JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 17, No. 9 : 2063~2072, Sep. 2013

안전한 스마트 그리드 환경을 위한 이중 해쉬 체인 기반 키 관리 프레임워크

이영석*

Key Management Framework based on Double Hash Chain for Secure Smart Grid Environments

Young-seok Lee*

Department of Telecommunication Engineering, Kunsan National University, Kunsan, Korea

요 약

스마트 그리드란 기존 전력망에 IT기술을 접목하여 공급자와 소비자가 양방향으로 실시간 전력정보를 교환함으로써 에너지 효율을 최적화하는 전력망이다. 기존의 폐쇄이던 전력망이 다양한 이해당사자가 참여하는 상호운용성이 보장되는 개방형 구조를 가지게 됨으로써 이에 대한 보안 기술 개발이 시급한 상태이다. 이러한 스마트그리드의 보안 위협에 대응할 수 있는 안전한 환경을 구축하기 위해서는 보안 메커니즘 개발에 핵심이 되는 키 관리 기법이 필수적으로 요구된다. 본 논문에서는 이중 해쉬 체인을 이용하여 스마트그리드 환경에 효율적으로 적용 가능한 키 관리 프레임워크를 제안하고, 제안하는 키 관리 프레임워크의 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 framework.

키워드 : 스마트 그리드, 스카다, 키관리, 이중 해쉬 체인

Key word : Smart Grid, SCADA, Key Management, Double Hash chain

접수일자 : 2013. 07. 18 심사완료일자 : 2013. 08. 09 게재확정일자 : 2013. 08. 27

* **Corresponding Author** Young-seok Lee(E-mail:leeys@kunsan.ac.kr, Tel:+82-63-469-4695)
Department of Telecommunication Engineering, Kunsan National University, Kunsan, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2013.17.9.2063 print ISSN: 2234-4772 online ISSN: 2288-4165

ⓒThis is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License(http://creativecommons.org/li-censes/by-nc/3.0/) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.
Copyright Ⓒ The Korea Institute of Information and Communication Engineering.

Ⅰ. 서 론

스마트 그리드란 기존 전력망에 IT기술을 접목하여 공급자와 소비자가 양방향으로 실시간 전력정보를 교환함으로써 에너지 효율을 최적화하는 차세대 전력망을 의미한다. 전력망이 스마트 그리드로 진화되면, 양방향 실시간 정보교환을 통하여 합리적 이고 효율적인 에너지 소비를 유도함으로써 고품질의 에너지 및 다양한 부가서비스의 제공이 가능해지고, 운영시스템의 개방적인 특성에 따라 신재생에너지발전, 전기차 등 청정 녹색기술의 접목 및 확장이 용이해 지게 된다.

이러한 스마트 그리드 환경에서는 신재생 에너지인 풍력, 태양광 등이 전력계통에 연계됨으로써 전력망 연결 접점이 많아지고, 기존 폐쇄적이던 전력망에 다양한 이해당사자가 참여함으로써 상호운영성이 보장되는 개방형 구조를 가지게 됨으로써 이에 대한 보안 기술 개발이 시급한 상태이다.

본 논문에서는 보다 안전하고 효율적인 스마트 그리드 통신 환경을 구축하기 위해 고려해야 하는 통신 품질 및 보안 요구사항들을 분석하고, 스마트 그리드의 통신 환경에 적용 가능한 키 관리 기법을 제안한다. 논문의 구성은 다음과 같다. 먼저 2장에서는 스마트 그리드 보안 요구사항과 함께 표준화 동향을 살펴본다. 3장에서는 기존 스마트 그리드 키 관리 기법들을 분석한다. 다음으로 4장에서는 스마트 그리드 환경에 적용 가능한 키 관리 기법을 제안하고, 5장에서는 제안하는 프로토콜의 안전성과 효율성을 분석하고 마지막으로 6장에서 결론을 맺는다.

Ⅱ. 스마트 그리드

2.1. 스마트 그리드

스마트 그리드의 구성요소에 대해서는 각 국가 별로 차이가 존재한다. 이는 스마트 그리드가 개발 완료된 시스템이 아니라 개발 중인 시스템이기 때문이다. 일반적으로 스마트 그리드를 구성하기 위해 요구되는 주요 구성요소는 다음과 같다.

먼저 전력의 송배전 등을 안전하고 효율적으로 관리하는 SCADA와 다양한 전력 관련 정보의 전달에 사용되는 통신로, 전력의 계량과 관련된 고도화된 검침 기반시설 (Advanced Metering Infrastructure), 사용자와 기기 간 정보 전달을 위한 시각화 기법 및 기기간의 호환성 등에 대한 인터페이스 등이 스마트 그리드의 주요 구성요소로 언급되고 있다.

이러한 스마트 그리드의 전체 구성과 그 안에서의 전기와 정보의 흐름을 표현한 것이 그림 1이다[1-2]. 그림에서 사용된 용어는 다음과 같다.

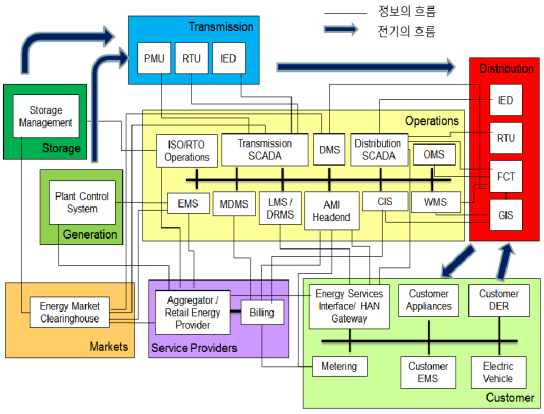

그림 1. 스마트 그리드 구성도
Fig. 1 Smar Grid Construction

- Customer EMS (Customer Energy Management System) : 고객 에너지 관리 시스템으로 고시된 전력 가격에 따라 전력 사용량을 조절하고, 잉여 전력을 판매함
- EMS (Energy Management System) : 전력의 수요에 맞게 효율적인 전력 생산이 가능하도록 관리하는 시스템
- PCS (Plant Control System) : 발전소를 관리하는시스템
- DMS (Distribution Management System) : 배전을 관리하는 시스템
- LMS/DRMS (Load Management System/Demand Response Management System) : 전력의 송배전데이터와 각 가정의 전력 사용량을 분석하고 이를 관리하는 시스템
- OMS (Outage Management System) : 단전을 관리하는 시스템
- WMS (Work Management System) : 수리가 필요한 작업을 관리하는 시스템

- CIS (Customer Information System) : 고객 정보를 관리하는 시스템
- GIS (Geographic Information System) : 지리 정보를 제공하는 시스템
- FCT (Field Crew Tools) : 무선 통신이 가능한 단말기로 배전과 고객, 지리정보를 이용하여 작업자가 이를 활용하여 단전 등의 기타 수리를 진행함
- ISO/RTO (Independent System Operator/Regional Transmission Oraganization) : 독립 시스템 운영기관/지역 송전 기관
- PMU (Phasor Measurement Unit) : 송전과정의electrical wave를 측정하는 장치
- IED (Intelligent Electronic Device) : RTU와 동일한 기능을 수행함

2.2. 스마트 그리드 보안 요구사항

- 데이터 기밀성 : 스마트 그리드 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 : 스마트 그리드 환경에서 전송되는 미터 사용량, 요금 관련 정보, 제어 메시지 등이 불법적인 접근에 의해 위・변조되지 않도록 보장해야 한다.
- 시스템 가용성 : 스마트 그리드 환경에서 안정적 이고 지속으로 실시간 양방향 통신을 제공하기 위해 디바이스, 시스템 및 네트워크의 가용성이 보장되어야 한다[3].
- 상호인증 : 스마트 그리드 환경에서 공격자가 정상적인 사용자로 위장함으로써 사용자 측에서 원활한 서비스 제공을 받지 못하게 하거나 공격자가 전력 공급자로 위장함으로써 사용자의 개인정보 등을 탈취하는 등의 위협에 대응하기 위해각 구성 요소들 간의 상호인증을 제공해야 한다.
- 접근제어 및 인가 : 스마트 그리드 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 : 스마트 그리드에서 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 보호수단에 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 스마트 그리드의 통신 네트워크를 오염시키거나 스마트 그리드 서비스의 가용성을 손상시킬 수 있다. 따라서 디바이스에 대한 무결성 검증이 요구된다.
- 프라이버시 보호 : 스마트 그리드 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.

2.3. 스마트 그리드 보안 표준화 동향

미국국립표준기술연구소인 NIST[4]는 스마트 그리드에 대한 표준화를 주도하며 스마트 그리드 연구개발 및 표준화를 비롯하여 산업계에 많은 영향을 주고 있다. NIST에서는 2010년 스마트 그리드 상호운용성을 위한 프레임워크 및 로드맵 1.0을 발표하여 시장, 운영, 서비스 제공자, 발전, 송전, 배전, 소비자 각 도메인에 따른 스마트 그리드 참조 모델을 정의하고 ISO, IEEE, NERC, ISA, OASIS 등 타 표준화기구의 스마트 그리드 표준을 검토함으로써 스마트 그리드 표준화가 필요한 8개의 우선 추진 영역을 표 1과 같이 선정하였다.

2012년 2월에는 스마트 그리드 상호운용성을 위한 프레임워크 및 로드맵 2.0[5]을 발표하여 1.0에서 정의한개념적인 참조 모델에 대한 내용을 업데이트하고, 사이버보안과 테스팅 및 인증 분야의 결과물들을 반영하였다.

표 1. 스마트 그리드 표준화 우선 추진 분야
Table. 1 First Propulsion for Smart Grid Standard

	주요 추진 분야
1	Energy Storage
2	Demand Response & Consumer Energy Efficiency
3	Wide-Area Situational Awareness
4	Electric Transportation
5	Advanced Metering Infrastructure
6	Distribution Grid Management
7	Cyber Security
8	Network Communications

또한 NIST에서는 스마트 그리드 표준들의 조화 및 신속한 표준화 추진을 위해 스마트 그리드 참여자 간의 의견 조정 역할을 수행하는 스마트 그리드 상호운용성 패널(Smart Grid Interoperability Panel, SGIP)을 설립하였고, SGIP에 스마트 그리드 보안을 담당하는 사이버 보안 워킹그룹(Cybersecurity Working Group)을 만들어 2010년 스마트 그리드 표준 개발 시 보안성 평가의 기준을 제공하는 스마트 그리드 사이버보안 가이드라인(NISTIR 7628)[6]을 발표하였다.

스마트 그리드 보안 가이드라인은 스마트 그리드 응용분야 및 서비스에 대한 적용 사례 분석에서 논리적 인터페이스 및 취약점 분석을 통한 보안 위협 평가, 논리적 인터페이스에 따른 상위 수준의 보안 요구사항 도출, 스마트 그리드 보안 구조 개발 및 관련 표준 분석, 보안 요구사항 및 구조에 대한 준수 여부를 검증하기 위한 평가기술 개발까지의 사이버보안 전략과 함께 스마트 그리드 논리적 구조 및 인터페이스, 상위 수준의 보안 요구사항, 암호 및 키 관리 이슈를 기술한다.

Ⅲ. 키 관리 기술 동향

현재 스마트 그리드와 관련하여 안전한 키 관리 기술이 연구되고 있는 분야는 SCADA와 AMI 부분이다. 3장에서는 SCADA에서의 키 관리 기술에 대해 살펴본다.

3.1. SKMA

Queensland University of Technology에서 발표한 SKMA는 SCADA 시스템을 위한 키 관리 방식이다[7]. SKE가 공개키 암호 알고리즘을 사용하는 반면 SKMA는 대칭키 암호 알고리즘으로만 이루어져 있다는 장점이 있다. 여기서 노드는 RTU, SUB-MTU, MTU 모두 될 수 있다. SKMA에서 사용되어지는 키는 다음과 같다.

- Long term node-KDC key: 이 키는 node와 KDC사이에 공유되는 키로 통신을 위해 키를 설정할 때 사용된다.
- Long term node-node key : 노드와 노드사이에 공유되는 키이다.
- Session Key : 메시지를 암호화 하는데 사용되는 키이다.
- Node-KDC Key : 이 키는 수동적으로 설치되며, node와 node사이의 키를 생성할 때 사용된다.

Node-KDC 키는 노드가 시스템에 배포되기 전에 설치된다. 새로운 노드가 추가될 때 node-node 키가 그림 2와 같은 과정을 통해서 교환된다.

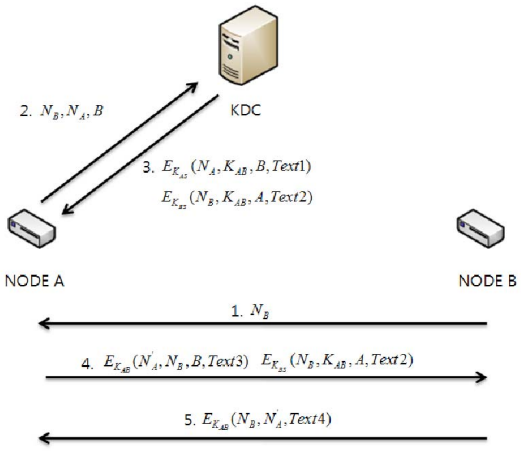

그림 2. SKMA 키 관리 방식
Fig. 2 SKAM Key Management Method

위와 같이 SKMA에서는 서버와 노드 A, 노드 B간의 3자간 키 확립 프로토콜을 사용하는데 이는 ISO 11770-2 메커니즘 9를 기본으로 한다[8]. 통신에서 데이터를 암호화하는데 사용되는 세션키는 3자간 키 확립프로토콜로 얻은 node-node 키와, 타임스탬프(세션의 유지기간에 기반을 둔)값의 해쉬하여 생성한다.

키 철회 메커니즘은 KDC에 의해서 수행되어진다. 키가 공격당했다는 사실을 자동적으로 알려주는 알고리즘은 현재 없다. 다만 시스템을 모니터링하다 이상행동을 발견하면 해당 노드와 관련된 키를 철회 한다. KDC 해당 노드의 키가 철회 되었다는 사실을 다른 모든 노드에게 알려야한다. 이때 사용되는 메시지는 각각의 노드와 KDC간의 키로 암호화해서 전송되어진다.

3.2. ASKMA

2008년에 Choi 등이 제안한 논문으로 LKH (Logical Key Hierarchy) 구조를 이용한 방식이다[9]. 제안하는 방식의 핵심은 RTU와 SUB-MTU사이의 키는 n-ary 방식으로 구성하고 SUB-MTU와 MTU 사이는 binary tree로 구성하는 것이다. 이를 그림으로 표현하면 그림 3과 같다.

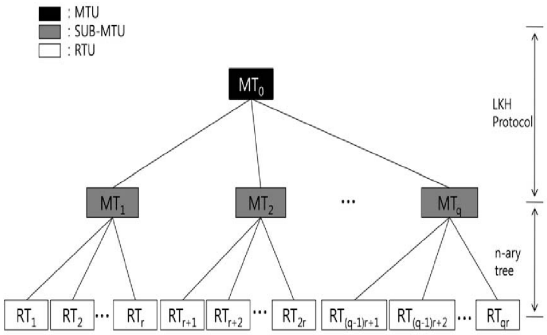

그림 3. ASKMA 키 관리 방식
Fig. 3 ASKAM Key Management Architecture

제안된 방법은 SKE 와 SKMA 방식이 broadcasting을 지원하지 못하는 반면에 ASKMA는 이를 지원하는 장점을 가지고 있다. 또한 이러한 키 관리 구조를 통해 RTU에 저장되는 키의 수를 최소화 하여 성능상의 제약을 가지고 있는 RTU에 계산상의 많은 부하가 걸리는 것을 방지하였다.

3.3. ASKMA++

2010년에 Choi 등이 제안한 논문으로 이전에 제안한 ASKMA에 효율성을 보다 향상시킨 논문이다[10]. 제안하는 핵심아이디어는 다음과 같다. 먼저 키 관리 구조를 MTU와 SUB-MTU 그리고 SUB-MTU와 RTU로 나누고 각각의 키 관리 구조를 LKH(Logical Key Hierarchy)구조로 구성하는 것이다. 그리고 이 두 개의 구조를 Ioulus Framework를 이용하여 연결시키는 방식을제안하고 있다. 구조는 그림 4와 같다.

제안하고 있는 방식은 RTU와 SUB-MTU간의 키 관리를 보다 효율적으로 사용이 가능하게 하였다. 또한 각의 SUB-MTU가 분리됨으로써 서로 영향을 주지 않아 더욱더 효율적이게 되었다.

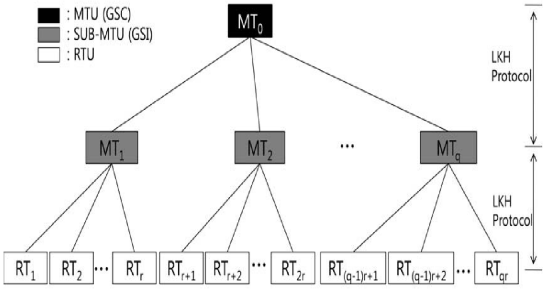

그림 4. ASKMA 키 관리 방식
Fig. 4 ASKAM Key Management Architecture

Ⅳ. 해쉬 체인 키 관리 프레임워크

4장에서는 스마트 그리드 환경에서 효율적으로 디바이스들을 관리하기 위해 필요한 그룹키 관리 기법을 제안한다. 제안하는 그룹키 관리 기법은 전력 사용자가 스마트 그리드 서비스를 제공받기 위해 새로운 스마트 미터를 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[11].

제안하는 그룹키 관리 기법에서 사용하는 표기와 의미는 표 2와 같다.

각 가정 또는 전력 사용자 측에 배치되는 스마트미터 M들과 DCU D들은 사전에 각자의 비밀키 K_M, K_D를 할당받아 안전하게 저장한다. 또한 AMI 서버 A와 DCU D들은 파라미터 b에 대해서 다음과 같이 k길이 만큼의 해쉬 체인을 사전에 계산하여 안전하게 저장한다.

표 2. 표기법
Table. 2 Notation

표기	의미
M_e	기존의 스마트미터
M_s	스마트그리드 서비스에 가입하는 스마트미터
M_w	스마트그리드 서비스를 탈퇴하는 스마트미터
K_M	스마트미터 M의 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(x)	해쉬함수

여기서 *i*는 해쉬 체인의 끝에서부터 증가하는 값을 의미한다.

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

그리고 원활한 그룹키 갱신을 수행하기 위해 파라미터 *f*에 대해서도 *k*길이만큼의 해쉬 체인을 계산하여 저장한다.

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

해쉬 함수(hash function)는 임의의 길이의 데이터를 특정 길이로 줄여주는 압축의 의미를 가지며, 시스템 구성 과정에서 데이터의 중복검사를 쉽게 한다. 실질적인 메시지의 무결성(identity)의 효과를 얻기 위해서 인증(authenticity) 기능을 갖는 암호함수와 결합되어 사용되는 경우가 많다. 일반적으로 단일 해쉬 체인은 seed 값 x가 주어졌을 때, 이를 기반으로 반복적인 일방향 해쉬 함수 *h*의 적용을 통해서 나오는 값들의 체인 $h^1(x), h^2(x), ..., h^n(x)$를 의미한다. 여기서 $h^i(x)$의 의미는 x에 해쉬 함수를 i번 반복 적용한 결과 값이다. $h^i(x)$로부터 $h^{i+1}(x)$의 값은 계산할 수 있으나, $h^{i-1}(x)$는 도출할 수 없는 일방향성 해쉬 함수 특성 때문에 해쉬 체인은 소액 전자현금이나 일회용 패스워드 매커니즘에 이용되어 왔다. 본 논문에서 제안하는 이중 해쉬 체인은 단일 해쉬 체인과 달리 특정 해쉬 체인 값이 주어졌을 때 양방향 모두 계산이 불가능 함으로써 특정 해쉬 체인 값의 무결성을 보장하기 위한 목적으로 제안된다. 단일 해쉬 체인이 아닌 이중 해쉬 체인을 생성하는 이유는, 하나의 해쉬 체인을 사용하는 경우 무결성을 위협하는 공격이 가해질 수 있기 때문이다[12].

2개의 seed 값 x와 y를 임의로 선정한 후, 일방향 해쉬함수 *h*를 이용하여 길이가 n인 2개의 해쉬 체인을 형성한다. 여기서 $h^n(x) \oplus h^n(y) = v$를 이중 해쉬 체인 확인자로 정의한다. 해쉬 체인을 작성한 사용자는 확인자 v에 대해서 자신의 서명한 값을 다른 사용자에게 전송하고, 서명을 수신한 사용자는 송신자의 공개키 확인 후 값을 저장한다. 그 해쉬 체인 작성자는 임의의 $j \in [1, n-1]$값을 그림 5와 같이 무결성이 보장되게 전송할 수 있다.

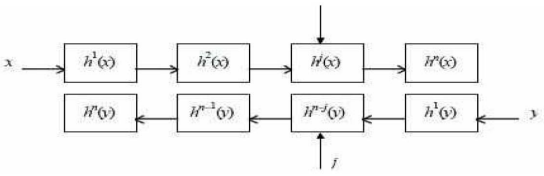

그림 5. 이중 해쉬 체인
Fig. 5 Double Hash Chain

$\{j, h^j(x), h^{n-j}(y)\}$ 메시지 수신자는 $h^j(x)$와 $h^{n-j}(y)$에, 각 각 n-j번과 j번의 해쉬 함수를 반복 적용하여 나온 결과 값 $h^n(x)$, $h^n(y)$를 XOR한 값과 자신이 저장하고 있던 확장자 v가 일치하는지 확인하게 된다. 해쉬 함수를 기반으로 하는 시스템의 안전성은 해쉬 함수가 역방향으로 계산하기 어렵다는 해쉬 함수의 일방향성에 기반한다. 이러한 해쉬 함수를 이용하여 해쉬 체인을 구성하고 두 개의 해쉬 체인을 이용하여 이중 해쉬 체인 알고리즘을 구성한다.

제안하는 그룹키 기법에서 *i*+*j*번째 그룹키 K_G^{i+j}는 스마트미터 *M*의 가입 또는 탈퇴에 따라 파라미터 *b*에 대한 해쉬체인의 값 $h^{k-1}(b)$과 파라미터 *f*에 대한 해쉬 체인 값 $h^j(f)$을 선택하고, 두 값을 XOR 연산하여 생성한다. 여기서 *i*값은 기존의 스마트미터 M_e가 탈퇴했을 때 증가하고 *j*값은 새로운 스마트미터 M_s가 가입했

을 경우 증가한다.

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

또한 제안하는 키 관리 기법에서는 AMI 서버 *A*에서 DCU *D*및 스마트미터 *M*의 물리적 위치를 알고 있다고 가정하며, 키 구조는 그림 6과 같이 AMI 서버 *A*와 DCU *D*그리고 DCU *D*와 스마트미터 *M*간에는 n-ary트리로 구성된다. 하지만 각각의 DCU *D*에 속해 있는 스마트미터 *M*들의 개수는 DCU *D*마다 다를 수 있다.

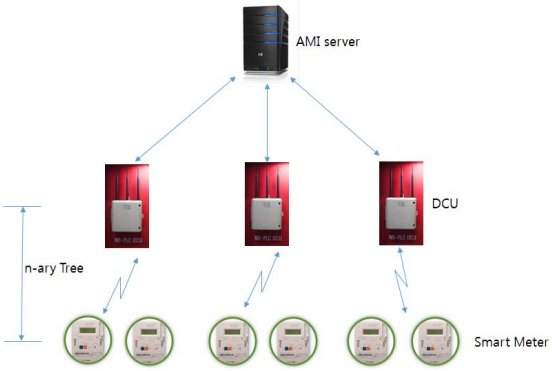

그림 6. 키 관리 구조
Fig. 6 Key Management Structure

AMI 시스템에 새로운 스마트미터 M_s를 등록하기 위한 프로토콜은 다음과 같다.

1. AMI 서버 A는 전력 사용자의 물리적 위치를 파악한 후, 스마트미터 M_s의 비밀키 K_{M_s}를 해당 DCU D에게 전달한다.
2. DCU *D*는 현재 DCU *D*에서 관리하는 기존의 스마트미터 M_e들이 가지고 있는 파라미터 *b*에 대한 해쉬체인의 값이 $h^{k-i}(b)$이고 파라미터 *f*에 대한 해쉬체인의 값이 $h^j(f)$일 경우, 새롭게 가입한 스마트미터 M_s에게 $h^{k-i}(b)$값과 $h^{j+1}(f)$값을 스마트미터 M_s의 비밀키 K_{M_s}로 암호화하여 전달한다.
3. 스마트미터 M_s는 DCU *D*로부터 전달받은 메시지를 자신의 비밀키 K_{M_s}로 복호화하여 $h^{k-i}(b)$과 $h^{j+1}(f)$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 *D*에게 올바른 그룹키 K_G^{i+j+1}생성을 알리기 위해 자신의 비밀키 K_{M_s}와 그룹키 K_G^{i+j+1}을 해쉬한 값 $h(K_{M_s} \| K_G^{i+j+1})$을 DCU *D*에게 전달한다.

스마트미터의 고장과 같은 원인으로 기존의 스마트미터 M_e를 교체해야 할 경우 다음의 탈퇴 프로토콜을 수행한다.

1. AMI 서버 *A*는 탈퇴하는 스마트미터 M_w의 물리적 위치 및 스마트미터 M_w의 비밀키 K_{M_W}등과 같은 전력 사용자의 개인 정보들을 AMI 서버 *A*에서 삭제한다. 그 후에 DCU *D*에게 스마트미터 M_w의 탈퇴 사실과 함께 그룹키 갱신 메시지를 전달한다.
2. DCU *D*는 탈퇴한 스마트미터 M_w가 그룹 통신에 대한 정보를 알 수 없도록 현재의 그룹키 K_G^{i+j}에 대한 그룹키 갱신 절차를 수행한다. 가입 프로토콜에서와 마찬가지로 현재 DCU *D*에서 관리하는기존의 스마트미터 M_e들이 가지고 있는 파라미터 *b*에 대한 해쉬체인의 값이 $h^{k-i}(b)$이고 파라미터 *f*에 대한 해쉬체인의 값이 $h^j(f)$일 경우, DCU *D*는 $h^{k-(i+1)}(b)$을 탈퇴한 스마트미터 M_w를 제외한 기존의 스마트미터 M_e들에게 각자의 비밀키 K_{M_e}로 암호화하여 각각 전달한다.
3. 기존의 스마트미터 M_e는 DCU *D*로부터 전달받은 메시지를 자신의 비밀키 K_{M_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 *D*에게 올바른 그룹키 K_G^{i+j+1}가 생성되었음을 알리기 위해 자신의 비밀키 K_{M_e}와 생성한 그룹키 K_G^{i+j+1}을 해쉬한 값 $h(K_{M_e} \| K_G^{i+j+1})$을 DCU *D*에게 전달한다.
4. DCU *D*는 기존의 스마트미터 M_e들에게 전달받은 값 $h(K_{M_e} \| K_G^{i+j+1})$와 자신이 생성한 $h(K_{M_e} \| K_G^{i+j+1})$이 동일한지 판단함으로써 각각의 스마트미터 M_e

에서 올바른 그룹키 K_G^{i+j+1}을 생성하였는지 확인한다.

Ⅴ. 보안성 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 스마트 그리드 서비스에 등록된 스마트미터 *M*에게만 그룹키 K_G^{i+j}에 대한 키 재료(material)인 파라미터 *b*의 해쉬체인 값 $h^{k-i}(b)$와 파라미터 *f*의 해쉬체인 값 $h^j(f)$을 스마트미터 의 비밀키 K_M로 암호화하여 안전하게 전달한다. 제안하는 키 관리 기법에서는 스마트 그리드 서비스에 등록되지 않은 사용자의 경우, DCU *D*에 자신의 스마트미터 비밀키 K_M가 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. 그러므로 제안하는 키 관리 기법은 그룹키 안전성을 제공한다.
- 전방향 안전성(Forward Secrecy) : 그룹키의 전방향 안전성은 스마트 그리드 서비스를 해지한 스마트미터 M_w이 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 *M*가 서비스를 해지할 경우, 해지한 스마트미터 M_w을 제외한 기존의 스마트미터 M_e들에게 $h^{k-(i+1)}(b)$를 기존 스마트미터들의 비밀키로 암호화하여 전달함으로써 그룹키 $K_G^{i+1} = h^{k-(i+1)}(b) \oplus h^j(f)$를 갱신한다. 하지만 탈퇴한 스마트미터 M_w은 키 재료 $h^{k-(i+1)}(b)$를 받지 못하므로 새로운 그룹키$K_G^{i+1} = h^{k-(i+1)}(b) \oplus h^j(f)$를 계산할 수 없다. 따라서 제안하는 키관리 기법은 그룹키에 대한 전방향 안전성을 제공한다.
- 후방향 안전성(Backward Secrecy) : 그룹키의 후방향 안전성은 스마트 그리드 서비스에 가입한 새로운 스마트미터 M_s가 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 M_s가 서비스 그룹에 가입한 경우, 새로운 스마트미터에게 $h^{k-i}(b)$와 $h^{j+1}(f)$를 안전하게 전달하여 새로운 스마트미터 M_s가 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 관리기법은 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 영향주지 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 3, 표 4와 같다.

표 3. 보안성 비교 분석
Table. 3 Security Analysis

방식	메시지 브로드캐스트	그룹키 안전성	전방향 안정성	후방향 안전성
SKMA	×	-	-	-
ASKMA	×	O	O	O
제안기법	O	O	O	O

표 4. 메시지 수 및 키 수 비교 분석
Table. 4 Message and Key count Analysis

방식	스마트미터에 저장되는 키의 수	스마트미터 탈퇴시 변경되는 그룹키의 수	스마트미터 탈퇴시 전송되는 메시지의 수
SKMA	1	-	-
ASKMA	$2+\log_2 q$	$1+\log_2 q$	n
제안기법	2	1	n-1

Ⅵ. 결 론

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 스마트 그리드에서 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 스마트 그리드 통신 환경에서 고려해야 하는 통신 품질 및 보안 요구사항들을 분석하였고, 안전하고 효율적인 스마트 그리드 통신 환경을 구축하는데 필요한 그룹키 관리 기법을 제안하였다. 제안하는 그룹키 관리 기법은 안전하게 생성된 그룹키를 사용함으로써 스마트 그리드에서 발생할 수 있는 누전이나 정전과 같은 전력사고 시에 적절한 그룹 메시지를 전송함으로써 위급상황에 대한 빠른 인식과 함께 다수의 디바이스를 효율적으로 관리함으로써 스마트 그리드의 안정적인 운영을 도울 수 있을 것이라 기대한다.

또한, 제안하는 그룹키 관리 기법은 스마트 그리드 통신 환경 이외에도 센서 네트워크와 같이 상대적으로 낮은 사양의 디바이스를 사용하는 그룹 네트워크에서도 활용 가능하기 때문에 다양한 응용 환경에서 적용될 수 있을 것이다.

감사의 글

이 논문은 2011년도 군산대학교 교수장기국외 연수경비의 지원에 의해 연구되었음.

REFERENCES

[1] NIST, “NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0”, NIST Special Publication, 01. 2010.

[2] NIST, “Smart Grid Cyber Security Strategy and Requirements”, Draft NISTIR 7628, 02. 2010.

[3] Y. G. Jung, et al, “Smart Grid Security Trend”, Korea Institute of Information Security & Cryptology, Vol. 20, No. 4, pp. 66-79, Aug. 2010.

[4] NIST smart grid, http://www.nist.gov/smartgrid/

[5] NIST Special Publication 1108R2, “NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0”, 2012. 2.

[6] NISTIR 7628, “Guidelines for Smart Grid Cyber Security”, 2010. 8.

[7] R. D. Colin, C. Boyd, J. Manuel, and G. Nieto, “KMA-A key management architecture for SCADA systems,” in Proc. 4th Australasian Inf. Security Workshop, Vol.54, pp. 138-192, 2006.

[8] Information Technology - Security Techniques - Key Management - Part 2: Mechani는 Using Symmetric Techniques ISO/IEC 11770-2 International Standard, 1996.

[9] D. Choi, H. Kim, D. Won, and S. Kim, “Advanced Key Management Architecture for Secure SCADA Communications”, IEEE Transactions on Power Delivery, Vol.24, No.3, pp.1154-1163, 2009.

[10] D. Choi, S. Lee, D. Won, and S. Kim, “Efficient Secure Group Communications for SCADA”, IEEE Transactions on Power Delivery, Vol.25 No.2, pp. 714-722, 2010.

[11] S. K. Eun, S.H. Oh, “Hash chain based Group Key Management Mechanism for Smart Grid Environments,” Korea Institute of Information Security & Cryptology, Vol. 21, No. 4, pp. 149-160, Aug. 2011.

[12] Yoon-Su Jeong, “A Key Pre-distribution Scheme Using Double Hash Chain for Strong Security Strength of Wireless Sensor Node,”pp.569~643,2008.

이영석(Young-seok Lee)

1992년 충남대학교 컴퓨터공학과 공학사
1994년 충남대학교 컴퓨터공학과 공학석사
2002년 충남대학교 컴퓨터공학과 공학박사
1994년 ~ 1997년 LG전자정보통신연구소 연구원
2002년 ~ 2004년 한국전자통신연구원 선임연구원
2004년 ~ 현재 군산대학교 정보통신공학과 부교수
※관심분야 : 정보보호, 이동컴퓨팅, 컴퓨터네트워크