1918호
2019.10.16.
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
1918호
ISSN 1225-6447

chapter 1

사이버 보안 표준 및 위협 분석 기법 동향

도성룡 ‖ 상명대학교 특임교수

최근 사물인터넷 혁명으로 인해 자동차, 철도, 의료 등의 모든 산업 시스템들과 외부의 연결이 급격히 증가하고 있다. 이로 인해, 오늘날 거의 모든 시스템들은 다양한 사이버 보안 위협에 노출되어 있으며, 기술이 발전됨에 따라 이러한 위협은 더욱 증가할 것이다. 본 고에서는 산업 시스템들이 사물인터넷 기반의 CPS(Cyber Physical System) 패러다임으로 전환되는 흐름을 반영하여, 사이버 보안 사고를 사전에 예방하기 위한 관련 국제 표준 및 위협 분석 기법 동향에 대해 살펴본다.

I. 서론

고도화된 ICT 인프라를 통해 생성, 수집, 축적된 데이터와 인공지능이 결합한 지능정보기술이 경제, 사회, 삶 모든 분야에 보편적으로 활용됨으로써 새로운 가치를 창출하고 발전하는 사회를 지능정보사회라고 부른다[1].

지능정보사회에서는 모든 사물들이 유/무선으로 연결됨에 따라, 사이버 보안에 대한 중요성이 높아지고 있다. 특히, 자동차, 철도, 의료 등과 같은 안전 필수 시스템(Safety Critical System)의 보안 취약점은 치명적인 사고로 이어질 수 있으며, 사회적 이슈가

* 본 내용은 도성룡 특임교수(☎ 02-781-7667, imdsr@smu.ac.kr))에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.

OPEN 출처표시 상업용금지 공공누리 공공저작물 자유이용허락

되고 있다. 예를 들어, 자동차, 의료 등 안전 필수 시스템이 갖고 있는 보안 취약점을 해커들이 의도적으로 공격하는 사례가 증가하고 있다. 대표적으로 2015년 7월 크라이슬러의 지프(Jeep) 체로키의 컨트롤 시스템에 접속하여 자동차의 펌웨어를 변경 후 제어권을 탈취한 사례, 2017년 5월 워너크라이(Wanna Cry) 랜섬웨어 공격으로 영국의 국민건강서비스 산하 40여개 병원의 PC가 감염되어 모든 의료 서비스가 중단된 사례 등이 있다.

오늘날 거의 모든 소프트웨어 시스템은 다양한 사이버 보안 위협에 노출되어 있으며, 기술이 발전됨에 따라 위협은 더욱 증가할 것이다. 포브스 자료에 의하면, 2018년 2분기에 소프트웨어 취약성을 악용하는 악성 코드가 151% 증가했으며, 사이버 범죄 피해 비용은 2021년까지 6조 달러에 이를 것으로 추정되고 있다[2].

본 고에서는 최근에 자동차, 철도, 의료 등의 모든 산업 시스템들이 사물인터넷 기반의 CPS(Cyber Physical System) 패러다임으로 전환되는 흐름을 반영하여, 사이버 보안 사고를 사전에 예방하기 위한 관련 국제 표준 및 위협 분석 기법 동향에 대해 살펴본다.

II. 사이버 보안 개념

사이버 보안이란 무엇일까? 사이버 보안은 사이버 환경에서 네트워크를 통해 연결된 조직/사용자 자산을 보호하기 위해 사용되는 기술적 수단, 보안 정책, 개념, 보안 안전장치, 가이드라인, 위기관리방법, 보안 행동, 교육/훈련, 모범사례, 보안 보증, 보안 기술들의 집합을 의미한다[3].

사이버 보안은 정보 보안과 마찬가지로는 [표 1]의 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)을 목표로 한다[4].

[표 1] 사이버 보안의 목표

사이버 보안 목표	설명
기밀성(Confidentiality)	허락되지 않은 사용자 또는 객체가 정보의 내용을 알 수 없도록 함
무결성(Integrity)	허락되지 않은 사용자 또는 객체가 정보를 임의로 수정할 수 없도록 함
가용성(Availability)	허락된 사용자 또는 객체가 정보에 접근하려고 할 때 허용할 수 있도록 함

〈자료〉 Y. R. Hong & D. S. Kim., "Analysis of the Effects of Common Criteria Certification on the Information Security Solutions," Journal of Society for e-Business Studies, 17(4), 2013, pp.57-68.

하지만, 사이버 보안의 3가지 목표는 다양한 공격에 의해서 달성되지 않을 수 있다.

첫째, 기밀성(Confidentiality)은 위장(Impersonation), 스누핑(Snooping), 도청(Sniffing), 백도어(Backdoor), 트로이목마(Trojan Horse) 공격에 의해 위협받을 수 있다. 대표적으로 스누핑이란 네트워크 상의 중요 정보를 모르게 획득하는 행위를 의미하며, 백도어란 정상적인 인증 절차를 거치지 않고, 특정 시스템에 접근하는 행위를 의미한다.

둘째, 무결성(Integrity)은 변장(Masquerading), 스푸핑(Spoofing), 부인(Repudiation) 공격에 의해 위협받을 수 있다. 대표적으로 스푸핑이란 인터넷 프로토콜인 TCP/IP의 구조적 결함을 이용해 사용자의 시스템 권한을 획득한 뒤, 정보를 탈취하는 행위를 의미하고, 부인이란 메시지의 송수신자가 송수신 사실을 인정하지 않는 행위를 의미한다.

셋째, 가용성(Availability)은 서비스 거부(Denial of Service: DoS) 공격에 의해 위협받을 수 있다. 서비스 거부란 특정 시스템에 대량의 접속을 유발해 해당 시스템의 서비스를 마비시키는 행위를 의미한다.

사이버 보안의 목표를 위협하는 공격 유형은 기술이 발전함에 따라 계속해서 진화하고 있고, 우리 삶에 심각한 문제를 초래하고 있으며, 앞으로 더욱 큰 영향을 미칠 것이다. 이러한 문제를 해결하고자 사이버 보안 관련 국제 표준 개발 및 다양한 사이버 보안 위협 분석 기법 연구가 진행되고 있다. 본 고에서는 이와 관련하여 III장에서는 사이버 보안 국제 표준화 동향에 대해, IV장에서는 사이버 보안 위협 분석 기법에 대한 간략한 개요를 살펴본다.

III. 사이버 보안 국제 표준화 동향

사이버 보안 관련 국제 표준은 기존 정보 보안 관리 시스템(Information Security Management Systems)으로 알려진 ISO/IEC 27000 시리즈를 기반으로 사이버 보안에 특화하여 제정 중에 있다. 본 고에서는 [표 2]의 대표적인 사이버 보안 국제 표준에 대해서 살펴본다.

[표 2] 대표적인 사이버 보안 국제 표준 목록(표준 제정 현황은 2019년 8월 기준)

사이버 보안 국제 표준	표준 명칭	제정 현황
ISO/IEC 27100	Information technology -- Cybersecurity -- Overview and concepts	WD
ISO/IEC 27101	Information technology -- Security techniques - Cybersecurity -- Framework development guidelines	WD
ISO/IEC 27102	Information security management -- Guidelines for cyber-insurance	IS
ISO/IEC 27103	Information technology -- Security techniques -- Cybersecurity and ISO and IEC Standards	IS(TR)
ISO/IEC 27032	Information technology -- Security techniques -- Guidelines for cybersecurity	IS(개정 중)

* 국제 표준 제정 단계
  - WD: Working Draft의 약자, 국제표준 워킹그룹에서 초안을 준비하는 단계
  - CD: Committee Draft의 약자, 국제표준 위원회에서 초안을 검토하는 단계
  - DIS: Draft International Standard의 약자, 초안이 등록되어, 모든 위원들의 찬반 의견을 수렴하는 단계
  - FDIS: Final Draft International Standard의 약자, 모든 위원들의 2/3이상 찬성할 경우, FDIS가 됨
  - IS: International Standard의 약자, 최종적으로 국제 표준으로 채택됨
* TR은 Technical Report를 의미
〈자료〉 ISO/IEC 27100: Information technology -- Cybersecurity -- Overview and concepts
ISO/IEC 27101: Information technology -- Security techniques - Cybersecurity — Framework development guidelines
ISO/IEC 27102: Information security management -- Guidelines for cyber-insurance
ISO/IEC 27103: Information technology -- Security techniques -- Cybersecurity and ISO and IEC Standards
ISO/IEC 27032: Information technology -- Security techniques -- Guidelines for cybersecurity

1. ISO/IEC 27100

ISO/IEC 27100의 명칭은 Information technology -- Cybersecurity -- Overview and concepts이고[5], 2019년 8월 기준 WD(Working Draft) 상태이며, 2021년 제정을 목표로 하고 있다. 본 표준은 ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection에서 담당하고 있다. 주요 내용은 사이버 보안에 관한 전반적인 개념과 시리즈 표준에서 사용되는 사이버 보안 관련 정의를 포함하고 있다.

2. ISO/IEC 27101

ISO/IEC 27101의 명칭은 Information technology -- Security techniques - Cybersecurity -- Framework development guidelines이고[6], 2019년 8월 기준 WD 상태이며, 2020년 제정을 목표로 하고 있다. 본 표준은 ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection에서 담당하고 있다. 주요 내용은 조직에서 사이버 보안 프레임워크를 개발하고 구축하기 위한 가이드라인을

포함하고 있다. 사이버 보안 프레임워크를 Identify, Protect, Detect, Respond, Recover의 단계로 구분하고, 각 단계별 입력과 출력 그리고 세부 활동을 정의하고 있다. 또한, 국가별 사이버 보안 프레임워크를 소개하고 있다.

3. ISO/IEC 27102

ISO/IEC 27102의 명칭은 Information security management -- Guidelines for cyber-insurance이고[7], 2019년 8월 기준 IS(International Standard) 상태이다. 본 표준은 ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection에서 담당하고 있다. 주요 내용은 조직 내 사이버 사고로 인한 영향을 관리하기 위한 방안으로서, 사이버 보험을 도입하기 위한 가이드라인을 포함하고 있다. 즉, 사이버 보험 개요, 사이버 보험 정책, 사이버 보험이 커버하는 사이버 사고의 유형, 사이버 보험 지원 측면에서 ISMS(Information Security Management System)의 역할 등의 내용을 담고 있다.

4. ISO/IEC 27103

ISO/IEC 27103의 명칭은 Information technology -- Security techniques -- Cybersecurity and ISO and IEC Standards이고[8], 2019년 8월 기준 IS 상태이다. 본 표준은 ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection에서 담당하고 있다. 주요 내용은 조직이 정보 보안 표준을 기반으로 사이버 보안 프레임워크를 활용하여 체계적으로 사이버 보안을 관리하기 위한 방법에 대한 내용을 포함하고 있다. 즉, 위험 기반(Risk-based), 우선순위 지정(Prioritized), 성과 중심(Outcome-focused) 등의 속성을 기반으로 하는 사이버 보안 프레임워크의 목표와 활용 방법에 대해서 설명하며, 기존 표준들과의 매핑 정보를 제공한다.

5. ISO/IEC 27032

ISO/IEC 27032의 명칭은 Information technology -- Security techniques -- Guidelines for cybersecurity이고[9], 2019년 8월 기준 IS 상태이고, 개정 중이다. 본

표준은 ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection에서 담당하고 있다. 주요 내용은 사이버 보안 개요, 사이버 보안과 다른 보안 유형 간의 관계, 이해 관계자의 정의와 사이버 보안에서의 역할, 일반적인 사이버 보안 문제를 해결하기 위한 지침에 대한 내용을 포함하고 있다. 또한, ISO/IEC 27001에 명시된 사이버 보안 프레임워크를 기반으로 맬웨어(Malware), 허가받지 않은 단체의 공격 준비, 공격 탐지 및 모니터링, 공격에 대응하는 모범 사례를 제공한다.

IV. 사이버 보안 위협 분석 기법

사이버 보안 위협 분석은 가상의 공격자 관점에서 시스템의 구조적 취약점과 같은 잠재적인 위협을 식별 및 분류하고, 영향도를 평가하며, 우선순위를 지정하는 프로세스로, 본고에서는 [표 3]의 대표적인 사이버 보안 위협 분석 기법에 대해서 설명한다.

[표 3] 대표적인 사이버 보안 위협 분석 기법 목록

사이버 보안 위협 분석 기법	개발기관/개발자
STRIDE	Microsoft
PASTA	Tony UcedaVelez, Marco M. Morana
OCTAVE	SEI
TVRA	ETSI
STPA-sec	Nancy Leveson, William Young

〈자료〉 Hernan, S., Lambert, S., Ostwald, T., & Shostack, A., "Threat modeling-uncover security design flaws using the stride approach," MSDN Magazine-Louisville, 2006. pp.68-75.
Tony U., & Marco M., "Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis," John Wiley & Sons, 2015, pp.1-696.
Christopher A., Audrey D., James S., & Carol W., "Introduction to the OCTAVE Approach," SEI, 2003, pp.1-37.
"ETSI TS 102 165-1 v4.2.3 - Telecommunications and Internet converged Services and Protocols for Advanced Networking(TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis," 2011, pp.1-79.
Young, W., & Leveson, N., "Systems thinking for safety and security," In Proceedings of the 29th Annual Computer Security Applications Conference, 2013, pp.1-8.

1. STRIDE

STRIDE(Spoofing identify, Tampering with data, Repudiation, Information

disclosure, Denial of service, Elevation of privilege)는 Microsoft사에서 1999년에 개발한 보안 위협 모델링 방법이다. STRIDE는 인증, 무결성, 부인 방지, 기밀성, 가용성, 권한 부여와 같은 보안 속성을 고려하고, DFD(Data Flow Diagram)의 개체, 프로세스 등에 존재하는 위협을 식별한다[10]. 예를 들어, 사용자란 개체에 Spoofing identify 키워드를 적용할 때, 해커가 사용자로 위장하여, 시스템 접근 권한을 획득한다와 같은 위협을 식별할 수 있다.

[표 4] STRIDE의 위협 분류 및 정의

STRIDE 위협	관련 보안 속성	위협 정의
Spoofing identify	인증(Authentication)	거짓된 계정 등을 이용하여 시스템 접근 권한 획득함
Tampering with data	무결성(Integrity)	불법적으로 데이터를 변경함
Repudiation	부인 방지 (Non-repudiation)	특정 서비스를 수행하지 않았다고 부인하거나 책임이 없다고 부인함
Information disclosure	기밀성(Confidentiality)	접근 권한이 없는 누군가에게 정보를 제공함
Denial of service	가용성(Availability)	서비스 또는 애플리케이션이 정상적으로 수행되지 않게 함
Elevation of privilege	권한 부여(Authorization)	누군가가 권한을 부여받아 권한이 없는 서비스를 수행함

〈자료〉 Hernan, S., Lambert, S., Ostwald, T., & Shostack, A., "Threat modeling-uncover security design flaws using the stride approach," MSDN Magazine-Louisville, 2006. pp.68-75.

2. PASTA

PASTA(The Process for Attack Simulation and Threat Analysis)는 Tony Uceda Velez와 Marco M. Morana가 2012년에 개발한 리스크 기반의 위협 모델링 프레임워크이다. PASTA의 목적은 방어자가 자산 중심의 완화 전략(Asset Centric Mitigation Strategy)을 개발할 수 있는 응용 프로그램 및 인프라에 대한 공격자 중심의 관점(Attacker Centric View)을 제공하는 것이다. PASTA는 동적인(Dynamic) 위협을 식별 및 열거하고, 스코어링(Scoring)하는 등의 7단계 프로세스를 정의하고 있다.

PASTA의 프로세스는 [그림 1]과 같이 비즈니스의 목적을 정의하는 단계(Step 1. Define Objectives), 위협 분석할 인프라, 애플리케이션 등의 범위를 정의하는 단계(Step 2. Define Technical Scope), Use Case, DFD(Data Flow Diagram)를 이용하여 애플리케이션을 분해하는 단계(Step 3. Application Decomposition), 공격 시나리오 분석

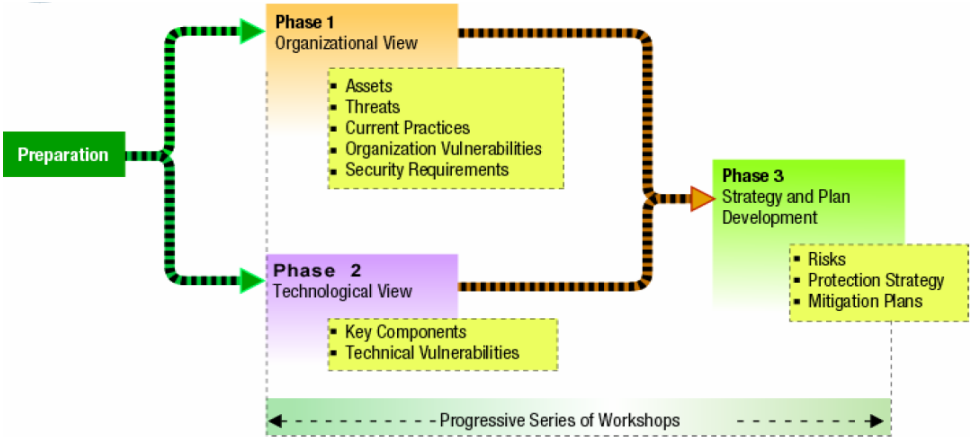
〈자료〉 Tony U., & Marco M., "Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis," John Wiley & Sons, 2015, pp.1-696.

[그림 1] PASTA 적용 프로세스

등을 통해 위협을 분석하는 단계(Step 4. Threat Analysis), 취약점을 분석하는 단계(Step 5. Vulnerability & Weakness Analysis), 공격 트리 등을 개발하는 공격 모델링 단계(Step 6. Attack Modeling), 위협에 따른 정성적/정량적 리스크의 영향을 분석하는 단계(Step 7. Risk & Impact Analysis)로 구성되어 있다[11].

3. OCTAVE

OCTAVE(Operationally Critical Threat Asset and Vulnerability Evaluation)는 카네기멜론대학의 SEI(Software Engineering Institute)에서 2003년에 개발한 위협 분



〈자료〉 Christopher A., Audrey D., James S., & Carol W., "Introduction to the OCTAVE Approach," SEI, 2003, pp.1-37.

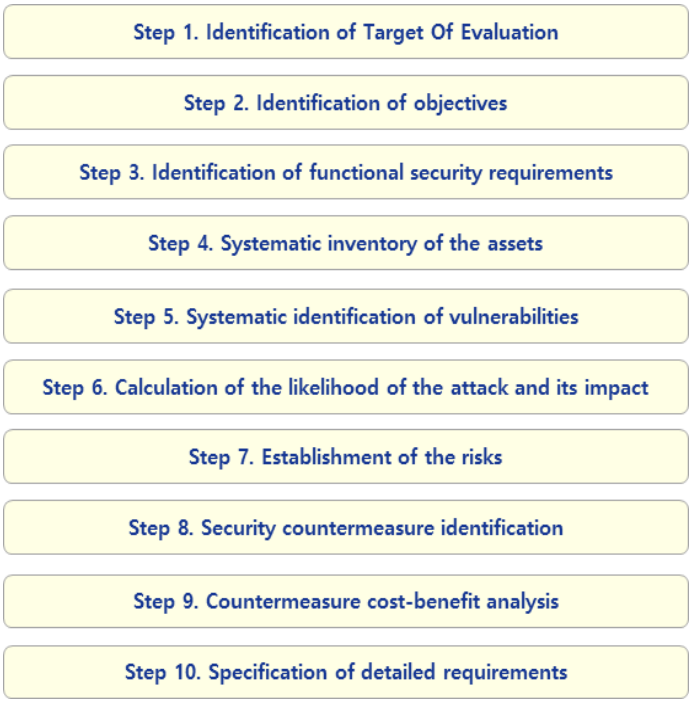
[그림 2] OCTAVE 적용 프로세스

석 및 리스크 평가 방법론이다. OCTAVE의 목적은 조직의 리스크 관리를 체계적으로 수행하기 위해 운영자 중심의 위협 모델링(Operations Centric Threat Modeling) 방법을 제공하는 것이다. OCTAVE는 조직 내부의 전문가들로 분석팀을 구성하여 정보의 수집 및 분석, 전략을 개발하는 등의 자가 진단(Self-Direction) 방식으로 추진한다는 특징이 있다. OCTAVE는 조직의 비즈니스 수행에 필요한 중요 자산과 자산에 대한 위협과 취약성을 식별하고, 리스크를 완화하기 위한 전략을 수립하는 프로세스를 정의하고 있다.

OCTAVE의 프로세스는 [그림 2]와 같이 조직 자산에 기초하여 위협 프로파일을 구축하는 단계(Phase 1. Organizational View), 인프라의 취약성을 정의하는 단계(Phase 2. Technological View), 보안전략 및 계획 개발 단계(Phase 3. Strategy and Plan Development)로 구성되어 있다[12].

4. TVRA

TVRA(Threat, Risk, Vulnerability Analysis)는 ETSI(European Telecommunications Standards Institute)에서 2011년에 통신 시스템의 위협 분석 및 리스크 평가를 위해 개발한 방법론이다. TVRA는 위협의 대상이 되는 주요 자산을 식별하고, 현장에서 개인의



〈자료〉 "ETSI TS 102 165-1 v4.2.3 - Telecommunications and Internet converged Services and Protocols for Advanced Networking(TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis," 2011, pp.1-79.

[그림 3] TVRA 적용 프로세스

안전과 주요 인프라의 운영에 미치는 영향에 대해 평가하기 위한 시나리오를 도출한다. 시나리오는 식별된 위협, 해당 위협에 영향을 받는 개체 및 결과를 포함한 관련 조건으로 구성된 가상의 상황을 의미한다.

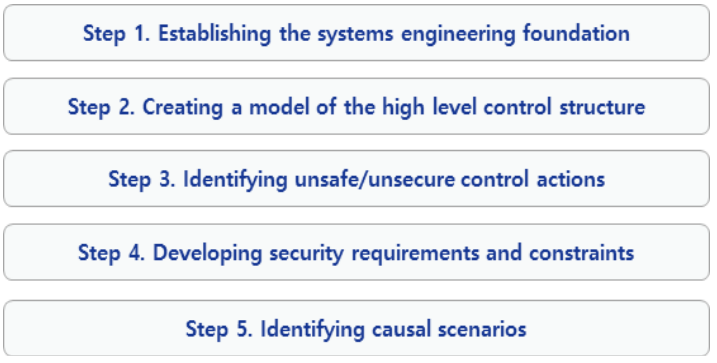
TVRA의 프로세스는 [그림 3]과 같이 평가 대상(Target Of Evaluation)을 식별하는 단계(Step 1. Identification of Target Of Evaluation), 해결해야 할 보안 목표를 식별하는 단계(Step 2. Identification of objectives), 기능적 보안 요구사항을 식별하는 단계(Step 3. Identification of functional security requirements), 자산을 물리적(Physical), 인적(Human), 논리적(Logical) 목록으로 분류하는 단계(Step 4. Systematic inventory of the assets), 취약점을 체계적으로 식별하는 단계(Step 5. Systematic identification of vulnerabilities), 공격 가능성과 영향도를 정량화하는 단계(Step 6. Calculation of the likelihood of the attack and its impact), 리스크(Risks)를 결정

하는 단계(Step 7. Establishment of the risks), 리스크를 완화하기 위한 보안 대책을 식별하는 단계(Step 8. Security countermeasure identification), 리스크 저감 보안 대책에 대해 비용과/이점을 분석하는 단계(Step 9. Countermeasure cost-benefit analysis), 상세한 보안 요구사항을 명세하는 단계(Step 10. Specification of detailed requirements)로 구성되어 있다[13].

5. STPA-sec

STPA-sec(System Theoretic Process Analysis for Security)은 MIT의 Nancy Leveson, William Young이 2013년에 개발한 시스템 이론 기반의 사이버 보안 분석 기법이다. Nancy Leveson 교수가 제안한 STAMP(System Theoretic Accident Model and Processes) 기반의 해저드 분석 기법인 STPA(System Theoretic Process Analysis)를 사이버 보안 분야에 적용한 방법이다.

STPA-sec의 프로세스는 [그림 4]와 같이 시스템이 최종적으로 로스(Loss)를 보는 상황을 식별하는 단계(Step 1. Establishing the systems engineering foundation), 상위 수준의 제어 구조도를 작성하는 단계(Step 2. Creating a model of the high level control structure), 제어 명령(Control Action)이 로스로 이어질 수 있는 잘못된 경우를 식별하는 단계(Step 3. Identifying unsafe/unsecure control actions), Unsafe/Unsecure한 제어 명령을 완화하거나 제거하기 위한 보안 요구사항과 제약사항을 개발하



〈자료〉 Young, W., & Leveson, N., "Systems thinking for safety and security," In Proceedings of the 29th Annual Computer Security Applications Conference, 2013, pp.1-8.

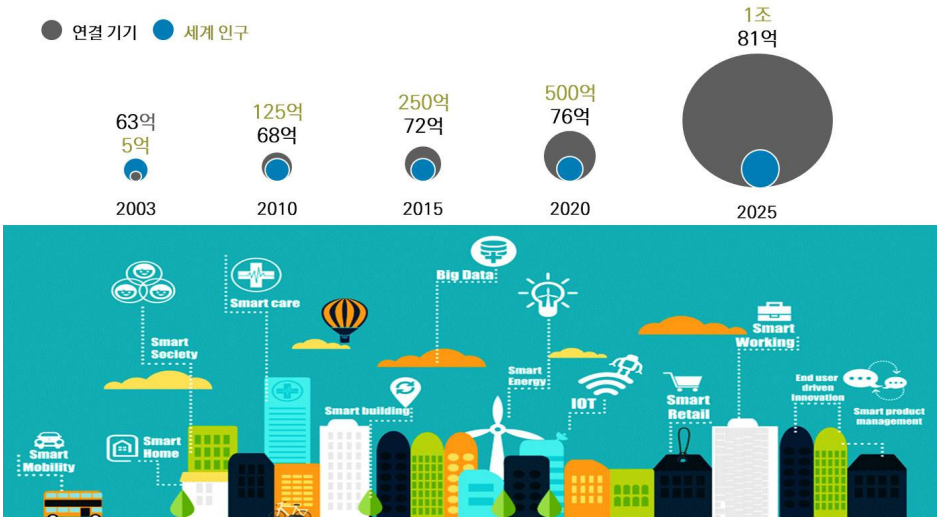
[그림 4] STPA-sec 적용 프로세스

는 단계(Step 4. Developing security requirements and constraints), 보안 요구사항과 제약사항을 위반할 수 있는 다양한 시나리오를 분석하는 단계(Step 5. Identifying causal scenarios)로 구성되어 있다[14].

이 외에도 LINDDUN(Linkability, Identifiability, Nonrepudiation, Detectability, Disclosure of Information, Unawareness, Noncompliance)[15], CVSS(Common Vulnerability Scoring System)[16], Attack Tree[17], Security Cards[18], HTMM (Hybrid Threat Modeling Method)[19], Trike[20], VAST(Visual, Agile, and Simple Threat) Modeling[21] 등 다양한 사이버 보안 위협 분석 기법이 활용되고 있다.

V. 맺음말

최근 전 세계를 대상으로 하는 사이버 보안 사고가 계속해서 증가하고 있다. 특히, 사물인터넷 혁명으로 인해 [그림 5]와 같이 자동차, 철도, 의료 등의 모든 산업 시스템들의 경우 외부와의 연결이 급격히 증가함에 따라[22], 이로 인한 사이버 보안 사고는 더욱 증가할 것이다.



〈자료〉 Evans, D., "The internet of things: How the next evolution of the internet is changing everything," CISCO white paper, 2011, pp.1-11.

[그림 5] 사물인터넷 혁명으로 인한 시스템의 연결성 증가

이에 미국과 영국 등 선진 국가를 중심으로 사이버 보안 전담 부처 또는 기관을 설립하여 대응 전략을 시행하는 등 정책적인 노력을 하고 있다. 또 한편으로는 사이버 보안 필수 시스템의 체계적인 개발을 위해 국제 표준 및 사이버 보안 위협 분석 기법에 관한 연구가 활발히 진행 중에 있다.

이의 일환으로 본 고에서는 사이버 보안 관련 국제 표준으로 ISO/IEC 27100, ISO/IEC 27101, ISO/IEC 27102, ISO/IEC 27103, ISO/IEC 27032에 대한 개요와 제정 현황을 소개하였다. 또한, STRIDE, PASTA, OCTAVE, TVRA, STPA-sec 등의 사이버 보안 위협 분석 기법의 소개와 프로세스를 살펴보았다.

본 고에서 살펴본 사이버 보안 관련 국제 표준이 제정되면, 시스템 개발에 반드시 적용하도록 요구할 것이다. 또한, 관련된 사이버 보안 위협 분석 기법에 대해서도 적용을 요구할 것이다. 이미 선진 조직들은 사이버 보안 표준에서 요구하는 내용과 위협 분석 기법을 적용한 연구들을 발표하고 있다. 하지만 국내 조직들은 이러한 흐름에 많이 뒤쳐진 것이 현실이다.

국내 조직들은 시스템의 안전성 확보를 위해 관련 표준과 해저드 분석 기법 적용에 집중해 왔다. 이제는 사이버 보안과 안전성을 통합하는 연구로 흐름이 변화하고 있다. 국내 조직들이 이러한 흐름을 이해하고, 적용할 수 있도록 관련 역량을 확보하기 위한 다양한 연구와 국가적 지원이 필요하다.

[참고문헌]

[1] 최양희, “지능정보사회 중장기 종합대책 추진방향”, 관계부처 합동, 2016, pp.1-72.
[2] Chuck Brooks, “A Scoville Heat Scale For Measuring Cybersecurity,” Forbes, 2018.
[3] 심현보, “정보 보안에서 사이버 보안까지”, 한국과학기술정보연구원, 2014. pp.1-5.
[4] Y. R. Hong & D. S. Kim., “Analysis of the Effects of Common Criteria Certification on the Information Security Solutions,” Journal of Society for e-Business Studies, 17(4), 2013, pp.57-68.
[5] ISO/IEC 27100: Information technology -- Cybersecurity -- Overview and concepts.
[6] ISO/IEC 27101: Information technology -- Security techniques - Cybersecurity -- Framework development guidelines.
[7] ISO/IEC 27102: Information security management -- Guidelines for cyber-insurance.
[8] ISO/IEC 27103: Information technology -- Security techniques -- Cybersecurity and ISO and IEC Standards.

[9] ISO/IEC 27032: Information technology -- Security techniques -- Guidelines for cybersecurity.
[10] Hernan, S., Lambert, S., Ostwald, T., & Shostack, A., "Threat modeling-uncover security design flaws using the stride approach," MSDN Magazine-Louisville, 2006. pp.68-75.
[11] Tony U., & Marco M., "Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis," John Wiley & Sons, 2015, pp.1-696.
[12] Christopher A., Audrey D., James S., & Carol W., "Introduction to the OCTAVE Approach," SEI, 2003, pp.1-37.
[13] "ETSI TS 102 165-1 v4.2.3 - Telecommunications and Internet converged Services and Protocols for Advanced Networking(TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis," 2011, pp.1-79.
[14] Young, W., & Leveson, N., "Systems thinking for safety and security," In Proceedings of the 29th Annual Computer Security Applications Conference, 2013, pp.1-8.
[15] Wuyts, K., & Joosen, W., "LINDDUN privacy threat modeling: a tutorial," 2015, pp.1-38.
[16] Mell, P., Scarfone, K., & Romanosky, S., "Common vulnerability scoring system," IEEE Security & Privacy, 4(6), 2006, pp.85-89.
[17] Potteiger, B., Martins, G., & Koutsoukos, X., "Software and attack centric integrated threat modeling for quantitative risk assessment," In Proceedings of the Symposium and Bootcamp on the Science of Security, 2016, pp.99-108.
[18] Tamara D., Batya F., Tadayoshi K,, "Poster - the security cards: a security threat brainstorming toolkit," University of Washington, 2013.
[19] Mead, N., Shull, F., Vemuru, K., & Villadsen, O., "A Hybrid Threat Modeling Method," Carnegie Mellon University - Software Engineering Institute, 2018, pp.1-53.
[20] Saitta, P., Larcom, B., & Eddington, M., "Trike v1 methodology document," 2005, pp.1-17.
[21] Agarwal, A., "Vast methodology: Visual, agile, and simple threat modeling," Prescott Valley, 2016.
[22] Evans, D., "The internet of things: How the next evolution of the internet is changing everything," CISCO white paper, 2011, pp.1-11.

chapter 2

시설 관리 및 재난 대응을 위한 드론 통신 및 보안 기술 동향

왕기철 ‖ 한국전자통신연구원 책임연구원
이병선 ‖ 한국전자통신연구원 실장
안재영 ‖ 한국전자통신연구원 단장

I. 서론

드론 혹은 UAV(Unmanned Aerial Vehicle)는 조종사를 비행하는 기체에 태우지 않고 원격으로 조종하거나 자율적으로 비행하며 탑재된 임무 장비를 이용하여 자신의 임무를 수행하는 비행 장치를 의미한다. 최근 들어, 드론 관련 기술이 비약적으로 발전함에 따라 드론에 대한 관심이 일반 대중은 물론 공공기관, 산업계, 학계 등에서 커지고 있으며, 다양한 비행 기체들이 등장하고 있다. 드론의 주요 응용 분야로는 댐, 공장, 건물, 교량, 터널, 전력망, 가스관, 태양광 패널 등과 같은 주요 인프라를 감시하는 시설 인프라 관리 응용, 재난/재해의 예측, 상황 파악, 복구 지원을 수행하는 재난 지원 응용, 교통 상황 감시, 순찰, 범인 추적, 실종자 수색을 수행하는 치안 응용, 환경 데이터 수집 및 정밀 기상 관측을 수행하는 환경 탐사 응용, 3차원 정밀 지도 및 건축물 영상 분석 등을 수행하는 공간정보 구축 및 관리 응용, 농작물 작황 및 경작지 상태 감시와 병충해 감시 및 대응 등을 수행하는 정밀 농임업 응용, 해양상태 및 오염지도 제작과 양식장 관리 및 어획 등을

* 본 내용은 왕기철 책임연구원(☎ 042-860-1377, gcwang@etri.re.kr)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.
***본 논문은 2019년도 ETRI 정부출연금의 재원으로 수행된 연구결과임(19ZR1110, 초실감 공간미디어 원천기술 개발)

OPEN 출처표시 상업용금지 공공누리 공공저작물 자유이용허락

[표 1] 드론의 주요 응용 분야

분야	세부 응용 기술
드론 이용 시설 인프라 관리 기술	① 드론 이용 교통 인프라(교량, 도로, 터널 등) 관리 기술 ② 드론 이용 에너지 인프라(발전시설, 전력망, 가스관, 태양광 패널 등) 관리 기술 ③ 드론 이용 통신 인프라 관리 기술 ④ 드론 이용 주요시설(댐, 공장, 건물 등) 관리 기술
드론 이용 재난 재해 감시 및 대응기술	① 드론 이용 자연재해 감지 및 예측 기술 ② 드론 이용 재난·재해 현장 상황 파악 기술 ③ 드론 이용 화재 감시 및 진화 기술 ④ 드론 이용 재난·재해 구조 및 복구 기술 ⑤ 극한 환경 하에서의 탐색 기술 ⑥ 재난·재해 감지 및 예측을 위한 드론 획득 데이터 처리 기술
드론 이용 치안 기술	① 드론 이용 지상 교통 상황 감시 기술 ② 드론 이용 순찰 기술 ③ 드론 이용 범인/차량 탐지 및 추적 기술 ④ 드론 이용 실종자/조난자 수색 기술
드론 이용 환경탐사 기술	① 드론 이용 미세먼지 데이터 수집 기술 ② 드론 기반 광역 환경 데이터 수집 무빙 센서 네트워크 기술 ③ 드론 이용 녹조·적조 데이터 수집 기술 ④ 드론 이용 정밀 기상 관측 기술 ⑥ 환경 오염 감지 및 예측을 위한 드론 획득 데이터 처리 기술
드론 이용 공간정보 구축 및 관리 기술	① 드론 이용 3D 정밀 맵 생성 기술 ② 드론 이용 지상 적재물 부피 측정 기술 ③ 시계열 3D 맵 데이터 관리 및 분석 기술 ④ 다수 드론 지도 데이터 통합 기술 ⑤ 드론 이용 건축물 영상분석(BIM 등) 기술
드론 이용 정밀 농·임업 기술	① 드론 이용 농작물 작황 모니터링 기술 ② 드론 이용 농작물 파종 및 병충해 대응 기술 ③ 드론 이용 경작지 상태 모니터링 기술 ④ 드론 이용 삼림 병충해 감시 및 예측 기술 ⑤ 드론 이용 수목 분포 관리 기술
드론 이용 정밀 수산업 기술	① 드론 이용 해양 상태·오염 지도 제작 기술 ② 드론 이용 해양 어종 및 분포 확인 기술 ③ 드론 이용 양식장 관리 기술 ④ 드론 이용 어획(fishing) 기술

〈자료〉 한국전자통신연구원 자체 작성

수행하는 정밀 수산업 응용 등이 있다. [표 1]은 이러한 드론의 다양한 응용들을 정리하였다.

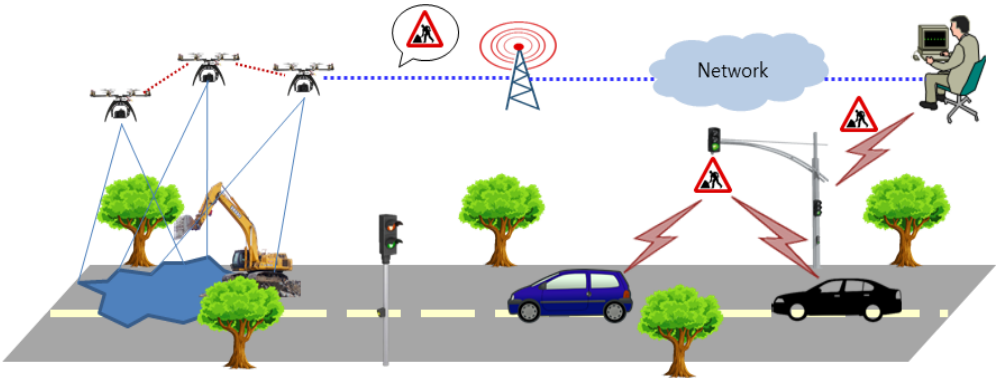
한편, 드론을 원격으로 조종하거나 자율적으로 비행하도록 하기 위해서는 여러 기술들이 필요하며, 대표적으로는 통신 및 보안기술, 탐지 및 인식 기술, 자율비행 기술, 배터리 기술, 카운터 드론 기술, 비행 제어 기술, 자동 착륙 기술, 군집 및 협력 비행 기술 등이

있다. 본 고에서는 다양한 드론 핵심 기술들 중에서 통신 및 보안 기술을 다루는데, 이는 드론의 안전한 정보 교환과 신뢰성 있는 드론의 제어는 고신뢰도의 안전한 통신과 보안 기술 없이는 획득할 수 없기 때문이다. 먼저, II장에서는 기존에 상용화되었거나 소개된 드론 응용들 중에서 시설 인프라 관리 및 재난 대응에 관한 대표적인 응용들을 하나씩 자세히 소개하며, III장에서는 시설 인프라 관리 및 재난 대응 응용들을 지원하기 위해 필요한 통신 및 보안 기술들을 살펴보고, IV장에서는 본 고의 결론을 제시한다.

II. 시설관리 및 재난 대응을 위한 드론 기반의 응용

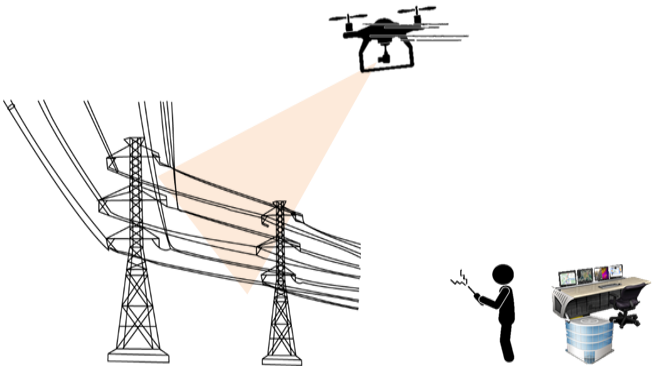
도로 인프라 관리 응용으로, 도로 상에서 긴급한 공사를 진행해야 하는 경우에 드론을 띄워서 현 도로 상의 공사 상황을 신속히 교통관리체계 서버에 전파할 수 있다. 이후에 교통관리체계 서버는 드론들로부터 수집되는 정보를 통합하고 체계화하여 도로 상의 차량들이 공사 지점들을 신속히 파악할 수 있도록 공지하고, 공사 지점을 우회할 수 있는 우회도로를 안내함으로써 교통정체를 완화시킬 수 있다[1]. 또한, 도로 상의 표지판이나 신호등, 교차로, 횡단보도 등의 교통 인프라를 감시하여 신속한 정비를 통해 교통사고를 미연에 방지할 수 있다. [그림 1]은 드론을 이용한 교통 인프라 관리 응용을 보여준다.

전력선은 사람이 육안으로 직접 결함이나 파손 여부를 점검하기에는 위험이 따르고,



〈자료〉 H. Menouar, I. Guvenc, K. Akkaya, A. S. Uluagac, A. Kadri, and A. Tuncer, “UAV-Enabled Intelligent Transportation Systems for the Smart City: Applications and Challenges,” IEEE Communications Magazine, Vol.55, No.3, Mar. 2017, pp.22-28.

[그림 1] 드론 기반의 교통 인프라 관리 응용

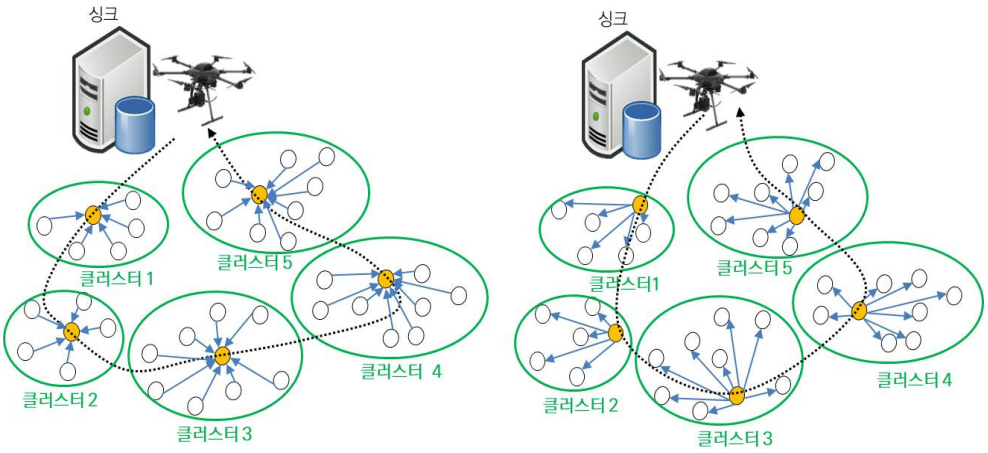


〈자료〉 한국전자통신연구원 자체 작성

[그림 2] 드론 기반의 송전선 및 송전탑 점검 응용

많은 시간이 소요되는 문제점이 발생한다. 드론이 촬영하는 이미지들을 이용하면 전력선의 파손 여부를 정확히 파악하는데 큰 도움이 되고, 이에 따른 위험성이나 인력 낭비를 크게 줄일 수 있음이 증명되었다[2]. [그림 2]는 드론 기반의 전력선 점검 응용을 보여준다.

해양에서 녹조나 적조의 발생 현황을 조사하거나 원자력 발전소의 방사능이 누출되어 토질 오염을 조사하는 경우에 드론이 활용될 수 있다. 이때 드론 단독으로 임무를 수행하는 것 보다는 감시 센서들을 조사 지역에 배치하여 조사 데이터를 수집하도록 하고, 드론이 각 지역에서 수집된 데이터를 비행하면서 모으는 것이 더 효율적이다. 드론은 이렇게

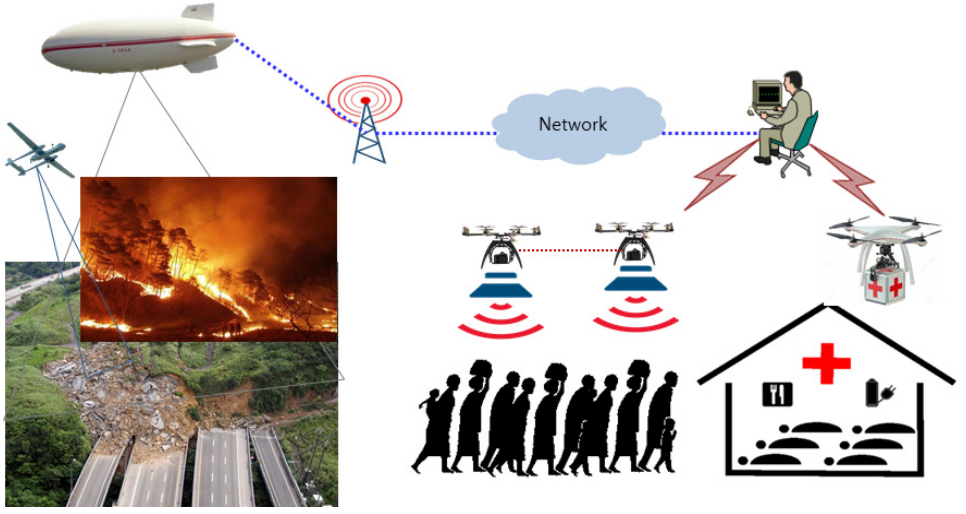


〈자료〉 한국전자통신연구원 자체 작성

[그림 3] 드론 기반의 재난 상황 파악 응용

모아진 데이터를 싱크에 전달하고, 싱크는 수집된 데이터를 분석하여 의사결정을 위한 데이터를 생성할 수 있다. [그림 3]은 드론 기반의 재난 상황 파악 응용을 보여주는 것으로 오른쪽 그림에서 보는 것처럼 드론을 이용하여 센서 노드들에게 특정 정보를 신속하게 배포할 수도 있다.

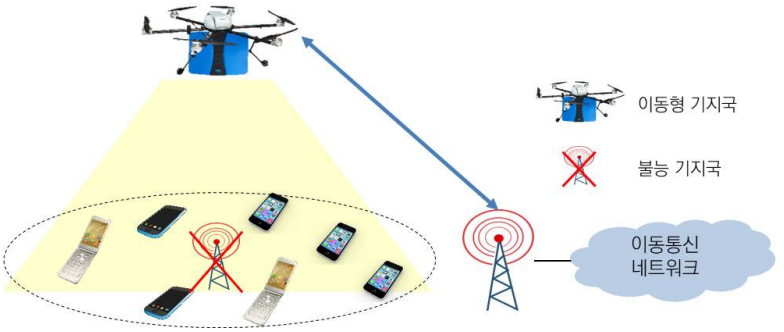
드론을 통한 재난 상황 감시 응용은 지진, 홍수, 산사태, 화재, 해일과 같은 재난 상황이 발생하기 전에 이를 조기에 감지하여 주변의 주민들이 대피하도록 알림으로써, 인명 피해를 획기적으로 줄일 수 있게 해준다. 또한, 재난이 발생한 경우에, 그 피해 상황을 신속하고 정확하게 파악할 수 있게 해준다. [그림 4]는 드론을 이용한 재난 감지 및 예측 응용을 보여준다.



〈자료〉 한국전자통신연구원 자체 작성

[그림 4] 드론 기반의 재난 감지 및 예측 응용

재난이 발생한 경우에 해당 지역의 이동통신 서비스 제공 인프라가 일부 혹은 완전 붕괴되어 가입자들의 통신이 불가능해지거나 원활하지 않게 되는 경우가 발생한다. 이때, 재난으로 이동통신 서비스가 불가능하거나 병목현상으로 느린 서비스를 제공받는 가입자들은 드론이라는 이동형 기지국들을 통해 정상적인 이동통신 서비스를 제공받을 수 있다. 2016년 미국에서는 Global City Teams Challenge를 통해 드론을 통한 LTE 기지국 서비스를 구현하였으며, 직경 2km 이내의 영역에서 128명의 사용자에게 서비스를 지원하였다[3]. [그림 5]는 드론을 이용한 이동통신 서비스 제공 응용을 보여준다.



〈자료〉 한국전자통신연구원 자체 작성

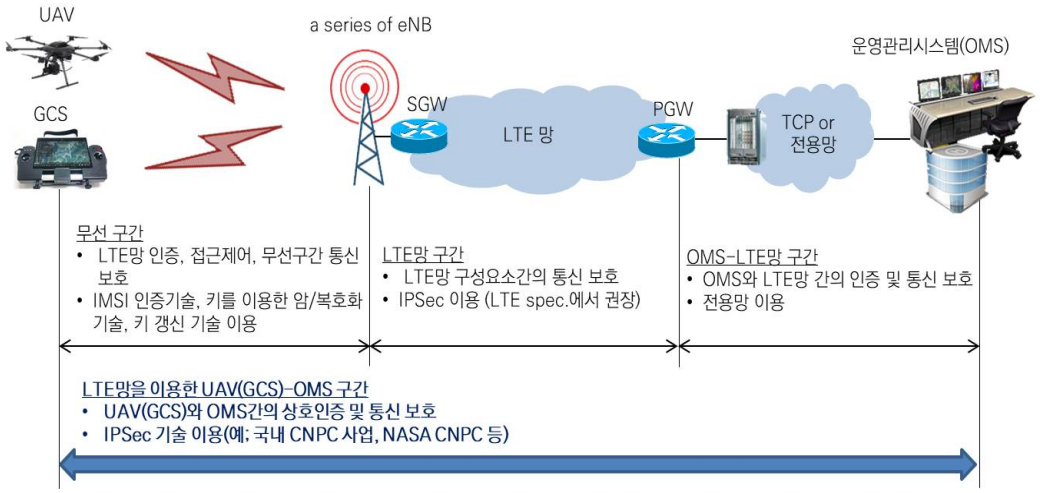
[그림 5] 드론 기반의 이동통신 서비스 지원 응용

III. 드론 기반 응용을 위한 통신 및 보안 방안

원격지 조종사가 드론을 제어하고 드론으로부터 위치, 자세, 상태 등의 정보를 수신하기 위한 무선 통신 기술로는 널리 사용되고 있는 WiFi(802.11 a/b/g/n)부터 IEEE 802.16, XBee-PRO, LTE, P-34/TETRA Enhanced Data Service(TEDS), C대역 통신 등이 있다. 일반적으로 드론 기반의 시설 관리 및 재난 응용에서는 신속한 상황 보고 및 영상 전송, 빠른 응답 등을 위해 가능한 고속의 무선 통신 기술을 이용할 필요가 있다. 따라서 전송속도와 지연 및 기술 성숙도에서 유리한 LTE, WiFi, C대역 통신 중에서 적절한 하나를 선택하거나 이들을 적절히 조합하여 사용한다. 본 고에서는 이러한 시설 인프라 관리 및 재난 대응을 위한 통신 및 통신들의 조합을 살펴보고, 각 통신 및 통신 조합을 보호하기 위한 보안 방안도 같이 살펴본다.

1. LTE 기반의 통신 및 보안 방안

일반적으로 드론을 이용한 시설 관리 및 재난 대응을 위한 응용에서는 단일 드론을 이용하기보다는 다중의 드론을 임무에 투입하여 임무수행의 효율화, 단일 실패점 문제해결, 협력 임무의 분할 수행 등의 이점을 얻을 수 있다[4]. 또한, 이러한 다중 드론을 이용한 효율적 임무수행 및 관리를 위해서는 다중 드론의 운영관리시스템(Operation Management



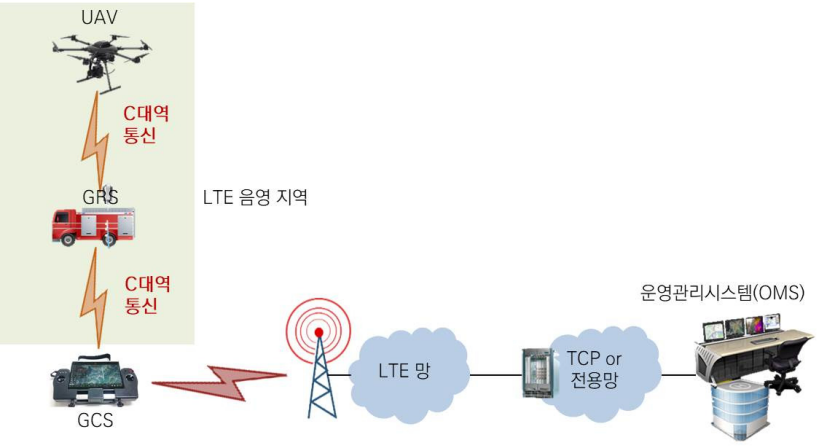
〈자료〉 한국전자통신연구원 자체 작성

[그림 6] LTE 네트워크를 이용한 통신 및 보안

System: OMS)을 두어서, 이들의 임무수행을 모니터링하고 제어할 필요가 있다. OMS를 통한 다중 드론의 임무 관리는 드론의 조종기와 드론 간 통신이 항상 운영관리시스템을 통해 이루어지게 함으로써, 모든 드론의 상황을 중앙집중적으로 통제하고 관리하게 된다. 만일 드론의 조종사와 드론이 비행하는 영역이 모두 LTE 서비스 영역 내에 있는 경우에는 LTE 네트워크를 통해 다중 드론과 그들의 조종사를 연결할 수 있다. [그림 6]은 LTE 네트워크를 이용한 시설관리 및 재난 대응 통신과 보안 구조를 보여준다. 이러한 통신 구조에서 통신 구간은 세 개의 구간으로 분리되며, 각 구간은 이미 검증이 완료된 보안 기술들을 활용하여 통신 보호가 가능하다. 그러나 종단간의 통신(즉, 드론과 OMS 혹은 GCS(Ground Control Station)와 OMS간 통신) 구간은 정해진 보안 기술이 없으며, 이를 위해서는 IPSec(Internet Protocol Security)과 같은 종단간 통신 보안 기술을 사용하는 것이 필요하다[5]. 실제로, 국내의 CNPC 과제나 미국 NASA의 CNPC 시범 사업 등도 모두 IPSec을 기반으로 종단간 통신 보안을 구현하였다.

2. C대역 기반의 통신 및 보안 방안

C대역(5,030~5,091MHz: 제어용, 5,091~5,150MHz: 임무용)을 이용한 드론 통신은



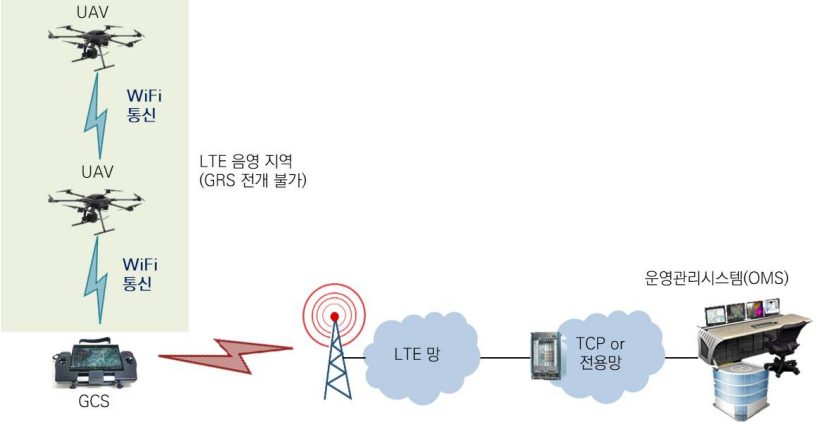
* TCP: Transmission Control Protocol
〈자료〉 한국전자통신연구원 자체 작성

[그림 7] C대역 통신을 이용한 통신 및 보안

두 가지 형태로 구분될 수 있다. 하나는 드론과 조종기가 모두 LTE 음영지역에 존재하기 때문에, C대역 GRS(Ground Relay Station)를 통해 조종기가 직접 드론을 제어하는 통신이다. 이 경우에 드론은 자신의 자세 및 위치 정보를 GCS를 통해 OMS에 전달한다. 반대로, GCS에서 드론으로 전달하는 제어 정보는 GRS를 통해 직접 드론으로 전달된다. 이 경우에 보안은 GCS와 드론 간에 상호 인증을 수행하고, 이후 키 설정을 통해 생성된 키를 이용한 암복호화를 통해 이루어져야 한다. 다른 형태의 C대역 통신은 드론이 LTE 서비스 음영지역에서 비행하고 조종기는 LTE 서비스 영역에 존재하는 경우이다. [그림 7]은 이러한 C대역 통신과 LTE 통신이 결합된 예를 보여준다. 즉, 드론의 자세와 위치정보 등은 GCS를 통해 LTE 네트워크 종단에 있는 OMS로 전달된다. 반대로, GCS의 제어 명령은 GRS를 통해 드론에 직접 전달함과 동시에 같은 메시지가 LTE 네트워크를 통해 OMS에게 전달된다. 이러한 통신 구조에서 LTE 무선 구간에 있는 GCS와 OMS는 IPSec과 같은 종단간 보안 방법을 이용해야 한다. 또한, GCS와 드론간 보안은 상호인증 후에 키 설정을 수행하여 암복호화를 제공하는 방법으로 수행되어야 한다. 이 경우에 보안은 선 공유된 비밀키 기반의 단순한 상호인증 후에 이를 기반으로 공유키를 설정하는 방식 혹은 IPSec이나 TLS(Transport Layer Security)처럼 인증서 기반의 상호 인증 후에 보안협상을 통해 공유키를 설정하는 약간 복잡한 방식 모두 가능하다.

3. WiFi와 LTE 네트워크 결합 통신 및 보안 방안

드론이 임무를 수행하는 도중에, LTE 음영지역이지만 이동형 C대역 GRS를 배치하여 사용할 수 없는 곳(터널)으로 들어가야 하는 경우가 발생한다. 이 상황에서는 드론 간 WiFi 통신 중계를 활용하여 임무수행 드론을 제어하고, 임무수행 드론의 영상 및 위치 정보 등을 수신할 수 있다. [그림 8]은 WiFi 통신과 LTE 네트워크가 결합된 통신 및 보안을 보여준다. 드론에 대한 제어 정보를 전송하는 경우에 GCS는 제어 메시지를 중계 드론을 통해 임무수행 드론에 전달하고, 동시에 같은 메시지를 LTE 네트워크를 통해 OMS에 전송한다. 이 경우에 GCS와 중계드론, 그리고 임무수행 드론은 FANET(Flying Ad-hoc NETwork)를 형성하므로, FANET 보안기법들을 이용하여 해당 구간의 통신을 보호해야 한다. FANET은 MANET(Mobile Ad-hoc NETwork)의 특수한 한 종류로 볼 수 있으나, 이동성과 위상 변화가 심하고 이로 인한 링크 단절 및 품질 저하가 자주 발생하는 문제점이 있다. 이러한 속성들로 인해 FANET에 보안기술을 적용하는 것은 MANET에 비해 더 어렵다[6]. [표 2]는 FANET과 MANET의 속성 비교를 보여 준다. 이러한 속성들을 가진 FANET의 통신을 보호하기 위해서는, 먼저 통신 주체 간에 인증서 기반의 상호 인증을 수행해야 한다. 이러한 인증서 교환은 통신 주체 간의 RREQ(Route REQuest) 및 RREP (Route REPly) 메시지의 교환 시에 첨부되어 교환될 수 있다. 상호 인증이 완료 되면, 통신 주체 간에 데이터를 전달해 줄 정상적인 노드들로만 구성된 안전한 경로를 설정



〈자료〉 한국전자통신연구원 자체 작성

[그림 8] WiFi와 LTE 통신을 이용한 통신 및 보안

[표 2] FANET과 MANET의 속성 비교

속성	FANET	MANET
연결성	낮은 노드 밀도	높은 노드 밀도
	낮은 연결성	높은 연결성
	낮은 확장성	보통의 확장성
이동 모델	고속 이동	저속 이동
	상시적 이동	간헐적 이동
	3차원 위상	2차원 위상
	3차원 이동	2차원 이동
위상 변화	잦은 링크 단절	간헐적 링크 단절
	잦은 링크 품질 저하	간헐적 링크 품질 저하

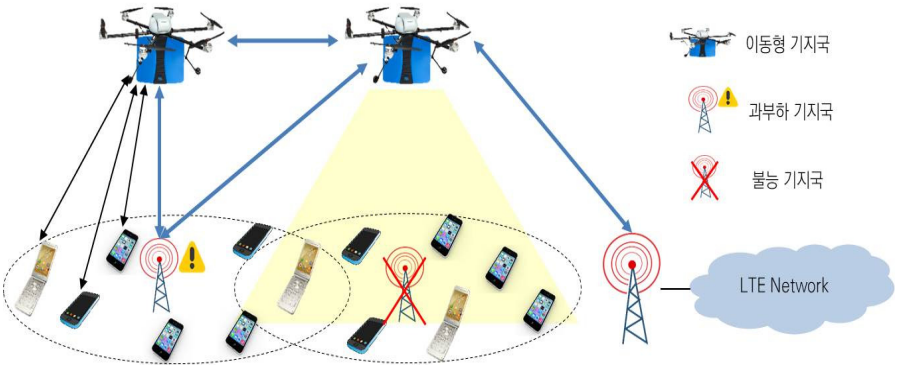
〈자료〉 한국전자통신연구원 자체 작성

해야 한다. FANET에서 안전한 통신 경로 설정 방법들로는 PASER(Position-Aware, Secure, and Efficient mesh Routing)나 SUAP(Secure UAV Ad hoc routing Protocol)이 있다[6]. 다음으로, 경로 중간에 있는 노드들은 부분키를 각각 생성하여 통신 주체들에게 안전하게 전송하고, 통신 주체들은 수신된 부분키들을 조합하여 둘 사이에 세션키를 설정할 수 있다[7]. 이 세션 키를 이용하여 통신 주체 간의 메시지를 안전하게 보호할 수 있다.

LTE 음영지역에서 임무를 수행하는 드론의 상태 및 임무 정보는 중계 드론을 통해 GCS로 전달되고, GCS는 다시 이를 LTE 네트워크를 통해 OMS에게 전달하게 된다. 이 경우에 임무수행 드론과 GCS 간은 FANET 보안을 이용하고, GCS와 OMS 간은 IPSec과 같은 종단간 보안 프로토콜을 사용하여 통신을 보호해야 한다.

4. 재난 지역 이동통신 서비스 제공 통신 및 보안 방안

[그림 9]는 드론을 이용한 LTE 서비스 영역 확장 통신 및 보안을 보여준다. 이때, 이동형 기지국인 드론과 LTE 네트워크 간의 통신은 LTE 네트워크 자체에서 제공하는 보안 서비스를 통해 보호될 수 있다. 반면에, [그림 9]와 같이 이동형 기지국들과 고정형 기지국들 간의 연결은 FANET을 형성하게 되며, 앞서 살펴본 FANET 보안 기법들을 이용하여 통신을 보호할 수 있다.



〈자료〉 한국전자통신연구원 자체 작성

[그림 9] 드론을 이용한 LTE 서비스 영역 확장 통신 및 보안

한편, 이동형 기지국 서비스를 제공하는 드론은 가능한 오랫동안 공중정지(hovering) 비행을 수행하는 것이 필요하나, 제한된 용량의 전원을 장착하여 비행하게 되므로 전원을 보충하기 위한 방법이 필수적이다[8]. 이를 위해서 지근거리에 완충된 드론을 대기시켰다가 전원이 소진된 드론과 교대하는 방법과 지근거리에 완충된 배터리를 구비했다가 전원이 소진된 드론이 오면 완충된 배터리로 교환해주는 방법이 있다. 다만, 이 방법은 배터리 혹은 드론을 교체하는데 소요되는 시간 동안, 서비스가 중단되는 문제점이 있다. 또 다른 방법은 근거리에 있는 높은 건물 옥상에서 레이저와 같은 무선 전파를 이용하여 공중정지 비행하는 드론을 실시간으로 재충전하는 방법이다. 이 방법은 서비스 중단 시간이 없다는 장점이 있으나, 드론과 무선 충전장치 사이에 장애물이 없어야 동작한다.

Ⅳ. 결론

본 고에서는 드론의 주된 응용 분야들 중에서 시설 인프라 관리 및 재난 대응에 관한 대표적인 응용들을 하나씩 자세히 소개하였다. 또한, LTE, WiFi, C대역 통신 및 이들의 적절한 조합을 통해 이들 응용들을 위한 통신을 제공할 수 있음을 보였으며, 이러한 통신을 보호하기 위한 보안 방안들을 살펴보았다. 드론의 통신 및 보안 방안과 관련된 과제로서, 드론이 비행 전에 교통관리 서버와 상호 인증을 수행하고 이를 통해 키를 설정한 후에, 이 키를 통해 드론이 방송하는 정보의 기밀성과 무결성을 보호하는 과제가 현재 진행되고

있다. 이 과제에서는 상호인증을 위해 TLS의 공개키 기반 구조를 이용하고, 암호 알고리즘으로는 AES의 GCM(Galois Counter Mode) 모드를 사용한다. 최근에는 양자 난수 생성 및 유선 및 무선 구간에서의 양자 키분배도 활발히 연구되고 있어서, 드론 통신의 보안에 적용되면 보안 수준을 크게 높일 것으로 기대된다. 일반적인 드론은 부착된 배터리의 수명 동안 비행을 수행하며 촬영, 모니터링, 수색, 데이터 수집 등의 임무를 수행한다. 그러나 재난 상황에서 이동 기지국 서비스 제공 등을 수행하는 드론은 공중정지 비행을 장기간 수행해야 하므로, 서비스 정지 시간을 최대한 줄이면서도 실시간으로 전원을 보충하거나 교체하는 방안이 마련되어야 한다.

[참고문헌]

[1] H. Menouar, I. Gűvenc, K. Akkaya, A. S. Uluagac, A. Kadri, and A. Tuncer, "UAV-Enabled Intelligent Transportation Systems for the Smart City: Applications and Challenges," IEEE Comm. Mag., 55(3), Mar. 2017, pp.22-28.

[2] M. H. Frederiksen, O. V. Mouridsen, and M. P. Knudsen, "Drones for inspection of infrastructure: Barriers, opportunities and successful uses," Tech. Memo, Southern Denmark University: 30.05.2019, Jun. 2019.

[3] K. Namuduri, "When Disaster Strikes, Flying Cell Towers Could Aid Search and Rescue," IEEE Spectrum, Aug. 2017.

[4] A. Tsourdos, B. White, and M. Shanmugavel, "Cooperative Path Planning of Unmanned Aerial Vehicles," American Institute of Aeronautics and Astronautics, John Wiley & Sons, Ltd, Nov. 2010.

[5] I. Vidal, F. Valera, M. A. Diaz, and M. Bagnulo, "Design and Practical Deployment of a Network-Centric Remotely Piloted Aircraft System," IEEE Comm. Mag., 52(10), Oct. 2014, pp.22-29.

[6] O. S. Oubbati, A. Lakas, F. Zhou, M. Guneş, M. B. Yagoubi, "A Survey on Position-based Routing Protocols for Flying Ad Hoc Networks(FANETs)," Vehicular Communications, 10, 2017, pp. 29-56.

[7] G. Wang and G. Cho, "Compromise-Resistant Pairwise Key Establishments for Mobile Ad hoc Networks," ETRI Journal, 28(3), Jun. 2006, pp.375-378.

[8] B. Galkin, J. Kibilda, and L. A. DaSilva, "UAVs as Mobile Infrastructure: Addressing Battery Lifetime," IEEE Comm. Mag., 57(6), Jun. 2019, pp.132-137.

chapter 3-1

5G 네트워크 제어 플랫폼 기술

최영일 ‖ 한국전자통신연구원 책임연구원

I. 결과물 개요

개발목표시기	2019. 8.	기술성숙도(TRL)	개발 후 TRL 6
결과물 형태	SW-Platform	검증방법	자체검증
Keywords	5G 코어 네트워크, AMF, SMF		
외부기술요소	100% 개발 기술	권리성	특허, SW, SW-IP, 설계문서

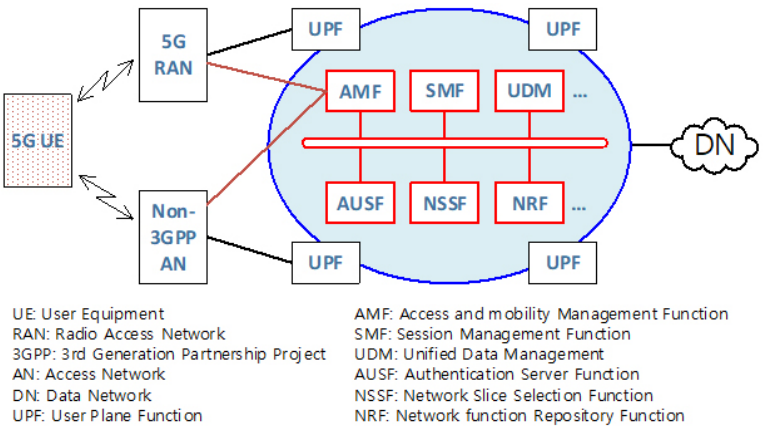
II. 기술의 개념 및 내용

1. 기술의 개념

➢ 5G네트워크는 코어망와 액세스망으로 구성되며, 액세스망은 사용자로부터의 무선접속을 제공하는 반면 코어망은 5G UE(사용자)의 위치 및 사용자 정보를 관리, 인증하고

* 본 내용은 최영일 책임연구원(☎ 042-860-3763)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

사용자가 데이터 서비스를 사용할 수 있도록 세션 연결을 제공하며, 또한 ATSSS(Access Traffic Steering, Switchg, Splitting)을 위한 접속관리, 세션관리 기능을 포함

- 본 기술은 사용자가 5G RAN(Radio Access Network) 또는 Non-3GPP AN(Access Network)의 액세스망을 통한 5G 네트워크 서비스를 제공할 수 있는 5G 네트워크 제어 플랫폼으로, 서비스 제공을 제어하는 제어 평면과 사용자의 데이터 전달을 담당하는 데이터 평면으로 구분되며, 제어평면은 AMF(Access and mobility Management Function), SMF(Session Management Function)를 비롯한 다양한 제어 기능 요소로 구성됨
- 5G UE로부터의 접속 요청에 대해, 접속망이 다르더라도 일관된 시그널링 절차를 통해 접속 서비스를 인증하고 해당 사용자의 위치를 등록/관리하며 접속 서비스를 제공함
- 성공적으로 접속된 5G UE로부터의 세션 요청에 대해 접속망이 다르더라도 일관된 시그널링 절차를 통해 세션 서비스를 검증하고 해당 사용자가 데이터 네트워크의 데이터 서비스를 사용할 수 있도록 세션 서비스를 제공함

2. 기술의 상세내용 및 사업화 제약사항

- 기술의 상세내용
  - AMF(Access and mobility Management Function) 기술

- SMF(Session Management Function) 기술
- 5G 네트워크 기능 에뮬레이터 기술

➢ 기술이전 범위

- AMF(Access and mobility Management Function) 기술
  ※ N1 NAS(Non Access Stratum) 시그널 처리 기술
  ※ N2AP 시그널 처리 기술
  ※ UEID(UE Identifier) 관리 기술
  ※ 다중 접속 및 등록 상태 관리 기술
  ※ 다중 세션 신호 라우팅 기술
- SMF(Session Management Function) 기술
  ※ N1 NAS SM(Session Management) 시그널 처리 기술
  ※ 세션 관리 기술
  ※ UPF 선택 기술
  ※ IP주소 할당 관리 기술
  ※ QoS 관리 기술
  ※ UP PFCP(Packet Forwarding Control Protocol) 콘텍스트 관리 기술
  ※ ATSSS를 위한 다중 Leg 관리 기술
  ※ Interim UPF 관리 기술
- 5G 네트워크 기능 에뮬레이터 기술
  ※ UDM(Unified Data Management) 에뮬레이션 기술
  ※ AUSF(Authentication Server Function)
  ※ NSSF(Network Slice Selection Function)
  ※ NRF(Network function Repository Function)
  ※ 5G BS 에뮬레이션 기술
  ※ 5G UE/OAM 에뮬레이션 기술

➢ 사업화 제약사항

- Policy Control Function(PCF)는 제공되지 않으며 사업화 시에 사업자의 용도에 맞추어 적용이 필요

- 인증 및 보안에 필요한 암호화 알고리즘은 포함되지 않으며 사업화 시에 사업자의 용도에 맞추어 적용이 필요

III. 국내외 기술 동향 및 경쟁력

1. 국내 기술 동향

➢ 삼성전자

- 5G 표준 Rel.15를 적용한 통신 칩 엑시노스 모뎀 5100의 무선 송수신 시험에 성공
- 엑시노스 모뎀 5100은 하나의 칩으로 5G뿐만 아니라 GSM/CDMA, WCDMA/TD-SCDMA/HSPA, LTE 등을 모두 지원하는 '멀티모드' 방식
- 6GHz 이하 주파수 대역에서 4G보다 1.7배 빠른 2Gbps를 지원하고, 초고주파 대역에서는 5배 빠른 6Gbps를 지원

➢ LG전자

- 2019년 상반기 스프린트에 5G 스마트폰을 공급할 계획
- LTE기반 V2X(Vehicle to Everything) 단말 및 자율주행 안전기술 개발에 성공
- 5G기반 V2X 기술을 적극 개발 중

2. 해외 기술 동향

➢ 미국

- 인텔은 디바이스에서 데이터센터에 이르는 네트워크 전체까지 진출하기 위해 노력하고 있으며, 이동통신 네트워크와 와이파이, cmWave/mmWave 대역에서 끊김 없는 통신을 위한 기술을 개발 중
- 퀄컴은 다양한 기기들 간의 직접통신(Device to Device: D2D) 및 고품질의 네트워크 서비스를 제공하기 위한 스몰셀을 통한 네트워크 구축에 필요한 기술을 개발 중

➢ 유럽

- 노키아는 면허/비면허 대역에서 기존 무선기술 및 새로운 무선전송 기술을 포함하여,

다중 안테나(Massive Multiple-Input Multiple-Output: MIMO) 기술, cmWave/mmWave 기술, 진전된 변복조 기술, 다수 Radio Access Technology(RAT) 통합 기술, 무선 가상화 기술, 고속 이동성 제공 기술 등 전 분야의 기술을 개발 중

- 에릭슨은 고속 모바일 데이터 트래픽 및 Machine to Machine, 동시 전송 기술인 “Dual Connectivity” 기술 등을 포함한 전 분야의 기술을 개발 중

➢ 일본

- NEC는 Software Defined Networking(SDN)/Network Functions Virtualization (NFV)를, 파나소닉은 모바일 데이터 트래픽 처리, 사물인터넷 등의 새로운 애플리케이션의 적용 기술을 개발 중

➢ 중국

- 화웨이는 2009년 이후 5G 이동통신 네트워크 기술개발에 착수하여, RAN을 경유한 데이터들을 효과적으로 백본망으로 유도하기 위한 자율 백홀, Device-to-Device (D2D) 통신, 동적 주파수 재분배 및 무선 액세스 인프라 공유 등을 적용한 5G 네트워크 전 분야의 기술을 개발 중
- ZTE는 네트워크 용량만 강화하는 것이 아니라 사용자의 경험(user experience) 향상을 위한 안테나 효율성, 셀 사이트 밀도 향상 및 주파수 활용대역 확대 등을 포함한 기술을 개발 중

3. 표준화 동향

➢ ITU

- 2015년 ITU(International Telecommunication Union)에서 5G요구사항이 담긴 5G 비전 권고와 함께 5G를 IMT-2020으로 승인하면서 표준화가 시작
- eMBB(Enhanced Mobile BroadBand), MTC(Machine Type Communication), URLLC(Ultra-Reliable Low-Latency Communication)의 서로 다른 세 가지 시나리오를 제시
- 2019년 7월까지 각 표준화기관으로부터 IMT-2020 후보 기술을 제안 받아 2020년 2월까지 제안된 기술에 대한 평가 및 의견 수렴을 거쳐 2020년 10월에 IMT- 2020

표준을 완료할 예정

➢ 3GPP

- 다수의 국제 표준화 단체 중 유일하게 5G기술을 표준화하고 있는 단체
- Release 14(2014.9~2017.6)에서 5G기술의 타당성, 요구사항 등을 연구
- Release 15(2016.9~2018.6)에서 5G기술 표준화로 TS23.501, TS23.502, TS23.503을 작성
- Release 16(2017.3~2020.3)에서 5G기술 phase2의 표준화로 TS23.501, TS23.502, TS23.503을 업데이트하고 기타 새로운 기능을 위한 표준안을 작성 중

  ※ Vertical and LAN Services, Vehicle to Everything(V2X), Cellular IoT(CIoT), Network Automation(eNA), Ultra-Reliable Low-Latency Communication (URLLC), Service Based Architecture(SBA), Network Slicing 등이 최근 주목받고 활발히 연구 중인 study item임

- 한국전자통신연구원은 유/무선 액세스에 비종속적인 Unified Access Control을 제공하기 위한 기술, 다중 액세스를 이용한 ATSSS를 위한 기술, 네트워크 슬라이싱 기술, 네트워크 자동화, 버티컬랜 등의 기술과 관련된 표준화 활동을 진행 중

4. 기술의 경쟁력

경쟁기술	본 기술의 우수성 및 차별성
LTE	➢ LTE에 비해 빠른 데이터 속도 및 유연한 네트워크 구성이 가능 - 4G와 5G의 기술적인 차이에서 기인됨
노키아	➢ 노키아 기술에 비해 본 기술은 저렴하고, 소스레벨로 신규 서비스 추가가 용이함 - 노키아 기술은 높은 가격대를 형성, 신규서비스 요구 시에 대응이 늦은 문제점이 있음 - 본 기술은 적은 금액으로 신뢰도와 안정성을 추구할 수 있으며, 신규서비스 도입에 용이한 소스레벨로 제공되므로 빠른 대응이 가능함
에릭슨	➢ 에릭슨 기술에 비해 본 기술은 저렴하고, 소스레벨로 신규 서비스 추가가 용이함 - 에릭슨 기술은 높은 기술 신뢰도와 안정성을 제공하지만 가장 높은 가격대를 형성하고 있으며, 신규 서비스 추가 시에도 높은 가격의 지불이 필요함 - 본 기술은 적은 금액으로 신뢰도와 안정성을 추구할 수 있으며, 신규 서비스 도입에 용이한 소스 레벨로 제공함
화웨이	➢ 망운용 안정성 및 보안 위협이 있으나 본 기술은 안전함 - 최근 화웨이 장비의 안정성과 보안 이슈가 국내외적으로 제기되고 있음 - 본 기술은 소스레벨로 제공되어 안정성과 보안 문제를 담보할 수 있음

Ⅳ. 국내외 시장 동향 및 전망

1. 국내 시장 동향 및 전망

➢ 5G 국내 시장 동향

- 5G 기술은 3GPP에서 표준화하고 있어, 국내 시장 동향을 별도로 조사하기 어려움
- 3GPP 표준화에 국내업체로는 삼성전자와 LG전자가 적극적으로 참여하고 있음

➢ 5G 국내 시장 전망

- 4G(LTE)에 총 20.6조를 투자한 바 있으며 5G에는 5년간 7.5조를 투자할 계획으로 알려짐(2018년 국회국정감사, 이데일리사)
- 5G 코어망은 전체 5G 투자액의 1%인 750억 이상으로 추산 가능하며, 5G에서 앞으로 개발될 새로운 기술의 적용을 위해 지속적인 유지보수 및 성능 개선 수요가 있을 것으로 예측됨

2. 해외 시장 동향 및 전망

➢ 5G 해외 시장 동향

- 고속 데이터에 대한 요구뿐만 아니라 모바일 데이터 서비스에 대한 수요, 통신망의 소프트화에 대한 요구, M2M 통신의 증가 등으로 5G 기술이 개발되고 시장이 형성되고 있음
- 미국의 인텔과 퀄컴, 유럽의 노키아와 에릭슨, 일본의 NEC, 미쓰비시, 파나소닉, 중국의 화웨이와 ZTE, 한국의 삼성전자와 LG전자가 주요 제조사임

➢ 5G 해외 시장 전망

- 5G 인프라 시장은 2020년에 20.86억 달러(약 2조 4,500억 달러)에 이를 것으로 예상되며, 이후 연평균 50.9% 성장하여 2026년에는 330.72억 달러(약 38조 7,000억)에 이를 것으로 전망되고 있음(MarketsandMarkets사)
- 5G 코어망의 시장규모는 전체 시장의 3%이상일 것으로 추산되며, 그 중 5G 네트워크 제어 플랫폼은 다시 5G 코어망 시장의 30% 정도로 추산됨

3. 제품화 및 활용 가능 분야

활용 분야(제품/서비스)	제품 및 활용 분야 세부내용
5G네트워크 제어플랫폼	➢ 5G의 제어 평면을 위한 플랫폼 - 제어 평면, 데이터 평면이 분리된 5G 코어 네트워크의 제어 평면 플랫폼으로 활용
5G네트워크 AMF	➢ 5G의 접속 관리 기능 요소 - 5G 코어 네트워크의 접속 및 이동성 관리 기능요소로 활용 - Non-3GPP 접속, 다중 접속망 및 통합인증 프레임워크 지원
5G네트워크 SMF	➢ 5G의 세션 관리 기능 요소 - 5G 코어 네트워크의 세션 관리 기능요소로 활용 - 다중DN, 다중세션, 인터게이트웨이 핸드오버, ATSSS 등 지원
5G네트워크 서비스 개발 플랫폼	➢ 5G네트워크에서 부가 서비스를 개발하기 위한 플랫폼 - 5G의 phase2 표준화에서 연구 중인 새로운 서비스를 개발하고 적용할 플랫폼으로 활용 - Vertical and LAN Services, Vehicle to Everything(V2X), Cellular IoT(CIoT), Network Automation(eNA), Ultra Reliable Low Latency Communication(URLLC) 등의 개발에 활용 가능

V. 기대효과

1. 기술도입으로 인한 경제적 효과

➢ 본 기술과 직·간접으로 연관된 세계시장은 2020년 기준 약 2조 원으로 추정되며, 2026년까지 매년 50%씩 성장할 것으로 전망

➢ 전체 5G 시장에서 5G 네트워크 제어 플랫폼이 적용될 수 있는 세계 시장 규모는 2020년 기준 660억 원으로 추정되며, 2026년에는 1조 원으로 성장 전망

➢ 본 기술을 적용한 5G 네트워크 제어 플랫폼 제품의 시장점유율을 10%로 계산하면, 2020년 기준 20억 원, 2026년 기준 320억 원으로 전망

2. 기술사업화로 인한 파급효과

➢ 국내 5G 코어망 관련 산업 경쟁력 강화 및 생태계 복원

➢ 국내 5G에서의 부가서비스 관련 중소·중견 기업의 기술 발전 및 해외 시장 진출 기여

➢ 5G 네트워크 제어 플랫폼 기술을 활용한 5G 서비스 생태계 구축 및 미래성장동력 공급

chapter 3-2

메트로 액세스 네트워크용 200Gb/s 광트랜시버 및 광송수신기 기술

이준기 ‖ 한국전자통신연구원 책임연구원

I. 결과물 개요

개발목표시기	2019. 10.	기술성숙도(TRL)	개발 전	개발 후
			TRL 4	TRL 6
결과물 형태	HW-Module	검증방법	공인 시험성적 (확인)서	
Keywords	메트로 액세스 네트워크, 직접수신 고차 변복조, 광트랜시버, 광송수신기, 광전송 디지털 신호처리			
외부기술요소	100% 개발 기술	권리성	특허, 설계도, SW	

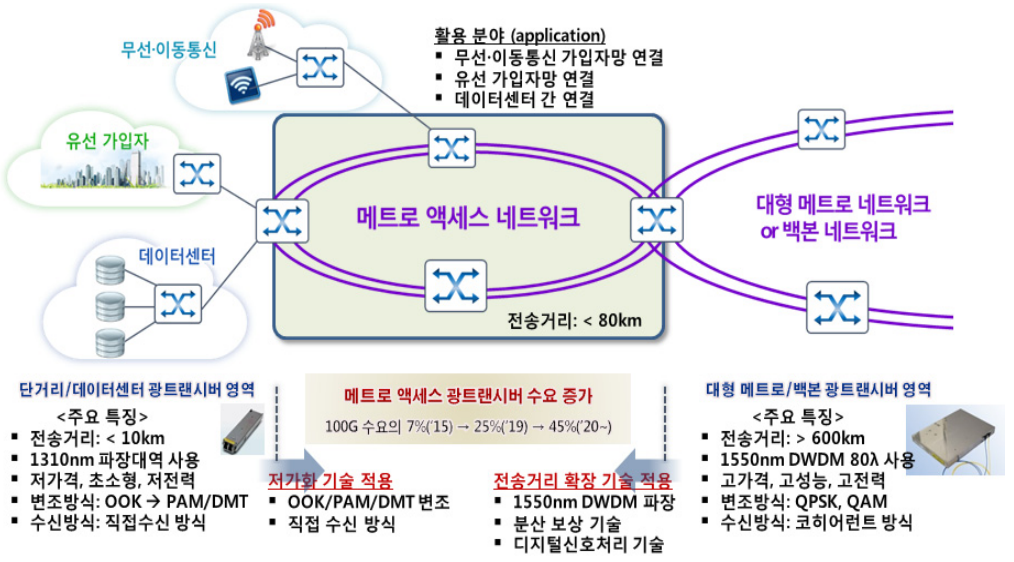
II. 기술의 개념 및 내용

1. 기술의 개념

➢ 5G, 빅데이터, IoT 등 초연결 서비스 등으로 인해 유무선 가입자 및 데이터센터 간 트래픽이 증가할 것이며, 이로 인해 소형 메트로 광전송 수요가 급증할 전망임

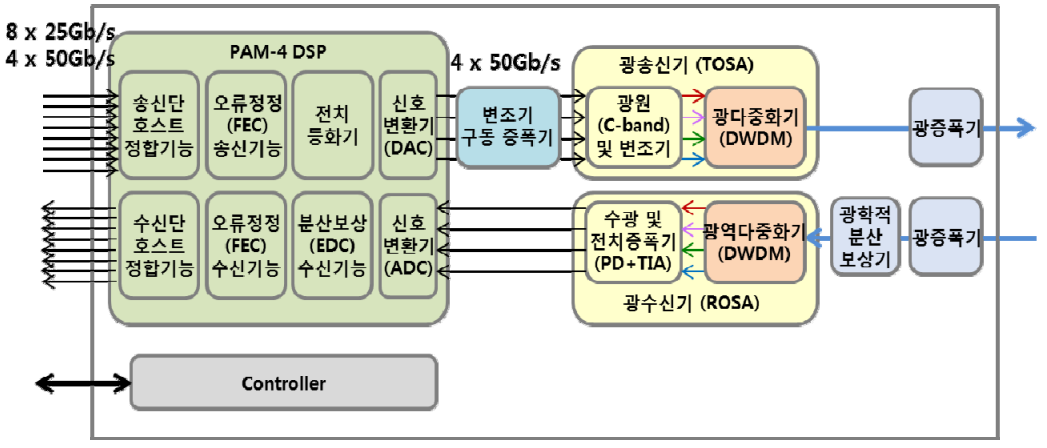
* 본 내용은 이준기 책임연구원(☎ 042-860-1659)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.
***정보통신기획평가원은 현재 개발 진행 및 완료 예정인 ICT R&D 성과 결과물을 과제 종료 이전에 공개하는 "ICT R&D 사업화를 위한 기술예고"를 2014년부터 실시하고 있는 바, 본 칼럼에서는 이를 통해 공개한 결과물의 기술이전, 사업화 등 기술 활용도 제고를 위해 매주 1~2건의 관련 기술을 소개함

OPEN 출처표시 상업용금지 공공누리 공공저작물 자유이용허락



[그림 1] 기술개념도

- 메트로 액세스 네트워크 광전송 시장은 향후 5년간 빠르게 성장할 신성장 분야로 80km 이하 전송구간의 대용량, 고효율, 저가 솔루션 개발이 필요함
- 광트랜시버는 전기신호를 광신호로 변환하여 전송하는 광송신 기능과 전송된 광신호를 전기신호로 변환하는 광수신 기능을 수행하는 광전송 시스템의 핵심 제품임
- 기존 80km 이하 전송 구간의 메트로 액세스 네트워크의 경우에는 파장당 10Gb/s



[그림 2] 200Gb/s 광트랜시버 블록도

속도의 NRZ-OOK(Non-Return to Zero On-Off-Keying) 방식의 광트랜시버나 고가의 코히어런트 방식의 광트랜시버 솔루션만 존재했으나, 파장당 속도 및 전송 효율을 10Gb/s에서 50Gb/s로 5배 증가하고, 광트랜시버당 전송용량을 100Gb/s급에서 200Gb/s급으로 2배 증가시킨 광트랜시버 기술을 제안

➢ 200Gb/s 광트랜시버 구성의 핵심 광모듈로, 메트로 액세스 네트워크용 광송신기(TOSA) 및 광수신기(ROSA) 모듈 기술을 포함

2. 기술의 상세내용 및 사업화 제약사항

➢ 기술의 상세내용

- 메트로 액세스 네트워크용 200Gb/s 광트랜시버 기술
  - ※ 직접수신 고차 변복조 신호 전송성능 최적화: 고차 변복조 신호의 80km 전송을 위한 광선로 손실 및 분산 보상, 신호대 잡음비 확보 기술, 송수신단 복잡도 증가에 따른 변복조부와 등화기, 오류정정을 이용한 전송 성능 최적화 기술
  - ※ 고속, 고밀도 신호 무결성(signal integrity) 설계 기술: 50Gb/s PAM-4 신호 경로에 대한 무결성 구조를 적용한 설계 기술
  - ※ 펌웨어 기반 관리 및 제어 기술: 산업체 표준에 따른 펌웨어 구현 및 광트랜시버 제어·관리 기술
- 메트로 액세스 네트워크용 200Gb/s 광송신기(TOSA) 및 광수신기(ROSA) 기술
  - ※ 고속 전기신호에 대한 선형성 보장 기술: 고속 전기신호 경로에 대한 특성 임피던스 정합, 임피던스 불연속 지점에 대한 보상을 통해 비선형 특성 발생 억제
  - ※ 다채널 광결합 및 광·전 집적화 기술: 광원과 광다중화기 및 PD와 광역다중화기 간 광결합 손실 최소화 및 큰 허용 정렬 오차 보장 구조 적용
  - ※ 광다중화기 및 역다중화기 기술: 삽입 손실 및 인접 채널 간 잡음 최소화 설계 및 제작, 광입출력 광결합 구조 설계
  - ※ 고(高) 방열 및 열적 분리 기술: 고집적화에 따른 효율적인 열 방출 구조 및 열적 분리 기술, 열 특성 안정화 및 열 잡음 억제를 통해 고(高) 품질의 신호 생성 및 수신 성능 보장

➢ 기술이전 범위

- 메트로 액세스 네트워크용 200Gb/s 광트랜시버(HW-Module)
  ※ 메트로 액세스 네트워크용 200Gb/s 광트랜시버 보드 설계도
  ※ 메트로 액세스 네트워크용 200Gb/s 광트랜시버 기구물 설계도
  ※ 메트로 액세스 네트워크용 200Gb/s 광트랜시버 운용 S/W
- 메트로 액세스 네트워크용 200Gb/s 광송수신기(HW-Module)
  ※ 메트로 액세스 네트워크용 200Gb/s 광송신기 및 광수신기 설계도
  ※ 메트로 액세스 네트워크용 200Gb/s 광송신기 및 광수신기 제작 기술

➢ 사업화 제약사항

- 없음

III. 국내외 기술 동향 및 경쟁력

1. 국내 기술 동향

➢ 국내 광트랜시버 업체에서는 주로 단거리 광트랜시버를 개발하여 판매하고 있으며, 하이엔드급의 중·장거리 광트랜시버 기술에 대한 투자 및 연구는 미미한 상황

➢ ETRI에서는 2004년 10G XFP(10G form-factor pluggable) 광트랜시버 개발을 시작으로, 40G CFP 광트랜시버, 100G CFP 광트랜시버(100GBASE-LR4), 100G CFP4 광트랜시버(100GBASE-LR4/ER4)에 이르기까지 다양한 광트랜시버를 개발하여 산업체에 기술이전하였음

➢ ETRI에서는 광트랜시버의 핵심 기능을 수행하는 광송신기 및 광수신기 모듈을 개발하여 10G TOSA, 4x25G ROSA 등의 OSA(Optical Sub-Assembly) 설계 및 제작 기술을 확보하였으며, 개발된 OSA 기술을 국내 광트랜시버 업체인 ㈜에이알텍, ㈜오이솔루션, ㈜빛과전자 등에 기술이전하여 상용화에 성공

➢ ㈜오이솔루션에서는 10G 관련 전제품 군에 대해 개발 완료 및 생산하고 있으며 40G QSFP+ SR4, LR4 개발을 완료하여 국내 삼성전자 등에 납품하고 있으며, 이외에도 무선 및 데이터센터에 적용 예정인 25G TOSA, ROSA 및 트랜시버 제품군을 개발하

여 샘플 제공 중에 있으며, 10km용 100G CFP4 광트랜시버 및 광수신기 기술을 ETRI로부터 기술전수 받아 상용화 개발 중임

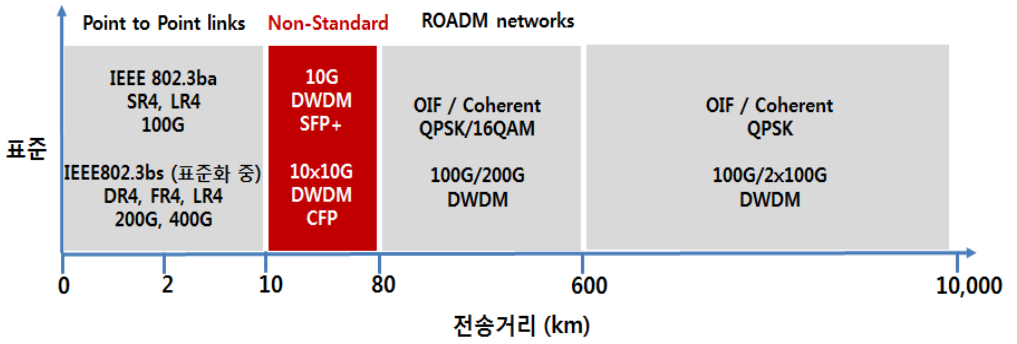
- ㈜에이알텍은 ETRI에서 기술을 이전받아 이동통신 중계국 간 연결을 위한 80km 전송용 100Gb/s(10λ×10Gb/s) CFP 광트랜시버를 개발하여 2014년부터 중국 ZTE에 납품 중임

2. 해외 기술 동향

- 전세계 데이터 트래픽이 급격히 증가함에 따라 100G, 200G, 400G 이더넷 등의 고속 데이터를 전송할 수 있는 광트랜시버 기술에 대한 요구가 증가하고 있으며, 이와 함께 클라우드 및 통신 사업자의 상면적, 소모전력, 투자 비용 등의 문제를 해결하기 위해 광트랜시버 및 관련 부품의 소형화, 집적화, 저전력화에 대한 필요성이 높아지고 있음
- 100G 이더넷용 광트랜시버로 CFP, CFP2 form-factor의 광트랜시버가 대량 생산되고 있으며, CFP4, QSFP28 form-factor로 소형화, 저전력화되고 있음
- 400G 이더넷 표준이 2017년 12월 승인되었으며, 이는 PAM-4 변조방식을 기본으로 하고 있으며, 이에 따라 글로벌 칩/모듈 선도업체에서는 최대 10km 전송이 가능한 데이터센터 내부용 100G/200G/400G급 PHY IC를 공개하고 있음
- Acacia, Oclaro에서는 대형 메트로 및 백본 네트워크에서 사용되는 DP-QPSK 또는 DP-16QAM 기반의 코히어런트 광트랜시버 기술을 메트로 액세스 네트워크용으로 이용하려는 연구를 지속하고 있음.
- InPhi에서 2×56Gb/s로 100Gb/s 80km PAM4 광트랜시버를 개발하여 Microsoft 데이터센터 네트워크에 적용

3. 표준화 동향

- 본 기술/제품과 직접적으로 관련 있는 표준은 현재 존재하지 않음
- [그림 3]과 같이 10km 이내의 전송 거리에서는 IEEE 802.3의 이더넷 표준화 그룹에서, 수백 km 이상의 전송 거리에서는 OIF(Optical Internetworking Forum)에서 표준화를 진행하고 있음



[그림 3] 전송거리별 광전송 표준

➢ IEEE 802.3ba에서는 100G 이더넷 표준을 2010년 6월에 승인하였으며, 광송수신 관련 표준은 [표 1]과 같음

[표 1] IEEE 802.3ba 표준

전송 거리	Physical Medium	100G 이더넷	광 인터페이스	변조 방식
100m OM3 125m OM4	MMF	100GBase-SR10	10fiber×10G	OOK
		100GBase-SR4	4fiber×25G	OOK
10km	SMF	100GBase-LR4	4λ×25G(LAN-WDM)	OOK
40km	SMF	100GBase-ER4	4λ×25G(LAN-WDM)	OOK

➢ IEEE 802.3bs에서는 400G 이더넷 표준화를 위하여 2014년 3월 Task Force가 생성되어 2017년 12월 표준이 승인되었으며, 광송수신 관련 표준은 [표 2]와 같음

[표 2] IEEE 802.3bs 표준

전송 거리	Physical Medium	400G 이더넷	광 인터페이스	변조 방식
100m	MMF	400GBase-SR16	16fiber×25G	OOK
500m	SMF	400GBase-DR4	4fiber×100G	PAM-4
2km	SMF	400GBase-FR8	8λ×50G	PAM-4
10km	SMF	400GBase-LR8	8λ×50G	PAM-4

4. 보유특허

No.	국가	출원번호(출원일)	상태	명칭
1	미국	16/023187(2018.06.29.)	출원 완료	Optical signal transmission apparatus for generating multi-level optical signal and method performed by the same
2	미국	16/010745(2018.06.18.)	출원 완료	Optical transmission method and apparatus
3	미국	16/033330(2018.07.12.)	출원 완료	Multi-channel optical transmitting module
4	미국	16/124766(2018.09.07.)	출원 완료	Optical multiplexing method
5	미국	16/194618(2018.11.19.)	출원 완료	Optical de-multiplexing method
6	미국	16/207557(2018.12.03.)	출원 완료	Optical transmitting module

5. 기술의 경쟁력

경쟁기술	본 기술의 우수성 및 차별성
10λ×10Gb/s 광트랜시버	경쟁 기술은 파장 당 10Gb/s, 전송 용량 100Gb/s이지만, 본 기술은 파장 당 50Gb/s, 전송 용량 200Gb/s로 4개의 파장 채널을 이용하여 2배의 전송 용량 제공
100GBASE-LR4/ER4 표준 광트랜시버	100GBASE-LR4/ER4 표준은 파장 당 25Gb/s, 전송 용량 100Gb/s로 최대 전송 거리가 각각 10km, 40km에 제한되나, 본 기술에서는 파장 당 50Gb/s, 전송 용량 200Gb/s로 최대 전송 거리 80km를 제공
100Gb/s 80km PAM-4 광트랜시버	경쟁 기술은 파장 당 50Gb/s, 전송 용량 100Gb/s의 광트랜시버이며, 본 기술은 전송 용량 200Gb/s로 2배의 전송 용량을 제공하고, 세계 최고 수준의 광 수신기의 수신 감도를 달성

IV. 국내외 시장 동향 및 전망

1. 국내외 시장 동향 및 전망

➢ (현황 및 단기전망) 세계 광트랜시버 시장규모는 2013년 19.4억 달러(약 2조 2,500억 원) 규모에서 2019년 31억 달러(약 3조 6,000억 원) 규모로 연평균(CAGR) 8.1% 성장

- 국내 시장은 동기간 동안 428억 원에서 683억 원으로 성장할 전망
- 국외 시장은 동기간 동안 19억 달러(약 2조 2,000억 원)에서 30.4억 달러(약 3조 5,500억 원)로 성장할 전망

[표 3] 제품시장 현황 및 단기 전망(2013~2019년)

구분		2013년	2014년	2015년	2016년	2017년	2018년	2019년	CAGR
텔레콤 광트랜시버	국내(억 원)	180	169	142	153	179	192	202	1.9%
	국외(백만 달러)	803	752	634	680	797	857	902	
	세계(백만 달러)	820	767	647	694	814	875	920	
데이터센터 광트랜시버	국내(억 원)	248	300	361	350	383	428	481	11.7%
	국외(백만 달러)	1,104	1,335	1,609	1,561	1,704	1,907	2,141	
	세계(백만 달러)	1,126	1,362	1,642	1,593	1,739	1,946	2,184	
합계	국내(억 원)	428	469	504	503	562	621	683	8.1%
	국외(백만 달러)	1,907	2,087	2,243	2,241	2,502	2,764	3,042	
	세계(백만 달러)	1,946	2,130	2,289	2,287	2,553	2,821	3,105	

* 국내 시장은 세계 시장의 2%로 가정하고, 1달러=1,100원 적용

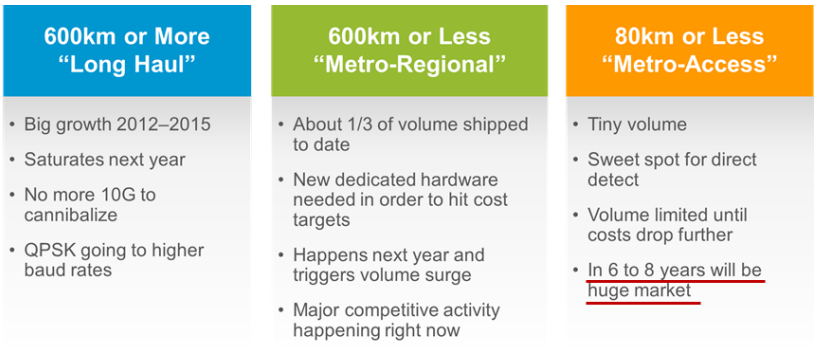
➢ (장기 전망) 세계 광트랜시버 시장규모는 2023년 41.2억 달러(약 4조 8,000억 원) 규모에서 2029년 47.3억 달러(약 5조 5,000억 원) 규모로 연평균(CAGR) 2.3% 성장

- 국내 시장은 동기간 동안 907억 원에서 1,042억 원으로 성장할 전망
- 국외 시장은 동기간 동안 40.4억 달러(약 4조 7,000억 원)에서 46.4억 달러(약 5조 4,000억 원)로 성장할 전망

[표 4] 제품시장 장기 전망(2023~2029년)

구분		2023년	2024년	2025년	2026년	2027년	2028년	2029년	CAGR
텔레콤 광트랜시버	국내(억 원)	219	223	227	232	236	241	246	1.9%
	국외(백만 달러)	974	993	1,013	1,032	1,053	1,073	1,094	
	세계(백만 달러)	994	1,014	1,033	1,054	1,074	1,095	1,116	
데이터센터 광트랜시버	국내(억 원)	689	712	733	752	769	783	796	2.5%
	국외(백만 달러)	3,068	3,170	3,264	3,348	3,424	3,490	3,547	
	세계(백만 달러)	3,130	3,235	3,330	3,417	3,493	3,561	3,620	
합계	국내(억 원)	907	935	960	983	1,005	1,024	1,042	2.3%
	국외(백만 달러)	4,042	4,164	4,276	4,381	4,476	4,563	4,641	
	세계(백만 달러)	4,124	4,249	4,364	4,470	4,568	4,656	4,736	

* 세계 시장은 제품의 특성을 고려하여 CAGR 및 추세 함수를 이용하여 전망하고, 국내 시장은 세계 시장의 2%로 가정



〈자료〉 Infonetics 2015. 10.

[그림 4] 광전송 시장별 전망

➢ 광전송 시장별 전망 자료에 의하면, 600km 이상 장거리용 광트랜시버 시장의 경우 성장이 정체되고, 600km 이하 메트로용 시장의 경우 현재 1/3 비율에서 완만하게 성장할 것이며, 80km 이하 메트로 액세스용 시장의 경우 현재 시장규모가 작지만 6~8년 후에 큰 시장으로 성장할 것으로 전망

2. 제품화 및 활용 가능 분야

활용 분야(제품/서비스)	제품 및 활용 분야 세부내용
5G 이동통신 백홀(back-haul) 장비	메트로 액세스 네트워크용 광트랜시버
대형 데이터센터 패킷-광 통합(PTN/POTN) 장비 및 코어 라우터 장비	메트로 액세스 네트워크용 광트랜시버
소형 메트로 망용 패킷-광 통합(PTN/POTN) 장비 및 DWDM/ROADM 장비	메트로 액세스 네트워크용 광트랜시버

V. 기대효과

1. 기술도입으로 인한 경제적 효과

➢ 국내 기업의 신규 시장 진출 및 글로벌 사업화

- 네트워크 발전에 따라 출현하는 신규 시장에 특화된 맞춤형 신기술로서, 국내 기업의 기술 수준을 높이고 가격 경쟁 위주 저가 광트랜시버 시장을 탈피하여 새로 형성되

는 고가의 중거리 광트랜시버 시장 선도 진출

➢ 국내 중소기업의 기술 경쟁력 확보 및 핵심 역량 강화

- 저가 전략을 기반으로 한 중국 업체의 추격에 대비하고, 글로벌 선진 업체의 수직 계열화로 인해 심화되고 있는 기술 격차를 줄여 광모듈/부품 산업의 기술 경쟁력 확보
- 핵심 부품에 대한 해외 수입 의존도 탈피 및 국가 공공 인프라 기술 자립화 실현

2. 기술사업화로 인한 파급효과

➢ 공공 측면

- 대용량 고효율 저가의 메트로 액세스 네트워크 구축으로 서비스 비용 감소와 데이터 처리 속도 향상을 통해 산업, 안전, 경제 전반의 활성화에 기여
- 유무선 융합이 가능한 메트로 액세스 네트워크 인프라 구축을 위한 핵심 기술 확보를 통해 세계 최고 수준의 인프라 구축 기술 및 운용 노하우를 습득하여 네트워크 서비스의 수준 제고에 기여

➢ 사회적 측면

- 서비스 공급자, 통신 사업자들이 추진 예정인 5G, IoT, 빅데이터 등 대용량 데이터 전달 기반의 네트워크 융합 환경 구축에 기여하여 새로운 통신 서비스를 제공할 수 있는 기반 구축
- 초고속 대용량 광트랜시버는 네트워크 인프라의 새로운 트렌드를 견인하여 과학, 산업 및 사회·문화·생활 전반의 디지털 정보화 시대 구현에 기여

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 1918호(2019-40)

발 행 년 월 일 : 2019년 10월 16일
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