# M2M 기술 및 보안 동향

이 근 호*

◈ 목 차 ◈



## 1. 서 론

최근 IT분야 융합의 급격한 발전은 다양한 디바이스와 기계간의 연결을 통한 다양한 무선기술의 발달 등으로 유비쿼터스 환경으로 빠르게 진화가 이뤄지고 있다. 유비쿼터스 환경은 IT분야를 기반으로 한 융합분야의 발전과 함께 많은 새로운 분야의 연구가 이뤄지는 계기가 되었다. 그동안 특정 산업 분야에서 제한적으로 이용되던 M2M 통신 서비스가 이동통신 사업자들의 새로운 비즈니스 모델로 대두되고 있으며, 이동통신 사업자와 연구자들간의 주요 기술 연구분야로 대두되고 있다. M2M은 Machine to Machine, Mobile to Machine, 그리고 Machine to Mobile의 통신을 의미한다. M2M(Machine-to-Machine)은 사물지능통신으로 불리며 사람과 기기 또는 기기와 기기 간의 통신을 의미하고, 광의적으로는 통신과 IT 기술을 결합해 원격지의 사물, 시스템, 차량, 사람의 상태, 위치정보 등을 확인하고 제어할 수 있는 솔루션으로 기계들과 우리의 일상생활 속에 널리 퍼져있는 기기장비간의 네트워킹에 관한 개념이다. M2M 통신은 기기의 기구들을 컴퓨터의 본체에서부터 일상적인 전자제품들까지 연결해 사용이 가능하도록 해 줄 것이다. 예를 들면, 집안에서의 가전제품과 자동차등의 운송수단을 비롯한 사람이 거주하는 건물 등에서 사용된다. 이 개념은 기계들이나 기기들이 원격지에서 이동통신과 전송매체를 통해서 자신이 원하는 데이터를 전송하는 것이 가능하도록 하는 것이다. 현재의 M2M 통신 개념은 GSM망을 넘어 다양한 유무선 네트워크를 활용하는 개념으로 확장되어가고 있다. 이러한 개념은 기계들이나 기기들이 원격지에 통신망과 같은 이동 통신을 통해서 자신의 데이터를 전송하는 것이다. 사람과 사물 사이의 상호작용을 통해 위치, 건강, 온도 등 다양한 데이터를 얻을 수 있다. 정보통신과 자동화 프로세서를 위한 정보 기술의 결합으로 IT시스템과 같은 모든 기업의 유동 자산을 통합하여 부가가치를 창출하는 차세대 네트워크이다. 본 논문에서는 M2M에 대한 국내외 현황을 기반으로 관련 기술과 보안 요소에 대한 동향을 살펴보고자 한다.

## 2. M2M 국·내외의 현황

### 2.1 M2M 추진현황

최근 전 세계적으로 통신시장에서 M2M(machine to machine)에 대한 관심이 급증하고 있다. 국내에서도 정부 또한 M2M을 '사물통신'으로 명명하고 관련 산업의 활성화를 위한 인프라 구축과 법률 정비에 나서고 있다. 사물통신의 진가가 조금씩 세상에 알려지면서 미래의 블루오션으로 떠오르고 있으며, 현재 국내·외에서는 M2M 통신 기술 확보를 위한 많은 연구가 진행되고 있다. 특히 아래의 (표 1)와 같이 이동통

* 백석대학교 정보통신학부

(표 1) 전 세계 주요 이동통신사의 M2M 추진 현황

| 이통사 | 전담부서 | 제휴업체 | 중점 분야 |
|---|---|---|---|
| AT&T | – Emerging Mobility Group<br>– Emerging Device Group | – Jasper Wireless<br>– Numerex | – Smart Grid, Fleet Mgt.. |
| Verizon | – Qulacomm과 M2M 솔루션 제공 위한 JV, 'nPhase' 설립 | – Qualcomm | – 의료, 제조, 유통, 공익 사업, 컨슈머용 제품 |
| Sprint | – M2M 솔루션 전담부서 'Emerging Solutions' | – DataSmart<br>– MVNO, MVNE 모두 지원 | – Smart Grid, Fleet Mgt, Healthcare |
| Vodafone | – 모바일 헬스케어를 위한 사업 부문 신설 | – 영국 및 독일의 전문 사업자들과 제휴 | – 스마트그리드 |
| Telefornica | – M2M 별도 사업부 신설 | – Orange, 獨 DT와 M2M 관련 제휴 | – 일반적인 M2M 어플 (보안, 차량관리 시스템) |
| Orange | – 자체 M2M 사업 추진 | – Mobistar, Sierra Wireless | – 스마트그리드, 헬스케어 |

* 각사 발표 자료, ATLAS 재구성

신 사업자와 단말 제조업체간에 신규 Biz Model 발굴 협력을 통해 M2M 사업을 본격화 하고 있다.

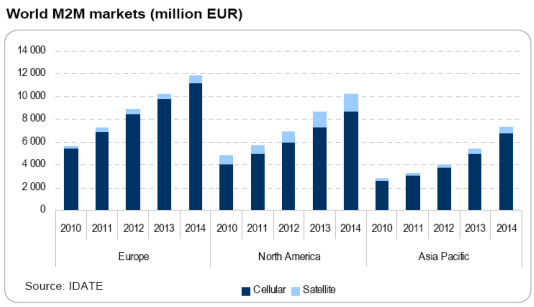
사물통신 장비도 2,500만개에서 1억 2,600만개까지 늘어날 것으로 예상되는 가운데 3GPP, WWRF, ITU-T, 802.16m 등 4G 차세대 네트워크에 대한 연구가 세계적으로 활발하게 진행되고 있으며, Device간에 융합(Convergence)에 따른 새로운 Biz Model 발굴이 이뤄지고 있다. 4G 네트워크에서는 융합에 따른 새로운 Biz Model로 차세대 네트워크 기반에서 machine to machine(M2M)으로 영역이 확장되고 있다. 특히 이동통신 사업자의 움직임이 활발하게 진행되고 있으며, 3GPP 표준내에서 machine 간의 통신을 촉진시키기 위한 MTC(machine Type Communication) 그룹을 만들어 활발하게 진행하고 있다. 또한 새로운 응용 서비스 중의 하나로써 기계장치들 간의 통신을 촉진시키기 위한 요구사항들을 정리하고 발전시키기 위해 S1 그룹 3GPP Meetings에서 TR(Technical Report) 22.868(Study on facilitating machine to machine communication in 3GPP system)에 대한 연구를 시작하여 지금까지 발전시켜 왔다.

MTC에 대상이 되는 장비로는 기존에 통신을 위한 목적으로 만들어진 휴대폰, 컴퓨터와 같은 통신 장비뿐 아니라 지금까지 독립된 장비였던 담배 자판기, 건강 진단 장비 그리고 차세대 전력 시스템으로 떠오르고 있는 스마트 그리드(Smart Grid)의 전력 검침 시스템 등이 있다. 사용자들은 MTC를 통해서 자신의 장비들을 모니터링하고 관리 할 수 있게 된다. 사용자들은 인터넷과 같은 통신을 통해서 자신의 장비들의 현재 상황을 모니터링하고 관리할 수 있으며, 필요에 따라서는 적절한 명령을 내려 직접 장비가 있는 곳으로 가지 않아도 효율적으로 작업을 할 수 있게 될 것이다. 이를 위해서는 외부에 사용자를 인증하고 사용자가 장비를 직접 관리하는 것과 동일한 수준의 서비스를 제공하여야 하는데 이를 위해서는 3GPP 내에 MTC을 위한 네트워크 서버가 존재하여 machine들을 관리 하도록 표준화가 진행 중이다[1,2,3].

## 2.2 M2M 시장의 현황

정부는 사물통신 시장이 2007년 15조 8,000억원에서 2013년 50조 7,000억원 규모로 약 3.2배 이상 성장할 것으로 전망했다. M2M 시장은 형성되지 얼마 되지 않은 초기 시장이다. 하지만 M2M의 많은 이점 때문에 연구기관들은 M2M시장의 성장률과 미래 성장 규모를 매우 낙관적이라고 발표하고 있다. M2MWorldNews에 따르면 전세계적으로 M2M 네트워크에 접속하는 연결 단말기 수가 2009년 5천만여대에서 매년 증가하여 2015년에는 30억여대에 근접할 것으로 추산하고 있다. (그림 1)에 의하면 M2M 접속 단말기 수의 빠른 증가는 곧 M2M 시장의 규모도 빠르게 성장한다는 것을 방증(傍證)하고 있으며 이와 관련된 전망수치들도 많이 나와 있다. 그 중 IDATE의 자료에 따르면 2010년 세계 M2M 시장규모가 140억EUR에서 2014년에는 300억EUR에 근접할 것이라고 예상하고 있다. IDATE에서

추정한 세계 M2M 시장 전망치를 보면 유럽, 북아메리카, 아시아태평양 지역만 수치를 내놓았는데, 이는 이동통신망 네트워크 구축이 잘되어있어 커버리지 범위가 넓은 지역만이 M2M 기술을 사용하는데 장애가 없기 때문이다. M2M 기술이 이동통신망을 이용하기 때문이다. 그렇기에 M2M 시장은 통신산업이 많이 활성화된 선진국들을 중심으로 성장하고 있다.




(그림 1) World M2M markets

## 2.3 M2M 시장의 환경 변화

M2M 시장은 작은 시장 규모와 단말기의 높은 가격 등으로 스마트 그리드, 헬스케어, 텔레메틱스 등 주로 기업용 시장에 집중되어 제한적으로 이용되어 왔던 분야가 현재는 많은 분야에서 응용하여 활용되고 있음을 표 2를 통해서 확인할 수 있다. 주요 이동통신사업자들은 직접 M2M 서비스 모델을 통해 직접 운영하는 대신 전문업체에 네트워크만을 임대하는 사업으로 운영하고 있다. 그러나 최근 근접통신 기술인 NFC, RFID, ZigBee 등 다양하고 저렴한 무선 통신 기술의 등장과 인터넷 접속이 가능한 커넥티드 관련 스마트기기 확산으로 비용이 하락하며 이동통신 시장의 새로운 부가가치 창출 사업으로 비즈니스 영역을 넓혀가고 있다. 음성매출 감소와 이동전화 보급률 포화에 따른 새로운 수익원 확보에 나선 이동통신 사업자들은 홈가전, 자판기, e-book 등 M2M 소비자 시장의 가능성이 확인되고 있다. 지금 많은 논의가 진행되고 있는 분야는 Telematics, Smart grids, Remote control and monitoring 등이 있다. 2008년 Smart grids 자료를 보면 이러한 응용분야 중에 Smart grids와 Telematics가 주를 이룸을 알 수 있다. Smart grids와 Telematics에 쓰이는 M2M 단말의 수요를 합하면 2008년 기준으로 약 47%를 차지하고 있다. 그 중에서 Telematics 분야는 29%를 차지하고 있으므로 이 부분에 많은 연구가 진행되고 있음을 알 수 있다. 또 Harbor Research에서 2013년까지의 수요예측을 한 자료에 의하면 2013년에 가장 많은 비중을 차지할 분야는 Building과 Transportation이다. 두 부분을 합치면 50%가 넘는다. M2M 단말의 응용분야로는 (표 2)와 같이 6개 정도의 큰 분류를 통해서 많은 응용 분야로 구분되고 Building과 Telematics를 가장 큰 시장으로 보고 있는 추세이다[1,2].

# 3. M2M 기술 동향

현재 다수의 국제 표준화 기구에서 M2M과 유사한 개념의 용어가 사용되고 있다. ETSI는 M2M을 키워드로 표준화 작업을 진행하고 있으며 “인간의 직접적인 개입이 꼭 필요하지 않은 둘 혹은 그 이상의 객체간에 일어나는 통신”으로 정의하고 있다. 3GPP의 경우 MTC라는 용어를 사용하고 “인간의 개입이 꼭 필요하지 않은 하나 혹은 그 이상의 객체가 관여하는 데이터 통신의 형태”로 정의하고 있다. 이에 반해 ITU-T의 경우 IoT와 MOC라는 용어를 사용하고 있으나 유사한 개념으로 적용하고 있다. IoT는 “모든 사물에까지 네트워크 연결을 제공하는 네트워크의 네트워크”로 MOC는 “인간의 직접적인 개입이 최소한으로 요구되거나, 혹은 요구되지 않는 둘 혹은 그 이상의 객체간의 통신” 으로 정의하고 있다. IEEE는 “가입자 장치와 기지국을 거쳐 코어-네트워크에 위치하는 서버간의 정보 교환 혹은 가입자 장치간 인간의 개입 없이 발생하는 정보 교환”으로 정의하고 있다. IoT의 경우 개념적인 특징이 강하고 M2M, MTC와 MOC는 동일한 정의와 인간의 개입이 필요하지 않다는 특징을 가지고 있다. ETSI의 M2M 구조에서 전송 네트워크는 3GPP, TISAPN 및 IETF 등에서 정의하고 있는 표준기술이 적용된다고 정의하고 있고, 3GPP의 MTC는 이러한 ETSI의 M2M 구조에서 전송 네트워크를 3GPP의 이동통신 네트워크로 한정하고 있다[1].

(표 2) M2M 응용서비스 분류

| 서비스 영역 | M2M 응용서비스 | 서비스 영역 | M2M 응용서비스 |
|---|---|---|---|
| Utilities/<br>Energy/<br>Metering | - Smart Meters<br>- Windmills, Solar fields<br>- Home Area Network<br>- Power<br>- Gas<br>- Water<br>- Heating<br>- Grid control<br>- Industrial metering | Tracking/<br>Tracing/<br>Telematics/<br>Transportation | - Fleet management<br>- Order management<br>- Pay as you drive<br>- Asset tracking<br>- Navigation, GPS<br>- Traffic management<br>- Road tolling<br>- Emergency Call<br>- Parking Meters<br>- Supply Chain |
| Remote<br>Maintenance/<br>Buildings | - Escalators<br>- HVAC<br>- Lighting<br>- Elevators<br>- Safety<br>- Fire systems<br>- Conveyor Systems<br>- Access Systems<br>- Smart Home | Security/<br>Payment | - Surveillance systems<br>- Backup for landline<br>- Control of physical access<br>- Car/driver security<br>- Point of sales<br>- Vending machines<br>- Gaming machines |
| Consumer<br>Electronics | - Home Automation<br>- Stereo/Hi Fi Audio<br>- Kitchen belnder<br>- Home Theater<br>- Digital camera<br>- DVD<br>- Home appliances:<br>dishwasher, refrigerator<br>- Devices<br>- Digital photo frame<br>- eBook | Healthcare | - Monitoring vital signs<br>- Supporting the aged<br>- Web access telemedicine points<br>- Remote diagnostics<br>- BAN/PAN<br>- MRI<br>- Implants<br>- Fitness equipment<br>- Clinic<br>- Diagnostics |

## 3.1 ETSI M2M 서비스 요구사항

ETSI TS 102 689는 M2M 서비스 요구사항을 정의하고 있는 표준규격으로, M2M 서비스의 일반적 요구사항, 관리, M2M 서비스를 위한 기능요구 사항, 보안, 네이밍 및 어드레싱 요구사항 등을 정의하고 있다. 다음은 M2M 서비스를 위한 일반적인 요구사항의 내용이다. M2M application communication principles, Message delivery for sleeping devices, Delivery modes, Message transmission scheduling, Message communication path selection, Communication with devices behind a M2M gateway, Communication failure notification, Abstraction of technologies heterogeneity, M2M trusted application, Confirm, Anonymity, Operator telco capabilities exposure, Scalability, Logging, M2M service capabilities discovery and registration, Mobility, Communications integrity, device/gateway integrity check, Continuous connectivity, Time stamp, Device/gateway failure robustness, Radio transmission activity indication and control, Location reporting support, Support of

multiple M2M application 등이 요구사항으로 표준에서 연구되어지고 있다[1].

### 3.2. 3GPP MTC 서비스 요구사항

3GPP MTC는 ETSI의 M2M 구조에서 전송 네트워크를 3GPP의 이동통신 네트워크로 한정하고 있으며 이를 위한 서비스 요구사항을 3GPP TS 22.368에서 정의하고 있다. 하나 혹은 그 이상의 MTC 서버와 MTC 디바이스 간의 통신과 MTC 디바이스 간의 통신은 서로 다른 operator domain 상에 존재하는 MTC 디바이스 간의 통신에서 볼 수 있듯이, 현재까지 3GPP는 단말 간 직접적인 통신은 지원하지 않고 있다. 단말 간의 통신도 통신망을 거치도록 되어 있으며 이러한 특징은 센서 노드 간 직접적인 통신을 지원하는 기존의 USN 혹은 센서 네트워크와 다른 점이기도 하다. 이와 같은 통신 형태에서 3GPP TS 22.368 는 MTC 서비스 요구사항을 공통 서비스 요구사항, MTC 응용과 관련된 부가 요구사항 등으로 나누어 정의한다. 다음은 MTC 응용별로 요구사항이 다를 수 있는 특징은 Low mobility, Time controlled, Time tolerant, PS only, Small data transmissions, Mobile originated only, Infrequent mobile terminated, MTC monitoring, Priority alarm, Secure connection, Location specific trigger, Network provided destination for uplink data, Infrequent transmission, Group based MTC features(Group based policing, Group based addressing)이다. MTC 응용의 종류에 관계없이 공통적으로 요구되는 서비스 요구사항은 General한 MTC 서비스에 대한 일반적인 요구사항으로 특정 ME/MTC 디바이스에서의 USIM 사용의 제한, 데이터 및 시그널링 메시지 양의 피크 제한 등을 정의하고 있으며, MTC device triggering, Addressing, Identifier, Charging requirements, Security requirements, Remote MTC device management 등이 있다[1].

## 4. M2M 기반 기술 분석

M2M 기반 기술 분석은 M2M 초창기 많은 연구가 진행이 되었던, Smart Grid, 지능형 자동차, 헬스케어의 3가지 분야를 기반으로 기술에 대한 분석을 하고자 한다.

### 4.1 지능형 자동차

지능형 자동차 분야 기술을 4개 분야인 차량 안전 운행, 교통 분야 공공 서비스, 교통 신호 확장, 차량 진단 분야로 나누어 볼 수 있다. 첫째, M2M을 응용한 차량 안전 운행을 위한 기술로는 다양한 시스템 기술을 통해 충돌 예방 관련 서비스를 제공할 수 있다. 교통신호, 차량 속도, 위치 및 기상 조건의 정보를 이용하여 교통 신호 위반의 위험 상황을 경고하거나, 도로 조건, 정지 신호등까지의 거리 정보를 이용하여 정지 신호의 위반을 경고 할 수 있다. 둘째, M2M을 응용하여 공공서비스를 제공할 수 있는데 사고시 구난 차량 또는 엠블런스 차량의 운행 시간 단축을 위하여 긴급 차량 접근 정보를 주변 차량에 전달할 수 있다. 셋째, M2M을 도로 시설과 차량에 응용하여 교통 신호 확장 서비스를 제공할 수 있다. 스쿨 존, 낙석 지역, 안개 지역, 동물 출몰 지역 등에서 도로 상황 정보를 운전자에게 전달할 수 있다. 넷째, 차량 진단 및 유지보수 관련 서비스를 제공하여 부품 교체, 각종 윤활유 등 교체 시기 차량 관리자에게 알려서 차량을 관리를 지원할 수 있다. 차량에서 수집된 위치와 속도 등의 정보를 이용한 작업 차량의 소재 파악, 택배 차량의 위치정보 등을 제공하거나, 위험물 차량의 운행 금지 구역을 감시할 수 있다. 지능형 자동차는 다양한 서비스 모델을 제시하고 있으며 이중에서 현재도 가능한 서비스도 있지만 아직 현실화 되지 않은 서비스도 많이 있다. 이를 위해서는 지능형 차량 서비스를 위한 인프라가 확충되어야 하는데 중요한 것은 이러한 서비스 시나리오는 자동차 제조업체뿐만 아니라 통신 사업자 및 포털 사업자에게도 많은 사업 기회가 줄 것으로 예상이 되고 있다. 그러나 이러한 서비스 활성화를 위한 기반기술 개발 및 법제도는 아직 활성화 되지 않아서 반드시 필요할 것이다. 기술 개발과 법제도가 활성화 되지 않을 경우 개인정보 및 프라이버시 침해, 차량/정보/통신메시지/트랙픽 정보 등으로 위변조 위협 등 많은 보안의 문제점이 발생하게 된다. 아직 전 세계적으로 이러한 보안의 문제에 대해서 초기 단계

에 머무르고 있고 몇몇 국가들은 국가적인 지원을 받아 연구에 박차를 가하고 있다. 지능형 자동차에서 차량 통신용 키 관리(폐기 및 갱신) 는 익명성을 위해서 반드시 해결해야하는 기술 분야이다[4].

### 4.2 Smart Grid

스마트 그리드 분야는 전력과 IT 기술을 융합하여 다양한 서비스를 가능하게 하는 AMI시스템은 물론이고 발전, 송전, 및 배전망의 전력계통 고도화 신재생 에너지의 활용, 전기자동차 등 에너지 및 환경 관련하여 이슈가 되고 있는 기술들 중 전기와 관련된 모든 것에 직간접적으로 관계를 맺고 있다. 컴퓨터나 통신 기술을 활용하여 현장에 직접 가지 않고도 원거리에 산재되어 있는 배전선로용 개폐기를 조작하고 고장구간을 자동 색출할 수 있는 전력설비 원격제어 시스템으로 정전구간 및 정전시간을 최소화시키는 효과를 보인다. 관련하여 전력 설비 자동화 시스템은 전력을 생산, 수송, 공급하는 대상설비에 따라 급전종합 자동화 설비(EMS), 원방감시제어설비(SCADA), 배전자동화 시스템(DAS)으로 계층구조를 형성한다. 급전종합자동화설비(EMS)는 발.변전소를 포함한 전 전력계통을 관장하는 컴퓨터 시스템으로 하위에 SCADA시스템으로부터 정보를 취득한다. 원방감시제어설비(SCADA)는 발전소를 제외한 송.변전설비를 관장하는 컴퓨터 시스템으로 관리처 단위로 설비를 운용한다. 배전자동화시스템(DAS)는 광범위하게 산재되어 있는 배전설비를 컴퓨터시스템을 이용하여 배전사령실에서 집중 원격감시와 제어를 통해 선로 고장구간 및 최적 계통전화 등 배전계통 운용업무를 현대화하는 설비이다. 스마트 그리드의 핵심 기술로는 AMI 기술 ,수요반응 기술 , 사용자 영역 네트워크 기술, 신재생 에너지 연계 기술 등으로 구성되며 이에 더불어 앞으로 안전하게 유지할 수 있는 보안 기술이 필요하게 된다[8].

### 4.3 U-Healthcare

유헬스케어는 다양한 기술들이 융합된 서비스 기술은 사용자의 생체 정보를 측정하고 모니터링하는 유헬스케어 측정기기(Instrument), 외부에서 생체인식 정보를 측정하는 이동식 측정기기(Movement Measuring Instrument), 기기 간 통신 및 데이터 송수신을 위한 유무선 네트워크를 위한 인터넷 공유기(Wireless AP)와 병원 내부의 서버(Hospital Server), 사용자의 생체정보를 분석하고 저장하는 병원데이터베이스(Hospital Database), 사용자의 생체정보를 진찰하여 진단하는 의료진, 헬스케어 제품이 필요하고 직접 사용하는 사용자 등으로 구성될 수 있다.

가정환경에서 사용하는 헬스케어 측정 기기와 이동식 측정기기를 이용하여 사용자의 혈압, 당뇨, 심전도 등 생체 정보를 측정하고 유무선 네트워크를 통해 건강정보를 병원 서버에 전송한다. 사용자의 신체정보는 병원서버를 통해 병원 데이터베이스로 저장 되고 병원 의료진들은 사용자의 생체 정보를 분석하고 진단을 내려 사용자에게 처방 해준다. 이 정보는 실시간으로 의료진과 사용자에게 전송되고 사용자의 상태가 좋지 않거나 상세한 검사를 요구할 경우 의료진은 사용자에게 연락하여 내원하여 치료를 받을 수 있도록 한다. 이러한 서비스를 통해 사용자는 자신의 건상상태를 실시간으로 알 수 있다. 이와 같이 유헬스케어는 개인의 생체 정보를 주로 다루고 있으므로 유무선 네트워크와 밀접한 관계가 있고 개인의 생체 정보는 매우 개인적인 정보이기 때문에 이러한 정보 전송 시 네트워크 보안과 사용자의 생체 정보가 해킹으로 인한 위·변조가 되지 않도록 하는 정보보안 기술이 필요하다[9].

## 5. M2M 보안 요소

M2M에서의 Device의 위협에는 기기간의 도청, 가로채기, 부인과 관련된 프라이버시 및 변조 위협요소가 있으며, Gateway에서는 불법 도용 및 접근을 통한 권한 위배, 물리적 침입, 재사용 공격, 중간자 공격의 위협요소가 존재한다. M2M 네트워크에서는 불법침투, 서비스 거부를 통한 마비, 바이러스, 웜, 트로이목마, 자원고갈 등의 보안 위협 요소가 있다. M2M에서는 잦은 네트워크의 변화와 무선채널의 위험에 따른 정보 수집의 어려움과 안정적인 관리와 효과적인 인증의 방법이 요구된다. M2M 은 기존 유.무선 통신보안의 특성을 이용하여 보안 위협요소로부터 안전한 정

보수집 등의 서비스를 제공해야 한다. M2M 통신 환경에서는 데이터 노출로 인한 위치, 개인정보, 과금 데이터 등의 민감한 정보를 전송을 하기 때문에 네트워크 어느 곳에서나 도청에 의해 수집되는 데이터 유출을 예방하기 위해 데이터의 기밀성을 보장해야 한다. 중간자(man-in-the-middle) 공격을 통한 데이터의 불법 변경 및 삭제, 위조된 데이터의 삽입 등에 대응하기 위한 무결성 보장이 필요하다. 서비스 거부공격(DoS)은 시스템의 가용성 및 생산성을 훼손함으로써 시스템 자원과 정보에 대한 접근 능력을 감소시킬 수 있다. 따라서 M2M 통신 환경에서도 주체 또는 디바이스들의 정보 접근 능력을 침해하지 않도록 시스템 가용성을 보장 할 수 있는 보안 메커니즘이 필요하다. 이동성을 제공을 위한 위치추적의 경우 M2M 디바이스는 디바이스의 위치정보 노출로 인해 디바이스 및 디바이스 소유자의 위치나 이동 경로가 노출될 가능성이 존재한다. 따라서 이동성을 제공하면서 추적 불가능성을 제공할 수 있는 보안 메커니즘이 필요하다 [5].

## 5.1 지능형 자동차 보안 요소

지능형 자동차는 융합분야 기술의 발전으로 인하여 홈네트워크, 텔레매틱스, 지능형 로봇 등이 접목되어 생활의 편리성을 제공하기 위한 다양한 형태의 서비스로 진화되고 있다. 지능형 자동차의 서비스 모델은 Car to Enterprise(C2E), Car to Car(C2C), Car to Home (C2H) 간의 다양한 모델을 제시하고 있다. 지능형 자동차 통신 환경은 차량간 통신과 차량과 RSU(Road Side Unit)과 같은 인프라 장비와의 통신 상태로 구분할 수 있다.

지능형 자동차 서비스에서의 주요 역기능으로 개인정보 및 프라이버시 침해, 차량정보, 차량간 통신 메시지, 통신트래픽 정보 등의 위변조 등의 위협 요소로부터 안전한 메시지 전송이 필요하다. 안전한 차량 서비스 및 통신을 위한 지능형 자동차의 보안 프레임워크에는 Secure Positioning, Vehicle-to-Infrastructure Secure Communication, Vehicle-to-Vehicle Secure Communication, User Access Control, VPKI(Vechicle PKI) 등을 포함하고 있다.

지능형 자동차에서의 보안 위협 요소로는 네트워크 측면에서 많은 위협이 발생할 수 있다. 거짓 정보를 발생시키는 공격 차량에 의해 일정 네트워크 영역안에 있는 다른 차량들에게 거짓 정보를 보내는 Forgery 위협과 일정 네트워크 영역안에서 다른 차량의 통신에 장애를 가하는 신호를 발생시키는 Jamming공격이 존재한다. 주행중에 메시지 또는 정보의 전달 과정에서 drop, corrupt, 또는 modify를 통한 정보의 위변조 공격하는 In-transit Traffic Tampering과 차량의 상태 정보를 변경하여 다른 차량으로 하여금 오인하도록 하는 공격하는 Impersonation 공격이 있다. 시간, 위치, 차량 ID, 이동 정보 등의 차량과 관련된 개인 프라이버시 정보에 대한 침해하는 Privacy Violation과 차량 내부의 정보인 속도, 위치, 차량 전장 부분의 상태, 각종 센싱 정보 등에 대한 위변조의 공격이 가능한 On-board Tampering이 위협요소이다[6,7].

## 5.2 U-Healthcare 보안 요소

정보보안 5대요소를 기초로 헬스케어 기반의 네트워크 보안 요소는 다음과 같다.

- 비밀성(Confidentiality)

쌍방향간 커뮤니케이션이 공인되지 않은 사용자에 의해서 누설되지 않는 것을 의미하는 용어로 스니핑 도구를 이용해 전송 패킷을 분석하거나 데이터를 가로채어 정보를 획득하고 사용자의 생체정보를 위·변조 하여 다른 정보를 전송하는 공격이 가능함으로 네트워크상에서 전송되는 모든 데이터는 기밀성이 보장되어야한다.

- 가용성(Availability)

전산 자원이나 데이터 접속이 필요한 사람이 필요한 시간에 사용 가능해야 함을 의미하고 Dos/DDos의 공격처럼 대량의 네트워크 트래픽을 발생시켜 네트워크 장애를 일으켜 정상적인 서비스를 제공하지 못하게 한다. Scanning 방지, 혼하지 않은 option 사용, 정상범위를 벗어난 폭주 패킷의 차단 기술을 이용한다.

- 무결성(Integrity)

자산이 인가된 당사자에 의해서, 인가된 방법으로만 변경 가능한 것으로 메시지 인증 코드(MAC)는 데이터의 무결성을 보장하기 위해 블록암호를 사용한다.

- 인증(Authentication)

여러 사람이 공유하고 있는 컴퓨터 시스템이나 통신망의 경우 이를 이용하려는 사람이나 응용프로그램의 신분을 확인하여 불법적인 사용자가 들어올 수 없도록 시스템 보안을 유지하는 방법을 제공해야 한다.

- 접근제어(access control)

시스템을 사용할 수 있는 자격을 가지고 있는 사용자만 시스템이나 자원에 접근 할 수 있도록 제어하는 기법이다.

유헬스케어 상황에서는 개인정보 보호는 매우 중요한 사항이다. 보안 5요소를 근거하여 보안위협에 대한 대응 방안은 비밀성에서는 SSH, SSL, IPSec 등을 좀 더 안전한 방법으로 사용하고 네트워크 상황에서는 RC4를 사용하여 데이터 완결성을 보장한다. 데이터 스트림에 포함된 체크섬을 방지하기 위한 방법으로 MD5, RC4 사용을 제안한다. 가용성 부분에서는 스니핑을 막기 위해 주파수 홉핑 방식을 이용하고 공개키 암호화 방식중 제로 날리지 패스워드(Zero Knowledge Password)를 사용하여 순간적인 키를 사용하고 인증이 끝나면 그 키는 바로 벼려지는 형식으로 사용함으로써 해커가 정보유출을 위해 사용자의 네트워크에 침입한다고 해도 원래의 메시지를 알아낼 수 없게 하여 사용자의 생체정보가 보호 될 수 있게 한다. 마지막으로 부인방지를 보장하기 위해 CA(인증기관)에 의해서 발행된 서명을 사용하여 네트워크상의 보안위협을 막아야 한다[9].

### 5.3 스마트그리드 보안 요소

스마트그리드는 폐쇄망을 이용하던 전력인프라에서 벗어나 사용자에게 전력 이용현황을 보여주기 위해 인터넷망 까지 연동해야 하기 때문에 사용자 개인정보가 쉽게 노출될 우려를 안고 있다. 특히 국가 전체 가구가 사용하게 될 스마트미터는 기기제어를 통해 가격신호 및 미터링 데이터 위조, 타인의 개인정보와 ID정보를 알아내 악용할 수 있고 나아가서는 스마트그리드 전체 네트워크에도 영향을 줄 수 있다. 이 때문에 외부공격에 의한 단전, 개인정보 유출, 전력사용 통제권 상실 등에 보안사고도 우려되는 상황이다. 스마트 미터의 보안 위험성을 말하자면, 프라이버시 및 데이터 보호관련 위험성, 커뮤니케이션 및 운영상의 위험성, 액세스 컨트롤 상의 위험성, 자산 관련 위험성, 물리적 환경 관련 위험성, HR 관련 위험성, IP 관련 위험성 등이 우려 된다. 센터와 스마트 박스간의 통신 프로토콜은 Web서비스와 같은 방법을 사용하여 http/XML 형식의 메시지를 사용 한다 센터와 스마트 박스간의 통신은 기존의 사용자가 사용하던 Web서비스를 사용하기 때문에 기존의 해킹 및 바이러스들에 대한 위험성이 나타날 수 있으며 이로 인해 전력을 관리하는 스마트 센터에 까지 영향을 미쳐 정전 및 전력 서비스 거부 공격 DDos 공격의 피해를 입을 수 있으며 전력을 사용하고 있는 소비자들에게 피해가 일어 날 수 있다[10].

## 6. 결 론

M2M 통신 서비스가 이동통신 사업자들의 새로운 비즈니스 모델로 대두되고 있으며, 이동통신 사업자와 연구자들간의 주요 기술 연구분야로 대두되고 있다. 사물통신망은 기계들이나 기기들이 원격지에 통신망과 같은 이동 통신을 통해서 자신의 데이터를 전송하는 것이다. 사람과 사물 사이의 상호작용을 통해 위치, 건강, 온도 등 다양한 데이터를 얻을 수 있다. 전기통신과 자동화 프로세서를 위한 정보 기술의 결합으로 IT시스템과 같은 모든 기업의 유동 자산을 통합하여 부가가치를 창출하는 차세대 네트워크이다. 본 논문에서는 M2M에 대한 시장 동향을 기반으로 관련 기술과 보안 위협요소에 대한 동향을 살펴보았다.

## 참 고 문 헌

[1] 유상근, 홍용근, 김형준, “스마트시대의 IT 정책 및 표준화 동향”, 전자통신동향분석 제 26권 제 28호,

pp.50~60, 2011년 4월
[2] 박성일, “사물지능통신 기술 및 서비스 전망”, TTA Journal Vol.134, pp.42~45, 2011, 3월
[3] STRABASE, “글로벌 이동통신사업자들의 M2M 서비스 추진 전략에 대한 사례 분석,” 2010.
[4] 오현서, 조한벽, 최혜옥, “차량통신기술동향,” 연구진흥원 주간기술동향포커스, 2007년 9월호.
[5] 이근호, “M2M(Machine to Machine)통신에서의 보안 위협 분석”, 한국산학기술학회 2010년도 춘계학술발표논문집, 제11권, 제1호, pp. 416-419, 2010년, 5월.
[6] 김기원, 김수균, 이근호, “M2M 환경에서 지능형 자동차 네트워크 기반의 보안 요구 사항”, 한국지식정보기술학회 논문지 제 5권, 제6호, pp. 124-129, 2010년, 12월.
[7] 최병철, 한승완, 정병호, 김정녀, “지능형 차량 보안 기술 동향”, 전자통신동향분석 제22권 제1호, pp.114-118], 2007년, 2월.
[8] 이일우, 한동원, “IT기반의 스마트 그리드 기술”, 한국정보기술학회지, 7(1), pp.25-30, 2009.
[9] 이소희, 이근호 “유헬스케어(U-Healthcare)서비스에서의 보안 위협” 한국융합학회 하계학술발표 논문집, 2011
[10] 디지털ITnet “국가 스마트그리드 보안 현황 과제”

## ◐ 저 자 소 개 ◑

**이 근 호(Keun-Ho Lee)**
2006년 8월 고려대학교 컴퓨터학과(이학박사)
2006년 9월~2010년 2월 삼성전자 DMC연구소 책임연구원
2010년 3월~현재 백석대학교 정보통신학부 조교수
2010년 9월~현재 백석대학교 쿰인성개발원 팀장
관심분야 : M2M 보안, 이동통신 보안, 융합 보안, 개인정보보호