안전한 사물인터넷 통신을 위한 IETF 표준기술 동향

박지예, 강남희*
University of Duisburg-Essen, 덕성여자대학교*

요 약

사물인터넷(IoT: Internet of Things)은 사물과 사물, 사물과 사람이 인터넷을 기반으로 상호 연결되어 유기적으로 교환되는 데이터를 기반으로 다양한 스마트 서비스를 제공할 수 있게 하는 촉망받는 차세대 패러다임이다. 세계적으로 사물인터넷 기술을 이용한 스마트 어플리케이션에 대한 관심이 높아지고 있고, 실제 사물인터넷 기술을 실 생활에 적용하기 위한 다양한 연구가 진행되고 있다. 사물인터넷에 대한 높은 관심만큼 보안에 대한 우려 또한 높아지고 있으며, 사물인터넷의 성공적인 서비스 정착을 위해서는 사용자와 서비스 제공자 모두가 만족할 수 있는 보안방안이 제공 되어야 한다. 이에 본 고에서는 국제 표준기구인 IETF 표준을 중심으로 사물인터넷 환경에서 고려해야 하는 보안 이슈를 다루고 관련된 표준 보안 기술 동향을 소개한다.

I. 서 론

현재 사용되고있는 일반적인 모바일 휴대폰, 태블릿, 컴퓨터를 넘어서 일상생활에서 사용되는 모든 물건을 인터넷에 연결하고자 하는 사물인터넷은 우리 생활을 크게 변화시킬 차세대 핵심 IT 기술이다. 이에 에릭슨-엘지의 스마트 미터링서비스, IoT 데이터 분석 솔루션, 필립스의 IoT 전구등과 같은 스마트 장치, 시스코의 IoT 플랫폼 등과 같이 수많은 기업들이 기존에 제공하고 있던 서비스를 사물인터넷 서비스로 확장하거나, 새롭게 만들어 사물인터넷 산업 리더로써 기술을 견인하기 위해 다양한 연구를 진행하고 있다.

사물인터넷 환경에서는 단순히 컴퓨터, 모바일 외에 일상생활에서 사용되는 일상의 사물들이 인터넷에 연결된다. 이를 통해 수집된 데이터는 클라우드 시스템에서 분석되고 가공되어 사용자에게 맞춤화, 자동화 된 서비스제공을 가능하게한다. 이러한 장점으로 사물인터넷은 스마트 시티, 스마트 카, 스마트 홈, 스마트 헬스케어, 스마트 그리드 등과 같은 다양한 융복합 서비스에 적용 될 수 있다. 구글의 스마트 드라이빙 카는 이미 테스트 주행중에 있고, 샌프란시스코나 인도네시아의 경우 시범적으로 스마트 LED를 가로수에 설치하여 에너지를 효율적으로 사용하고 비용을 낮추는 스마트 시티를 운영중에 있다. 사물인터넷의 실 생활 적용 사례는 점점 증가하고 있어 이는 먼 미래의 것이 아니라 근접한 미래의 삶을 변화시킬수 있는 중요한 기술이라 할 수 있다.

셀 수 없이 많은 사물이 인터넷에 연결되는 사물인터넷 개념의 특성상, 서로 다른 성능을 가지고 다양한 회사에서 만들어진 이기종 (heterogeneous) 장치들이 연결될 것이다. 이기종 장치간 원활한 통신을 위해서는 공통된 플랫폼의 제공이나 표준 통신 프로토콜의 사용이 필수적이다. 이를 위해 IETF에서는 CoRE 워킹 그룹[1]을 만들어 사물인터넷 장치를 위한 경량 통신 프로토콜인 CoAP(Constrained Application Protocol)을 표준 완료하였다.

이기종 장치 연결성의 문제를 해결하고자 하는 상기 표준 작업에도 불구하고 사물인터넷 서비스 활성화 정도가 기대에 못 미치는 이유 중 하나는 보안에 대한 우려이다. 실 예로, 커넥티드 카 시장이 점점 치열해지고있는데 반해 테슬라, 크라이슬러 등 거의 모든 회사의 자동차들이 보안에 취약하며 해킹이 가능함이 시연, 증명되고 있다. 뿐만 아니라 스마트 TV, 냉장고가 DoS 공격의 좀비 역할을 수행할 수 있고, 심장박동기와 같은 장치들이 해킹에 의해 작동이 중지되는 등의 침해 사례는 더 이상 새롭지 않다. 사람의 생명과 직접적으로 관련된 IoT 보안에 대한 위협은 기존 인터넷 환경에서 단순히 정보 유출과 같은 문제로 대두되었던 보안 위협과는 비교도 안될 큰 위협으로 사물인터넷이 활성화 되는데에 큰 걸림돌이 되고 있다.

하드웨어 기술의 발전으로 낮은 가격으로도 보다 성능이 나은 장치를 구입 할 수 있게 되었지만 모바일이나 태블릿과 같이 기존 인터넷에 연결되어있던 장치에 비하면 여전히 성능이 부족하다. 따라서 비대칭키의 연산이나, 인증서의 사용과 같은 방안이 메모리와 CPU, 배터리와 같은 자원이 경량화 되어

* 교신저자(kang@duksung.ac.kr)

있는 장치에는 부담이 될 수 있어 장치의 컴퓨팅 자원 제약성을 고려한 보안 방안이 요구된다. 대부분의 사물인터넷 장치들은 IEEE 802.15.4과 같은 저전력 네트워크 환경을 기반으로 통신하기 때문에 큰 패킷사이즈를 갖는 메시지가 전송되는 경우 작은 MTU크기에 맞게 다수의 프레임들로 분할되어 전송되어야 한다. 특히, 전송 과정에서 하나의 조각이라도 분실되는 경우 전체가 모두 재전송 되어야 하므로 쉽게DoS 공격으로 이어져 네트워크 가용성을 저하시키는 결과를 초래할 수 있다. 따라서 IoT 보안을 위해서는 장치의 경량성 뿐만 아니라 네트워크의 제한적인 특성까지 고려한 보안 방안이 제공 되어야 한다.

본 고에서는 국제표준기구인IETF의 사물인터넷 관련 워킹 그룹에서 현재까지 논의된 사물 인터넷 보안 관련 표준화 작업에 대해 알아보고, 앞으로 추가적으로 고려되어야 할 사물인터넷 보안 이슈를 소개한다. 또한 최근 회의에서 논의 된 표준 보안 동향을 CoRE 워킹그룹과 ACE워킹그룹 중심으로 다룬다.

II. IoT 보안 관련 표준 이슈

사물인터넷은 인터넷에 연결되는 장치의 증가로 공격자에게 공격할 수 있는 장치의 수가 더 증가 된 환경임을 의미하여, 자원이 경량화 된 장치라면 보안 위협은 더욱 커진다. CoRE 워킹그룹에서는 CoAP프로토콜 제안 단계에서부터 보안을 함께 고려하여 안전한 IoT 시스템 모델을 만들고자 하였다. UDP 전송 프로토콜을 이용하는 CoAP의 특성상 DTLS 프로토콜을 CoAP 사용을 위한 필수 보안 프로토콜로 제안하였다[2]. 모든 CoAP 장치는 표준에서 정의하고 있는 네가지 모드 중 NoSec모드와 RawPublicKey 모드가 반드시 구현 되어 있어야 하며, 각각의 모드는 DTLS 통신을 위한 핸드쉐이킹 과정에서 세션키를 공유하기 위한 방법을 명시한다.

- PreSharedKey 모드: 통신 피어간 사전에 공유된 키를 기반으로 DTLS 세션을 개설. 모든 통신 피어는 1:1로 키를 공유하며 두 통신 주체 이상이 하나의 키를 가지고 있을때는 그룹멤버임을 인증하는 용도로만 사용
- RawPublicKey 모드: RFC 7250에 정의된Out-of-band 메커니즘을 기반으로 인증서에 의존적이지 않은 비대칭키를 이용하여 DTLS 세션을 개설
- Certificate 모드: RFC5280에 정의된 X.509 certificate를 기반으로 DTLS 세션을 개설하며 이 모드를 이용할 경우 장치는 root trust anchor 의 리스트를 가지고 있어야 함
- NoSec 모드 : 프로토콜 레벨의 보안이 제공되지 않으며 DTLS 또한 사용되지 않음 NoSec 모드가 사용될 경우 다른 계층의 보안 방안이 반드시 제공되어야 함

하지만DTLS프로토콜은 컴퓨팅 자원이 충분한 장치를 기준으로 만들어진 프로토콜로, 저전력 네트워크 기반으로 메시지가 전송되는 IoT환경에 그대로 적용하기에는 여러가지 문제가 있다. 이에 2013년DICE(DTLS in Constrained Environment) 워킹그룹이 승인되어 DTLS프로토콜을 자원이 제한된IoT환경에 적용하기 위해 고려해야 할 사항에 대해 연구하였다. DICE 워킹그룹은 2016년 1월에 완료된 워킹그룹으로 전환되었으며 최종적으로 TLS/DTLS가 IoT환경에서 사용되기 위한 고려사항 프로파일[3]을 표준화 하였다. 표준 문서에서는 IoT 환경에서의 보안 프로토콜 사용을 위해TLS/DTLS 표준 프로토콜 스펙을 변경하지 않을 것임을 명시하고 있다. 따라서 [4]에서 정의된 장치 분류 중, 데이터 사이즈가 10KiB이하이고, 코드사이즈가 100KiB 이하인 Class0에 해당하는 장치에서는 TLS/DTLS 기반 보안통신이 불가능하여 사용될 수 없다. 뿐만 아니라 저전력 환경에서 발생할 수 있는 패킷 분할, 분실, 재전송으로 인한 네트워크 문제는 여전히 존재한다.

1. End-to-End 보안

CoAP표준 규격에서는 큰 특징 중 하나로 프록시와 캐싱 기능을 명시하고 있다[2]. 프록싱과 캐싱은 제한된 네트워크 환경에서 성능을 향상시키고 네트워크 트래픽을 제한하며 sleeping 모드를 사용하는 장치들이 엑세스 할 수 있는 방안을 제공한다. CoAP은 6LowPANs (IPv6 over Low-Power Wireless Personal Area Networks) 에 연결된 제한된RAM과ROM 사이즈를 가지는8bit 마이크로컨트롤러 장치를 위해 설계 되었으므로 CoAP에서 명시하고 있는 프록싱과 캐싱 기능은 상기 자원 제약성을 경감시키고 효율성을 높이며 확장성을 제공하는 핵심 기능이다. 프록시의 경우 수행하는 역할에 따라 클라이언트에 의해 선택되어져 클라이언트의 요청을 대신 수행하는 Forward-Proxy, 서버측을 위한Reverse-Proxy, 확장성을 위한CoAP-to-CoAP Proxy, HTTP-CoAP간 프로토콜 매핑을 위한Cross-Proxy로 구분된다.

하지만 프록시의 사용으로 실제 데이터를 요청하고 전송받는 클라이언트-서버의 종단간 보안이 깨지게 된다. 프록시 간 DTLS 보안 통신을 하더라도 클라이언트 또는 서버로 데이터가 전달되기 위한 또다른 DTLS 세션이 필요하게 되는Hop-by-Hop커뮤케이션이 일어난다 〈그림 1〉참조. 뿐만 아니라 이 경우 두 프록시를 포함한 전체 기기가 신뢰되는 환경에서만 기밀성이 유지되는 안전한 통신을 기대할 수 있다는 한계점이 있다.

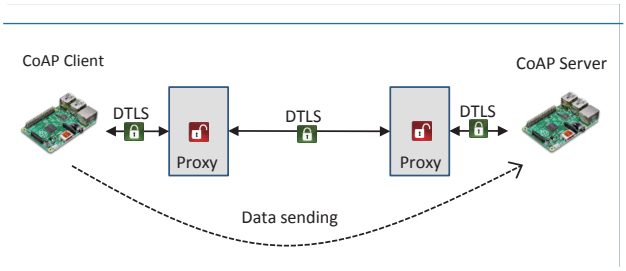


그림 1. 프록시 기능 사용시 발생하는 종단 보안 문제

종단간 보안을 위해 [5]에서는 프록시를 사용하여 종단간 보안이 깨지는 경우 발생 수 있는 공격에 대해 다음과 같이 명시하고 있다.

- Spoofing: CoAP클라이언트/서버 간 통신 시 프록시를 통하는경우 프록시에서 요청/응답이 위조되며, 위조된 경우 검증하지 못함
- Delaying: 프록시에서 의도적으로 요청/응답 전송을 지연시켜 서비스 가용성을 저하시키며, 실시간으로 전송되어야 하는 데이터의 경우 문제가 될 수 있음
- Withholding: 요청/응답을 종단으로 전송하지 않아 원활한 통신이 불가능하게 함
- Flooding: 종단 장치로 반복적인 요청/응답 전송하여 LLN(Low Power and Lossy Network) 환경에 부담을 주게 됨
- Eavesdropping: 종단 장치 간 전송되는 장치의 데이터 노출될 수 있으며, 이 경우 프록시를 이용한 통신은 프록시를 완전히 신뢰할 수 있는 경우에만 안전하게 통신할 수 있음
- Traffic Analysis: 서버로부터 전송되는 응답의 빈도, 통신 패턴을 분석하여 추가적인 정보를 얻는 공격이 가능

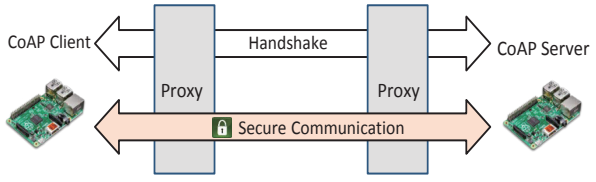


그림 2. 프록시 기능을 이용하지 않는 경우

〈그림 2〉에 나타낸 것처럼 프록시가 DTLS Handshake 과정에 관여하지 않고 단순 포워딩만 하는 경우 장치와 장치, 종단간 암호화 통신이 가능하지만 프록싱, 캐싱 등의 기능 등을 사용할 수 없어 확장성과 효율성이 크게 떨어진다.

2. 멀티캐스팅 보안

자원이 제한적인 사물인터넷 장치는 스마트 시티나 스마트 빌딩 시스템과 같은 실제 서비스에서 일정한 위치에 설치되어 서비스에 특화된 기능을 수행하는 경우가 대부분이다. 이 경우 설치된 위치에 따라, 그리고 수행하는 기능에 따라 서로 다른 그룹으로 분류하여 수많은 장치를 효율적으로 관리하고 효율적으로 데이터를 수집할 필요성이 있다. 이를 위해 CoAP기반 그룹 커뮤니케이션 기술이2014년 10월에CoRE 워킹 그룹의 Experimental RFC로 표준화되었다[6]. 표준 문서에서는 장치의 그룹을 유동적으로 정의하고 관리하기 위한 기술에 대해 명시하고 있다. 하지만 그룹 커뮤니케이션을 위한 기본 보안 방안으로 NoSec모드가 명시되어 있어 안전한 그룹 커뮤니케이션을 위해서는 DTLS나 TLS가 아닌 다른 계층의 보안 프로토콜이 반드시 사용되어야 한다.

이를 보완하기 위해 [7]에서 DTLS Record layer를 이용한 보안 그룹 커뮤니케이션 방안을 제안하였다. 제안된 방안은 그룹키를 가지고 있는 장치들이 DTLS Record 규격을 이용해 데이터를 암호화 하여 보낼 때, DTLS Record헤더 중 일련 번호(Sequence number)를 전송자를 구분하기 위한 SenderID와 일련번호로 나누어 통신에 참여하는 장치를 구분하게 하였다. 하지만 제안은DICE 워킹그룹의 공식 드래프트로 채택되지 못한채 DICE워킹그룹이 종료되었다. DICE 워킹그룹 종료 이후에도 그룹 커뮤니케이션 보안 제공을 위한 연구 필요성이 지속적으로 요구되었고 현재는 ACE워킹그룹에서 그룹커뮤니케이션 보안을 함께 다루고 있지만 아직까지 그룹커뮤니케이션을 위한 표준 보안 방안은 제공되지 않고 있다.

3. 펌웨어/소프트웨어 업데이트 관리

사물인터넷 환경에서 장치가 공공재로 사용되는 경우 서비스 제공을 위해 많은 수의 장치가 공공장소에 설치될 수 있다. 이 경우 서비스 제공 외에 장치 자체에 대한 관리의 주체가 명확하지 않아 지속적인 소프트웨어 업데이트의 부재로 인한 보안 문제가 발생 할 수 있다. 일 예로 스마트홈 서비스에 사용되는 사물인터넷 장치의 경우 구입 및 설치 이후 최소 수 년 이상 사용될 것으로 기대된다. 하지만 대부분의 사물인터넷 장치는 사용자 인터페이스가 충분하지 않아 사용자 스스로 주기적인 소프트웨어 업데이트를 통해 보안 패치를 수행하는 것이 매우 어렵다. 이미 공유기에 기본 패스워드를 사용해 공격자의 타켓이 되는 것은 아주 흔한 공격 시나리오며, 공격의 타켓이 사물인터넷 장치가 될 경우엔 직접적인 가전제품등의 조작이 가능해 더욱 큰 위협이 될 수 있다. 또한 보안 취약점이 공진 된 후 공격자는

쇼단(shodan)과 같은 장치 검색 엔진으로 취약점에 노출되는 장치들을 쉽게 찾을 수 있는 문제도 고민해야 한다.

ACE워킹그룹에 개인 드래프트로 제출된 [8]에서는 펌웨어/소프트웨어 업데이트의 경우 보안을 이유로 그룹 커뮤니케이션이 아닌 싱글 커뮤니케이션을 사용할 것을 권장하였다. 따라서 수많은 장치의 펌웨어를 안전하게 업데이트하는 효율적인 방안에 대한 연구가 요구된다. 이에2016년 5월 IAB(Internet Architecture Board)가 주관하는 IoTSU(Internet of Things Software Update) 워크샵에서 소프트업데이트를 위한 프로토콜 매커니즘, 안전한 업데이트를 위한 방안 등이 논의 되었으나, 아직 IETF 표준 워킹그룹에서는 소프트웨어 업데이트에 대한 내용이 다뤄지지 않고 있다.

III. IoT 보안을 위한 IETF 표준 기술

IETF에서는 사물인터넷을 인터넷에 연결하기위해 필요한 관련 기술을 각 계층별로 세분화 하여 워킹그룹을 운영하고 있다. CoRE워킹그룹은 어플리케이션 계층을 중심으로 프로토콜 포맷 정의, 장치 디스커버리와 같은 기술을 표준화 하고있다, 이밖에 6lo, 6tisch워킹 그룹은 IP계층을 중심으로 저전력 네트워크 구성을 위해 필요한 기술을 연구하고 표준화 하고 있다. LWIG 워킹그룹의 경우 구현 시 고려해야할 사항에 대한 가이드를 제공하고 있으며, ACE워킹그룹에서는과 인증과 권한관리, 기타 보안 사항에 대한 기술들을 다루고 있다. IRTF의 T2T리서치 그룹에서는 사물인터넷을 현실화 하기 위한 연구를 진행하고 있으며 W3C의 WoT 인터넷그룹과 데모를 시연 등 PlugREST를 함께 진행하고 있다. 최근 IETF 회의에서는 광대역 저전력 네트워크에 대한 필요성 대두로, LPWAN(IPv6 over Low-Power Wide Area netowks) BoF가 열려 LoRa, SIGFOX의 사용에 대한 논의가 이루어졌다. 본 장에서는IETF에서 논의되고 있는 표준 보안 기술을 중심으로 살펴본다.

1. CoAP 관련 보안 표준 동향

CoRE워킹 그룹에서는 링크 포맷에 대한 표준화를 시작으로 CoAP 의 표준화, 장치를 지속적으로 관찰(Observating)하기 위한 기술을 표준화 하였다[9]. 최근에는 펌웨어 업데이트와 같이 큰 사이즈의 데이터가 전송되어야 하는 경우 IP 계층에서의 분할(Fragmentation)에 의존하지 않고 CoAP에 정의 되어있는 Block옵션을 확장하여 블록단위로 데이터를 전송하고자 하는 방안(Block wise transferring)에 대한 기술을 표준 완료하였다[10].

올해 7월 독일 베를린에서 개최된 IETF 96 회의에서는 CoAP을 위한 메시지 전송 포맷과 인코딩 규칙에 관한 논의가 함께 이루어졌다. 회의에서 관심을 받은 CBOR(Concise Binary Object Representation)는 작은 코드 사이즈와 작은 메세지 사이즈를 가지는 데이터 포맷으로 2013년에 표준화 작업이 완료되었다[11]. CBOR는 JSON이나 XML보다 자원제한적인 IoT환경에 더 적합한 메세지 포맷으로 고려되고 있다. 이에JSON-JOSE와 같은 형식으로 CBOR을 위한 보안을 제공하기 위한 목적으로COSE(CBOR Object Signing and Encryption) 워킹그룹이2015년에 승인되었다[12]. COSE워킹그룹은 에서는CBOR 객체에 대한 사인(signing)과 암호화(Encryption)에 대한 명세를 정의하고있다. 현재 이에 대한 공식 드래프트가 COSE워킹그룹에서 다루어지고 있으며, 2016년 9월 진행된 T2T리서치그룹 미팅에서COSE관련 표준화 논의는 드래프트 주제에 따라 추후 CoRE워킹 그룹과 ACE워킹그룹으로 나뉘어져 다뤄질 것으로 논의 되었다.

또한 회의에서는 프록시가 사용되는 환경에서 종단간 보안이 깨지는 문제를 해결하기 위해 OSCOAP(Object Security of CoAP)[13]이 CoRE워킹그룹 세션에서 발표 되었다. OSCOAP은 COSE를 기반으로 어플리케이션 계층에서 보안을 제공하기 위한 방안으로 End-to-End보안, 무결성과 CoAP 페이로드에 대한 재전송 공격에 대한 해결책을 제공한다.

그림 3. OSCOAP기반 통신

OSCOAP은 CoAP의 옵션필드에 object security를 추가하여 OSCOAP으로 암호화 된 데이터임을 알린다. 또한 DTLS 사용되는 Key block과 같은 개념을 가지는 Security Context를 사용하여 데이터를 암호화 하고 무결성을 제공한다. OSCOAP은 여러가지 암호화 방안을 제공하는 COSE와는 달리, OSCOAP에서는 AES-CCM만을 사용하여 암호화, 무결성을 제공한다. 프록시에서 제공하는 기능을 이용함과 동시에 종단간 보안을 제공하기 위해 제안된 OSCOAP은 세션 발표에서 다수의 콜을 받았지만 아직까지 공식 드래프트로 채택 되지 않고 있다.

2. ACE WG 표준 기술 동향

ACE(Authentication and Authorization for Constrained Environments) WG은 2014년 정식 워킹그룹으로 승인되어 DICE워킹그룹에서 다뤄지지 않았던 인증과 자원접근에 대한 권한관리에 대한 문제를 해결하고 표준화하는 작업을 진행하고 있다[14]. 사물인터넷 환경에서 가능한 여러가지 서비스 시나리오를 정의하고 그에 따른 권한관리, 인증관리에대한 요구사항을 정리한 informational RFC은 최근 2016년 1월에 최종 업데이트 되었다[15].

ACE의 공식 드래프트로 다뤄지고 있는 [16]에서는 메모리 사이즈, 프로세싱 성능, 유저 인터페이스, 파워와 통신 대역 등이 제한되어있는 제한된 네트워크[4]에서 발생하는 문제를 정의하고 인증과 접근 권한 관리를 하기 위한 네트워크 구조 〈그림 4〉와 필요한 장치 요소, 용어를 정리하였다.

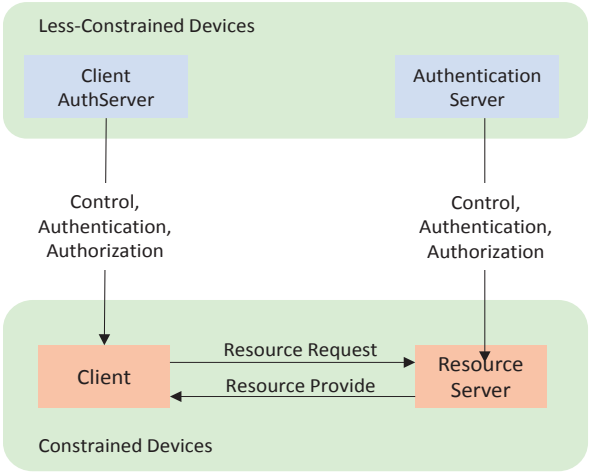


그림 4. 제안 네트워크 구조

최근 진행된 ACE 워킹 그룹 회의에서는 CWT(CBORE Web Token)[17]의 구현 이슈와OSCOAP 프로파일에 관한 발표가 있었다. CWT는 OAuth 2.0이나 OpenID에서 이미 사용되고 있는 표준화된 보안 토큰인JWT(JSON Web Token)와 유사한 개념으로JSON 포맷대신 CBOR 포맷을 이용한다는 차이를 가진다. CWT은 현재 표준 드래프트 작업중인 ACE Framework의 OAuth 2.0에서 사용될 수 있으며 토큰 자체의 보안은 COSE보안에 의존한다.

이와 더불어 ACE Framework에서 OSCOAP을 사용하기 위한 기술, EDHOC(Ephemeral Diffie-Hellman Over COSE)에 대한 논의가 이루어졌다.

IV. 결 론

본 고에서는 IETF 표준을 중심으로 완료된 표준작업에 대해 살펴보고, 여전히 남아있는 보안 이슈들에 대해 살펴보았다. IETF 표준 기구에서는 DTLS 에대한 프로파일 표준화 작업 이후 COSE를 기반으로 한 어플리케이션 계층의 보안에 대한 논의가 이루어지고 있다.

Acknowledgment

본 연구는 2016년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업 (No.2014R1A1A2056961)의 연구결과로 수행되었음.

참 고 문 헌

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

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

[3] H. Tschofenig, et. al., "Transport Layer Security (TLS) /Datagram Transport Layer Security (DTLS) Profiles for the Internet of Things," IETF RFC 7925, July 2016

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

[5] G. Selander, et. al., "Requirements for CoAP End-To-End Security," IETF draft, July 6, 2016

[6] A. Rahman, et. al., "Group Communication for the Constrained Application Protocol (CoAP)," IETF RFC 7390, October, 2014

[7] S. Keoh, et. al., "DTLS-based Multicast Security in Constrained Environments," IETF draft, July 03, 2014

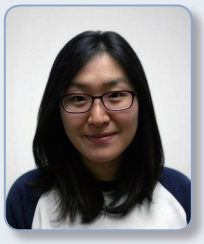
[8] A. Somaraju, et. al., "Security for Low-Latency Group Communication," IETF draft, January 15, 2016

[9] K. Hartke, "Observing Resources in the Constrained Application Protocol (CoAP)," IETF RFC 7641, September, 2015

[10] C. Bormann, et. al., "Block-Wise Transfers in the Constrained Application Protocol (CoAP)," IETF RFC 7959, August, 2016

[11] C. Bormann, et. al., "Concise Binary Object Representation (CBOR)," IETF RFC 7049, October 2013
[12] CBORE Object Signing and Encryption (COSE) Working Group. (http://datatracker.ietf.org/wg/cose/)
[13] G. Selander, et. al., "Object Security of CoAP (OSCOAP)," IETF draft, October 11, 2016
[14] Authentication and Authorization for Constrained Environments (ace) Working Group. (http://datatracker.ietf.org/wg/ace/)
[15] L. Seitz, et. al., "Use Cases for Authentication and Authorization," IETF RFC 7744, January 2016
[16] S. Gerdes, et, al., "An architecture for authorization in constrained environments," IETF draft, August 31, 2016
[17] E. Wahlstroem, et, al., "CBOR Web Token (CWT)," IETF draft, July 7, 2016

약 력



박 지 예

2013년 덕성여자대학교 공학사
2015년 덕성여자대학교 공학석사
2016년~현재 Duisburg-Essen대학(독) 박사과정
관심분야: 사물인터넷 보안, 표준 프로토콜, 유무선 네트워크

강 남 희

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