산업체 기고문

WoT(Web of Things)를 위한 Secure Communication 플랫폼의 필요성

김 동 성

(주) 청호컴넷

Ⅰ. 서 론

스마트폰, 태블릿 등 일반 스마트 디바이스의 실질적인 사용률 증가가 '폭증'으로 언급될 만큼 수년간 지속된 현 시점에서 전 세계적인 경기 불황에도 스마트 디바이스는 IT 시장의 가장 강력한 성장 동인이 되고 있으며, 2009년에서 2011년 사이에 한국은 전 세계에서 가장 빠른 스마트폰 보급률 증가 추세를 보이고 있다.

이러한 동인에 힘입어 휴대폰뿐만 아니라, TV, 세탁기, 냉장고, 에어컨 등의 다양한 가전제품과 개인용 기기들이 스마트 디바이스(smart device)라는 이름을 달고 등장하고 있으며, '디바이스+서비스' 시장의 패권을 두고 글로벌 업체 간의 경쟁이 더욱 치열해질 것으로 예상된다[1].

사물 지능 통신(WoT: Web of Things)은 URI(Uniform Resource Identifiers)를 사물에 부여하고, 보편화된 웹 프로토콜을 통해 브라우징, 검색 및 북마킹 등의 기능을 지원할 수 있는 사물 간의 통신을 말하고, 오픈 웹 API 기반 스마트 디바이스를 이용한다[2].

이러한 스마트 디바이스들이 인터넷으로 연결된 WoT 환경에서는 보편적 웹을 통한 접근이 쉬워지므로 기존의 폐쇄된 환경보다 외부 공격에 취약해진다. 따라서 스마트 홈(CCTV, 세탁기, 에어컨, 가스레인지, 냉난방기 등), 스마트 카(내비게이터, 블랙박스 등), 스마트 빌딩(전등, 엘리베이터, 복사기, 서버 보안/소방관제 단말 등) 등 우리의 생활공간 곳곳에 존재하는 이러한 기기들이 외부로부터 악의적인 공격이 가해질 경우, 개인적인 재산과 인명 피해는 물론 사회적인 대혼란을 초래할 수 있어 WoT를 위한 보안은 매우 중요한 이슈이다[3].

기존 IP(Internet Protocol)기반 웹 환경은 풍부한 자원을 갖춘 기기들(컴퓨터, 서버 등)로 구성되어 있으며, 이에 적합한 많은 보안 프로토콜(IKEv2/IPSec, TLS/SSL, DTLS, HIP, PANA, EAP 등)이 개발되어 있으나, 이러한 보안 솔루션을 WoT 환경에 그대로 적용하기에는 많은 어려움이 있다. 그래서 저사양의 소형기기(저속의 CPU, 저용량의 메모리 및 배터리)로 구성된 자원 제한적인 네트워크(resource-constrained networks)와 이종의 통신 방식(heterogeneous communications)에 적합한 형태로 기존의 보안 프로토콜을 재설계해야 하며, 다양한 매쉬업 서비스에 따라 가변적으로 보안 프로토콜을 제공해한다. 다시 말해서 전체 서비스 성능 및 환경에 따라 디바이스/게이트웨이/서버가 유기적으로 동작할 수 있도록 WoT를 위한 새로운 플랫폼(H/W 및 S/W)이 개발되어야 한다.

본고에서는 국내·외 기술, 시장 그리고 표준화 동향을 살펴봄으로써 미래의 WoT 환경을 위한 secure communication 플랫폼의 필요성을 살펴보도록 한다.

Ⅱ. 국내·외 기술 동향

WoT라는 개념은 2007년에 등장하기 시작하였고, 현재의 WoT 정의가 완성된 것은 2009년 5월에 Vlad Trifa와 Dominique Guinard(SAP Research)가 작성한 'Web of Things Whitepaper'에서 부터이고, 한국정보통신기술협회(TTA)를 비롯한 전 세계 7개 ICT 표준 개발기관(유럽 ETSI, 북미 ATIS/TIA, 중국 CCSA, 일본 ARIB/TTC)이 M2M 분야 글로벌 표준화 협력체인 oneM2M 설립에 2012년 1월에 합의함으로써 표준 개발에 힘쓰고 있다.

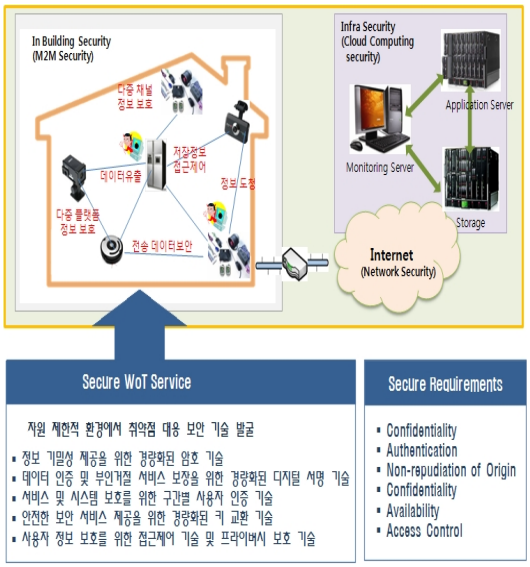
2-1 국내 기술 동향 및 수준

국내에는 'Smart IT를 통한 Smart KOREA 구현방향' 보고서(한국정보화진흥원, 2010년 9월)에서 Smart IT를 위한 WoT 기술이 소개되었다[4].

ITU-T에서 진행 중인 WoT 표준화 작업에 참여하고 있는 등 향후 WoT를 이용한 사물통신 연구에 대한 인식이 높아지고 있으나, REST를 이용한 웹 서비스 개발 활동(트위터, 구글 맵, 블로그 위젯 등)은 활발하나, 이를 사물에 적용시키는 연구 및 개발은 거의 이루어지지 않고 있어, 보다 많은 관심이 필요하다.

국내의 M2M이나 IoT 관련 보안 기술은 기존에 연구되었던 USN(Ubiquitous Sensor Networks)기술과 이를 응용 확장한 스마트 그리드에서의 보안이 주로 연구되고 있고, Open Web API 기반 WoT 환경에서의 보안 연구는 거의 이루어지고 있지 않고 있다. 따라서 환경 특성을 고려하여 최적의 보안 특성을 유도할 수 있는 기술에 대한 연구가 요구되고 있다. [그림 1]은 M2M 기반 WoT 서비스 환경에서 필요한 각 구간 별 보안 기술이다.

국내의 경우, 보안 기술의 경량화와 전송 데이터 양의 경량화 연구는 있지만, 응용의 성능과 암호학적 강도를 고려한 기술 적용에 관한 연구는 전무하다. 그리고 기존의 보안 모듈, 경량화 보안 프로토콜, 사



[그림 1] 전 세계 M2M 단말기 접속 수 현황 및 전망
※ 출처: ABI Research(2010. 5), 스트라베이스(2010. 11. 18), 재인용

생활 보호 기술 등의 단순 경량화 방식은 제한된 환경에서만 적용 가능하므로 전통적 보안 기술의 경량화나 단순 적용보다 WoT의 실 특성 분석과 다양한 적용 시나리오를 분석할 필요가 있다.

2-2 국외 기술 동향 및 수준

2-2-1 국외 WoT 기술 현황

국외의 WoT 기술 현황을 살펴보면, 실제 세계 사물의 기능 또는 데이터를 사물을 제어하는 고유의 프로토콜이나 방법으로 접근하는 방법에서 벗어나 보편적인 방법으로 벗어나 웹과 같이 보편적인 방법으로 접근하고자 하는 노력이 많이 제안되고 있다.

예를 들면, 웹 프로토콜(HTTP, CoAP 등)과 언어(HTML, XML, Javascript 등)를 활용하여 사물의 기능과 데이터를 접근 제어할 수 있으며, 이를 통해 보다 쉽게 원하는 기능을 개발할 수 있다. 그리고 웹을 이용할 경우, 접근 가능한 사물에 대해 브라우징, 검

색 및 북마킹 등의 기능이 지원되며, URI(Uniform Resource Identifiers)를 통해 사물과 통신할 수 있다.

따라서 실제의 사물이 웹에 통합되고, 이들이 단지 웹상에서 접근 가능한 하나의 서비스로 보일 경우, 각각의 서비스를 이용하여 새로운 매쉬업 서비스의 지원도 가능해질 수 있다.

2-2-2 스마트 기기 보안 기술

스마트 기기의 보안 기술은 스마트 기기와 W-LAN, WPAN 등의 통신 기술 활성화로 기기간 공유 및 데이터양 증가, 또한 활성화되는 스마트 패러다임 기반의 새로운 응용 서비스 등장으로 스마트 기기 보안 및 개인정보 보호에 대한 관심이 부각되고 있으나, 스마트 기기를 위한 보안 플랫폼 기술 개발은 아직 미비한 수준이다.

개방형 플랫폼으로 개발된 다양한 기기로 구성되는 WoT 환경의 경우, 악성 소프트웨어, 바이러스 감염 등에 따른 공역 위협이 크게 증가할 것으로 예측되어, TERESA나 OVERSEE 프로젝트와 같은 보안 기술 개발을 목표로 하는 단체들이 설립되어 활동하고 있다.

TERESA 프로젝트의 경우, 유럽의 산학 단체들이 참여하여 산업 제어, 스마트홈, 스미트미터링 등의 응용 서비스를 위한 시스템 소프트웨어 개발 방법론 및 모델링에서 안전성 및 보안 특성을 강화시킬 방법을 개발하고 있고, OVERSEE 프로젝트의 경우는 다양한 표준과 장치를 중심으로 운영되는 현재의 자동차 제어 시스템을 통합할 수 있는 장치를 개발하고, 접근 및 데이터 공유의 단일화를 통해 안정성 확보를 목표로 한다.

2-2-3 WoT/IoT 보안 기술

독일 아헨대학과 네덜란드 필립스사의 협동 연구로 CoAP 적용 환경에서 고려할 취약점과 보안 요구사항이 제안[5]되었으며, 제안된 보안 요구사항은 적용 디바이스의 전반적 생명 주기를 기반으로 분석되었다. <표 1>은 Secure WoT/IoT 환경 제공을 위한 보안 요구 사항 및 적용 가능 보안 기술이다.

<표 1> Secure IoT/WoT 환경 제공을 위한 보안 요구사항 및 적용가능 보안 기술

	Bootstrapping 단계	동작/운영 단계
보안 요구사항	- 기기 식별 및 등록 기술 - 키 생성/분배/관리 기술 - 안전한 그룹 생성 기술	- 종단간 보안 제공 - 노드 이동성 제공 - 그룹 관리 기술
보안 프로토콜	- IKEv2/MOBIKE - TLS/DTLS - HIP/DIet-HIP - PANA/EAP	- IKEv2/MOBIKE - TLS/DTLS - HIP/DIet-HIP

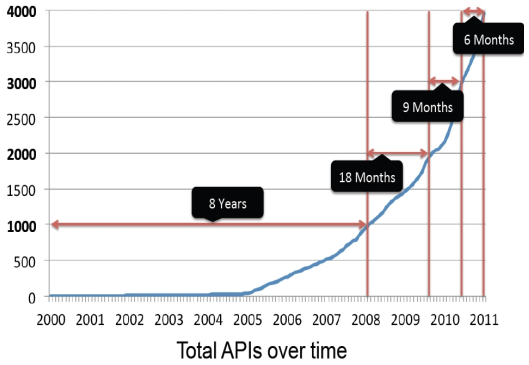
CoAP의 보안 기술의 표준화를 다루고 있는 IETF CORE(Constrained RESTful Environments) WG에서 CoAP의 보안 기술을 표준화 하고 있다. 현재 WG에서는 안전한 전송을 위해 UDP 환경의 통신 보안 기술인 DTLS 기술의 적용을 고려하고 있어, 이를 수용하기 위한 방안의 연구 필요성을 제기하고 있다.

또한 6LowPAN이 적용되는 제한된 WoT 환경(LLN: Lossy and Low Power Network)과 인터넷을 연동하는 Border Router의 기능상 정의가 필요하고, Bootstrapping 단계에서 보안 요구 사항 및 초기 정보의 안전한 전송 기술이 논의되고 있다.

2-2-4 임베디드 웹서비스 플랫폼 기술 현황

Web 2.0 기반 Open API 및 REST 관련 기술은 웹을 기반으로 하는 SNS의 활성화로 인하여 서비스의 확장 및 서비스 간의 매쉬업을 지원하기 위해 많이 사용되고 있다.

전 세계 Open API의 등록처 역할을 하는 Pro-



[그림 2] "ProgrammableWeb"에 등록된 Web 2.0 기반 Open API의 증가 추세

※ 출처: ProgrammerbleWeb, Oct. 2011

grammableWeb의 2011년 자료를 보면, 2005년에는 100여개에 불과했던 Open API 지원 서비스가 2008년에는 1,000개로 증가하였으며, 2011년 10월에는 4,000개에 이르게 되었다.

단순함과 명료함을 추구하는 HTTP 기반의 API 스타일의 REST는 Open API 기반 서비스 구축하는데 다른 API에 비해 이해가 빠르고, 애플리케이션 개발이 용이하여 Web 2.0 환경에서 쉽게 활용될 수 있고, 차지하는 비율 또한 증가하고 있다.

Ⅲ. 국내·외 시장 현황

ABI Research에 따르면 Cellular M2M 시장은 2011년 1.1억 개의 누적 단말수를 기록했고, 2017년까지 4.53억 개의 단말이 M2M망에 연동될 것으로 전망하고 있다.

3-1 시장 규모 및 현황

M2M(WoT, IoT)의 적용 영역이 매우 다양하고 범위가 넓어 전체 규모를 하나의 수치로 집계하기 어려운 실정이다.

〈표 2〉는 iDate Consulting & Research, Beecham Research('09) 자료를 재구성한 시장 전망을 나타내었다.

〈표 2〉 국외 M2M 시장 전망 (단위: 조 원)

구분	2010	2012	2014	2016	2018	2020
솔루션/정보	1.5	3.0	5.1	7.9	11.8	17.7
네트워크	0.3	0.6	1.1	1.6	2.4	3.6
하드웨어	0.5	0.9	1.4	2.2	3.2	4.8
Total	2.3	4.5	7.6	11.7	17.4	26

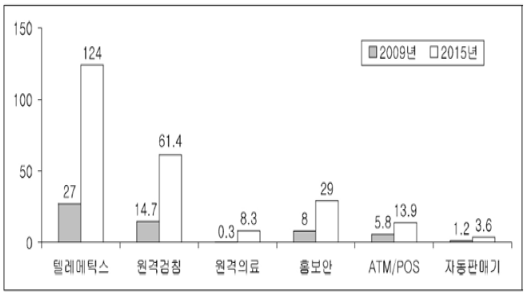
KT 경제 경영 연구소에서는 자체적으로 2009년의 M2M 시장 규모를 약 1.4조 원으로 집계한 바 있다. 〈표 3〉은 이를 기준으로 한 2011~2014년 시장 규모의 추정치이며, 이 수치는 단말, 네트워크, 솔루션 매출만을 포함한 것이다.

국내 M2M 시장은 2010년 2.3조원에서 2014년 7.6조 원 규모로 3.3배 성장할 것으로 전망되며, 성장률은 2014년까지 연평균 35 %의 고성장을 지속할 것으로 예상된다.

ABI Research의 2010년 자료에 의하면 전 세계 이

〈표 3〉 국내 M2M 시장 전망 (단위: 조 원)

구 분	2011	2012	2013	2014	CAGR
매출액	32	45	59.5	76	35%



[그림 3] 전 세계 M2M 단말기 접속 수 현황 및 전망

※ 출처 : ABI Research(2010. 5), 스트라베이스(2010. 11. 18), 재인용

〈표 4〉 전 세계 M2M 시장 규모 전망

(단위: 칩/모듈 및 서비스는 백만 달러, 단말기는 백만 대)

구 분	2009년			2013년			CAGR (%)
	B2C	B2B	합계	B2C	B2B	합계	
칩 /모듈	2,000	45,000	3,080	3,500	1,976	5,476	15.5
단말기	50	60	110	180	240	420	39.8
서비스	25,000	1,500	26,500	37,000	5,998	42,98	12.9

동통신망을 통한 M2M 단말의 접속건수가 2009년 약 5천 7백만 건 수준에서 2015년 2억만 건 이상으로 급증할 것으로 전망하였고, 서비스별로 텔레매틱스 및 원격 검침에 대한 접속 규모가 가장 큰 것으로 전망하고 있다.

Mogan Keegan은 전체 세계 M2M 시장을 칩, 모듈, 단말기, 서비스 시장으로 구분해 시장규모 전망하였으며, 최근 다양한 커넥티드 단말의 등장으로 M2M 단말기가 2009년 년 1억 1천만 대에서 2013년에는 4억 2천만 대로 연평균 약 40 % 급성장할 것으로 예상하고 있다.

3-2 수출입 현황

지식경제부에서 발표한 국내 IT 산업 수출입 통계를 수집한 Atlas Research 자료를 재구성하면 2010년부터의 IT산업 수출입 통계는 〈표 5〉와 같다.

〈표 5〉 IT 산업 총괄 년도별 수출입 통계 (단위: 억 달러)

연도	2010년	2011년	2012년*
수출	1,539.4	1,569.7	229.4
수입	756.2	815.2	123.9

* 2012년도는 1월, 2월 통계를 합산

※ 출처 : Atlas Research, 국내 IT산업 수출입 현황(2011. 12), 국내 IT산업 수출입 현황(2012. 1), 국내 IT산업 수출입 현황(2012. 2)

Ⅳ. 국내・외 표준화 현황

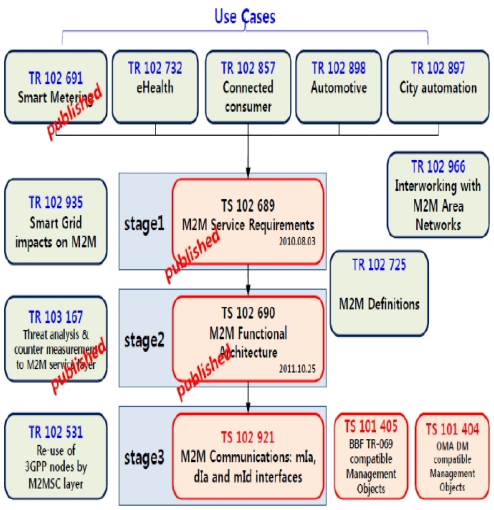
Secure Communication 플랫폼과 직접적으로 관련 있는 국내・외 표준화 현황을 살펴보도록 한다.

ETSI는 다양한 M2M 서비스 및 기술을 표준화된 플랫폼을 관리할 수 있도록 M2M Release 1(ETSI TS 102 689, ETSI TS 102 690, ETSI TS 102 921)을 발표하였다.

TS 102 689에서는 M2M Security Requirement를 정의하고 TR 102 690에서 M2M Security 관련 functional element(xSEC, NREM, MAS, MSBF)와 함께 M2M Service Bootstrap, provisioning, Service connection 절차를 정의하고 있음. 또한 TR 103 167은 M2M 서비스 레이어 상에서의 보안 위험 요소에 대한 정의 및 위험을 완화하는 방안을 정의하고 있다.

OMA(Open Mobile Alliance)는 모바일 전화 및 기기에 대한 원격 관리를 위한 규격을 제정하고 있으며, 2012. 7 현재까지 21개의 모바일 서비스 Enabler와 60개 이상의 관리대상을 정의하였다[6].

2012. 7 발표에 따르면 현재 전 세계적으로 14억



[그림 4] ETSI M2M 표준화 현황(2011. 2 기준)

개 모바일 전화와 연결되어 기기에서 OMA DM 모바일 서비스 Enabler가 배치되어 있다.

OMA는 현재 M2M을 위해 새로운 3건의 서비스 Enabler(CPNS, GwMO, Lightweight M2M Enabler)를 개발하고 있다.

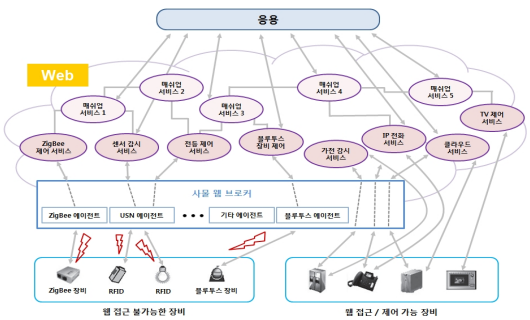
최근에는 센서 등과 같이 용량이 제한적인 기기를 지원함은 물론 복잡한 전산 또는 사용자 인터페이스 없이 기기를 원격으로 제어할 수 있도록 Lightweight M2M Enabler 규격을 제정 중이다.

한국정보통신기술협회(TTA)을 비롯한 전 세계 7개 ICT 표준개발기관(유럽 ETSI, 북미 ATIS/TIA, 중국 CCSA, 일본 ARIB/TTC)이 M2M 분야 글로벌 표준화 협력체인 oneM2M 설립에 2012년 1월에 합의하였다.

WoT 관련된 표준 개발은 ITU-T에서 가장 활발하게 진행시키고 있으며, 많은 부분에서 표준 개발이 진행되고 있다.

ITU-T SG13 산하의 Q.12에서 Y. WoT(Web of Things Framework)로 개발 진행 중에 있으며, 사물 웹 서비스 모델 개발과 구조 개발 등이 완료된 상태이다. Y.WoT 권고안은 2010년 5월에 시작되었으며, 2011년 12월에 ITU-T SG13 Q.12 Interim 회의가 개최되었다.

[그림 5]는 ITU-T SG13 Q.12 Y. WoT의 기본 모델[7]을 나타내고 있으며, 크게 웹 접근 불가능 장비와 웹 접근/제어 가능 장비로 분류될 수 있다.



[그림 5] WoT 모델

웹 접근 불가능 장비는 직접적으로 인터넷에 연결될 수 없지만, WoT 브로커에 자원을 등록하고 웹으로 접근할 수 있으며, 웹 접근/제어 가능 장비는 기본적인 HTTP 프로토콜 및 웹서버 같은 WWW의 기능을 모두 갖춘 디바이스로 WWW에서 직접적으로 접근과 WoT 브로커를 통한 접근이 모두 가능하다.

Ⅴ. 결 론

WoT와 관련된 구체적인 솔루션 및 적용된 상용 제품은 아직 존재하지 않으나, WoT에 대한 프로토타입 제작 및 검증은 이미 여러 연구 기관 및 회사에서 진행되었으며, 또한 제작 및 검증이 완료된 사례가 있으므로 머지않아 이와 관련된 상업적인 활동이 일어날 것이다.

이러한 상황에서 이종의 네트워크 환경에서 다양한 매쉬업 서비스를 우수한 품질로 안전하게 제공하고, 보안 기능을 강화할 수 있는 WoT를 위한 Secure Communication 플랫폼에 대한 연구 개발이 필요하다.

참 고 문 헌

[1] EU, European Commission - Press release, Retrieved Apr., 12, 2012, from http://europa.eu

[2] D. Zeng, S. Guo, and Z. Cheng, "The web of things: A survey", *Journal of Communications*, vol. 22, no. 6, pp. 424-438, 2011.

[3] Rolf H. Weber, "Internet of things - New security and privacy challenges", *Computer Law & Security Review*, vol. 26, Issue 1, pp. 23-30, Jan. 2010.

[4] 한국전파진흥원, "Smart IT를 통한 smart KOREA 구현 방향", 2011년.

[5] Z. Shelby, K. Hartke, and C. Bormann, "Constrained

Application Protocol(CoAP)", http://tools.ietf.org/id/draft-ietf-corecoap-08.txt, 2011.

[6] OMA Device Management Protocol, Version 1.2, Open Mobile Alliance, Jun. 2006.

[7] 인민교, "Draft recommendation Y. WoT, framework of web of things", ITU-T, 2011년.

≡ 필자소개 ≡

김 동 성

1995년 2월: 한국항공대학교 항공통신공학과 (공학사)

1997년 8월: 한국항공대학교 항공통신공학과 (공학석사)

현재: (주) 청호컴넷 연구소장

현재: 인하공업전문대학교 정보통신과 겸임교수

[주 관심분야] Web of Thins RFID/USN