# 디바이스 센싱 단계의 IoT 네트워크 보안 기술 프레임워크 구성

노시춘* · 김점구**

**요 약**

사물인터넷은 정보보안 위협에 노출되는 취약성을 광범위하게 가지고 있다. 그러나 이에 대처할 기본적 보안솔루션인 백신이 없고 데이터 전송에 암호화를 하지 않는다. 안전한 무선 센서 네트워크 환경의 구축을 위하여 노드 간에 전송되는 메시지를 암호화 및 인증이 요구된다. 센서 네트워크의 제약 조건 및 보안 요구사항을 만족시키기 위하여, 센서 환경에 적합한 경량 암호 및 인증기술, 경량 키 관리 기술이 요구된다. 센서 네트워크 보안기술의 필수항목은 프라이버시 보호 기술 부 채널 공격 방지, 기술이다. 안전한 무선 센서 네트워크 환경의 구축을 위하여 노드 간에 전송되는 메시지를 암호화하고 인증하는 것이 중요하다. 네트워크상에 존재하는 노드들을 안전하게 탐지할 수 있도록 lightweight 침입 탐지 메커니즘 기능을 적용해야 한다. 사람이 관여하지 않는 센서 노드는 단말의 진위파악 인증 기술, 체계가 필요하다. 사물인터넷환경에서 네트워크 보안 기술은 단말기와 센서 간 커뮤니케이션 채널의 안전성을 강화하는 기술이 중심이 되어야 한다.

# A Study of Phase Sensing Device IoT Network Security Technology Framework Configuration

SiChoon Noh* · Jeom goo Kim**

**Abstract**

Internet of Things has a wide range of vulnerabilities are exposed to information security threats. However, this does not deal with the basic solution, the vaccine does not secure encryption for the data transmission. The encryption and authentication message transmitted from one node to the construction of the secure wireless sensor networks is required. In order to satisfy the constraint, and security requirements of the sensor network, lightweight encryption and authentication technologies, the light key management technology for the sensor environment it is required. Mandatory sensor network security technology, privacy protection technology subchannel attack prevention, and technology. In order to establish a secure wireless sensor networks encrypt messages sent between the nodes and it is important to authenticate. Lightweight it shall apply the intrusion detection mechanism functions to securely detect the presence of the node on the network. From the sensor node is not involved will determine the authenticity of the terminal authentication technologies, there is a need for a system. Network security technology in an Internet environment objects is a technique for enhancing the security of communication channel between the devices and the sensor to be the center.

**keywords : Phase Sensing Device; IoT Network Security; Technology Framework; Configuration**

접수일(2015년 6월 2일), 게재확정일(2015년 6월 28일)

* 남서울대학교 컴퓨터학과
** 남서울대학교 컴퓨터학과

# 1. 서 론

사물(Things)은 상용 기기(Off-the-shelf gadgets), 간단한 도구(tools)로서 프로그래밍 기기(Programmable devices)이다. 사물인터넷 (IoT)은 센서네트워크 기기가 각종 센서에서 감지한 정보를 무선으로 수집 할 수 있도록 구성한 네트워크이다. IoT 서비스는 특정 상황이나 환경에 대한 센싱이 가능한 센서(Sensor Node)와 수집된 정보를 처리하는 프로세서, 데이터 송수신하는 장치(Sink Node) 등으로 구성된다. 물리적 구성요소와 기술 구성요소가 말단의 센서로부터 시작되어 사용자 서비스까지 seamless한 통신 및 정보 전달이 이루어진다. 사물인터넷으로 연결되는 사물 개수는 국내는 '12년 약 2,100만개 → '20년 약 4.4억개로 증가될 것으로 예상되고('12년:KT경제 경영연구소 /'20년: 한국정보 화진흥원), 세계적으로는 '13년 26억개 → '20년 260억개로 10배 이상 증가가 예측되고 있다 (Stracorp, 가트너, 2013). 산업측면에서는 사물인터넷은 2020년까지 전 세계 기업 총이 익을 21% 성장시키는 잠재력을 지닌 기술로, 향후 10년 간('13~'22) 19조불(공공 4.6조불, 민간 14.4조 불)의 경제효과 창출 추정(Cisco, 2013)된다. 사물인터넷 환경의  보안위협 확대에 대응하여 정보보안 필요성은 날로 증가되고 있다. 본 연구는 디바이스 센싱단계의 IoT 네트워크 보안기술 프레임워크를 제안한다. 센싱단계는 구성요소 연결부분에 다양한 보안 취약성이 존재한다. 센싱단계를 중심으로 사물 인터넷 환경에서 보안품질에 대한 중요성과 필요성을 공감하고 보안체계를 수립할 수 있도록 기술프레임워크가 필요하다. 연구순서는 서론, IoT 보안기술 환경, IoT시스템 구조와 기능, 센싱단계 보안 기술 프레임워크, 결론이다.

# 2. IoT 보안기술 환경

## 2.1 Pv6 기반 표준

IETF에서는 IoT 네트워크에 참여하는 사물들로 하여금 IPv6 기반으로 작동하도록 여러가지 표준을 제안해왔다. 우선 IEEE 802 .15.4 기반의 하드웨어와 같은 IoT 네트워크 하드웨어의 제약 조건을 극복하기 위해 IPv6 주소 체계와 IPv6 패킷 헤더(packet header)를 압축하는 6LoWPAN 기술을 RFC4944를 통해 2007 년에 표준화 하였다. RFC4944 이후, 저용량의 메모리로 IPv6 주소 체계를 활용할 수 있는 환경이 갖춰지자, IETF RoLL working group의 설립이 2007년 말에 제안되었다. 2008년 초 부터 IPv6 패킷을 활용하는 IoT 디바이스 간의 라우팅 문제를 해결하기 위한 연구를 시작하였다[2][3][5].

## 2.2 네트워크(Network) 기반기술

네트워크 기반기술은 유선망, 무선망, 이통망 등 다양한 기술이 적용될 전망이며, 사물 식별에 필요한 주소자원으로 IPv6 활용이 확산될 전망이다. 국내 IPv4 주소 수요 고려 시 '17년까지 약 3억 3천만개의 주소가 필요할 것으로 전망되나, 향후 2~3년 내 IPv4 주소는 고갈이 예상되고 모든 사물이 인터넷에 연결되는 과정에서 트래픽 급증이 예상된다. SW기반의 트래픽을 유연하게 처리하는 기술이 필요하다. SDN(Software Defined Network) Open API를 통해 네트워크의 트래픽 전달을 소프트웨어 기반의 컨트롤러에 의해 제어・관리하는 기술이 사용되며 통신비부담 없이 효과적으로 사물을 연결하기 위한 저전력(배터리 수명 10년 이상)/장거리(10Km 이상) 비면허 대역 통신 수요급증 전망된다. 5G 이동통신은 '20년 상용서비스가 개시되어, 기존 이동통신 시장을 점진적으로 대체할 전망이다.

## 2.3 암호·인증 기술 설계

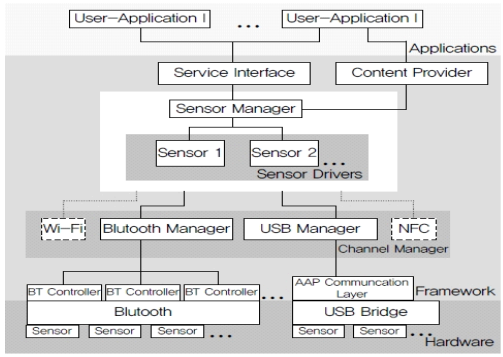
미국 NIST의 SHA-3 공모사업을 통해 암호 알고리즘 설계/분석 기술 수준이 급격하게 발전하고 있으며 RFID, 센서 네트워크 등의 실용화에 따라 경량 환경에 적합한 암호·인증 기술설계가 중점적으로 이루어지고 있다. 클라우드 확산 등  필요성이 높아진 암호화된 상태에 연산이 가능한 동형암호 연구가 활발히 진행되고 있다. 바이오정보, 특히 지문정보를 이용한 전자서명 키 생성 기법 등이 연구되고 있으며, 지문 외에도 망막, 홍채 등 다중 바이오 정보를 활용한 기술로 발전되고 있다. 바이오 정보를 이용하여 전자서명 기술에 대한 수요는 구체적으로 없으나, 향

후 증가할 것으로 전망된다. 국내의 경우 ARIA, SEED등 국내에서 자체 개발한 블록암호 알고리즘을 다양한 보안프로토콜에서 활용 할 수 있도록 NIST 에서 정의한 운용모드 기반으로 활용하는 방안을 마련하고 있다. VoIP 환경에서 안전한 통신을 위해 SRTP에서 ARIA, SEED 암호 알고리즘을 활용 할 수 있는 방법을 개발하고 있다(TTA. KO-12.0115 SRTP에서의 ARIA 암호 알고리즘 운용방법). 국제 표준 블록암호 대비 안전성과 효율성이 우수하며, 경량 ICT, 빅데이터 환경에 적합한 암호 알고리즘을 개발한다[1][2][5].

## 3. IoT시스템 구조와 기능

### 3.1 시스템 구성요소

사물범위는 고유 식별 가능 tools, devices이며 이들의 동작과정은 센싱 -네트워킹 -정보처리 - 지능적 관계 - 사물간 정보 교환이다. 각종 센서에서 감지한 정보를 무선으로 수집 할 수 있도록 구성한 네트워크를 말한다. 사물인터넷 을 실제 생활에 적용하기 위해서는 기반 기술들 을 통합적으로 구현해야 한다. 기반기술은 제어기, 통신칩과 같은 센서 및 네트워크 하드웨어 기술과 사물로 부터 받은 데이터를 저장, 분석 하는 미들웨어 소프트웨어 기술, 데이터를 의미 있는 결과물로 해석, 표현, 처리하는 재현 및 애플리케이션 소프트웨어 기술로 나눌 수 있다. 센서 및 네트워크 기술은 사물로부터 데이터를 인식하고 추출해낸 후 이를 인터넷으로 전송하는 가장 기본요소이다. 사물에 부착되는 센서는 사물의 종류, 애플리케이션의 종류에 따라 사물 인식 추적 RFID, 코드와 같은 태그 기술, 위치 추적 장치인 헨, 수평 감지 자이로스코프(Gyroscope), 속도감지가속도(Accelermometer) 등 다양하다. IoT 제품에 탑재되는 보안기술 에는 임베디드 OS, 센서 인증・암호화 등 IoT 보안기술 및 트래픽 폭증에 대비한 1GHz 폭 이상의 추가 주파수, 전력・장거리・비면허대역 통신 기술, 무제한 주소자원 IPv6 인프라가 있다 [4][7]




(그림1) ODK(Open Data Kit) sensor framework의 구조도, ETRI, 스마트 디바이스와 사물인터넷 (IoT) 융합기술 동향

### 3.2 시스템 동작과정

센서는 외부의 변화를 감지하는 입력장치로 시청각 정보는 물론 빛, 온도, 냄새 등 물리적, 화학적 에너지를 전기신호로 변환하여 준다. 센서는 수동형과 능동형으로 나누어지며, RFID는 무선으로 정보를 주고받을 수 있는 초소 형 태그로 바코드를 대체할 기술이다. 인식기술의 바탕위에 지능적 처리 기술이 적용 되는 것으로서 물리적 시간적, 신체적, 감정적 상황(또는 환경)과 그 상황속에 있는 개체를 대상으로 한다. 센서들 사이의 무선 또는 유선 네트워크를 구성하여 연결한다. 환경을 인지하고 판단하기 위한 센서와 프로세서 이다. 인간과 환경의 커뮤니케이션 기술이다. 네트워킹 전체과정은 센싱 정보측정 -> 디지털신호 변환 -> 근거리 무선전송 -> 클라우딩 호스트 로 전송 -> 분석센타 자동분석 -> 분석결과 회신으로 이루어진다[1][4].

#### 3.2.1 디바이스 센싱

IoT 구성요소는 감각에 해당하는 기능을 수행 하는 기술로 대상물의 상태를 파악하고 전기 신호로 전달한다. 센서종류는 온도, 가속도 , 위치 정보, 압력, 지문, 가스 등 다양하게 존재 한다. 스마트센서는 센서+통신+SW 등이 통합되어 센싱, 정보처리, 상황판단 등이 가능한 지능형 센서로서 스마트세서는 인터넷 연결을 기반으로 정보를 교환한다. 스마트 기기와 센서에 내장된 네트워크 인터페이스를 이용해 두 기

종 간 직접 통신을 가능하게 하는 방식이다. 통신방식으로 는 유선방식인 USB, 무선 방식인 블루투스, IEEE 802.15. 4(Zigbee), RFID(Radio Frequency Identification) / NFC(Near Field Communication), WiFi 등의 기술이 활용될 수 있다[5][6].

### 3.2.2 디바이스 고육식별 번호 인식

IoT 인증처리는 자동화된 장치로 상태정보를 추출하고 분석하여 정확하게 개체를 확인하는 기술이다. 넓은 뜻으로 생물 데이터를 측정, 분석하는 기술을 의미하나 정보 기술에서는 지문, 눈의 망막 및 홍채, 음성, 얼굴 표정, 손 측정 등 인증 목적으로 특성을 측정, 분석하는 기술이다. RFID는 무선 주파수를 이용한 인식 기술. 전파를 이용해 사물에 부착된 태그를 식별하여 정보/ID 및 주변 환경 정보를 수집해 저장-가공-추적해 측위- 원격 처리-관리 및 정보 교환을 가능하게 하는 기술이다. RFID에서 센서는 다양한 종류의 태그가 그 역할을 한다. 프로세서는 RFID 태그 안에 포함되는 칩을 의미한다. 원활한 커뮤니케이션을 위해서 RFID에 안테나를 부착하고 RFID 태그를 읽을 수 있는 리더기를 사용할 수 있다[7].

### 3.2.3 라우팅 처리

2009 년 8 월 새로운 라우팅 프로토콜인 RP L 라우팅 프로토콜의 설계가 시작되었고, 이는 RFC6550을 통해 2012년에 표준화 되었 다. RPL에서는 IoT 노드들로 하여금 게이트웨이 노드 혹은 루트 노드를 향한 Destination Oriented Directed Acyclic Graph(DODAG)을 형성하게 하여 many- to-one 네트워크를 우선 적으로 형성하게 하고, 이 DODAG의 connectivity 를 활용하여 루트 노드에서 각각의 노드를 접근할 수 있는 라우팅 방식을 두가지 제 안하였다. 그 첫번째 방식은 모든 IoT 노드들이 라우팅 테이블을 유지하여 hop-by-hop 라우팅을 하는 storing mode 방식이며, 두번째 방식은 게이트웨이 노드에서 패킷의 경로를 source routing header를 통해 패킷에 포함시켜 라우팅하는 방식이다[3][5].

### 3.2.4 무선랜(802.11b)전송

(1) 근거리 정보 송신

센서로 부터 추출된 데이터는 네트워크를 통 해 인터넷에 전달되는데 통신의 도달범위에 따라 구분된다. 근거리 정보를 송신하는 네트워크 기술은 지그비(Zigbee), NFC(Near Field Communication, 블루트스(Bluetooth) 등이 있으 며 원거리 인터넷 접속에는 무선랜(Wifi), 유선 랜(Ethernet)과 같은 LAN통신 네트워크, LTE, GSM과 같은 이동통신 기반 WAN(Wide Area Network)가 있다. PAN(Wireless Personal Area Network)은 단거리 무선접속을 위한 네트워크 기술로서 개인의 휴대단말, 센서의 무선 접속에 활용된다. 주요 표준기술로 블루투스(Bluetooth), 지그비(Zigbee), UWB (Ultra-Wideband) 등이 있다[6].

(2) WLAN(Wireless Local Area Network)

무선접속장치(AP)가 설치된 곳을 중심으로 일정거리 이내에서 담말기를 통해 초고속 인터넷을 이용한다. 이 구간에서는 일반적으로 2.4GHz ISM 대역의 무선랜(802.11b)을 사용한다. 전송거리는 300m outdoor, 30m indoor 정도이며 11Mbps 최대속도를 제공하는 DSSS 방식의 무선랜 표준을 사용한다. SSID(SSID는 무선랜을 통해 전송되는 패킷 헤더에 덧붙여지는 32바이트 길이 고유식 별자로서, 무선장치 들이 BSS(basicserviceset)에 접속할 때 마치 암호처럼 사한다. SSID는 하나의 무선랜을 다른 무선랜으로 부터 구분해 주므로, 특정 무선랜에 접속하려는 모든 AP나 무선장치들은 동일한 SSID를 사용한다. 원거리 통신인 경우는 장파, 중파, 단파가 사용된다. 통신 범위가 좁은 경우 는 초단파(VHF)대나 극초단파(UHF)대가 사용되며, 60MHz, 150MHz, 400MHz, 800MHz대가 주로 이용된다[8].

## 4. 센싱단계 보안기술 프레임워크

### 4.1 IoT보안 기술 체계

보안기술은 네트워크 보안에서 단말기와 센서 간 커뮤니케이션 채널의 안전성 강화 기술이 적용된다. 암호 알고리즘, 키관리 시스템을 위한 보안 프로토콜

이 필요하며 다수채널 생성 대용 량 데이터를 보호하여 사생활정보를 보호해야 한다. 네트워크 보안 기술은 단말기와 센서 간 커뮤니케이션 채널의 안전성 강화 기술이다. 사람이 관여하지 않는 센서 노드는 단말의 식별 번호 파악 인증 기술과 체계가 필요하다. 스마트 기기와 인터넷 환경의 변화로 트래픽 증가와 다양한 보안 위협 이 발생하므로 분석 데이터를 증가시킨다. 사생활 보호를 위해 암호 알고리즘, 키관리 시스템이 필요하며 보안 프로토콜이 필요하다. 모든 단말기는 OS, 웹브라우져 보안 응 이행하며 단말기 원격 접근제어와 사용하지 않을 때 비활성화 한다. 네트워크 디바이스에 어떤 연결이 되어 있는지 확인하며 키보드 없는 디바이스는 보안 인터넷 연결 장치인 모뎀 ·라우터를 보호한다. 이상과 같은 제반 보안 이행 사항을 정리하면 다음 표와 같다.

<표1> IoT보안 기술 체계

| 보안영역 | 대상분야 | 보안기술 항목 |
|---|---|---|
| 센서,싱크 노드 | 인간 비관여 IoT | 센서노드 고육번호 식별,인증 |
| | 인간 접근 IoT | 모든 디바이스 -> 비밀번호 나만 아는 비밀번호 |
| 무선게이트웨이 | 게이트웨이 디바이스 | 무선 스니핑 차단<br>데이터유출 통제 |
| 시스템(서버)보안 기술 | 서버시스템 | 해킹,악성코드 방어<br>OS, AP, 프로토콜,DB 보안,서버 보안패치, |
| 빅 데 이 타 보호 | 다수 채널 데이터서버 | 생성 대용량 데이터 암호 알고리즘, 암호 키관리 시스템 |
| 사용자 PC 디 바 이 스 보안 | 하드웨어, OS, 웹브라우저모니터 화면<br>키보드 없는 디바이스 | 모든 단말기의 원격제어<br>사용하지 않는 디바이스 비활성화,모든 디바이스 보안패치, 패치제조사 홈페이지 주기적 방문<br>화면, 키보드없는디바이스 보안 |
| 보안시스템 | 방화벽 | 네트워크 구성확인, 작동확인, 필터링규칙 확인 |
| 네트워크보안 | 라우터, 스위치, 허브장비 | 네트워크 구성확인,<br>인터넷 연결 장치 -> 모뎀·라우터 보호 |

## 4.2 센서 보안

센서 노드의 크기가 작아 전력 소모 및 컴퓨팅 능력, 메모 리 등에 제한이 가해지며, 무선을 통해 센싱된 값을 전달하는 특징을 가지므로 노드 포획, 도청, 서비스 거부 공격, 라우팅 경로 공격 등 다양한 공격에 노출될 수 있는 특징을 가진다. 이러한 센서 네트워크의 제약 조건 및 보안 요구사항을 만족시키기 위하여, 센서 환경에 적합한 경량 암호 및 인증 기술, 경량 키 관리 기술, 프라이버시 보호기술 부 채널 공격 방지, 기술 등을 포함하는 기술이 센서 네트워크 보안 기술이다. RFID는 무선 주파수를 이용한 인식 기술. 전파를 이용해 사물에 부착된 태그를 식별하여 정보/ID 및 주변 환경 정보를 수집해 저장 – 가공– 추적 해 측위 – 원격처리 – 관리 및 정보 교환을 가능하게하는 기술이다. RFID 환경에서 안전 하지 않는 Tag를 사용하는 경우 물리적 공격, 위조, Spoofing,도청, 트래픽 분석, DOS 공격 등에 의한 보안적 취약점에 노출되어진다.

## 4.3 AP 보안

AP 보호를 위한 첫 번째 사항은 물리적인 보안이다. AP는 전파가 건물 내에 한정되도록 전파 출력을 조정하고, 건물 안쪽의 중심부의 눈에 쉽게 띄지 않는 곳에 설치한다. 설치한 후에 AP의 기본 계정 패스워드는 반드시 재설정해 야 한다. SSID 브로드캐스팅 금지한다. AP를 탐색하면 나타나는 각 AP의 이름이 바로 SSID(Service Set Identifier)이다. 무선랜에서 가장 설정하기 쉬운 보안 사항은 이 SSID가 AP탐색에 쉽게 노출되지 않도록 SSID의 브로드캐스팅을 막는다.

## 4.4 무선 전송메시지 암호화

안전한 무선 센서 네트워크 환경 구축을 위하여 암호 알고리즘, 키관리 시스템은 보안 프로토콜이며 여러 채널 생성 대용량 데이터는 사생활 정보 보호기술이 필요하다. 센서 네트워크 환경에서 보안 요구사항을 만족시키기 위하여, 경량 암호 및 인증기술, 경량 키 관리 기술, 프라이버시 보호 기술, 부 채널 공격 방지, 기술 등이 센서 네트워크에 적용되어야 할 보안기술이다. 노드 간 전송 메시지를 암호화하고 인증하며 네트워크상에 존재하는 노드들을 안전하게 탐지할 수 있도록 lightweight 침입탐지 메커니즘 기능을 적용한다. 데이터 암호화를 강화하기 위해 TKIP(Temporal Key Integrity Protocol) 알고리즘을 사용한다. WEP와 달리 WPA는 단순한 패킷 수집을

통해서 크랙이 이루어지지 않지만, 최초 인증과정에서 인증 패킷이 노출될 경우 간단한 패스워드는 몇 시간~몇 일만에 크래킹 위험이 있다. EAP와 802.1x는 유선랜 환경에서 포트기반 인증 표준으로 사용되는 IEEE 802.1 x 표준과 함께, 다양한 인증 메카니즘을 수용할 수 있도록 IETF의 EAP 인증 프로토콜을 채택한 방식이다. 개인 무선 네트워크의 인증방식과 비교해 802.1x/EAP(Extensible Authentication Protocol)이 추가된 사항이며 사용자에 대한 인증을 수행한다. 동작과정은 다음 표와 같다.

<표2> EAP와 802.1x의 암호화 단계

| 동작 | 수행내용 |
|---|---|
| 접속 요청 | 클라이언트와 AP는 암호화 되지 않은 통신을 수행 |
| 인증 Challenge 전송 | RADIUS 서버는 클라이언트에 인증 Challenge를 전송 |
| Challenge 에 응답 | 전송받은 Challenge 값, 계정, 패스워드에 대한 해시 값을 구하여RADIUS 서버에게 전송 |
| 해시 값 비교 | RADIUS 서버는 사용자 관리 DB 정보에서 해당 계정 패스워드 확인 |
| 암호화 키 생성 | 해시 값이 일치하면 암호화 키를 생성 |
| 암호화 키 전달 | 전달받은 암호화 키를 이용 하여 암호화 통신을 수행 |

## 5. 결 론

센싱단계를 중심으로 사물 인터넷 환경에서 보안 품질에 대한 중요성과 필요성을 공감하고 보안체계를 수립할 수 있도록 기술프레임워크가 필요하다. 안전한 무선 센서 네트워크 환경의 구축을 위하여 노드 간 전송 메시지 암호화 및 인증이 요구된다. 암호 알고리즘, 키관리 시스템 은 보안 프로토콜이며 여러 채널 생성 대용량 데이터는 사생활 정보 보호기술이 필요하다. 이러한 보안 요구사항을 만족시키기 위하여, 센서 환경에 적합한 경량 암호 및 인증기술, 경량 키 관리 기술, 프라이버시 보호 기술 부 채널 공격 방지, 기술 등을 포함하는 기술이 센서 네트워크에 적용되어야 한다. 네트워크상에 존재하는 노드들을 안전하게 탐지할 수 있도록 lightweight 침입 탐지 메커니즘 기능을 적용한다. 사람이 관여하지 않는 센서 노드는 단말의 진위파악 인증 기술, 체계가 필요하다.

## 참고문헌

[1] KT M2M 사업추진 방향 http://plum.hufs.ac.kr/hsn2010/pdf/Session6-3.pdf

[2] SKT 사물통신 서비스 소개 http://blog.daum.net/nia-m2m/74

[3]M2M Activities in ETSI http://docbox.etsi.org/M2M/Open/Information/M2M_presentation.ppt

[4] Connected World Conference http://www.tiaonline.org/news_events/documents/CWPresentation_TR50_Chair_Numerex_CTO_Jeff_Smith.pdf

[5] Update of M2M Standard Work http://ftp.tiaonline.org/TR-50/TR-50_MAIN/Public/20100310_Denver_CO/TR50-20100310-005_Update%20of%20M2M%20Standard%20work%20v3%28Mitch%20Tseng%29.pdf

[6] Overview of M2M http://sites.google.com/site/hridayankit/M2M_overview_paper.pdf

[7] 이경화, 이주현, 박민수, 김재호, 신용태, An Enhanced Trust Center Based Authentication in Zigbee Networks, ISA, 2009.6

[8] 손영동, 김인정, 신용태, Information Security Policy to Cope with National, ISP-09, 2009.7

[9] 이경화, 이주현, 박민수, 김재호, 신용태, EECHE_An Energy-Efficient Cluster Head Election Algorithm in Sensor Networks, APNOMS, 2009.9

[10] 이협건, 이경화, 신용태, Implementation and Performance Analysis of AES-128 CBC algorithm in WSNs, ICACT, 2010.2

## [저 자 소 개]

**노 시 춘 (SiChoon Noh)**

1987년 : 고려대학교
경영정보학(석사)
2005년 : 경기대학교
정보보호기술(박사)
2002년 : KT 시스템보안부장
2004년 : KT 충청전산국장
2005년~현 재 : 남서울대학교
컴퓨터학과 교수,외래교수
2011년~현 재 : 남서울대학교
IT융합연구소 연구위원

email : nsc321@nsu.ac.kr

**김 점 구 (Jeom goo Kim)**

1990년 2월 광운대학교
전자계산학과 이학사
1997년 8월 광운대학교
전자계산학과 석사
2000년 8월 한남대학교
컴퓨터공학 박사
1999년 3월~ 현재 남서울대학교
컴퓨터학과 교수
IT융합연구소장

email : jgoo@nsu.ac.kr