情 報 保 護 學 會 誌
第22卷 第1號, 2012. 2

IoT 기술과 보안

김 호 원*, 김 동 규**

요 약

최근까지 정보 기술 분야에서는 유비쿼터스(Ubiquitous)라는 용어가 크게 유행한 적이 있다. 현재는 다소 식상하게 들리는 용어일지도 모르지만 사물의 지능화와 통신화라는 유비쿼터스 개념은 이미 우리의 생활에 깊이 파고 들어왔다. 최근 유행하는 IT 기술인 스마트폰이나 지능형 전력망, 와이파이, 소셜 네트워크, 센싱 데이터 처리 기술과 개념은 이러한 유비쿼터스 기술의 대표적인 사례로 볼 수 있다. 국내에서는 이러한 유비쿼터스라는 개념을 유비쿼터스 센서 네트워크(Ubiquitous Sensor Network: USN)라는 용어로서 2004년부터 정보통신부 혹은 지식경제부의 적극적인 지원에 힘입어 많은 기술적/산업적 성과를 이루기도 했다. 하지만 이러한 USN은 센서네트워크 개념으로 제한적으로 오용되는 경우가 많았다. 이에 본고에서는 이러한 유비쿼터스 환경을 실현하는 사물의 지능화/통신화에 대한 기술 동향과 보안 기술을 논하기 위해서 USN과 거의 비슷한 개념이지만 국내외적으로 더욱 보편적으로 사용되고 있는 IoT(Internet of Things) 용어를 사용할 것이며, 이러한 IoT에 대한 기술 동향과 보안 기술을 논하고자 한다.

Ⅰ. 서 론

인간 주위 환경인 모든 사물이 지능화 및 네트워크화 됨으로서 인간 생활의 삶의 질 향상과 기업의 생산성 증대, 공공서비스의 혁신을 꿈꾸는 유비쿼터스 사회의 실현은 정보통신(ICT: Information and Communication Technology) 기술, 특히 IoT(Internet of Things) 기술의 지속적인 발전으로 어느덧 현재 우리 생활의 일부분이 되었으며 앞으로도 지속적인 발전을 통해 우리의 생활을 급격히 변화시킬 것이다.

최근 세계 각국의 산업계와 학계, 정부에서는 M2M (Machine to Machine)이나 IoT(Internet of Things)라는 다양한 이름으로 사물의 지능화 및 네트워크화를 위한 기술 개발 및 서비스 개발 노력을 하고 있다. 한국에서는 본 논문에서 논하고자 하는 IoT의 개념과 유사한 개념인 USN(Ubiquitous Sensor Network) 개념을 정부 주도의 신성장 동력으로 추진하였다. 2004년 USN 기본 계획 I(정보통신부, 2004년 2월)과 2007년 12월 USN 기본계획 II를 필두로 선진 외국보다 일찍 범국가적으로 사물의 지능화 및 네트워크화에 필요한 기술 개발과 관련 서비스 개발 노력을 해왔다. 특히 한국에서는 USN 분야 중에서 모바일 RFID 기술 개발과 USN 기술 개발 등, 유비쿼터스 사회를 위한 핵심 기술 개발을 성공적으로 수행해 왔으며 u-IT 신기술 확산 사업 등을 통해 개발한 기술에 대한 실용화 및 산업화도 적극적으로 추진해 왔다. 현재 모바일 RFID 기술은 NFC와 스마트폰의 시장 성장에 힘입어 상업적인 성공이 예상되며 USN 기술은 스마트그리드, 수자원 관리, 센싱 데이터 처리 등, 각종 융복합 응용에 많이 사용되고 있다. 하지만, 최근 국내의 IoT 산업 활성화를 위한 국내 민관연의 노력은 최근의 급격한 사회 패러다임의 변화와 시장 수요 변화, 기술의 급속한 발전, 전통적인 IoT 산업 활성화 부진 등의 사유로 인하여 현시점에서 IoT 산업 현황에 대한 분석을 토대로 국내 IoT 산업 활성화를 위한 전략을 재검토할 필요성이 강하게 재기되기도 하였다 [1].

먼저 본 논문에서는 IoT 기술의 개념 및 정의를 살펴볼 것이다. 전술한 것처럼 국내에서는 IoT를 USN이라는 이름으로 많이 불렀으며 USN이라는 것은 사용기술 객체에 부착된 태그 혹은 센서노드로부터 객체 및 환경

이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.2010-0026621)
* 부산대학교 공과대학 정보컴퓨터공학부 (howonkim@pusan.ac.kr), 교신저자
** 한양대학교 공과대학 융합전자공학부 (dqkim@hanyang.ac.kr)

정보를 감지, 가공, 저장, 통합하며, 상황인식 정보 및 지식 콘텐츠 생성을 통해, 언제, 어디서, 누구나 원하는 맞춤형 지식 서비스를 이용할 수 있는 네트워크 인프라 기술로 정의했기 때문에 이 개념을 먼저 살펴보고자 한다.

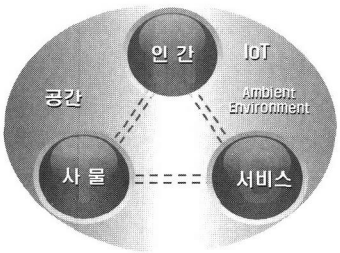
Ⅱ. IoT 기술

2.1 IoT 개념

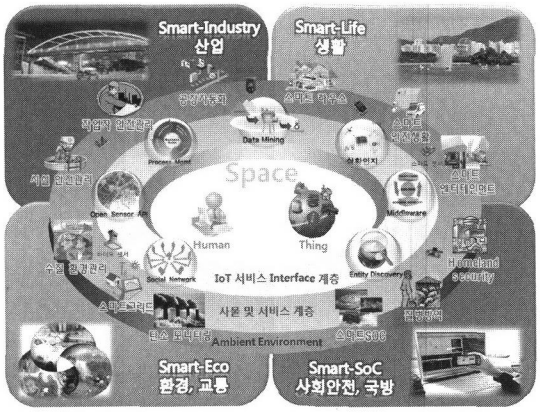
IoT는 아래 [그림 1]과 같이 인체망이나 디지털 홈, 물류/유통/텔레매틱스/물자관리/보안관리, 교통/방재/구급/국방 등과 같은 다양한 응용 서비스를 상호 연결해 주는 서비스 연결망으로서의 역할을 수행한다. 이와 같은 IoT에 대한 정의는 유비쿼터스 환경을 실현하는 기술 및 수단임을 강조한 정의로서 궁극적으로 IoT은 인간과 사물, 서비스 세 가지 분산된 환경 요소에 대해 인간의 명시적 개입 없이 상호 협력적으로 센싱, 네트워킹, 정보 처리 등 지능적 관계를 형성하는 사물 공간 연결망으로 볼 수 있다[1].

[그림 1]은 IoT가 인간과 사물, 서비스를 포함하는 인간 주변 환경(Ambient Environment)을 상호 연결해 주는 개념을 도식적으로 보여주는데 인간은 IoT을 통하여 사물 및 서비스와 소통하며, 사물과 서비스도 IoT 기술을 통하여 서로 소통한다. 이는 기존의 통신 및 네트워크 기술은 인간의 개입하에 인간과 사물, 인간과 서비스간 관계가 형성되었지만, IoT를 통하면, 사물과 서비스간에 자체 연결(reflexive) 뿐만 아니라, 사물과 사물, 서비스간에 천이적 (transitive) 연결을 가능하게 한다.

IoT 기술을 구체적으로 살펴보면 아래 [그림 2]와 같다. IoT는 인간과 주변 환경과의 상호 연결을 위해 센싱 기술과 각종 유무선 네트워크 기술을 사용하고 있으며, 연결망을 통한 정보에 대해서는 상황 인지 소프트웨어,



〔그림 1〕 인간과 사물, 서비스 IoT 3대 주요 구성 요소



〔그림 2〕 인간과 주변 환경의 관계 형성자로서의 IoT 개념도

오픈 플랫폼 기술, 미들웨어 기술, 웹 서비스 기술, 소셜 네트워크에 의해 가공/처리 되며, 이를 통해, 유무형의 사물과 각종 서비스와 연결된다.

2.2 IoT 주요 구성 요소

IoT는 전술한 것처럼 인간과 사물, 서비스와 같은 3대 주요 요소로 이뤄진다. 이들 3대 주요 구성 요소의 특성을 살펴보면 다음과 같다.

- 인간
  - 독립적 주체로서의 사람과 그 사람의 사고, 행동 양식 등을 의미함
- 사물
  - 유형의 사물과 무형의 사물로 구성됨
  - 유형의 사물은 물리적 객체로서의 사물이며, 무형의 사물은 가상 객체로서의 사물임. 무형의 사물로는 IT 서비스에서 특정 기능을 수행하는 함수, 객체 등이 될 수 있으며, 아바타도 무형의 사물로 정의할 수 있음
- 서비스
  - 인간 환경의 3대 요소에서 특정 목적을 위해 구현된 프로세스와 동작 메커니즘 집합을 의미함

IoT의 주요 구성 요소인 사물은 유무선 네트워크에서의 end-device 뿐만 아니라, 인간, 차량, 교량, 각종 전자 장비, 문화재, 자연 환경을 구성하는 물리적 사물 등이 포함됨. 무형의 사물로는 특정 서비스 수행 주체, 특정 기능을 수행하는 기능 등, 가상 객체로 대표할 수 있다. 서비스는 인체망이나 디지털 홈, 물류/유통/텔레

매틱스, 물자관리/보안관리, 교통/방재, 국방 등과 같은 전통적인 IoT 서비스 뿐만 아니라, 스마트그리드, 조선/기계 등 각종 IT 융합 서비스도 이에 속한다. 위치나 모션 등의 센싱 정보를 기반으로 하여 가공된 유무형 사물의 복합적 정보를 실제 현실에 덧붙여 실생활을 풍요롭게 해주는 증강 현실 서비스 등 가상 현실과 실제 공간을 끊김없이 이어주는 서비스도 포함된다.

IoT의 주요 구성 요소간의 소통 사례를 살펴보면 IoT의 특성을 좀 더 쉽게 파악할 수 있다. 먼저 첫 번째로 인간을 중심으로 인간과 인간, 인간과 사물, 인간과 서비스 소통 사례를 보면 다음과 같다.

- 인간과 인간
  - 인간과 인간의 직접적인 통신 수단(3G 휴대폰, Ethernet을 통한 이메일 등)과 인간 행동 양식이나 사고에 대한 소통(트위터, 소셜 네트워크 등)을 예로 들 수 있다.
- 인간과 사물
  - WSN(Wireless Sensor Network) 및 RFID, 바코드, QR 코드 기술, 전력량계, IP카메라 등 사물 정보를 인간이 얻는 경우와 그리고 Actuator나 가속 페달 등 인간의 행동 양식, 사고 등의 인간 정보를 사물이 얻는 경우를 예로 들 수 있다.
- 인간과 서비스
  - 인간과 서비스간의 상호 작용으로서 노인의 건강 상태를 지속적으로 모니터링하여 노인의 건강을 유지할 수 있도록 하는 경우를 예로 들 수 있다.

두 번째로 사물을 중심으로 사물과 사물, 사물과 서비스, 서비스와 서비스의 소통 사례를 보면 다음과 같다.

- 사물과 사물
  - 센싱과 통신 기능을 가진 사물이 통신 및 상호 작용하여 더욱 정교하거나 복합적인 정보를 얻는다. 예를 들어, 먼지 등, 가정내의 오염 정도를 센싱하는 센서노드와 로봇청소기(혹은 공기청정기)가 서로 통신하여, 해당 지역에 대한 먼지 제거 및 청소 업무를 수행하는 경우를 예로 들 수 있다.
- 사물과 서비스
  - 사물과 특정 기능을 수행하는 서비스간의 통신 및 상호 작용으로서, 예를 들어, 전력 부족량을 모니터링하는 서비스와 스마트그리드의 송배전 스위치 장치간의 상호 작용을 통해 특정 지역에 전력을 안정적으로 공급하는 경우를 그 예로 볼 수 있다.
- 서비스와 서비스
  - 서비스와 서비스간의 통신 및 상호 작용을 통해 value added 된 서비스를 창출할 수 있다. 예를 들어, 노인의 건강 상태를 모니터링하는 헬스케어 서비스(서비스 A)와 해당 노인의 거주지 혹은 여행지의 외부 환경(온도, 습도 등) 모니터링 서비스(서비스 B)와의 상호작용을 통해 노인의 건강 상태를 최적으로 유지할 수 있도록 하는 서비스가 이에 해당된다. 여기서 서비스 A로부터 얻은 정보와 서비스 B로부터 얻은 정보에 대한 상황 인식을 통해 고부가가치의 새로운 서비스를 해당 노인에게 제공할 수도 있다. 이처럼 다양한 서비스 조합에 대해서도 고부가가치를 제공할 수 있는 상황 인식 및 데이터마이닝 기능을 갖춘 IoT 기술이 필요하게 된다.

2.3 IoT의 3대 주요 요소 기술

2011년 발간된 USN 산업발전 전략 보고서에서 정의한 USN 기술은 IoT를 바라보는 국내의 시각을 보여주고 있다. 여기서 IoT의 3대 주요 요소 기술을 센싱 기술, 유무선 통신/네트워킹 기술, USN 서비스 인터페이스 기술로 정의했으며, 각 요소 기술을 살펴보면 다음과 같다.

- 센싱 기술
  - 센싱 기능으로는 전통적인 온도/습도/열/가스/조도/초음파 센서 등에서부터 원격 감지, SAR, 레이더, 위치, 모션, 영상 센서 등 유형 사물과 주위 환경으로부터 정보를 얻을 수 있는 물리적 센서를 포함한다.
  - 최근 물리적인 센서는 응용 특성을 좋게 하기 위해 표준화된 인터페이스와 정보 처리 능력을 내장한 스마트 센서로 발전하고 있으며, 또한, 센싱 기능에는 무형 사물, 즉 이미 센싱한 데이터로부터 특정 정보를 추출하는 가상 센싱 기능도 포함됨. 가상 센싱 기술은 실제 IoT 서비스 인터페이스에 구현된다.
  - 이는 기존의 독립적이고 개별적인 센서보다 한 차원 높은 다중(다분야) 센서기술을 사용하기 때문에 한층 더 지능적이고 고차원적인 정보를 추출할 수 있다.
- 유무선 통신 및 네트워크 인프라 기술
  - IoT의 유무선 통신 및 네트워크 장치로는 기존의

WPAN, WiFi, 3G/4G/LTE, Bluetooth, Ethernet, BcN, 위성통신, Microware, 시리얼 통신, PLC 등, 인간과 사물, 서비스를 연결 시킬 수 있는 모든 유무선 네트워크를 의미한다. 이에 IoT의 보안 이슈를 유무선 통신 및 네트워크 인프라 관점에서 봤을 때 각 통신 방식과 프로토콜에 따라 다양한 보안 이슈가 있음을 알 수 있다.

• IoT 서비스 인터페이스 기술
- IoT 서비스 인터페이스는 IoT의 주요 3대 구성 요소인 인간, 사물, 서비스를 특정 기능을 수행하는 응용 서비스와 연동하는 역할을 수행하는 부분을 의미한다.
- IoT 서비스 인터페이스는 네트워크 인터페이스의 개념이 아니라, 정보를 센싱, 가공/추출/처리, 저장, 판단, 상황 인식, 인지, 보안/프라이버시 보호, 인증/인가, 디스커버리, 객체 정형화, 온톨러지기반의 시맨틱, 오픈 센서 API, 가상화, 위치확인, 프로세스 관리, 오픈 플랫폼 기술, 미들웨어 기술, 데이터 마이닝 기술, 웹 서비스 기술, 소셜네트워크 등, 서비스 제공을 위해 인터페이스(저장, 처리, 변환 등) 역할 수행한다.
- 예를 들어, Text analytics, Data fusion, 데이터마이닝 등의 기술은 단순 센싱(가공되지 않은)한 방대한 양의 데이터를 기반으로 사용자의 수요에 따라 재조합 및 재구성하여 그에 부합하는 의미 있는 정보를 새롭게 취할 수 있도록 함. 즉, 서로 연관성이 없어 보이는 무질서한 기존 센싱 데이터를 분류 및 가공, 처리함으로서 상황에 맞는 의미 있는 정보를 추출할 수 있다.

Ⅲ. IoT 보안 기술

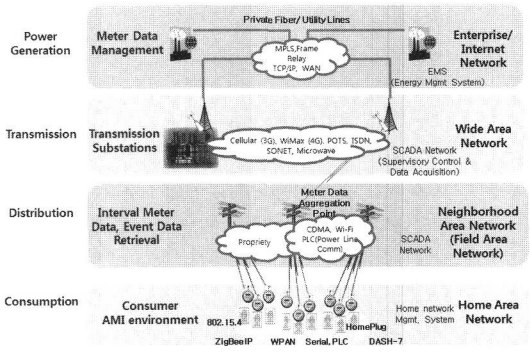
3.1 IoT 응용과 보안

IoT는 전술한 것처럼 인간과 사물, 서비스의 3대 요소가 각종 센싱 기술, 유무선 통신 및 네트워크 인프라 기술, IoT 서비스 인터페이스 기술에 의해 연결된다. 이와 같은 정의에 의하면 현재 우리 생활 주위에 존재하는 거의 모든 IT 기술 혹은 IT를 기반으로하는 융합 기술은 IoT의 한 종류로 볼 수 있게 된다. 이처럼 광범위한 IoT에 대한 보안 이슈를 정의하는 것은 현실적으로 가능하지 않을지도 모른다. 이 때문에 본 논문에서는 일반적인 IoT의 특성을 잘 표현 할 수 있는 IoT 한 응용에 대한 보안 취약성과 보안 기술을 살펴보기로 한다. 본 논문에서 보안 특성 분석 대상이 된 IoT 응용 환경은 스마트그리드 응용으로서 스마트그리드는 다양한 유무선 통신 기술과 프로토콜 기술이 사용되며 스마트미터, 스위치, DCU(Data Concentrator Unit), EMS (Energy Management System), ESS(Energy Storage System) 등 다양한 구성요소와 서비스가 센싱 및 통신과 같은 상호 작용을 한다.

3.2 IoT 보안 사례(스마트그리드 보안)

IoT는 다양한 종류의 유무선 통신 인프라를 가지며 많은 종류의 사물과 서비스가 복합적으로 존재하는 특성을 가진다. 이러한 IoT의 대표적인 사례로서 스마트그리드 응용을 들 수 있다. 스마트그리드란 진보된 감지와 통신, 제어 기술을 사용하여 발전, 송/변전, 배전을 좀 더 효율적, 경제적, 안정적으로 하는 현대적인 전력망을 의미한다. 이는 기존 전력망(발전/송전/배전/소비 관련 설비 및 기기 모두 포함)에 정보통신기술(ICT)을 접목하여 전력망의 효율성, 경제성, 안전성, 신뢰성을 향상시키는 것이 목적이다. 스마트그리드에는 에너지원과 전력 송배전, 제어, 통신, 소프트웨어, 컴퓨팅, 가전기기, 보안 등 다양한 기술과 정책이 복합적으로 얽혀있는 특성을 가진다.

특히 스마트그리드 환경은 (1) 기능적으로 서로 독립적인 요소로 구성되며, (2) 관리차원에서는 서로 독립적이면서 의존적이며, (3) 개별적으로 지속적인 진화가 필요하며 (4) 기존에 존재하지 않았던 새로운 기능이나



〔그림 3〕 네트워크 관점에서 본 스마트그리드 구조

특성이 발생할 수 있으며(5) 지역적으로 분산되어 있다는 특성 때문에 System of Systems(SoS)라고 정의하기도 한다 [2]. 이러한 특성으로 인하여 스마트그리드에서 필요로 하는 보안 기술은 매우 다양하고 복잡하며 각각의 구성 시스템간의 인터페이스에 따라 각각에 적합한 보안 기술을 필요로 한다 [3].

위 그림은 네트워크 인프라 관점에서 본 스마트그리드 구조도이다. 구성 요소의 특성과 응용 서비스 특성, 관리 특성 등을 고려하지 않고 오직 네트워크 관점에서만 스마트그리드를 보는 경우에도 다양한 유무선 통신 방식과 프로토콜이 존재하므로 각각에 적합한 보안 기술을 구현하는 것은 쉬운 일이 아니다.

예를 들어, 스마트그리드의 HAN(Home Area Network) 영역에서는 스마트미터와 DCU(Data Concentrator Unit)를 연결하기 위해 ZigBee, WPAN, Serial, PLC, DASH-7, WiFi 등 다양한 유무선 통신 프로토콜이 사용될 수 있다. 한편, HAN 영역은 스마트그리드 구성 요소 중에서 end-point에 해당하는 영역으로서 사물과의 직접적인 연결망 역할을 하기 때문에 HAN 영역 프로토콜 보안 기술은 전체 스마트그리드 보안 기술에 절대적인 영향을 준다.

그런데 이러한 HAN 영역 유무선 통신 프로토콜에 대한 보안 기술은 현재 표준에서도 정의 되어 있지 않거나 비록 표준에서 보안 기술이 정의되어도 기밀성 및 무결성만을 제공하는 수준에 불과한 경우가 많다. 또한, 이들 유무선 통신 프로토콜은 서로 상호 연결되어 사용되는 것을 고려하여 개발된 통신 프로토콜이 아니므로 상호 연결이 용이하지 않으며, 특히 보안 기술에 있어서 서로 다르기 때문에 보안 기술을 통합하여 사용하는 것은 어렵다. 참고로 WiFi 상에서는 EAP(Extended Authentication Protocol) 프레임워크를 사용하여 다른 인증 프로토콜과 결합이 가능하지만, ZigBee, PLC, DASH-7 프로토콜 보안 표준은 상호 호환성이 없기 때문에 보안을 연결하여 사용하는 것은 어렵다.

스마트그리드의 보안 요구 사항 중에서 HAN 영역에서 수집한 전력 센싱 데이터값을 EMS(Energy Management System)까지 중간에 암호화된 값을 복호화하지 않고 전송되어야 한다는 요구사항이 제기되었는데, 이러한 보안 요구 사항을 만족시키기 위해서는 다음과 같은 사항을 고려해야 한다. 먼저 통신 프로토콜을 살펴보면 다음과 같다.

- HAN 영역에서는 ZigBee 혹은 PLC를 사용하여 보안 전력 센싱 값을 암호화하여 통신함
- DCU에서는 해당 센싱 값을 복호화하지 말아야 함
- DCU와 EMS 시스템은 다양한 유무선 통신 방식(WiFi, Ethernet)으로 연결됨

〔표 1〕 스마트그리드 HAN 영역 유무선 프로토콜 보안 기술

HAN용 통신프로토콜	보안 기술
ZigBee	• 통신 프레임 보안(기밀성/무결성) 제공 • network 계층, APS 계층 보안기술 정의 • 키 설정, 전송 기능 제공 • Master key, link key, network key 개념 사용 • 디바이스 인증 기능 제공
WPAN (IEEE 802.15.4)	• 통신 프레임 보안(기밀성/무결성) 제공
Serial	• 표준에서는 보안기술 정의되어 있지 않음 • 스트림 암호, 대칭키 암호를 사용하여 serial 통신 데이터 암호화 사용 [4]
PLC	• Homeplug 등에서 기밀성, 무결성 표준 정의 • 키 관리 기법 정의
DASH-7	• 통신 프레임 보안(기밀성/무결성) 제공 • 키 관리, 키 교환 방식에 있어서 공개키 암호(타원곡선 암호) 정의
WiFi	• 통신 프레임 보안(기밀성/무결성) 제공 • WPA, WPA2 등 정의되어 있음

이 경우, 전력 센싱값은 ZigBee의 프레임 보안 표준에 따라 AES-CCM으로 암호화 될 수 있다. 또한 여기서 암호화에 사용된 암호화 키 값은 EMS 시스템으로부터 분배되었다고 가정할 수 있다.

ZigBee 프로토콜로 전송된 암호화된 센싱 값을 DCU에서 EMS 시스템으로 그대로 전송하거나 혹은 다시 암호화하여 전송한다면 전술한 요구사항을 만족시키는 셈이 된다. 하지만, 여기서 문제가 발생한다. HAN 영역은 유무선 통신 프로토콜은 에러율이 높고(특히 PLC인 경우) DCU에서 EMS로 전송되는 메시지 트래픽을 줄이기 위해 동일한 값 혹은 오류가 있는 값인 경우에는 적절한 필터링 기법을 사용해야 한다. 하지만, 암호화된 전력 센싱 값인 경우 DCU에서 복호화할 수 없거나 혹은 전력 센싱 값을 시퀀스 번호를 사용하여 암호화 될 경우 동일한 전력 센싱값에 대해서도 서로 다른 암호화된 값을 가지므로 필터링 기법을 적용할 수 없게 된다.

〔표 2〕 스마트그리드 주요 보안 요구사항

보안 요구 사항	대상 환경	적용 가능 기술
제어/센싱 메시지 보호/인증	스마트그리드 송배전 스위칭 소자, 스마트그리드 구성 유무선 네트워크 및 라우터 등	• 대칭키 기반 보안 프로토콜(AES-CCM) • 해쉬 및 MIC 기반 보안 프로토콜
디바이스 인증	스위칭 소자, RTU, DCU, 릴레이, AMI 단말, 스마트미터 등	• 대칭키/해쉬 기반 인증/인가 프로토콜 • 멀티캐스트 인증/인가 프로토콜 • 공개키 암호 기반 서명/검증 프로토콜(ECDSA, etc.)
키 분배/관리	각종 스위칭 소자와 AMI 디바이스, 유무선 네트워크 장치, 서버, 게이트웨이 등	• 공개키 기반 키 분배/관리기술(PKI-like 키 관리기술) • Master 비밀키 기반 키 분배/관리 기술
보안 모니터링 및 보안 관리	유무선 네트워크 환경(WAN, LAN, Wi-Fi, CDMA, 3G, 4G, ISDN, IEEE 802.15.4,WPAN 등)	• SCADA 기술 • Dedicated 보안 모니터링/관리 기술
프라이버시 보호	센싱 정보 저장 DB, 서버, 응용 서비스, 네트워킹 환경 등	• 대칭키 기반 기밀성 제공, 공개키 기반 암호화 프로토콜 등 • DB 보안, 권한 제어, ownership 제어
신뢰성 증명	스위칭 소자, RTU, 릴레이, AMI 단말, 서버, 플랫폼, 응용 서비스 등	• TPM과 같은 Trust Anchor 개념 적용 • AIK(Attestation Identity Key) 개념 적용 등
물리적 안전성/신뢰성	AMI 디바이스, 스위칭 소자, 응용 서비스 구성 플랫폼 등	• Tamper resistance/evidence 기술 • Side channel resistance 기술 • Anti-reverse engineering 기술 등

이처럼, HAN 영역과 NAN 영역, EMS 영역 전체 구간에 걸쳐 중간 단계에서 복호화 없이 암호화를 수행해야한다는 요구 사항을 만족시켜야 한다면 이는 과도한 트래픽을 유발하며 결국 시스템의 과부하를 초래한다. 이 예는 스마트그리드 환경에 보안을 적용할 경우 발생할 수 있는 문제 중에서 하나의 사례에 불과하다. 이 외에도 각 구성 요소간 키 관리의 차이, 보안 메커니즘 차이, 이종 시스템에 대한 동일한 접근 제어 기법 적용의 어려움 등, 다양성과 이기종, 분산 특성을 가지는 IoT 환경에서는 보안성 제공을 위해서 해결해야하는 많은 문제가 존재한다.

표 2는 스마트그리드 주요 구성 요소에 대한 보안 요구 사항과 적용 가능한 보안 기술을 기술하고 있다. 스마트그리드 환경에서의 보안 요구 사항은 다양한 방법으로 정의할 수 있으며, 정의하는 방법에 따라 각각 다양한 수준의 보안 기술이 정의 될 수 있다. 본 논문에서는 스마트그리드 구성 요소의 일반적인 보안 요구 사항을 기술하고 각각의 구성 요소에서 필요로 하는 보안 기술을 정리했다.

표 2를 보면 제어 및 센싱 메시지 보호 및 인증을 위해서는 해당 네트워크 프로토콜에 적합한 형태의 기밀성 및 무결성이 제공되어야 한다. 이는 각 표준에서 정의한 방법에 의존하지만 대표적인 통신 프레임 보안을 위한 기법으로는 AES-CCM과 MIC(Message Integrity Code)를 사용하는 것이 일반적이다. 또한 스위칭 소자, RTU, DCU, 릴레이, AMI 단말, 스마트미터 등과 같은 디바이스 인증을 위해서는 대칭키/해쉬 기반 인증/인가 프로토콜과 멀티캐스트 인증/인가 프로토콜, 공개키 암호 기반 서명/검증 프로토콜(ECDSA, etc.)등이 사용될 수 있다. 이 뿐만 아니라, 키 분배/관리, 보안 모니터링 및 보안 관리, 프라이버시 보호, 신뢰성 증명, 물리적 안전성/신뢰성 증명을 위한 적용 대상 환경과 보안 기술이 정의 되었다.

여기서 정의된 보안 요구 사항은 상위 수준에서 정의한 보안 요구 사항으로서 이러한 보안 요구 사항을 실제 시스템상에서 만족시키기 위해선 각 구성 요소의 특성과 인터페이스 등을 고려해야 한다.

V. 결 론

본 논문에서는 인간과 사물, 서비스가 센싱과 유무선 통신/네트워킹 기술, IoT 서비스 인터페이스 기술을 통해 상호 작용함으로서 다양한 IT 응용 서비스를 제공하는 IoT에 대해 살펴봤으며 이에 대한 보안 요구 사항과 적용 가능한 보안 기술에 대해 살펴봤다.

IoT는 매우 다양한 요소와 특성을 가지므로 필요한 보안 기술과 보안 특성을 정형화하는 것은 쉽지 않다. 이에 본 논문에서는 SoS(System of Systems) 특성을 가지는 대표적인 IoT 응용인 스마트그리드 환경에 대한 보안 요구 사항과 보안 특성을 살펴봤다. 스마트그리드의 보안 특성을 살펴봄으로서 소위 기밀성, 무결성, 가

용성이라는 기본적인 보안 요구 사항과 인증/인가, 부인 방지, 접근제어 등과 같은 보안 요소는 IoT 응용 서비스의 구성 요소와 인터페이스 특성, 제반 유무선 통신 특성/프로토콜에 따라 개별적으로 정의되어야 한다는 것을 확인했다. 특히 IoT 환경은 센싱 역할을 하는 end-point에서는 자원 제약성(resource constraints)이 높기 때문(예: 스마트미터, 센서 노드 등 HAN 영역)에 기존의 IT 시스템에서 사용하던 전통적인 IT 보안 기술을 적용하는 것이 용이하지 않다. 또한, IoT를 서비스를 실현하는데 사용되는 다수의 유무선 통신 프로토콜은 IPsec, SSL 등과 같은 통신 보안 프로토콜처럼 정교하게 정의되지 않았거나 아예 표준에서는 보안 기능을 포함하지 않았기 때문에 보안 기능을 제공하는데 있어서 많은 어려움이 있다. 더욱이 IoT 시스템의 분산, 이기종, 멀티도메인 특성 등, SoS 특성으로 인하여 기존의 접근 제어 기법, 인증/인가 기법, 보안 관리 기법을 적용하는 것이 용이하지 않다. 요약하면 본 논문에서는 IoT 기술을 디바이스 중심의 무선 센서네트워크와 같은 수준이 아닌 복합적이며 다양한 사람과 사물, 서비스의 복합체로 인식하여 여기서 필요한 보안 요구 사항과 적용 가능한 보안 기술을 살펴봄으로서 IoT 서비스에서 필요로 하는 보안 기술에 대한 이해를 돕고자 하였다.

참고문헌

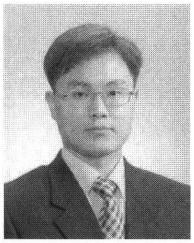
[1] 김호원, "USN산업발전 전략 수립 연구 최종 보고서", 지식경제부, 2011.2

[2] Maier, M.W., and Rechtin E. The Art of Systems Architecting, 2nd Edition. CRC Press, London, 2000

[3] NISTIR 7628 Guidelines for Smart Grid Cyber Security, NIST, 2010.8

[4] Serial Data Encrypter, http://www.dcbnet.com/datasheet/se6600ds.html

〈著者紹介〉



김 호 원 (Howon Kim)
정회원
1989년 3월~1993년 2월 : 경북대학교 전자공학과 학사
1993년 3월~1995년 2월 : 포항공과대학교 전자전기공학과 공학석사
1995년 2월~1999년 2월 : 포항공과대학교 전자전기공학과 공학박사
1998년 12월~2008년 2월 : 한국전자통신연구원(ETRI)
정보보호연구단 선임연구원 / 팀장
2003년 6월~2004년 7월 : Ruhr University Bochum Post Doctorial
2008년 3월~현재 : 부산대학교 정보컴퓨터공학부 부교수
<관심분야> 스마트그리드 보안, RFID/USN 보안, PKC 암호, VLSI, 부채널 공격, APT

김 동 규 (Kim, Dong Kyue)
정회원
1992년 2월 : 서울대학교 컴퓨터공학과 졸업
1994년 2월 : 서울대학교 컴퓨터공학과 석사
1999년 2월 : 서울대학교 컴퓨터공학과 박사
1999년 9월~2006년 2월 : 부산대학교 컴퓨터공학과
2006년 3월~현재 : 한양대학교 전자통신컴퓨터공학부 및 융합전자공학부
<관심분야> 암호 알고리즘, 임베디드보안시스템 설계, Security System on Chip(SoC)