security mechanism, is required. Using a hash chain, this paper suggests a group key management mechanism that is efficiently applicable to the smart grid environment with its hierarchical structure, and analyzes the security and efficiency of the suggested group key management mechanism.

Keywords: Smart Grid, SCADA, Group Key, Hash chain

접수일(2011년 5월 30일), 게재확정일(2011년 8월 1일)
* 이 논문은 2011년도 호서대학교의 재원으로 학술연구비 지원을 받아 수행된 연구임(2011-0042)

† 주저자, eunsunki@gmail.com
‡ 교신저자, shoh@hoseo.edu

I. 서 론

최근 전 세계적 주요 과제 가운데 하나가 녹색성장으로, 기후변화로 상징되는 '환경' 위기와 고유가로 대표되는 '자원' 위기를 동시에 해결하면서 지속가능한 경제 성장을 이루기 위한 다양한 노력들이 진행되고 있다. 우리나라 역시 녹색성장을 기회로 녹색강국으로 발돋움하기 위해서 다양한 녹색 기술들이 제시되고 있으며, 그 중 가장 주목 받고 있는 기술이 바로 스마트그리드(Smart Grid)이다. 스마트그리드는 기존의 전력 시스템에 정보통신기술(ICT: Information & Communication Technology)을 융합하여 전력 공급자와 소비자가 양방향으로 실시간 정보를 교환하고, 이를 통해 에너지 효율을 최적화할 수 있는 차세대 지능형 전력망을 의미한다[15]. 국내에서는 점차적으로 지능형 소비자(Smart Consumer), 지능형 운송(Smart Transportation), 지능형 신재생 발전(Smart Renewable) 및 지능형 전력서비스(Smart Electricity Service)를 확장해 나감으로써 세계 최초의 국가단위 스마트그리드 구축을 추진하고 있다[10].

이러한 스마트그리드를 구축하기 위한 핵심 기반 시설인 AMI(Advanced Metering Infrastructure) 통신 구조는 스마트미터(smart meter), DCU(Data Concentration Unit) 및 AMI 서버와 같은 지능형 장치들로 구성되며, 이들 지능형 장치 간에는 유·무선의 통신 기술을 사용함으로써 소비 전력 및 부가적인 정보를 교환할 수 있다. 이렇게 교환되는 정보를 통해 각 가정이나 사무실 및 공장과 같은 소비자 영역에서는 전력 요금을 실시간으로 확인할 수 있어 보다 능동적인 전력 소비를 유도할 수 있다. 그리고 전력 공급자 측면에서는 현재의 전력 소비량을 바탕으로 예상 발전량을 측정할 수 있으므로 보다 안정적으로 전력 시스템을 운용할 수 있다는 장점이 있다[9].

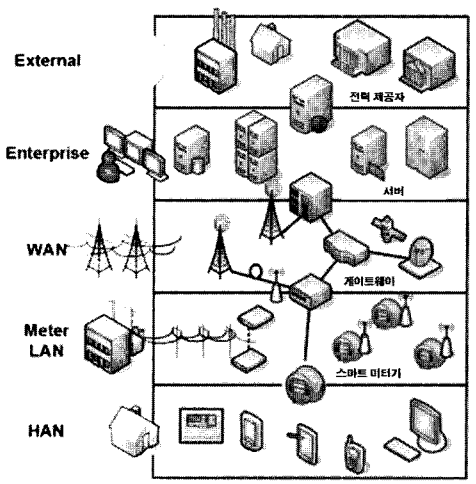
하지만, AMI 통신 구조에서 사용되는 다양한 통신 장치와 기술로 인해 기존의 통신 환경에서 존재하던 데이터 도용 및 불법 수정 등과 같은 보안 위협들이 스마트그리드 환경으로 전이 될 수 있으며, 또한 스마트그리드의 특성으로 인한 개인정보 노출 및 악용과 같은 추가적인 보안 위협들이 발생할 가능성이 있다[6][11]. 더욱이 스마트그리드 환경의 보안 취약성들을 악용한 보안 사고의 경우, 기존의 통신 네트워크에서 발생하는 보안 사고에 비해 국가의 핵심기반 시설인 전력 시스템을 기반으로 하는 보안 사고라는 점에서 그 파급력은 배가될 수 있다. 따라서 스마트그리드의 이점을 살리고 안정적인 서비스를 제공하기 위해서 스마트그리드 통신 환경에서 고려되어야 하는 보안 요구사항의 분석하고 이를 충족할 수 있는 보안 메커니즘의 개발이 필요하다.

본 논문에서는 보다 안전하고 효율적인 스마트그리드 통신 환경을 구축하기 위해 고려해야 하는 통신 품질 및 보안 요구사항들을 분석하고, 스마트그리드의 통신 환경에 적용 가능한 그룹키 관리 기법을 제안한다. 논문의 구성은 다음과 같다. 먼저 2장에서는 스마트그리드 통신 환경의 구조와 고려해야 하는 통신 품질 및 보안 요구사항과 함께 기존 전력시스템인 SCADA 통신 환경에서 제안된 키 관리 기법들을 분석한다. 다음으로 3장에서는 스마트그리드 통신 환경에 적용 가능한 그룹키 관리 기법을 제안하고, 4장에서는 제안하는 프로토콜의 안전성과 효율성을 분석하고 마지막으로 5장에서 결론을 맺는다.

II. 관련연구

2.1 스마트그리드의 통신 환경

스마트그리드를 구성하는 전력 시스템과 제어 시스템들 간의 상호연동을 위한 주요 통신 인프라인 AMI 통신 구조는 [그림 1]과 같이 구성된다. AMI의 통신 인프라는 이더넷(Ethernet) 및 PLC(Power Line Communication) 등과 같은 유선 통신 기술과 ZigBee, Wi-Fi 및 3GPP 등과 같은 무선 통신 기술



[그림 1] AMI 통신 인프라 구조

을 사용하여 구성 가능하다[5][13]. 그리고 스마트그리드의 소비자 영역부터 전력 제공자간의 통신망 구조를 살펴보면 다음과 같이 3가지 영역으로 분류된다.

- HAN(Home Area Network): 스마트그리드의 소비자 영역인 가정에서의 통신 영역으로, 전력선 통신인 PLC나 근거리 무선 통신 기술인 ZigBee 등을 사용할 수 있다. 그리고 전력이 소비되는 장소에 따라 HAN 대신 BAN(Building Area Network) 또는 IAN(Industry Area Network)으로 사용된다.
- FAN(Field Area Network): 스마트그리드의 필드 영역은 PLC와 같은 유선 기술과 IEEE 802.11, Wi-Fi 메시(mesh), IEEE 802.15.4g SUN(Smart Utility Network)과 같은 무선 기술 그리고 CDMA(Code Division Multiple Access)와 같은 이동통신 기술을 사용한다. 그리고 FAN 대신에 NAN(Neighborhood Area Network)으로 불리기도 한다.
- WAN(Wide Area Network): 스마트그리드의 WAN 영역은 코어(Core) 네트워크 또는 MAN(Metro Area Network) 및 백홀(Backhaul) 네트워크로 구성된다. 중계 시스템간의 연동은 주로 이더넷 기반의 유선 네트워크가 사용되며, 종종 무선 및 이동통신 네트워크 기술도 사용되고 있다.

AMI 통신 환경에서 다수의 스마트미터는 게이트웨이 역할을 수행하는 하나의 DCU에 접속하게 되며, 다수의 DCU 역시 WAN을 통해 전력 사업자의 AMI 서버에 접속하는 계층형 통신 구조로 구성된다.

2.2 스마트그리드의 통신 품질 및 보안 요구사항

스마트그리드의 통신 환경인 AMI 통신 구조에서는 실시간의 양방향 통신 제공과 함께 원활한 개체 관리를 위해 요구되는 통신 품질을 고려해야 한다. 이외에도 기존의 네트워크 인프라를 통해 유입되거나 새롭게 도입될 수 있는 데이터 노출, 데이터 도용, 데이터 불법 변경 및 삭제, 프라이버시 침해 그리고 디바이스 도난 등의 보안 위협들에 대응할 수 있는 보안 메커니즘의 개발이 필요하다. 따라서 본 절에서는 스마트그리드의 통신 품질에 대한 요구사항과 함께 안전한 스마트그리드의 통신 환경을 구축하기 위한 보안 요구사항들을 기술한다.

2.2.1 통신품질 요구사항

- **실시간성** : 전력 시스템에서 사용하는 통신 시스템의 경우 네트워크 지연에 매우 민감하며, 이는 스마트그리드 통신 환경에서도 동일하게 적용된다. 스마트그리드를 안전하게 제어하기 위해서 전송되는 제어 메시지나 긴급 상황을 알리기 위한 긴급 메시지의 경우, 최대한 빠른 시간에 도착해야 오동작에 의한 피해를 줄이고 적절한 대응책을 준비할 수 있다. 따라서 스마트그리드의 원활한 서비스 제공을 위해 통신 품질에 대한 실시간성이 요구된다[9].
- **메시지 브로드캐스트** : 스마트그리드의 통신 개체들을 원활하게 관리하기 위해서는 동일한 제어 메시지 또는 긴급 메시지를 다수의 통신 개체들에게 전송하기 위한 메시지 브로드캐스트가 요구된다. 또한 대부분의 브로드캐스트를 통해 전송되는 메시지의 경우, 제어 또는 긴급 메시지와 같이 중요한 정보를 포함하므로 이에 대한 기밀성이 요구된다.

2.2.2 보안 요구사항

- **데이터 기밀성** : 스마트그리드 통신 환경에서는 과금이나 제어 메시지 등과 같은 민감한 정보들이 네트워크를 통해 전송되므로 비 인가된 제 3자가 데이터의 내용을 알 수 없도록 암호화를 통해 송/수신되는 정보를 보호해야 한다.
- **데이터 무결성** : 스마트그리드 환경에서 전송되는 미터 사용량, 요금 관련 정보, 제어 메시지 등이 불법적인 접근에 의해 위·변조되지 않도록 보장해야 한다.
- **시스템 가용성** : 스마트그리드 환경에서 안정적이고 지속으로 실시간 양방향 통신을 제공하기 위해 디바이스, 시스템 및 네트워크의 가용성이 보장되어야 한다[14].
- **상호인증** : 스마트그리드 환경에서 공격자가 정상적인 사용자로 위장함으로써 사용자 측에서 원활한 서비스 제공을 받지 못하게 하거나 공격자가 전력 공급자로 위장함으로써 사용자의 개인정보 등을 탈취하는 등의 위협에 대응하기 위해

각 구성 요소들 간의 상호인증을 제공해야 한다.

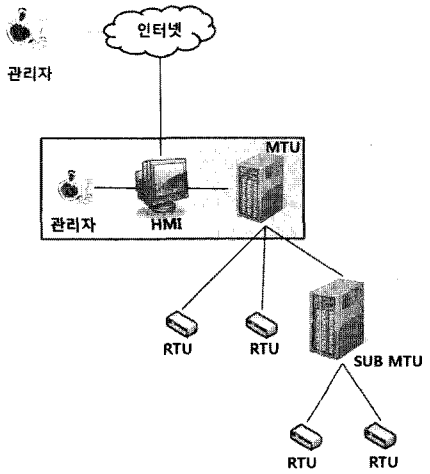
- **접근제어 및 인가** : 스마트그리드 통신 환경에서는 사용자 이외에 서비스 관리자가 원격으로 스마트미터 또는 다른 장치에 접근할 수 있으므로, 디바이스에 대한 부적절한 접근 및 인가 권한으로 초래될 수 있는 보안 위협들을 예방하기 위해 적절한 접근제어 및 인가 메커니즘이 요구된다.
- **부인방지** : 스마트그리드에서 스마트미터를 통해 측정된 실시간 과금 정보에 대해 사용자가 부인할 수 없도록 스마트미터에 기록된 메시지에 대한 부인방지 메커니즘이 필요하다.
- **디바이스의 무결성 보호** : 스마트미터나 DCU와 같은 디바이스의 경우, 사람이나 다른 보호 수단에 의해 보호되지 않거나 또는 상대적으로 물리적 보안이 취약한 장소에 배치될 수 있으므로 디바이스의 하드웨어, 소프트웨어 및 펌웨어에 대한 보호 장치가 필요하다. 만약 디바이스에 대한 무결성 검증이 보장되지 않는 경우, 공격자가 디바이스에 악성 소프트웨어를 삽입하거나 용도 변경을 통해 스마트그리드의 통신 네트워크를 오염시키거나 스마트그리드 서비스의 가용성을 손상시킬 수 있다. 따라서 디바이스에 대한 무결성 검증이 요구된다.
- **프라이버시 보호** : 스마트그리드 통신 환경에서 전송되는 거래 이력, 활동, 전력 사용 패턴 등의 정보를 통해 개인의 사생활과 밀접하게 연관된 정보들이 노출될 수 있다. 따라서 개인의 프라이버시와 관련된 정보들을 보호하기 위해 기술적으로는 암호화 기법을 통한 개인정보의 보호와 함께 프라이버시 침해 방지를 위한 법·제도적 보완장치가 요구된다[12].

2.3 SCADA 시스템의 키 관리 기법

현재까지 스마트그리드 통신 환경을 위한 표준화된 키 관리 기술은 없으며, 스마트그리드를 구성하는 구성 요소 별로 키 관리에 관한 연구가 진행 중이다. 그 중 송/배전시 사용되는 SCADA(Supervisory Control And Data Acquisition) 시스템에서의 키 관리 기술이 제안되어 있다. 본 절에서는 SCADA 시스템에서 제안된 키 관리 기법들을 설명한다.

SCADA 시스템은 일반적으로 원격지에 설치된 센서 또는 디바이스들의 상태정보를 수집하여 중앙의 제어 시스템에 전달함으로써, 중앙에서 원격장치를 효율적으로 감시 및 제어하기 위한 시스템이다. 이러한 SCADA 시스템은 현재 국가의 핵심 기반시설인 전력, 가스, 상하수도 및 철도 등을 통합 제어하기 위해 사용되고 있다. SCADA 시스템의 통신 환경은 스마트그리드의 AMI 구조와 유사한 계층적 통신 구조로 구성되어 있다. [그림 2]는 SCADA 시스템의 통신구조이며, 각 구성요소에 대한 설명은 다음과 같다.

- HMI(Human-Machine Interface): 운영자의 편리를 위해 제공되는 사용자 인터페이스로 주로 GUI를 지원한다.
- MTU(Master Terminal Unit): SCADA 시스템의 최상위에 위치한 관리 디바이스로 RTU들을 감독하고 제어하는 역할을 한다. SCADA 시스템은 일반적으로 하나의 중앙 MTU를 가지고 있고 그 아래 다수의 SUB-MTU를 가진다. MTU와 SUB-MTU는 최소한 데스크톱 수준의 연산능력 및 자원을 가진다.
- RTU(Remote Terminal Unit): RTU는 원격지에 설치되어 필요한 정보를 수집하고 이를 MTU나 SUB-MTU에게 전송하는 제어 디바이스 및 관측 센서이다. 이러한 RTU는 물리적 보안에 취약하고 제한된 연산능력 및 자원을 지닌다.



[그림 2] SCADA 시스템의 통신 구조

하지만 SCADA 시스템에서의 원격 디바이스인 RTU와 스마트그리드의 스마트미터 간에는 다소 차이

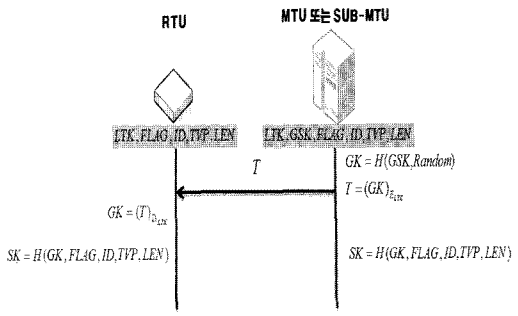
가 있다. 스마트그리드의 경우 최근의 기술을 사용함으로써 디바이스에 대한 자원 및 컴퓨팅 제약사항이 SCADA 시스템 보다 적은 반면, 기존의 SCADA 시스템은 상대적으로 낙후된 기술을 사용하고 디바이스의 교체 주기도 보통 20년 정도의 긴 생명주기를 가짐으로써 디바이스, 즉 RTU에 대한 자원 및 컴퓨팅 제약사항이 엄격하다. 따라서 원격 디바이스에 대한 제약사항으로 RTU에서는 공개키 연산과 같은 강도 높은 컴퓨팅 연산과 함께 다수의 키들을 저장할 수 없다.

2.3.1 SKE

SKE는 Sandia National Laboratories의 Beaver 등이 SCADA 시스템을 위해 제안한 키 관리 프로토콜로 사용되는 통신 형태를 2가지로 분류하고 있다[1]. 우선 MTU와 RTU 또는 SUB-MTU와 RTU와 같은 계층적 구조에서의 통신은 C-S(Controller to Subordinate) 형태를 사용하며, SUB-MTU들 간의 통신은 P-P(Peer-to-Peer) 형태를 사용한다. SKE에서 제안한 주요 통신 프로토콜은 계층적 구조에서 사용되는 C-S로 다음과 같은 키들을 사용한다.

- LTK(Long Term Key): 각각의 종속 디바이스인 RTU와 상위 제어 디바이스인 MTU 또는 SUB-MTU 간에 공유하는 키로 사전에 직접 삽입과 같은 안전한 방법으로 공유된다. LTK는 GK를 갱신하기 위해 사용된다.
- GSK(General Seed Key): MTU 및 SUB-MTU에서 GK를 생성하기 위해 사용하는 키이다.
- GK(General Key): SK를 파생하기 위해 사용되는 키로 MTU 및 SUB-MTU에서 생성되고 LTK를 사용하여 암호화되어 RTU에게 전달된다.
- SK(Session Key): 실제로 데이터를 암/복호화 하기 위해 사용되는 키로 GK로부터 파생된다.

SKE에서 세션키를 생성하기 위해서는 사전에 MTU 및 SUB-MTU와 같은 제어 디바이스와 종속 디바이스인 RTU에 LTK, FLAG, ID, TVP 및 LEN을 공유하고 있어야 한다. [그림 3]은 SKE의 세션키 생성 과정이다.



[그림 3] SKE의 세션키 생성 과정

[SKE의 세션키 생성 과정]

① 제어 디바이스에서 GSK와 랜덤수를 사용하여 GK 생성
② 생성된 GK를 종속 디바이스만이 알고 있는 LTK로 암호화하여 전달
③ 종속 디바이스에서 LTK를 사용하여 복호하고 GK 획득
④ 서로 공유한 GK, FLAG, ID, TVP, LEN을 해쉬함으로써 메시지 암호화에 사용할 세션키 생성

2.3.2 SKMA

SKMA는 Dawson 등이 제안한 프로토콜로 새로운 RTU가 SCADA 시스템에 등록되었을 경우, RTU간의 세션키 설립을 통해 안전한 통신을 제공한다. 다음은 SKMA에서 사용하는 키의 형태이다[7].

- K_{AC}(long term node-KDC key): 노드 A와 KDC C 사이에 공유하는 키
- K_{AB}(long term node-node key): 노드 A와 노드 B 사이에 공유하는 키
- 세션키: 메시지를 암호화하기 위해 사용하는 키

SCADA 시스템에서의 노드 즉, RTU를 원격지에 배치하기 전에 node-KDC 키를 삽입함으로써 RTU와 제어 디바이스인 MTU 및 SUB-MTU간에 node-KDC 키를 안전하게 공유한다. 그 후에 새로운 RTU가 SCADA 시스템에 배치되어 RTU간의 통신을 하기 위해서는 다음과 같은 방식으로 node-node

키 설립 과정을 수행한다. 키 설립 과정에서 A는 SCADA 시스템에 이미 배치되어있던 RTU이며, B는 새롭게 SCADA 시스템에 배치되는 RTU를 의미한다. 그리고 C는 KDC를 포함하는 MTU 또는 SUB-MTU이며, NA는 RTU A에서 생성한 Nonce 값, NB는 RTU B에서 생성한 Nonce 값, Text 1/2/3/4는 메시지 1/2/3/4를 나타낸다.

〔SKMA의 키 설립과정〕

① 새롭게 SCADA 시스템에 배치되는 RTU B는 이미 배치되어 있는 RTU A에게 Nonce 값 N_B 전송

② RTU A는 Nonce 값 N_A를 생성하고 KDC를 포함한 MTU C에게 N_A, N_B, B 전송

③ KDC를 포함한 MTU C는 RTU A와 RTU B 간의 공유키 K_{AB} 를 생성하고 RTU A 에게 $\{N_A, K_{AB}, B, Text1\}_{K_{AC}}$, $\{N_B, K_{AB}, A, Text2\}_{K_{BC}}$ 전송

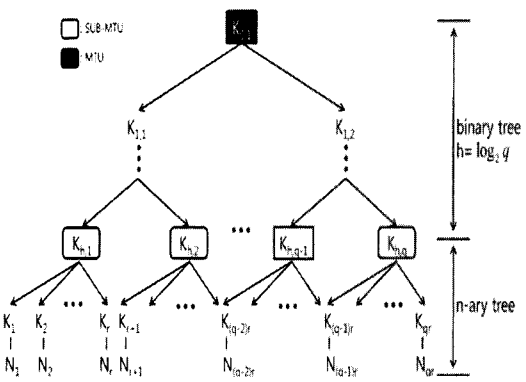
④ RTU A는 전달받은 $\{N_A, K_{AB}, B, Text1\}_{K_{AC}}$을 복호하여 자신과 RTU B간의 공유키 K_{AB}를 획득한다. 그리고 나서 Nonce 값 N'_A를 생성하고 RTU B에게 $\{N_B, K_{AB}, A, Text2\}_{K_{BC}}$, $\{N'_A, N_B, B, Text3\}_{K_{AB}}$ 전송

⑤ RTU B는 전달받은 $\{N_B, K_{AB}, A, Text2\}_{K_{BC}}$을 복호하여 자신과 RTU A간의 공유키 K_{AB}를 획득한다. 그리고 나서 공유키 K_{AB}를 사용하여 $\{N'_A, N_B, B, Text3\}_{K_{AB}}$를 복호함으로써 Nonce 값 N'_A를 획득하고 RTU A에게 $\{N_B, N'_A, Text4\}_{K_{AB}}$ 전송

SKMA에서는 제어 디바이스인 MTU 또는 SUB-MTU, 기존의 RTU 그리고 새롭게 추가되는 RTU 간의 키 확립을 통해 RTU들 간의 node-node 키를 설립한다. 이렇게 node-node 키가 설립된 이후에 타임스탬프 값과 node-node 키의 해쉬 값을 계산하여 세션키를 생성한다.

2.3.3 ASKMA

ASKMA는 Choi 등이 제안한 키 관리 기법으로 LKH(Logical Key Hierarchy) 구조를 이용한 방식이다[2]. ASKMA의 키 관리 구조는 〔그림 4〕와 같다. 상위의 MTU와 SUB-MTU들 간의 관계는 이진트리 형식으로 구성되며, MTU와 RTU들 또는 SUB-MTU와 RTU들 간에는 $n-ary$ 트리 형식으로 구성된다[3].



〔그림 4〕 ASKMA의 키 관리 구조

ASKMA에서는 메시지 브로드캐스트를 지원하는 그룹키 관리 기법을 제공한다. 이를 위해 새로운 RTU가 SCADA 시스템에 가입하거나 기존의 RTU가 SCADA 시스템을 탈퇴할 경우, 그룹키의 안전성을 보장한다는 장점이 있다[8].

III. 제안하는 그룹키 관리 기법

본 장에서는 스마트그리드 환경에서 효율적으로 디바이스들을 관리하기 위해 필요한 그룹키 관리 기법을 제안한다. 제안하는 그룹키 관리 기법은 전력 사용자가 스마트그리드 서비스를 제공받기 위해 새로운 스마트미터를 등록하는 가입 프로토콜과 기존의 전력 사용자가 스마트그리드 서비스를 해지하기 위한 탈퇴 프로토콜 그리고 AMI 서버와 DCU 간의 그룹키 관리 방식으로 구성된다. 그리고 제안하는 그룹키 관리 기법은 그룹키 안전성, 전방향 안전성 및 후방향 안전성을 제공한다는 장점이 있다.

3.1 표기법 및 그룹키 생성

제안하는 그룹키 관리 기법에서 사용하는 표기와 의미는 〔표 1〕과 같다.

각 가정 또는 전력 사용자 측에 배치되는 스마트미터 S들과 DCU D들은 사전에 각자의 비밀키 K_S, K_D를 할당받아 안전하게 저장한다. 또한 AMI 서버 S와

〔표 1〕 표기법

표기	의미
S_e	기존의 스마트미터
S_j	스마트그리드 서비스에 가입하는 스마트미터
S_l	스마트그리드 서비스를 탈퇴하는 스마트미터
K_S	스마트미터 S의 비밀키
K_D	DCU D의 비밀키
K_G^i	i번째 그룹키
b	그룹키의 전방향 안전성을 제공하기 위한 파라미터
f	그룹키의 후방향 안전성을 제공하기 위한 파라미터
$\oplus$	XOR 연산
$h(\cdot)$	해쉬함수

DCU D들은 파라미터 b에 대해서 다음과 같이 k길이만큼의 해쉬체인을 사전에 계산하여 안전하게 저장한다. 여기서 i는 해쉬체인의 끝에서부터 증가하는 값을 의미한다.

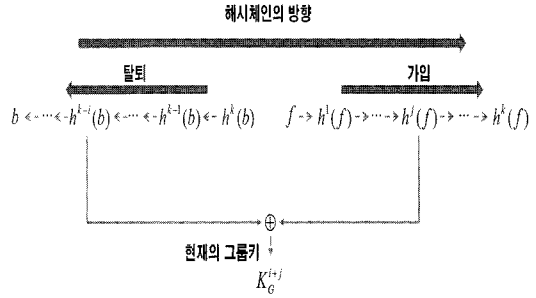
$$b \rightarrow h^1(b) \rightarrow h^2(b) \rightarrow \ldots \rightarrow h^{k-i}(b) \rightarrow \ldots \rightarrow h^{k-1}(b) \rightarrow h^k(b)$$

그리고 원활한 그룹키 갱신을 수행하기 위해 파라미터 f에 대해서도 k길이만큼의 해쉬체인을 계산하여 저장한다.

$$f \rightarrow h^1(f) \rightarrow h^2(f) \rightarrow \ldots \rightarrow h^j(f) \rightarrow \ldots \rightarrow h^{k-1}(f) \rightarrow h^k(f)$$

제안하는 그룹키 기법에서는 해쉬함수의 일방향성과 Lamport의 Reverse Hash Chain 기법을 이용하여 그룹키를 생성한다. Reverse Hash Chain 기법은 연속된 해쉬체인 값들을 역방향으로 사용하는 방법으로 자신만이 메시지 A를 알고 있고 상대방이 메시지 A의 해쉬 값을 가지고 있는 경우, 상대방에게 메시지 A를 제공함으로써 자신이 정당한 사용자임을 인증하는 기법이다. 이는 해쉬함수의 일방향성을 이용한 것으로 메시지 A의 해쉬 값을 통해 해쉬함수의 수행 이전 값을 계산할 수 없으며, 정당한 사용자만이 메시지 A를 제공할 수 있다[4].

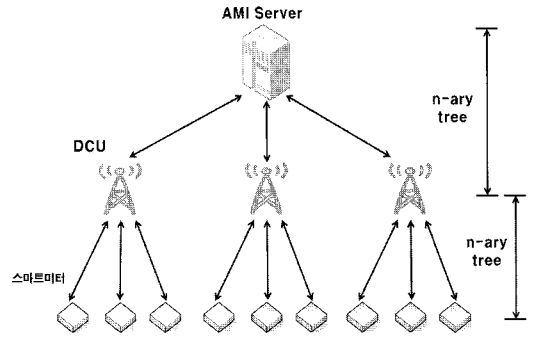
제안하는 그룹키 기법에서 $i+j$번째 그룹키 K_G^{i+j}는 스마트미터 S의 가입 또는 탈퇴에 따라 파라미터 b에 대한 해쉬체인의 값 $h^{k-i}(b)$과 파라미터 f에 대한 해쉬체인 값 $h^j(f)$을 선택하고, 두 값을 XOR 연산하여 생성한다. 여기서 i 값은 기존의 스마트미터 S_e가 탈퇴했을 때 증가하고 j 값은 새로운 스마트미터 S_j가 가입했을 경우 증가한다. 〔그림 5〕는 그룹키 생성 방법을 나타낸다.



〔그림 5〕 그룹키 생성 방법

$$K_G^{i+j} = h^{k-i}(b) \oplus h^j(f)$$

또한 제안하는 키 관리 기법에서는 AMI 서버 A에서 DCU D 및 스마트미터 S의 물리적 위치를 알고 있다고 가정하며, 키 구조는 〔그림 6〕과 같이 AMI 서버 A와 DCU D 그리고 DCU D와 스마트미터 S간에는 $n-ary$ 트리로 구성된다. 하지만 각각의 DCU D에 속해 있는 스마트미터 S들의 개수는 DCU D마다 다를 수 있다.



〔그림 6〕 제안하는 키 구조

3.2 가입 프로토콜

가입 프로토콜은 스마트미터를 구입한 전력 사용자가 스마트그리드 서비스를 제공받기 위해 AMI 시스템에 새로운 스마트미터 S_j를 등록하기 위한 프로토콜이며 절차는 다음과 같다.

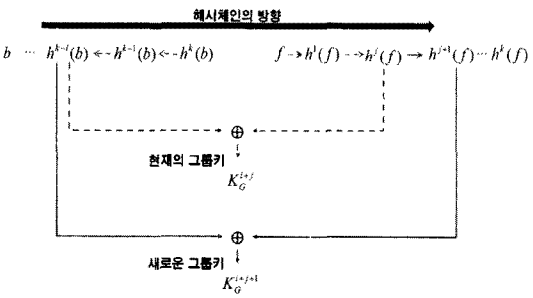
〔단계 1〕 AMI 서버 A: 전력 사용자의 물리적 위치를

파악한 후, 스마트미터 S_j의 비밀키 K_{S_j}를 해당 DCU D에게 안전하게 전달한다.

〔단계 2〕 DCU D: 현재 DCU D에서 관리하는 기존의 스마트미터 S_e들이 가지고 있는 파라미터 b에 대한 해쉬체인의 값이 $h^{k-i}(b)$이고 파라미터 f에 대한 해쉬체인의 값이 $h^j(f)$일 경우, 새롭게 가입한 스마트미터 S_j에게 $h^{k-i}(b)$ 값과 $h^{j+1}(f)$ 값을 스마트미터 S_j의 비밀키 K_{S_j}로 암호화하여 전달한다.

〔단계 3〕 새로운 스마트미터 S_j: DCU D로부터 전달받은 메시지를 자신의 비밀키 K_{S_j}로 복호화하여 $h^{k-i}(b)$ 값과 $h^{j+1}(f)$ 값을 획득한다. 그리고 $h^{k-i}(b)$ 값과 $h^{j+1}(f)$ 값을 XOR 연산을 수행하여 그룹키 $K_G^{i+j+1}=h^{k-i}(b)\oplus h^{j+1}(f)$을 계산한다. DCU D에게 올바른 그룹키 K_G^{i+j+1} 생성을 알리기 위해 자신의 비밀키 K_{S_j}와 그룹키 K_G^{i+j+1}을 해쉬한 값 $h(K_{S_j}\|K_G^{i+j+1})$을 DCU D에게 전달한다.

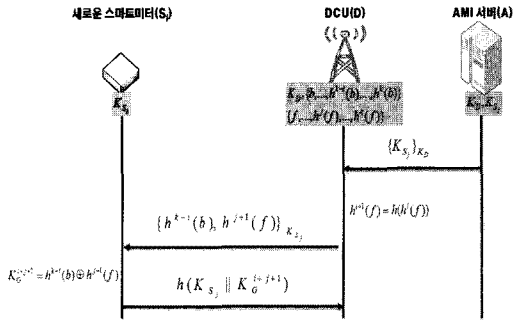
〔그림 7〕은 가입 프로토콜의 그룹키 생성 과정을 나타낸다.



〔그림 7〕 가입 프로토콜의 그룹키 생성 과정

전력 사용자의 스마트그리드 서비스 가입으로 인한 새로운 스마트미터 S_j의 가입 프로토콜의 단계 1부터 단계 3까지의 절차를 도식화하면 〔그림 8〕과 같다.

〔단계 4〕 DCU D: 새로운 스마트미터 S_j에게 전달받은 $h(K_{S_j}\|K_G^{i+j+1})$ 값과 자신이 생성한 $h(K'_{S_j}\|K'^{i+j+1}_G)$이 동일한지 판단하고 같을 경우, 기존의 스마트미터 S_e들에게 그룹키 갱신 메시지와 이에 대한 MAC 값을 함께 전달한다.

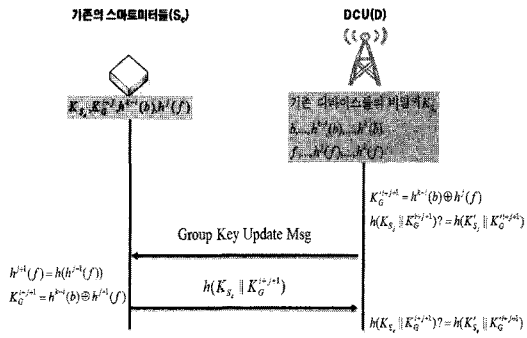


〔그림 8〕 가입 프로토콜의 단계 1부터 단계 3까지의 절차

〔단계 5〕 기존의 스마트미터 S_e: DCU D로부터 그룹키 갱신 메시지를 받은 기존의 스마트미터 S_e들은 저장되어 있던 f에 대한 해쉬체인의 값 $h^j(f)$을 한 번 더 해쉬하여 $h^{j+1}(f)$을 계산한다. 그리고 $h^{k-i}(b)$ 값과 $h^{j+1}(f)$ 값을 XOR 연산을 수행하여 그룹키 $K_G^{i+j+1}=h^{k-i}(b)\oplus h^{j+1}(f)$을 계산한다. 또한 기존의 스마트미터 S_e들은 DCU D에게 올바른 그룹키 K_G^{i+j+1} 생성을 알리기 위해 자신의 비밀키 K_{S_e}와 그룹키 K_G^{i+j+1}을 해쉬한 값 $h(K_{S_e}\|K_G^{i+j+1})$을 DCU D에게 전달한다.

〔단계 6〕 DCU D: 기존의 스마트미터 S_e들에게 전달받은 값 $h(K_{S_e}\|K_G^{i+j+1})$와 자신이 생성한 $h(K'_{S_e}\|K'^{i+j+1}_G)$이 동일한지 비교함으로써 각각의 스마트미터 S_e에서 올바른 그룹키 K_G^{i+j+1}을 생성하였음을 확인한다.

〔그림 9〕는 가입 프로토콜의 단계 4부터 단계 6까지의 절차를 나타낸 것이다.



〔그림 9〕 가입 프로토콜의 단계 4부터 단계 6까지의 절차

3.3 탈퇴 프로토콜

스마트그리드 서비스를 제공받던 전력 사용자가 스마트그리드 서비스를 탈퇴하거나 또는 스마트미터의 고장과 같은 원인으로 기존의 스마트미터 S_e를 교체해야 할 경우 다음의 탈퇴 프로토콜을 수행한다.

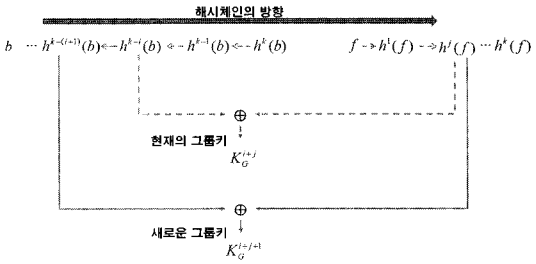
〔**단계 1**〕 AMI 서버 A: 탈퇴하는 스마트미터 S_l의 물리적 위치 및 스마트미터 S_l의 비밀키 K_{S_l} 등과 같은 전력 사용자의 개인 정보들을 AMI 서버 A에서 삭제한다. 그후에 DCU D에게 스마트미터 S_l의 탈퇴 사실과 함께 그룹키 갱신 메시지를 전달한다.

〔**단계 2**〕 DCU D: DCU D는 탈퇴한 스마트미터 S_l가 그룹 통신에 대한 정보를 알 수 없도록 현재의 그룹키 K_G^{i+j}에 대한 그룹키 갱신 절차를 수행한다. 가입 프로토콜에서와 마찬가지로 현재 DCU D에서 관리하는 기존의 스마트미터 S_e들이 가지고 있는 파라미터 b에 대한 해쉬체인의 값이 $h^{k-i}(b)$이고 파라미터 f에 대한 해쉬체인의 값이 $h^j(f)$일 경우, DCU D는 $h^{k-(i+1)}(b)$을 탈퇴한 스마트미터 S_l를 제외한 기존의 스마트미터 S_e들에게 각자의 비밀키 K_{s_e}로 암호화하여 각각 전달한다.

〔**단계 3**〕 기존의 스마트미터 S_e: DCU D로부터 전달받은 메시지를 자신의 비밀키 K_{s_e}로 복호화하여 $h^{k-(i+1)}(b)$ 값을 획득한다. 그리고 나서 획득한 $h^{k-(i+1)}(b)$ 값과 저장되어 있는 $h^j(f)$ 값을 XOR 연산함으로써 그룹키 $K_G^{i+j+1} = h^{k-(i+1)}(b) \oplus h^j(f)$를 계산한다. 또한 DCU D에게 올바른 그룹키 K_G^{i+j+1}가 생성되었음을 알리기 위해 자신의 비밀키 K_{s_e}와 생성한 그룹키 K_G^{i+j+1}을 해쉬한 값 $h(K_{S_e} \| K_G^{i+j+1})$을 DCU D에게 전달한다.

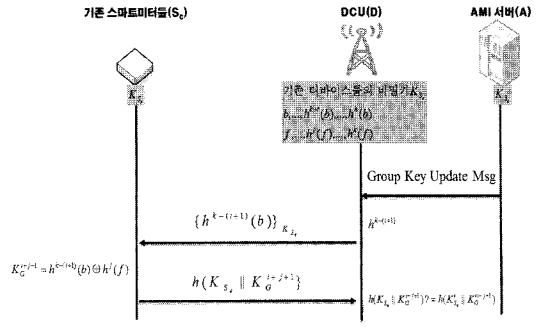
〔**단계 4**〕 DCU D: 기존의 스마트미터 S_e들에게 전달받은 값 $h(K_{S_e} \| K_G^{i+j+1})$와 자신이 생성한 $h(K'_{S_e} \| K'^{i+j+1}_G)$이 동일한지 판단함으로써 각각의 스마트미터 S_e에서 올바른 그룹키 K_G^{i+j+1}을 생성하였는지 확인한다.

〔그림 10〕은 스마트미터의 탈퇴가 발생할 경우, 새로운 그룹키 생성 과정을 나타낸다.



〔그림 10〕 탈퇴 프로토콜에서의 새로운 그룹키 생성 과정

기존 전력 사용자의 스마트그리드 서비스 해지로 인한 탈퇴 프로토콜의 절차는 〔그림 11〕과 같다.



〔그림 11〕 탈퇴 프로토콜의 절차

IV. 안전성 및 효율성 분석

본 장에서는 제안하는 스마트그리드 환경에 적합한 그룹키 관리 기법에 대해 그룹키 안전성, 전방향 안전성, 후방향 안전성, 계산 효율성을 분석하고 기존의 기법들과의 비교 결과를 제시한다.

- **그룹키 안전성(Group Key Secrecy)** : 제안하는 키 관리 기법은 스마트그리드 서비스에 등록된 스마트미터 S에게만 그룹키 K_G^{i+j}에 대한 키 매트리얼(material)인 파라미터 b의 해쉬체인 값 $h^{k-i}(b)$와 파라미터 f의 해쉬체인 값 $h^j(f)$을 스마트미터 S의 비밀키 K_s로 암호화하여 안전하게 전달한다. 제안하는 키 관리 기법에서는 스마트그리드 서비스에 등록되지 않은 사용자의 경우, DCU D에 자신의 스마트미터 비밀키 K_s가 등록되어 있지 않으므로 올바른 $h^{k-i}(b)$ 값과 $h^j(f)$을 복호할 수 없고, 따라서 그룹키 $K_G^i = h^{k-i}(b) \oplus h^j(f)$를 계산할 수 없다. 그

러므로 제안하는 키 관리 기법은 그룹키 안전성을 제공한다.

- **전방향 안전성(Forward Secrecy)** : 그룹키의 전방향 안전성은 스마트그리드 서비스를 해지한 스마트미터 S_i이 기존에 저장된 그룹키 K_G^i를 사용하여 서비스 해지 이후의 그룹키 K_G^{i+1}를 계산할 수 없도록 보장하는 것을 의미한다. 제안하는 프로토콜에서는 스마트미터 S_i가 서비스를 해지할 경우, 해지한 스마트미터 S_i을 제외한 기존의 스마트미터 S_e들에게 $h^{k-(i+1)}(b)$를 기존 스마트미터들의 비밀키로 암호화하여 전달함으로써 그룹키 $K_G^{i+1} = h^{k-(i+1)}(b) \oplus h^i(f)$를 갱신한다. 하지만 탈퇴한 스마트미터 S_i은 키 매트리얼 $h^{k-(i+1)}(b)$를 받지 못하므로 새로운 그룹키 $K_G^{i+1} = h^{k-(i+1)}(b) \oplus h^i(f)$를 계산할 수 없다. 따라서 제안하는 키관리 기법은 그룹키에 대한 전방향 안전성을 제공한다.

- **후방향 안전성(Backward Secrecy)** : 그룹키의 후방향 안전성은 스마트그리드 서비스에 가입한 새로운 스마트미터 S_j가 현재의 그룹키 K_G^{i+1}를 사용하여 서비스 가입 이전의 그룹키 K_G^i를 계산할 수 없도록 보장하는 것을 의미한다. 제안하는 프로토콜에서는 새로운 스마트미터 S_j가 서비스 그룹에 가입한 경우, 새로운 스마트미터에게 $h^{k-i}(b)$와 $h^{j+1}(f)$를 안전하게 전달하여 새로운 스마트미터 S_j가 현재의 그룹키 $K_G^{i+1} = h^{k-i}(b) \oplus h^{j+1}(f)$를 계산할 수 있지만, 해쉬함수의 일방향성으로 인해 이전의 그룹키 $K_G^i = h^{k-i}(b) \oplus h^j(f)$를 계산하는 것은 불가능하다. 따라서 제안하는 키관리 기법은 그룹키에 대한 후방향 안전성을 제공한다.

- **효율성(Efficiency)** : 제안하는 그룹키 관리 기법은 SKE와 SKMA 방식에서 지원하지 않는 메시지 브로드캐스트를 지원한다. 그리고 ASKMA와는 달리 스마트미터와 DCU 그리고 DCU와 AMI 서버 영역으로 통신 그룹을 분리함으로써 스마트미터에서 관리되는 키의 개수를 2개로 줄일 수 있다. 그리고 스마트미터의 가입 및 탈퇴로 인한 그룹키 변경이 타 그룹에 영향 주지 않는다는 장점으로 인해 ASKMA에서는 RTU의 탈퇴로 변경되는 그룹키의 개수가 $\log_2 q+1$이지만, 제안하는 그룹키 관리 기법에서 스마트미터의 탈퇴로 변경되는 그룹키의 개수는 1개로 보다 효율적인 키 관리를 수행할 수 있다. 또한 그룹키 생성 및 갱신 과정에서 사용되는 연산이 해쉬함수와 XOR 연산으로 이루어지므로 계산상 효율적이라 할 수 있다.

제안하는 그룹키 관리 기법과 기존 관련연구들과의 안전성 및 효율성을 비교한 결과는 〔표 2〕와 같다.

〔표 2〕 제안하는 기법과 관련연구와의 안전성 및 효율성 비교

	SKE & SKMA	ASKMA	제안하는 키 관리 메커니즘
메시지 브로드캐스트	x	x	o
그룹키 안전성	-	o	o
전방향 안전성	-	o	o
후방향 안전성	-	o	o
스마트미터에 저장되는 키의 수	1	$2+\log_2 q$	2
스마트미터 탈퇴 시 변경되는 그룹키 수	-	$1+\log_2 q$	1
스마트미터 탈퇴 시 전송되는 메시지 수	-	n	$n-1$

V. 결 론

최근 들어 환경 위기와 자원 위기를 동시에 해결하고 지속적인 경제 발전을 이룩할 수 있는 주요 기술로 스마트그리드가 주목받고 있다.

그러나 통신 기술을 활용한 지능형 장치의 사용으로 데이터 송·수신시에 발생할 수 있는 데이터 노출, 데이터 도용 및 다양한 보안 위협들이 존재할 가능성이 있으며, 이는 국가 중요 기반기설인 전력 시스템과 연계된 스마트그리드에서 사이버 테러와 같은 보안 사고를 야기할 수 있다. 따라서 이러한 보안 위협들에 대해 발견 즉시 대응하고, 효율적인 디바이스 관리를 위한 다양한 보안 메커니즘의 개발이 요구된다.

본 논문에서는 스마트그리드 통신 환경에서 고려해야 하는 통신 품질 및 보안 요구사항들을 분석하였고, 안전하고 효율적인 스마트그리드 통신 환경을 구축하

는데 필요한 그룹키 관리 기법을 제안하였다. 제안하는 그룹키 관리 기법은 안전하게 생성된 그룹키를 사용함으로써 스마트그리드에서 발생할 수 있는 누전이나 정전과 같은 전력사고 시에 적절한 그룹 메시지를 전송함으로써 위급상황에 대한 빠른 인식과 함께 다수의 디바이스를 효율적으로 관리함으로써 스마트그리드의 안정적인 운영을 도울 수 있을 것이라 기대한다. 또한, 제안하는 그룹키 관리 기법은 스마트그리드 통신 환경 이외에도 센서 네트워크와 같이 상대적으로 낮은 사양의 디바이스를 사용하는 그룹 네트워크에서도 활용 가능하기 때문에 다양한 응용 환경에서 적용될 수 있을 것이다.

현재 우리나라뿐만 아니라 세계 각국에서는 스마트그리드 구축을 통해 녹색강국으로 발돋움하기 위한 노력으로 스마트그리드 관련 연구들이 활발히 진행되고 있다. 하지만 스마트그리드의 구축에 있어 무엇보다 중요한 것이 바로 스마트그리드 보안으로 안전한 통신 환경에서 원활한 스마트그리드 서비스를 제공해야 한다. 이에 따라 본 논문에서 제안하는 스마트그리드 통신 환경에 적용 가능한 효율적인 키 관리 기법은 안전한 스마트그리드 환경 구축에 활용될 수 있을 것으로 기대한다.

참고문헌

[1] C.L. Beaver, D.R. Gallup, W.D. NeuMann, and M.D. Torgerson, "Key management for SCADA," Technical Report, SAND 2001-3252, Mar. 2002.

[2] Chung Kei Wong, Mohamed Gouda, and Simon S. Lam, "Secure group communications using key graphs," IEEE/ACM Transactions on Networking, vol. 8, no. 1, pp. 16-30 , Feb. 2000.

[3] Donghyun Choi, Hakman Kim, Dongho Won, and Seungjoo Kim, "Advanced key-management architecture for secure SCADA communications," IEEE Transactions on Power Delivery, vol. 24, no. 3, pp. 1154-1163, Jul. 2009.

[4] Leslie Lamport, "Password authentication with insecure communication," Communications of the ACM, vol. 24, no. 11, pp. 770-772, Nov. 1981.

[5] National Energy Technology Laboratory, "Appendix B1: A systems view of the modern grid integrated communications," v2.0, Feb. 2007.

[6] NIST, "Smart Grid Cyber Security Strategy and Requirements," DRAFT NISTIR 7628, Feb. 2010.

[7] Robert Dawson, Colin Boyd, Ed Dawson and Juan Manuel Gonzalez Nieto, "SKMA: a key management architecture for SCADA systems," in Proceeding 4th Australasian Information Security Workshop, vol. 54, pp 138-192, 2006.

[8] T. Hardjono, B. Cain, and B. Dorsawamy, "A framework for group key management for multicast security," IETF Internet Draft, draft-ietf-ipsec-gkmframework-03.txt, Aug. 2000.

[9] 문승일, "스마트그리드 개념," 한국통신학회지, 제27권 제4호, pp. 3-9, 2010년 3월.

[10] 박창민, "스마트그리드 표준 기술," 한국통신학회지, 제27권 제4호, pp. 31-37, 2010년 3월.

[11] 이건희, 서정택, 이철원, "스마트그리드와 사이버 보안," 한국통신학회지, 제27권 제4호, pp. 23-30, 2010년 3월.

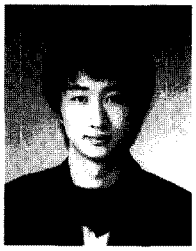
[12] 이경복, 독고지은, 유지연, 이숙연, 임종인, "스마트 그리드에서의 소비자 참여와 보안 이슈," 정보보호학회지, 제19권 제4호, pp. 11-20, 2009년 8월.

[13] 전용희, "스마트 그리드의 취약성, 특성, 설계 원칙 및 보안 요구사항 분석," 정보보호학회지, 제20권 제3호, pp. 79-89, 2010년 6월.

[14] 정영곤, 최현우, 염흥열, "스마트 그리드 보안 동향," 제20권 제4호, pp. 66-79, 정보보호학회지, 2010년 8월.

[15] 지식경제부, "세계최초 Smart Grid(지능형 전력망) 구축을 위한 상세 로드맵 수립착수," 지식경제부 전력산업과 보도자료, 2009년 3월.

〈著者紹介〉



은 선 기 (Sun-Ki Eun) 학생회원
2008년 8월: 호서대학교 정보보호학과 졸업(공학사)
2011년 2월: 호서대학교 정보보호학과 대학원 졸업(공학석사)
〈관심분야〉 네트워크 보안, 보안 프로토콜, 시스템 평가 및 인증

오 수 현 (Soo-Hyun Oh) 종신회원
1998년 2월: 성균관대학교 정보공학과 졸업(공학사)
2000년 2월: 성균관대학교 전기전자 및 컴퓨터공학과 석사(공학석사)
2003년 8월: 성균관대학교 전기전자 및 컴퓨터공학과 박사(공학박사)
2004년 3월~현재: 호서대학교 정보보호학과 교수
〈관심분야〉 암호학, 네트워크 보안 프로토콜, 시스템 평가 및 인증