# AMI Collector 를 이용한 Advanced Metering Infrastructure 시스템 보안 방안

*편희범, **이일우, ***조상욱, *홍충선

*경희대학교 컴퓨터공학과 네트워킹 연구실, **한국전자통신연구원, ***KT

*h8115@khu.ac.kr, **ilwoo@etri.re.kr, ***chosw@kt.com and *cshong@khu.ac.kr,

# Advanced Metering Infrastructure Security Using AMI Collector

*Hee Bum Pyun, **Il Woo Lee, ***Sang Wook Cho, *Choong Seon Hong

*Networking Lab, Department of Computer Engineering,

Kyung Hee University

**Electronics and Telecommunications Research Institute,***KT

**요 약**

에너지 자원의 효율적인 관리에 대한 관심이 높아지면서 스마트 그리드(Smart Grid)에 관한 연구가 전 세계적으로 진행되고 있다. 이런 추세에 맞추어 국내에서도 스마트 그리드에 대한 관심이 높아지면서 스마트 그리드 환경에 필수적인 AMI(Advanced Metering Infrastructure)에 대한 연구가 진행되고 있다. AMI에서 가장 중요한 부분은 검침 기기에 대한 정보를 수집하는 스마트 미터(Smart Meter)와 유틸리티 간의 통신이다. 유틸리티와 각 스마트 미터간에 이루어지는 정보들은 보안성을 가장 중요시한다. 그러나 서로 다른 비밀키를 사용하여 데이터를 전송하는 것은 네트워크 대역폭과 연산의 측면에서 비 효율적이다. 비밀성을 만족하는 IP 멀티 캐스트를 사용하면 스마트 미터와 유틸리티 간의 키 연산 비용을 효율적으로 줄일 수 있다. 본 논문에서는 AMI Collector을 최상위 노드 및 Base Station으로 하여 LKH(Local Key Hierarchy)를 이용한 키 노드를 구성하여 키 연산에 따른 비용을 줄이고, DEP(Dual Encryption Protocol)을 이용하여 보안을 강화하는 방안을 제안하고자 한다.

## 1. 서 론

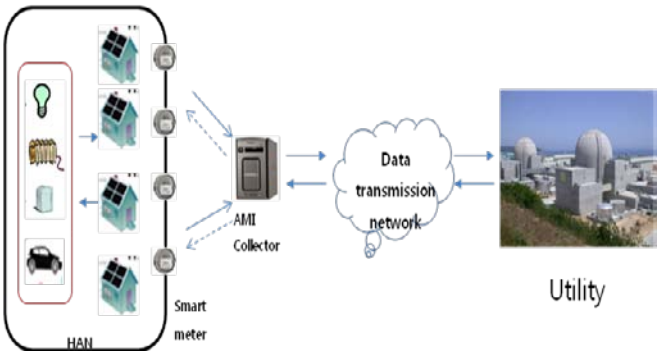
전 세계적인 에너지 확보 위기와 이산화탄소 과다 배출로 인한 환경 문제로 인하여 그린 IT(Green IT)가 주목 받고 있다. 그린 IT는 IT와 통신 기술을 접목하여 에너지 활용의 효율성을 높여 저 탄소 녹색 성장을 이루고자 하는 기술을 말한다. 이러한 그린 IT 분야의 대표적인 기술로는 스마트 그리드(Smart Grid)가 있으며, 이는 차세대 전력 망 시스템으로, 기존의 전력 생산, 운반, 소비의 과정에서 정보통신 기술을 도입하여 에너지 관리 시스템의 효율성을 높인 것이다. 스마트 그리드의 주요 분야 중 하나인 AMI(Advanced Metering Infrastructure)는 전력 소비자와 전력 회사 사이의 전력 서비스 인프라로써 스마트 그리드 구현에 필요한 핵심 시스템이다.[1] AMI를 통하여 전력 생산자 측은 현재 최대 소비량에 맞춰진 생산 시스템을 개선하여 효율적인 전력 생산을 할 수 있다. 이러한AMI 시스템 구축에 따라 새로운 문제점들이 등장하게 되는데 가장 중요한 것은 바로 보안 문제이다.[2] 유틸리티에서 smart meter로 데이터 전송을 할 시엔 각 개인의 요금 정책에 따라 암호화된 데이터가 전송되어야 하는 경우가 생긴다. 이 때 각 smart meter 마다 다른 비밀키를 사용하여 데이터를 전송하게 된다면 네트워크 대역폭 측면이나 키 연산 량 측면에서 비효율적이다. 멀티캐스트 방식을 이용하면 하나의 메시지를 이용하여 다수의 smart meter에게 네트워크 대역폭을 효율적으로 활용하여 전달할 수 있다.[3] 비밀성이 요구되었을 때 멀티캐스트를 이용하기 위해서는 그룹에 속한 모든 멤버들이 같은 비밀키를 공유해야 한다. 이를 위해 사용되는 암호 프로토콜이 다자간 키 확립 프로토콜이다. 다자간 키 확립 프로토콜은 중앙 서버의 필요성에 따라 중앙 집중형(centralized), 비중앙집중형(decentralized), 분산형(distributed)으로

[1] This work was supported by the KT R&D Program. [A development of the technology for UMCI Model to set-up smart place based on HAN]. Dr. CS Hong is the corresponding author.

나누어지며 본 논문에서는 smart meter의 데이터가 집중되는 AMI Collector을 Base Station으로 하여 smart meter 그룹을 관리할 수 있는 중앙 집중형 그룹 키 관리 방안을 제안한다. 국내에서는 외국과는 다르게 단일 유틸리티에서 전력을 공급하는 시스템을 갖는다. 그렇기에 AMI 시스템의 보안을 강화하기 위해서 AMI Collector를 유틸리티의 지역 지부 별로 두고 DEP(Dual Key Encryption)을 이용하여 보다 강화된 보안 체계를 제안하고자 한다. 본 논문에서는 각 smart meter 들은 사전 키 분배 방법에 의해 AMI Collector과 공유하는 비밀키를 갖는다고 가정하였고, AMI Collector는 전체적인 AMI 시스템의 특성상 Attacker들의 공격에 의해서 자유롭다고 가정하였다.

## 2. 전체적인 AMI 시스템

본 논문에서 제안하는 AMI System은 아래 그림 1과 같이 나타난다.[4]




<그림 1> AMI 구조

그림 1에서 나타난 것과 같이 AMI 시스템은 AMI Collector을 상위 노드로 한 계층적인 구조를 갖는다고 가정하였다. 기본적인 AMI 시스템은 에서의 각 스마트 미터들은 HAN내의 타 지능형 장비들과 통신하며 장비들의 전력 소모량을 측정하게 된다. 소비자 입장에서는 스마트 미터에서 수집된 데이터를 바탕으로 자동화된 기기 제어를 통해 에너지 사용을 제어함으로써 가정 및 기업에서의 에너지 비용을 절감할 수 있으며 유틸리티에서는 소비자의 전력 수요 시간을 확인하여 피크 타임 대를 설정할 수 있고, 검침 및 유지관리 비용의 절감과 에너지 부하제어를 통해 에너지 생산 비용 및 추가적인 인프라 확장을 방지하는 효과를 기대할 수 있다.[5] 그러나 유틸리티와 각 스마트 미터간에 직접적으로 통신을 하게 된다면 유틸리티에서 가정 내 전력 사용량 체크를 위한 데이터 수집이나 부하 제어 등의 데이터 전송시에 비효율적으로 많은 연산과 네트워크를 사용하게 된다. 그렇기에 각 지역별로 스마트 미터를 그룹으로 묶어 관리할 수 있는 AMI Collector을 두게 된다면 스마트 미터가 HAN내의 타 지능형 장비와 통신한 Metering 정보, 전력 품질 모니터링, 에너지 사용 현황 등을 수집한 후 이를 주기적으로 유틸리티에 전송할 수 있게 하여 보다 더 효율적으로 데이터를 관리할 수 있다. 본 논문에서는 LKH를 사용하여 AMI Collector을 최상위 노드로 키 관리 노드를 구성하여 그룹 키를 이용한 멀티 캐스트 통신이 가능한 네트워크 망을 구성하였다.[6][7] 가정사항으로는 국내의 전력 공급 시장이 단일 유틸리티에서 공급되고 있으므로, AMII Collector과 스마트 미터간에는 사전에 공유할 수 있는 비밀키가 설정되어 있고 AMI Collector은 물리적으로 노출되지 않으며 Attacker들의 공격에 영향을 받지 않는다고 가정하였다.

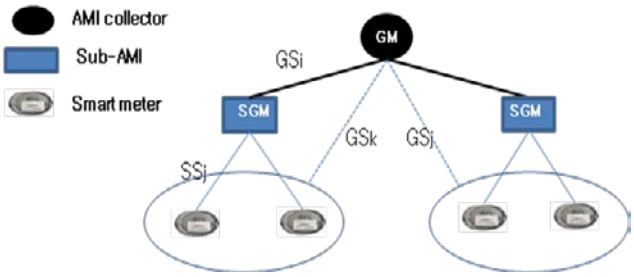
## 3. AMI 시스템의 보안 위협 문제

AMI는 각 계량기와 같은 네트워크 접속 장치들로부터 계량 값을 측정하고 에너지 사용을 분석한다. AMI는 분석한 데이터를 바탕으로 TOU(time of use rate), 최고부하 가격책정과 같은 수용응답 기능과 정전 감지 및 평가 기능을 사용함으로써 소비자들의 에너지 사용을 조절할 수 있다. 만약 공격이 발생할 시에는 정전 심지어는 전력 공급 망의 불안정성까지도 포함될 수 있다. 스마트 미터기에 물리적으로 손대는 일을 제외하면 알려진 취약점의 대부분은 통신 미디어 및 통신 프로토콜과 관련이 있다. 이는 전력 공급 망이 본래부터 보안상의 약점을 지닌 인터넷에 연결되기 때문이다. 그리하여 본 논문에서는 각 공격자의 침입에서 자유롭다고 가정한 AMI Collector에서 DEP(Dual Encryption Protocol)을 이용하여 보안을 강화하였다.

## 4. 제안 방안

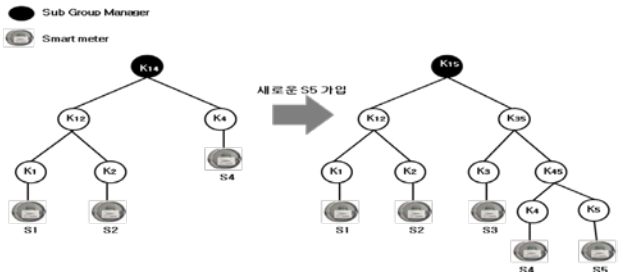
AMI 시스템은 가정 혹은 기업에 설치되는 것으로 한번 스마트 미터가 설치되게 되면 키의 변동이 쉽게 이루어지지 않는다. 본 논문에서는 스마트 미터들을 지역에 기반하여 세분화 하여 AMI 시스템을 LKH를 이용한 그룹키 관리에 따라 키 연산 비용을 줄이고 AMI Collector를 신뢰성 있는 Base station으로 한 DEP(Dual Encryption Protocol)[8]를 이용하여 보안을 강화하는 시스템을 제안한다.

본 논문이 제안하는 키 관리 구조는 다음 그림 2와 같다.



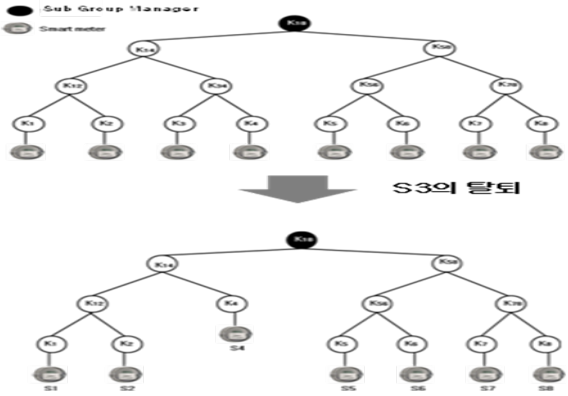

<그림 2> AMI 시스템의 키 관리 구조

AMI Collector를 그룹 매니저로 하여 스마트 미터와 계층적 구조를 형성한다. 또한 중간의 키 노드들을 서브 그룹 매니저로 하여 많은 양의 스마트 미터들을 관리할 수 있게 하였다. 스마트 미터들과 AMI Collector간에는 사전에 키를 분배하여 그룹키를 이용한 멀티 캐스트 통신이 가능하게 한다. 스마트 미터들은 하나의 서브 그룹에만 속할 수 있고 다른 그룹에 속하지 않으므로 여러 개의 서브 그룹으로 분할되게 된다. 이를 통해 그룹 키 연산에 필요한 연산을 줄일 수 있다. GM인 AMI Collector과 스마트 미터간에는 두 개의 비밀키를 공유하도록 한다. 첫 번째 키는 그룹 키를 형성하는 키로 활용한다. 두 번째 키는 서브 그룹 매니저를 통하지 않고 직접적으로 스마트 미터와 통신하는 키로 상정한다. 스마트 미터의 가입과 탈퇴가 일어날 시에는 서브 그룹 매니저를 통하여 서브 그룹 내에서만 처리하게 하여 전체적인 시스템에서의 키 갱신이 일어나지 않게 해 그룹 키 연산 비용을 줄일 수 있다. 기본 적인 키 관리 구조는 서브 그룹 내에서 이루어지며 그 과정은 다음과 같다.




<그림 3> Join Protocol

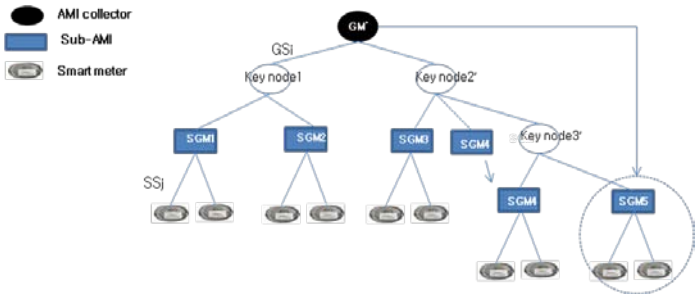
탈퇴의 경우에도 가입과 마찬가지로 서브 그룹 내에서만의 변화를 통하여 전체적인 키 갱신 비용을 O(log n)에 보장하도록 한다.




<그림 4> Leave Protocol

위의 그림 3, 4에서 나타난 것과 같이 서브 그룹 매니저를 활용하면 키 갱신을 서브 그룹 내로 제한할 수 있고 GM 또한 전체의 키를 갱신하는 것이 아닌 SGM의 키 만을 갱신하여 키 연산 비용을 효율적으로 줄일 수 있다.

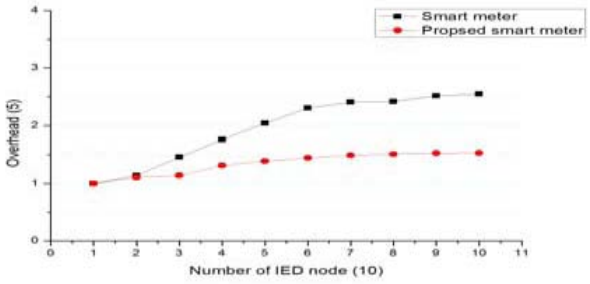
본 논문에서는 강화된 보안을 위하여 서브 그룹 매니저를 배제하고 스마트 미터와 통신할 수 있는 또 하나의 비밀키를 제안하였다. 멤버인 스마트 미터의 가입 및 탈퇴가 발생할 시에는 서브 그룹 멤버들의 그룹키가 변화하게 된다. AMI collector은 그룹 매니저로 변화한 서브 그룹을 감지하게 되며 그룹 키가 변경된 서브 그룹 내의 멤버들과 직접적으로 비밀키를 가지고 통신하게 된다. 서브 그룹 매니저를 통하여 수집된 데이터와 직접적으로 통신하여 얻은 데이터를 비교하여 둘의 데이터가 동일할 시에만 그 데이터가 공격을 받지 않았다고 인증한 후 그룹 키 통신을 재개하게 된다.




<그림 5> Proposed AMI Key management

## 5. 평가

본 논문에서 제안한 방법을 이용할 경우 기존의 AMI 방식에서 AMI Collector를 이용한 그룹 키 관리 방식에 의하여 유틸리티에서 직접 smart meter와 통신할 때 소요되는 통신 비용과 키 계산 비용을 줄일 수 있다. 또한 보안성의 측면에서도 보다 강화될 수 있다. 그림 6은 시뮬레이션을 통하여 키 관리에 따른 오버헤드를 측정한 것이다.




<그림 6> 제안된 기법에 따른 오버헤드 측정

그림 에서 보여진 것과 같이 스마트 미터의 수가 늘어남에도 오버헤드가 크게 증가하지 않는 것을 확인할 수 있다. Dual key 사용에 따른 보안성의 측정은 아직 AMI Collector에 대한 네트워크 표준이 명확하지 않고 그 성능 역시도 표준이 정립되지 않았다. 그렇지만 국내의 전력 공급 시장 상황에 비추어 봤을 때, AMI Collector은 단일 유틸리티 업체의 각 지부에서 사용된다고 가정할 수 있고 이는 Dual key를 사용하여도 충분히 그 성능을 발휘할 수 있을 것이라고 판단된다.

### 5. 결론 및 향후 연구

현재의 AMI 시스템은 별도의 보안 장치 없이 원격 검침 방식으로만 유지되고 있다. 이는 앞으로 유틸리티와 쌍방향 통신을 통하여 사용자의 과금 데이터, 에너지 사용 여부, signal cost에 따른 과금 정책, 사용자의 요금 정책 등의 데이터 수집과 전송의 보안 측면에서 심각한 위협을 초래할 수 있다. 그리하여 본 논문에서는 우선 smart meter를 그룹으로 관리하여 유틸리티에서 전체적으로 메시지를 전송하거나, 특정 그룹에게만 메시지를 전송할 때의 네트워크 대역폭과 소모 비용을 줄이기 위하여 LKH(Logical Key Hierarchy)를 이용한 중앙 집중 형 그룹 키 관리 방식을 제안하였고 AMI Collector을 보안 위협이 없는 Base Station 으로 하여 Dual Key를 이용하여 수집된 데이터에 대한 신뢰성을 확보하였다. 앞으로 본 제안 사항에 Dual Key 사용에 따른 연산 비용을 시뮬레이션이나 구현을 통하여 검증할 것이다. 그리고 Smart meter의 표준이 나오는 경우 본 제안 사항이 어떻게 사용 될지 와 어떻게 보안할지에 관한 연구를 진행할 것이다.

## Reference

[1] Korea Electric Power Research Institute “A Study on Deployment and Technology For Advanced Metering Infrastructure” 2009
[2] NIST." NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0 Draft). September 2009
[3] R Canetti, J Garay, G Itkis, D Micciancio, M Naor, B, "Multicast security: A taxonomy and some efficient constructions"IEEE INFOCOM, 1999
[4] 전자통신동향분석 “USN 기반 AMI 서비스 및 기술동향:전력 산업과 USN 산업의 융합기술”, 제 23권 제 5호 2008년 10월
[5] The Modern Grid Strategy" ADVANCED METERING INFRASTRUCTURE, (www.netl.doe.gov/moderngrid).
[6] Suvo Mittra, ”Iolus: A Framework for Scalable Secure Multicasting”, Proceedings of the ACM SIGCOMM'97 conference on . 1997
[7] S Rafaeli, D Hutchison, “A survey of key management for secure group communication”, ACM Computing Surveys (CSUR), 2003
[8] L. R. Dondeti, S. Mukherjee, A. Samal, "Scalable Secure one-to-many Group Communication using Dual Encryption," Proc. of IEEE International Symposium on Computer Communication, 1999