스마트 그리드 환경에서 윈도우를 이용한 경량화된 그룹 키 분배 기법 연구

고웅*, 곽진**
*순천향대학교 정보보호학과 정보보호응용및보증연구실
**순천향대학교 정보보호학과
e-mail:wgo@sch.ac.kr, jkwak@sch.ac.kr

A Study on Lightweight Group Key Distribution using Window for Smart Grid

Woong Go*, Jin Kwak**
*ISAA, Dept of Information Security Engineering, Soonchunhyang University
**Dept of Information Security Engineering, Soonchunhyang University

요 약

스마트 그리드는 기존의 전력망과 함께 양방향 통신을 위한 정보통신기술이 접목된 형태로, 전기의 생산, 운반, 소비뿐만 아니라 사용량 확인, 상호작용 등의 과정을 효율적으로 제공한다. 이와 같은 환경에서 전송되는 정보는 개인의 소비 성향과 같은 민감한 정보를 포함하고 있으므로, 안전한 통신을 위한 암호화가 필수적으로 요구된다. 특히, 다수의 장치가 계층적 구조를 이루는 스마트 그리드 환경에서는 암호화를 위하여 효율적인 그룹 키 사용이 필수적으로 요구된다. 따라서 본 논문에서는 스마트 그리드 환경에서 효율적인 그룹 키 분배를 위하여 그룹 키 원소 배열에서 일정 범위를 한정하는 윈도우를 이용한 기법을 제안한다.

1. 서론

전 세계적으로 효율적인 에너지 관리 및 안전한 서비스 제공을 위한 관심이 증가하면서, 기존 전력망에 정보통신기술을 접목한 스마트 그리드에 대한 연구 및 서비스 개발이 활발히 진행되고 있다. 스마트 그리드는 기존 전력망과 함께 양방향 통신을 위한 정보통신기술이 접목된 형태로, 전기의 생산, 운반, 소비뿐만 아니라 사용량 확인, 상호작용 등의 과정을 효율적으로 제공한다[1].

이와 같이 스마트 그리드에 적용된 정보통신기술로 인해 전력회사는 실시간으로 전력 소비량을 확인하고 분석할 수 있으며, 결과를 바탕으로 전력 공급을 효율적으로 관리할 수 있게 된다. 또한, 사용자의 경우에는 현재 사용하는 가전기기의 전력 사용량을 실시간으로 확인할 수 있으며, 가정 내 전력 사용을 효율적으로 관리할 수 있다. 이러한 시스템이 가능한 이유는 양방향 통신을 통해 사용자의 정보 및 전력 사용량 등이 실시간으로 송수신되기 때문이다. 따라서 사용자의 전력 소비 성향, 가정 내 사람의 유무 등과 같은 민감한 개인정보를 포함하고 있는 송수신 데이터를 안전하게 보호하기 위한 기술이 필수적으로 요구된다[3].

그러나 아직까지 스마트 그리드에서 데이터 보안에 대한 연구가 초기 단계에 머물러 있어서, 이와 관련된 그룹 키 관리 기술 연구가 미흡한 상황이며, 기존 네트워크에서 발생하던 데이터 유출 및 위/변조 등의 보안상 문제가 스마트 그리드에서 전송되는 전력 정보에도 동일하게 발생할 가능성이 존재한다. 따라서 스마트 그리드 환경에 적합한 효율적인 그룹 키 관리 기술 개발이 필수적으로 요구된다.

따라서 본 논문에서는 스마트 그리드 환경에서 안전한 통신을 위하여 윈도우를 이용한 경량화 된 그룹 키 분배 기법을 제안한다. 본 기법은 그룹 키 원소 배열을 구성하고 일정한 윈도우 간격마다 원소를 추출하여 그룹키를 생성하는 방식이다.

본 논문의 구성은 다음과 같다. 2장은 스마트 그리드에 대한 분석을 하고, 3장은 스마트 그리드의 문제점을 분석한다. 4장은 본 논문의 제안사항을 기술하고, 5장을 결론으로 끝을 맺는다.

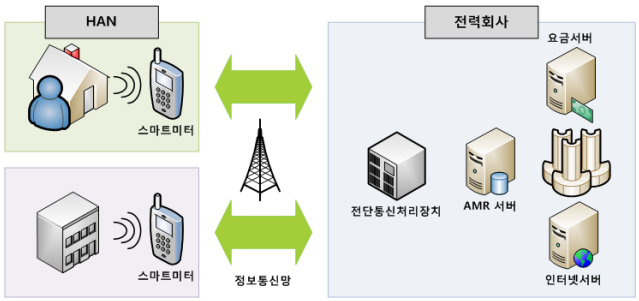
2. 관련연구

2.1 스마트 그리드

스마트 그리드는 전력망과 정보통신기술의 융합을 이용한 지능형 전력망으로 중전, 통신, 가전, 건설, 자동차, 에너지 등과 같은 유관 산업과의 시너지 기회를 제공할 수 있는 국가 단위의 녹색성장 플랫폼이라고 할 수 있다[2]. 이러한 스마트 그리드는 전 세계적으로 관심이 증가하고 있으며, 환경 구축을 위한 다양한 연구가 진행되고 있다.

본 연구는 지식경제부 및 정보통신산업진흥원의 대학IT연구센터육성 지원사업의 연구결과로 수행되었음.
(NIPA-2012-H0301-12-3007)

기존의 전력망이 전력 공급자에 의한 일방적인 의사소통이 이루어졌다면, 스마트 그리드 환경에서는 정보통신 기술로 인해 전력 공급자와 사용자가 양방향으로 실시간 전력 정보를 교환할 수 있다. 따라서, 전력 공급자와 사용자 사이에서 보다 효율적으로 전력 운영이 가능하다[3].



(그림 1) 스마트 그리드의 구조

2.2 키 분배 기술

스마트 그리드 환경에서의 키 분배 기술 연구는 송/배전시 사용되는 SCADA(Supervisory Control And Data Acquisition) 시스템에서의 연구가 주를 이루고 있다. 현재까지 스마트 그리드에서 표준으로 지정된 키 관리 기술은 없으며, 이를 위한 다양한 연구가 진행되고 있다.

SCADA 시스템은 원격지에 설치된 센서들의 정보를 수집하여 중앙에서 효율적으로 감시 및 제어하기 위한 시스템이다. 이와 관련하여 Sandia National Laboratories에서 제안한 SKE 프로토콜[4]이 있으며, MTU와 RTU 또는 SUB-MTU와 RTU 사이의 계층적 구조에서의 키 분배 프로토콜을 제안하고 있다. 또한, Dawson 등에 제안한 SKMA 프로토콜[5]은 새로운 RTU가 시스템에 등록될 경우, RTU간의 세션키 설립을 위한 키 관리 기법을 제안하고 있다. ASKMA[6]는 LKH(Logical Key Hierachy) 구조를 이용한 방식으로, 상위 MTU와 SUB-MTU 간의 이진 트리 형식으로 구성된 관계에서 메시지 브로드캐스트를 지원하는 그룹키 관리 기법을 제공한다[7].

3. 문제점 분석

3.1 전력 정보 노출

스마트 그리드에서는 사용자가 사용한 전력 정보를 실시간으로 송수신할 수 있는 환경을 제공한다. 전력정보의 경우, 이를 불법적으로 도청하여 전력 사용 내역을 분석하게 되면 사용자의 전력 소비 성향, 가정 내 가전기기의 유무, 사용자가 집에 머물고 있는지 여부 등을 알아낼 수 있다. 분석 결과를 이용하여 공격자가 사용자가 집에 없는 시간에 침입하여 물건을 훔치는 등 2차적인 피해를 발생시킬 수 있으며, 사용자 개인의 사생활 정보들을 알아낼 수 있게 된다.

3.2 불법적인 전력 정보 위/변조

현재 전력망은 사용한 전력량에 대한 과금을 집행하고 있다. 따라서 전송되는 전력 사용량을 불법적으로 위/변조할 경우, 사용자와 전력회사의 경제적 문제가 발생할 수 있다. 먼저, 공격자가 특정 사용자의 전력 사용량을 위/변조하여 실제 사용하지 않은 전력량을 추가하게 되면, 사용자는 자신이 사용하지 않은 전력량에 대한 과금을 수행하여야 하는 문제가 발생할 수 있다. 또한, 불법적으로 전력 사용량을 축소할 경우, 실제 사용된 전력량보다 적은 비용을 과금하게 됨으로써 전력회사의 피해가 발생하게 된다.

4. 제안 기법

본 논문에서는 스마트 그리드에서 스마트미터와 전력회사 간의 데이터를 안전하게 송수신하기 위한 그룹 키 분배 기법을 제안한다. 제안하는 기법은 최초 그룹 키를 생성하기 위해 전력회사와 스마트미터가 동일한 난수생성 알고리즘을 통해 랜덤하게 키 원소 배열을 생성하고, 임의의 크기의 윈도우를 선택하게 된다. 그 후, 키 원소 배열에서 윈도우 크기 간격으로 키 원소를 선택하여 그룹 키를 생성한다.

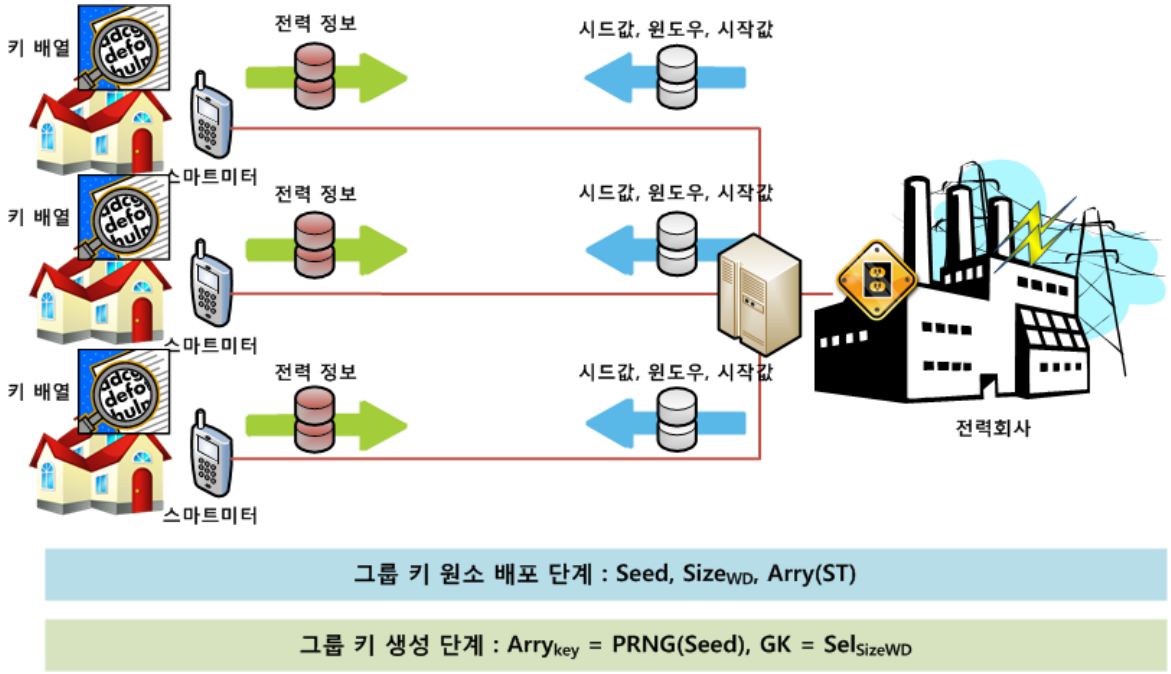
본 기법은 그룹 키 생성 요소 분배 단계와 그룹 키 생성 단계로 나뉘며, 그룹 키 생성 요소 분배 단계에서는 전력회사가 랜덤한 키 원소 배열을 생성하기 위한 시드값과 윈도우 크기, 시작 위치를 선택하여 스마트미터에 배포하는 단계이다. 그룹 키 생성 단계는 시드값을 이용하여 랜덤 키 원소 배열을 생성하고, 윈도우 크기에 따른 간격에서 원소를 선택하여 그룹 키를 생성한다. 그룹 키 생성 요소를 안전하게 전송하기 위한 암호화키는 최초 스마트미터를 제작할 때 전력회사가 포함시킨다. 그림 2는 본 논문의 제안 기법 구조를 나타낸 것이다.

4.1 표기법

다음 표 1은 본 논문에서 제안한 기법에 사용된 표기들을 나열한 것이다.

<표 1> 표기법

표기법	설명
$Seed$	시드값
$Size_{WD}$	윈도우 크기값
$Arry_{ST}$	시작 원소 지정값
k	암/복호화 키 (사전 분배된 대칭키)
$Arry_{key}[]$	그룹키 생성을 위한 원소 배열
$PRNG()$	의사난수생성기
$Sel_{Arry_{ST}}$	배열의 시작 원소 위치 지정
GK	그룹 키
$Sel_{ST+Size_{WD}}()$	시작 위치에서부터 윈도우 간격 이후의 원소 추출



(그림 2) 제안 기법 구조도

4.2 그룹 키 생성 요소 분배 단계

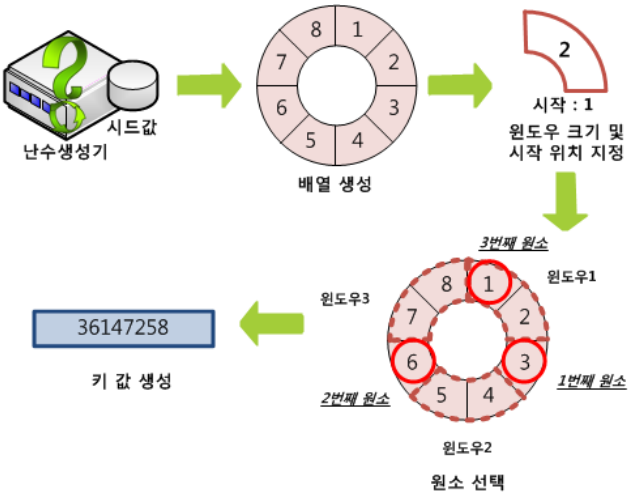
본 단계에서는 스마트미터와 전력회사 사이에 그룹키(GK) 생성을 위하여 그룹 키 생성 요소를 분배하는 단계이다. 이를 위하여 전력회사가 키 원소 배열 생성을 위한 시드값($Seed$)과 일정한 간격에서 키 원소를 추출하기 위한 윈도우 크기값($Size_{WD}$)을 생성한다. 또한 배열에서 원소를 추출하기 위한 시작 위치($Arry(ST)$)도 지정한다. 시작 위치를 지정하게 되면, 동일한 키 원소 배열을 사용하더라도 생성되는 그룹 키의 경우의 수를 증가시킬 수 있으며, 이는 공격자가 키 원소 배열을 알고 있더라도 그룹 키의 추측이 어렵게 만드는 이점을 가진다. 최종적으로 전력회사가 $Seed$, $Size_{WD}$, $Arry(ST)$를 선택한 후, 각 스마트 미터에 최초 저장된 암호화키를 이용하여 암호화하여 분배하게 된다.

4.3 그룹 키 생성 단계

본 단계에서는 스마트미터와 전력회사가 각각 배열을 생성하고, 윈도우 간격에 따라 원소를 선택하여 그룹 키를 생성하는 단계이다.

먼저 스마트미터와 전력회사는 동일한 난수생성기에 전력회사에서 생성한 시드값을 입력하여 배열($Arry_{key}$)을 생성한다. 생성되는 배열의 키 원소는 동일한 값을 갖는다. 이는 추후 그룹 키 생성시 추출되는 배열의 원소들이 동일해야하기 때문이다. 배열의 크기는 추후 데이터 통신 시 암호화를 위해 사용되는 키의 길이를 갖으며, 128bit, 256bit, 512bit, 1024bit, 2048bit의 선택을 할 수 있다. 생성된 배열은 원형배열의 형태를 갖는데, 이는 윈도우 크기에 따라 원소를 선택할 때, 마지막 키 원소를 선택할 때까지 반복적으로 수행될 수 있어야하기 때문이다.

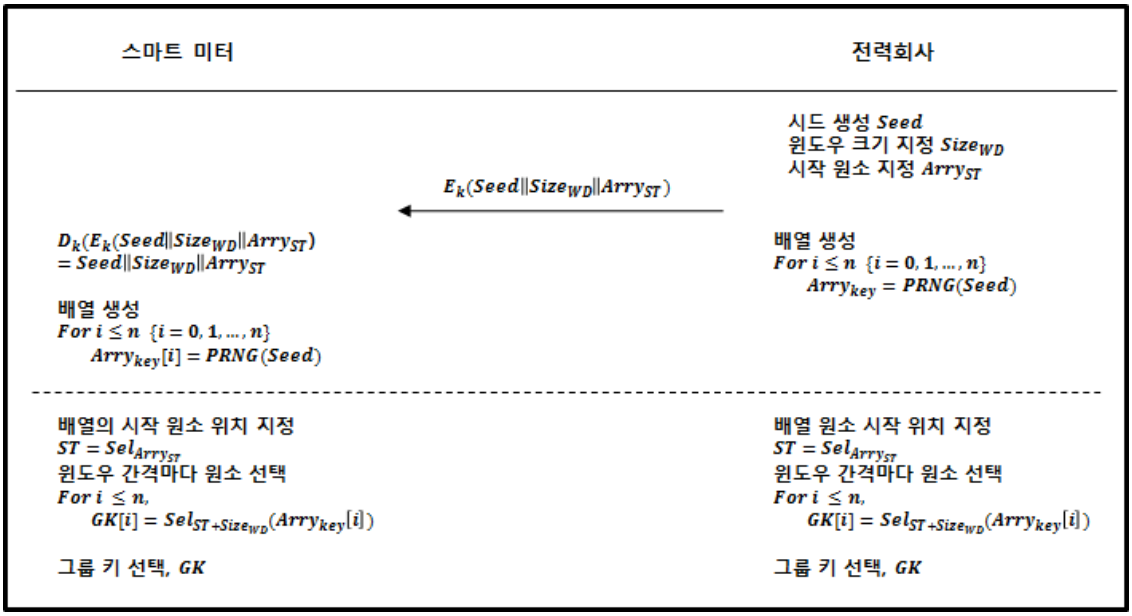
배열이 생성되고 나면, 지정된 시작 위치에 따라 배열의 임의의 위치에서부터 윈도우 간격에 따라 키를 선택한다. 예를 들어 배열의 크기가 8이고, 시작 위치가 1인 상태에서 윈도우의 크기가 2인 경우에는 다음 그림 3과 같은 형태로 원소를 선택하게 된다.



(그림 3) 키 배열 및 그룹키 생성 단계

이와 같은 방식을 동일하게 사용함으로써 전력회사와 스마트 미터가 동일한 위치의 원소를 원소를 지속적으로 추출할 수 있다.

모든 스마트미터와 전력회사는 본 단계를 통하여 그룹 키 원소 배열을 생성하고, 동일한 위치의 키 원소를 추출할 수 있으며, 최종적으로 동일하고 유일한 그룹 키를 생성할 수 있다. 이렇게 생성된 그룹 키를 이용하여 추후 전력 사용량 송수신시 암호화에 사용한다.



(그림 4) 제안 기법 프로토콜

4.4 프로토콜

다음 그림 4는 그룹 키 생성 요소 분배 단계와 그룹 키 생성 단계를 프로토콜로 구성하여 나타낸 것이다. 각 스마트미터와 전력회사는 한 번의 통신만을 이용하여 동일한 그룹 키를 생성할 수 있다. 그림 4는 제안 기법에서 동작하는 프로토콜을 나타낸 것이다. 프로토콜의 동작과정은 다음과 같다.

- STEP 1: 전력회사가 시드값, 윈도우 크기값, 시작 원소를 지정하여 암호화키 k 로 암호화한 후 스마트 미터에 전송.
- STEP 2: 스마트 미터는 전송받은 정보를 복호화하여 정보를 알아내고, 시드값을 이용하여 그룹 키 원소 배열을 생성.
  전력회사 역시 동일한 시드값을 이용하여 배열을 생성.
- STEP 3: 스마트미터와 전력회사는 시작 원소를 이용하여 시작점부터 윈도우 크기의 간격마다 원소를 선택. 이를 조합하여 그룹키 선택.

5. 결론

스마트 그리드 환경은 전력회사와 사용자간의 양방향 통신을 통하여, 전력 공급 및 사용을 효율적으로 관리할 수 있도록 기존 전력망에 정보통신기술을 접목한 기술이다. 따라서 전력정보의 유출 및 위/변조 등으로부터 안전하게 정보를 전송할 수 있는 암호화 방식과 여기에 사용될 키가 필수적으로 요구된다. 그러나 아직까지 스마트 그리드에 대한 연구는 초기 단계에 머물러 있어 이에 대한 연구가 미흡한 실정이다.

본 논문에서는 이와 같은 문제를 해결하기 위하여 스마트 그리드 환경에서 그룹 키 분배 기법에 대하여 제안하였다. 본 제안 기법은 전력회사와 스마트 미터가 그룹 키를 생성할 수 있는 원소를 공유함으로써 각자 그룹 키를 생성할 수 있는 기법이다. 이를 통해 통신상에서 키를 분배하지 않고 동일한 그룹 키를 생성할 수 있다.

참고문헌

[1] 고웅, 곽진, “스마트 그리드 환경에서 프라이버시 보호를 위한 안전한 데이터 전송 프로토콜”, 한국정보통신학회 논문지, 제16권, 제8호, pp.1701-1710, 2012.

[2] H. Tai and E. O. Hogain, “Behind the Buzz [In My View],” IEEE Power and Energy Magazine, vol.7, no.2, pp.87 - 92, 2009.

[3] 이건희, 서정택, 이철원, “스마트그리드와 사이버 보안”, 한국통신학회지, 제27권, 제4호, pp.23-30, 2010.

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

[5] 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.

[6] 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.

[7] 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.