Chapter 01

5G 네트워크에서의 의도 기반 네트워킹 기술 동향

정재훈_성균관대학교 교수

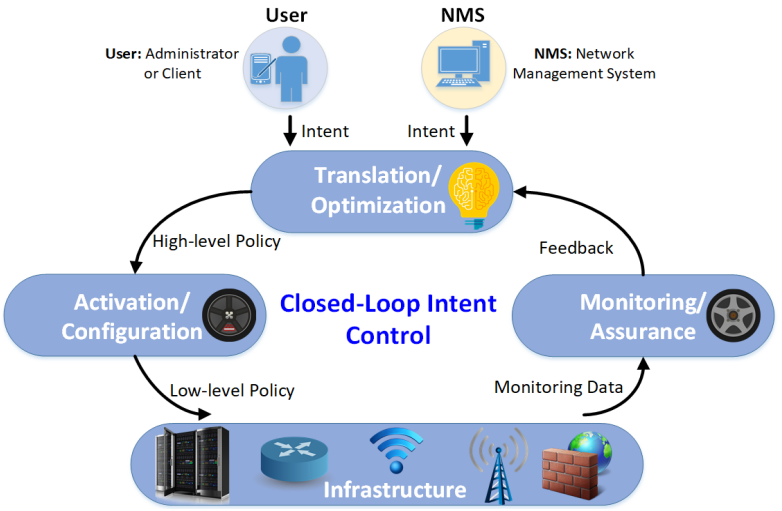
본 고는 5G 네트워크에서의 의도 기반 네트워킹(Intent-Based Networking: IBN)의 기술 개발 및 표준화 동향을 소개한다. IBN 기술은 네트워크 사용자 또는 관리자가 원하는 서비스를 표현한 의도(intent)를 네트워크 오퍼레이터(5G 네트워크 사업자)에게 전달하면 원하는 네트워크 및 응용 서비스를 제공하는 기술이다. 최근에 급속도로 발전한 인공지능, 기계학습 및 딥러닝 기술의 발전과 특히 자연어처리(Natural Language Processing: NLP)의 정수인 거대 언어 모델(Large Language Model: LLM) 발전으로 이러한 IBN 기술 개발 및 서비스가 가능하다. 본 고에서는 IBN 기술의 개발 및 표준화 동향과 본 고의 저자가 참여하는 IBN 관련 기술 개발 및 국제 표준화 활동을 소개한다.

I. 의도 기반 네트워킹 기술

의도 기반 네트워킹은 네트워크 관리자의 의도(intent; 선언적인 명령)를 인공지능 기술로 파악하여 인터넷을 구성하는 유선망과 무선망 설정을 자동으로 수행하는 기술이다. 의도는 순차적인 명령(imperative command)이라기보다는 원하는 서비스의 목적을 나타나는 선언적인 명령(declarative command)이다[1]. [그림 1]은 글로벌 네트워크 벤더인 시스코(Cisco)가 제안한 의도 기반 네트워킹을 보여준다[2]. [그림 1]과 같이 네트워크 관리자 또는 고객인 사용자(user) 또는 네트워크 관리 시스템(Network Management System: NMS)은 음성이나 텍스트 형태의 의도를 번역(translation) 및

* 본 내용은 정재훈 교수(☎ 031-299-4957, pauljeong@skku.edu)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.
***본 고는 2024년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No. RS-2024-00398199, No. RS-2022-II221199).

OPEN 출처표시 상업용금지 공공누리 공공저작물 자유이용허락



〈자료〉 Cisco, "Why Your Campus Network Needs Intent", https://blogs.cisco.com/networking/why-your-campus-network-needs-intent

[그림 1] 의도 기반 네트워킹(Intent-Based Networking) 개념도

최적화(optimization) 모듈에게 송부한다. 번역 및 최적화 모듈은 의도를 컴퓨터가 이해할 수 있는 상위 레벨 정책(high-level policy: 순차적인 명령)으로 번역한다. 이러한 의도를 나타내는 자연어(natural language) 정책을 나타내는 컴퓨터 스크립트(computer scripture)로 자동 번역하기 위해 거대 언어 모델(Large Language Model: LLM)[3][4]이 이용된다.

번역된 상위 레벨 정책은 설치(activation) 및 설정(configuration) 모듈에서 전달된다. 이 모듈은 인프라(infrastructure)에서 요청된 네트워크 서비스를 수행할 네트워크 시스템 또는 가상화 시스템(가상 머신, 컨테이너)을 활성화하고, 이 활성화된 시스템에게 해당 테스크(task)를 지시하기 위해 수신된 상위 레벨 정책(high-level policy)을 하위 레벨 정책(low-level policy)으로 번역한다. 하위 레벨 정책은 해당 네트워크 시스템 또는 가상화 시스템에게 전달되어 해당 네트워크 서비스를 수행한다.

[그림 1]과 같이 모니터링(monitoring) 및 보증(assurance) 모듈은 인프라에 있는 네트워크 시스템 또는 가상화 시스템으로부터 모니터링 데이터를 수집해서 분석하여 본 네트워크 서비스가 의도대로 잘 동작하고 있는지 검정(validation)을 하고, 의도에

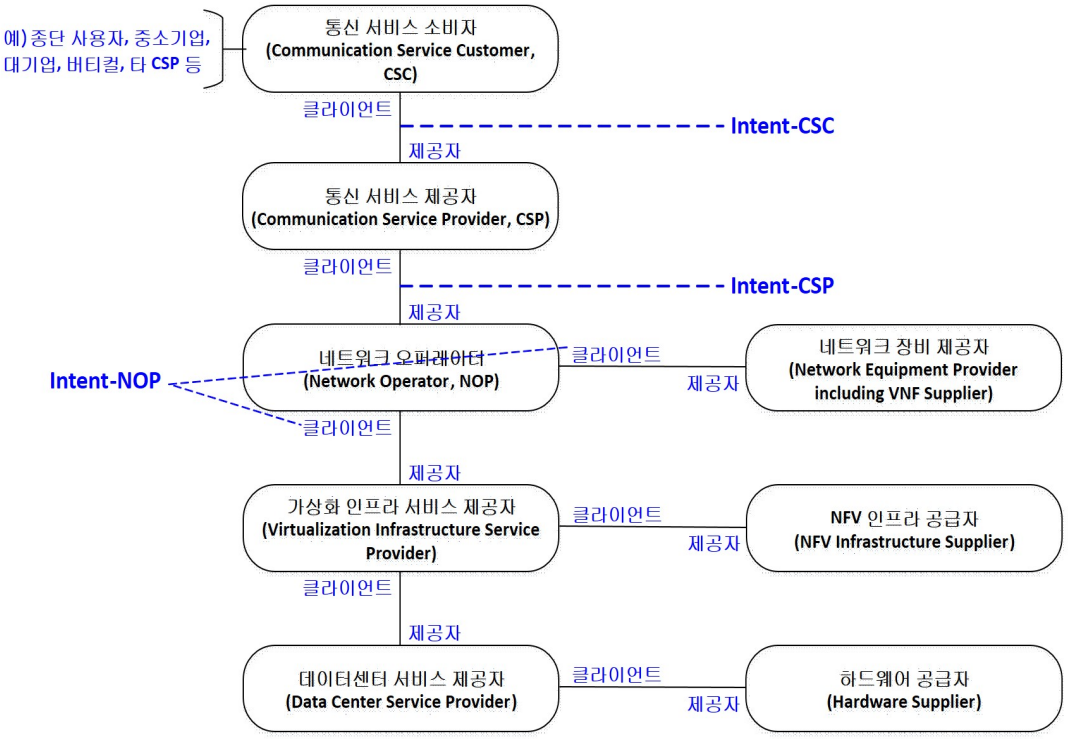
부합되지 않거나 요청된 성능이 제대로 제공되지 않으면 정책을 보완하거나 새로운 정책을 생성하여 피드백(feedback) 메시지를 번역 및 최적화 모듈에게 송부하여 네트워크 재설정을 수행하게 한다. 이처럼 모니터링과 피드백 기반의 재설정 과정을 폐쇄 루프 의도 제어(closed-loop intent control)라고 한다. 이와 같이 IBN 기술은 의도 번역(intent translation), 의도 적용(intent deployment), 의도 모니터링(intent monitoring), 의도 검정(intent validation) 및 의도 재설정(intent reconfiguration)에 일련의 의도 라이프 사이클(intent life cycle)로 네트워크에 적용 및 운용되는 자동화 기술이다.

5G 이동통신망은 코어 네트워크(core network)와 무선 액세스 네트워크(Radio Access Network: RAN)로 구성된다[5]. 코어 네트워크와 무선 액세스 네트워크는 네트워크 함수 가상화(Network Functions Virtualization: NFV)[6][7]와 소프트웨어 정의 네트워크(Software-Defined Networking: SDN)[8]로 구성된다. 즉, 코어 네트워크와 RAN의 네트워크 함수(Network Function: NF)가 NFV의 가상 네트워크 함수(Virtual Network Function: VNF) 또는 클라우드 네이티브 함수(Cloud-Native Network Function: CNF)로 구현된다.

3GPP는 코어 네트워크와 RAN에 대해 의도 기반 네트워킹(IBN)으로 표준화하고 있다[9]. 의도는 특정한 서비스 또는 네트워크 워크플로우에 대한 요구사항, 목표 및 제약사항을 포함한다. 의도는 특정한 목표와 관련 세부사항에 대한 정보를 제공할 수 있다. 다음은 의도의 일반적인 개념을 설명한다.

- 개념 1: 의도는 사람에 의해 이해되고, 모호성 없이 기계에 의해 해석되어야 한다.
- 개념 2: 의도는 무엇(즉, 목표 및 요구사항)이 성취되어야 함에 더 많이 집중되어 있고, 그것을 어떻게 성취해야 하는 것에는 상대적으로 더 적게 집중되어 있다.
- 개념 3: 의도는 기대사항을 성취하기 위한 하부 시스템 구현, 관련 기술 및 인프라와는 무관하다.
- 개념 4: 의도는 성취도 측정/평가를 위해 네트워크 데이터 기반 정량화가 필요하다.

[그림 2]는 다른 역할에 의해 표현되는 다른 종류의 의도 상위 레벨 모델로, 소비자와 제공자(공급자) 간의 의도 송신/수신 관계를 보여주고 있다. 예를 들면, 통신 서비스

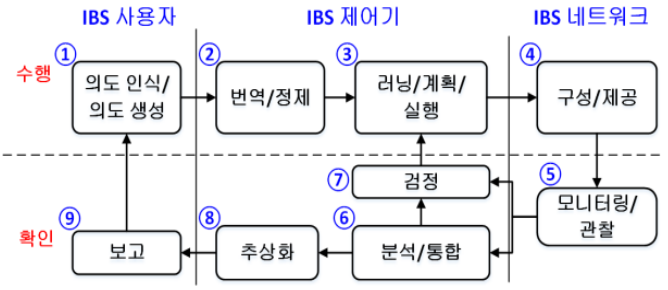


〈자료〉 3GPP, "Intent Driven Management Services for Mobile Networks", 3GPP TS 28.312 V18.1.1, Sep. 2023.

[그림 2] 다른 역할에 의해 표현되는 다른 종류 의도의 상위 레벨 모델

소비자(Communication Service Customer: CSC)는 원하는 서비스를 표현하는 CSC의 의도(Intent-CSC)를 통신 서비스 제공자(Communication Service Provider: CSP)에게 전달한다. 통신 서비스 제공자는 수신한 CSC-의도를 처리하기 위해 네트워크 오퍼레이터(Network Operator: NOP)에게 자신의 CSP-의도(Intent-CSP)를 송신한다. 이와 같이 소비자는 자신과 바로 연관된 제공자(또는 공급자)에게 해당 의도를 생성 및 송신함으로써 원하는 서비스를 제공받을 수 있다.

IBN은 IETF NMRG(Network Management Research Group)[10]에서 IBN의 정의와 개념을 정립한 표준문서인 RFC 9315[1]에 잘 기술되어 있다. 이 표준문서는 IBN을 통해 동작하는 의도 기반 시스템(Intent-Based System: IBS)을 정의한다. IBS는 먼저 관리자가 네트워크 의도를 정의하게 하고, 의도를 IBS 제어기에게 전달해서 구체적인



〈자료〉 A. Clemm, L. Ciavaglia, L. Granville, and J. Tantsura, “Intent-Based Networking - Concepts and Definitions”, RFC 9315, Oct. 2022.

[그림 3] 의도 전주기(Intent Life Cycle) 다이어그램

구성(configuration) 파일로 번역하고, 구성 파일이 해당 서비스 함수(Service Function: SF)에 전달되어 원하는 서비스를 수행하게 하고, 서비스를 모니터링하여 수정 사항이 있으면 수정하게 한다.

[그림 3]은 IBS를 위해 RFC 9315에 정의된 의도 라이프 싸이클, 즉 의도 전주기에 대한 다이어그램이다. 의도 전주기는 의도 이행(intent fulfillment)과 의도 보증(intent assurance) 구간으로 구성된다. 의도 이행은 관리자의 의도대로 네트워크를 설정하고 운용하는 것이다. 의도 보증은 의도대로 네트워크가 운용되고 있는지를 검정하고, 설정 및 운영의 최적화를 수행하며, 검정 결과를 관리자에게 보고하는 것이다. 이와 같이 IBS는 의도 전주기 다이어그램에 따라 동작한다. [표 1]은 [그림 3]의 IBS의 의도 전주기에 대한 단계별 오퍼레이션을 나타낸다. 이와 같이 의도 전주기는 의도가 서비스 함수(SF)에 설정되어 서비스를 수행하고, SF의 동작 결과를 분석 및 검정하여 개선된 정책 생성 및 최적화를 수행하는 폐쇄 루프 제어 시스템(closed-loop control system)을 지원한다.

IETF NMRG는 인공지능 기반 네트워크 관리를 위한 IBN을 본격적으로 표준화하고 있다[1][10]. NMRG는 의도 기반 네트워킹에 대한 개념과 정의에 대한 문서[1]와 의도 자동 분류에 대한 문서[11]를 표준으로 제정했다. NMRG는 현재 의도 기반 네트워킹에 대한 다양한 유스케이스를 다루는 문서[12]와 AI 서비스를 효율적으로 지원하기 위한 네트워크와 시스템 고려사항 문서를 개발하고 있다[13].

[표 1] 의도 전주기의 단계별 수행 내용

단계	수행 내용
1	의도 인식/의도 생성(Intent Recognition/Intent Generation)
	IBS 사용자는 네트워크, 보안 및 응용 서비스에 대한 요청인 텍스트/음성을 인식하여 의도를 생성한다. IBS 사용자는 의도를 IBS 제어기에서 송신한다.
2	번역/정제(Translation/Refinement)
	IBS 제어기는 수신한 의도를 번역하여 네트워크, 보안 및 응용 서비스를 수행할 서비스 함수(Service Function: SF)가 이해할 수 있는 정책(policy)으로 번역(translation)한다.
3	러닝/계획/실행(Learning/Plan/Deployment)
	IBS 제어기는 번역된 정책을 실행할 네트워크, 보안 및 응용 서비스를 수행할 SF를 선택하여 정책을 송부한다.
4	구성/제공(Configuration/Provisioning)
	IBS 네트워크의 SF는 정책을 전달받으면 정책에 따른 서비스를 수행할 구성을 수행하고, 요청된 서비스를 실행한다.
5	모니터링/관찰(Monitoring/Observation)
	IBS 네트워크의 서비스 함수들은 자신의 동작이 모니터링되고 분석되기 위해 모니터링 데이터를 생성하여 분석기(analyzer)에게 송신한다.
6	분석/통합(Analysis/Aggregation)
	IBS 네트워크의 분석기는 SF들로부터 모니터링 데이터를 수신하면 인공지능(Artificial Intelligence: AI) 또는 기계학습(Machine Learning: ML) 알고리즘으로 분석하여 서비스 함수들의 관찰 내용을 통합한다.
7	검정(Validation)
	검정기(validator)는 분석 내용을 통해 SF들이 의도된 서비스를 제대로 수행하고 있는지 확인한다. SF의 기능 및 성능이 불충분하거나 최적화(optimization)할 사항이 있으면 정책 재구성(policy reconfiguration) 또는 피드백 정보(feedback information)를 IBS 제어기에게 송부한다.
8	추상화(Abstraction)
	추상화기(abstractor)는 보완할 정책 또는 피드백 정보를 관리자가 쉽게 이해할 수 있게 추상화 작업을 수행하여 추상화 정보를 IBS 사용자의 보고기(reporter)에게 송부한다.
9	보고(Reporting)
	보고기(reporter)는 추상화 정보를 수신하면 IBS 사용자에게 전달할 보고서를 생성하여 IBS 사용자에게 전달한다. IBS 사용자는 수신한 보고서를 다시 의도 인식 및 의도 생성 모듈에게 전달하여 보고서를 가지고 기존의 의도를 보완해서 1번부터 8번까지의 단계를 반복 수행한다.

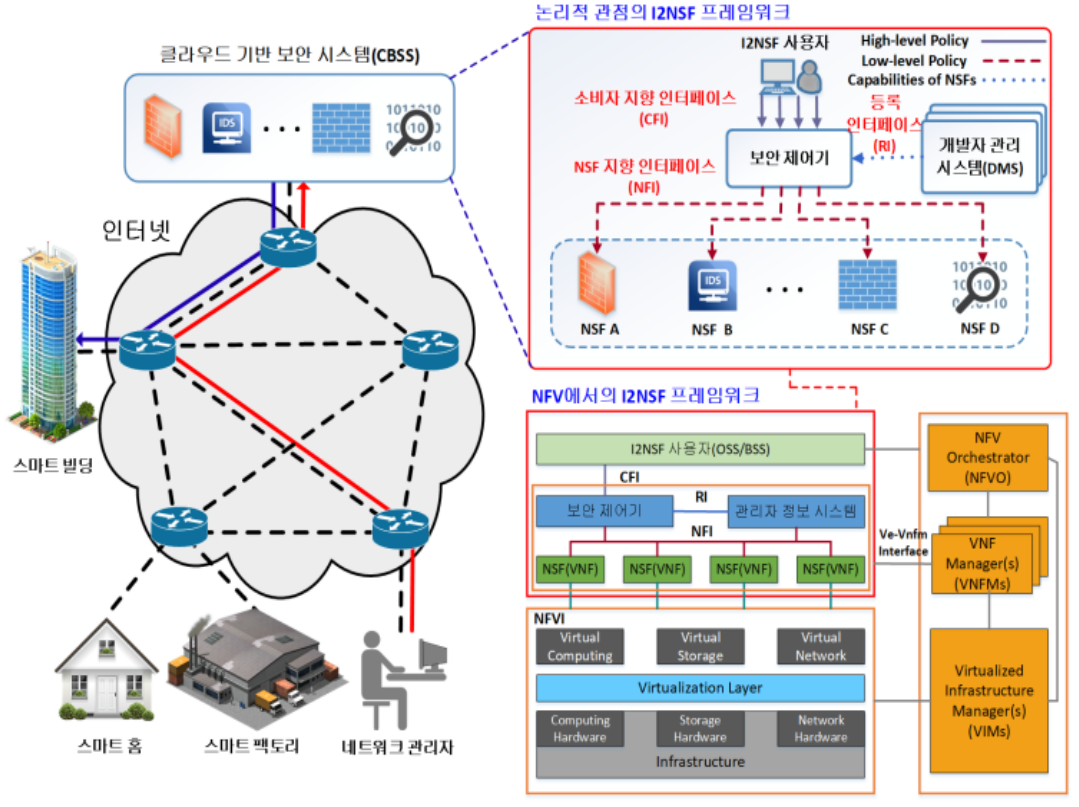
〈자료〉 성균관대학교 자체 작성

II. 의도 기반 보안 서비스 관리 기술

의도 기반 네트워킹 기술의 대표적인 예로서 의도 기반 보안 서비스 관리 기술을 소개한다. 5G 네트워크에 연결되는 스마트폰, 전기차, 자율주행차 등의 다양한 단말에 대한

의도 기반 클라우드 및 엣지 보안 서비스를 위해 IETF I2NSF(Interface to Network Security Functions) 워킹그룹(Working Group: WG)[14]은 I2NSF 프레임워크 및 인터페이스의 표준화를 수행했다[15]. I2NSF WG는 클라우드 기반 보안 서비스를 제공하는 프레임워크의 인터페이스를 정의하기 위해 모델링 언어인 YANG 기반으로 5개의 I2NSF 데이터 모델을 표준화하였다[15].

[그림 4]는 I2NSF를 이용한 클라우드 기반 보안 서비스 시스템을 보여주고 있다. 그림의 오른쪽 상단은 논리적 관점의 I2NSF 프레임워크[16]-[18]를 나타낸다. 네트워크 관리자가 I2NSF 사용자클라이언트를 이용하여 타깃 도메인(스마트빌딩, 스마트홈, 스마트

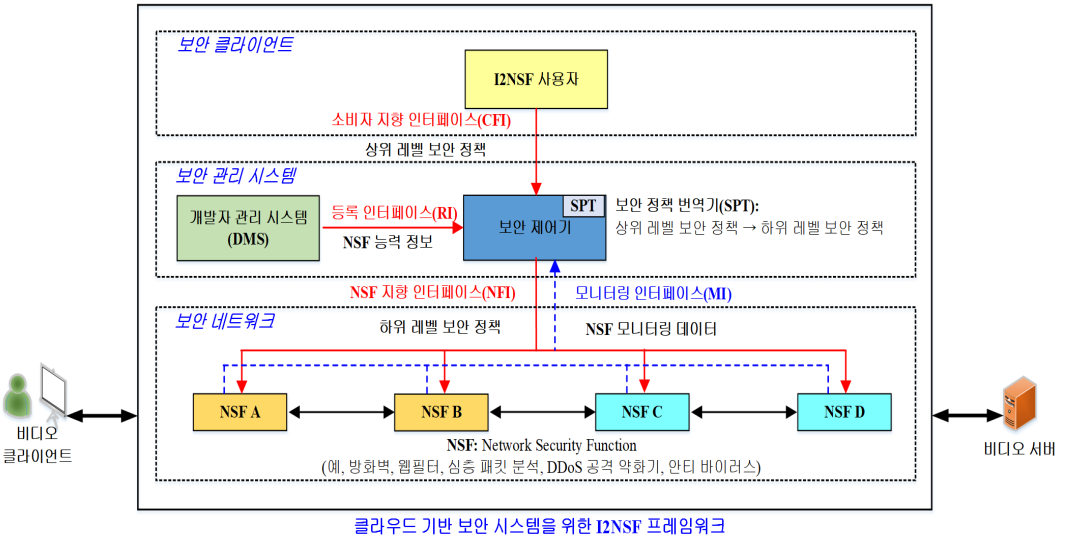


〈자료〉 J. Kim, E. Kim, J. Yang, J. Jeong, H. Kim, S. Hyun, H. Yang, J. Oh, Y. Kim, S. Hares and L. Dunbar, "IBCS: Intent-Based Cloud Services for Security Applications", IEEE Communications Magazine, Vol.58, No.4, Apr. 2020, pp.45-51.

[그림 4] 클라우드 기반 보안 서비스 시스템

팩토리)에 의도에 해당하는 상위 레벨 보안 정책(high-level security policy)을 소비자 지향 인터페이스(Consumer-Facing Interface: CFI)를 통해 I2NSF 프레임워크의 보안 제어기(security controller)에게 전달한다. 보안 제어기는 보안 정책 번역기(Security Policy Translator: SPT)를 통해 수신한 상위 레벨 보안 정책을 네트워크 보안 함수(Network Security Function: NSF)가 이해할 수 있는 하위 레벨 보안 정책(low-level security policy)으로 번역한다[19]. 보안 제어기는 번역된 하위 레벨 보안 정책을 NSF 지향 인터페이스(NSF-Facing Interface: NFI)를 통해 적합한 NSF에게 전달하여 요청된 보안 서비스를 수행하게 한다. 이러한 I2NSF 프레임워크는 그림의 오른쪽 하단처럼 NFV 플랫폼(오픈스택[20]) 상에서 물리적으로 구현될 수 있다.

[그림 5]는 네트워크 보안 함수 인터페이스인 I2NSF 프레임워크[16][18]의 좀 더 자세한 구조를 보여주고 있다. 개발자 관리 시스템(Developer's Management System: DMS)은 네트워크 보안 함수인 NSF를 생성하고 관리하는 I2NSF 프레임워크의 구성요소이다. DMS는 등록 인터페이스(registration interface)를 통해 NSF의 능력(capability)과



클라우드 기반 보안 시스템을 위한 I2NSF 프레임워크

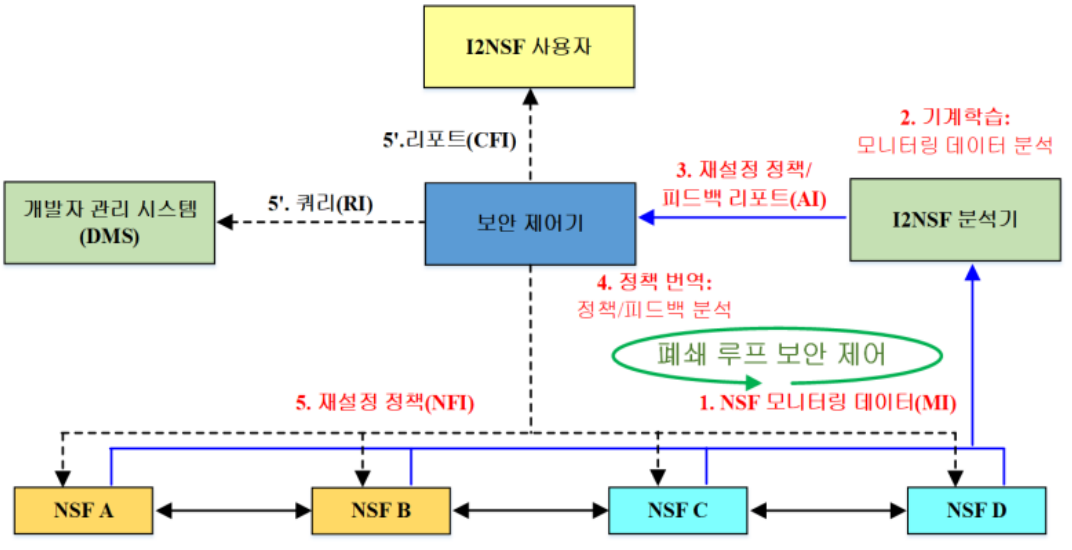
〈자료〉 D. Lopez, E. Lopez, L. Dunbar, J. Strassner and R. Kumar, "Framework for Interface to Network Security Functions", RFC 8329, Feb. 2018.

[그림 5] 네트워크 보안 함수 인터페이스(I2NSF)를 위한 프레임워크

NSF의 접근 정보(access information)인 IP 주소와 포트 번호를 보안 제어기에 등록한다. 이 그림에서 I2NSF 사용자는 비디오 클라이언트와 비디오 서버 사이 네트워크에게 보안 서비스로써 '방화벽', '웹필터', 'DDoS(Distributed Denial-of-Service) 공격 약화기' 서비스를 요청하는 의도를 생성하여 보안 제어기에게 송부한다. 이러한 의도(즉, 상위 레벨 보안 정책)를 수신한 보안 제어기는 보안 정책 번역기(SPT)를 통해 하위 레벨 보안 정책으로 번역하고, 관련 NSF들을 선택하여 하위 레벨 보안 정책을 송부하여 원하는 보안 서비스를 제공하게 한다[19].

[그림 6]은 I2NSF 프레임워크에서의 폐쇄 루프 보안 제어(closed-loop security control)를 보여주고 있다[18]. 요청된 의도의 보안 서비스가 제대로 잘 제공되고 있는지를 확인하는 과정이 필요하다. [표 2]는 I2NSF 폐쇄 루프 보안 제어의 단계별 오퍼레이션 보여주는데, 보안 서비스 적용 확인 과정은 5단계로 수행된다.

보안 제어기는 NSF에 대한 피드백(CPU, 메모리 또는 하드디스크 용량 증설)에 대한 쿼리(Query)를 생성하여 등록 인터페이스(Registration Interface: RI)를 통해 개발자



〈자료〉 J. Jeong and P. Lingga, "CBSS: Cloud-Based Security System with Interface to Network Security Functions", ICMU 2023, Nov. 29, 2023.

[그림 6] I2NSF 프레임워크에서의 폐쇄 루프 보안 제어

[표 2] I2NSF 폐쇄 루프 보안 제어의 단계별 수행 내용

단계	수행 내용
1	NSF 모니터링 데이터 수집
	NSF는 자신의 NSF 모니터링 데이터를 모니터링 인터페이스(Monitoring Interface: MI)를 통해 I2NSF 분석기에게 전달한다.
2	기계학습 기반 모니터링 데이터 분석
	I2NSF 분석기는 수집한 NSF 모니터링 데이터를 기계학습으로 분석하여 보안 공격 또는 NSF에 대한 문제점(과부하, 리소스 부족, 고장)을 탐색한다.
3	재설정 정책 및 피드백 리포트 전달
	I2NSF 분석기가 NSF 모니터링 데이터로부터 새로운 보안 공격을 발견하면 이를 방어할 상위 레벨 보안 정책을 재설정 정책(reconfiguration policy)으로 생성한다. 만약에 수신한 모니터링 데이터가 NSF에 대한 시스템 알람 또는 이벤트일 때, 이를 해결할 수 있는 피드백 리포트를 생성한다. I2NSF 분석기는 생성한 재설정 정책 또는 피드백 리포트 메시지를 분석 인터페이스(Analytics Interface: AI)를 통해 보안 제어기에게 송부한다.
4	정책 번역을 통한 정책 및 피드백 분석
	보안 제어기는 수신한 재설정 정책 또는 피드백 리포트를 수신하여 분석 및 번역을 수행한다.
5	재설정 정책 및 피드백 수행
	보안 제어기가 수신한 메시지가 재설정 정책이면 스텝 5.1을 수행한다. 보안 제어기가 수신한 메시지가 피드백 리포트이면 스텝 5.2를 수행한다.
5.1	재설정 정책 수행
	보안 제어기는 재설정 정책을 하위 레벨 보안 정책으로 번역하여 해당 NSF들에게 그 보안 정책을 송부하여 요청되는 보안 서비스를 수행하게 한다.
5.2	피드백에 대한 쿼리 및 리포트 전달
	보안 제어기는 NSF에 대한 피드백(CPU, 메모리 또는 하드디스크 용량 증설)에 대한 쿼리(Query)를 생성하여 등록 인터페이스(Registration Interface: RI)를 통해 개발자 관리 시스템(DMS)에게 쿼리를 송부하여 피드백에 해당되는 서비스를 요청한다. 이러한 피드백 정보를 담은 레포트를 소비지 지향 인터페이스(Consumer-Facing Interface: CFI)를 통해 I2NSF 사용자에게 전달하여 I2NSF 시스템에서의 현황을 파악하게 한다.

〈자료〉 성균관대학교 자체 작성

관리 시스템(DMS)에게 송부하여 피드백에 해당되는 서비스를 요청한다. 이러한 피드백 정보를 담은 레포트를 소비자 지향 인터페이스(Consumer-Facing Interface: CFI)를 통해 I2NSF 사용자에게 전달하여 I2NSF 시스템에서의 현황을 파악하게 한다.

III. 의도 기반 네트워킹 기술 개발 동향

IBN 기술 연구 개발은 전세계 학계, 네트워크 벤더, 네트워크 오퍼레이터에 의해 활발히

진행되고 있다[21]. IBN 시장에서는 점점 더 많은 요구사항과 제품이 개발되고 있다. 이에 따라 의도 기반 네트워킹 시장은 많은 부가가치를 창출할 전망이므로 네트워크 벤더와 네트워크 오퍼레이터가 IBN 제품 및 서비스 개발 및 적용에 적극적으로 참여하고 있다. IBN 시장에서 네트워크 벤더, 즉 네트워크 장비 제조사(시스코(Cisco), 화웨이(Huawei), 노키아(Nokia) 등)와 네트워크 오퍼레이터, 즉 텔레콤 회사들(차이나 모바일(China Mobile), 텔레포니카(Telefonica) 등)은 IBN 기술 개발 및 IETF 표준화에 적극 참여하고 있다.

특히, 시스코는 의도 기반 네트워킹(IBN) 기술 개발을 선도하고 있다[1][22][23]. [그림 1]과 같이 사용자 또는 NMS의 의도를 입력받아서 실행 가능한 정책으로 번역하여 해당 네트워크 장비에 그 정책을 적용하는 IBN 솔루션을 제공하고 있다[1][22]. 이러한 IBN 솔루션은 의도 번역뿐만 아니라 번역된 정책이 물리적 네트워크 인프라 또는 가상 네트워크 인프라에 설정되게 하는 네트워크 자동화를 지원한다. 또한, 네트워크를 지속적으로 모니터링하고 모니터링 데이터를 기계학습으로 분석하여 원하는 의도가 잘 적용되고 있는지를 검사한다. 시스코는 적용한 고화질 화상회의를 위한 단말들의 종단간 서비스 품질을 보장하는 네트워크 대역 및 지연시간 설정을 위한 5G 네트워크 슬라이싱 기술을 개발하고 있다[23].

화웨이는 NFV와 SDN 기술 개발 및 표준화를 선도하고 있다. 이를 기반으로 5G/6G를 위해 인공지능(AI) 모델 기반의 IBN 기술 개발 및 표준화에 많은 투자를 하고 있다[24]. 화웨이는 캠퍼스 네트워크에서의 네트워크 인터페이스 설정, 무선 서비스 설정, 가상랜(Virtual LAN: VLAN) 생성 등을 자동화 하는데 IBN 기술을 활용한다. 또한, 화웨이는 차이나 모바일과 함께 오픈 소스 기반의 네트워크 자동화 플랫폼인 ONAP(Open Network Automation Platform)[25]에서 IBN 기반 네트워크 슬라이싱 기술을 개발하여 소개하였다[26].

GMI(Global Market Insights)에 따르면 의도 기반 네트워킹 시장 규모는 2022년에 USD 1.5 billion(약 2조 원)을 넘었고, 2023년부터 2032년까지 연평균 25% 성장(Compound Annual Growth Rate: CAGR)할 것으로 예측된다[그림 7][27].

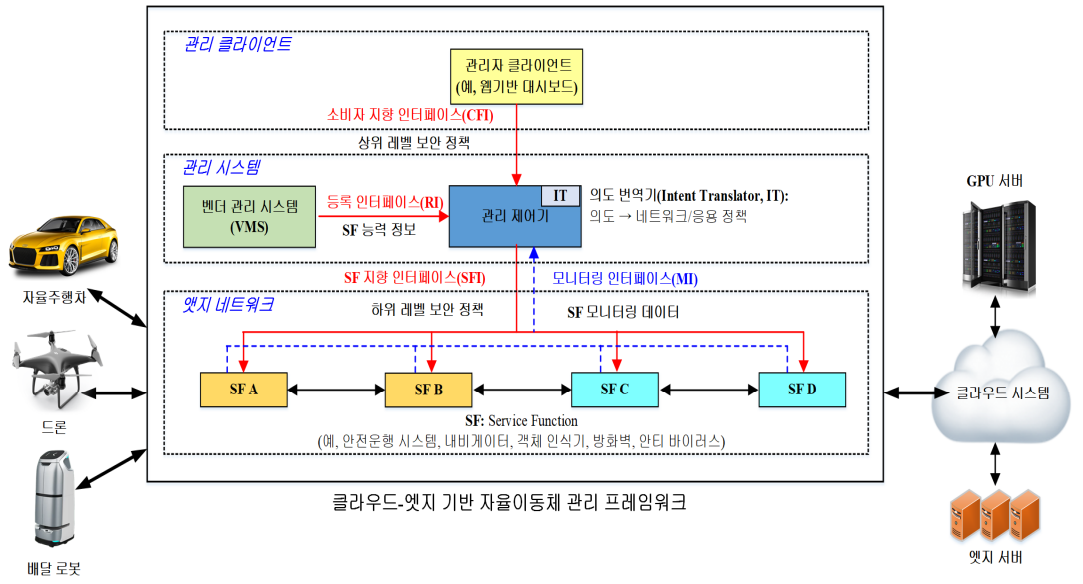
〈자료〉 Global Market Insights, "Intent-Based Networking(IBN) Market", https://www.gminsights.com/industry-analysis/intent-based-networking-ibn-market

[그림 7] 의도 기반 네트워킹 시장 규모

IV. 의도 기반 인-네트워크 함수 관리 기술

본 고의 저자인 성균관대 연구팀은 IBN 기술 개발 및 표준화에 활발히 참여하고 있다. 특히, IETF에서 IBN 기술 표준화에 적극 참여하고 있다[12][28][29]. 성균관대 연구팀은 "클라우드-엣지 시스템 기반 자율이동체(자율주행차, 드론, 로봇) 안전주행 지원 네트워크, 보안, 응용 서비스 관리 프레임워크 표준개발"을 목표로 한다[28][29]. [그림 8]은 클라우드-엣지 기반 자율이동체 관리 프레임워크를 보여주고 있다[29].

지금이 IBN 기반의 클라우드-엣지 기반 자율이동체 관리를 위한 프레임워크 기술 개발 및 표준화의 적기로 사료된다. 현재까지 IETF에서 IBN 관련 표준화된 기술은 사용자 단말기(데스크탑 컴퓨터, 노트북, 스마트폰)에 특화된 클라우드 보안 서비스가 주류를 이루고 있다. 향후 5년 이내에 보편화될 자율이동체(자율주행차, 드론, 배달 로봇)를 위한 네트워크, 보안 및 응용 설정 및 관리를 위한 표준화된 프레임워크와 인터페이스의 부재로 다양한 기업들의 제품과 네트워크 사업자들의 네트워크 서비스 연동에 어려움이 예상된다. 따라서 IBN 기반 자율이동체에 다양한 서비스를 지원할 클라우드-엣지 간의 연동 서비스의 기술 개발 및 표준화가 필요한 상황이다. 이러한 클라우드-엣지 시스템 기반 자율이동체의 관리를 위한 표준 프레임워크를 통해 안전주행과 효율적 내비게이션 지원을 위한 네트



〈자료〉 J. Jeong, Y. Shen, Y. Ahn, Y. Kim and E. Duarte Jr. and K. Yao, “A Framework for Interface to In-Network Functions(I2INF)”, draft-jeong-opsawg-i2inf-framework-01, Oct. 2024.

[그림 8] IBN 기반 클라우드-엣지 기반 자율이동체 관리 프레임워크

워크, 보안, 응용 서비스를 효과적으로 제공할 수 있을 것으로 전망된다.

[그림 8]의 IBN 기반 클라우드-엣지 기반 자율이동체 관리 프레임워크 개발 및 표준화 사항은 다음과 같다.

- 클라우드-엣지 시스템 기반 자율이동체 관리 프레임워크 표준개발
- 자율이동체 관리 프레임워크 주요 컴포넌트 간의 인터페이스의 데이터 모델 표준개발 ([그림 8]에서 인터페이스들에 대한 YANG 데이터 모델)
- 자율이동체 관리 프레임워크 기반 유스케이스 표준개발

위의 세 가지 표준 개발을 위해 성균관대 연구팀은 현재 IETF OPSAWG(Operations and Management Area WG)[30]에서 인-네트워크 함수 인터페이스(I2INF)에 대한 문제 정의 문서[28]와 I2INF 프레임워크 문서[29]의 표준화를 시작하였다.

자율이동체가 실생활에 도입된 상황에서 IBN 기반 자율이동체 관리 표준 프레임워크 기술은 국내외 자율이동체 시장을 주도할 수 있는 핵심 기술이다. 또한 관련 기술의 지적

재산권(Intellectual Property Right: IPR)을 확보하여 국제적 기술 우위를 선점하여 기술 개발 및 표준화를 선도할 수 있을 것이다. 성균관대는 협력 기관으로 스페인의 텔레포니카, 중국의 차이나 모바일 및 화웨이와 긴밀히 협력하여 본 IBN 기술 개발과 IETF 표준화를 수행할 예정이다.

V. 결론

본 고는 최근 세계적으로 큰 이슈가 되고 있는 거대 언어 모델(LLM) 중심의 인공지능 기술이 네트워크와 보안 서비스 관리를 자동화 할 수 있는 의도 기반 네트워킹(IBN)의 기술 개발 및 표준화 동향을 소개하였다. 이러한 IBN 기술은 5G 네트워크에서의 네트워크 및 보안 서비스를 위해 활발히 개발 및 표준화되고 있다. IBN 기술은 크게 의도 번역(intent translation), 의도 적용(intent deployment), 의도 모니터링(intent monitoring), 의도 검정(intent validation) 및 의도 재설정(intent reconfiguration)의 다섯 단계로 구성되며 각각의 단계에서 LLM, 기계학습, 딥러닝 및 최적화 기술이 적용된다. IBN 기술은 5G 코어 네트워크와 무선 액세스 네트워크(RAN) 뿐만 아니라 5G 네트워크에 접속하여 서비스를 받는 다양한 단말인 소프트웨어 정의 차량(Software-Defined Vehicle: SDV), 드론 같은 무인항공기(Unmanned Aerial Vehicle: UAV), 도심 항공 이동 차량(Urban Air Mobility: UAM)에게 네트워크, 보안 및 응용 서비스를 효과적으로 제공할 수 있다. 이러한 IBN 기술은 Beyond 5G와 6G 네트워크에서도 계속 발전되어 사용될 것으로 예측되므로 국내 산 · 학 · 연은 IBN 기술 개발 및 표준화에 많은 관심과 투자를 하여 미래의 IBN 기술 선두주자에 합류하기를 권고한다.

참고문헌

[1] A. Clemm, L. Ciavaglia, L. Granville and J. Tantsura, “Intent-Based Networking - Concepts and Definitions”, RFC 9315, Oct. 2022.

[2] Cisco, “Why Your Campus Network Needs,

Intent".https://blogs.cisco.com/networking/why-your-campus-network-needs-intent
[3] J. Devlin, M. Chang, K. Lee and K. Toutanova, "BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding", Proceedings of Conference of the North American Chapter of the Association of Computational Linguistics - Human Language Technology (NAACL-HLT), June 2019.
[4] M. Romero-Sandoval, S. Calderon-Ramirez and M. Solis, "Using GPT-3 as a Text Data Augmentator for a Complex Text Detector," 2023 IEEE 5th International Conference on BioInspired Processing(BIP), Nov. 2023.
[5] 3GPP, "System Architecture for the 5G System(5GS); Stage 2", TS 23.501 V19.0.0, June 2024.
[6] ETSI, "Network Functions Virtualisation(NFV); Architectural Framework", ETSI GS NFV 002 V1.2.1, Dec. 2014.
[7] ETSI, "Network Functions Virtualisation(NFV) Release 2; Management and Orchestration; Architectural Framework Specification", ETSI GS NFV 006 V2.1.1, Jan. 2021.
[8] M. Boucadair and C. Jacquenet, "Software-Defined Networking: A Perspective from within a Service Provider Environment", RFC 7149, Mar. 2014.
[9] 3GPP, "Intent Driven Management Services for Mobile Networks", 3GPP TS 28.312 V18.1.1, Sep. 2023.
[10] NMRG, https://datatracker.ietf.org/group/nmrg/about/
[11] C. Li, O. Havel, A. Olariu, P. Martinez-Julia, J. Nobre and D. Lopez, "Intent Classification", RFC 9316, Oct. 2022.
[12] K. Yao, D. Chen, J. Jeong, Q. Wu, C. Yang, L. Contreras and G. Fioccola, "Use Cases and Practices for Intent-Based Networking", Oct.2024.
[13] NMRG Documents, https://datatracker.ietf.org/group/nmrg/documents/
[14] I2NSF Working Group, https://datatracker.ietf.org/wg/i2nsf/about/
[15] I2NSF Working Group Documents, https://datatracker.ietf.org/group/i2nsf/documents/
[16] D. Lopez, E. Lopez, L. Dunbar, J. Strassner and R. Kumar, "Framework for Interface to Network Security Functions", RFC 8329, Feb. 2018.
[17] J. Kim, E. Kim, J. Yang, J. Jeong, H. Kim, S. Hyun, H. Yang, J. Oh, Y. Kim, S. Hares and L. Dunbar, "IBCS: Intent-Based Cloud Services for Security Applications", IEEE Communications Magazine, Vol.58, No.4, Apr. 2020, pp.45-51.
[18] J. Jeong and P. Lingga, "CBSS: Cloud-Based Security System with Interface to Network Security Functions", ICMU 2023, Nov. 29, 2023.
[19] P. Lingga, J. Jeong, J. Yang and J. Kim, "SPT: Security Policy Translator for Network Security Functions in Cloud-Based Security Services", IEEE Transactions on Dependable and Secure Computing, Feb. 2024.

[20] OpenStack Website, https://www.openstack.org/
[21] A. Leivadeas and M. Falkner, “A Survey on Intent-Based Networking”, IEEE Communications Surveys & Tutorials, Vol.25, No.1, Fir. 2023, pp.625-655.
[22] Cisco, “What is intent-based networking(IBN)?”, https://www.cisco.com/c/en/us/solutions/intent-based-networking.html
[23] P. Kelly, “Intent-Based Networking: Automated Assurance’s Critical Success Factor”, Whitepaper, Appledore Reseach and Cisco, Mar. 2023.
[24] Huawei, “What Is Intent-driven Deployment?”, https://info.support.huawei.com/info-finder/encyclopedia/en/Intent-driven+Deployment.html
[25] Open Network Automation Platform(ONAP) Website, https://www.onap.org/
[26] L. Deng and C. Chen, “A General Implementation with Intent-Based Network in ONAP”, https://youtu.be/l5g066xiXmk?si=9HbhexTcoN48X9e9
[27] Global Market Insights, “Intent-Based Networking(IBN) Market”, https://www.gminsights.com/industry-analysis/intent-based-networking-ibn-market
[28] J. Jeong, Y. Shen, Y. Ahn, Y. Kim, E. Duarte Jr. and K. Yao, “Interface to In-Network Functions(I2INF): Problem Statement”, Oct. 2024.
[29] J. Jeong, Y. Shen, Y. Ahn, Y. Kim, and E. Duarte Jr. and K. Yao, “A Framework for Interface to In-Network Functions(I2INF)”, Oct. 2024.
[30] OPSAWG, https://datatracker.ietf.org/group/opsawg/about/