해외 표준화기구 동향

TTA 표준화본부 표준기획단

1. 국제표준화기구의 최근 동향

1.1 국제전기통신연합(ITU)

1.1.1 ITU, 패스워드 보안 한계를 극복하는 2개의 표준 승인[1]

2018년 12월 18일, ITU-T SG17(Security)은 패스워드 기반 보안 인증의 한계를 극복하기 위해 두 가지의 새로운 국제표준을 승인하였다. 이는 모바일 기기와 웹 사용자를 인증하기 위해 외부 인증자(external authenticator)를 사용하고 모바일 기기에서 생체 인증을 처리 가능하게 하는 국제표준이다.

두 가지 새로운 국제표준은 FIDO Alliance에 의해 제출된 것으로 FIDO Alliance는 패스워드나 원타임패스워드(OTP)보다 사용성이 편리하고 인증성이 강력한 공개키 암호 기반의 개방형(Open) 표준을 통해 온라인 인증을 개선하기 위한 작업을 중점 추진하고 있다.

FIDO UAF(FIDO Universal Authentication Framework, FIDO 범용인증프레임워크)와 ITU X.1277은 모바일 기기에서 고급 생체 인증을 지원하며, CTAP(Client To Authenticator Protocol/Universal 2-factor framework, 클라이언트 인증 프로토콜/범용 2-요소 프레임워크)와 ITU X.1278은 FIDO 보안 키, 모바일 기기와 같은 외부 인증자가 USB(Universal Serial Bus, 범용직렬버스), NFC(Near-field communication, 근거리통신)를 통해 웹 사용자를 인증한다.

2. 지역 및 국가별 표준화기구 동향

2.1 유럽

2.1.1 ETSI, 차세대 IP 프로토콜에 대한 규격 및 보고서 발표[2]

2018년 11월 27일, ETSI 차세대 프로토콜(NGP, Next Generation Protocol), 산업규격그룹(ISG, Industry Specification Group)은 차

* TTA는 해외 표준화기구의 최신 동향을 조사하여 주간/월간으로 '해외 ICT 표준화 동향 정보'를 제공하고 있습니다. 본 원고는 2018년 11월 말부터 2019년 1월 초까지 게재한 정보를 요약 정리하였습니다.

세대 IP 프로토콜과 관련된 새로운 규격(GS, Goup Specification) 및 보고서(GR, Group Report)를 발표하였다.

이 보고서는 네트워크 슬라이싱 또는 초고신뢰 저지연 통신(URLLC, Ultra-reliable Low Latency Communication)과 같이 5G에 제안된 새로운 서비스의 성능, 효율성 및 확장성을 최적화하기 위한 내용을 담고 있으며 각 보고서의 구체적인 내용은 다음과 같다.

- **ETSI GS NGP 013**: 사용자 평면, 패킷 형식과 전달 메커니즘에서 효율적인 결정적 패킷 전달(Flexilink: an efficient deterministic packet forwarding in user plane as well as packet formats and forwarding mechanisms), ETSI GS NGP 012[i.3]에 문서화된 요구 사항과 GR NGP 003[i.2]과 같은 ETSI의 기술을 기반으로 5G 코어 및 액세스 네트워크에 대한 사용자 평면 패킷 형식과 라우팅 메커니즘을 지정한다.
- **ETSI GR NGP 010 v1.1.1**: 새로운 전송 기술에 대한 권장사항(Recommendation for New Transport Technologies), 5G와 그 이상의 차세대 아키텍처와 관련된 새로운 전송 기술에 중점을 두고 있으며, 슬라이싱을 구현하는 고급 기능과 메커니즘에 대해 설명하고 보안 고려 사항을 다루고 있다.
- **ETSI GR NGP 011**: 앤드 투 앤드 네트워크 슬라이싱 참조 프레임워크 및 정보 모델(E2E Network Slicing Reference Framework and Information Model), 여러 관리 및 기술 영역에서 자원 보장 멀티테넌시(Multi-tenancy)를 제공하기 위해 네트워크 조각(Slice)에서 사용하는 리소스의 정보 규격을 설명한다.

2.1.2 ETSI, 사이버대응을 위한 보안통제 기술보고서 발표[3]

2018년 11월 5일, ETSI CYBER TC(Technical Committee, 기술위원회)는 eTLS(enterprise Transport Layer Security, 기업 전송계층 보안)로 알려진 중간장비(middlebox) 보안 프로토콜 규격(ETSI TS 103 523-3 v1.1.1. profile for enterprise network and data centre access control)을 발표하였다고 보도하였다.

이 기술 규격은 TLS 1.3 버전의 특정키 교환 방식에 대한 변경을 반영하고 있다. 수동으로 TLS 1.3 세션의 암호를 해독할 수 있는 방법 중 하나는 각 TLS 세션에 대해 생성된 임시키를 중간장비로 보내는 것이지만, 이러한 접근방식의 개선사항이 요구되어 eTLS는 여러 세션에서 재사용되는 수명이 긴 정적 Diffie-Hellman(디피-헬먼)키를 사용한다. 이는 키를 실시간 해독하여 중간장비에 미리 배포할 수 있으므로 저장 및 암호화된 패킷 저장 시스템과 관련된 키 수를 크게 줄일 수 있다. 또한, 세션의 수동 암호 해독이 필요한 운영 환경에서는 이러한 사용 사례를 지원하는 키 교환 메시지와 연결 인증서를 사용하여 최종 사용자에게 공개 정보를 전달한다.

eTLS를 통해 데이터 센터 및 엔터프라이즈 네트워크 운영자는 서비스 계약 및 법적 의무를 준수할 수 있으며 데이터에 접근하는 대상이 누구인지 알 수 있도록 보호할 수 있다.

2.1.3 ETSI, 블록체인 관련 새로운 산업 규격그룹(ISG PDL) 신설 발표[4]

2018년 12월 18일, ETSI는 블록체인 기술의 핵심요소인 PDL(Permissioned Distributed Ledgers, 허가형 분산원장)에 대한 새로운 ISG(Industry Specification Group, 산업규격그룹) 신설을 발표하였다.

ISG PDL은 다양한 산업과 정부 기관들이 참여하여 인터페이스, APIs, 프로토콜 및 정보, 데이터 모델 등을 포함하여 PDL 운영을 위한 기능, 비즈니스 사용 사례, 아키텍처 및 솔루션과

관련된 과제를 작업할 계획이며, 1차 킥오프 회의는 2019년 1월 24일 마드리드에서 개최될 예정이다.

2.2 미국

2.2.1 ATSI, CBRS 얼라이언스와 3.5GHz CBRS 밴드 상용화 협력키로[5]

2018년 12월 18일, ATIS(Alliance for Telecommunications Industry Solutions)는 CBRS(Citizens Broadband Radio Service, 민간광대역무선서비스) 얼라이언스와 3.5GHz CBRS 대역의 상용화를 협력(Liaison)하기로 하였다.*

* 비면허대역과 더불어 공유대역에 대한 관심이 높아지면서 FCC(미국연방통신위원회)는 3.5GHz 주변 150MHz 공유대역을 CBRS로 할당하였으며, 이 주파수 대역에서 LTE 기반 기술을 전개하기 위해 CBRS 얼라이언스가 출범하였다.

ATIS와 CBRS는 IMSI(International Mobile Subscriber Identity, 국제이동국 식별번호), HNI(Home Network Identity, 가입자네트워크 식별번호), 우선순위 서비스(Priority Services) 및 무선 접속망(Radio Access Networks)과 같은 CBRS 얼라이언스와 ATIS 솔루션 간의 기술 연동에 중점을 둘 예정이며, ATIS는 이번 협약의 일환으로 3.5GHz CBRS 대역 내에서 HNI 이니셔티브의 파트너로 참여할 예정이다.

전통적으로 HNI는 모바일 가입자의 홈 네트워크를 식별하고 국제 로밍 기능을 갖춘 모바일 네트워크 사업자에게 할당할 수 있지만, 3,550~3,700MHz 대역은 독점적인 용도가 아니기 때문에 일부 사용자는 FCC 주파수 면허를 받지 않는 대신 사용자는 인증을 받은 기지국을 사용하며, ATIS의 IMSI IOC(IMSI Oversight Council, 감독위원회)는 3.5GHz CBRS 대역 내 사용자에게 IMSI 블록을 할당하는 전략을 도출하였고, 3.5GHz 대역 내에서 공유된 HNI는 CBRS 작업을 식별하여 HNI 자원을 보존하는 데 사용되고 있다.

2.2.2 ANSI, 무인항공기 시스템에 대한 표준화 로드맵 발표[6]

2018년 12월 20일, ANSI(American National Standards Institue, 미국표준협회)는 UAS(Unmanned Aircraft Systems, 무인항공기 시스템)에 대한 표준화 로드맵을 발표하였다.

같은해 9월, ANSI는 UASSC(Unmanned Aircraft Systems Standardization Collaborative, 무인 항공기 시스템 표준화 협업)에 의해 개발 중인 무인 항공기 시스템 표준화 로드맵(Version 1.0)의 초안을 공개하였고 공개 검토 의견을 요청한 바 있다.

UASSC는 UAS를 미국의 영공 시스템에 안전하게 통합하는데 필요한 표준 및 적합성 평가 프로그램의 개발을 조정하고 가속화하기 위해 설립되었으며, FAA(Federal Aviation Administration, 연방항공국), 미국연방정부기관, SDOs(Standards Developing Organizations, 표준개발기구), 산업계, 학계 등을 포함하여 175개 공공 및 민간기관의 300명 이상의 사람들이 이 로드맵의 문서 개발을 적극 지원하였다.

이 로드맵은 지난 15개월 동안 UASSC의 4개 WG에서 해당 표준화 기구의 기존 표준 및 개발 중인 표준 사이의 격차를 파악하여 사전 표준화 R&D 등 추가적인 표준화 필요성이 있는 우선순위 영역에 대한 권장사항을 만들기 위한 현황을

제공하고 있다.

UASSC WG에서 다루고 있는 내용은 다음과 같다.

- **WG1**-감항성(Airworthiness): 항공기 시스템과 GCS와의 통신을 다룸(Covers aircraft systems and communications with the Ground Control Station)
- **WG2**-항공 운항과 인사 자격(Flight Operations and Personnel Qualifications): 일반적인 비행 계획, 운항 고려사항, 개인 훈련, 인사 자격, 자격표준을 다룸(Covers general flight planning and operational concerns, plus Personnel training, qualifications, and certification standards)
- **WG3**-중요한 인프라 구조와 환경(Critical Infrastructure and Environment): 수직, 선형 및 광역 환경 인프라 검사, 정밀 농업 및 상업용 패키지 배송에 대한 운영 고려사항을 다룸(Cover specific operational concerns for vertical, linear, and wide area environment infrastructure inspections, precision agriculture, and commercial package delivery)
- **WG4**-응급 및 의료적 조치(Emergency and Medical Response): 공공 안전 작업 수행을 위한 운영상의 고려사항을 다룸(Covers specific operational concerns for conducting public safety operations)

2.3 중국

2.3.1 중국, 지능형 네트워크 차량 산업 행동계획(Action Plan) 발표[7]

2018년 12월 28일, 중국 공업정보화부(MIIT, Ministry of Industry and Information Technology)는 다음과 같은 내용의 지능형 네트워크 차량(Intelligent Networked Vehicles)산업 행동계획(Action Plan)을 발표하였다.

① 지능형 네트워크 차량의 시스템 개발 및 적용을 가속화하고 지능형 네트워크 차량의 의사 결정 제어 플랫폼 구축

② 차량 인터넷의 핵심 표준 개발, 주파수 라이선스 발급 개선, 지능형 네트워크 테스트 및 평가 시스템을 구축하는 등 표준 시스템을 개선하여 테스트 검증과 애플리케이션 구현

③ LTE-V2X와 5G-V2X 같은 무선 통신 기술을 기반으로 네트워크 인프라를 구축하여 자동차 네트워킹 산업 인프라 촉진

④ 스마트여행과 같은 혁신적인 응용 프로그램을 개발, 전기 자동차 실시간 온라인 모니터링 시스템 개발, 교통안전을 위한 협업 애플리케이션 제어 기술 등 애플리케이션 개발과 시장 침투

⑤ 보안 시스템의 개선을 위해 기술과 기술의 결합

중국은 행동계획을 통해 적극적인 혁신·안전 및 신뢰성·그리고 강력한 경쟁력을 바탕으로 산업 간 협력을 강화하고, 행동계획의 실행을 통해 산업 기반을 통합하여 차량 네트워크 산업의 새로운 생태계를 형성할 계획을 밝혔다.

3. 사실표준화 기구 동향

3.1 IEEE, 네트워크 기반 공존 방식 표준 발표[8]

2018년 11월 28일, IEEE는 2018년 6월에 개발된 IEEE 802.19.1TM-2018: Wireless Network Coexistence Methods(무선 네트워크 공존 방식) 표준을 발표하였다.

이 표준은 비슷하지 않거나 독립적으로 운영되는 네트워크 간의 네트워크 기반 공존을 위해 무선 기술에 독립적인 방법을 지정하며, TV 대역 유휴 채널(TVWS, TV band White Spaces), 5GHz 비면허 대역 및 3.5GHz 사설 광대역망 서비스(CBRS, Citizens Broadband Radio Service) 간이면허 대역과 같은 일반적인 승인하에 작동하는 지리적 위치 인식 장치에 대해 정의하고 있다.

IEEE 802® 계열의 무선 표준은 일반 승인 하에 유사하지 않거나 독립적으로 운영되는 무선 네트워크 간의 표준화된 공존 방식을 제공함으로써 비면허 또는 간이면허(lightly licensed) 장치의 효과적인 활용을 가능하게 한다.

이 표준은 지리적 위치 인식과 정보 데이터베이스 접근을 포함하는 비면허 기기의 인지 무선 기능 활용 방법, 무선 네트워크 공존 정보를 수집하고 제공하기 위한 공존 발견 및 정보 서버, 다양한 시나리오는 물론 공통 공존 아키텍처와 프로토콜에서 공존 시스템의 비용 효율적이고 유연한 배포를 가능하게 하는 프로필 제공 등의 내용을 다루고 있다.

IEEE 802.19.1™ 표준은 공정하고 효율적인 스펙트럼 공유를 보장하는 데 도움이 될 것으로 기대한다.

3.2 IEEE, 프론트홀을 위한 시간 - 민감형 네트워킹 프로파일 표준 발표[9]

2018년 11월 29일, IEEE는 근거리 통신망(LAN, Local Area Network)과 도시 통신망(MAN, Metropolitan Area Network)에서의 프론트홀을 위한 시간-민감형 네트워킹 기술을 정의하는 표준(IEEE 802.1CM™-2018—IEEE Standard for Local and metropolitan area networks—Time-Sensitive Networking for Fronthaul)을 발표하였다.

시간-민감형 네트워킹(TSN, Time-Sensitive Networking)은 이더넷(Ethernet)/브리지(Bridge) 기반의 L2(Layer 2) 네트워크를 통해 확정형 지연(deterministic latency) 및 무손실(zero packet loss) 특성을 요구하는 서비스를 제공하기 위한 기술이다.

이 새로운 표준은 특히 이더넷/브리지 기술 기반의 패킷 네트워크를 통해 이동 통신의 무선 장비(RE, Radio Equipment)와 컨트롤러(REC, Radio Equipment Control) 간을 연결하기 위해 개발된 최초의 IEEE 표준이다.

이 표준은 시간에 민감한 프론트홀 스트림을 전송할 수 있는 네트워크를 구축하는 데 필요한 브리지, 스테이션 및 LAN의 기능, 옵션, 구성, 기본값, 프로토콜 및 절차를 선택하는 프로파일을 정의하며, IEEE 802.1CM™은 기존 CPRI 및 최근 발표된 이더넷 기반 프론트홀을 위한 eCPRI 규격과 같은 프론트홀 인터페이스를 지원한다.

[참고문헌]

[1] https://news.itu.int/new-itu-standards-to-overcome-the-security-limitations-of-passwords/

[2] https://www.etsi.org/news-events/news/1361-etsi-releases-specification-and-reports-on-next-generation-ip-protocols

[3] https://www.etsi.org/news-events/news/1358-2018-11-press-etsi-releases-standards-for-enterprise-security-and-data-centre-management

[4] https://www.etsi.org/news-events/news/1369-2018-12-press-etsi-launches-new-industry-specification-group-on-blockchain

[5] https://sites.atis.org/insights/cbrs-alliance-and-atis-enter-liaison-agreement-to-advance-commercialization-of-the-35-ghz-cbrs-band/

[6] https://www.ansi.org/news_publications/news_story?menuid=7&articleid=58757077-aeb7-4554-b359-4aa34ae8881d

[7] http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057497/n3057503/c6565712/content.html

[8] https://standards.ieee.org/news/2018/ieee-publishes-standard-for-network-basedcoexistence-methods.html

[9] https://standards.ieee.org/news/2018/ieee-publishes-802_1cm-2018.html