편집위원 : 이재훈 (동국대)

사물인터넷 보안을 위한 표준기술 동향

강남희
덕성여자대학교

요 약

사물인터넷 (IoT: Internet of Things) 기술은 사람과 사람, 사람과 사물들의 연결에서 생활 속 모든 것들(daily life objects)을 상호 연결시켜 초-연결(Hyper-connectivity) 사회를 구축할 수 있는 기반 기술이다. 이미 인터넷에 연결된 PC나 스마트 기기의 양적 증가가 아닌, 기존에는 인터넷과의 연결을 고려하지 않았던 가전기기, 센서, 동/식물 등 다양한 일상의 사물들이 인터넷과 연결되고, 더 나아가 프로세스 그리고 가상 콘텐츠까지 연결의 대상으로 확장되고 있다. 이러한 IoT 기술의 활성화 및 신규 서비스 창출을 위해 보안은 반드시 제공해야 하는 핵심기술이다. 적용 환경과 시나리오에 따라 보안은 정보 보호 차원을 넘어 사람의 생명과도 직결되기 때문이다. 이에 본고에서는 사물인터넷 환경에서 고려해야 하는 보안 이슈들을 살펴보고, 유관된IETF (Internet Engineering Task Force) 표준기술 동향을 다룬다.

Ⅰ. 서 론

최근 다양한 분야에서 사물인터넷 기술에 대한 관심이 고조되고 있다. 종래의ICT 기술 기반 서비스와 사용자 주변의 사물들로 구성된 물리 환경이 메쉬업(physical mesh-up)되면서 사물들의 정보를 축적, 분석, 가공, 관리 후 이용하기 위한 다양한 서비스 플랫폼 및 기술들이 개발되고 있다. 가트너는 현재 1% 미만의 사물들만이 인터넷에 연결된 상황이라고 보고한 바 있고, 시스코는 2020년에는 인터넷에 연결되는 사물들의 수를 가트너의 예상치인 260억개 보다 많은 500억 개 이상으로 예측하고 있다. 최근 정부도 포스트 스마트폰 시대에서 시장을 주도할 수 있는 신성장 동력으로 사물인터넷 기술을 선정하였고 6년뒤 30조원의 거대 시장으로 육성하기 위한 계획을 제시하고 있다 [1].

물리적으로 제한된 크기의 공간에서 사전에 정의된 서비스를 제공하기 위해 센싱 정보를 취득하여 활용하던 USN과 M2M 기술들과는 다르게 사물인터넷이 적용되는 환경은 다양한 서비스들이 상의한 관리 도메인에 소속되더라도 유동적으로 상호 운영되는 융합(integration) 환경으로 정의할 수 있다. 〈그림 1〉은 사용자 중심의 IoT 기반 환경의 예시를 나타낸다.

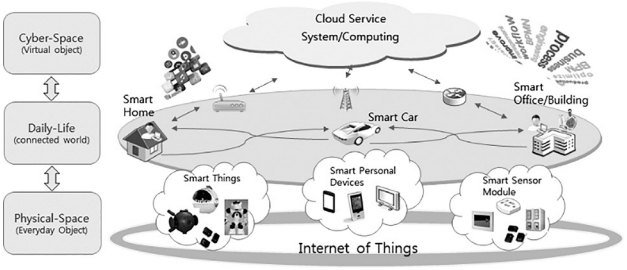

그림 1. 사용자 중심의 IoT 기반 초연결 사회

일과에 따라 변하는 사용자의 동선에 필요한 응용과 서비스들이 제공되기 위해 사용자 중심의 일상 사물들과 가상 공간의 서비스 제공 기술들이 협업하게 된다. ICT 기반 서비스와 사용자 주변의 사물 환경들이 메쉬업되어 사물의 상황 정보를 서비스에서 활용할 수 있는 다양한 방식들이 개발될 것이다.

사물들의 통신과 협업을 위해 개방형 플랫폼과 개방형 표준기술은 반드시 필요하다. 또한 초-연결 사회를 제공하기 위해 이종의 사물(컴퓨팅, 메모리, 제공 서비스의 다양성)들과 네트워크 기술(BAN, CAN, LAN, MAN, WAN 등)들이 경계 없이 융합되어 발전될 것이다.

그러나, 〈그림 1〉에 나타낸 예시처럼, 네트워크에 연결된 장치 수의 증가는 공격할 수 있는 대상의 증가와 위협 요소의 확장을 의미한다. 특히 의료 서비스나 산업 시설 제어 서비스에 적용되는 사물인터넷 장치와 통신 기술에는 보안 기술이 필수적이다. 이러한 서비스가 침해되었을 경우 단순한 경제적 피해를 넘어서 인명 피해가 유발될 수 있기 때문이다. 또한 주변의 일상 사물들이 연결된다는 것은 개인 정보 유출이나 프라이버시 침해가 우려되는 범위의 증가를 의미하고, 그 침해 정도도 현재와 비교할 수 없을 정도로 증폭될 것은 자명하다.

기하 급수적으로 증가하게 될 사물인터넷 통신 주체들은 작게는 데이터를 수집하는 센서와 간단한 제어가 가능한 액츄에이터를 포함하여 복수개의 센서와 액튜에이터를 갖는 다양한 이종 시스템들을 포함한다. 기존의 인터넷 보안 기술로 안전을 설계하기는 무리가 따르는 부분이다. IoT가 지향하는 스마트 세상을 만들기 위해서는 자원(CPU, 메모리, 전력 등)이 제한적인 일상의 사물들과 이들이 연결되는 저전력 네트워크 및 인터넷 연동을 수용하는 IoT 보안 기술이 제공되어야 한다.

본 고에서는 관심이 고조되고 있는 사물인터넷 환경에서의 보안 이슈를 다룬다. 특히 자원이 제한적인 초소형 장치들이 인터넷 기술과 연동되어 서비스될 경우 고려해야 하는 위협과 취약점을 살펴보고, 이를 해결하기 위해 제안되고 있는 표준 기술의 동향을 IETF 중심으로 다루어 보고자 한다.

Ⅱ. 사물인터넷 보안 이슈

기존에 사용하던 이종의 장치(인터넷 접속과 무관했던 사물 포함)들이 사물인터넷 환경에서는 인터넷과 접속되어 다양한 서비스가 제공될 것으로 예상된다. 결국 데이터 통신 및 시스템 보안의 관점에서 생각하면 기존 인터넷 환경에서 발생할 수 있는 모든 위협들과 취약점들은 사물인터넷에서도 발생될 수 있다. 그림2는 인터넷 프로토콜의 계층별 위협요소들과 대응 기술들을 정리하고 있다[2].

자원이 제한적인 사물들과 저전력 통신 기술을 적용한 네트워크에서는 그림 2에 예시된 위협요소들이 노출될 가능성이 더욱 높다. 또한 자원이 제한적인 장치와 네트워크에서는 신규 위협요소들이 등장할 것이다. 대표적인 예가 CoAP(Constrained Application Protocol) 표준 기술에서 권고되는 보안 프로토콜인 DTLS (Datagram TLS, RFC6347)를 적용할 경우 발생 가능한 단편화(fragmentation) 공격이다[3].

단편화는 인터넷을 구성하는 이종 네트워크 사이에서 데이터 전송 매체가 전송할 수 있는 최대 프레임 크기인 MTU의 차이를 보상하기 위한 기술이다. IP 기반 유선 인터넷에서 많이 적용되는 MTU인 1500byte와 6LowPAN이 적용되는 저전력 네트워크인 LLN (IEEE 802.15.4)에서의 MUT인 127byte가 하나의 예가 된다. 즉, LLN이 인터넷과 연동되었을 경우 인터넷 송신에서 전송되는 데이터는 LLN의 접속 지점인 6LBR (6LoWPAN Border Router)에서 127byte의 크기로 단편화되어 전송되고 수신 장치에서 재조립되어 원 데이터의 모습을 만드는 방식이 사용된다.

Layer	Threat	Requirements	Targets[1]	Approaches
Transport	Ping/ICMP flood	attacker being part of the network, ICMP	All connected devices	
	Synflood	TCP, attacker being part of the network	All connected devices	
Network	Neighbor discovery attack	Neighbor Discovery protocol	Networks using unauthenticated ND protocol	Authentication support for ND protocols
	Wormhole	Mesh networking	Multihop wireless networks	Specific hardware, time constraints on packet delivery
	Black hole	Attacker being part of the network	Multihop wireless networks	Don't use plain distance-vector based protocols.
Link	Spoofing	-	All networks, especially wireless	Packet authentication
	Eavesdropping	-	Wireless networks	Encryption
	DoS – Collision	-	Wireless networks	Use UWB, increase datarate
	DoS – Exhaustion	-	Embedded wireless networks	Link-layer Intrusion detection
	Replay protection att.	Replay protection	Multihop wireless networks	RANBAR, Tesla

그림 2. 인터넷 계층별 위협 및 대응 기술

공격자는 이러한 단편화 기능의 처리 절차와 수신 장치의 자원 제한적인 특성(특히 적은 메모리 공간)을 악용하여 공격을 수행할 수 있다. 최근 발표된 [3]에서는 6LoWPAN 계층에서 데이터 인증을 수행하는 기능의 부재를 이용한 공격 시나리오와 'fragment duplication' 공격 및 'buffer reservation' 공격을 소개했다. 더욱이 공격자는 자원을 많이 사용하지 않더라도 단편화 기능을 수행하는 장치들의 가용성을 침해하고, 더 나아가 목적 장치의 동작을 마비시키는 DoS 공격으로 확장시킬 수 있다. [3]에서 예시한 시나리오처럼 공격자의 장치 역시 소형 장치이므로 자원이 제한적이다라는 가정을 하지 않는다면 공격의 위협 및 범위는 더욱 증가할 것이다.

기존 인터넷에서는 단편화 공격에 대응하기 위해 단편화가 수행될 만큼 큰 데이터는 전송되지 못하도록 제한하기도 한다. 그러나 LLN의 경우 네트워크 관리자의 의도나 제어 방식과 무관하게 단편화가 수행될 수 밖에 없는 상황이 존재한다. 작은 장치들의 펌웨어를 갱신하거나 DTLS를 적용할 경우 사전에 수행되는 핸드쉐이크 절차에서 전송되는 데이터가 대표적인 예가 된다. IETF 에서 논의된 바에 따르면 데이터 전송의 양이 적을 것으로 생각되는 ECDHE, ECDSA, AES를 기반으로 수행되는 핸드쉐이크 과정에서도 800byte 이상의 데이터가 전송되어야 하고 LLN의 MTU를 고려할 경우 많게는 27개의 단편화 프레임으로 분리되어 전송될 수 밖에 없다[4]. 안전한 보안 채널이 형성되기 전에 수행되는 핸드쉐이크 과정이므로 인증에는 취약하고 따라서 [3]에서 예시한 단편화 공격이 발생하게 된다. 또한 다중 홉으로 사물인터넷의 접속 네트워크가 구성될 경우 단편화된 프레임들은 순서가 바뀌어 도착할 수 있고, LLN의 특성으로 손실될 수 있다. 수신 장치는 단편화가 실패할 경우 재전

송을 받아야 하므로 자원 낭비의 악순환은 반복된다.

상기 예를 포함하여, 사물인터넷 보안이 제 기능을 수행하지 못할 경우 매우 심각한 상황이 초래될 수 있다. 최근 사물인터넷 기술을 이용하여 서비스가 활성화 될 것으로 큰 기대를 받고 있는 헬스케어 서비스에서는 보안 기능이 수행되지 않을 경우 사용자의 목숨까지 위협받게 된다. 실 사례로 2013년 블랙햇 학술대회에서 인슐린 펌프를 해킹하여 환자에게 과다 약물을 투여할 수 있고, 해커의 사망으로 시연되진 않았지만 심박조율기를 해킹하여 조작할 경우 환자를 사망하도록 할 수 있음도 보고된 바 있다. 동일 행사에서 자동차가 해킹될 경우 운전자의 사망까지 초래할 수 있다는 사례도 발표되었다. 보안이 데이터의 보호와 프라이버시 침해를 막는 수준이 아닌 생존의 문제까지 확대될 수 있다는 시사점이 된다.

〈그림 2〉의 예와 더불어 신규로 등장하게 될 사물인터넷 위협들에 대응하기 위해 개발되는 보안 기술들은 다음과 같은 일상 사물들의 제한 사항을 고려해야 한다.

- IoT 기반 응용 서비스의 종단 시스템(data source and sink)들의 제한적 자원(CPU, ROM, RAM, 배터리 의존 등)
- 이종(heterogeneous)의 제한적인 무선 통신 환경(IEEE 802.15.4, Bluetooth 등)의 손실율, 전송율, MTU 크기
- 사용자 인터페이스 제한(키보드/마우스 등의 입출력 인터페이스 부재, 웹 기반 설정 SW 부재)
- 이종 사물들의 이동 특성이 상이함 (Stationary or Nomadic or Mobile)
- IoT 서비스 환경에서 작은 센서가 서버의 역할을 수행 할 수 있음 (인터넷 브라우저의 요청에 정보 제공)
- 시간 및 장소에 무관하게 유기적으로 연결될 수 있으므로 초기 설정, 갱신, 주체간 trust 설정 및 인증 필수

Ⅲ. IoT 보안을 위한 IETF 표준 기술

사물인터넷 관련 기술들의 표준화는 ITU (International Telecommunication Union)와 유럽의 ETSI(European Telecommunications Standards Institute)가 서비스 모델과 서비스 연동의 관점에서 구조적으로 접근하고 있으며, IETF에서 IP 기반 프로토콜 표준을 주도하고 있다. 이 이외에도 IPSO (Internet Protocol of Smart Objects), OMA(Open Mobile Alliance) 등의 사설 표준 기관에서도 IoT 관련 표준 적용을 논의하고 있다.

IETF에서는 다양한 무선 접속 네트워크 환경에 IP를 적용할 수 있는 기술들을 표준화하기 위해 6LowPAN, 6Lo, 6tisch, ROLL, LWIG 등의 워킹 그룹(WG: Working Group)들을 결성했다. 또한 IETF에서는 응용 데이터의 전송을 위해 CORE WG을 결성하여 자원 제한적인 장치들이 경량화된 방식으로 메시지를 주고 받을 수 있는 CoAP기술을 표준화하고 있다[5]. OMA의 LWM2M(Lightweight M2M) 구조에서도 CoAP과 DTLS를 전송 프로토콜로 고려하고 있다. 본 장에서는IETF에서 논의되고 있는 표준 보안 기술들을 살펴본다.

1. CoAP 보안 기술

IETF 표준화 기구에서는 자원이 제한적인 장치들로 구성된 저전력 손실 네트워크와 인터넷과의 연동을 제공하기 위한 기술들을 다양한 워킹 그룹들을 통해 표준화 하고 있다. 이들 중 응용 데이터의 전송을 위해 CORE(Constrained RESTful environments) 워킹 그룹을 결성하여 자원 제한적인 장치들이 상호 발견하고(discovery) 경량화된 방식으로 정보를 주고 받을 수 있는 기술들을 논의하고 있다[6]. 최근 웹 전송 표준 프로토콜인 HTTP와 유사한 특성을 갖는 CoAP 기술에 대한 표준화 작업을 완료했다[5].

CoAP은 기본적으로 8비트 마이크로컨트롤러와 저용량 저장공간(ROM 및 RAM)이 탑재된 장치를 주요 적용 대상으로 하고 있다. 무선 통신 환경도 데이터 손실률이 높고 초당 수십 Kbits 정도의 전송률을 고려하고 있다. 하지만 확장 적용하면 브라우저와 같은 종래의 웹 기반 서비스 객체들이 작은 일상의 사물들과도 정보를 주고 받을 수 있다. 사물인터넷 환경에 적용될 경량 장치의 상세한 분류 및 CoAP 구현 가이드라인은 LWIG(Light-Weight Implementation Guidance) WG에서 논의 되고 있다[7].

CoAP 표준은 장치 간 전송되는 데이터의 기밀성(confidentiality)과 무결성(integrity)과 같은 보안서비스의 제공을 위해 UDP 기반 TLS(Transport Layer Security, RFC5246) 방식인 DTLS의 사용을 권고하고 있다[5]. DTLS를 적용하면 통신 주체 간 인증, 데이터 기밀성과 무결성 서비스를 제공할 수 있고 재전송 공격에 대응할 수 있다. DTLS를 적용한 CoAP은 다음과 같은 3가지 보안 모드를 제공한다.

- PreSharedKey 모드: 전송 주체간 사전에 설정된 PSK(Pre-Shared Key)를 기반으로 하여 DTLS 세션을 개설
- RawPublicKey 모드: 공개키 방식의 DTLS를 사용하지만 인증기관에서 발행하는 인증서에 의존하지는 않음; 이러한 out-of-band 방식의 예로 센서가 정보를 전송할 서버(dedicated web server)가 고정된 경우 센서를 제조할 때

서버의 공개키와 주소, 센서의 공개키 페어를 장치에 포함시키는 방식, RFC6698에 정의된 DANE(DNS 보안)를 이용, LDAP을 이용하는 방식 등이 적용될 수 있음[8]

- Certificate 모드: RFC5280에 정의된 X.509 certificate를 사용하여 통신 주체의 공개키를 획득하여 DTLS를 적용; 센서 장치는 인증서를 공인할 수 있는 root trust anchor들의 목록을 관리해야 함

CoAP의 보안을 위해 DTLS를 적용할 경우 많은 제한사항이 따른다. 컴퓨팅 자원이나 네트워크 대역폭이 제한적이지 않은 기존 인터넷 환경에서 사용하던 DTLS 프로토콜의 구현 크기는 LWIG 워킹 그룹의 [7]에서 정의한 Class 0와 Class 1에 해당하는 초소형 장치들의 RAM과 ROM을 고려할 경우 설치 운영되기에는 무리가 있다. 〈그림 3〉은 각 Class 단위의 RAM과 ROM의 크기를 나타낸다.

Name	Data size (e.g., RAM)	Code size (e.g., Flash)
Class 0	<< 10 KiB	<< 100 KiB
Class 1	~ 10 KiB	~ 100 KiB
Class 2	~50 KiB	~ 250 KiB

그림 3. 센서의 자원에 따른 분류

하나의 예로, 2012년 Smart object security 회의에서 발표된 DTLS의 구현크기는 표 1에 기술된 보안 알고리즘들이 구현되어 탑재될 경우 총 35,960 바이트가 된다. 따라서 Class 0와 Class 1에서 동작될 수 없다[9].

표 1. Crypto 프리미티브 코드 크기

Library	Code Size
MD5	4,856 bytes
SHA1	2,432 bytes
HMAC	2,928 bytes
RSA	3,984 bytes
Big Integer Implementation	8,328 bytes
AES	7,096 bytes
RC4	1,496 bytes
Random Number Generator	4,840 bytes

더욱이 앞서 언급했듯, 인증서 교환을 포함하여 총 6개의 메시지 교환 방식을 기본으로 하는 DTLS 핸드쉐이크 과정은 MTU가 127byte인 802.15.4 네트워크 환경에서 단편화된 많은 프레임을 발생시킨다. LLN에서 분할된 수많은 프레임은 손실율 증가와 재전송으로 발생되는 지연 등의 문제를 유발하고, 소형 장치들을 대상으로 하는 단편화 공격의 주 원인이 될 수 있다.

이러한 제한 사항을 해결하기 위해 DLTS의 구현 크기를 LLN 장치들에 적합하도록 경량화하는 구현 방안이 제안되었다[10]. 또한 LLN 내 오버헤드를 줄이기 위한 방안으로는 DLTS 헤더를 압축하여 전송되는 메시지 사이즈를 줄이는 등의 방안도 제안되었다[11]. 최근에는 LLN내의 단편화로 인한 성능 저하와 위협 요소를 줄이기 위한 다른 방안도 제안되고 있다. 독일의 Aachen 대학에서 제한한 기술은 인증서 기반 DTLS의 핸드쉐이크 과정을 위임(delegation) 장치를 통해 수행하고, 핸드쉐이크 후 생성되는 세션의 정보들을 소형 장치에 전달하는 방식을 사용한다[12]. 전달된 세션 정보를 이용하여 장치는 통신의 종단과 session resumption기술을 이용하여 핸드쉐이크 오버헤드를 줄일 수 있게 된다.

2. DICE WG 표준 기술 동향

CoAP 프로토콜의 보안 권고 기술인 DTLS를 자원이 제한된 소형 경량장치들과 저용량 네트워크 환경에 적용할 경우 1절에 기술한 많은 제한사항이 존재한다. 이러한 문제의 해결방안을 논의하기 위해 IETF내에 DICE(DTLS In Constrained Environments) BOF가 2013년 6월 구성되었고, 같은 해 9월 정식 워킹 그룹으로 승인되어 표준화 논의가 진행 중이다 [13]. DICE 워킹 그룹은 다음에 기술된 3가지 기술을 초기 표준의 목적으로 삼고 있다.

- CoAP 표준 기술에서 권고하는 3가지 보안 모드의 구현을 위한 DTLS 프로파일의 표준화
- 안전하게 멀티캐스트 메시지를 전송하기 위해 DTLS record 계층을 사용할 수 있는 기술
- 자원 제한적인 환경에서 DTLS 핸드쉐이크의 제한 사항(성능 및 보안 이슈)을 현실적으로 해결하기 위한 방안

상기 목적 중 첫 번째에 해당하는 기술인 "IoT를 위한 DTLS 1.2 프로파일" 문서가 WG-draft로 논의되고 있다. 이 문서는 DTLS 1.2 표준을 수정하지 않는 범위에서 IoT 환경을 구성하는 자원 제한적인 노드에서 합리적으로 구현될 수 있는 방안을 주요 내용으로 하고 있다. 그 동안 논의를 통해 Keep-alive 확장, perfect forward secrecy, 클라이언트 인증서 URLs 등의 이슈들이 다루어졌다.

두 번째 목적에 해당하는 멀티캐스트 보안 기술의 경우, 관련 문서가 여러 번 갱신되었지만 WG 문서로 채택되진 못하고 있다. 기고문의 핵심 내용은 CoAP의 보안을 위해 장치들에

DTLS를 구현했다면 멀티캐스트 보안에서도 활용해보자는 것이다. 특이한 내용으로, 다음 그림처럼 M:N 멀티캐스트를 지원하기 위해 DTLS record 헤더의 일련번호 영역을 나누어 M개의 송신을 구분할 수 있는 Sender ID 영역의 사용을 제안하고 있다.

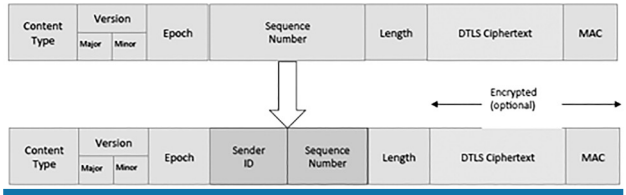

그림 4. 멀티캐스트 보안을 위한 헤더 구조

그러나 그룹 보안을 위한 암호키의 설정 및 관리 방안과 그룹 멤버 관리 등 주요한 사항을 다루고 있지 않고, 멤버가 송신에게 응답해야 하는 경우 응답 메시지의flooding 문제가 발생할 수 있는 문제가 있다. 또한 프록시를 사용할 경우 송신과 수신 사이에서 종단간 보안을 제공할 수 없다는 것도 문제로 지적할 수 있다.

마지막 목적인 DTLS 핸드쉐이크로 인한 문제점은 3.1절에 기술된 것처럼 헤더 압축, 핸드쉐이크 위임 모듈, session resumption 활용 등 다양한 해결 방안들이 제안되고 있다.

3. ACE WG 표준 기술 동향

ACE(Authentication and Authorization for Constrained Environments) WG은 올해 정식 WG으로 승인되어 7월 IETF 90회의에서 첫 논의가 진행되었다. 워킹 그룹의 이름에서 나타나듯 인증을 포함하여 DTLS 기술로 해결하기 어려운 자원의 인가와 접근 제어 문제를 논의한다. 종래의 유무선 인터넷 서비스에서 자원 인가와 접근 제어를 제공하기 위한 기술은 다양하게 제안되어왔고 제 3 장치(TTP)의 신용과 중재를 기반한 표준 기술들도 존재한다. Kerberos, PKI, AAA 등과 같이 긴 시간 논의되고 갱신된 기술들도 있고, 최근 표준화가 진행중인 OAuth나 ABFAB와 같은 기술들도 있다. 이러한 기술들의 목적은 유사하겠지만 적용하고자 하는 환경이나 동작 방식 그리고 전송 메시지에는 차이점이 많다.

ACE 워킹 그룹은 사물인터넷 환경을 위한 인가 및 접근 제어 프로토콜을 신규로 표준화하기 전에 기존에 사용되던 방식을 적용할 수 있는지의 여부를 먼저 논의하기로 했다. 이를 위해 사물인터넷 환경에서 인가 및 접근제어가 필요한 use case들을 찾고, 종래의 기술을 적용할 때 고려해야 하는 장점과 단점을 먼저 논의하고 있다.

사물인터넷 환경을 위한 자원 인가와 접근 제어 기술들에서 고려되어야 하는 사항은 다양하다. 특히, 헬스케어 서비스에 주로 사용되는 장치들의 경우, 메모리 등의 자원도 제한적이고 배터리에 의존하게 되므로 인가를 위해 적용하는 보안 기술로 인해 발생되는 송/수신 메시지의 크기와 전송 회수, 계산의 복잡도 등은 서비스 성능의 문제를 포함하여 서비스 거부 공격에 노출될 가능성도 있음을 염두에 두어야 한다. 또한 일반적인 사용자는 장치의 기본 설정을 그대로 사용하는 경우가 많고, 초소형 장치에는 설정을 위한 사용자 인터페이스(모니터나 키보드 등)가 제한적이므로 초기 설정 및 펌웨어 갱신의 보안을 반드시 고려해야 한다.

최근 진행된ACE 워킹 그룹의 첫 회의에서 접근제어를 제공하기 위해 필요한 구성요소와 이들의 역할이 주요 안건으로 논의됐다. 〈그림 5〉에 나타낸 것처럼, IoT 환경에는 사용할 수 있는 자원의 제한성을 고려하여 초소형 IoT 장치에 해당하는 C(Client)와 RS(Resource Server)를 보조할 수 있는 AM(Authentication Manager)이나 AS(Authorization Server), 그리고 이 장치들의 설정이나 정책을 책임지는 CO(Client Owner), RO(Resource Owner)등이 구성 요소가 된다. 〈그림 5〉는 논의에 사용되었던 발표자료에 포함된 내용이다[14].

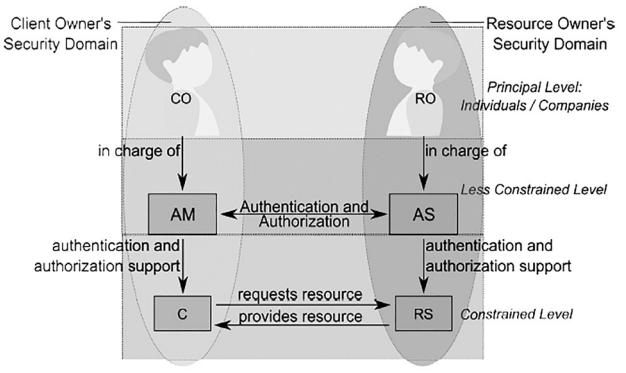

그림 5. 접근제어를 위한 구성요소

이와 더불어, 서두에 언급한 다양한 종래의 보안 기술(i.e. Kerberos, OAuth 등)들의 적용과 제한사항들이 논의됐다.

Ⅳ. 결 론

본 고에서는 사물인터넷 환경에서 고려해야 하는 보안 취약점들을 살펴보고, 이에 대응하기 위해 논의되고 있는 표준 기술을 살펴봤다. IETF 표준 기구에서는 사물인터넷을 구성하는 소형 장치 간 전송되는 데이터의 암호화와 무결성 제공을 위해 DTLS의 재사용을 권고하고 있고, 정보 자원의 사용 인가와 제어를 위한 다양한 기술들에 대한 논의가 시작되었다.

Acknowledgment

본 연구는 미래창조과학부 및 정보통신산업진흥원의 대학 ICT연구센터육성지원사업의 연구결과로 수행되었음 (NIPA-2014-H0301-14-1010)

참 고 문 헌

[1] 미래창조과학부, "사물인터넷기본계획," (http://www.msip.go.kr/)

[2] Erin Anzelmo, et. al., "Discussion Paper on the Internet of Things," commissioned by the Institute for Internet and Society, Berlin Oct. 2011. (http://www.theinternetofthings.eu/)

[3] R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafaqh, K. Wehrle, "6LoWPAN fragmentation attacks and mitigation mechanisms," In Proc. of ACM WiSec, 2013.

[4] K. Hartke, "Practical Issues with Datagram Transport Layer Security in Constrained Environments,"IETF draft, Apr. 8, 2014.

[5] Z. Shelby, et. al., "The Constrained Application Protocol," IETF RFC7252, June 2014.

[6] IETF Constrained RESTful Environments (core) Working Group. (http://datatracker.ietf.org/wg/core/)

[7] C. Bormann, et. al., "Terminology for Constrained-Node Networks," IETF RFC7228, May 2014.

[8] P. Wouters, et. al., "Using Raw Public Keys in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS),"IETF RFC7250, June. 2014.

[9] H. Tschofenig, "Smart Object Security: Considerations for Transport Layer Security Implementations," In Proc, SMART OBJECT SECURITY Workshop, Paris, FRANCE, Mar., 2012

[10] Tinydtls Documentation. (http://tinydtls.sourceforge.net/)

[11] R. Shahid, et. al., "6LoWPAN compressed DTLS for CoAP." Proc. of Distributed Computing in Sensor Systems (DCOSS), IEEE. 2012.

[12] R. Hummen, "Towards viable certificate-based authentication for the internet of things,"Proc.of HotWiSec13, ACM, 2013.

[13] IETF DTLS In Constrained Environments Working Group. (http://datatracker.ietf.org/wg/dice/)

[14] S. Gerdes, "Actors in the ACE Architecture," IETF draft, July. 2014.

약 력

강 남 희

1999년 숭실대학교 공학사
2001년 숭실대학교 공학석사
2004년 Siegen대학교(독) 공학박사
2005년~2006년 다산네트웍스 UT연구센터 선임연구원
2009년~현재 덕성여자대학교 디지털미디어학과 조교수
관심분야: 유무선 네트워크(QoS, Mobility), 시스템/인터넷 보안