정 보 보 호 학 회 지
제25권 제5호, 2015. 10

# Industrial IoT 환경의 사이버보안 이슈 연구

장 현 수*, 김 현 진*, 손 태 식**

요 약

산업사물인터넷(IIoT)은 사물인터넷(IoT)과 같이 기존의 여러 ICT 기술들과 무선센서네트워크 및 다양한 통신 기술들이 산업제어시스템에 적용된 것을 의미한다. IIoT는 일반적인 상용 IoT와 많은 부분 공통점과 그 기반 기술에 있어서의 동일한 성격을 가지지만 적용 대상 환경에 있어 차이를 가지고 있기 때문에 산업제어영역에서 IoT기술을 도입하기 위해서는 추가적으로 고려해야할 사항들이 존재한다. 본 논문에서는 IoT와 IIoT에 대하여 간단히 설명하고 IIoT 환경의 특수성에 대해서 다룬다. 그 후 상용 IoT에서 발생한 보안 사고관련 사례들을 살펴보고 산업제어영역에서 사이버보안 사고 발생 시 그 피해 규모를 살펴본다. 그리고 IIoT를 도입하면서 보안관점에서 필요한 사항들에 대해 서술하였다.

## Ⅰ. 서 론

최근 다양한 분야에서 사물인터넷(Internet of Things, IoT) 기술에 대하여 자주 언급되면서 업계에서는 이에 대한 관심이 고조되고 있다. 사물인터넷은 인터넷에서 물체 간의 연결성을 기반으로 하는 기술 및 서비스를 포함하는 개념으로 물리적으로 존재하는 구동장치(Actuator) 혹은 센서 등에 ICT 기술을 접목하고 네트워크에 연결시켜 사람과 상호작용 없이 상황에 따른 서비스를 제공하는 무선센서망(Wireless Sensor Network, WSN), IoT 개념은 물체를 네트워크에 연결함으로써 독립적으로 분산되어 있던 서비스들을 연결하여 새로운 서비스를 창출하거나 기존 시스템보다 개선된 서비스를 제공하고 있다.

이러한 업계 흐름은 산업제어 분야에도 영향을 미쳤으며 기존의 산업제어시스템 기술과 IoT가 결합된 산업사물인터넷(Industrial Internet of Things, IIoT)가 등장하였다. 기존에 폐쇄성을 띄고 있던 산업제어시스템에 IoT개념이 도입되기 시작하면서 개방성을 지니게 되었다. 개방성을 지님으로써 여러 이점이 생겼지만 이면에 외부와의 접근성이 증가하여 공격자와의 접촉점이 증가하였고 기존 시스템에서는 반드시 고려하지 않아도 되었던 보안이 필수적이게 되어가고 있다. IoT 디바이스는 출시 이후에 유지보수, 보안 업데이트 적용 등 사후 보안조치가 불가능하거나 고비용이 수반되기 때문에 출시 이전에 보안에 대하여 숙고해야한다.(1) 특히나 IIoT 영역의 경우 기반시설로 불릴 수 있는 대부분의 산업현장에 적용 가능하며 범국가적인 규모를 이루어고 있기 때문에 보안사고 발생 시 국가단위 혹은 그 이상의 금전적 손해와 사회 전반에 막대한 파급 효과를 미칠 수 있다. 이를 방지하기 위하여 본 논문에서는 IIoT 환경에서 필수적으로 고려해야할 보안사항들을 제시한다.

전체적인 구성은 2장에서 IoT와 IIoT의 정의와 특징에 대해 서술하고 3장에서 IIoT 환경의 특수성과 보안 이슈에 대해 다룬다. 그 후에 4장에서 IIoT를 도입함에 있어 보안관점에서 고려해야할 사항들을 제시한 후 결론으로 논문이 마무리 된다.

## Ⅱ. IoT와 IIoT

### 2.1. Internet of Things (IoT)

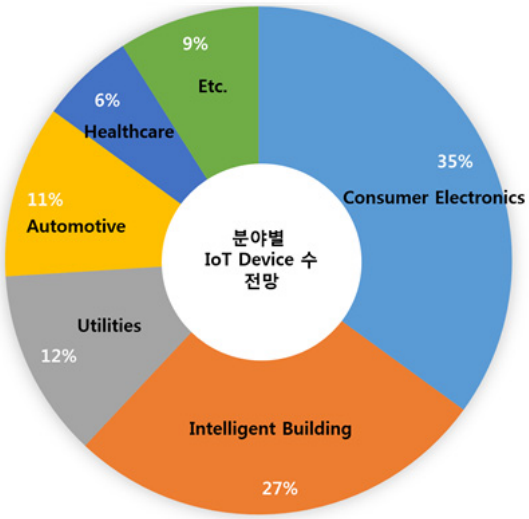
IoT는 여러 기술들이 융합된 복합적인 개념으로 이에 대한 정의가 다양하게 이루어졌었다. Radio Frequency Identification (RFID)을 이용하여 각 사물에 고유의 신분을 부여하는 개념으로부터 시작하여(2) 오늘날에는 임베디드, 유비쿼터스, 모바일, M2M(Machine-to-Machine), WSN, 클라우드 컴퓨팅

* 아주대학교 컴퓨터공학과(ics_dant@naver.com, ny24007@gmail.com)
** 아주대학교 정보컴퓨터공학과(tsshon@ajou.ac.kr)

등 여러 기술들이 복합적으로 융합되어 사물들이 스스로 네트워크를 형성하고 인터넷과 연결하여 사물들이 인터넷에 접속하고 서로 간에 대화(통신)를 할 수 있도록 해주는 기반을 의미하게 되었다.(3)

디바이스 스스로 네트워크를 형성하고 정보를 교환하는 M2M, WSN 등의 기술에 기반하는 IoT 개념이 기존 네트워크에 도입되면서 기존에 비해 유연하고 개방적인 특성을 지니게 되었고 이러한 유연성과 개방성이 서비스의 질을 높인 다는 인식이 업계에 퍼지게 되면서 다양한 서비스에 적용되기 시작했다.

(그림 1)은 2020년에 M2M으로 엮여있는 서비스별 IoT 디바이스의 분포를 나타내는 도표이다. 가장 많은 수의 디바이스는 사용자의 가정에서 사용할 가전제품이 될 것으로 여겨지고 스마트빌딩, 공익사업(전기, 수도, 난방 등), 교통, 건강관리 등에 관련된 디바이스들이 그 뒤를 이을 것이라 전망 되고 있다. 즉, 대표적인 IoT 서비스들은 가전제품, 스마트빌딩, 공익사업, 교통, 건강관리에 접목된 서비스일 것이라 여길 수 있다.




〔그림 1〕 2020년 IoT Device 분포 전망, M2M Global Forecast and Analysis 2011-22, Machina, 2012 (4)

### 2.2. Industrial IoT (IIoT)

앞에서 다룬 것처럼 IoT는 복합적인 기술을 기반으로 여러 서비스 분야에 접목되고 있다. 여러 서비스 중 산업제어영역에 적용된 IoT를 산업사물인터넷(Industrial Internet of Things, IIoT)라 부른다.

전력생산, 송전, 가스공급, 수도공급 등의 공익사업과 제조업관련 산업을 포함하는 산업제어영역은 기존에 폐쇄적이고 독립적 성격을 띠며 단방향으로 운영되는 서비스를 제공하였었다. 최근 이러한 폐쇄적인 시스템에 ICT기술을 도입하면서 독립적으로 운영되던 시설들이 서로 연결되었고 상호운용화되어 기존보다 유연하고 효율적으로 그리고 양방향으로 작업을 처리하는 스마트 그리드가 등장하여 산업계에 바람을 일으켰었다. 여기에 IoT의 센싱 기술이 접목되면서 산업제어시스템에서 개선된 상황 인지 모니터링이 제공되었고 산업계에 IoT를 도입하였다하여 Industrial과 IoT를 합쳐 IIoT라 부른다

학계에서는 센서가 저렴해짐에 따라 IIoT의 시대가 도래하고 있으며, 향후 15년 내에 전세계 GDP가 10~15조 달러(한화 약 200,000,000억)이상의 성장을 할 수 있을 것이라 전망하였고(5) IoT 국제학회(6)에서도 2014년에 IIoT를 주제로 워크샵을 열어 Exxon Mobil, Simense와 같은 업체들이 Process Control에 IIoT를 접목하는 사례를 주제로 발표하였다.

업계에서는 ABB, AT&T, Cisco, GE, Intel, KETI, Samsung 등 189개의 업체와 Carnegie Mellon, John Hopkin 등 총 9개의 대학 연구진들이 참여하여 Industrial Internet Consortium (IIC)이라는 협력단체를 구성하여 표준 및 테스트베드 개발 및 에너지, 의료, 생산, 공공, 수송 분야에 대해 주요 연구를 수행하고 중에 있다.

## Ⅲ. IIoT 환경의 특수성 및 보안 필요성

### 3.1. IIoT 환경의 특수성

상용 IoT와 다른 특수성을 지닌다. 가장 보편적으로 IoT가 적용되는 곳은 홈 가전 영역의 디바이스들이다. 이 디바이스들은 서비스의 가장 끝단에 있기 때문에 보안사고가 발생하더라도 그 주변 네트워크에서 파급력이 끝나게 된다. 때문에 보안에 투자하기 보다는 저전력, 설치 용이성, 낮은 설치비용 등에 초점이 맞춰져 있다. 하지만 산업제어환경은 보통 공급자의 위치에 있기 때문에 어떠한 사고가 발생할 경우 그에 대한 파급 효과

는 공급을 받는 소비자까지 영향을 미치게 된다. 특히나 산업제어환경의 서비스 공급범위가 작게는 도시 크게는 국가단위이다 보니 문제가 발생할 경우 영향력이 엄청나다. 때문에 IIoT는 강력한 보안요구사항, 인간에 의한 제어 최소화, 극한의 환경에서의 강력한 내성 등 기존 IoT에서와 다르게 강력한 조건들이 필요하다.

### 3.2. IoT에서의 피해 사례

IoT는 우리 일상생활에서 주요 제어시스템까지 여러 분야에 접목되어 효율성 및 편리성 등을 증가시킬 수 있지만 보안이 취약하여 공격이 성공한다면 피해 규모와 파급력 또한 클 것이다.

IoT에 대한 보안 위협은 매년 증가할 것으로 예상되며 IoT 등 융합보안 침해사고에 따른 피해규모는 2015년 약 13조 4천억원에서 2030년 약 26조 7천원에 이를 것으로 예상된다. (7)

〔표 1〕 IoT 공격 사례

| IoT 기기 | 사례 |
|---|---|
| 스마트 홈 | 2014년 보안 업체인 프루프포인트(Proofpoint)는 씽봇(Thingbot) 해킹 툴이 스마트 홈 네트워크를 통해 스마트 TV, 냉장고 등의 스마트 가전제품을 감염시켜 해당 기기를 이용하여 75만개 이상의 스팸 메일이 개인 및 기업에게 전송되었음을 발견함 (8) |
| 스마트카 | 2015년 모바일 데이터 네트워크와 연결된 스마트카의 엔터테인먼트 시스템을 해킹하여 스마트카를 원격에서 제어할 수 있음을 보였으며 이에 자동차 회사는 140만대의 해당 스마트카를 리콜하였음 (9)<br>해당 공격에 대한 자료 및 방법은 '블랙햇 보안 컨퍼런스 2015'에서 발표될 계획 |
| 웨어러블 디바이스 | 2015년 시만텍 보고서에서 스마트폰에 설치된 랜섬웨어 apk파일이 스마트워치와 스마트폰이 페어링을 수행할 때 스마트워치에 자동으로 설치될 수 있음을 보임(10) |
| 스마트 그리드 | 2009년 블랙햇 컨퍼런스에서 스마트미터의 취약점을 이용하여 한 스마트미터를 감염시킨 후 연결된 모든 스마트미터를 조정할 수 있음을 보여 도시 전체를 정전시킬 수 있음을 보임 |
| 스마트 시티 | 2014년 미국 보안업체인 IOActive는 무인항공기에 장비를 탑재하여 자가증식 형태의 웜을 통해 세계 10개국 이상에서 사용되고 있는 교통시스템 장비에 침입 후 제어할 수 있음을 보임(11) |

실제로 최근 IoT 환경을 이용한 공격으로 인해 피해 사례가 발생하였으며 [표 1]와 같이 IoT 기기 공격에 대한 발표도 활발히 이루어지고 있다.

### 3.3. 산업 사고 발생 시 피해 규모

서비스 공급범위가 도시에서 국가단위로까지 확대될 수 있는 산업 제어 시스템은 공격으로 인한 사고가 발생 시 [표 2]와 같이 막대한 금전적 피해뿐만 아니라 심각한 사회적 혼란이 야기될 수 있다.

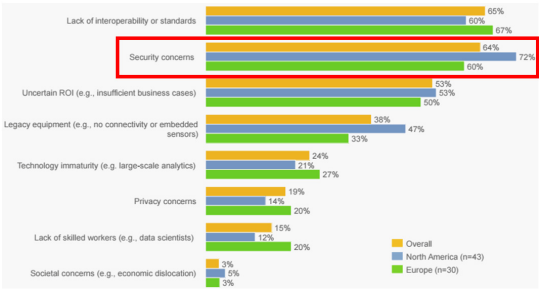
업계에서도 이러한 피해 가능성을 염두에 두고 보안이 중요한 고려사항으로 여기는 것을 World Economic Forum의 자료에서 확인 할 수 있다. 또한 ICS-CERT의 통계에 따르면 제어시스템 대상의 사이버 공격은 증가하는 추세이며 기존 폐쇄망이었던 산업 제어시스템이 IIoT 도입으로 인해 기존 IT 기술과 IoT환경에 존재하는 보안 위협이 유입될 수 있기 때문에 보안에 대한 고려가 더욱 필요하다.

이에 IIoT 도입에 있어서 필요한 보안 고려사항을 다음 장에서 다룬다.

IIoT 시설 하나가 상용 IoT 규모에 비해 크기 때문에 한 번 설치 된 후에는 시설을 바꾸거나 업데이트하기

〔표 2〕 산업 사고 피해 규모

| 사례 | 피해 금액(원) |
|---|---|
| 9.15 정전 | 약 600억 |
| 울산화학공업단지 정전 | 약 1000억 |
| 고리 원자력 발전소 | 약 628조 |




〔그림 2〕 IIoT를 산업 및 사업에 적용할 때 주요 고려사항, Industrial IoT: Unleashing the Potential of Connected Products and Services, 2015.01 (12)

위해선 거금을 투자해야한다. 특히나 보안 문제가 발생할 경우 원거리 제어를 통해 시스템 마비 혹은 물리적 피해를 야기 할 수 있다.

업계에서도 이러한 위협 가능성을 염두에 두고 보안을 중요한 고려사항으로 여기고 있음을 World Economic Forum의 자료에서 확인 할 수 있다. 이에 IIoT 도입에 있어서 필요한 보안 고려사항을 다음 장에서 다룬다.

## Ⅳ. IIoT에 보안 관점에서 필요한 사항들

현재의 IoT는 연결성과 데이터 공유를 초점에 두고 많은 연구와 사업이 진행되고 있기 때문에 앞서 다룬 것과 같이 여러 보안사고가 발생 가능하고 이를 산업제어로 그대로 가져올 경우 걷잡을 수 없는 피해를 야기할 수 있다. 때문에 IIoT를 도입하기 위해선 다음과 같이 저전력 암호화, 더 철저한 인증 방식, 디바이스 별 로그 수집 방안, 유선과 무선 네트워크의 혼용, 물리적 보안 등을 고려해야한다.

### 4.1. 경량화 암호

IIoT가 일반적인 상용 IoT보다 보안을 우선 시 해야하지만 그렇다고 소비전력과 시간 자원 낭비를 무시할 수 없다. 암호화의 강도와 자원 소비량의 절충점(trade-off)을 고려하여 선택해야 할 것이다. 이외에도 암호화 강도는 네트워크의 유·무선 여부, 디바이스 내 정보의 가치, 제한된 작업시간 등의 환경적인 요소들 또한 고려하여 선택해야한다.

### 4.2. 개선된 인증 방식 필요

IoT를 산업제어에 적용하기 위해선 상용 IoT와는 다른 인증 방식을 채택해야한다. 상용 IoT 환경에서는 디바이스 인증을 사람의 간섭 없이 자동적으로 이루어지는 것과 저비용에 초점을 맞춰져 있기 때문에 사람을 쓰지 않았다. 때문에 인증에 있어서 디바이스 내부에 있는 정보(MAC 주소, IP 주소 등)나 클라우드에 등록하는 방식의 인증 시스템을 사용한다.

하지만 MAC 주소, IP 주소 등은 ARP 포이즈닝, IP 스푸핑 공격 등에 의해 공격자가 허위 인증 될 수 있다. 클라우드 기반 인증 시스템은 특정 벤더에서 나온 제품들만 관리할 수 있기 때문에 기존의 장비를 이용하거나 다른 벤더의 장비들을 추가하여 상호호환성을 중요시하는 산업 환경에서는 사용하기 부적합하다. 해서 IIoT를 도입하기 위해선 산업 환경에 적합한 인증 방식을 도출해야 할 것이다.

### 4.3. 비정상적 작업 탐지

IIoT 환경에서 만약 사고가 발생하게 된다면 이는 상용 IoT에서의 피해에 비교할 수 없을 정도로 큰 파장 및 피해를 입힐 것이라고 앞에서 다루었다. 이러한 피해들을 예방하기 위해선 운영자는 항시 공격 징후 등을 파악해야한다.

기존의 IT환경에서는 방화벽이나 침입탐지시스템(Intrusion Detection System) 혹은 침입방지시스템(Intrusion Prevention System) 등을 이용하여 공격 및 침입에 대해 방어하였다. 하지만 이는 가상적인 환경에서 오가는 정보(traffic, packet, data)만을 토대로 공격을 막는 방식이었다. 하지만 이는 여러 물리적인 시스템들이 결합되어 있는 IIoT 환경에서는 네트워크 정보만으로는 위험한 상황을 인지하기 어려울 것이다.

이를 타파하기 위해선 IIoT로 들어오면서 도입된 센서들을 이용하여 시설의 물리적 환경에서의 감지된 정보를 수집하고 분석하여 이를 토대로 이상 징후를 찾아내는 방식 또한 도입되어야 할 것이다.

### 4.4. 각 디바이스 별 로그 수집

IIoT는 사전준비도 중요하지만 규모가 크기 때문에 사고가 일어난 후나 징후가 발견되었을 때 이에 대해 파악할 수 있도록 준비해야되므로 로그 기능이 필요하다.

이러한 로그들은 각 디바이스들에서 일어난 중요 이벤트 및 작업들을 기록해야하고 외부에서는 접근이 불가능하게 설정해야된다. 또한 내부에서도 저장 공간이 가득차서 새로운 공간이 필요한 것이 아닌 이상 이전 기록들을 지우지 않아야 할 것이다.

현재로써는 각 디바이스들에서 네트워크 로그, 시스템 로그와 같은 로그들을 수집할 정도로 저장장치들이 커다랗지 않다. 해서 로그들을 효율적으로 기록하는 것

에 대한 연구도 필요하다.

### 4.5. 물리적 보호

IIoT에서는 구성요소들의 물리적 피해, 오용, 절도 등의 물리 환경에서의 보안 또한 고려해야한다. 이를 위해서 물리적 접근제한, 물리적 방호, 접근하는 자에 대한 인증 등을 확실하게 하여 물리적인 피해 방지를 할 수 있도록 해야 할 것이다.

이외에도 산업현장 및 기반시설 자체의 사이버보안 관점의 다양한 위협요인을 계속하여 식별하고 그에 맞는 대응방안을 적용하는 노력이 필요하다.

## Ⅴ. 결 론

현재 IT업계는 IoT라는 개념을 자신의 제품들에 입하고 있다. 이에 많은 서비스 영역에 IoT가 스며들었고 산업제어시스템 분야에서도 이 개념을 도입하려는 움직임이 드러나고 있는 추세이다.

하지만 산업제어환경의 특수성을 고려했을 때 기존의 상용IoT를 그대로 적용하기엔 무리가 있으며, 기존에 폐쇄성을 띠고 있던 산업제어환경에 개방적인 성격의 IoT가 그대로 도입될 경우 개방성 증가 및 기존 기술들의 보안 위협 그리고 새로운 보안 위협들이 발생할 가능성이 있기 때문에 IIoT환경에서는 상용 IoT에 비해 보안적 관점에서 더 많은 것을 고려해야한다.

본 논문에서는 IIoT의 특수성에 따라 추가적으로 고려해야할 보안적인 사항들에 대해 서술하기 위하여 상용 IoT환경에서의 보안 위협과 사례들의 살피고 IIoT 도입에 있어서 보안 관점에서의 고려사항들을 도출하였다. 추후엔 본 논문에서 다룬 보안 고려사항외 고려사항을 추가로 도출하여 개선된 IIoT 보안 요구조건을 도출하고 이를 토대로 보안 가이드라인을 작성하는 연구가 필요 할 것으로 여겨진다.

## 참 고 문 헌

[1] Ministry of Science, ICT and Future Planning, “Internet of Things(IoT) Information Security Roadmap 3year Plan”, Deputy Director General of Information Security, pp. 3, 2015

[2] K. Ashton, “The Internet of Things”, RFID Journal. June. 2009.

[3] R. an Kranenburg, “The Internet of Things: A Critique of Ambient Technology and the All-Seeing Network of RFID”, Institute of Network Cultures. 2008.

[4] Matt Hatton, “The Global M2M Market in 2013”, Machina Research White Paper, Jan. 2013.

[5] Marco Annuziata, “Welcome to the age of the industrial internet”, TED, Dec. 2013.

[6] International Conference Internet of Things, “Workshop on Industrial Internet of Things”, Oct. 2014.

[7] KIET, “Safe network and Convergence Security in the Age of Internet of Things”, Apr. 2014.

[8] Proofpoint, "Proofpoint Uncovers Internet of Things (IoT) Cyberattack", Jan, 2014.

[9] Kaspersky daily, "Black Hat USA 2015: The full story of how that Jeep was hacked", Aug. 2015.

[10] symantec report, "The evolution of ransomware", Aug. 2015.

[11] IOActive blog, "Hacking Washington DC traffic control systems", Jul. 2014.

[12] World Economic Forum, “Industrial Internet of Things: Unleashing the Potential of Connected Products and Services”, Jan. 2015

[13] SGIP, “Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security”, Sep. 2010.

## 〈저 자 소 개〉


**장 현 수 (Hyun Soo Chang)**
학생회원

2014년 2월 : 아주대학교 정보컴퓨터공학부 졸업
2014년 3월~현재 : 아주대학교 컴퓨터공학과 석사
관심분야 : IoT 보안, 비정상행위탐지, ICT융합보안, 디지털 포렌식

**김 현 진 (Hyun Soo Chang)**
학생회원

2014년 8월 : 아주대학교 정보컴퓨터공학부 졸업
2014년 9월~현재 : 아주대학교 컴퓨터공학과 석사
관심분야 : 전력제어시스템 보안, 비정상행위탐지, ICT 융합보안

**손 태 식 (Taeshik Shon)**
종신회원

2000년 2월 : 아주대학교 정보 컴퓨터공학부 공학사
2002년 2월 : 아주대학교 정보 통신 전문대학원 공학석사
2005년 8월 : 고려대학교 정보보호학과 공학박사
2004년 2월~2005년 2월 : Research Scholar, University of Minnesota
2005년 8월~2011년 2월 : 삼전전자 통신/DMC 연구소 책임연구원
2011년 3월~현재 : 아주대학교 정보컴퓨터공학과 부교수
관심분야 : 산업제어시스템 보안, 비정상행위탐지, 디지털 포렌식