Dual Secret Key 를 이용한 스마트그리드 내의 AMI 시스템 보안 기법

*편희범, **홍충선
경희대학교

*hb8115@khu.ac.kr, **cshong@khu.ac.kr

Dual Secret Key Scheme for AMI System Security in Smart Grid

Hee Bum Pyun, Choong Seon Hong
Networking Lab, Department of Computer Engineering, Kyung Hee University

Abstract

본 논문은 점차로 에너지의 효율적인 관리에 대한 요구가 높아짐에 주목하여 스마트 그리드(Smart Grid)에 관한 주제를 기반으로 진행되었다. 스마트 그리드에 대한 관심이 높아지면서 스마트 그리드 환경에 필수적인 AMI(Advanced Metering Infrastructure)에 대한 연구가 진행되고 있다. 그러나 AMI 시스템에서의 보안 연구는 활발히 이루어지고 있으니 그 진행이 미약한 편이다. 본 논문에서는 AMI 시스템에서의 보안을 강화하기 위한 방법으로 지능형 키 관리 서버를 제안하였으며, 제안된 키 관리 서버에서의 Overhead 와 AMI 시스템 내의 스마트 미터와 유틸리티 간에 보안을 강화하기 위한 방법으로 Dual Secret Key 기법을 제안하고자 한다.

Ⅰ. INTRODUCTION

AMI 시스템 구축을 위해서는 먼저 보안 문제와 효율적인 에너지 관리에 관하여 고려해야 한다.[1] 유틸리티에서 스마트 미터로 전송되는 부하 제어 메시지는 소비자에 의해 정해진 요금 정책에 따라 달라지게 되지만 유사한 요금 정책에 의해서 그룹 별로 분류할 수 있다.[2]

만약 각 스마트 미터가 유틸리티와 의 통신을 위해 개별적으로 키를 가지고 통신하게 된다면 네트워크 대역폭과 키 연산 값 측면에서 매우 비효율적이다. 그러므로 멀티캐스트 방식을 이용한 그룹 키 통신을 이용하고 AMI Collector 라 명명된 키 관리 서버를 도입한 새로운 기법을 제안하고자 한다.

AMI Collector 는 유틸리티와 스마트 미터 사이에 위치하게 되며, 그것은 스마트 미터로부터 전송되는 데이터를 수집하고 수집된 데이터를 일정한 시간 간격으로 유틸리티에게 전송하게 된다.[3] AMI Collector 와 스마트 미터간의 계층 구조는 키 연산 비용과 네트워크 대역폭을 위해 멀티캐스트를 이용한 그룹 키 통신을 하며 이는 Iolus Framework 를 따르도록 한다.[4]

본 논문에서는 이러한 AMI collector 과 스마트 미터간의 신뢰성을 강화하기 위한 방법으로 Dual Secret Key(DSK) 기법을 제안한다. 본 논문에서 스마트 미터에서의 키는 제조사에 의해 사전 분배 되며 이 키들은 AMI Collector 에서 공유하는 유틸리티 서버에 등록된다.

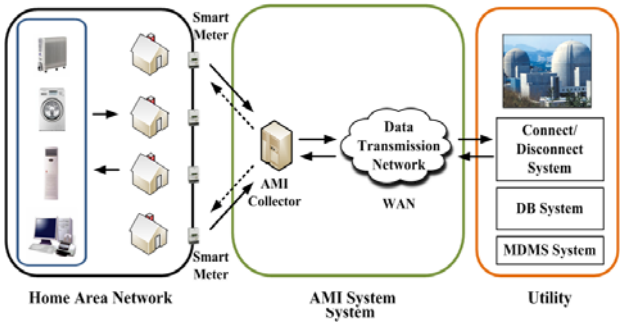
II. PROBLEM STATEMENT

스마트 그리드 에서의 유틸리티 서비스는 AMI 데이터를 수집하고 분석하여 소비자의 전력 소비 요구에 맞게 서비스를 제공한다. 만약 스마트 미터에서 전송되는 데이터가 공격자에 의해 침해를 받게 되면 유틸리티는 이를 판정하지 못하고 잘못된 데이터에 기반하여 서비스를 제공하게 된다. 침해 사례가 병원, 발전소, 가스 공급소 등에 일어나게 되면 그 피해는 더욱 커지게 된다.

본 논문에서는 전송되는 데이터의 신뢰성을 확보하기 위하여 DSK 기법을 제안하였으며, DSK 의 키 관리 서버가 되는 AMI Collector 은 전력 망의 특수한 네트워크 상황을 고려하여 공격에 안전하다고 가정하였다.

III. PROPOSED MECHANISM

이번 장 에서는 AMI 시스템을 지원하기 위한 멀티캐스트 방법과 보안에 관하여 설명한다. 그림 1 은 AMI 시스템의 전체적인 모습을 나타낸다.



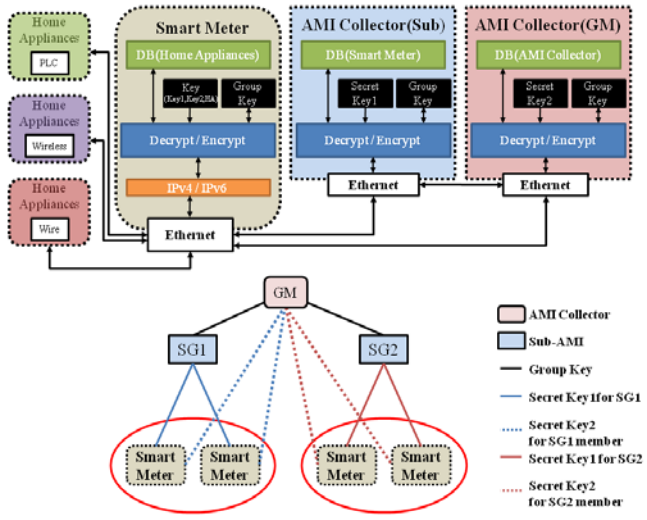
. <그림 1> 제안된 AMI System

먼저, 모든 스마트 미터들은 제조사에 의해 Secret-1 과 Secret-2 를 사용하는 DSK(Dual Secret Key)를 사전 분배 받는다. 이 DSK 는 유틸리티 서버에 등록된다. 스마트 미터가 AMI Collector 에 등록될 때 스마트 미터는 Secret-1 을 이용하여 AMI Collector 에게 인증을 요청한다. 인증 요청이 발생하면 AMI Collector 는 스마트 미터로부터 받은 Secret-1 을 유틸리티 서버에 전송한다. 유틸리티 서버에서는 전송 받은 Secret-1 을 확인하여, 등록 여부를 확인 후 인증을 수행한다. 인증 과정이 수행되면, 각 스마트 미터들은 요금 혹은 그 외의 그룹 분류 정책에 따라 Sub-AMI Collector 를 이용, Iolus Framework 에 따라 그룹을 형성한다.

현재 단계까지는 Secret-1 만을 사용하여 통신을 하며 이 키를 이용하여 AMI, Sub-AMI, 스마트 미터간의 그룹 키를 생성한다.

Secret-2 는 스마트 미터의 Join, Leave 혹은 정전과 같이 스마트 미터로부터 오는 데이터의 흐름에 이상이 생겼을 경우 사용된다. Secret-2 를 이용하여 AMI Collector 는 스마트 미터로 직접 통신을 진행한다. 이 과정에서 AMI Collector 는 Secert-1 을 사용하여 Sub-AMI 에서 받은 데이터와 Secret-2 를 사용하여 스마트 미터와 직접 통신하여 받은 데이터를 비교한다.

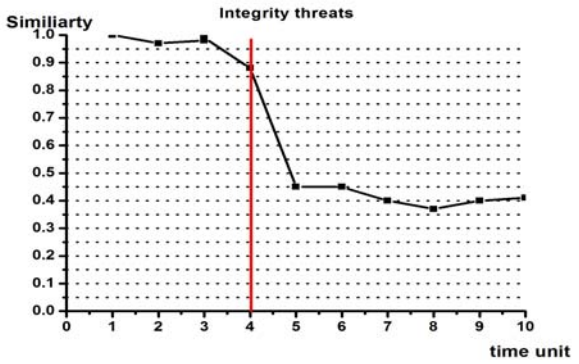
두 데이터를 비교하는 과정 동안 유틸리티 서버로의 데이터 전송을 보류하게 된다. AMI Collector 에서 Sub-AMI 와 스마트 미터에서 받은 두 데이터가 일치하였을 경우 공격이 없었다고 판정하여 데이터 전송을 재개하게 된다. 그림 2 는 이러한 과정을 나타내고 있다.



<그림 2> 제안된 DSK 기법을 이용한 AMI 시스템

III. EVALUATION

본 논문의 결과는 Omnet++을 이용하여 평가하였다. 그림 3 은 전송되는 두 데이터의 유사성을 비교하는 모습을 나타낸다. 공격이 이루어지게 되면 전송된 두 데이터의 유사성이 명확히 떨어짐을 확인할 수 있다. 이를 통하여 전송된 데이터가 신뢰성을 잃었음을 판단한다. AMI Collector 는 데이터간 유사성이 떨어지면 이를 유틸리티와 사용자에게 알려 데이터 신뢰성을 회복하도록 한다.



<그림 3> 제안된 DSK 기법을 통한 신뢰성 판단

IV. CONCLUSION

본 논문에서는 AMI 시스템의 보안을 위해 AMI Collector 을 제안하였고, DSK 기법을 제안하여 보안을 강화하였다. 또한 시뮬레이션을 통해 그 기법의 효용을 확인하였다. 본 논문의 제안된 기법은 전력 망이라는 특수한 네트워크 망을 고려하여 진행하였다. 앞으로 본 연구를 바탕으로 보다 복잡한 그룹 내에서의 키 판단 여부와 공격 탐지 여부를 확인할 것이다.

ACKNOWLEDGMENT

“ 본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음” (NIPA-2010-(C1090-1031-0005)). Dr. CS Hong is the corresponding author.

참 고 문 헌

[1] Hart, D.G. “ Using AMI to realize the Smart Grid” Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE

[2] Cleveland, F.M. “ Cyber security issues for Advanced Metering Infrasttructure (AMI) “ Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE

[3] NETL Modern Grid Strategy Powering our 21st-Century Economy “ ADVANCED METERING INFRASTRUCTURE” February 2008

[4] S. Mittra, “ Iolus: A framework for scalable secure multicasting,” in Proc. ACM SIGCOMM, 1997, pp. 277- 88.