IETF NMRG 의도 기반 네트워킹 표준화 동향

정재훈
성균관대학교

요 약

본 고에서는 국제 표준화 기구 IETF(Internet Engineering Task Force)의 의도 기반 네트워킹(Intent-Based Networking: IBN) 표준화 동향을 소개한다. IBN 기술은 네트워크 관리자의 의도에 따라 해당 네트워크 서비스를 위한 구성 및 명령이 타겟 네트워크에 설정되고, 의도에 부합하는 성능을 제공하는지 검증하여 네트워크 구성을 자율적으로 보완한다. 본 고는 또한 IBN 유스케이스 문서 및 IBN 표준화 현황을 소개한다.

Ⅰ. 서 론

우리는 인공지능(Artificial Intelligence: AI) 기술의 발달로 인해 자연어(Natural Language)의 텍스트 인식 및 자동번역, 이미지(Image) 인식 및 생성이 보편화된 시대에 살고 있다. 이러한 AI 기술은 인터넷을 운영하는데 필요한 네트워크 관리(Network Management: NM) 분야에 적용되기 시작하였다. 국제인터넷 표준화기구인 Internet Engineering Task Force(IETF)[1]는 이러한 AI의 인터넷 적용을 위한 노력을 기하고 있다. IETF의 동료 리서치 기구인 Internet Research Task Force(IRTF)[2]는 네트워크 관리 리서치 그룹(Network Management Research Group: NMRG)[3]를 통해 AI의 기술을 네트워크 관리 도메인 적용하기 위한 연구를 활발히 하고 있다.

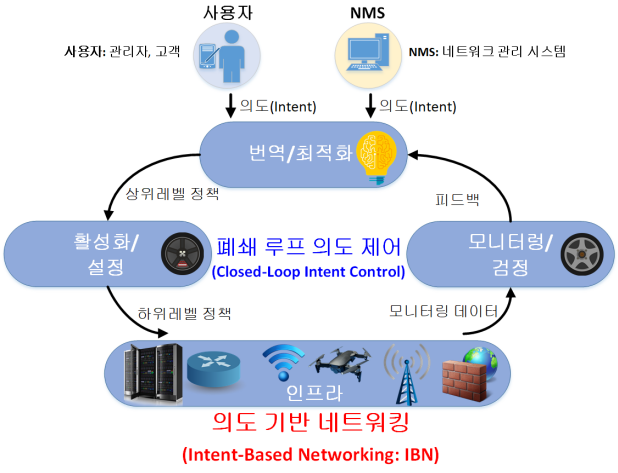

그림 1. 의도 기반 네트워킹 구조도[4][5]

네트워크 관리 자동화를 위해 최근에 의도 기반 네트워킹(Intent-Based Networking: IBN)이 네트워크 벤더, 오퍼레이터, IETF 및 학계에서 활발히 연구되고 있다. 글로벌 네트워크 벤더인 시스코는 의도 기반 네트워킹 개념 정립 및 상용화를 주도하고 있다. 〈그림 1〉은 의도 기반 네트워킹 구조도를 보여주고 있다[4][5]. 그림과 같이 사용자 또는 네트워크 관리 시스템(Network Management System: NMS)은 네트워크 관리 의도를 번역 및 최적화 모듈에게 전달한다. 번역 및 최적화 모듈은 의도를 네트워크 시스템이 이해할 수 있는 상위레벨 정책(High-level Policy)으로 번역한다. 이러한 의도를 상위레벨 정책으로 번역하기 위해 거대 언어 모델(Large Language Model: LLM)[6][7]이 이용될 수 있다. 번역된 상위레벨 정책은 설치 및 설정 모듈에서 전달되어 네트워크 인프라 시스템이 이해할 수 있는 하위레벨 정책(Low-level Policy)으로 번역된다. 이 하위레벨 정책은 인프라에 있는 해당 서비스를 수행할 네트워크 인프라 엔터티(Network Infrastructure Entity)인 라우터, 기지국, 이동기지국, 서버로 전달되어 설정한다. 또한 〈그림 1〉에서 각 엔터티가 잘 동작하는지 검사하기 위해 각 엔터티는 자신의 모니터링 데이터를 모니터링 및 보증 모듈에게 송부한다. 이 모듈은 모니터링 데이터를 분석하여 본 엔터티가 설정된 의도대로 잘 동작하고 있는지 검정한다. 만약 의도에 잘 부합되지 않으면 번역된 정책을 보완하거나 새로운 정책을 생성하여 문제 및 해결방안을 알리는 피드백 메시지를 번역 및 최적화 모듈에게 전달한다. 이 모듈은 이러한 피드백을 수집하여 의도대로 인프라 엔터티가 잘 동작하도록 네트워크 재설정을 수행한다. 이와 같이 모니터링과 피드백 기반의 재설정 과정을 폐쇄 루프 의도 제어(Closed-Loop Intent Control)라고 명명한다. 이와 같이 의도 기반 네트워킹 기술인 의도 번역, 의도 적용, 의도 모니터링, 의도 검정 및 의도 재설정의 과정을 폐쇄 루프로 사이클을 형성한

다. 이러한 사이클을 의도 라이프 사이클(Intent Life Cycle)이라고 명명하고 네트워크 관리 자동화의 핵심 절차로 사용된다.

본 고에서는 이러한 의도 기반 네트워킹인 IBN 기술을 IETF NMRG에서의 표준화를 중심으로 소개하고자 한다.

Ⅱ. NMRG 의도 기반 네트워킹 표준화

NMRG는 의도 기반 네트워킹(IBN)의 개념 정립 및 시스템 정의[8] 그리고 의도 분류 구조화[9]를 표준화했다.

1. 의도 기반 네트워킹 개념 및 정의

RFC9315는 의도 기반 네트워킹의 개념 및 정의를 기술하고 있다[8]. 의도(Intent)는 네트워크 엔터티 설정 또는 서비스 구성을 요청을 하는 개념적인 목표를 나타내는 선언적인 명령(Declarative Command)으로 정의된다[4][8]. 이러한 의도는 의도 번역기를 통해 설정 및 작업의 순서를 명시적으로 나타내는 순차적인 명령(Imperative Command)으로 번역된다.

〈그림 2〉는 인공지능 기술을 통한 네트워크 관리 자동화를 위한 의도 기반 시스템(Intent-Based System: IBS)의 설정 및 운영을 위한 라이프 사이클을 보여준다[5][8]. 이러한 의도 라이프 사이클은 의도 이행(Intent Fulfillment)과 의도 보증(Intent Assurance)의 두 단계로 구성된다. 의도 이행은 관리자의 의도에 해당하는 네트워크 서비스를 설정 및 운용하는 단계이다. 의도 보증은 의도대로 네트워크 서비스가 잘 운용되고 있는지를 검정하고 부족한 기능 보완 및 성능 향상을 위해 최적화 과정을 거쳐서 의도 이행을 보완한다. 이러한 운영 상황을 보고서(Report)로 작성하여 사용자에게 보고한다. 이와 같이 IBS는 의도 라이프 사이클에 따라 예측하기 어려운 네트워크 상황을 고려하여 요청된 서비스를 최상의 품질로 제공하고자 한다. 〈표 1〉은 〈그림 2〉의 IBS의 의도 라이프 사이클의 과정을 스텝별로 기술한다[5][8]. 이 의도 라이프 사이클은 모두 9스텝으로 구성되어 있고, 의도 대로 네트워크 서비스가 잘 수행될 수 있게 폐쇄 루프 의도 제어에 의해 수행된다. 이러한 의도 라이프 사이클은 의도 기반 네트워킹의 초석으로 활용되어 IBN 시스템 프레임워크 설계 및 유스케이스 작성에 활용된다.

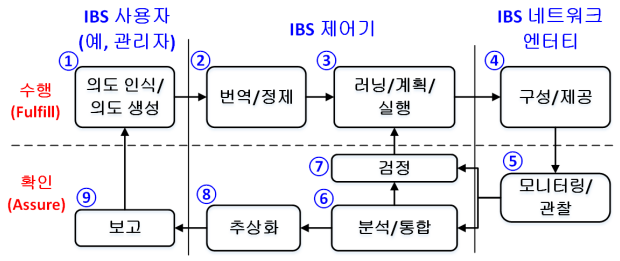

그림 2. 의도 기반 시스템의 라이프 사이클[5][8]

표 1. 의도 전주기의 단계별 오퍼레이션[5][8]

단계	오퍼레이션
1 (의도 인식/ 의도 생성)	IBS 사용자(user)는 네트워크 서비스에 대한 요청인 텍스트/음성을 인식하여 의도를 생성한다. IBS 사용자는 의도를 IBS 제어기에서 송신한다.
2 (번역/정제)	IBS 제어기(controller)는 수신한 의도를 번역하여 네트워크 서비스를 수행할 서비스 함수(Service Function: SF)가 이해할 수 있는 정책으로 번역한다.
3 (러닝/계획/실행)	IBS 제어기(controller)는 번역된 정책을 실행할 네트워크 서비스를 수행할 서비스 함수를 선택하여 정책을 송부한다.
4 (구성/제공)	IBS 네트워크의 서비스 함수는 정책을 전달받으면 정책에 따른 서비스를 수행할 구성을 수행하고, 요청된 서비스를 실행한다.
5 (모니터링/관찰)	IBS 네트워크의 서비스 함수들은 자신의 동작이 모니터링되고 분석되기 위해 모니터링 데이터를 생성하여 분석기(analyzer)에게 송신한다.
6 (분석/통합)	IBS 네트워크의 분석기(analyzer)는 서비스 함수들로부터 모니터링 데이터를 수신하면 인공지능 또는 기계학습 알고리즘으로 분석하여 서비스 함수들의 관찰 내용을 통합한다.
7 (검정)	검정기(validator)는 분석 내용을 통해 서비스 함수들이 의도된 서비스를 제대로 수행하고 있는지 확인한다. 서비스 함수의 기능 및 성능이 불충분하거나 최적화할 사항이 있으면 정책 재구성 또는 피드백 정보를 IBS 제어기에게 송부한다.
8 (추상화)	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)	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. 즉 폐쇄 루프 의도 사이클을 수행한다.

2. 의도 분류

RFC9316은 의도 기반 네트워킹에서의 의도 분류를 기술하고 있다[9]. 의도는 네트워크를 위해 운영하기 위해 사용되는 추상적 상위레벨 정책을 의미한다. 의도 기반 시스템(IBS)은 사용자가 요청 사항을 입력하기 위한 인터페이스를 포함한다. 아울러 IBS는 의도 라이프 사이클 상에서 의도를 네트워크 구성(Network Configuration)으로 번역하기 위한 엔진(즉 의도 번역기)를 제공해야 한다. RFC9316은 네트워크 의도의 개념을 논

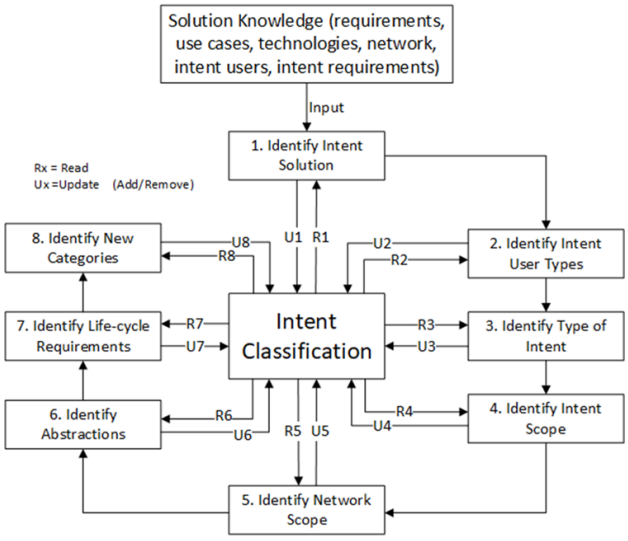

그림 3. 의도 분류 방법론[9]

의하고, 아울러 다른 타입의 의도를 기술하고 있다. 본 문서는 의도의 스테이크홀더(Stakeholder) 관점을 조명하고, 의도를 분류하고 인코딩하는 방법을 기술한다.

〈그림 3〉은 의도 분류 방법론을 보여주고 있다[9]. 이 방법론은 처음부터 솔루션 지식(Solution Knowledge)을 분석함으로써 새로운 의도 분류를 생성하기 위해 사용될 수 있다. 또한 이 방법론은 미래의 시나리오, 응용 및 도메인 지원하기 위해 다른 솔루션, 의도 사용자 또는 의도 타입을 추가하거나 제외함으로써 기존의 분류 테이블을 갱신할 수 있다. 이러한 의도 분류는 의도 번역기 개발의 초석이 된다.

Ⅲ. NMRG 의도 기반 네트워킹 유스케이스

NMRG는 IBN의 네트워크 및 보안 관리를 위해 IBN 유스케이스 표준화를 진행하고 있다[10].

1. IBN 시스템 구축 방법론

의도 기반 네트워킹(IBN) 시스템(즉, IBS)의 구축을 위해 RFC9315[8]의 의도 라이프 사이클을 참고할 수 있다. 이러한 IBN 시스템 구축 방법론은 (i) 시스템 인식과 데이터 수집 그리고 (ii) 통합 및 적용, 평가, 최적화, 의도와 정책의 재설정을 고려하는 IBN 시스템 구축으로 구성된다.

가. 시스템 인식 및 데이터 수집

시스템 인식은 네트워크 트래픽과 리소스와 같은 다양한 네트워크 상태 지표들의 수집을 필요로 한다. 의미있는 데이터셋을 수집하는 것이 IBN 시스템 구축에 아주 중요하다. 통찰력을 주는 데이터 수집은 적합한 방법 및 도구, 적합한 샘플링 메트릭(Metric) 및 데이터 수집을 위한 합리적인 데이터에 대한 정밀도(Granularity)에 의존한다.

(1) 방법 및 도구

데이터 수집 방법으로 능동적 측정(Active Measurement)와 수동적 측정(Passive Measurement)가 있다. In-band Network Telemetry(INT) 같은 능동적 측정은 온-패스 패킷(On-Path Packet)의 프로그래머블 필드(Programmable Field)에 타임스탬프를 삽입함으로써 네트워킹 정보를 추출할 수 있다.

수동적 측정은 종단점 서버(Endpoint Server)와 같은 특정 타겟에서 데이터를 수집하기 위해 Tcpdump와 Wireshark 같은 측정 툴을 사용한다. IBN 시스템은 그것이 적용되는 시나리오에 따라 데이터를 수집하는 방법을 사용한다.

(2) 메트릭

메트릭은 트랙픽 연관된 정보와 네트워크 연관된 정보를 포함한다. 트래픽 연관된 메트릭은 지연, 처리율 및 트래픽 체증 시그널 같은 성능 지표를 포함한다. 네트워크 연관된 메트릭은 포트 수와 상태와 네트워크 토폴로지 정보(예, 링크 연결성, 구조) 같은 네트워크 디바이스 정보를 포함한다.

전체 네트워크에서의 트래픽 로드 밸런스와 트래픽 체증 제거와 같은 특정 사용자 의도를 충족시키기 위해서는 IBN 시스템은 트래픽 및 디바이스 관련 정보를 수집 및 처리해야 한다.

(3) 정밀도

데이터에 대한 정밀도(Granularity)는 네트워크 트래픽, 시간 정밀도, 공간 정밀도를 고려한다. 네트워크 트래픽은 패킷 단위(Per-Packet)과 플로우 단위(Per-Flow)와 같이 다양한 타입으로 수집된다. 패킷 단위 트래킹(Tracking)은 각 패킷이 개별적으로 트래킹되게 해서 매우 정밀하게 패킷을 전달과정을 분석할 수 있으나 측정 및 관리 오버헤드가 크다. 본 방법을 대규모 네트워크에서 적용하기에는 확장성(Scalability) 측면에서는 좋지 않다. 반면에 플로우 단위 트래킹은 많은 상태를 유지할 필요가 없어서 확장성 측면에서 유리하다. 플로우는 다섯 튜플(즉, 송신자 IP 주소, 수신자 IP 주소, 송신자 포트 번호, 수신자 포트 번호, 프로토콜)로 구분된다.

시간 정밀도는 데이터 수집을 위해 데이터 샘플링을 위해 적합한 시간 간격을 채택함을 의미한다. 극단적인 경우로서 데이터가 인터럽션(Interruption)없이 수집될 수 있다. 이러한 수집은 너무 많은 중복된 정보를 수집하는 단점이 있다. 장점은 네트워크 시스템의 마이크로 버스트(Micro-Burst)를 잘 관찰하여 해당 네트워크 시스템을 정교하게 관리할 수 있다.

공간 정밀도는 데이터 수집의 적합한 물리적인 범위를 선택하는 것을 의미한다. 어떤 경우에는 전체 네트워크 또는 도메인 기반의 정보 수집이 모든 상황에 적합하지 않을 수도 있다. 대규모 네트워크에 대한 측정 정확도가 떨어질 수 있고, 측정을 위한 오버헤드가 크다. 따라서 사용자 의도에 대한 적합한 공간 정밀도를 선택하여 데이터 수집을 수행하는 것이 효과적이다.

나. IBN 시스템 구축

IBN 시스템 구축에서 의도 번역 모듈, 정책 생성 및 매핑 모듈 및 의도 검증 모듈이 중요한 역할을 수행한다. 〈표 2〉는 7단계로 구성된 IBN 시스템 구축 단계를 보여준다[10].

표 2. IBN 시스템 구축 단계[10]

단계	오퍼레이션
1 (의도 번역)	의도 번역 및 정제는 다른 서비스 의도의 시맨틱스(semantics) 관계를 탐색하는 시스템을 필요로 한다. 자연어로 표현된 의도를 LLM 기술로 정책으로 번역한다.
2 (정책 생성/매핑)	주어진 의도를 의도와 네트워크 상태를 모두 고려하여 수행될 수 있는 정책으로 번역한다. 본 정책을 수행할 네트워크 엔터티를 선정한다.
3 (의도 검증)	의도 검증은 번역된 정책이 기존의 다른 정책과 충돌하는지 검사하고, 특정 사용자의 요구사항을 만족시키는지를 확인하다. 정책이 충돌할 때는 정책 충돌 해소 기법을 통해 정책 충돌을 해결한다. 사용자의 요구사항 만족 확인을 위해 IBN 시스템은 사용자에게 피드백을 제공하고 사용자가 서비스 품질에 만족하는지 질의한다. 다른 방법으로 심층 강화 학습(deep reinforcement learning)을 통해 AI 에이전트를 통해 원하는 사용자 메트릭이 만족되는지 확인한다.
4 (의도 적용)	의도 적용은 번역된 정책을 타겟 네트워크에 적용하고 정책에 대한 구성 및 명령이 해당 네트워크에서 실행되게 한다.
5 (모니터링)	수집기(collector)는 네트워크 엔터티(예, 스위치, 라우터, 방화벽, 웹필터, DDoS 공격 약화기)로부터 모니터링 데이터를 수집한다.
6 (검정)	분석기(analyzer)는 데이터 수집기로부터 전달받은 모니터링 데이터를 기계학습을 통해 분석하여 의도에 대한 네트워크 서비스가 만족되는지 확인한다. 분석기는 분석 결과를 최적화기(optimizer)에게 전달한다.
7 (최적화)	최적화(optimizer)는 수신한 분석 결과를 기반으로 사용자의 의도를 만족시키기 위해 정책을 재설정하기나 신규 정책을 생성하여, 해당 네트워크 엔터티에게 전달한다.

2. IBN 유스케이스

IBN 유스케이스 문서는 IBN 기술을 네트워크, 보안 및 응용 서비스에 적용하는 다양한 유스케이스(즉 시나리오)를 기술하고 있다. 예를 들면, 클라우드 기반 보안 서비스 프레임워크[11]-[14]와 소프트웨어 정의 차량 프레임워크 관리 유스케이스[15][16][17]를 설명한다.

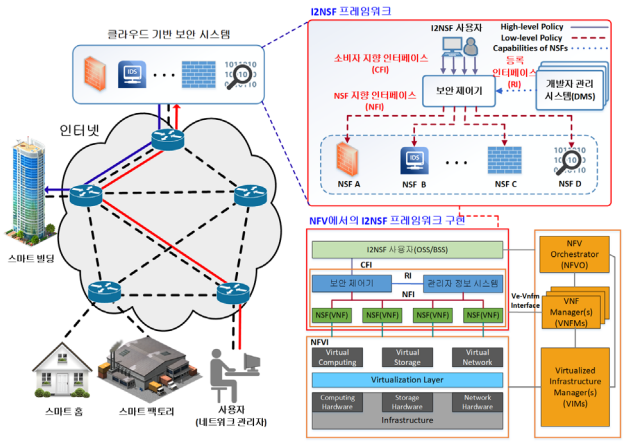

그림 4. 클라우드 기반 보안 서비스 시스템[12]

가. 클라우드 기반 보안 서비스 프레임워크

IBN 시스템의 대표적인 사례는 클라우드 기반 보안 서비스를 위한 프레임워크이다[11]-[14]. 본 프레임워크는 IETF에서 클라우드 기반 보안 서비스를 위한 I2NSF(Interface to Network Security Functions) 기반으로 구현된다[11]. 〈그림 4〉는 클라우드 기반 보안 서비스 시스템을 보여주고 있다[12]. 사용자(예, 네트워크 관리자)는 본 시스템을 통해 스마트 빌딩의 보안 정책에 대한 의도(Intent)를 작성 후 보안 제어기(Security Controller)에게 전달함으로써 원하는 보안 서비스(예, 시간 기반 방화벽 서비스, 웹필터 서비스)를 수행할 수 있다.

〈그림 4〉에서 I2NSF 사용자가 보안 서비스에 대한 의도(즉 상위레벨 보안 정책)를 생성해서 보안 제어기에서 송신하면, 보안 제어기는 보안 정책 번역기(Security Policy Translator)[14]를 통해 보안 서비스 함수(예, 방화벽, 웹필터)가 이해할 수 있는 하위레벨 보안 정책으로 번역한다.

〈그림 5〉는 의도 기반 네트워킹(IBN)을 지원하는 I2NSF 프레임워크를 보여주고 있다[12][13]. 그림처럼 6단계로 폐쇄 루프 보안 제어를 통해 I2NSF 사용자의 보안 의도에 부합하는 보안 서비스를 제공할 수 있다. 보안 서비스를 제공하는 네트워크 보안 함수(Network Security Function: NSF)는 자신의 모니터링 데이터를 I2NSF 분석기에게 제공한다. I2NSF 분석기는 제공받은 모니터링 데이터를 기계학습(Machine Learning: ML)으로 분석하여 NSF가 새로운 보안 공격을 발견했는지, NSF가 보안공격을 받고 있는지, NSF의 보안 서비스를 위한 하드웨어 리소스(예, CPU, 메모리, 디스크)가 부족한지를 분석한다. 만약 새로운 보안 공격의 발견 또는 자신이 보안 공격을 받았으면 I2NSF 분석기는 이러한 보안 공격을 무력화시키기 위해 기존의 보안 정책을 보완하거나 새로운 보안정책을 생성하는 재설정 정

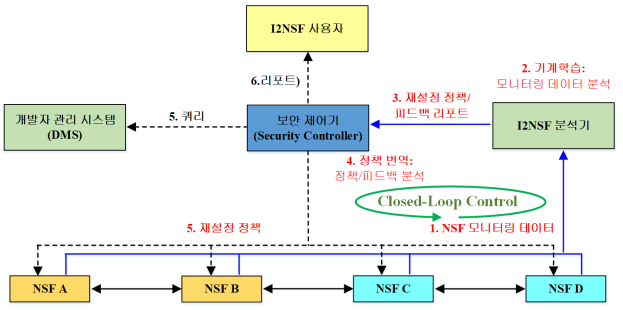

그림 5. IBN 지원하는 I2NSF 프레임워크[12][13]

책(Reconfiguration Policy)을 생성한다. 반면에 NSF 관련 하드웨어 리소스 부족이 발견되면 I2NSF 분석기는 피드백 리포트(Feedback Report)를 생성하여 보안 제어기에게 전달하여 하드웨어 리소스 보충을 요청한다. 이와 같이 I2NSF 시스템은 폐쇄루프 제어(Closed-Loop Control)을 통해 I2NSF 사용자의 개입 없이 자율적으로 보안 공격 및 리소스 이슈에 대한 대응을 수행할 수 있다.

나. 소프트웨어 정의 차량 프레임워크

IBN 시스템의 두 번째 유스케이스로서 이동 객체(Mobile Object: MO)인 소프트웨어 정의 차량(Software-Defined Vehicle: SDV)의 내부 네트워크(In-Vehicle Network)의 네트워크 함수, 보안 함수 및 응용 함수 등의 서비스 함수(Service Function: SF)를 차량 클라우드(Vehicular Cloud)를 통해 설정 및 관리할 수 있다[15].

〈그림 6〉은 소프트웨어 정의 차량 프레임워크를 보여주고 있다[15]. 차량 클라우드를 통해 SDV 사용자가 정한 네트워크 함수(예, 라우터), 보안 함수(예, 방화벽), 응용 함수(예, 자율주행 모듈, 내비게이터)에 대한 정책이 SDV에게 전달되고, SDV는 차량 내부 클라우드의 다양한 서비스 함수들을 위한 컨테이너들을 설정할 수 있다.

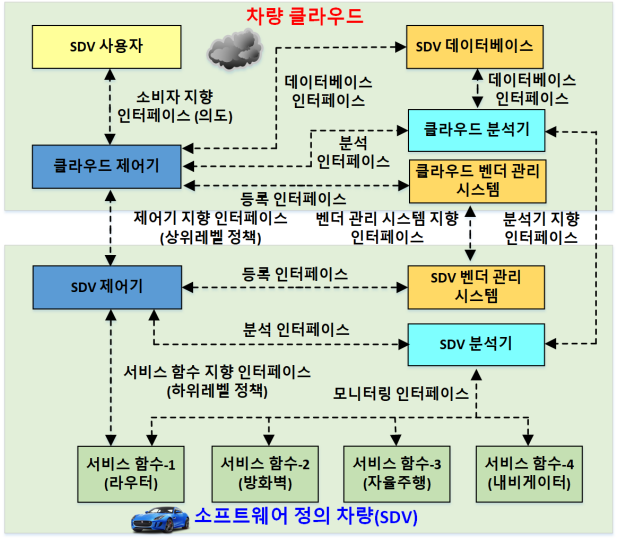

그림 6. 소프트웨어 정의 차량 프레임워크[15]

SDV뿐만 아니라 무인비행기(Unmanned Aerial Vehicle: UAV)와 비행자동차(Urban Air Mobility: UAM) 같은 이동 객체(MO)의 내부 네트워크에서 다양한 서비스 함수(예, 네트워크, 보안, AI 응용 서비스)인 인-네트워크 함수(In-Network Function: INF)에 대한 설정 및 모니터링이 필요하다. 이러한 인-네트워크 함수(INF)에 대한 인터페이스(Interface to In-Network Functions: I2INF)에 대한 문제정의[16], I2INF 프레임워크[17] 및 유스케이스[18]가 IETF에서 논의되고 있다. 이러한 I2INF 표준화는 이동 객체 뿐만 아니라 엣지 컴퓨팅(Edge Computing)을 위한 엣지 클라우드(Edge Cloud)의 내부 네트워크 INF 구성 및 모니터링도 고려하고 있다. 이러한 I2INF를 위한 문제정의, 프레임워크 및 유스케이스 표준화를 위해 IETF 내에 I2ICF(Interface to In-Network Computing Functions) 그룹이 창립되었다[19]. I2ICF 그룹은 2025년에 워킹그룹(Working Group: WG) 형성을 위한 미팅인 Birds of a Feather(BoF)를 IETF 정기회의에서 추진할 계획이다.

3. IBN 적용의 학습 결과

글로벌 네트워크 벤더인 시스코, 화웨이, 노키아 등은 IBN 기술 및 표준화에 적극 참여하고 있다[20]-[23]. 이들 기업들은 ONAP(Open Network Automation Platform) 같은 오픈소스[24]를 기반으로IBN 기술 개발 및 실제 네트워크 및 클라우드에 IBN 적용을 위한 노력을 하고 있다.

시스코는 IBN 기술의 선도 주자로서 네트워크 장비 관리 및 네트워크 서비스 프로비저닝(Provisioning)에 IBN을 적용하고 있다[20][21]. 물리적 네트워크 인프라 또는 가상 네트워크 인프라에서 네트워크 자동화를 지원한다. 또한 시스코는 고화질 화상회의 같은 종단간 서비스 품질 보장 네트워크 설정을 위한 네트워크 슬라이싱(Network Slicing) 기술을 개발하고 있다.

화웨이는 네트워크 함수 가상화(Network Functions Virtualization: NFV)[25][26]와 소프트웨어 정의 네트워킹(Software-Defined Networking: SDN)[27] 기술 개발을 통해 IBN 관련 기술 개발 및 표준화에 많은 투자를 하고 있다[22][23]. 화웨이는 네트워크 인터페이스 설정, 무선 서비스 설정, 가상랜(Virtual LAN: VLAN) 생성, 네트워크 슬라이싱 등의 네트워크 자동화에 IBN 기술을 적용하고 있다.

이와 같은 네트워크 벤더들의 IBN 기술 경험을 기반으로 다음

의 연구 방향을 고려해야 한다.

- 라이프 사이클 검증을 위한 일반적인 의도 모델
- 자율적인 단대단(End-to-End) 네트워크 정책 생성
- 거대 언어 모델(LLM)[6][7]을 통한 의도 번역

Ⅳ. 결 론

본 고에서는 IETF의 의도 기반 네트워킹(즉 Intent-Based Networking: IBN)의 표준화 동향을 설명하였다. 본 IBN 기술은 현재 NMRG에서 표준화되었고, 2024년 11월에 IBN 유스케이스 문서가 NMRG 메일링 리스트를 통해 NMRG Adoption Call이 진행되었고, 산업체와 학계로부터 많은 지지를 받았으므로 2025년초에 RG 문서로 채택될 예정이다. I2ICF 그룹은 IBN 기술을 인-네트워크 함수 설정 및 모니터링을 위한 프레임워크와 인터페이스 표준화를 위해 워킹그룹 창립을 위해 노력을 할 예정이다. 이와 같이 IBN 기술은 IETF 중심의 표준화기구 뿐만 아니라 학계와 산업체에서 활발히 연구 및 개발되어 인공지능(AI) 기반의 지능형 서비스를 위한 네트워크, 보안 및 응용 서비스의 핵심 기술로 확산될 전망이다.

Acknowledgements

이 논문은 2025년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No. RS-2024-00398199, RS-2022-II221015).

참 고 문 헌

[1] IETF, https://www.ietf.org/

[2] IRTF, https://www.irtf.org/

[3] NMRG. https://datatracker.ietf.org/group/nmrg/about/

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

[5] J. Jeong, "The Technology Trends of Intent-Based Networking in 5G Networks", IITP Weekly ICT Trends, Nov. 2024.

[6] 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.

[7] 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.

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

[9] C. Li, O. Havel, A. Olariu, P. Martinez-Julia, J. Nobre, and D. Lopez, "Intent Classification", RFC 9316, Oct. 2022.

[10] K. Yao, D. Chen, J. Jeong, Q. Wu, C. Yang, L. Contreras, and G. Fioccola, "Use Cases and Practices for Intent-Based Networking", Internet-Draft, draft-kdj-nmrg-ibn-usecases-02, Oct. 2024.

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

[12] J. Jeong and P. Lingga, "CBSS: Cloud-Based Security System with Interface to Network Security Functions", 14th International Conference on Mobile Computing and Ubiquitous Networking (ICMU), Nov. 29, 2023.

[13] P. Lingga, J. Jeong, and L. Dunbar, "ICSC: Intent-Based Closed-Loop Security Control System for Cloud-Based Security Services", IEEE Communications Magazine, Dec. 2024.

[14] 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.

[15] J. Jeong, Y. Shen, Y. Ahn, and M. Gu, "An Intent-Based Management Framework for Software-Defined Vehicles in Intelligent Transportation Systems", Internet-Draft, draft-jeong-opsawg-intent-based-sdv-framework-03, Dec. 2024.

[16] J. Jeong, Y. Shen, Y. Ahn, Y. Kim, E. Duarte Jr., and K. Yao, "Interface to In-Network Functions (I2INF):

Problem Statement", Internet-Draft, draft-jeong-opsawg-i2inf-problem-statement-02, Nov. 2024.
[17] J. Jeong, Y. Shen, Y. Ahn, Y. Kim, E. Duarte Jr., and K. Yao, "A Framework for the Interface to In-Network Functions (I2INF)", Internet-Draft, draft-jeong-opsawg-i2inf-framework-02, Nov. 2024.
[18] K. Yao, W. Wu, and J. Jeong, "Interfaces of In-Network Functions in Data Center Networking", Internet-Draft, draft-ywj-opsawg-i2inf-data-center-networking-00, Nov. 2024.
[19] I2ICF, https://mailarchive.ietf.org/arch/browse/i2icf/
[20] Cisco, "What is intent-based networking (IBN)?", https://www.cisco.com/c/en/us/solutions/intent-based-networking.html
[21] P. Kelly, "Intent-Based Networking: Automated Assurance's Critical Success Factor", Whitepaper, Appledore Research and Cisco, Mar. 2023.
[22] Huawei, "What Is Intent-driven Deployment?", https://info.support.huawei.com/info-finder/encyclopedia/en/Intent-driven+Deployment.html
[23] L. Deng and C. Chen, "A General Implementation with Intent-Based Network in ONAP", https://youtu.be/I5g066xiXmk?si=9HbhexTcoN48X9e9
[24] Open Network Automation Platform (ONAP) Website, https://www.onap.org/
[25] ETSI, "Network Functions Virtualisation (NFV); Architectural Framework", ETSI GS NFV 002 V1.2.1, Dec. 2014.
[26] ETSI, "Network Functions Virtualisation (NFV) Release 2; Management and Orchestration; Architectural Framework Specification", ETSI GS NFV 006 V2.1.1, Jan. 2021.
[27] M. Boucadair and C. Jacquenet, "Software-Defined Networking: A Perspective from within a Service Provider Environment", RFC 7149, Mar. 2014.

약 력

정 재 훈

1999년 성균관대학교 정보공학과 학사
2001년 서울대학교 컴퓨터공학과 석사
2009년 University of Minnesota 컴퓨터공학과 박사
2001년~2004년 한국전자통신연구원 표준연구센터 연구원
2010년~2012년 Brocade Communications Systems 소프트웨어 엔지니어
2012년~현재 성균관대학교 소프트웨어학과 교수
2015년~현재 TTA ICT 국제표준화 전문가
관심분야: 의도 기반 네트워킹, 차량 네트워킹, 사물인터넷, 네트워크 보안, IETF 표준화.
Email: pauljeong@skku.edu