1917호
2019.10.09.
ISSN 1225-6447

Weekly ICT Trends

주간기술동향

IITP 정보통신기획평가원

- 「주간기술동향」은 **과학기술정보통신부** 「ICT 동향분석 및 정책지원」 과제의 일환으로 정보통신기획평가원(IITP)에서 발간하고 있습니다.
- 「주간기술동향」은 인터넷(http://www.itfind.or.kr)을 통해 서비스를 이용할 수 있으며, 본 고의 내용은 필자의 주관적인 의견으로 IITP의 공식적인 입장이 아님을 밝힙니다.
- 정보통신기획평가원의 「주간기술동향」 저작물은 공공누리 "출처표시-상업적 이용금지" 조건에 따라 이용할 수 있습니다. 즉, 공공누리의 제2유형에 따라 상업적 이용은 금지하나, "별도의 이용 허락"을 받은 경우에는 가능하오니 이용하실 때 공공누리 출처표시 지침을 참조하시기 바랍니다.
  (http://www.kogl.or.kr/info/license.do 참고)

  예시) "본 저작물은 'OOO(기관명)'에서 'OO년' 작성하여 공공누리 제O유형으로 개방한 '저작물명(작성자:OOO)'을 이용하였으며, 해당 저작물은 'OOO(기관명), OOO(홈페이지 주소)'에서 무료로 다운받으실 수 있습니다."

Weekly ICT Trends

주간기술동향

1917호

ISSN 1225-6447

chapter 1

5G 네트워크 기술 진화에 따른 보안 이슈와 사이버대응 기술의 고려사항

김환국 ‖ 한국인터넷진흥원 팀장
최보민 ‖ 한국인터넷진흥원 선임연구원
박성민 ‖ 한국인터넷진흥원 책임연구원
심원태 ‖ 한국인터넷진흥원 본부장

2019년 4월, 4세대 이동통신보다 최대 20배 빠른 속도, 10배 많은 IoT 기기의 연결, 10배 짧은 저지연 서비스를 제공하기 위해 5G세대 이동통신이 세계최초로 상용화되었다. 5G 모바일 네트워크에서는 기존 음성 및 데이터 통신을 제공할 뿐만 아니라 지연 속도와 신뢰성에 민감한 IoT 기기를 수용하기 위해 다양한 최신 기술을 적용하는 기술적 진보가 있었다. 그러나 5G 네트워크 및 서비스가 개방성, 확장성, 유연성을 제공하기 위해 채택한 분산화 코어 네트워크 구조와 소프트웨어기반 아키텍처(SDN·NFV, MEC, 클라우드 컴퓨팅 등)로의 기술적 변화는 새로운 공격 접근 경로와 논리적인 보안 가시성과 복잡성 이슈 등의 사이버보안 상의 새로운 도전(Challenges)이 되고 있다. 이에 본 고에서는 사이버보안 관점에서 5G 모바일 네트워크의 기술적 변화에 따른 보안위협과 5G 보안 아키텍처 연구동향을 통해 5G 보안기술 설계 요구사항을 고찰하고자 한다.

I. 서론

5G 네트워크 기술은 3GPP(The 3rd Generation Partnership Project) 표준화기구

* 본 내용은 김환국 팀장(☎ 061-820-1272, rinyfeel@kisa.or.kr)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.
***이 논문은 2019년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No.2019-0-00793, 국가기간망 사이버공격 사전예방을 위한 지능형 5G 코어망 비정상 공격 탐지 및 대응 기술개발)

OPEN 출처표시 상업용금지 공공누리 공공저작물 자유이용허락

에서 제정된 5세대 무선통신 표준기술로서 ITU에서 정의하는 정식명칭은 IMT-2020이다. 3GPP는 모바일 트래픽 양 증가, 사물 디바이스 수 증가에 대응하기 위해 2010년부터 5G 기술 표준화를 추진하였다. 표준화 로드맵 상 현재 1차 표준화(Release 15)가 완료되어 4G 기술과 일부 5G 기술이 적용된 eMBB 서비스 중심의 NSA(Non Standalone, 단말기와 기지국은 5G 기술, 코어 네트워크는 4G EPC 코어망 연결) 구조 방식의 상용 서비스가 개시되었고, uRLLC와 mMTC 서비스를 반영하기 위한 SA(Standalone) 구조 방식의 2차 표준화(Release 16)가 2019년 말 표준 제정을 목표로 진행 중에 있다[1].

이동통신 기술의 진화 관점에서 살펴보면 4세대 이동통신까지는 스마트폰을 중심으로 무선 전송 속도와 대용량 성능 향상에 초점을 두어 발전해 왔다[2]. 한편, 5세대 이동통신 기술은 AI, 자율주행차 등 초연결 사회 구현을 위해 다양한 IoT 기기(Massive IoT·Mission Critical IoT)의 특성과 서비스 요구사항을 수용할 수 있는 모바일 네트워크 환경 구축에 초점을 두어 기술적 진보가 진행되고 있다[3]. 즉, 데이터 송·수신 용량과 속도 관점에서 유·무선 간 차이가 없을 정도의 빨라진 “이동통신 환경”을 제공하여 스마트폰뿐만 아니라 AR, VR, 드론 등 새로운 기기를 통해 4K·8K 및 AR/VR 등 실감형 멀티미디어 콘텐츠들을 제공하고, IoT 기기 사용에 있어 저전력으로 동작하는 많은 기기들이 접속하는 환경에서도 서비스의 안정성을 보장하는 “IoT 통신 환경”을 본격적으로 구현할 수 있다[3].

ITU-R에서는 5G 이동통신 기술의 3대 서비스로 [표1]과 같이 속도, 대역폭, 지연시간 등 각 서비스 요구사항에 따라 초고속 및 대용량(eMBB), 고신뢰 및 초저지연(uRLLC), 대량연결통신(mMTC) 세 가지로 구분하고 있다. 또한, [표 2]와 같이 5G 서비스의 성능목

[표 1] ITU-R, 5G 서비스의 주요 특징 및 비교

특성	설명	유스케이스	4G	5G	비고
초고속 대용량 통신 (eMBB)	최대 20Gpbs 및 일상적으로 100Mbps 속도가 가능한 ‘고속성(High Speed)’과 기존보다 1만 배 이상 더 많은 트래픽을 수용하는 ‘대용량(High Capacity)’	4K, 8K, 홀로그램, AR/VR 등	최대전송속도		20배
			(1Gbps)	(20Gbps)	
고신뢰 초저지연 통신 (uRLLC)	1ms 이하의 “낮은 지연시간(Low Latency)”, 이동 간 제로 중단을 실현하는 “높은 안정성(High Reliability)”	자율주행차, 공장자동화, 원격의료 등	전송지연		1/10
			10ms (0.01초)	1ms (0.001초)	
대량연결통신 (mMTC)	1평방 km 당 100만 개 기기가 가능한 ‘고밀집(High Density)’, 배터리 하나로 10년간 구동 가능한 ‘고에너지 효율(High Energy Efficiency)’	스마트시티, 스마트빌딩, 물류 등	$1km^2$ 당 기기 연결 수		10배
			10만 개	100만 개	

〈자료〉 넷마니아즈, NIA(신동형) 자료 재인용

[표 2] ITU-R, 4G 대비 5G 네트워크의 기술적 특성과 진화 방향

구성요소		현재 4G 기술	5G 기술 진화 방향(SA 구조 기준)	특징
UE(사용자장치)		스마트폰, 테블릿 등 개인용 기기 (음성, 문자, 영상, 인터넷 등)	B2B 비즈니스용 IoT 수용 (스마트폰, AR·VR, 드론, 의료센서 등)	연결 기기 확대
무선 액세스 네트워크	접속 방식	단일 무선 RAT 액세스 (2G, 3G, 4G 별도 구조)	다중 액세스(Multi-RAT Access) (WiFi 등 Non-3GPP Access 수용)	다양한 유·무선 액세스 기술을 동일한 인터페이스(One-connectivity)로 통합 제어
	기지국	매크로셀, 펨토셀 등	초고밀도 소형 셀 구축 증가	
	구현 기술	Centralized RAN	Cloud RAN 구조 (기능 분할, 가상화 기술 사용)	
코어 네트워크	배치	중앙 집중형 단일 코어망(EPC)	분산 클라우드 기반 코어 네트워크 (코어 기능의 지역적 분산화)	분산 에지 클라우드 및 네트워크 슬라이싱 서비스 제공과 MEC 지원이 용이하도록 소프트웨어 기반 구조(SDI)를 채택하여 유연한 코어 네트워킹 기능을 제공하고 3rd Party NF 연동과 애플리케이션을 개방
	전송 망	물리적 공유, 단일 네트워크 제공	종단간 네트워크 슬라이싱 (논리적 망 분리)	
	장비 형태	물리적 장비(PNF) 중심 (Physical Network Function)	가상화NF(SDN/NFV 기술 적용) (Visualization Network Function)	
	인터 페이스	Peer-to-Peer I/F Architecture (multiple 인터페이스)	SOA(Service-based I/F Architecture(HTTP2/RESTful))	
	제어 신호	CUPS (UP 기능과 CP 기능의 분리)	SDN/NFV 기반 CUPS 가속화 (UPF 기능 분산 및 에지 재배치)	
	기능 모듈화	네트워크 컴퓨팅 기능과 데이터 저장 기능이 한군데 처리	무상태(Stateless) 네트워크 기능 (네트워크 기능과 데이터 저장소 분리)	
외부 연동 및 애플리케이션		통신사의 코어망과 외부 GW(SGi 등)를 거쳐 연결	MEC(내부 에지 네트워크 전진 배치)	API 개방화

〈자료〉 넷마니아즈, ETRI(신명기), NIA(신동형),삼성 자료 인용하여 재구성

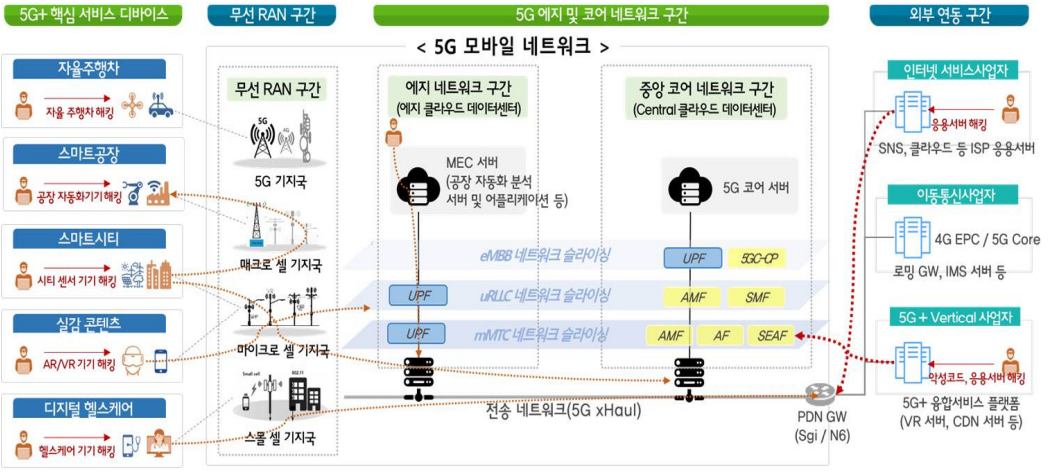
표를 달성하고 동적 서비스 및 비즈니스 환경에 따라 유연하고 확장 가능한 소프트웨어 인프라를 제공하기 위해 4G 기술 대비 5G 기술 진화 방향을 구성요소별(사용자장치, 무선 액세스 네트워크, 코어 네트워크, 외부 연동 애플리케이션)로 비교하였다[3]-[6].

본 고에서는 사이버보안 관점에서 5G 네트워크 및 서비스의 기술적 진화 방향에 따른 보안 이슈와 대응기술의 요구사항을 알아보고자 한다. II장에서는 5G 네트워크 기술 진화에 따른 보안위협을 살펴보고, III장에서는 3GPP 보안 표준, 유럽 5PPP(Public-Private Partnership Programme), 에릭슨, 화웨이 등 해외 5G 보안 아키텍처 연구 동향을 중심으로 5G 네트워크의 보안 요구사항을 구체적으로 설명한다. 마지막으로 IV장에서 본 고의 결론을 제시한다.

II. 5G 네트워크 기술 진화에 따른 보안위협

SA기반의 5G 서비스는 2020년 이후에 상용화될 것으로 예상되고 있다. 따라서 본 장에서 서술하는 5G 네트워크 기술 진화는 SA기반의 5G 구조를 기준으로 기술적 진화 특성에 따른 보안 위협을 [그림 1]과 같이 4가지 구간으로 나누어 살펴보도록 한다[7].

일반적으로 모바일 트래픽은 사용자 단말(User Equipment: UE)로부터 무선 액세스 네트워크(Radio Access Network: RAN, 기지국)와 코어 네트워크(이동성 관리, 인증, 과금 등을 위한 모바일 네트워킹 기능)를 거쳐 IP 서비스망(인터넷 서비스 사업자, 국가간 로밍 연동 등)의 응용 서버로 연결된다.



사용자 장치(UE)	무선 RAN 구간	5G 에지 및 코어 네트워크 구간	외부 서비스 연동 구간
악성코드 감염 펌웨어 해킹 디바이스 탬퍼링 IoT 봇넷 감염	무선 자원 재밍(Jamming) RAN DDoS 허위 기지국(Rogue BS)	(플랫폼) SDN/NFV 플랫폼 취약점, MEC 서버 취약점 (API) 3rd Party 어플리케이션 API 및 부적절한 권한 접근 (서비스) DDoS 서비스 장애, 네트워크 슬라이싱 위협 (네트워크) 분산 코어 네트워크 망 장애, 보안 관리 · 유지	응용 서버 취약점 API 취약점 공격 로밍 취약점, 가입자 정보 가로채기

〈자료〉 Cisco Systems, “5G Security Innovation with Cisco” 자료 인용하여 재구성

[그림 1] 5G 네트워크 구간 별 사이버보안 위협 Landscape

1. 5G 디바이스 보안 이슈

5G 디바이스의 가장 큰 위협요인은 5G 네트워크에 연결될 것으로 예상되는 수백억 개의 보안이 취약한 Massive IoT 기기들이다. 스마트폰과는 달리, IoT 기기는 서비스별

기기 유형(스마트공장 기기, 스마트시티 센서, CCTV 등)과 탑재 애플리케이션, 공급망 생태계가 다양하기 때문에 공통된 표준이나 아키텍처 설계가 쉽지 않다. 특히, 저사양 IoT 디바이스는 고수준의 보안 기능을 탑재하기 어려워 취약한 패스워드 및 오래된 보안 취약점을 내포한 채 운영되거나 디바이스 탬퍼링에 의한 변조에 취약하고 악성 애플리케이션에 의한 부적절한 접근 또는 중간자공격으로 인한 가입자 정보(IMSI) 유출 등의 보안위협에 취약한 환경에 노출될 가능성이 높다. 사이버 공격자는 보안이 취약한 IoT 기기의 제로데이 취약점을 찾고, 수많은 IoT 기기를 “원격 재부팅” 악성코드에 감염시켜 Massive IoT 봇넷을 구성하여 C&C 서버를 통한 원격제어를 수행하여 5G RAN 대상으로 DDoS 공격을 수행하는 등 IoT 기기를 공격수단으로 활용할 수 있다[7].

2. 5G 네트워크 인프라 DDoS 위협

대규모로 연결된 보안이 취약한 디바이스를 통한 DoS 및 DDoS 공격은 5G 네트워크에 직접적 위협이 될 수 있다. 유럽 ENISA Threat Landscape Report 2018 보고서에 따르면 DDoS 공격 용량은 지속적으로 대형화 추세이며, 2016년 IoT 봇넷을 통한 DDoS 공격이 출현하였고, 2018년 GitHub(1.35Tbps) 대상으로 초당 1테라급 DDoS 공격이 발생한 이후 공격 규모가 최대 1.7테라급으로 점차 커지고 있다[8]. 특히, 5G 네트워크는 4G보다 20배 빠른 높은 속도로 10배 많은 IoT 기기의 접속이 가능하기 때문에 IoT DDoS 공격의 강도가 점차 커질 수 있음을 우려하고 있다. 주요 공격 대상은 ① 5G 네트워크 인프라(RAN, 코어장비, 네트워크 슬라이스, 물리적 공유되는 플랫폼의 메모리 등), ② 5G 네트워크 인프라를 경유하여 연결되는 인터넷 서비스의 응용서버, ③ 5G에 연결된 디바이스가 될 수 있으며, 이때 상호 연결된 네트워크 인프라 리소스가 고갈되어 대규모 서비스 장애가 발생될 수 있다[9].

3. 5G 무선 액세스 네트워크(RAN) 보안 이슈

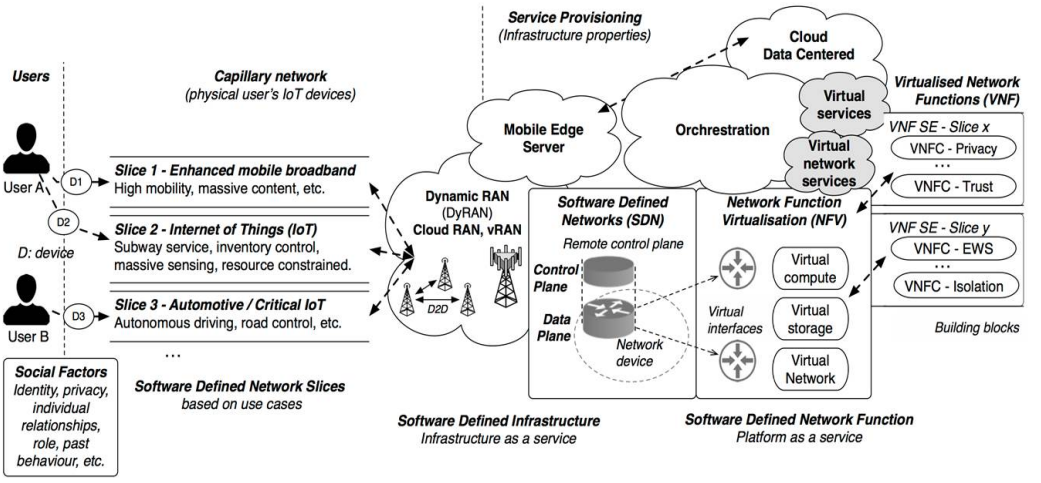
5G RAN 기술은 3GPP 액세스 기술(2G, 3G, 4G 등)뿐만 아니라 와이파이, 유선 인터넷 등 Non 3GPP 액세스 기술을 수용하여 동일 인터페이스에서 5G 네트워크 접속을 허용하는 것을 특징으로 하고 있다[4]. RAN 구간의 주요 보안위협[9]은 첫 번째, 악성코

드에 감염된 대량의 IoT 봇넷에 의해 무선 자원에 과도한 접속을 요청하는 RAN DDoS 공격과 무선 신호 채널에 대한 재밍(Jamming) 공격이다. 이러한 RAN DDoS와 전파 방해 재밍 공격을 통해 RAN 구간의 무선 인터페이스 자원을 고갈시켜 정상적인 데이터 수신을 방해하는 가용성 이슈가 발생될 수 있다. 두 번째는 허위 기지국(Rogue Base Station) 이슈로서, 사이버 공격자는 허위 기지국을 이용하여 모바일 사용자 장치(UE)와 5G 네트워크 사이에서 중간자 공격을 통해 모바일 사용자와 네트워크 사이에서 사용자 위치 정보 탈취, 전송 정보의 변조, 디도스 공격 등 다양한 공격을 수행할 수 있다. 이러한 이슈는 과거 4G 및 기존 네트워크에서도 지속적으로 제기되어 5G 네트워크에서 다양한 개선사항이 적용되어 도입됨에도 불구하고, 초고밀도 소형셀 구축이 확산될 경우, 보안관리가 취약한 소형 셀을 겨냥한 해커들의 해킹으로 통제권이 상실된 상태의 허위 기지국(Rogue Base Station) 이슈가 여전히 제기되고 있다.

4. 소프트웨어기반 5G 분산 코어 네트워크 보안 이슈

5G 코어 네트워크에서는 코어와 에지 네트워크의 분리, MEC(Multiaccess Edge Computing) 도입, 네트워크 슬라이싱, 가상화된 NF(Network Function) 기능 등을 제공하기 위해 하드웨어 종속적인 인프라에서 SDN/NFV 기술을 활용한 소프트웨어 기반 인프라로의 전환이 가속화될 것으로 예상된다[4]. 이에 따라 SDN/NFV 보안 이슈, 네트워크 슬라이싱 등 복잡한 논리계층의 보안 이슈들이 발생할 수 있다[7],[9],[10],[11].

첫 번째는 SDN 및 NFV 보안 이슈이다. SDN 네트워크는 네트워크 제어 기능(SDN 컨트롤러)과 트래픽 전달(SDN 스위치) 기능을 분리하여, 하드웨어적으로 구현된 네트워크 전달 기능에 대한 제어를 소프트웨어로 제어하고 통제하기 위한 기술이다[5]. 이에 SDN 컨트롤러와 SDN 스위치 간에 취약한 프로토콜 인터페이스를 이용할 경우 전체 시스템을 공격에 대해 취약하게 만드는 요인이 될 수 있다. SDN/NFV 인터페이스 구성상 취약점을 악용하여 SDN 컨트롤러와 스위치 통신의 무결성과 기밀성에 대한 공격, 스위치와 컨트롤러 무단 제어 또는 자원 고갈 DoS 공격이 발생할 수 있다. 예를 들어, SDN 컨트롤러를 공격하여 SDN 스위치의 플로우 테이블을 소진시키는 포화 공격이 발생될 수 있다. 또한, SDN 컨트롤러와 응용 프로그램 간의 신뢰관계, 즉 응용 프로그램의 변경 또는 인증과 네트워킹 기능에 대한 권한 부여 이슈가 중요하다. 응용 프로그램의 인증



〈자료〉 Ana N., Antonio A., Gerardo F., "Crowdsourcing analysis in 5G IoT: Cybersecurity Threats and Mitigation," Mobile Networks and Applications(MONET), Vol(24), Issues(3), 2019.

[그림 2] 5G Vertical Cross-layer Attack

및 권한 부여에 대한 강력한 메커니즘이 없다면 3rd Party의 악성 응용 프로그램이 SDN 컨트롤러로부터 네트워크 정보를 얻을 수 있다[16],[18].

두 번째는 네트워크 슬라이싱 보안 이슈이다. 네트워크 슬라이스는 eMBB, uRLLC, mMTC 서비스별 다른 애플리케이션 또는 테넌트를 위해 논리적으로 분리할 수 있다. 이때 네트워크 슬라이싱을 적절히 격리하지 않으면 공격자가 하나의 슬라이스에서 다른 슬라이스로 공격을 수행할 가능성이 있다. 예를 들어, 공격자는 특정 서비스 전용의 네트워크 슬라이스에 악의적으로 트래픽 용량을 초과시켜 다른 네트워크 슬라이스에 영향을 주는 자원고갈 공격을 수행할 수 있다. 또한, 특정 애플리케이션을 이용하여 다수의 네트워크 슬라이스를 동시에 활성화할 수 있으며, 네트워크 슬라이스에 적절한 암호화가 적용되어 있지 않다면 공격자는 다른 슬라이스에 속한 데이터를 도청하거나 변조할 수 있다.

5. 다중 액세스 에지 컴퓨팅(MEC) 보안 이슈

다중 액세스 에지 컴퓨팅은 사용자 기기와 가까운 네트워크에서 컴퓨팅을 지원하는 것을 말하며, 데이터가 수집되는 에지 네트워크에서 데이터를 분석할 수 있는 장점이 있어 초저지연 서비스를 제공할 수 있다. 특히, MEC 컴퓨팅은 모바일 통신 사업자의 5G 에지

네트워크 내부의 사용자 평면 기능(UPF)과 연결되기 때문에 새로운 연결경로가 생기게 된다. 여기서, MEC 시스템은 클라우드 및 가상화를 포함한 다양한 기술을 지원하고, 3rd Party 응용 프로그램을 배포할 수 있는 개방형 에코 시스템에서 상호 운영되기 때문에 MEC의 개방성, 이질성과 다양성은 전체 MEC 시스템에 주요 위협이 될 수 있다[10]. 예를 들면, MEC 플랫폼이 가상화 플랫폼으로 구축되어 일부 VNF(Virtual Network Functions)와 동일한 플랫폼에서 MEC 응용 프로그램이 실행될 수 있다. 이때 MEC 응용 프로그램이 모바일 통신 사업자가 통제하기 어려운 3rd Party 응용 프로그램일 경우, 가상화 네트워크 리소스 자원을 소모하거나 부적절한 API 권한으로 승인되지 않은 민감 정보에 액세스할 수 있다는 우려가 있다. 두 번째로, 공격자는 악의적인 응용 프로그램을 삽입하여 분산된 5G 네트워크 내부 장비인 UPF 등 에지 네트워크 기능에 공격을 시도할 수 있는 새로운 공격 경로를 제공할 위험이 있다. 즉, MEC와 5G 에지 네트워크 간 경계에서 가상화된 기능으로 민감한 보안 자산이 손상되면 공격자는 악의적으로 재사용하여 연결을 얻거나 스푸핑, 도청 또는 데이터 조작 공격을 수행할 수 있다[12].

III. 5G 보안 아키텍처 연구 동향

초연결 사회의 핵심 인프라인 5G 네트워크, 사용자 트래픽과 서비스를 안전하게 보호하기 위해서는 새로운 보안기술이 설계되고 솔루션이 개발되어 네트워크에 구축되어 운영되어야 하며, 이를 위해 표준화, 장비개발, 네트워크 구축 및 운영의 각 단계별로 고려해

[표 3] 단계별 보안 요구사항 및 보안 이슈

단계	보안 요구사항	이슈사항
표준화 단계 (Standardization)	국가 간 망의 상호연동을 위해 안전한 통신 프로토콜 설계	표준 프로토콜 취약점 기본적 보안 요구사항·스펙만 정의
장비제조사 개발 단계 (Implementation)	표준에서 요구하는 보안 기준 및 목표 수준에 맞는 장비 개발	장비 구현 취약점 공통 기능을 다르게 구현, SW 오류 등
통신 사업자 구축 단계 (Deployment)	안전한 네트워크 및 서비스 설계와 구축	망 구축 취약점 구성 설정 오류, 오픈소스, 3rd Party SW
서비스 운영 단계 (Operation)	사이버공격에 대한 탐지 및 모니터링, 사고대응 관리	운영 취약점 취약점 대응, 공급망 보안제어 및 보증

〈자료〉 "A guide to 5G network security" 에릭슨 자료를 재구성하여 인용함

야할 사항은 [표 3]과 같다[13].

먼저 표준화 단계에서는 국가 간 네트워크 및 시스템의 상호 연동을 위해 통신 프로토콜과 인터페이스가 안전하게 설계되어야 한다. 지금까지 3GPP 표준에서는 사용자와 네트워크 간에 상호인증을 위한 인증 및 키 관리, 제어 평면(Control Plane)의 시그널링 메시지와 사용자 평면(User Plane)의 데이터를 보호하기 위한 보안 표준들을 개발하여 모바일 네트워크의 보안성을 지속적으로 강화해 왔으나, 표준은 최소한 기본적인 보안 요구사항과 스펙만을 정의하기 때문에 표준 프로토콜 상의 취약점이 존재할 수 있다.

두 번째로, 장비 개발 제조사들은 표준에서 요구하는 보안 기준과 목표 수준에 맞는 장비를 개발해야 한다. 예를 들어, 각 장비 제조사별로 보안 기능이 다르게 구현되거나, SW로 구현된 장비들이 SW 오류를 내포하거나, 장비 구현 당시에는 알려지지 않았던 보안 취약점(Unknown Vulnerabilities)이 시간이 지나 지속적으로 발견되는 등의 장비 구현 상의 보안 취약점 이슈가 지속적으로 발생한다.

세 번째로, 통신 사업자는 장비 제조사들의 통신장비와 서비스 애플리케이션들이 보안 요구사항에 맞게 구현되었는지 공급망 제품을 검증하여 안전한 네트워크와 서비스를 설계하고 구축해야 한다. 그럼에도 불구하고 네트워크와 서비스를 구축하는 과정에서 구성설정 오류가 존재할 수 있고, 통신 사업자가 아닌 3rd 애플리케이션 등의 보안 이슈는 지속적으로 제기되고 있다.

마지막 서비스 운영 단계에서는 고도화되고 지능화된 사이버공격에 대한 취약점 제거와 침해사고 발생 후 복원력이 중요하다. 또한, 각 단계별 보안 이슈사항을 해결하는데 소요되는 대응조치 시간도 장애요소가 될 수 있으므로, 이를 최소화하는 노력이 필요하다. 즉, 표준 프로토콜 상의 보안 취약점의 경우 표준에 반영되기까지 수년의 시간이 소요되며, 장비 구현 취약점은 SW 패치부터 안전성 검증까지 약 6개월 이상의 시간이 소요되기 때문에 각 단계 간 보안 갭(Security Gap)을 줄여나가는 것이 매우 중요하다고 할 수 있다.

1. 5G 보안 표준화 동향

5G와 관련된 보안 표준화는 전 세계적으로 시작 단계에 있으며, 국제표준기구와 사실표준단체에서 5G 기본적 보안 요구사항과 아키텍처에 관한 표준 연구가 활발하게 진행 중에 있다. 3GPP 보안 표준은 SA3(Service and System Aspects, Security Group)

워킹그룹에서 주로 다루고 있으며, 1세대부터 5세대 이동통신 기술까지 모바일 네트워크 보안을 강화하기 위한 보안표준을 지속적으로 발표해 왔다. 2세대 이동통신에서는 무선 인터페이스 도청 및 메시지 스팸 이슈를 해결하기 위해 무선 인터페이스 암호화 및 SIM 카드가 최초로 도입되었고, 3세대 이동통신에서는 상호인증(AKA) 및 무선자원관리 시그널링 보호기능(RRC 메시지 암호화 등)을 강화해 왔다. 4세대 이동통신에서는 NAS/AS (Non Access Stratum/Access Stratum) 보안기능을 통해 시그널링 메시지에 대한 보안이 지속적으로 강화되었다[14],[21],[22].

5G 보안 표준과 관련해서는 2015년부터 보안 아키텍처, RAN 보안 인증 메카니즘, 네트워크 슬라이싱 보안, 가입자 정보보호 표준에 대한 논의가 시작되었고, 2018년 8월 5G Release 15에서 보안표준이(SA3 TS 33.501) 발표되었다[15]. 이 표준에서는 이전 세대 대비 가입자 정보(SIM카드에 저장된 IMSI 사용자 식별자 등) 보호를 위한 IMSI (International Mobile Subscriber Identity) 정보 암호화 기능, 로밍 도메인 간 보안 이슈였던 SS7(Signalig System No.7) 이슈를 해결하고 서로 다른 통신 사업자(Public Land Mobile Network: PLMN) 간 애플리케이션 계층 간의 보안을 구현하기 위한 SEPP(Security Edge Protection Proxy) 기능, 3GPP 액세스와 Non-3GPP 액세스에 대해 동일한 인증방법을 사용할 수 있도록 한 통합 인증 프레임워크 기능이 도입되었다. SEAF를 사용하면 장치가 서로 다른 액세스 네트워크 간을 이동하거나 서로 다른 서비스 네트워크 사이에서 이동하는 경우에도 전체 인증 방법(예; AKA 인증)을 실행하지 않고 재인증될 수 있다[9]. 또한, 유럽집행위, 제조사, 통신사, 서비스사업자, 연구기관이 참여한 5G PPP의 Security WG에서는 주로 5G 보안 아키텍처 연구(2017. 5G PPP 보안 백서)가 진행 중이다. 국제 이동통신사업자 중심의 NGMN(Next Generation Mobile Networks) 5G 워킹그룹에서는 네트워크 슬라이싱, MEC의 보안 요구사항에 대한 연구를 다루고 있다. ETSI(유럽통신표준협회) NFV SEC(NFV Security) WG에서는 NFV 플랫폼의 보안 스펙을 주로 다루고 있다. ITU(SG17)에서는 5G 보안에 관한 보안 규격에 대해 본격적으로 논의가 시작되었다[16].

2. 장비개발 및 구축 단계에서 5G 보안 아키텍처 설계 고려사항

5G가 분산되고 유연한 아키텍처 특성을 기반으로 새로운 서비스와 기능의 손쉬운 배치

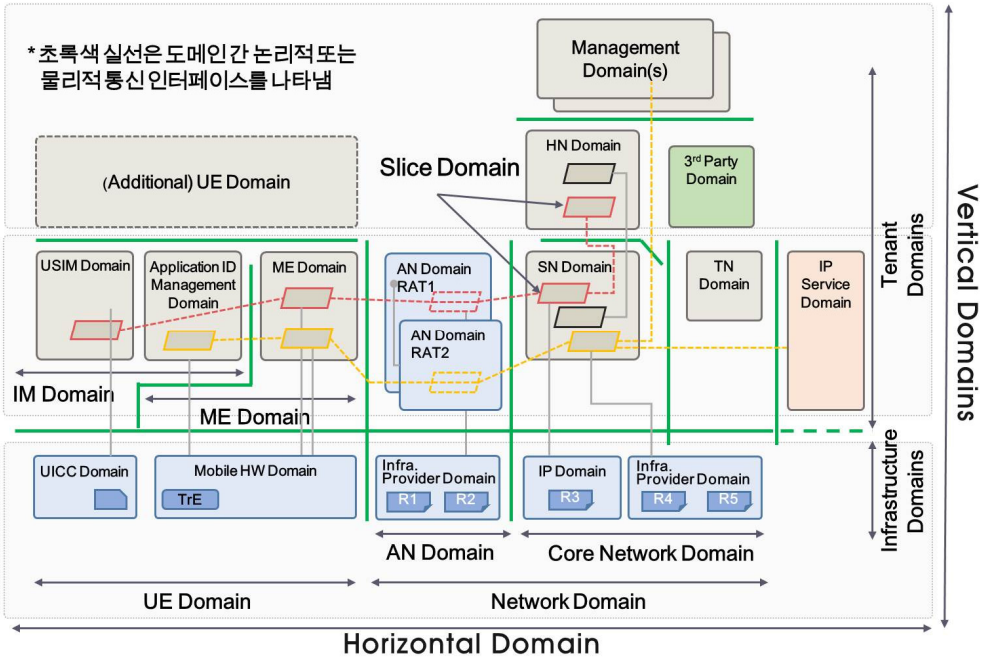
가 가능하게 되었지만, 이는 보안 환경을 복잡하게 만드는 보안 가시성 이슈를 야기시킨다. 최근 영국 정부는 5G 보안 아키텍처와 보안 요구사항에 관한 연구결과를 발표하였다[12]. 주요 내용으로 5G 환경은 이전 이동통신 환경보다 다양한 유형의 네트워크, 장치 및 관련 서비스를 제공하므로 네트워크, 시스템 및 서비스의 보안은 점차 어려워지고 있음을 강조하였고, 5G 보안 메카니즘으로 다음의 4가지 고려사항을 제시하였다.

첫 번째는 종단 간 보안(End to end security or Horizontal Security)이다. 기존 4G 모바일 네트워크와 마찬가지로 사용자 장치로부터 무선 액세스 및 전송 네트워크를 포함하여 코어 네트워크의 종료 지점 간의 수평적 통신 경로에 대한 보안을 유지하는 종단 간 보안 기술이 필요하다.

두 번째는 계층 간 보안(Cross-layer Security or Vertical Security)이다. 5G는 분산되고 유연한 특성으로 인해 수평적 도메인 간 경계방어와 종단 간 보안만으로는 해결하기 어렵다. 예를 들어, SDN/NFV 기반 가상화 네트워크 플랫폼, 논리적인 네트워크 슬라이싱, 클라우드 기반의 MEC는 물리적 인프라를 물리적 계층, 가상화 계층, 애플리케이션 계층 같은 수직적 계층(Vertical Layer)으로 나눌 수 있어, 각각의 계층에 적합한 보안 기술이 효과적일 수 있다. 따라서 서로 다른 보안 계층의 보안 기술 조정을 위해 수직적인 보안(Vertical Security) 통합 프레임워크가 필요하다.

세 번째는 멀티 도메인 간 보안(Domain Security)이다. 네트워크, 서비스 및 장비를 포함한 다양한 공급자(사업자) 도메인이 공존함으로써 보안 문제가 발생할 수 있다. 예를 들면, 논리적인 네트워크 슬라이싱 기능을 제공하기 위해서는 여러 물리적 도메인(단말, 액세스 네트워크, 코어 네트워크 등)과 수직적 도메인(장비 제조사, 가상화 솔루션 업체, 3rd 애플리케이션 개발업체 등)에 걸쳐 구현될 수 있고, 이때 각 도메인별로 구축되는 보안 솔루션과 정책을 일정 수준 동일하게 유지하기 위해서는 네트워크망 사업자, 가상화 솔루션, Vertical Service Provider 등 새로운 공급자 도메인 간의 보안 솔루션들이 상호 연계가 되도록 구현되어야 한다. 각 도메인별 또는 멀티 도메인에 걸쳐 계층 간 보안(Cross-layer Security)이 보장되어야 다른 도메인과 안전하게 작동할 수 있다.

네 번째는 보안 내재화(Security by design)이다. 보안기술은 표준화 단계부터 장비 개발과 네트워크 설계 프로세스의 일부로서 초기에 고려되고 배포되어야 한다. 이러한 접근 방식은 시스템이 완전히 구축되어 작동한 후에는 다루기가 쉽지 않은 잠재적 보안



* IM(Identify Management), ME(Mobile Equipment), SN(Serving Network), HN(Home Newtork), TN(Trust Network), IP(Internet Provider), Tenant(자원공유 환경)
〈자료〉 "Domain overview of the 5G-ENSURE 5G security architecture" 자료 인용함

[그림 3] 5G PPP의 Security Architecture 개념도

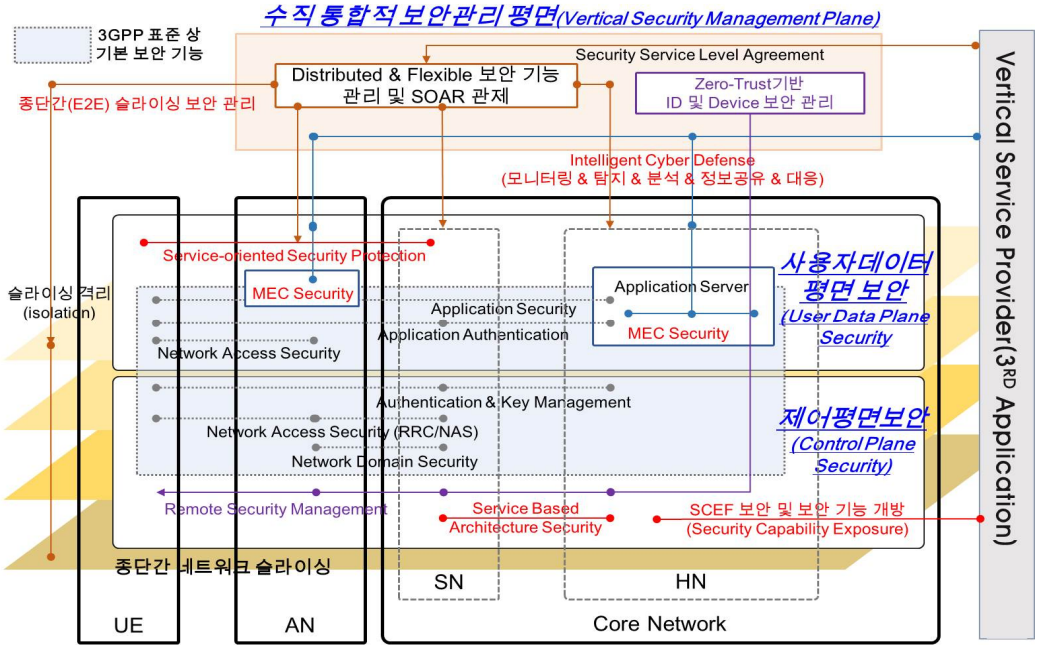
갭 차이를 최소화할 수 있다. 특히, SW 개발주기에 대한 빠른 피드백으로 알려지지 않은 취약점 등 잠재적 보안 이슈가 운영 환경에 피해를 발생 및 확산시키는 것을 완화할 수 있는 DevSec Ops 보안 설계 적용이 매우 중요하다.

또한, EU의 Horizon 2020 연구 프로젝트로 수행중인 5G PPP의 ENSURE(Enablers for Network and System Security and Resilience) 프로젝트에서는 5G Security Architecture를 [그림 3]과 같이 제시하였으며, 수평적 도메인별 보안뿐만 아니라 각각의 도메인 상에 다양한 수직적 생태계가 존재하며, 수직적 보안(Vertical Domain Security)의 필요성을 강조하였다[17],[18]. 예들 들어, 사용자 단말 장치(UE) 동일 플랫폼 상에는 HW 제조사 보안영역, USIM 보안, 애플리케이션 ID 보안, 슬라이스 서비스 보안 등이 수직적으로 존재하여 각기 다른 보안 기능을 일관되게 유지하는 것이 중요함을 강조하였다.

3. 운영단계에서 지능형 사이버공격 방어를 위한 고려사항

5G 서비스 운영 단계에서 지능형 사이버 공격에 효과적으로 방어하기 위해 화웨이[19]는 [그림 4]와 같이 사용자장치(UE) 도메인부터 액세스 네트워크(AN), 코어 네트워크 도메인까지 5G 아키텍처 상에서 논리적인 수직 계층(네트워크 슬라이스 서비스와 관련된 Vertical Service Provider)을 포함하여 사각지대가 없는 5G 네트워크 및 서비스 기능 보호와 사이버공격 방어 체계 프레임워크와 3가지 고려사항을 제시하였다.

첫 번째는 분산 사이버공격 방어(Distributed Security)이다. 모바일 트래픽은 제어 트래픽과 사용자 데이터 트래픽이 분리되어 서로 다른 경로로 여러 도메인을 걸쳐 전송되기 때문에 각 도메인(무선 RAN 구간, 에지 네트워크 구간 등)에서 발생되는 보안위협과 요구하는 보안 수준이 상이하므로 효과적인 사이버 공격 탐지 기능들이 분산되어 배치될 필요가 있다. 예를 들어, 잠재적인 공격 지점과 가까운 위치에 방어 기능을 배치하고 대응 속도를 높이기 위해, Massive IoT DDoS에 의한 RAN 과부하 공격에 대한 대응은 기지



* UE(사용자 장치), AN(Access Network), SN(Serving Network), HN(Home Newtork),
〈자료〉 화웨이 "5G Security Architecture Framework" 자료 내용을 인용하여 보안 요구사항을 재구성함

[그림 4] 지능형 사이버공격 방어를 위한 5G Security Architecture Framework

국 또는 에지 네트워크에 공격 탐지 기능을 배치하는 것이 효과적일 수 있다[9].

두 번째는 유연하고 확장 가능한 보안(Flexible & Scalable Security)이다. 5G 네트워크 인프라는 물리적인 x86 범용서버를 가상화하여 가상머신(Virtual Machine) 상에서 서로 다른 서비스 요구사항에 맞게 통신기능(NFs)들을 동적으로 생성, 확장 제어하고, 3rd Party 서비스 사업자에게 내부 네트워크 기능이 오픈되는 서비스 기반 아키텍처 구조(Service-based Architecture)를 도입하였다[4]. 이때, 5G 서비스 보안은 제어 평면(Control Plane)과 사용자 데이터 평면(User Plane) 계층별로 3GPP 표준의 기본적 보안기능이 제공되어야 하며, 5G 서비스별로 다양하고 복잡한 보안 요구사항을 만족하기 위해 각 서비스 슬라이싱별로 차등화된 보안 기능의 구성과 호출이 유연하게 적용되어야 한다[22]. 예를 들어, 네트워크 슬라이스별로 인증 방법과 암호화를 차등 지원(예; eMBB 서비스는 LTE 유사 수준, 저비용 IoT 센서의 경우 경량 인증, uRLLC 서비스의 경우 빠른 액세스 인증과 강한 암호 기능 제공)하거나 슬라이스 서비스별로 보안 기능(Service oriented security)을 선택할 수 있어야 한다. 또한, 네트워크 슬라이스 상에서 사이버공격 탐지와 완화 그리고 슬라이스 간 격리(isolation) 등이 동적으로 모니터링되고 통합 관리되어야 한다.

세 번째는 사이버공격 기술은 현재의 보안기술을 우회하고 취약한 보안 사각지대를 찾기 위해 점차 정교해지고 자동화되고 있기 때문에 지능형 사이버공격의 대응 속도를 높이기 위해서는 수직 통합적 보안관제의 자동화가 필요하다. 5G 네트워크에서는 멀티 도메인 상에서 논리적 수직적 계층(Cross-layer)에 걸쳐 보안이 다루어지기 때문에 여러 도메인에 걸친 수직 계층 간 보안을 관리하고, 각 논리적 계층의 사이버공격을 모니터링하고 탐지하는 구조가 중요하다. 이때 네트워크 슬라이스별로 제공되는 제어평면(Control Signaling) 보안과 사용자 데이터 평면(User Data Plane) 보안과 연계되어 수직적인 계층까지 포괄하는 수직 통합적 사이버 방어 계층이 필요하다. 주요 기능은 각 도메인별 기본적 보안 기능(로그분석 등) 관리뿐만 아니라 다중 도메인에 걸친 네트워크 슬라이싱 보안, 3rd Party 수직적 서비스 사업자에게 개방되는 API 보안, 제로 트러스트 기반 IoT 기기들의 원격 보안 관리 기능, AI 기술을 활용한 지능형 사이버공격 탐지, 복잡한 보안 가시성 문제를 해결하기 위한 보안 오케스레이션 기술 등 보안 시큐리티 자동 관제 기술(Security Orchestration Automation Response: SOAR)이 포함될 수 있다.

IV. 결론

지금까지 살펴본 5G 네트워크의 기술적 특성과 진화 방향은 사이버보안 관점에서 새로운 도전과제를 주고 있다. 대량의 IoT 기기 연결로 인한 사이버공격의 대형화, 분산 소프트웨어기반 코어 아키텍처로 인한 보안 가시성의 복잡성 증가, MEC, 3rd Party 애플리케이션 및 코어 기능의 API 개방화는 새로운 공격 연결 경로 이슈이다. 이러한 새로운 보안 이슈를 해결하기 위해 3GPP, 5G PPP, 5G Americas 등 해외 주요 연구기관들은 5G 보안 아키텍처 연구를 통해 도메인별 경계방어 중심에서 다양한 도메인과 수직적 계층을 포괄하는 사이버보안의 중요성을 강조하였다. 2020년 이후 본격적인 5G 시대가 도래할 것을 대비하여 국내에서도 5G 기술 특성에 따른 새로운 5G 보안 아키텍처 설계 및 신기술 연구가 시급히 추진되어야 할 시점이라고 생각된다.

[참고문헌]

[1] 김윤선, “5G 국제표준의 이해”, 삼성 리서치, 삼성 국제표준 백서, 2018.
[2] 이상협, “5G 통신의 현재와 미래”, IT동아(이문규), 4차 산업혁명과 직업의 미래, 2018.
[3] 신동형, “5G가 만들 새로운 세상”, NIA, DNA 플러스, 2019, pp.4-11.
[4] 신명기, 이수환, 이승익, 이종화, 안병준, “5G 네트워크/시스템 표준기술 동향”, TTA, TTA Journal, Vol(184), 2019, pp.40-49.
[5] 손장우, “‘KT, SK Telecom 5G 상용망 비교’, ‘통신사업자의 MEC 수용구조(4G, 5G)’”. 2019.
[6] “5G Core Vision”, SAMSUNG, Technical Report, 2019, pp.4-14.
[7] Michael G., Pramod N., “5G Security Innovation with CISCO,” CISO Systems, White Paper, 2018.
[8] Louis M., Andreas S., Cristos D., Louis M., Marco L., Omid R.,“ENISA Threat Landscape Report 2018,” ENISA, 2019, pp.47-53.
[9] “The Evolution of Security in 5G,” 5G americas, White Paper, 2018, pp.18-35.
[10] Jim H., “5G Security Strategy Considerations,” Jniper, Technical Report, 2019, pp.2-9.
[11] Ana N., Antonio A., Gerardo F., “Crowdsourcing analysis in 5G IoT: Cybersecurity Threats and Mitigation,” Mobile Networks and Applications(MONET), Vol(24), Issues(3), 2019, pp.881-889.
[12] Serdar V. et. al. “5G Network Architecture and Security,” UK DCMS, Technical Paper, 2018, pp.19-36.
[13] “A guide to 5G network security,” Ericsson White Paper, 2018.
[14] “An overview of the 3GPP 5G security standard,” Ericsson White Paper, 2019.

[15] 3GPP, “Security architecture and procedures for 5G system(TS 33.501),” 2018.
[16] Ijaz A. Tanesh K., Madhusanka L., Jude O., Mika Y., Andrei G., “Overview of 5G security Challenges and Solutions,” IEEE, Communications Standards Magazine, 2018, pp.36-43.
[17] Rolf B., et. al, “5G Enablers for Network and System Security and Resilience: Security Architecture,” 5G PPP Security WG, 2017, pp.15-47.
[18] Manuel P., Gregorio P., “5G PPP Phase 1 Security Landscape,” 5G PPP Security WG, 2017, pp.7-63.
[19] “5G Security Architecture white paper,” Huawei, White Paper, 2017, pp.11-14.
[20] 신상호, “SDN/NFV기반 5G 통신망 인프라의 진화”, NIA AI Network Lab 인사이트 제4호, 2019, pp.11-14.
[21] Ijaz A. Shahriar S. Tanesh K. Jude O., Andrei G., Mika Y., “Security for 5G and Beyond,” IEEE Communications Surveys & Tutorials, May 2019, pp.4-6.
[22] Ericsson, “5G Security - Scenarios and solutions,” Ericsson white paper, June 2017.

chapter 2

AMI 2.0과 차세대 전력선 통신 IoT-PLC

박배영 ‖ ㈜아이앤씨테크놀로지 수석연구원

I. 서론

'스마트그리드'라고도 불리는 지능형 전력망은 전력망에 정보통신기술을 적용하여 전기 에너지 공급자와 소비자가 실시간으로 정보를 교환하는 등의 방법을 통해 전기를 공급함으로써 에너지 이용 효율을 극대화하는 전력망을 일컫는다.

2016년을 기점으로 시작된 한국전력의 2,250만호 AMI(Advanced Metering Infrastructure, 지능형 검침 인프라) 구축 사업은 3년여가 경과되면서, 향상된 성능을 갖는 유무선 통신 기술, 효율적 운영 및 강화된 보안에 대한 필요성이 대두되어 왔다. 이러한 요구를 수용하기 위해 2019년 상반기에 한국전력과 각종 기기 제조사가 참여하는 공청회가 열렸고, 이를 통해 기존의 AMI를 한 단계 개선시킨 AMI 2.0이라는 개념을 정립하였다.

AMI 2.0에는 다양한 유무선 통신기술, 보안 강화형 전력량계, 제한적 성능을 갖는 각종 기기를 지원하기 위한 기기 관리 플랫폼, 복수의 통신시스템을 수용하는 스마트미터링 게이트웨이, 각종 기기들에 대한 상호운용성 확보 및 통합시험 환경 구축 등에 대한 내용들을 포함하고 있다.

II장에서는 AMI 2.0을 통해 도입되는 여러 내용 중에서 경량형 기기를 위해 활용될

* 본 내용은 박배영 수석연구원(☎ 031-696-3543, backswim@naver.com)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.

OPEN 출처표시 상업용금지 공공누리 공공저작물 자유이용허락

수 있는 망 관리용 플랫폼인 LWM2M(Lightweight Machine to Machine)과 2020년부터 적용 예정인 SNMP(Simple Network Management Protocol) v3, ARM사에서 IoT 기기용으로 개발한 실시간 운영체제인 MBed OS, 보안강화형 전력량계 및 각종 유무선 통신기술에 대해 소개할 것이다.

III장에서는 전력선을 매체로 하는 통신 방식 중에서 기존 방식에 비해 전송 거리의 확장과 지중 포설된 열악한 통신 환경에서도 향상된 신뢰성을 갖는 차세대 전력선 통신 방식인 IoT-PLC(Internet of Things-Power Line Communication) 기술에 대해 소개하고[1], 마지막 장에서는 AMI 2.0 도입에 따른 기대효과와 발전 방향에 대해 제시한다.

II. AMI 2.0

1. AMI 에너지 플랫폼의 변화

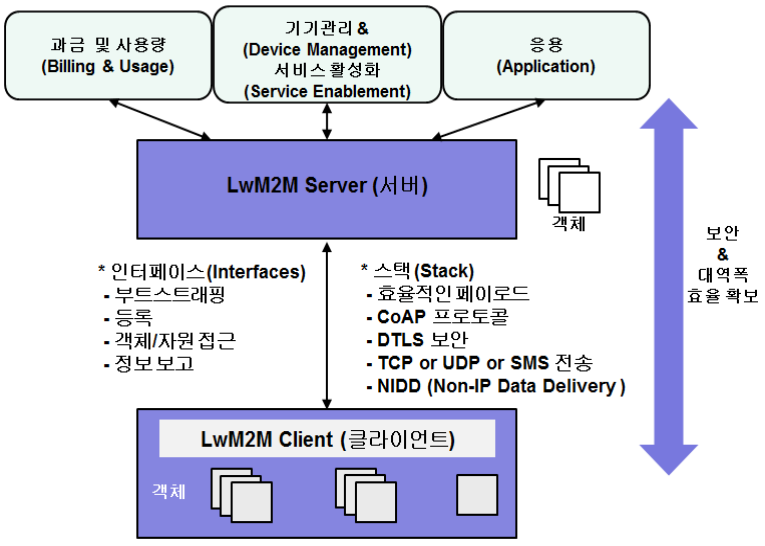
현재 운용 중인 에너지 플랫폼에는 검침용 데이터 관리를 위한 FEP(Front End Processor) 서버와 AMI 네트워크 및 네트워크에 연결된 각종 기기를 관리하기 위한 네트워크 관리 시스템(Network Management System: NMS) FEP 서버가 사용된다.

NMS는 네트워크의 전반적인 상태, 성능 등의 모니터링과 각종 제어를 위한 시스템으로, 이를 구현하는 프로토콜로서 현재는 SNMP가 사용되고 있다. AMI 2.0에서는 IoT 기기에 적합한 LWM2M 플랫폼이 적용될 예정이고, 2020년부터는 보안이 강화된 SNMP v3로 업그레이드될 예정이다.

가. LWM2M

LWM2M은 OMA(Open Mobile Alliance)에서 기존 이동통신 생태계에 적용하던 기기 관리(Device Management: DM) 기능을 비교적 낮은 성능을 갖는 제한적인 CPU와 메모리를 갖는 IoT 기기에 활용할 수 있도록 경량화한 플랫폼이다[2].

[그림 1]에서 보여지는 LWM2M 플랫폼은 네트워크 내에서 IoT 기기의 초기설정(Bootstrap), 등록, 해제, 소프트웨어/펌웨어 다운로드, 기기의 상태진단(Diagnosis) 및 배터리/메모리 등 하드웨어의 모니터링, 기기 주변장치 제어, 시스템 리부팅, 이벤트 로깅



〈자료〉 ㈜아이앤씨테크놀로지 자체 작성(LWM2M 참조)

[그림 1] LWM2M 구성도

(Logging) 등을 위한 기술을 포함한다[3].

최근에 발표된 Version 1.1에서는 방화벽(Firewall)이나 NAT(Network Address Translation) 환경에서도 각종 IoT에 활용되는 응용계층 프로토콜인 CoAP(Constrained Application Protocol)를 지원할 수 있도록 했고, 메시지 전송계층으로서 UDP, SMS (Short Message Service) 이외에 TCP(Transmission Control Protocol) 계층이 추가되었다. 또한, 비-IP 기기 데이터(Non-IP Device Data: NIDD) 교환 기능을 지원한다[4].

[표 1] OMA-DM과 LWM2M 비교

구분	OMA-DM 1.x	LWM2M
기기 관리	규격화 및 확정적	규격화 작업 및 확장 중
펌웨어 업데이트	부분적 표준화	부분적 표준화 및 영역 확장 중
유연성	고성능 기기에 한정적	다양한 범위의 기기 지원
제한적 성능의 기기 지원	미지원	지원
IoT 기능 지원	고성능 기기에 한정적	경량기기에도 적용 가능
서비스 레벨 표준화	없음	IRTF를 중심으로 OCF, W3C WoT 등으로 표준화 영역 확장
표준화 그룹	GSMA, 3GPP	GSMA, IETF, IRTF, one M2M, IPSO 등

〈자료〉 ㈜아이앤씨테크놀로지 자체 작성

[표 1]은 기존 모바일 기기 관리를 위한 OMA-DM과 LWM2M의 차이를 비교한 것이다.

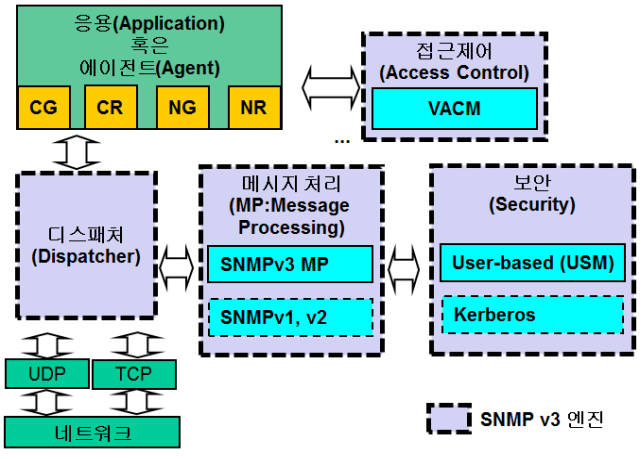
나. SNMP v3

전력망을 구축하는 각종 장비들에 대한 성능, 구성, 장애, 보안 등의 관리를 위한 네트워크 관리시스템의 프로토콜로 사용되는 SNMP는 Manager(관리자), Agent(에이전트), MIB(Management Information Base, 관리정보기반) 등으로 구성된다.

관리자는 전력공급자 망의 서버에서 실행되며, 에이전트는 네트워크에 연결된 기기에서 실행된다. MIB란 객체(Object)와 유사한 용어로 설명될 수 있는데, 기기 내부의 각종 속성, 설정 값 등을 의미한다. 네트워크에 설치된 모뎀 설비에서 MIB의 예를 들면 모뎀에 할당된 IP주소, MAC 주소, 제조 일련 번호, 통신 신호 세기 등이 있다.

SNMP 에이전트는 데이터 집중장치와 수용가(가정 혹은 공장 등)에 설치된 설비 등에서 운영되는 소프트웨어 형태로서, 모뎀과 연결된 전력량계의 등록, 각종 설정 변경, 모뎀 신호의 중계 경로(Repeating path), 상태 모니터링, 유무선 통신망의 품질측정, 원격 소프트웨어 업그레이드 등의 기능 수행을 담당한다.

SNMP v3는 사용자 보안 모델(User Security Model: USM)과 뷰-기반 접근제어(View-Based Access Control Model: VACM)를 정의한다. USM은 SNMP에 인증과



〈자료〉 ㈜아이앤씨테크놀로지 자체 작성(IETF SNMPv3 참조)

[그림 2] SNMP v3 아키텍처

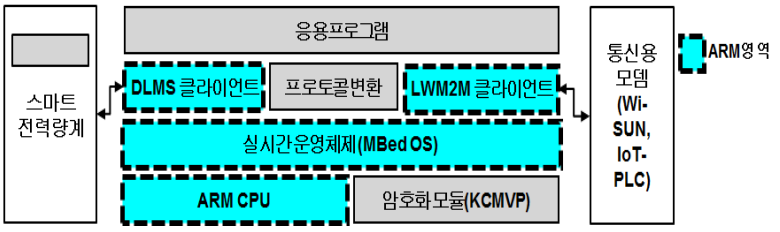
기밀성 서비스를 제공하는데, 이를 위해 기밀키와 인증키가 사용된다[5].

뷰-기반 접근제어는 관리되는 객체(MIB)에 대해 원격 주체로부터의 접근 허가 여부를 결정하는 메커니즘을 정의하고 있으며, 이를 위해 그룹, 보안 레벨, 컨텍스트, MIB 뷰, 접근정책 등으로 구성된다.

다. ARM MBed OS

고사양 모바일 기기부터 저전력 MCU(Micro Controller Unit)까지 다양한 제품군을 중심으로 영역을 넓혀 가고 있는 ARM은 IoT 기기용으로 활용될 수 있는 오픈 플랫폼으로 실시간 운영체제인 MBed OS를 발표했고[6], ARM 개발자들에게 IoT 제품 개발이 빠르게 이루어질 수 있도록 다양한 컴포넌트를 제공함으로써 임베디드 생태계를 확장시켜 나가고 있다.

최근에 발표한 MBed OS버전에는 LTE(Long-Term Evolution) 기반의 협대역 통신 방식인 NB-IoT(Narrow Band-IoT), Cat-M1 기반 프로토콜을 포함하여 블루투스, Wi-Fi, LoRa 등의 연결성(Connectivity)을 제공하며, AMI 2.0에서 도입되는 IoT-PLC와 Wi-SUN(Wireless Smart Utility Network)에 대한 연결성을 도입할 계획이다.



〈자료〉 ㈜아이앤씨테크놀로지 자체 작성

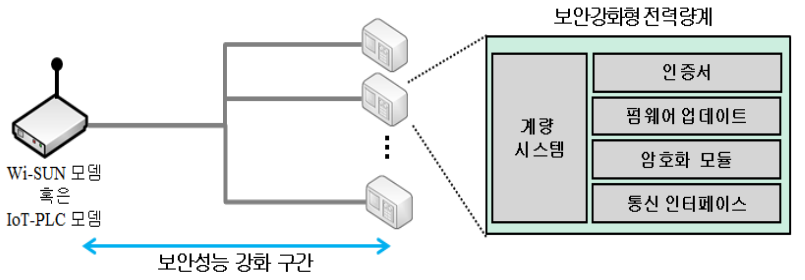
[그림 3] ARM 기반 AMI 2.0 기기 블록다이어그램

ARM은 AMI 2.0을 통해 각종 통신용 모뎀, 지능형 데이터 처리장치 등에 MBed OS 등의 실시간 운영체제를 탑재하면서 각종 다양한 전력 서비스를 지원하기 위해 지난 2018년 한국전력과 개방형 AMI 과제 협력 계약을 체결했으며, 2021년까지 높은 보안성을 갖는 AMI용 SoC(시스템 반도체) 및 기기 관리를 위한 솔루션 개발을 목표로 하고 있다.

2. 보안강화형 스마트 전력량계

전력량계는 사용 전압에 따라 고압용, 저압용으로 나뉘고, 외부와 통신할 수 있는 모뎀과의 결합 형태에 따라 IrDA(Infrared Data Association)를 사용하는 표준형, 외장형 모뎀 연결방식의 E-type, 규격화된 통신용 모뎀 내장이 가능한 G-type 및 Advanced E-type으로 구분된다[7]. 전력 사용량에 따른 알루미늄 원판의 회전수를 이용하여 유효 전력량만을 측정할 수 있었던 기존의 아날로그 전력량계는 검침원의 수기 검침으로만 전력량이 집계되었으나, 현재는 여러 형태의 통신기술을 기반으로 자동 검침이 가능한 전력량계로 교체되고 있다.

현재 운용되는 AMI 시스템에서 보안성의 강화가 요구되는 부분은 전력소비자 측에 설치되는 전력량계와 통신모뎀 구간과 계기에 탑재되는 펌웨어 업데이트 부분이다. 보안강화형 전력량계는 인증서 및 PKI(Public Key Infrastructure) 구조를 통해 인증되지 않은 계기가 전력망에 접속할 수 있는 가능성을 차단하고, 전력량계와 모뎀 간 데이터 교환 규격인 DLMS(Device Language Message Specification) 프로토콜에서의 보안 상위 규격인 HLS(High Level Security)를 채택하였다.



〈자료〉 ㈜아이앤씨테크놀로지 자체 작성

[그림 4] 보안강화형 전력량계

또한, 계량시스템이나 추후 개정될 수 있는 각종 규격의 반영이 가능하도록 전력량계 펌웨어 업그레이드를 지원하며, 이 때 펌웨어의 무결성 검증을 통해 인증 받지 않은 펌웨어의 설치로 인해 오작동할 수 있는 보안 위협을 최소화한다.

3. 유무선 통신기술

현재 구축되어 운용 중에 있거나 AMI 2.0을 통해 활용할 유무선 통신기술의 형태는 [표 2]와 같다. 기존 형태에서 전력선 통신 방식으로 IoT-PLC 기술과 유선 CAN(Controller Area Network) 통신이 별도로 추가되었다.

[표 2] 지능형 전력인프라(AMI)에 활용중이거나 AMI 2.0을 통해 활용할 유무선 통신기술

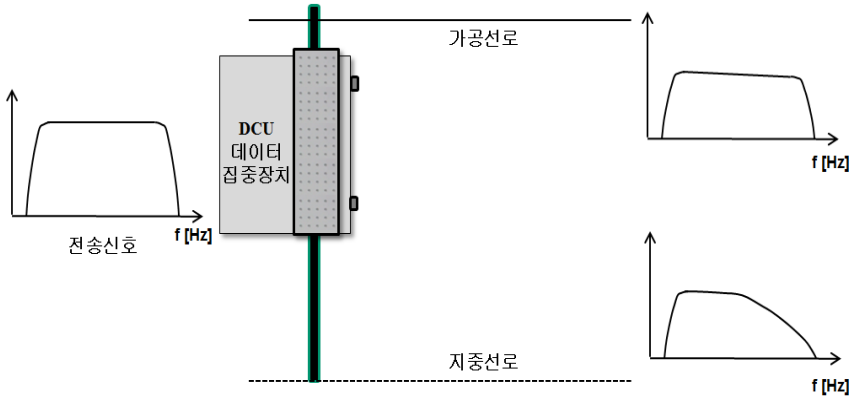
구분	주요 내용
전력선 통신기술	➢ 전력량계와 데이터 집중장치 구간을 연결하는 통신 방식 1. HS-PLC: 기존 가공 형태로 구축된 한국형 전력선 통신기술 2. HPGP: 기존 지중 형태로 구축된 미국 방식 전력선 통신기술 3. IoT-PLC: AMI 2.0에서 채용되는 장거리 전송 및 감쇄가 심한 지중에서도 효과적 활용이 가능한 전력선 통신 기술[1]
유선 CAN (Controller Area Network)	➢ 통신 모뎀과 다수개의 전력량계 간을 연결하는 통신 방식 - CSMA/NBA ID기반 우선순위 다중 동시 접속 방식(CSMA/NBA: Carrier Sense Multiple Access with Non-destructive Bitwise Arbitration) - ISO11898-2 PHY/CAN 2.0B 확장 ID모드 사용 - 통신 속도: 500kbps, 250kbps, 125kbps
유선 RS485	➢ 통신 모뎀과 다수개의 전력량계 간 연결 시(충돌이 미고려된 네트워크) 활용 - 통신 속도: 115.2kbps(기존 9.6Kbps, 38.4Kbps) - 다중 접속 관련 규격에 대한 논의 중
무선 Wi-SUN (Wireless Smart Utility Network)	➢ 전력량계와 데이터 집중장치 구간을 연결하는 통신 방식 - IEEE 802.15.4-2015 SUN 규격 기반 무선통신 기술[8],[11] - PHY: SUN-2FSK, 917~923.5MHz, 940MHz 대역, 데이터 집중장치의 경우 최대 200mW까지 전력 증대 가능 - MAC: CSMA/CA or TSCH(Time Slotted Channel Hopping) - 메시 형태의 토폴로지 지원
무선 Zigbee PRO	➢ 전력량계와 데이터 집중장치 구간을 연결하는 통신 방식 - IEEE 802.15.4 LR-WPAN기반 PHY, MAC을 기반으로 네트워크 계층 및 응용계층 객체, 프로파일 등을 지원하며, 기존 Zigbee 기술에서 보안성을 강화함 - AMI2.0에서는 활용되지 않음
무선 LTE	➢ 전력량계와 전력공급자의 검침용 플랫폼 구간 혹은 데이터 집중장치와 FEP 서버 구간을 연결하는 통신 방식 - 3GPP Release 8 이상의 규격을 만족하는 이동통신규격 - Cat.1 혹은 Cat.M1급 이상의 통신 속도 지원(10Mbps~1Mbps) - 전송 데이터의 양이 적을 경우 NB-IoT 기술도 활용 가능(약 160Kbps)

〈자료〉 ㈜아이앤씨테크놀로지 작성

III. 차세대 전력선 통신 IoT PLC

1. 등장 배경

전력선은 전력 에너지를 전달하기 위한 매체이지만 이러한 매체를 이용하여 양방향 정보교환을 목적으로 도입된 기술이 전력선 통신 기술이다. 2017년부터 구축 중인 지능형 검침 인프라(AMI) 통신 기술에서 가장 높은 비율을 차지하는 것은 한국형 고속 전력선 통신(KS-PLC, ISO/IEC-12139) 방식으로서, 포설된 전력선이 가공(架空, Overhead Wire) 형태일 경우에 활용되고 있다. 전력선이 지중에 매설될 경우 대지가 용량성 리액턴스로 작용하여 통신을 위한 전송로가 저역통과 필터(Low Pass Filter: LPF)와 유사한 특성을 갖게 되므로, 높은 주파수 영역 성분 신호의 감쇄로 인해 원활한 통신이 어렵게 된다[10].



〈자료〉 ㈜아이앤씨테크놀로지 자체 작성

[그림 5] 가공/지중구간 통과에 따른 전력선 신호 특성

이를 극복하기 위한 대안으로 무선통신 기술인 Wi-SUN(IEEE 802.15.4-2015 SUN) 통신설비를 구축하거나, 외산 전력선 통신 기술인 IEEE 1901 기반의 HPGP(Home Plug Green PHY) 통신설비를 활용해 왔다[8],[9].

IoT-PLC는 지중구간에서 발생하는 고주파 신호 영역 감쇄에 효과적으로 대응할 수 있을 뿐만 아니라, 기존의 전력선 통신 방식에서의 거리로 인한 성능 제한을 상당 부분 극복할 수 있도록 물리계층, 매체접속제어계층 기술을 정의하고 있다.

2. 물리계층(PHY) 기술

IoT-PLC는 변복조 방식으로 직교 주파수 분할 다중(Orthogonal Frequency Division Multiplexing: OFDM) 방식을 사용하고, 이용 대역폭은 2~31.25MHz이다.

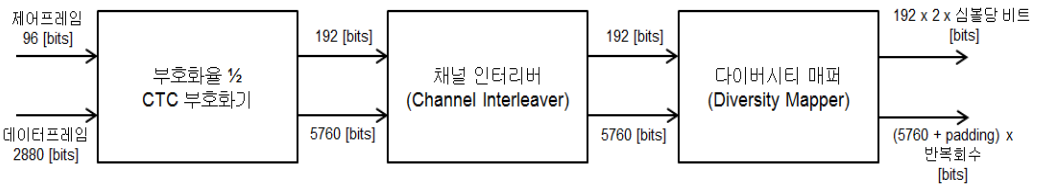
[표 3] IoT-PLC의 물리계층(OFDM) 규격

항목 (짧은 심볼/긴 심볼)	짧은 심볼 (Preamble Frame)		긴 심볼 (Reference Training Symbol/ Control Frame/Data Frame)	
	샘플	시간(㎲)	샘플	시간(㎲)
신호 대역폭	2~31.25MHz			
샘플링 주파수	62.5MHz			
부반송파 간격(SCS)	97.656KHz		24.414KHz	
IFFT 간격(FFT_S/FFT_L)	640	10.24	2560	40.96
보호대역 간격(GI_S/GI_L)	140	2.24	624	9.984
롤 오프 간격(Roll-off linterval)	20	0.32	320	5.12
순환전치부 간격(CP Length)	160	2.56	944	15.104
순환후치부 간격(CS)	0	0	336	5.376
심볼 길이(Symbol duration)	780	12.48	3520	56.32

〈자료〉 ㈜아이앤씨테크놀로지 자체 작성

OFDM 심볼에는 짧은 심볼(Short Symbol)과 긴 심볼(Long Symbol)로 나눌 수 있는데, 짧은 심볼은 프리앰블 전송 시 사용되며, 긴 심볼은 참조훈련(Reference Training) 심볼, 제어 프레임 및 데이터 프레임을 전송하는데 사용된다. OFDM 심볼 간 간섭(Inter Symbol Interference: ISI)을 제거하기 위해 944샘플의 순환 전치(Cyclic Prefix: CP)와 336샘플의 순환 후치(Cyclic Suffix: CS)를 합한 1,280샘플의 순환 확장(Cyclic Extension: CE)을 사용하며, 320샘플의 상승 코사인 윈도(Raised Cosine Window)를 사용하여 스펙트럼 특성을 개선했다[1].

기존에 사용되었던 HS-PLC의 경우 비동기식(Non-Coherent) 변조 방식인 DBPSK (Differential Binary Phase-Shift Keying), DQPSK(Differential Quadrature PSK), D8PSK(Differential 8-PSK) 등을 지원하면서 모뎀의 단순화, 소형화 등 경제성 쪽에 중심을 두었다면, IoT-PLC의 경우 비동기식 및 동기식(Coherent) 변조를 지원하면서,



〈자료〉 ㈜아이앤씨테크놀로지 자체 작성

[그림 6] IoT-PLC 통신 방식에서의 오류 제어

채널 환경이 양호한 경우 QPSK, 16QAM(16 Quadrature Amplitude Modulation) 등의 고차변조를 지원하여 대역폭 이용 효율을 높일 수 있다.

전송 채널 상에서 발생할 수 있는 오류에 대한 대책으로, 컨볼루셔널 터보 코드(Convolutional Turbo Code: CTC) 방식의 채널 부호화 방식을 채용했고, 전송 데이터 순서의 재배치를 통해 채널의 연속 오류(Burst Error)에 의한 데이터 손실이 집중되는 것을 분산시키는 채널 인터리버를 사용하고 있다. 여기에 다이버시티 매퍼(Diversity Mapper)를 통해 전송 프레임을 반복(Repetition)하여 전송함으로써 수신측에서의 신뢰성을 향상시키고자 하였다.

3. 매체접속제어(MAC) 기술

MAC(Media Access Control)은 상위 링크계층으로의 논리적 인터페이스를 제공하며, 하위 PHY의 물리적 매체 사용을 제어하는 기능을 제공하여 IoT-PLC 기기 간의 통신을 가능하게 하는 역할을 한다.

IoT-PLC의 장치 종류에는 IEEE 802.11에서의 용어와 유사한 액세스 포인트(AP)와 스테이션(STA) 두 가지가 있으며, AP는 STA들과 연결성을 제공하고 외부 네트워크와의 접속점(게이트웨이) 역할을 한다. STA이 요청할 경우 AP는 비컨 프레임을 전송하여 접속할 수 있는 기반을 제공한다[1],[8].

매체 공유 방식으로는 반송파 감지 다중접속/충돌회피(Carrier Sense Multiple Access with Collision Avoidance: CSMA/CA) 방식을 기본적으로 사용하고, 가상 반송파 감지, 중복 프레임 감지, 재전송, 충돌감지, 복구 등의 기능을 제공한다. 프레임 전송 시에는 암호화된 형태로 전송되어야 하며 사용되는 암호화 방식은 AES(Advanced Encryption

Standard) 128-GCM(Galois/Counter Mode) 또는 ARIA(Academy, Research Institute, Agency) 128-GCM 모드가 사용된다.

IoT의 특성인 비교적 짧은 길이의 데이터를 보내기에 적합하도록 페이로드 길이를 360 바이트로 제한하고 있으며, 이는 하나의 노드가 데이터 전송 시 요구되는 공유채널 점유 시간을 최소화하기 위한 목적이다.

[표 4]에서는 한국형 고속 PLC와 IoT-PLC 간의 물리계층 및 MAC 계층에서의 각종 특성들에 대해 비교하고 있다.

[표 4] KS-PLC와 IoT-PLC의 규격 비교

구분	KS-PLC	IoT-PLC
규격	ISO/IEC 12139-1	KOEMA-0915(단체 표준)
변조방식	DMT(Discrete Multi Tone)	OFDM
심볼 길이(CP 제외)	10.24us	40.96us
주파수 오프셋 및 데이터 전송률	미지원 (Non-coherent 방식)	지원 (Coherent 방식)
사용대역폭 및 데이터 전송률	2.15~23.15MHz 최대 24Mbps	2~31.25MHz 최대 14Mbps
디지털 변조	DBSPK, DQPSK, D8PSK	BPSK, QPSK, QAM
수신 감도	약 -80dBm	약 -95dBm
매체공유 방식	CSMA/CA	CSMA/CA (IEEE 802.15.4 표준 기반)
프레임 길이	1,600bytes 이상	360bytes
프로토콜 프로파일	이더넷(IEEE 802.3)	6LowPAN/IPv6/UDP
보안	AES128 CTR	AES128/ARIA128 CTR/GCM
MAC 프레임 종류	Management/Data/Ack	Beacon/Control/Command/Data

〈자료〉 ㈜아이앤씨테크놀로지 자체 작성

IV. 결론

지금까지 AMI 2.0이라는 패러다임에 포함되는 플랫폼과 각종 설비에 포함되는 각종 실시간 운영체제, 보안강화형 전력량계 및 차세대 전력선 통신기술인 IoT-PLC에 대해

살펴보았다.

AMI 2.0을 통해 얻을 수 있는 기대효과는 산업 측면, 소비자 측면, 전력시스템 측면으로 구분해서 볼 수 있다. 산업 측면에서는 새로운 플랫폼과 다양한 기술의 수용을 통해서 일어나는 융복합으로 새로운 사업기회를 만들어 낼 수 있고, 이는 양질의 일자리 창출로 이어질 수 있다. 소비자 측면에서는 전력 ICT 기반시스템의 안정적 운영을 통해 정확한 전력사용 정보를 제공받아 보다 효율적이고 합리적인 전력소비를 가능하게 한다. 마지막으로 전력시스템 측면에서는 기 구축된 시스템과의 효율적 운영을 통해 전체적인 운영비용을 낮추면서, 전력 수급 변동에 유연하게 대응할 수 있다[12].

[참고문헌]

[1] 한국전기산업진흥회, “사물인터넷(IoT)을 위한 전력선 통신 매체접근제어(MAC) 및 물리계층(PHY) 일반 요구사항”, SPS-KOEMA 0915, 2018, p.89.
[2] OMA LWM2M v1.1 Specification, Open Mobile Alliance, 2019, p.31.
[3] Sergey Slovetskiy, Poornima Magadevan, OMA LWM2M White Paper, 2018, p.21.
[4] 오승훈, 고석갑, 손승철, 이병탁, 김영선, “이동통신 기반 IoT 장치관리 표준 프로토콜 동향”, 한국전자통신연구원, 전자통신동향분석, Vol.30 No.1, 2015, p.8.
[5] D. Levi, P. Meyer, B. Stewart, SNMP v3, RFC 2263, RFC 2264, RFC 2265, IETF, 1998.
[6] Mihail Stoyanov, Introduction to mbed OS, ARM, 2016, p.31.
[7] KEPCO, “전자조달시스템-구매규격-저압 AMI시스템 구축용 통신자재”, 2019.
[8] IEEE Standard for Low-Rate Wireless Networks 802.15.4-2015
[9] 안선종, “전기자동차 충전시스템을 위한 HS-PLC 방식 SLAC 구현에 대한 연구”, 학위(석사)논문, 2016, p.37.
[10] 박배영, “IoT 게이트웨이로서의 데이터 집중장치(DCU)”, 정보통신기술센터, 주간기술동향 1804호 2017, p.12.
[11] 박배영, “Wi-SUN 프로토콜 및 활용 동향”, 정보통신기획평가원, 주간기술동향 1864호 2018, p.12.
[12] 산업통상자원부, “제2차 지능형전력망 기본계획(2018~2022)”, 산업통상자원부 공고 제2018-432호, 2018, p.23.

chapter 3-1

로봇 손 물체 조작을 위한 물체 인식 기술

김종환 ‖ 한국과학기술원 교수

I. 결과물 개요

개발목표시기	2019. 12.	기술성숙도(TRL)	개발 전	개발 후
			TRL 3	TRL 5
결과물 형태	SW Library	검증방법	자체검증	
Keywords	object recognition, object detection, object manipulation, object grasp			
외부기술요소	Open Source 사용	권리성	특허, SW	

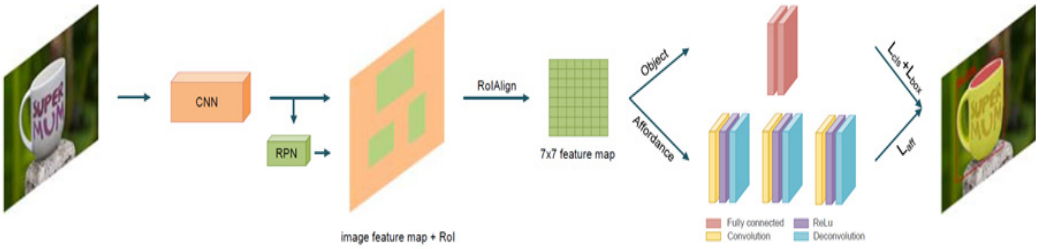
II. 기술의 개념 및 내용

1. 기술의 개념

➢ 로봇 핸드의 물체 파지(把指, 손으로 쥠)를 위해 RGB-D 센서 입력 영상으로부터 목표 물체를 검출 및 인식하고, 해당 물체의 파지 가능 영역을 검출하여 파지 정보를 생성함

* 본 내용은 김종환 책임연구원(☎ 042-350-3448)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.
***정보통신기획평가원은 현재 개발 진행 및 완료 예정인 ICT R&D 성과 결과물을 과제 종료 이전에 공개하는 "ICT R&D 사업화를 위한 기술예고"를 2014년부터 실시하고 있는 바, 본 칼럼에서는 이를 통해 공개한 결과물의 기술이전, 사업화 등 기술 활용도 제고를 위해 매주 1~2건의 관련 기술을 소개함

OPEN 출처표시 상업용금지 공공누리 공공저작물 자유이용허락



[그림 1] 기술개념도

2. 기술의 상세내용 및 사업화 제약사항

➢ 기술의 상세내용

- 물체별로 위치 정보가 주어진 학습 영상뿐 아니라, 물체의 기능에 따라 파지 가능 영역 등의 labeling 정보가 별도로 제공되는 훈련 영상들로부터 convolutional neural networks 기반의 물체 학습 및 인식을 수행함
- 인식된 영역에 대해 물체의 사용성을 고려한 파지 가능 영역을 추가로 검출하며, 해당 파지 가능 영역에 대한 형상 분석을 통해 로봇 손이 물체를 조작할 수 있도록 파지 정보를 생성함

➢ 기술이전 범위

- 물체 인식 및 물체의 사용성을 고려한 물체 파트 인식 기술
- 로봇 손 물체 조작을 위한 물체 파지 정보 생성 기술

➢ 사업화 제약사항

- Open source library의 상용화 이용 시 라이센스 허용 범위 확인 필요

III. 국내외 기술 동향 및 경쟁력

1. 국내기술 동향

➢ 물체 인식 및 파지 정보 생성 기술

- 중앙대에서 YOLO Detector, image segmentation, PCA를 사용한 물체의 사용성 특징 검출에 대해 연구하였음
- 한국과학기술연구원에서 depth 센서를 기반으로 파지 가능한 경계영역을 검출하고 형상을 분석하여 물체의 기능을 고려한 물체 파지 기술에 대해 연구하였음

2. 해외기술 동향

➢ 물체 인식 및 파지 정보 생성 기술

- 이탈리아 IIT에서는 object detector로 물체의 후보 bounding box를 검출한 후, depth feature를 결합한 CNN 및 Dense CRF를 시용하여 물체 사용성 인식을 수행하고 파지 정보를 생성하는 연구를 수행하였음
- 중국 남경대에서는 각 물체의 종류에 따라 사전에 정의된 파지 정보를 이용하여 RGB-D 데이터와 3D 메시 데이터를 결합하여 파지 정보를 생성하는 연구를 수행하였음

3. 표준화 동향

➢ 물체 인식 기술

- 물체 인식 기술과 관련된 표준화된 규정은 없으나, imageNet, PASCAL, COCO 영상DB 등 일반화된 데이터베이스에 대한 객관화된 인식 성능 비교가 이루어지고 있음

4. 관련 보유특허

No.	국가	출원번호(출원일)	상태	명칭
1	대한민국	2019-0005728 (2019-01-16)	출원	다양한 환경 변화에 강인한 라인세그먼트 추출 방법
2	대한민국	2018-0055259 (2018-05-15)	출원	물체 크기와 자세 변화에 강인한 단일 모델 기반의 물체 추적 방법
3	대한민국	2014-002003 (2014-02-21)	등록	소실점 추정을 이용한 평행선 검출 방법

No.	국가	출원번호(출원일)	상태	명칭
4	대한민국	2013-012239 (2013-10-15)	등록	이분된 로컬 영역을 가지는 윤곽선 분할 기반 특징을 이용한 물체 인식 방법
5	대한민국	2013-001117 (2013-01-31)	등록	크기 변화에 강건한 범주 물체 인식을 위한 모델 학습 및 인식 방법
6	대한민국	2011-0096764 (2011-09-26)	등록	범주 인식에 의한 파지점 생성방법 및 그 방법에 대한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체
7	대한민국	2010-0136158 (2010-12-28)	등록	물체의 시점변화에 강건한 윤곽선 기반의 범주 물체 인식 방법 및 장치

5. 기술적 경쟁력

경쟁기술	본 기술의 우수성 및 차별성
IIT	물체 사용성 인식을 통한 파지 가능 영역에 대한 3차원 형상 분석 기반의 파지 정보 생성
남경대	추가적인 3D 메시 데이터 없이 RGB-D 데이터에 대한 3차원 형상 분석 기반의 파지 정보 생성
DexNet	Top-view 카메라에서의 무작위 파지 학습이 아닌, 물체 인식 및 물체의 사용성을 고려한 파지 수행

IV. 국내외 시장 동향 및 전망

1. 국내 시장 동향 및 전망

➢ 서비스용 로봇 국내 시장 현황 및 전망

- 한국로봇산업진흥원 2016 로봇산업 실태조사 결과보고서에 따르면, 로봇 매출 규모는 전년대비 9.0% 증가한 4조 5,972억 원이며, 생산 규모는 12.9% 증가한 4조 4,750억 원을 기록
- 서비스용 로봇의 경우 IoT, 인공지능, 빅데이터, 클라우드 등의 기술 발전에 힘입어 새로운 분야 및 서비스에 로봇 활용이 확산되고 있으며, 향후 서비스 로봇 분야의 연구 개발이 중요해질 전망임

2. 해외 시장 동향 및 전망

➢ 서비스용 로봇 해외 시장 현황 및 전망

- World Robotics 2016에 따르면, 2015년 세계 개인 서비스용 로봇 시장 규모는 전년대비 5% 성장한 22억 1,617만 달러로 규모는 크지 않으나, 수요가 급증할 시장으로 기대됨
- 분야별 세계 개인 서비스용 로봇 시장은 성장세를 지속하여 2018~2020년도에는 총 113억 달러 상당의 규모로 성장할 것으로 전망

3. 제품화 및 활용 분야

활용 분야(제품/서비스)	제품 및 활용 분야 세부내용
서비스로봇	물건 정리정돈 및 물건 전달 심부름
산업용 로봇	다품종 부품 조립을 위한 파지

V. 기대효과

1. 기술도입으로 인한 경제적 효과

➢ 산업용 로봇 시장뿐 아니라 개인화 또는 전문화된 서비스를 제공할 수 있는 서비스 로봇 시장의 활성화에 기여하며 시장을 확대시킬 수 있는 기반 마련

➢ 빠른 속도로 성장하고 있는 서비스 로봇 시장을 선도하여 기술력 선점을 통한 국가 경쟁력 제고

2. 기술사업화로 인한 파급효과

➢ 로봇 손의 다양한 물체 조작을 위한 인식 기술에 대한 사업화를 통해 연관 산업 발전에 기여

chapter 3-2

시각 기반 휴먼 행동 검출 및 인식 기술

이재연 ‖ 한국전자통신연구원 책임연구원

I. 결과물 개요

개발목표시기	2020. 2.	기술성숙도(TRL)	개발 전	개발 후
			TRL 4	TRL 6
결과물 형태	SW	검증방법	자체검증, 시험인증	
Keywords	행동 검출, 행동 인식			
외부기술요소	Open Source 사용	권리성	SW	

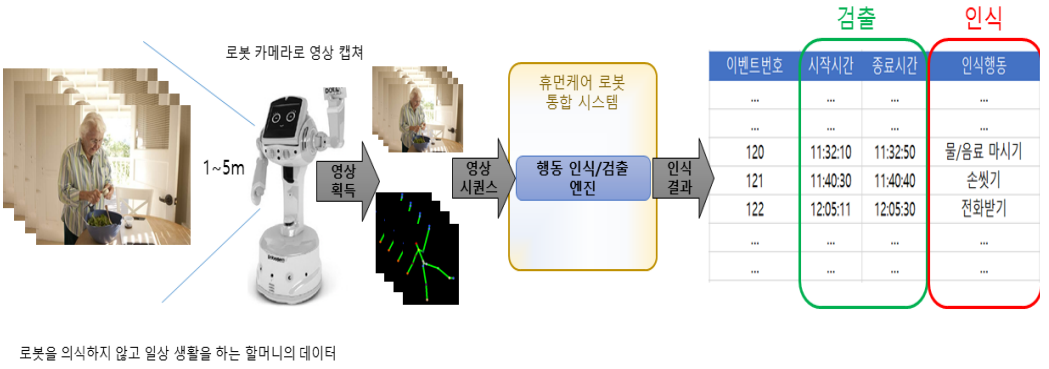
II. 기술의 개념 및 내용

1. 기술의 개념

➢ 카메라 등 비전 기기를 이용하여 사람의 현재 행동을 검출 및 인식하는 기술 및 서비스에 있어서, 서비스에 따라 필요한 행동 종류가 다른데, 이에 대해 소규모 데이터로도

* 본 내용은 이재연 책임연구원(☎ 042-860-5507)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.
***정보통신기획평가원은 현재 개발 진행 및 완료 예정인 ICT R&D 성과 결과물을 과제 종료 이전에 공개하는 "ICT R&D 사업화를 위한 기술예고"를 2014년부터 실시하고 있는 바, 본 칼럼에서는 이를 통해 공개한 결과물의 기술이전, 사업화 등 기술 활용도 제고를 위해 매주 1~2건의 관련 기술을 소개함

OPEN 출처표시 상업용금지 공공누리 공공저작물 자유이용허락



[그림 1] 기술개념도

빠르게 학습이 가능하도록 하는 기술

- 서비스에 따라 필요로 하는 인식 행동이 다른데, 이에 대해 소규모의 데이터만을 갖고도 빠르게 고성능의 인식기를 만들 수 있음
- 관절 정보를 기반으로 인식하기 때문에 필요로 하는 데이터가 적고 그에 따라 연산량이 적고 가벼움
- 배경이나 조명으로부터 오는 노이즈의 영향을 받지 않아 안정적인 성능을 제공
- 제스처 수준의 간단한 행동부터 복합 행동과 같은 복잡한 수준의 행동까지 검출 및 인식이 가능
- 소인부터 고령자까지 모든 연령대에 대해 동일한 인식기 적용이 가능

2. 기술의 상세내용 및 사업화 제약사항

➢ 기술의 상세내용

- 본 기술은 “시각 기반의 행동 검출 및 인식 기술”로, 시각 기기에 의해 사용자를 촬영한 데이터로부터 시간 축에서의 행동 후보를 검출해내는 기술과 그 후보에 대한 행동 인식 기술을 포함

➢ 기술이전 범위

- 행동 후보 검출 기술

※ 검출용 네트워크의 Weight
※ 행동 검출용 코드
※ 요구사항 정의서 및 시험 결과서

- 행동 인식 기술
※ 행동 인식용 네트워크의 Weight
※ 행동 인식용 코드
※ 요구사항 정의서 및 시험 결과서

➢ 사업화 제약사항
- 하고자 하는 서비스에 따라서 인식 대상이 되는 행동의 종류가 다양하며, 그에 따라서 그 행동에 대한 데이터가 일부 필요
- 3D 관절 정보를 사용하지 못할 경우, RGB 영상으로부터 2D 관절을 추출하는 기술을 사용해야 하므로 3D 관절에 비해 성능이 소폭 저하될 여지가 있음
- Deep Neural Network를 사용하기 때문에 GPU나 그에 준하는 연산기기가 필요, 혹은 Network Compression 기술이 필요

III. 국내외 기술 동향 및 경쟁력

1. 국내 기술 동향

➢ 국내에서는 서울대 곽노준 교수 연구실에서 행동인식 관련 Charades Challenge에 참가하여 상위권 성적을 기록함

2. 해외 기술 동향

➢ 2016년에 싱가포르의 NTU에서 총 60가지 행동에 대한 대규모 Dataset을 공개한데 이어, 2019년에 120가지 행동에 대한 Dataset을 재공개하였으며, 또한 이를 기반으로 한 연구가 활발히 진행 중
➢ 매년 ActivityNet이라는 이름으로 RGB 영상 기반의 행동 인식 대규모 Challenge를

개최

- 2017년 Google에서 나온 I3D 네트워크가 RGB 혹은 Depth 기반의 행동인식에서 기반기술로 널리 사용
- 행동 검출의 경우, 베이징 대학교에서 2017년에 공개한 PKU-MMD Dataset에서 대규모로 행동의 시작-끝을 함께 제공해 이를 기반으로 한 연구가 활발히 진행 중

3. 기술적 경쟁력

경쟁기술	본 기술의 우수성 및 차별성
I3D	관절 정보를 쓰기 때문에 속도가 빠르고, 환경적인 요소의 영향을 적게 받음
HCN	사전에 Candidate Frame을 추출하여 인식하기 때문에 속도 및 연산에서 효율적
c-ConvNet	시계열 정보를 압축 없이 그대로 반영할 수 있음

IV. 국내외 시장 동향 및 전망

1. 국내 시장 동향 및 전망

- 인구 고령화에 따른 해결책으로 휴먼케어 로봇이 제안되고 있으며, 이를 위해서는 대상자의 현재 상태를 파악해야 하는데, 행동인식 기술은 이를 위해 꼭 필요한 기술
- 제스처 수준의 인식기술은 주로 게임 시장에서 활발히 사용되었으며, 현재는 VR 등의 산업이 발전함에 따라서 더 복잡한 수준의 행동 인식이 필요해질 것으로 기대됨
- 보안 및 방범 이슈에서도 비정상적인 행동을 하는 사람을 검출하는 기술이 꾸준히 요구되고 있음

2. 해외 시장 동향 및 전망

- CMU의 OpenPose 기술은 RGB 영상으로부터 관절 정보를 추출해내는 기술로, 행동인식 기술의 전처리로 사용되는 경우가 많은데, 이 OpenPose 기술의 사용료는 한 대 당 연 25,000만 달러에 이름

- 3D 관절 정보를 가장 잘 추출하는 Microsoft의 Kinect는 2019년 v3를 내놓을 예정
- 3D 카메라의 세계 시장규모는 2015년 12.5억 달러에서 2021년 약 79억 달러로 성장할 것으로 전망(자료: Global 3D Camera Market Set for Rapid Growth to Reach Around USD 7.89 Billion by 2021)
- 모바일 3D 시장규모는 2015년 약 1.3억 대에서 2021년 약 23.4억 대로 성장할 것으로 예상(자료: Mobile 3D Market Size to Touch Nearly 2,337 Million Units By 2021)
- 세계 영상 감시 시장은 2016년부터 2022년까지 연평균 4.1% 성장하여 2022년에는 30.6억 달러에 이를 것으로 전망(자료: S&T Market Report)

3. 제품화 및 활용 분야

활용 분야(제품/서비스)	제품 및 활용 분야 세부내용
Human-care Robot	로봇이 사람의 행동 및 상태를 분석하여 적합한 대응을 할 수 있음
VR/AR Games	사용자 혹은 상대방의 행동을 정확하게 인식해 게임에 반영
CCTV	이상행동이나 범죄 등을 검출 및 인식해 신속한 대응 가능

V. 기대효과

- 기술도입으로 인한 경제적 효과
  - 로봇을 통해 안전에 비교적 취약한 고령자들의 가정 내에서의 사고 예방과 함께 생활 전반에 걸쳐 케어가 가능해져 고령화 사회를 맞이하여 사회적, 경제적으로 큰 효과가 기대됨
  - CCTV 등에서 부적절한 행동, 혹은 수상한 행동을 하는 사람에 대해 즉각적으로 자동 검출이 가능해져 범죄예방, 안전한 사회 구현 등에 큰 효과가 기대됨

주간기술동향 원고 공모

정보통신기획평가원은 주간기술동향의 ICT 기획시리즈에 게재할 **"스마트시티"** 분야 원고를 모집하고 있습니다.

관심 있는 전문가 분들의 많은 참여를 바랍니다.

❑ 원고 주제 : **스마트시티 관련 기술·시장·정책 동향**
(※ 제목과 목차는 저자가 자율적으로 결정)

❑ 제출 자격 : 대학, 연구기관, 산업체 재직자

❑ 접수 기간 : **2019년 9월 1일~10월 31일 기간 내 수시접수**

❑ 제 출 처 : 주간기술동향 원고접수메일(wttrends@iitp.kr)로 제출

❑ 원고 양식: 파일참조(원고양식)

❑ 원고 분량: 13페이지 내외

❑ 기타

- 게재 원고에 대하여 소정의 원고료 지급(200자 원고지 10,000원/1매, 최고 40만 원)
- 기획시리즈 칼럼은 매주 1편씩 발간 예정
- 원고제출 시 반드시 원고심의의뢰서(첨부파일참조)를 함께 제출하여 주시기 바랍니다.
- 게재된 원고로 인해 지적재산권 침해문제가 발생할 경우, 원고저자는 원고료 반환, 게시물 삭제 및 정보통신기획평가원이 입게 될 손실·비용에 대한 배상 등의 불이익을 받을 수 있습니다.

❑ 제출 및 문의처

- (34054) 대전광역시 유성구 화암동 58-4번지 정보통신기획평가원
기술정책단 산업분석팀 주간기술동향 담당
- Tel : 042-612-8296, 8214 / Fax : 042-612-8209 / E-mail : wttrends@iitp.kr

IITP 정보통신기획평가원

- 사업책임자: 문형돈(기술정책단장)
- 과제책임자: 이성용(산업분석팀장)
- 참여연구원: 이재환, 이효은, 이상길, 안기찬, 김용균, 정해식, 김우진, 장예지, 전영미(위촉)

주간기술동향

통권 1917호(2019-39)

발 행 년 월 일 : 2019년 10월 9일
발 행 소 : IITP 정보통신기획평가원
편집인겸 발행인 : 석제범
등 록 번 호 : 대전 다-01003
등 록 년 월 일 : 1985년 11월 4일
인 쇄 인 : ㈜승일미디어그룹

IITP 정보통신기획평가원

(34054) 대전광역시 유성구 유성대로 1548(화암동 58-4번지)
전화 : (042) 612-8296, 8214 팩스 : (042) 612-8209

깨끗한 IITP, 신뢰받는 IITP

IITP 정보통신기획평가원

http://www.iitp.kr

IITP 부정비리 신고센터