공학석사 학위논문

사물통신 네트워크 보안 프레임워크에 관한 연구

2011년 2월

부경대학교 대학원

정 보 시 스 템 학 과

김 호 영

공학석사 학위논문

사물통신 네트워크 보안 프레임워크에 관한 연구

지도교수 이 경 현

이 논문을 공학석사 학위논문으로 제출함.

2011년 2월

부경대학교 대 학 원

정 보 시 스 템 학 과

김 호 영

김호영의 공학석사 학위논문을 제출함.

2011년 2월

주　　심　이학박사　박 만 곤 (인)

위　　원　공학박사　김 창 수 (인)

위　　원　이학박사　이 경 현 (인)

<차 례>

<표 차례>

<그림 차례>

A Study on Secure Framework for
Object to Object Network

Ho Young Kim

Interdisciplinary Program of Information System
The Graduate School
Pukyong National University

Abstract

A converged form of "Informationization" where people, devices and computers come together is currently taking place influenced by the rapid growth of broadcasting and telecommunication technologies in conjunction with digital convergence. Information gathering and utilization, previously limited to "Human vs. Human" relations, has evolved to "Human vs. Object" and "Object vs. Object" where information sharing between all 'Objects' is possible. Therefore, the "Object to Object Communication Network" based on ubiquitous computing technology is an essential technology is realizing a ubiquitos information service based Society.

"Object to Object Communication Network Technology" is provided on a wireless communication infrasturcture due to ease of installation and relocation of devices or where cost

effectiveness is achieved over wired infrastructure in rural or mountainous areas. For this reason, data is constantly exposed, prone to theft and easy to alter as well as being vulnerable to physical attacks being installed in the open. It is critical that a plan be established, from a communication infrastructure standpoint, to assure safe and secure “Object to Object Communication Network”. Device integrity, wireless data encryption, device reliability, routing security, data security, system utilization, privacy protection must be addressed and implemented on “Object to Object Communication Networks”.

The “Object to Object Communication Network” is a “Converged Service” based on many existing technologies. Individual technological components, excluding RFID and IPv6, are currently in the early phase of standardization. Also, some “Object to Object Communication” services are based on existing wired/wireless technologies.

In this thesis, we are presenting potential security threats that exist on current wired/wireless technologies. In doing so, we have suggested a “Security Framework for Object to Object Communications Network,” based on the IETF device connectivity standard network architecture, taking into consideration potential security threats, requests and request guarantees.

By applying security technologies to device integrity, wireless

data encryption, device reliability, routing security, data security and privacy protection we expect that a safe and reliable “Object to Object Communication Network” can be achieved.

Ⅰ. 서 론

1. 연구 배경

최근 방송통신관련 기술이 비약적으로 발전하고 디지털 컨버전스(Digital Convergence)화 되면서 사람, 기기(단말), 컴퓨터 등이 융합된 형태의 정보화가 진행되고 있다. 또한 정보의 수집과 활용이 종전의 인간 對 인간 관계에서 인간 對 사물, 사물 對 사물까지 진화되어 모든 객체간의 정보 공유가 가능해지고 있다[1]. 따라서 사물통신 네트워크는 유비쿼터스 컴퓨팅・네트워킹 기술에 기반하여 궁극적인 유비쿼터스 정보 서비스 사회를 만들기 위한 필수적인 기술이라 할 수 있다.

미국 타임지는 2008년 최고의 발명품으로 사물 인터넷(The Internet of things, 모든 사물・기기가 인터넷과 연결되는 새로운 개념의 미래 인터넷)을 채택하였고, 국내 언론에서도 현재 인터넷은 사용 주체인 사람을 중심으로 관리하지만 미래에는 센서가 달린 사물까지 관리하게 될 전망이며, 국내 언론에서는 이렇게 되면 2020년에는 1,000억 대가 넘는 기기가 인터넷으로 연결될 것으로 전망하고 있으며 사물통신 네트워크가 본격화될 2010년 이후에는 모든 사물이 네트워크로 연결되어 언제 어디서나 다양한 기기들을 통하여 정보를 이용하고 활용하는 시대가 될 것이다.

현재의 통신·인터넷·방송 등 개별 미디어의 융합이 IT2.0 이라면 인간과 모든 사물 및 환경을 연결하는 지능형 네트워크의 융합이 IT3.0 시대의 사물통신 네트워크이며 2012년까지 양방향·초광대역 융합망을 기반으로 인간과 정보단말기, 통신수단을 연결하지만 2012-2020년에는 사물통신 네트워크를 기반으로 인간, 자연물, 사물이 통신하면서 기존과 다른 형태의 지능

공간 서비스를 제공하게 될 것이다.

현재 인터넷에 연결된 각종 장치는 50억 개로 2013-2015년에는 그 수가 폭발적으로 증가할 것으로 전망된다[2]. 하지만 사물통신 기술은 디바이스의 설치 또는 이전의 용이성, 산간, 격오지 등 유선망 대비 비용효율성 측면에서 무선통신 인프라를 기본[3]으로 서비스되는 체계를 가지고 있어 데이터 노출, 데이터 도용과 통신 데이터에 대한 위변조가 용이하고, 외부 환경에 노출되어 물리적인 공격에 취약점을 가지고 있어 안전한 사물통신 서비스를 제공하기 위해서는 이러한 통신 인프라 관점에서의 보안 위협에 대한 대책이 필요하다[4,5].

2. 연구 범위 및 목표

사물통신을 위한 네트워킹 기술로 크게 유선(Fixed)네트워크, 무선(Wireless) 네트워크, 이동통신(Mobile) 네트워크 등을 들 수 있을 것이다.

그러나, 대부분의 사물통신은 모든 사물에 컴퓨팅 및 커뮤니케이션 기능을 부여하여 anytime, anywhere, anynetwork, anydevice, anyservice 통신이 가능한 환경을 구현하기 위해 무선 랜과 같은 무선 네트워크나 3G나 4G와 같은 이동통신기술과 같은 무선통신 인프라를 기반으로 정보를 관리하기 때문에 높은 보안위협을 가지고 있다. 또한 정형화된 네트워크 토폴로지를 가지고 있지 않기 때문에 데이터 노출, 데이터 도용과 통신 데이터에 대한 위변조가 용이하고 외부 환경에 노출되어 물리적인 공격 또는 손상이 가능하다[4,5].

따라서 본 논문에서는 안전한 사물통신 네트워크를 위해 고려해야 하는 보안 위협요소를 도출하고 보안 체계를 강화하기 위해 필요한 사물통신 네트워크 보안 프레임워크를 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 사물통신 네트워크의 개요 및 표준화 동향, 서비스 구축 현황을 소개하고, 3장에서는 사물통신 네트워크에서 가능한 보안 위협 요소를 분석한다. 4장에서는 3장의 보안 위협 요소를 고려하여 안전한 사물통신 네트워크를 위한 보안 프레임워크를 제안하며 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 관련 연구

1. 사물통신의 개요

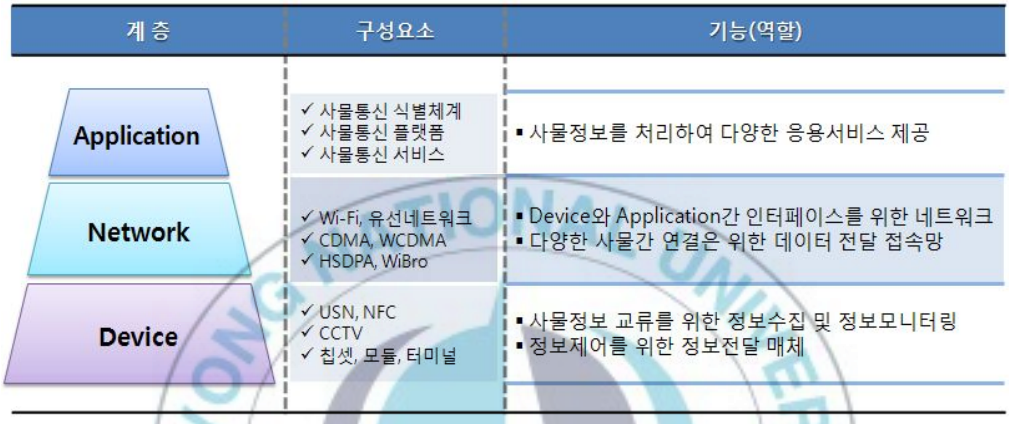
사물통신이란 주변의 사물이나 기기에 정보를 수집하고 통신을 가능하게 하는 장치를 설치한 후 이를 통하여 수집되거나 상호 공유되는 정보를 이용하여 사용자 혹은 사물 자체에게 정보를 제공한다.

협의의 의미로는 그림 1과 같이 사물간의 통신 및 사람이 작동하는 장치와 기계간의 통신으로 볼 수 있으며, 광의의 의미로는 광대역통합망(BcN), 차세대 인터넷 주소체계(IPv6) 등 사람 중심의 인터넷 인프라를 인간 대 사물, 사물 대 사물 간의 영역으로 확대·연계하여 이동통신(2G/3G)과 와이브로 기반기술을 활용함으로써 언제 어디서나 광범위한 확장성과 이동성을 통해 사물 간의 통신 및 원격지 사물의 상태정보를 안전하고 편리하게 감지, 전달할 수 있는 미래 방송통신융합 인프라를 뜻한다.

<그림 1> 사물통신 네트워크 개념도[6]

2. 사물통신 표준모델 계층별 구조

사물통신 표준모델의 계층, 구성요소, 기능(역할) 등 기본적인 규격은 그림 2와 같다.



<그림 2> 사물통신 표준모델 계층별 구조[6]

- Application 계층 구성요소

<표 1> Application계층 세부구성요소

사물통신 식별체계	- 사물 또는 센서의 효율적 관리 및 정보의 안전한 유통을 위한 사물 정보의 식별체계
사물통신 플랫폼	- 사물통신 네트워크 관련 사업 및 서비스의 기능을 지원하기 위해 필요한 프로세스
사물통신 서비스	- 센서망에서 전달된 정보 및 생활정보를 지능적으로 조합하여 원하는 정보 및 서비스 제공

- Network 계층 구성요소

<표 2> Network계층 세부구성요소

Wi-Fi	- IEEE 802.11 기반의 무선랜 연결과 장치 간 연결 구성 등을 지원하는 일련의 기술
유선 네트워크	- Ethernet 기반의 가장 광범위한 근거리 통신 기술
CDMA	- 코드 분할 다중 접속으로 코드를 이용하여 하나의 셀에 다중의 사용자가 접속할 수 있도록 하는 기술
WCDMA	- 광대역 부호 분할 다중 접속으로 확산대역 기술을 이용한 3세대 이동통신 표준 기술
HSDPA	- WCDMA 기반의 고속 데이터 패킷 기반의 데이터 서비스
WiBro	- 무선 인터넷 접속 규격의 하나로 무선 인터넷에 이동성을 보장하는 무선 광대역 인터넷 기술

- Device 계층 구성요소

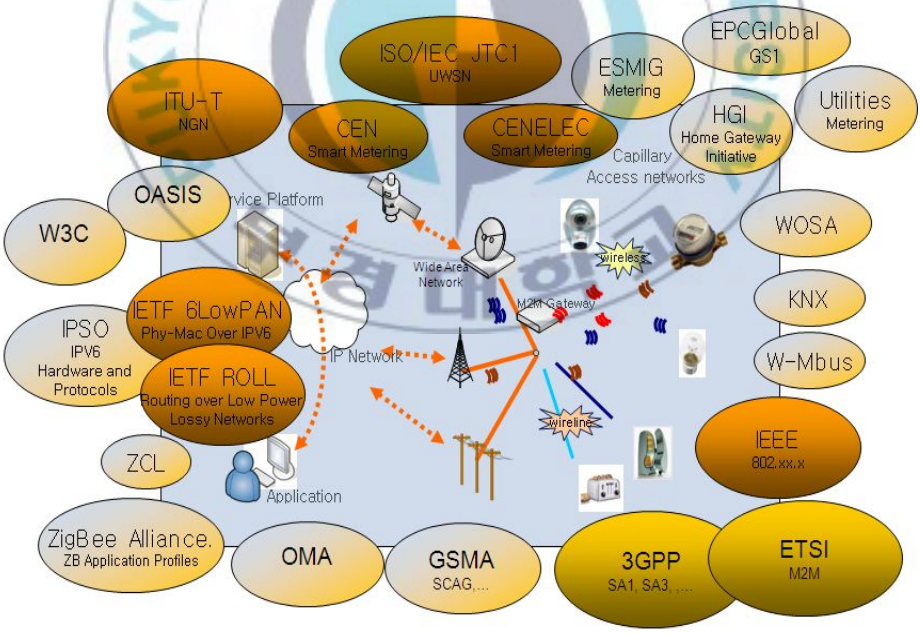
<표 3> Device계층 세부구성요소

USN	- 태그와 센서로부터 사물 및 환경 정보를 수집하고 상황인식 정보 및 지식 콘텐츠를 생성하는 기반 인프라
NFC	- 10cm 이내의 기기간 통신을 위한 초단거리 무선통신
CCTV	- 사물 및 환경 정보를 영상을 이용해서 수집할 수 있는 감시용카메라
칩셋/모듈 /터미널	- 정보 수집 및 제공을 위해 여러 통신에 적용, 호환 가능하게 하는 기기 또는 시스템

3. 사물통신 네트워크 표준화 동향

사물통신 네트워크 자체는 기존의 많은 기술들을 활용하여 서비스되는 융합 서비스(convergence service)의 개념으로 각 요소 기술별로 각각의 표준화 그룹에서 표준화 진행 중이며 RFID, IPv6 등을 제외하고는 대부분 시작 단계이거나 부분적으로만 개발이 진행된 상태이다[1,7].

외국에서는 그림 3과 같이 ETSI가 사물간 통신에 대한 표준화를 이미 수년전 시작하였고, 차세대 이동통신 분야에서는 3GPP의 MTC, 3GPP2의 SED, 그 외 IEEE 802.16m에서도 본격적으로 사물간 통신에 대한 표준화 작업이 시작하였으며 국내에서도 O2N포럼과 TTA에서도 표준화에 관한 내용을 연구 추진하고 있다.



<그림 3> 세계 표준화 단체[8]

가. 사물통신 네트워크 해외 표준화 활동

- ETSI (European Telecommunications Standards Institute)

ETSI에서는 기기간 통신에 대한 표준화를 위하여 2009년 1월 기기간 통신 기술 분과(Machine to Machine Communications Technical Committee)를 신설하였다. 특별히 기기간 통신 관련한 기술 및 표준들이 특정 응용 분야를 중심으로 난립하는 현황에서 ETSI 기기간 통신 기술 분과에서는 응용 분야에서부터 물리계층, 기기간 통신 서비스 제공자로부터 실제 사용자에 이르는 전 영역을 아우르는 표준을 제공할 것을 목적으로 현재 표준화를 진행 중에 있다[9].

<표 4> ETSI TC 표준화 문서

Service Requirement (Draft : ETSI TS 102 689 V0.5.1, Jan.2010)	서비스 요구사항
Functional Architecture (Draft : ETSI TS 102 690 V0.1.2, Jan.2010)	기능적인 구조
Smart Metering (Draft : ETSI TR 102 691 v0.3.2, Jan.2010)	자동검침의 적용사례 및 요구사항
e-Health (Draft : ETSI TR 102 732 V0.2.1, Sep.2009)	e-Health 응용을 위한 적용사례 및 요구사항
Connected Consumer (Draft : ETSI TR 102 857 V0.0.1, Dec.2009)	연결된 기기에 적용하기 위한 적용사례
City Automation (Draft : ETSI TR 102 897 V0.0.2, Jan.2010)	도시 자동화를 위한 적용사례 및 요구사항
Automotive Applications (Draft : ETSI TR 102 898 V0.1.0, Jan.2010)	차량 응용을 위한 적용사례 및 요구사항

- 3GPP (3rd Generation Partnership Project)

3GPP의 표준화는 이동통신 기반의 사물통신 네트워크 최적화를 기반으로 하고 있으며 2005년 9월 SA1에서 최초 Study(Facilitation Machine to Machine Communication in GSM and UMTS)를 시작하였다. 2007년부터는 SA1 그룹을 통해 이동통신 기반의 사물통신 서비스 실현 여부를 검토 하였고, SA2 그룹을 통하여 USIM 기반의 사물통신 서비스 초기등록 및 원격 제어기술이 표준화 되었다. 인간의 개입이 없는 통신의 Security가 이슈화됨에 따라 2007년 SA3에서 M2M 보안 기술 연구(Remote management of USIM application on M2M Equipment)를 시작하였다[10,11].

<표 5> 3GPP 표준화 문서

Study on facilitating Machine to Machine communication in 3GPP systems (TR 22.868 V8.0.0, Mar 2007)	효율적인 사물통신 네트워크를 위한 요구사항
Service requirements for machine-type communications(TR 22.368 V1.1.1)	MTC 네트워크에 관한 서비스 요구사항
System improvement for machine-type communications (TR 23.888 V0.1.2)	MTC의 시스템향상의 구조적인 면에 대한 연구 및 평가

- ITU-T (International Telecommunications Union - Telecommunication Standardization Sector)

ITU에서는 기기간 통신을 사물 인터넷(IoT: Internet of Things)라는 주제로 2005년 11월 보고서를 발간하여 사물 인터넷의 개념, 사물 인

터넷을 가능하게 하는 주요 기술, 시장, 과제(challenge) 등을 제시하였다. 기존의 RFID/USN을 확장하여 통신망 기술로 정의하는 작업을 위해 새로이 결성된 이 그룹은 기기간 통신을 위한 장치를 식별하기 위해 차세대 통신망 관점에서 FG IdM(Focus Group on Identity Management)을 구성하여 집중적인 연구를 수행하여 SG 17을 통해 보고서를 발간하였다[12]. 그리고 SG(Study Group) 12의 주도하에 차량 통신 분야를 집중연구 하였고, 2009년 11월까지의 2차 연구를 마치고 이어 3차 연구를 수행하고 있다. SG(Study Group) 13에서는 차세대 통신망에서 M2M과 관련된 센서 네트워크 지원을 위한 요구사항을 2010년 1월에 Y.2221 표준으로 승인 하였다[13].

- **IETF (Internet Engineering Task Force)**

인터넷 표준화 기관인 IETF에서는 2010년 3월 모든 종류의 센서 네트워크, 사물 통신망(Internet of Things)의 응용서비스에 목적을 둔 CoRE(Constrained RESTful Environments) Working Group을 신설하여 제한된 네트워크를 위한 통신 프로토콜 프레임 워크를 제공한다.[12] 이 그룹은 2010년 12월까지 CoAP(Constrained Application Protocol) 프로토콜을 제안표준으로 IESG(Internet Engineering Steering Group)에 제출하는 것을 목표로 하고 있으며 2011년 1월부터 제안된 부분에서 빠진 부분에 대한 추가적인 표준의 제정을 위한 WG(Working Group)의 새로운 결성을 목표로 하고 있다[14]. 또한 ROLL Working Group에서는 임베디드 시스템의 통신을 대상으로 저전력 라우팅에 대해, 6LoWPAN Working Group에서는 IEEE 802.15에서 IPv6를 이용한 데이터 전송 표준을 추진하고 있다.

- IEEE (Institute of Electrical and Electronics Engineers)

IEEE 802.16 Working Group에서는 2010년 말로 예상되는 802.16m (IMT-Advance 후보기술) 표준화 작업의 완료 이후 기술에 대한 검토 작업을 시작하고 있다. 여기에는 사람의 개입하지 않고 device와 device간 서로 정보를 주고받도록 하기 위한 M2M(Machine to Machine) 기술도 고려되고 있다. 대단히 많은 수의 Device접속 지원, 저가이면서도 전력소모를 최소화하는 기술 그리고 다양한 M2M망과의 공존기술 드에 대한 검토가 필요할 것으로 예상된다. 새로운 Project를 위한 PAR(Project Authorization Request)를 2010년에 제출하고 2012년 1분기까지 표준화 작업을 완료할 예정이다.

나. 사물통신 네트워크 국내 표준화 활동

- O2N (Object to Object Network) 포럼

우리나라에서는 사물지능 통신포럼을 2009년 11월에 설립하여 사물지능통신의 비전과 전략을 개발하여 사물지능 통신 사업을 발굴하고 이를 활성화할 수 있도록 지원하고 있으며 사물지능 통신을 구성하는 계층별 통신 구조 및 융합 서비스 시나리오 연구를 통하여 사물지능 통신 기술, 표준 제정 및 로드맵을 도출하는 역할을 맡고 있다. 사물지능 통신 기반구축 지원 및 사물지능 통신 확산 환경을 조성하는 것이 주된 이 포럼의 목적이며 2010년 현재 기술 분과, 서비스 분과, 표준 분과에 관한 내용을 연구 추진하고 있다[7].

- TTA (Telecommunications Technology Association)

현재 공식적으로 TTA 미래인터넷 PG(Project Group)내의 사물통신 표준화 실무반이 만들어 지지는 않았지만 2011년 표준화 로드맵 미래인터넷 분야를 도출하는 과정에서, 방송통신위원회 미래인터넷 PM실과 모바일 PM실과의 협의에 따라 사물통신 분야를 미래인터넷 로드맵에 함께 포함하여 기술하는 것으로 협의되어 미래인터넷 전략맵 전담반에서 표준화 작업을 진행하고 있다. 2010년 9월 3일에는 ETSI와 사물통신(M2M)이 포함된 기술분야 협력을 강화하는 내용의 MOU를 체결했다.

4. 사물통신 네트워크 구축 현황

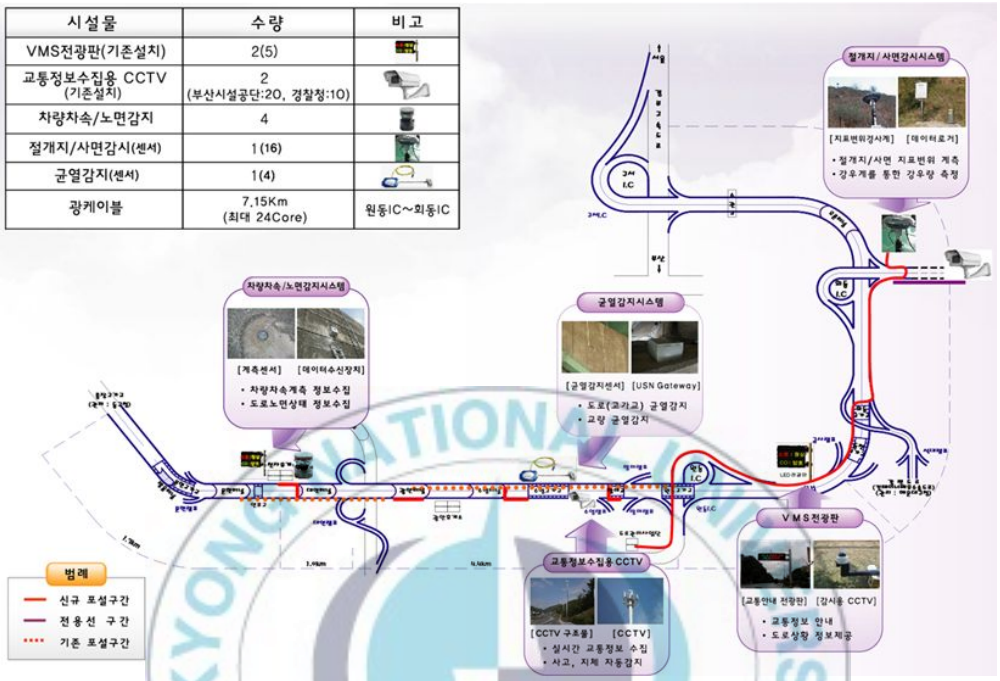
사물통신 네트워크는 인간의 생활공간 주변에 있는 모든 사물에 컴퓨팅·네트워킹 기능을 부여하여 환경과 상황의 자동 인지를 통해 사용자에 최적의 서비스를 제공함으로써 인간 생활의 편리성과 안정성을 고도화 한다. 따라서 이와 같은 기술을 응용한 사물통신 네트워크 서비스는 그림 4와 같이 생활 전반에 다양하게 적용될 수 있다.

<그림 4> 사물통신 응용 서비스 사례[6]

가. 사물통신 네트워크 서비스 현황

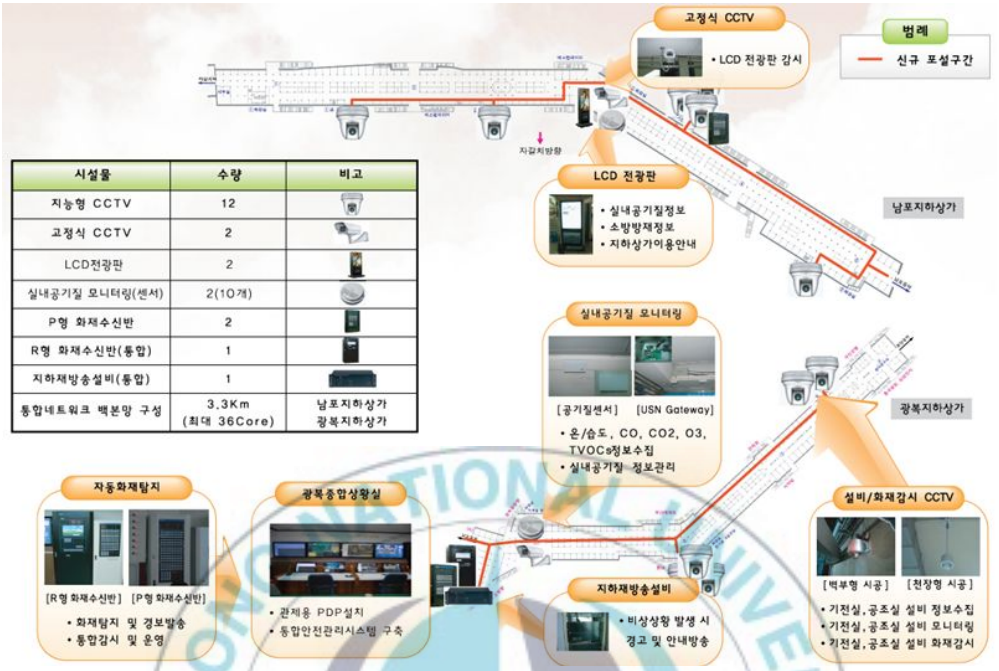
- **부산시 u-IT기반 도시시설물 안전서비스 모델**

2009년 행정안전부 “u-City 구축 기반조성사업”의 공모과제로 u-IT 기술을 도시시설물에 접목하여 시민생활의 안전과 편의를 위한 그림 5와 같이 u-IT 기반 도시시설물 안전 서비스 모델을 구축하였다. 도시고속도로에는 교통안내 제공을 위한 VMS전광판과 교통정보수집용 CCTV를 설치하였으며 또한 원동IC 방향 대연터널 입구 4개 차로에 차량차속 및 노면상태 감지 센서 설치, 회동IC 인근 절개지/사면 감시 센서와 감우량계 설치, 수영고가교 중심교각과 상판에 균열감지 센서를 설치하여 시설물에 대한 안전관리 서비스를 수행하고 있다.



<그림 5> u-도시고속도로 서비스

남포, 광복지하도 상가에는 그림 6과 같이 시설물 감시용 CCTV, 화재 감시용 CCTV 및 화재감지 센서를 설치하고, 지하도상가의 실내 공기를 실시간으로 측정하는 감지 센서를 설치하여 지하도상가에 대한 안전관리 서비스를 수행하고 있다.



시설물	수량	비고
지능형 CCTV	12	
고정식 CCTV	2	
LCD전광판	2	
실내공기질 모니터링(센서)	2(10개)	
P형 화재수신반	2	
R형 화재수신반(통합)	1	
지하재방송설비(통합)	1	
통합네트워크 백본망 구성	3.3Km (최대 36Core)	남포지하상가 광복지하상가

<그림 6> u-지하도상가 서비스

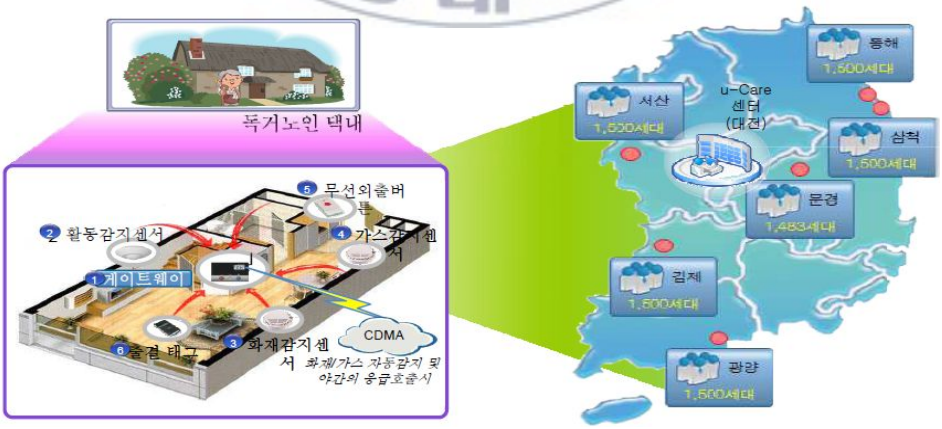
- **특정 범죄자 위치추적 시스템(전자발찌)**

CDMA M2M Platform을 활용하여, 그림 7과 같이 특정 범죄자의 재택여부 및 이동 동선을 실시간으로 모니터링하여 범죄 재발 상황을 신속히 파악 및 조치할 수 있도록 하는 시스템으로 감시대상자의 위치를 24시간 추적하는 시스템이다.

<그림 7> 범죄자 위치추적 서비스

- 독거노인 u-Care 시스템

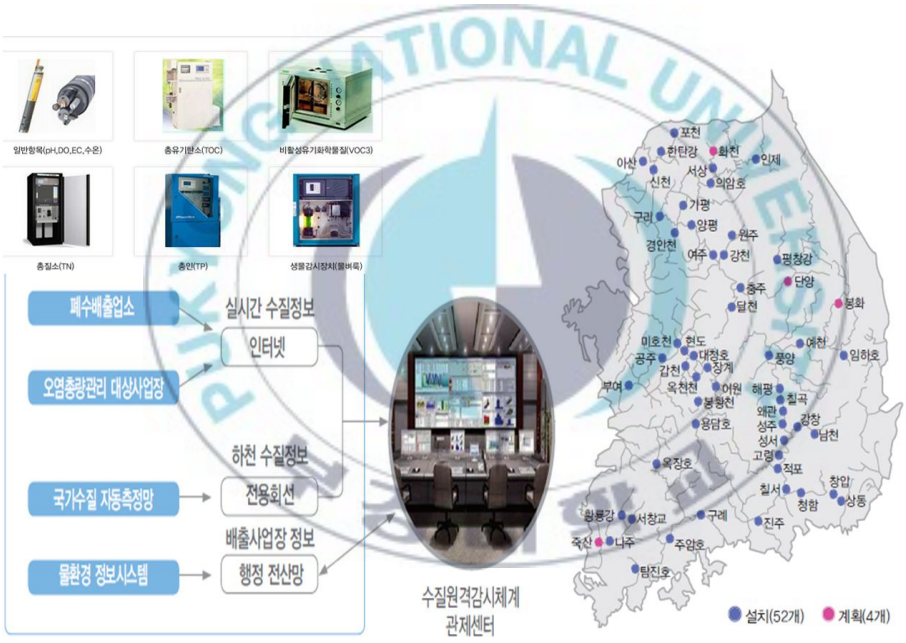
독거노인의 댁내 활동 및 안전사고를 원격에서 모니터링하여 CDMA 망을 통해 그림 8과 같이 실시간으로 확인할 수 있도록 하는 선진 고령자 복지서비스로 댁내 활동감지센서, 화재감시센서, 가스감지센서 등을 설치하여 가스, 화재, 활동, 외출에 관한 정보를 수집하는 서비스이다.



<그림 8> 독거노인 u-Care 서비스

- **4대강 수질자동측정망**

4대강 수계의 물관리 종합대책과 연계하여 그림 9와 같이 수질오염감시를 위한 수질감시 센서를 52개 지점에 설치하여 수온, pH, DO, 전기전도도, TOC, 생물독성, 휘발성유기화합물, 총질소 등 16개 항목에 대한 측정 데이터를 5분 간격으로 수집하여 과학적인 하천수질관리 서비스이다.



<그림 9> 4대강 수질자동측정 서비스

Ⅲ. 사물통신 네트워크의 보안 위협요소

사물통신 네트워크는 다양한 통신 기술 및 디바이스를 이용하여 언제 어디서나 사람, 사물, 다양한 콘텐츠 데이터를 전송한다. 이때 만일 데이터 전송 메커니즘이 보호받지 못한다면, 도청에 의해 정보가 누출되거나 위·변조에 의한 허위 정보가 유입될 수 있다. 이러한 침해를 방지하기 위해서는 데이터 통신을 암호화하여 보호하고, 보안 기능을 관리할 수 있는 매커니즘이 제공되어야 한다. 사물통신 네트워크에서 주로 이용되는 무선통신은 근본적인 특성으로 인해 일반적인 네트워크보다 보안에 취약하다는 특성을 가지게 된다. 사물통신 네트워크 디바이스의 성능 제약으로 인해 다양한 보안 기법을 적용하기 힘들 뿐만 아니라 디바이스가 설치된 물리적 환경이 공격에 그대로 노출되어 전송되는 정보가 쉽게 변경되거나 정당하지 않은 디바이스가 네트워크에 참여해 허위정보를 전송함으로써 전체 정보의 무결성을 쉽게 손상시킬 수 있다.

뿐만 아니라 악의적인 디바이스가 불필요한 정보를 계속 발생시켜 주변의 다른 디바이스들의 자원을 소모시킴으로써 네트워크의 수명을 단축시켜 정상적인 운영을 방해할 수 있다. 이처럼 간단한 공격만으로도 네트워크 전체를 쉽게 붕괴시킬 수 있으므로 보안침해로 인한 위험이 상상을 초월할 수도 있다. 따라서 다음과 같이 발생 가능한 대표적인 보안 위협 요소에 대한 보안 체계를 강화하여 보다 안전한 사물통신 네트워크를 구축하여야 한다.

[보안 위협 1] 물리적 템퍼링 공격

디바이스 하드웨어적 파괴 또는 분해를 통하여 해당 디바이스의 불법 개조 또는 보안정보를 추출하는 위협[15].

- 공격 방법: 물리적으로 디바이스를 탈취해 하드웨어적 파괴 또는 분해를 통해 디바이스 내부의 정보를 획득
- 예상 피해: 디바이스 손실 또는 정보 유출

[보안 위협 2] Rogue AP 공격

악의를 가진 공격자는 출력을 높일 수 있는 안테나를 설치하거나 높은 출력의 AP를 구성하여 사용자를 자신의 위장 네트워크로 자동접속토록 유도하여 무선네트워크 사용자를 공격하는 위협.

- 공격 방법: 주변에 존재하는 AP를 검색하고 검색된 무선 접속정보를 이용하여 가짜 AP를 설치하여 연결되도록 유도
- 예상 피해: 디바이스 통신이 두절되고 중요 정보를 갈취할 수 있으며 무선 장비에 접속하여 백본 네트워크까지 침입

[보안 위협 3] 라우팅 공격

가짜 라우팅 정보를 제공하고, 라우팅 프로토콜을 조작함으로서 수신된 라우팅 메시지를 스푸핑, 변경 또는 재전송하여 라우팅을 교란함으로써 라우팅 루프의 생성, 전송지연을 야기할 수 있는 위협.

- 공격 방법: 라우팅 프로토콜에 대한 다양한 취약점을 이용하여 라우팅 과정에 참여하여 공격
- 예상 피해: 라우팅에 대한 직접적인 공격으로 정상적인 서비스가 이루어지 않아 전체 또는 일부 네트워크 마비

[보안 위협 4] 스니핑(도청)

유·무선 네트워크의 트래픽 또는 신호(Signal) 메시지를 가로채서 정보를 엿듣거나 다른 공격을 위한 분석용으로 악용할 수 있는 위협.

- 공격 방법: 네트워크 취약점을 통해 스니핑 도구를 탐재한 컴퓨터를 이용하여 네트워크 구간에 침투하여 도청
- 예상 피해: 네트워크 구간에서의 전송되는 데이터에 대해서 전송 패킷을 분석하여 모든 정보가 노출

[보안 위협 5] 서비스 거부 공격

정보를 몰래 빼내가거나 그 외의 다른 보안 상실을 유발하지는 않지만 시스템의 CPU나 메모리, 통신 대역폭과 같은 자원을 고갈시켜 서비스 제공자가 사용자나 기관에 제공하는 서비스를 방해하거나 더 이상 받지 못하게 만드는 공격 위협.

- 공격 방법: 네트워크 취약점 또는 서비스 취약점을 통해 웜, 악성 코드, 바이러스를 유포하여 네트워크 또는 서비스 공격
- 예상 피해: 사물통신 네트워크 서비스 방해 또는 불가

[보안 위협 6] 개인정보 수집 및 도용

사용자가 사물통신 네트워크 서비스를 사용하는데 따른 개인 정보 보호와 프라이버시 침해에 대한 위협[1].

- 공격 방법: 스니핑 장비를 이용하여 사용자에게 전달되는 트래픽을 분석
- 예상 피해: 개인과 관련되는 기밀 정보의 유출

Ⅳ. 사물통신 네트워크 보안기술

본 장에서는 IETF(Internet Engineering Task Force)의 사물통신 네트워크 표준 아키텍처를 기준으로 각 Layer별 보안 위협요소에 대응하기 위해 그림 10과 같이 보안 요구사항 및 보장방안을 제안한다.

1. 사물통신 네트워크 보안 프레임워크

<그림 10> 사물통신 네트워크 보안 프레임워크[6]

그림 10에서 보듯이 PHY/MAC 계층은 물리적 템퍼링 공격위협에 대한 디바이스 무결성 및 무선구간에 대한 암호화, PHY/MAC 인터페이스를 위한 Adaptation 계층은 Rogue AP 공격, 라우팅 공격 위협에 대한 디바이스 신뢰성 및 라우팅 보안성, Network 및 Transport 계층은 데이터 위·변조 위협에 대한 데이터 기밀성, Application 계층은 서비스 거부공격, 개인정보 수집 및 도용 위협에 대한 서비스 가용성과 프라이버시 보호에 대한 보안 요구사항이 고려되어야 한다.

2. 사물통신 네트워크 보안기술 적용방안

사물통신 네트워크의 보안 요구사항을 보장하기 위한 보안기술은 다음과 같다.

- **디바이스 무결성**

사물통신 네트워크 디바이스는 옥외에 설치되어 외부 환경 정보를 센싱하여 이를 처리하는 목적으로 많이 사용되기 때문에, 쉽게 외부의 물적인 공격에 노출되기 때문에 물리적인 공격으로부터[16] 시스템 및 내부 데이터 보호를 위한 디바이스 무결성이 요구된다.

□ 보안기술 적용방안

- 물리적 방어구조물 설치 및 CCTV를 통한 감시시스템 적용
- 디바이스에 전자봉인 기술 적용
- SNMP를 이용한 디바이스 상태감지를 통해 네트워크 단절시 해당 디바이스 프로그램 Locking 기능 적용

- **무선구간 데이터 암호화**

사물통신 네트워크 디바이스의 통신 정보에 대한 기밀성이 제공되지 않을 경우 어떤 정보가 전송되는지 쉽게 획득할 수 있다. 디바이스의 정보 보호를 위한 디바이스 정보 암호화가 요구된다.

□ 보안기술 적용방안

- 링크계층에서 데이터 보안을 위해 IEEE 802.11i 표준 암호화 방식인 AES-CCMP(Advanced Encryption Standard-Counter Mode with CBC-MAC Protocl)를 통한 암호화 보안기법 적용[6]

• 라우팅 보안

사물통신 네트워크 디바이스와 장치간의 통신을 위해 경로설정을 하는 라우팅은 통신 경로에 대한 중요한 정보를 관리한다. 따라서 라우팅 프로토콜 공격을 통해 특정 네트워크에 도달하지 못하도록 전송방해, 네트워크 패킷의 도청 및 가로채기, 최적의 경로가 아닌 차선의 경로를 통한 전달, 허위 라우팅 정보 업데이트를 통해 라우팅 테이블 손상 등 데이터 전송을 중단시킬 수 있는 라우팅 공격으로부터 라우팅 참여 및 라우팅 테이블 보호를 위한 라우팅 보안이 필요하다.

□ 보안기술 적용방안

- 라우팅 프로토콜 자체의 인증을 사용하여 인증 절차를 통해서만 네트워킹에 참여하도록 라우팅 프로토콜 인증 적용
- 라우팅 프로토콜 인증 적용 시 인증키 자체에도 암호화를 적용하여 인증키에 대한 해킹을 방지
- 경로 설정을 위한 네트워크 설정 시 사용하는 IP 대역에 대한 정확한 네트워크 선언 및 미사용 IP 대역은 네트워크에 참여할 수 없도록 IP 대역 필터링을 적용

- **디바이스 신뢰성**

사물통신 네트워크가 접속되는 무선랜에 대한 공격을 목적으로 설치하는 AP를 Rogue AP(비인가 AP)라 한다. Rogue AP를 이용하여 사용자의 데이터를 수집하거나 변조하는 중간자 공격(Man in the middle attack)을 시도할 수 있다. 이런 Rogue AP에 대한 공격으로부터 무선랜을 통해 전송되는 데이터 보호를 위해 디바이스 신뢰성 보장이 필요하다.

□ 보안기술 적용방안

- RADIUS(Remote Authentication Dial-In User Service) 서버를 활용하여 EAP(Extensible Authentication Protocol) 기반의 인증 적용[17]
- 무선랜 서비스를 식별하기 위한 SSID(Service Set Identifier) 브로드캐스트하지 않도록 설정하고, 인가된 디바이스에 대해 수동 무선연결 방식을 적용
- 무선랜 관리시스템을 이용한 주기적인 Rogue AP 탐지

- **데이터 기밀성**

스니핑 도구를 이용해 전송 패킷 분석을 통해 네트워크 구간에서의 전송되는 데이터를 가로채어 정보를 획득하여 내부 정보를 유출하거나 메세지를 변조하여 불필요한 데이터를 전송하여 또 다른 공격 방법으로 사용될 수 있다. 이런 전송 패킷 분석은 모든 전송 데이터를 볼 수 있어 심각한 문제가 발생하기 때문에 네트워크 구간의 정보유출 보호

를 위해 데이터 기밀성 보장이 필요하다.

□ 보안기술 적용방안

- 전송되는 패킷에 대해서 암호화 통신을 통해 패킷을 도청할 수 없도록 적용[18]
- 암호화 통신을 사용하면 패킷 도청을 당해도 전송되는 데이터에 대한 정보를 알 수 없음
- 차세대 인터넷 주소체계인 IPv6를 사용하여 IPSec 구현 및 보안 확장자 헤더를 통해 안전한 데이터 전송을 통한 기밀성 보장

- **시스템 가용성**

서비스 거부 공격은 대량의 네트워크 트래픽을 발생시켜 네트워크의 폭주 및 심지어는 네트워크의 장애로 인하여 네트워크의 심각한 영향을 주어 정상적인 서비스를 제공하지 못하게 한다. 이러한 서비스 거부 공격은 서비스 자체를 못하게 하는 공격 형태로써 시스템에 치명적인 영향을 주기 때문에 시스템 가용성 보장이 필요하다.

□ 보안기술 적용방안

- 특정 서비스 또는 패턴을 가진 패킷이 단위시간 동안 일정량 이상 초과할 경우 그 이상의 패킷을 통과하지 않도록 Rate-Limit 적용
- 출발지 및 목적지 IP 주소, 서비스 포트 그리고 콘텐츠 기반의 패킷 필터링 적용
- BGP 라우팅 프로토콜을 활용하여 블랙홀 서버와 각 라우터간

iBGP를 설정하여 특정 목적지로 가는 트래픽을 차단하는 블랙홀 라우팅 적용[19]

- 출발지 IP 주소를 확인하여 해당 IP로 갈 수 있는 역경로(Reverse Path)가 존재하는지 확인함으로써 출발지 IP주소를 위장한 공격을 차단해 줄 수 있는 uRPF(unicast Reverse Path Forwarding) 적용

- **프라이버시 보호**

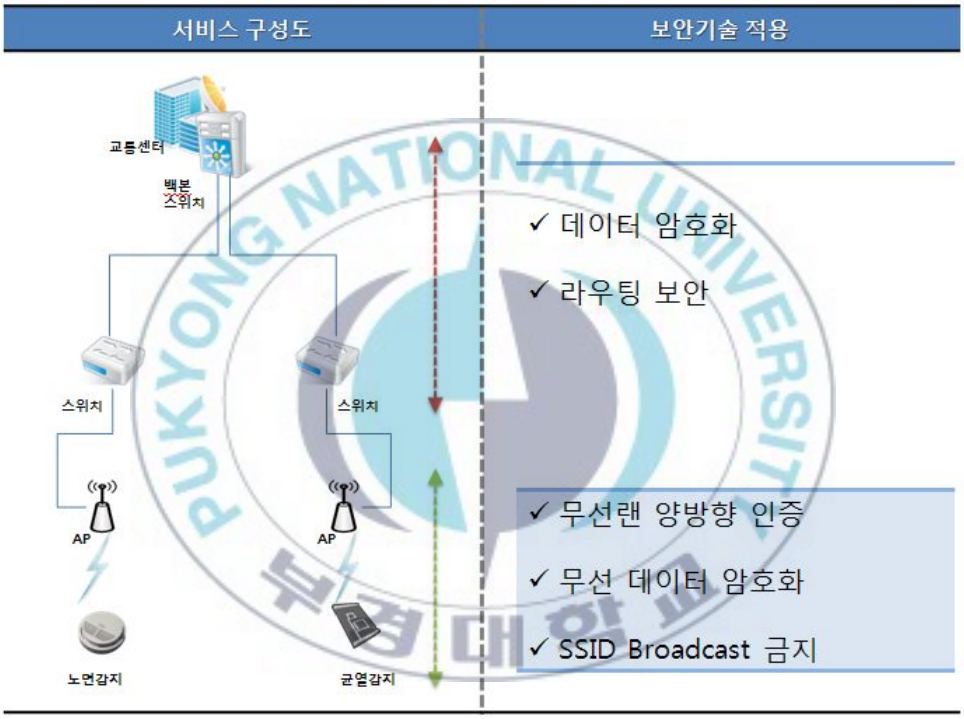
사물통신 네트워크 디바이스는 사람의 일상과 밀접하게 연관되어 지극히 개인적인 정보(이동, 취미, 선호도, 생리적 정보 등)를 추적할 수 있으므로[1] 사용자 데이터들이 불법적으로 노출되는 경우, 개인정보 유출 및 금전적 피해가 발생할 수 있으므로 이를 방지하기 위한 프라이버시 보호가 필요하다.

□ 보안기술 적용방안

- DB에 대한 접근 제어 및 개인 정보 저장 시 암호화 적용
- 디바이스에서 개인정보에 대한 요청 시 DB서버에 바로 요청하는 형태가 아니라 개인정보 요청에 대한 별도의 미들웨어를 구성

3. 사물통신 네트워크 보안기술 적용사례

제안한 사물통신 네트워크 보안 프레임워크를 그림 11과 같이 "u-도시고속도로 서비스"에 적용하여 안전한 사물통신 네트워크를 구축하였으며 적용 결과에 대한 세부 내용은 다음과 같다.

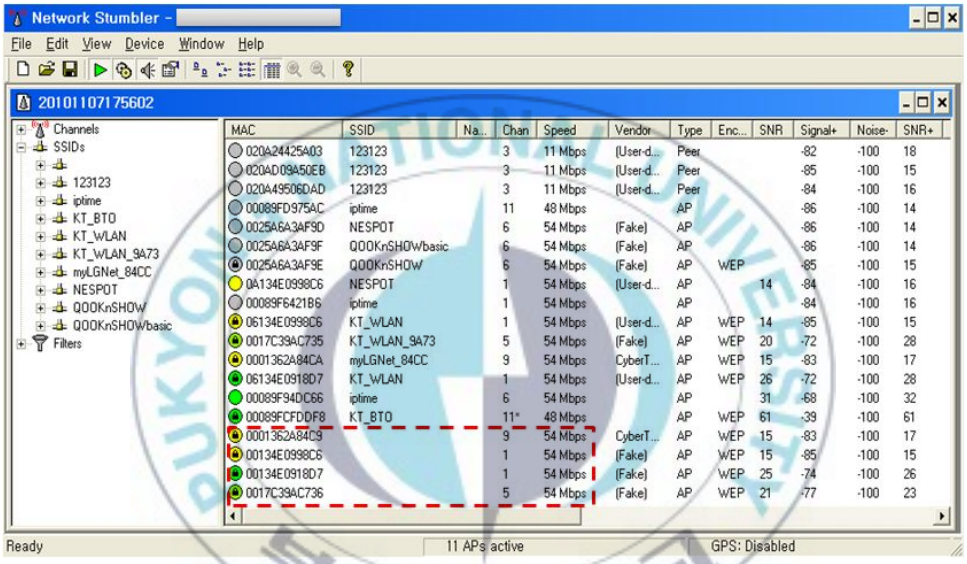


<그림 11> u-도시고속도로 서비스 보안기술 적용

- SSID Broadcast 금지

SSID(Service Set Identifier)는 무선 AP를 이용해 구성되는 무선 네트워크를 구별하는 식별자로서 다수의 무선 네트워크가 존재하는 경우, 무선 클라이언트가 접속할 네트워크를 구분하는 역할을 하게 된다. 대

부분의 무선 AP는 무선 클라이언트가 무선 네트워크의 존재를 인식할 수 있도록 SSID를 Broadcast 하도록 설정되어 있는 것이 일반적이다. 하지만, SSID 값의 Broadcast로 인해 공격자는 공격대상이 되는 무선 네트워크의 존재를 쉽게 인식할 수 있게 되므로 SSID Broadcast를 사용하지 않으면 그림 12와 같이 무선 Sacn을 해도 SSID를 확인할 수 없어 보안수준을 향상시킬 수 있다.

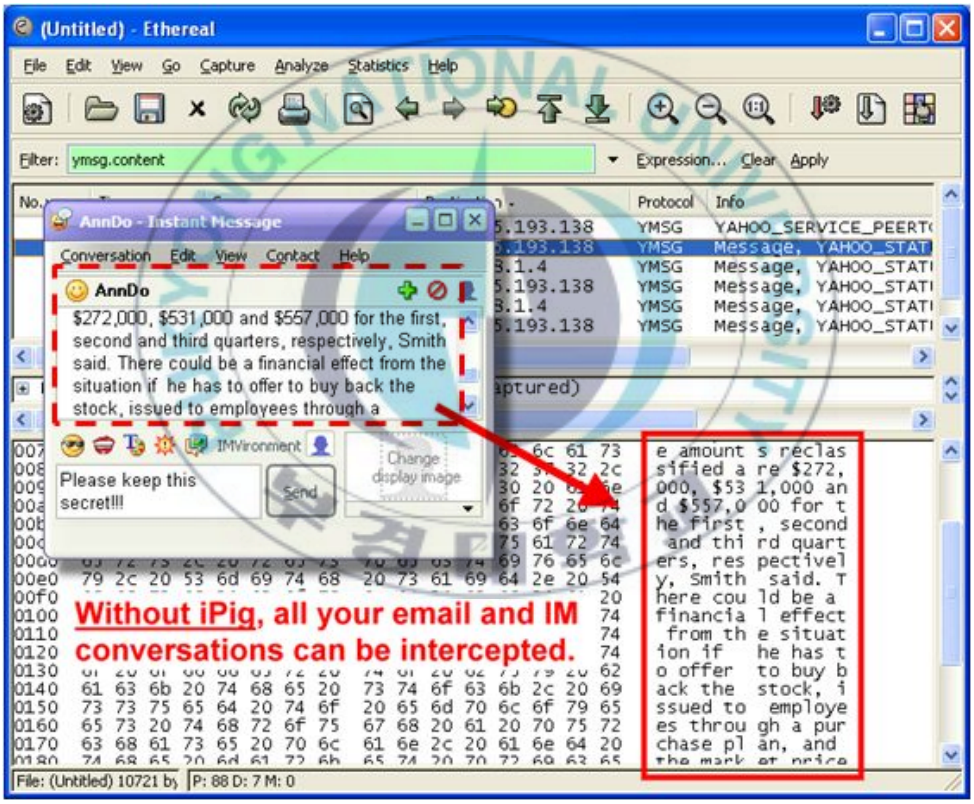


<그림 12> 무선랜 분석기를 통한 SSID Broadcast 확인

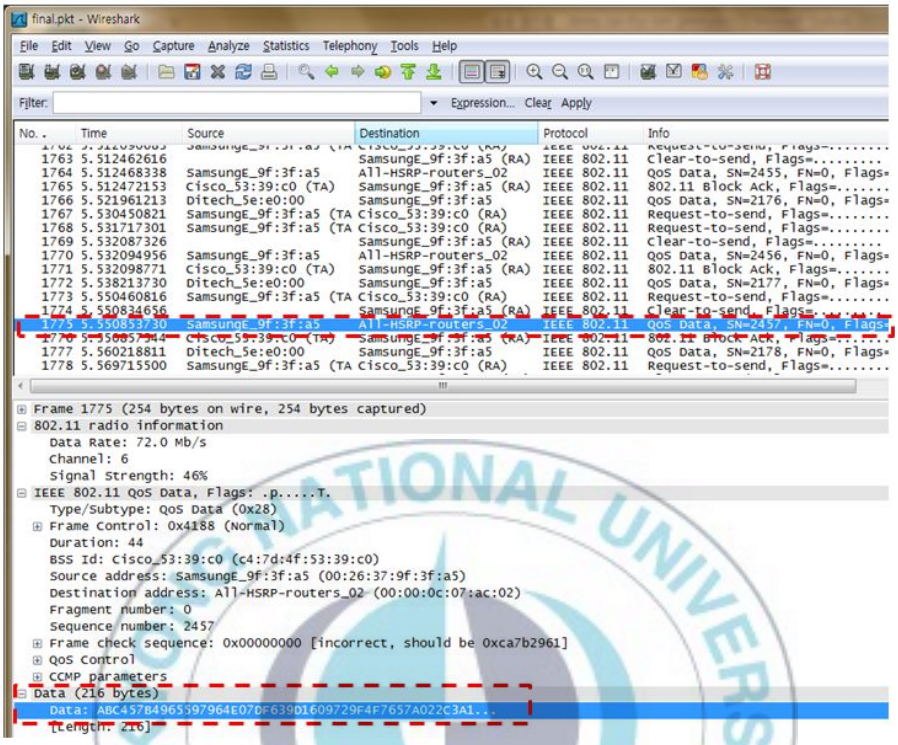
- **무선 데이터 암호화**

무선 데이터 보안은 일반적으로 무선 클라이언트와 무선 AP와의 구간에서의 보안성 유지를 위해 전송 데이터 암호화를 사용하는 것이다. 무선 전파를 이용하여 사용자 데이터를 전송하는 과정에서 무선랜 단말기나 무선랜 패킷 분석도구에 의해서 도청이나 감청이 되는 경우가

발생한다. 무선랜 서비스 영역 안에서 공격자가 정상 사용자와 AP 사이의 무선 패킷을 분석하는 것은 아주 쉽게 행하여 질 수 있어, 발생 빈도도 높게 나타나고 있다. 만일 무선 데이터가 암호화 되어있지 않은 경우 그림 13과 같이 모든 전송 데이터를 볼 수 있어 심각한 문제가 발생하게 된다. 이러한 도청과 감청으로부터 사용자 데이터를 보호하기 위해 그림 14와 같이 무선 전송데이터를 암호화함으로서 보안을 강화한다.



<그림 13> 무선 데이터 평문 전송

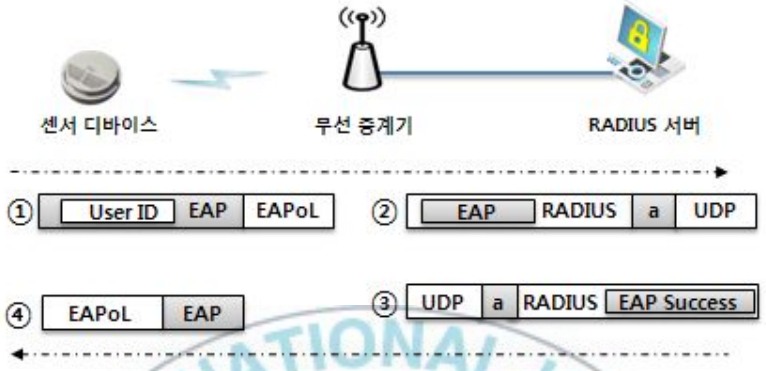


<그림 14> 무선 데이터 AES 암호화 적용

- RADIUS(Remote Authentication Dial-In User Service) 서버를 활용하여 EAP(Extensible Authentication Protocol) 기반의 인증

사물통신 네트워크에서 무선 디바이스 인증은 그림 15와 같이 RADIUS(Remote Authentication Dial-In User Service) 서버를 활용하여 EAP(Extensible Authentication Protocol) 기반의 양방향 인증을 통해 사물통신 네트워크에 참여할 수 있는 디바이스 정보를 별도로 관리하여 허가받은 디바이스에게만 무선랜의 사용을 허용하여 디바이스

의 신뢰성을 보장할 수 있다. 추가적으로 RADIUS 서버에 접근 제한을 통해 일반 무선 디바이스가 접속할 수 없도록 제한하여야 한다.



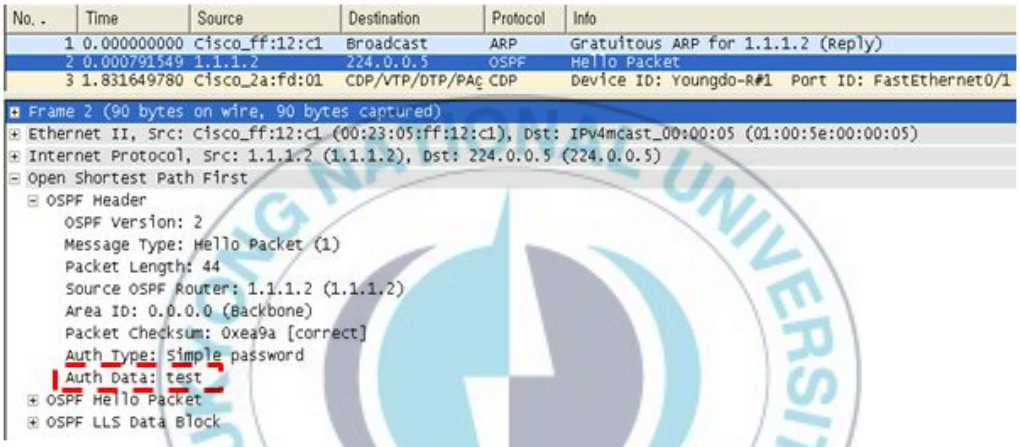
<그림 15> RADIUS 서버를 활용한 상호인증과정

1) 무선 디바이스는 사용자 계정을 포함한 EAP 메시지를 무선 AP로 송신 (무선구간)
2) 무선 AP는 수신된 EAP 패킷을 RADIUS 패킷으로 싸서 RADIUS 서버로 전달 (유선구간)
3) RADIUS 서버는 사용자 계정 DB와 비교하여 유효한 사용자인지를 판단 후, 결과를 정상 사용자의 경우, EAP Success 메시지가 내포된(Encapsulation)된 RADIUS Access-Accept 메시지를 무선 AP로 전달
4) 무선 AP는 해당 사용자의 무선 인터넷 접속을 허용, EAP Success 메시지를 EAPoL(Extensible Authentication Protocol Over LAN) 패킷에 내포하여 디바이스에게 전달

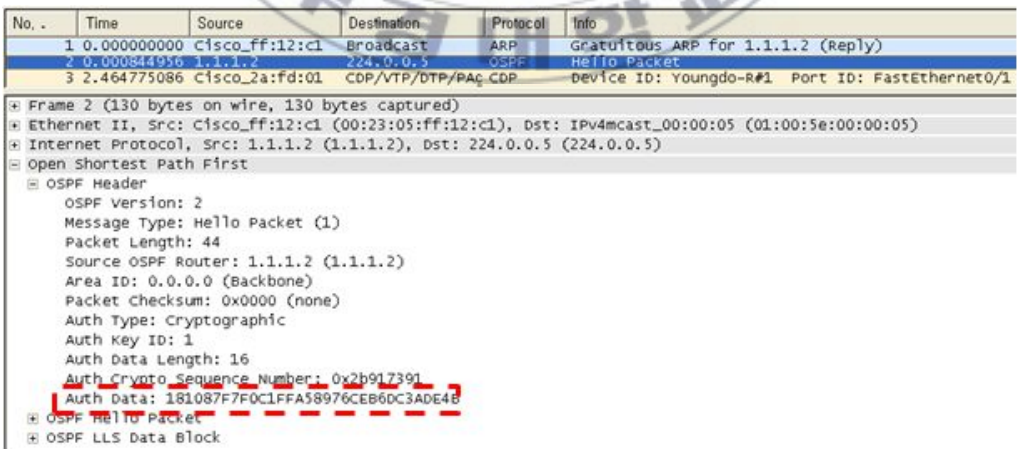
- **라우팅 보안**

통신 경로에 대한 중요한 정보를 관리하는 라우팅 설정 시 라우팅 연결을 위한 Authentication-key 설정을 통해 라우팅 참여 및 라우팅 테

이블 보호를 통해 라우팅 공격으로부터 보안성을 확보할 수 있으며 추가적으로 라우팅 Authentication-Key에 대해 암호화 적용을 통해 라우팅 보안성을 보장할 수 있다. Authentication-Key 설정 시 암호화를 적용하지 않으면 그림 16과 같이 스니핑 도구를 이용해 쉽게 Authentication-Key를 해킹할 수 있으며 그림 17은 암호화가 적용되어 Authentication-Key를 해킹할 수 없다.



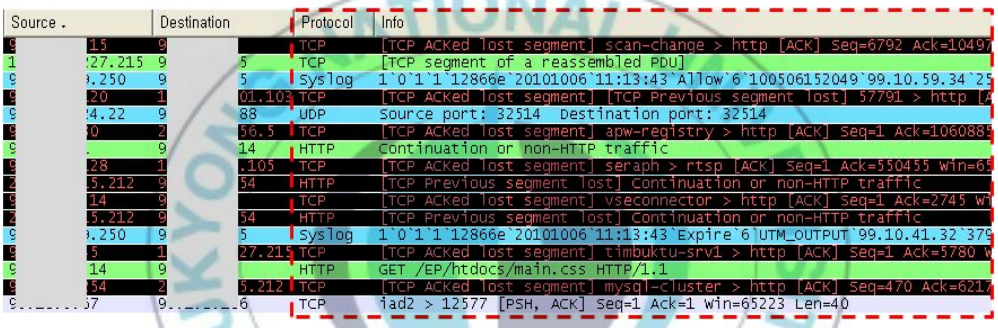
<그림 16> 라우팅 Authentication-Key 암호화 적용 전



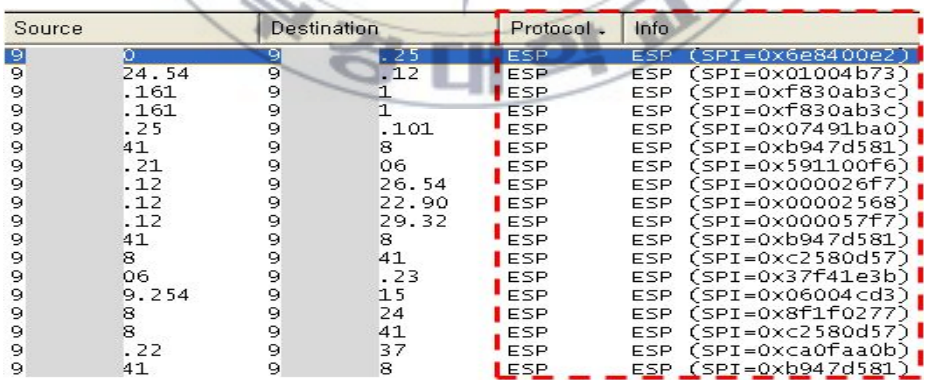
<그림 17> 라우팅 Authentication-Key 암호화 적용 후

- **데이터 암호화**

네트워크 구간에 스니핑 도구를 이용해 전송되는 패킷을 분석한 결과 그림 18과 같이 암호화 적용 전 전송 패킷은 정보를 그대로 볼 수 있으나 그림 19와 같이 암호화를 적용하면 ESP(Encapsulation Security Payload)에 암호화 되어 패킷 정보를 확인할 수 없다. 이와 같이 암호화 통신을 통해 데이터 기밀성을 보장할 수 있다.



<그림 18> 통신 데이터 IPSec 적용 전



<그림 19> 통신 데이터 IPSec 적용 후

Ⅴ. 결 론

사물통신 네트워크 자체는 기존의 많은 기술들을 활용하여 서비스되는 융합 서비스 개념(convergence service)[7]이며 현재 제공되는 일부 사물통신 서비스 자체도 기존의 유·무선 통신 기술을 기반으로 하고 있다. 또한 기술 표준화도 각 표준화 그룹에서 표준화 진행 중이며 대부분이 시작 단계이거나 부분적으로 개발이 진행된 상태이므로 미래에 어떤 기술이 개발되고 적용될지 예측하기 어렵다. 따라서 본 논문에서는 유·무선 보안기술을 중심으로 안전한 사물통신 네트워크 서비스를 제공하기 위해서는 고려되어야 하는 물리적 템퍼링 공격위협에 대한 디바이스 무결성 및 무선구간에 대한 암호화, Rogue AP 공격, 라우팅 공격위협에 대한 디바이스 신뢰성 및 라우팅 보안성, 데이터 위·변조 위협에 대한 데이터 기밀성, 서비스 거부공격, 개인정보 수집 및 도용에 대한 서비스 가용성과 프라이버시 보호에 대한 보안 위협요소 및 요구사항을 제시하였다.

제시한 보안 위협요소를 해결하기 위한 물리적 공격으로부터 시스템 및 내부 데이터 보호, 무선구간 무선 데이터 암호화, 라우팅 인증 및 암호화, 무선AP 양방향 인증, IPSec을 통한 암호화 통신, 서비스 거부 공격으로부터 네트워크 트래픽 제어, DB에 대한 접근제어 및 암호화 보안 기술적용 방안을 제안하였다. 이렇게 제안한 사물통신 네트워크 프레임워크는 4장의 보안기술 적용사례처럼 실제 사물통신 네트워크 서비스 구축에 사용하여 안정적인 사물통신 서비스 제공에 도움을 주고 있다.

결론적으로, 제안한 사물통신 네트워크 프레임워크는 안전하고 신뢰성 있는 사물통신 네트워크 구성에 중요한 역할을 할 수 있을 것으로 기대한다.

참 고 문 헌

[1] 김형준, “사물간 통신 네트워크의 이해”, 한국통신학회지, 제27권, 제7호, pp. 21-28, 2010.

[2] 오세근, “네트워크 NEW 패러다임, 사물통신 네트워크”, 주간기술동향, 통권, pp. 13-26, 2009.

[3] 김우용, “이동통신망 기반의 사물통신 서비스 현황 및 이슈”, 한국통신학회지, 제27권, 제7호, pp. 16-20, 2010.

[4] 은선기, 전서관, 안재영, 오수현 “안전한 M2M 통신 구축을 위한 상호 인증 및 키 교환 프로토콜”, 정보보호학회논문지, 제20권, 제1호, pp. 73-83, 2010.

[5] 서운석, 신순자, 구자동, 임진수 “유비쿼터스 컴퓨팅 환경에서 보안 및 인증서비스 방향연구”, 한국정보사회진흥원, 2004.

[6] 방송통신위원회, “사물지능통신 기반구축 기본계획”, 2010.

[7] 유상근, “IoT(Internet of Things) 추진현황 및 표준화 전략”, 한국전자통신연구원, 2010.

[8] David Boswarthick, “M2M Activities in ETSI, SCS Conference”, 2009.

[9] 심동희, “IT Standard Weekly, 기기간 통신(Machine to Machine Communication) 표준화 동향-유럽을 중심으로”, 한국정보통신기술협회, 2010.

[10] 박성일, “3GPPs M2M activities, 공공기관 사물지능통신 실무협의회 워크샵”, 방송통신위원회, 2010.

[11] 남동규, “사물지능통신(O2N)이 열어가는 미래사회, ICT FORUM KOREA 2010”, 한국전파진흥원, 2010.

[12] 김상언, “M2M 해외 기술동향 및 해외사업자 사례”, KT경제경영연구소, 2010.

[13] ITU-T Rec. Y.2221, "Requirements for support of Ubiquitous Sensor Network(USN) applications and services in NGN environment", Jan. 2010

[14] 송성학, “CoAP(Constrained Application Protocol)표준화 동향, IT Standard Weekly”, 한국정보통신기술협회, 2010.

[15] 한국정보화진흥원, “사물통신(IP-USN) 보안/신뢰성 확보 방안 마련에 관한 연구”, 2009.

[16] 김호원, 이석준, 오경희 “센서네트워크 보안 기술 개발 동향”, 정보보호학회지, 제18권, 2호, pp. 33-39, 2008

[17] 방송통신위원회, 한국인터넷진흥원 “무선랜 보안 안내서”, 2010.

[18] ETSI TS 102 689, “Machine-to-Manchine communications;M2M service requirements", 2010.

[19] 구자현, “서비스 거부 공격(Denial of Service)의 유형 및 대응”, 정보통신연구진흥원, 2008.

감사의 글

대학 졸업 후 10년 만에 대학원을 진학해서 열심히 공부는 했으나 부족한 점이 많았습니다. 이제 비로소 모든 과정을 마치고 논문의 마지막 마무리를 글로 남기려 합니다. 저를 도와주신 모든 분에게 일일이 찾아뵙고 감사드리지 못하는 점 용서를 구합니다.

직장생활과 학업을 병행해서 진행하다보니 부족한 점이 많았지만 많은 도움과 격려를 주신 지도교수 이경현 교수님의 은혜에 고개 숙여 깊이 감사드립니다. 바쁘신 가운데 초라한 논문을 맡아서 열과 성으로 심사해 주신 박만곤 교수님, 김창수 교수님 감사합니다.

저를 대신해 자질구레한 일들을 처리해 준 연구실 영신, 인제, 창현이 고맙고, 졸업 후에도 좋은 직장에 취직해서 앞으로 잘 해나길 바란다.

등록금도 주시고 공부하는 동안 아이들을 잘 키워주신 장모님, 장인어른께는 죄송하다는 말씀과 감사하다는 말씀을 동시에 드립니다.

끝으로 공부한다고 주말에 같이 놀아주지 못한 민준, 우준 두 아들과 만학의 길을 이끌어 이윤정 박사님 고맙고 사랑합니다.