스마트그리드 환경에서 안전한 키 분배 기법

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

Secure Key Distribution Scheme in Smartgrid Environment

Su-Young Jung*, Jin Kwak**
*ISAA Lab, Dept of Information Security Engineering, Soonchunhyang University
**Dept of Information Security Engineering, Soonchunhyang University

요 약

스마트그리드는 기존의 전력망에 IT기술을 접목하여 기존 전력망의 노후화, 안정적인 전력 공급 등의 문제를 해결할 수 있도록 개발되었고 안정적인 전력 공급, 신재생에너지의 효율적 활용, 각 가정의 전력 구매/판매 가능 등의 장점을 갖고 있다. 하지만 폐쇄 망으로 운영되는 환경을 공개망으로 전환하기 때문에 소비자의 정보, 전력 사용량 등을 전송하는 통신과정에서 악성코드 유포, 해킹 등의 보안 위협에 노출될 수 있다. 따라서 본 논문에서는 스마트미터와 AMI 서버간의 안전한 통신을 할 수 있는 안전한 키 분배 기법을 제안한다.

1. 서론

스마트그리드는 풍력, 태양열 등 불안정한 전력을 관리하여 안정적으로 공급할 수 있게 해주고, 각 가정에서 전력을 구매/판매할 수 있게 하고, 실시간 전력 정보 제공, 전력 모니터링을 통한 안정적인 전력 공급 등을 가능하게 하는 시스템이다. 실시간으로 전력에 대한 정보를 제공하기 때문에 공급자 입장에서는 전력 사용량을 모니터링 할 수 있어 전력 사용량이 많은 시간에는 요금을 차등적으로 부과해 사용량을 제어할 수 있어 안정적으로 전력을 공급할 수 있다. 소비자 입장에서는 전력 사용 요금에 따라 개인 전력 사용량을 제어할 수 있어 효율적인 전력 사용이 가능하다[1].

앞에서 언급한 것과 같이 스마트그리드의 장점을 제공하기 위해서는 기존의 폐쇄적으로 운영되었던 전력망에 공개망을 접목시켜야 한다. 기존 전력망이 공개망과 접목되면 기존의 공개망에서 발생할 수 있는 악성코드, 해킹 등의 보안위협이 스마트그리드 환경에서도 그대로 발생할 수 있다.

이와 같은 보안위협은 스마트그리드 환경의 통신구조인 스마트미터-DCU(Data Concentration Unit)-AMI 서버 사이의 양방향 통신과정에서 소비자의 정보 노출, 전력 사용 정보 조작, 위장공격 등의 위협이 발생할 수 있기 때문에 대응 방안이 필요하다.

따라서 본 논문에서는 스마트그리드 환경에 적합하고 안전하게 통신을 할 수 있는 안전한 키 분배 기법을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 스마트그리드 환경에서 발생할 수 있는 문제점을 기술하고 3장에서는 스마트미터-DCU-AMI 서버 간의 안전한 키 분배 기법을 제안한다. 4장에서는 제안한 키 분배 기법에 대한 안전성을 분석하고, 마지막으로 5장에서는 결론을 맺는다.

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

2. 문제점

스마트그리드 환경은 스마트미터-DCU-AMI 서버 사이의 통신으로 전력 사용량, 소비자의 정보, 요금 정보 등이 전송된다. 이와 같이 전송되는 정보는 안전하게 암호화되어 전송되어야 한다. 만약 공격자가 전송되는 값을 복호화할 수 있으면 소비자의 전력 사용량 조작, 개인정보 확인, 요금 조작 등의 공격을 할 수 있기 때문에 안전하게 정보를 전송하기 위한 기법이 필요하다.

❒ 소비자의 정보 수집

각 스마트미터를 소유하고 있는 소유주의 정보가 중간에 공격자에 의해 유출되거나 전기 사용에 대한 패턴 분석을 통해 어떤 가전제품을 많이 사용하고 현재 집에 있는 유무도 판별할 수 있기 때문에 가택 침임과 같은 2차적인 범죄에 이용될 수 있다.

❒ 정보 조작

각 스마트미터에서는 각 가정에서 사용한 전력량을 AMI 서버로 전송하고 AMI 서버는 이에 대한 요금을 책

정하여 알려준다. 이 과정에서 공격자가 전력 사용량을 조작하여 많이 사용한 것처럼 한다거나 적게 사용한 것처럼 조작하고 요금도 마찬가지로 조작할 가능성이 있다. 이와 같은 경우 소비자는 본래의 정상적인 정보가 아닌 조작된 정보를 받게 되고 이로 인해 금전적인 손해를 입을 수 있다.

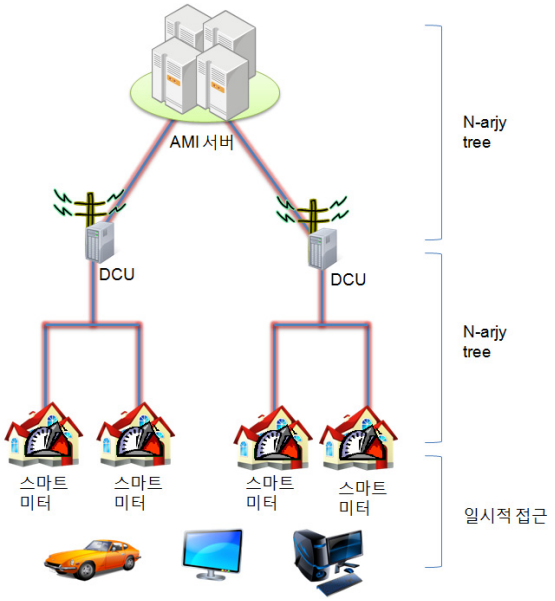
❒ 정보의 가용성

스마트그리드 환경은 스마트미터-DCU-AMI 서버 사이의 트리 구조로 이루어져 있다. 각각 스마트미터와 DCU사이에는 서로의 정보를 열람할 수 없어야 하고 각 미터와 DCU를 관리하는 상위 단에서만 확인 할 수 있어야 한다. 만약 서로의 정보를 열람할 수 있게 되면 정보 유출, 조작 등의 문제가 발생할 수 있기 때문에 앞에서 설명한 스마트그리드 구조에 맞는 키 관리 방식이 필요하다.

3. 스마트그리드 키 분배 기법

(그림 1)과 같이 스마트그리드 환경은 AMI 서버를 최상위 단으로 n개의 DCU를 하위 단으로 갖고 있고 각각의 DCU는 n개의 스마트미터를 하위 단으로 갖고 있다. 이와 같은 구조를 갖는 스마트그리드에 적합한 키 분배 기법에 대한 연구가 필요하다.

본 논문에서는 스마트미터-DCU-AMI 서버로 이루어진 스마트그리드 구조에서 안전한 키 분배 기법을 제안한다. 또한 디바이스를 추가/삭제할 때마다 매번 키를 새로 분배할 경우 효율적이지 못하고 하나의 키만 계속 사용할 경우 키가 노출되게 되면 안전성의 문제가 발생하기 때문에 키에 유효기간을 담은 정보를 포함시켜 매번 새로 분배할 필요없이 안전하게 키를 분배하여 사용할 수 있도록 하였다.



(그림 1) 스마트그리드 키 구조

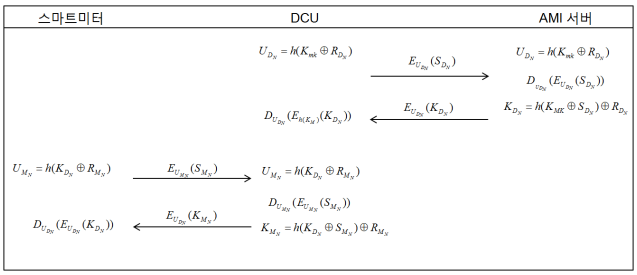
3.1 파라미터

<표 1> 파라미터

파라미터	설명
M_A	스마트 미터 A
D_A	DCU A
S_A	A의 시리얼 넘버
K_{mk}	서버의 마스터키
E_A	디바이스 A
K_A	A의 키
U_A	제조 당시 만들어지는 A의 키
R_A	A의 랜덤 값
$E(A)/D(A)$	A의 암호화/복호화
TE_A	A의 유효기간 값

3.2 스마트그리드 환경의 키 분배

AMI 서버/DCU는 각각 자신에게 연결되어 있는 DCU/스마트미터의 랜덤 값인 R_D/R_M의 리스트를 갖고 있다고 가정한다. 이 리스트를 이용하여 스마트미터-DCU-AMI 서버 사이에 안전하게 키를 분배할 수 있다.



(그림 2) 스마트그리드 환경의 키 분배

Step 1. DCU는 자신의 S_{D_N}을 사전에 공유된 서버의 키 U_{D_N}으로 암호화한 $E_{U_{D_N}}(S_{D_N})$를 AMI 서버에게 전송한다.

Step 2. AMI 서버는 전송받은 값 $E_{U_{D_N}}(S_{D_N})$을 복호화하여 DCU의 S_{D_N}를 얻는다. 이후 자신의 마스터키 값, DCU의 시리얼 넘버, 랜덤 값을 연산하여 DCU의 키 $K_{D_N} = h(K_M \oplus S_{D_N}) \oplus R_{D_N}$를 생성한다. 이후 DCU에게 이 키를 암호화한 $E_{h(K_S)}(h(K_{D_N}))$를 전송한다.

Step 3. DCU는 전송된 값 $E_{h(K_S)}(h(K_{D_N}))$을 복호화하여 DCU의 키 K_{D_N}을 얻고 저장한다.

Step 4. 스마트미터는 키를 분배 받기위해 자신의 S_{M_N}을 DCU로 전송한다. 전송할 때는 U_{M_N}을 이용하여 암호

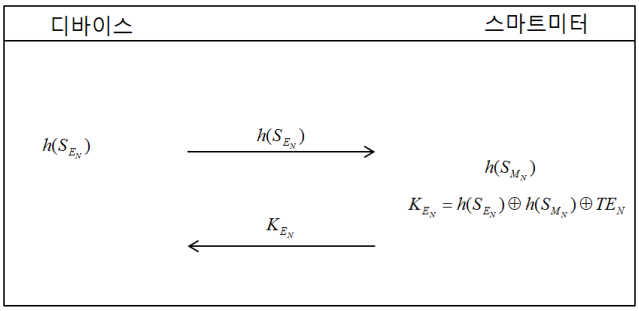
화한다($E_{h(K_S)}(S_{M_N})$).

Step 5. DCU는 전송받은 값을 U_{M_N}으로 복호화하여 스마트미터의 S_{M_N}를 얻는다. 이후 해당 DCU와 AMI 서버사이에 키 값과 DCU의 시리얼 넘버, 랜덤 값을 연산하여 스마트미터의 키 값$K_{M_N} = h(K_{D_N} \oplus S_{M_N}) \oplus R_{M_N}$를 생성한다.

Step 6. 스마트미터는 DCU로부터 전송받은 값 $E_{U_{M_N}}(K_{M_N})$를 갖고 있는 키 U_{M_N}으로 복호화하여 스마트미터의 키 K_{M_N}를 얻고 저장한다.

3.3 디바이스 키 분배

스마트미터에 연결되는 디바이스는 사용할 때만 연결하고 사용하지 않을 때는 연결을 끊기 때문에 유동적이다. 이를 해결하기 위해 키를 발급할 때 키를 사용 가능한 유효기간 값을 키에 넣어 디바이스를 연결 할 때마다 새로운 키를 발급/삭제 할 필요가 없고 유효기간이 끝나면 새로 발급 받는다. 항상 같은 키 값을 사용하는 것이 아니기 때문에 효율적인 키를 생성할 수 있다.



(그림 3) 디바이스 키 분배

Step 1. 디바이스를 연결한 후 디바이스는 자신이 시리얼 넘버 $h(S_{E_N})$를 스마트미터로 전송한다.

Step 2. 스마트미터는 전송받은 디바이스의 시리얼 넘버를 자신의 시리얼 넘버와 키를 사용할 수 있는 수명에 대한 유효기간을 나타내는 값 TE_N으로 디바이스의 키 $K_{E_N} = h(S_{E_N}) \oplus h(S_{M_N}) \oplus TE_N$를 생성한다.

Step 3. 디바이스는 키를 스마트미터로부터 발급받고 저장한다.

4. 안전성 분석

❒ 소비자 정보 수집

스마트미터-DCU-AMI 서버의 통신과정에서 정보가 노출되지 않도록 제조당시에 저장되는 AMI 서버의 해쉬연산한 마스터키를 이용하여 암호화를 한다. 이로 인해 전송되는 키는 안전하게 전송할 수 있고 이 키를 이용하여 소비자의 정보를 안전하게 전송할 수 있다. 또한 해쉬연산한 마스터키는 처음에 키를 분배할 당시에만 사용하기 때문에 노출될 경우 발생할 수 있는 피해를 최소화 할 수 있다.

❒ 정보 조작

실시간으로 통신을 하며 정보를 전송하는 스마트그리드 환경에서 공격자의 중간자 공격으로부터 안전할 수 있도록 암호화 통신을 한다. 이 암호화를 하는 키는 그룹 키로 자신의 상위 단에서만 알고 있고 이 키 또한 안전하게 분배된다.

❒ 정보의 가용성

스마트그리드 환경은 AMI 서버 하위 단에 n개의 DCU가 있고 그 하위 단에는 n개의 DCU가 있다. 또한 스마트미터에 연결되는 미터는 전기를 저장/판매하기 위해 연결하거나 자주 연결/해제를 반복하는 유동적인 디바이스를 관리하기 위해 키에 유효기간을 설정하여 관리함으로써 효율성을 향상시킬 수 있다.

5. 결론

본 논문에서는 스마트그리드 환경에서 통신할 때 전송되는 정보를 해킹, 악성코드 등의 위협으로부터 안전하게 전송할 수 있도록 스마트그리드 환경에 효율적인 키 분배 기법을 제안했다. 또한 디바이스에 분배되는 키에 유효기간을 설정하여 디바이스를 연결할 때마다 매번 분배할 필요없이 효율적으로 키를 분배하여 사용할 수 있다.

참고문헌

[1] 이일우, 박완기, 박광로, 손승원, “ 스마트그리드 기술동향”, 한국통신학회지(정보와통신), 제 26권 제 9호, pp.24-33, 08. 2009.

[2] 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.

[3] Chung Kei Wong, Hohamed Gouda, Simon S. Lam, "Secure Group Communications Using Key Graphs" In Proceedings of the ACM SIGCOMM '98 Conference on Applications, Technologies, Architecture, and Protocols for Computer Communication, pp.68-79, 1998.

[4] 전용희, “스마트그리드의 취약성, 특성, 설계 원칙 및 보안 요구사항 분석.” 정보보호학회지, 제 20권 제 3호, pp.79-89, 2010년 6월