논문 22-47-04-09 The Journal of Korean Institute of Communications and Information Sciences '22-04 Vol.47 No.04
https://doi.org/10.7840/kics.2022.47.4.625

네트워크 지능화를 위한 인공지능/기계학습 모델 및 데이터셋 기술동향

이 주 영◆°, 신 승 재*, 윤 승 현*, 김 태 연*

Survey on Artificial Intelligence & Machine Learning Models and Datasets for Network Intelligence

Jooyoung Lee◆°, Seungjae Shin*, Seunghyun Yoon*, Taeyeon Kim*

요 약

근래 등장한 심층신경망 기술의 발달로 인해 인공지능/기계학습 기술은 다양한 산업분야에서 지능화를 통한 비즈니스 혁신을 이끄는 핵심기술로 주목받고 있다. 이에 따라, 막대한 규모와 트래픽의 폭증 및 운용 복잡성이 예상되는 미래 인터넷의 효율적 제어를 위한 방안으로 인공지능/기계학습 모델을 활용하는 네트워크 지능화 연구의 사례가 증가하고 있다. 성공적인 네트워크 지능화를 위해서는 먼저 양질의 데이터셋을 확보하고 양질의 인공지능/기계학습 모델을 구성하여 학습시키는 것이 핵심이다. 본 고에서는 근래 5년간 저명한 학술지 및 학술대회에서 발표된 다수의 논문들을 분석한 결과를 기반으로, 네트워크 지능화를 위한 데이터셋 및 인공지능/기계학습 모델 기술에 대한 최근의 연구동향을 소개 및 분석한다. 이를 통해 최근 수행된 네트워크 지능화 기술들의 현황을 파악하기 위한 유용한 가이드라인을 제시하고자 한다.

키워드 : 네트워크 지능화, 데이터셋, 인공지능, 기계학습, 학습모델
Key Words : Network Intelligence, Datasets, Artificial Intelligence, Machine Learning

ABSTRACT

Thanks to the recent advancements in deep neural networks, artificial intelligence & machine learning technologies are getting more attentions as one of the key enablers to innovate business processes in a variety of industries and application domains. Along with this trend, we are seeing a considerable number of researches on network intelligence that exploit the artificial intelligence & machine learning models to effectively control future Internet environment which is expected to be much more large, complex, and exploded by traffics than ever before. In order to realize successful network intelligence, it is important to obtain desirable datasets and construct models with excellent accuracy. In this paper, we review and summarize recent trends of datasets and artificial intelligence & machine learning models for network intelligence based on going through a number of papers that are introduced in high-quality academic journals and conferences for recent five years. We believe that our review and summary can be a useful guideline to identify the current research trends on network intelligence.

※ 이 논문은 2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임[No.2021-0-00851, 주문형 데이터 기반 네트워크 지능화 프레임워크 기술 개발].

◆° First & Corresponding Author : Intelligent Network Research Section, Electronics and Telecommunications Research Institute, joolee@etri.re.kr, 정회원

* Intelligent Network Research Section, Electronics and Telecommunications Research Institute, {sjshin0505, shpyoon, tykim}@etri.re.kr, 정회원

논문번호 : 202112-326-B-RN, Received December 1, 2021; Revised January 17, 2022; Accepted January 24, 2022

Ⅰ. 서 론

근래 눈부시게 발전한 AI/ML (Artificial Intelligence & Machine Learning) 기술은 다양한 응용 도메인(Domain)에서 각종 비즈니스 프로세스 (Business Process) 및 품질 혁신을 위한 유망한 핵심 촉진자 (Key Enabler) 기술로써 관심을 모으고 있다. 이에 따라, 막대한 규모, 트래픽 (Traffic) 폭증 및 높은 복잡성이 예상되는 미래 인터넷 시대에 대비하기 위해 통신 및 네트워크 (Network) 시스템 제어 분야에서도 AI/ML 기술을 접목하여 예측성, 자율성 및 최적성의 증대를 꾀하는 다양한 기술적 시도들이 나타나고 있다[1,2].

네트워크 시스템 제어를 위한 대표적인 관측 데이터로는 망을 통과하는 패킷 (Packet)들이 모인 트래픽과 서버에서 처리하는 워크로드 (Workload) 등을 들 수 있다. 이들은 대개, 방대한 규모에 따른 레이블링 (Labeling)의 어려움과 개인정보보호와 관련된 법적 이슈들로 인해 수집, 처리 및 공개가 용이하지 않다. 따라서 다양한 상황을 포괄적으로 대표할 수 있는 보편적 네트워크 데이터셋 (Dataset)의 구축 및 지능화를 위한 기술적 노력이 필요한 상황이다.

본 고에서는 2016년부터 2021년 사이에 통신 및 네트워크 분야를 다루는 저명 학술지 및 학술대회에 발표된 112편의 논문을 선정하여 분석하고, 네트워크 지능화 연구 시 사용하는 데이터들을 데이터 소스, 원시 데이터, 측정단위 및 특징값이라는 기준을 사용하여 분류한다. 또한 네트워크 지능화를 위한 시스템의 응용 도메인 및 활용되는 AI/ML 모델들을 사례 중심으로 소개한다. 본 고에서 제시하는 분류 (Taxonomy) 및 사례들이 근래 수행된 네트워크 지능화 시스템 연구의 현황을 파악하기 위한 하나의 가이드라인으로 사용되길 기대한다.

본 논문의 남은 구성은 다음과 같다. 먼저 2장에서 네트워크 지능화 시스템을 위한 데이터셋 구축 시 고려해야 할 기준들을 논의하고, 이를 기반으로 데이터셋의 유형과 사례를 제시 및 분류한다. 3장에서는 네트워크 지능화의 세부 응용분야와 이들 각각에 따른 AI/ML 모델의 적용 사례를 제시한다. 마지막으로 4장에서 전체적인 결론을 제시함으로써 논문을 마무리한다.

Ⅱ. 네트워크 학습 데이터셋 분류

2.1 네트워크 학습데이터 수집을 위한 고려사항

네트워크 지능화 목적의 시스템에서 활용되는 데이터셋은 수집 및 처리 과정에서 텍스트 (Text), 음성 (Voice), 영상 (Video) 등과 같이 기존 응용에서 사용되던 데이터셋과 차이가 있다. 먼저, 데이터 수집 소스 (Source), 물리적 수집 위치 및 시간에 따라 획득한 데이터의 특성과 분포가 다르다. 특히, 네트워크 트래픽은 연속성 및 시계열적 특성을 가지고 있으며, 데이터셋 내에 다수의 정보가 혼재되어있다. 이에 따라, 네트워크 지능화를 위한 데이터셋 구축은 다음의 사항을 결정하는 과정으로 볼 수 있다.

- 데이터 소스 (Data Source)
- 원시 데이터 (Raw Data)
- 측정단위 (Measurement Units)
- 학습/추론을 위한 특징값 (Features)

본 절에서는 상기 4종의 기준에 따라 근래 제안된 네트워크 지능화 기술들이 AI/ML 모델의 입력으로 사용한 데이터 유형을 분류하고 각 유형별 사례를 기술한다. 그림 1은 상기 4종의 기준을 다시 61종의 세부유형으로 나눈 분류체계를 도시한 것이다. 도면에서 해당 유형에 속한 문헌의 수가 많을수록, 청색 연결선을 더 굵게 표현하였다.

2.1.1 데이터 소스 (Data Source)

최근 네트워크 지능화 목적의 연구들은 단일 소스 혹은 다중 소스에서 수집한 데이터셋들을 활용했으며, 주로 사용한 데이터 소스들은 다음과 같다.

- 백본망 (Backbone Network)
- 시뮬레이션 (Simulation)
- 클라우드 (Cloud) 및 데이터센터 (Datacenter)
- 라우터 (Router)
- 스위치 (Switch)
- 게이트웨이 (Gateway)
- 서버 (Server)
- 무선 (Air) 구간
- 사용자기기 (User Equipment: UE)

다수의 연구들이 실제 운용 중인 백본망에서 수집된 데이터를 사용하였으며[3-9], 비슷한 수의 연구들이 시뮬레이션 환경을 구성하고 이로부터 생성한 데이터

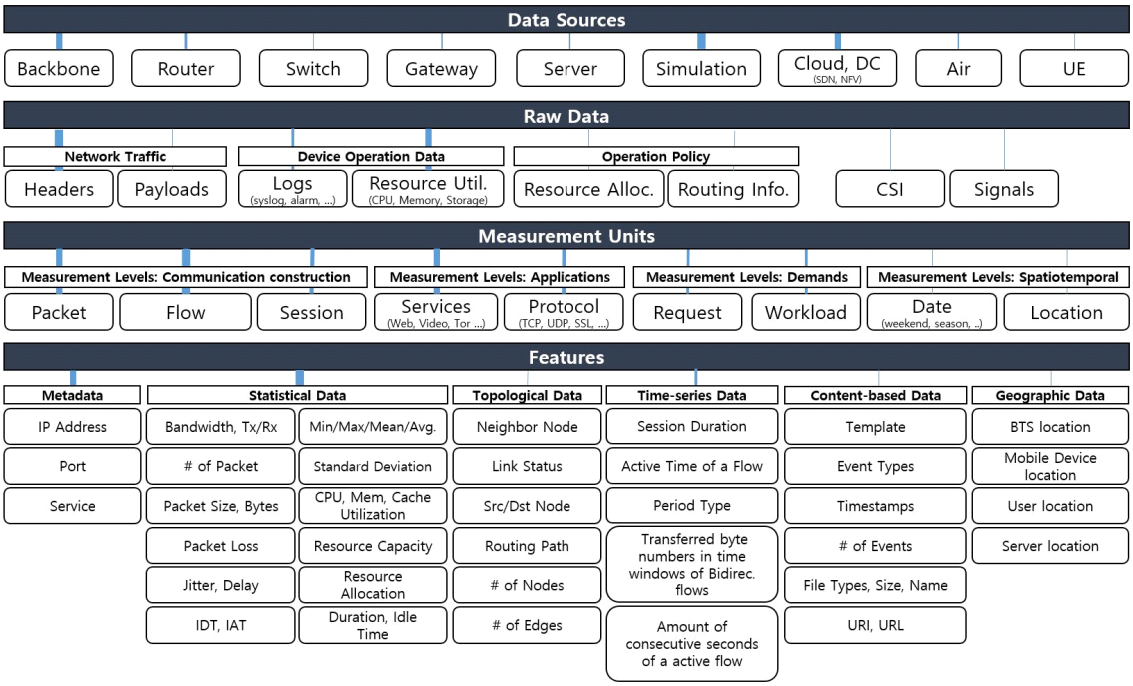


그림 1. 네트워크 지능화를 위한 데이터셋 유형 분류
Fig. 1. Taxonomy of datasets for network intelligence

를 활용하였다[10-13]. 하지만, 네트워크 트래픽은 수집 위치에 따라 데이터의 분포 및 특성이 달라질 수 있으며 이는 AI/ML 모델의 학습 품질에도 영향을 미칠 수 있다. 그럼에도 불구하고 다수의 문헌들이 데이터 수집의 물리적 위치와 그 영향에 대해 명시하고 있지 않다. 마찬가지로 시뮬레이션 환경을 구성해 트래픽을 생성하는 경우에도 유사한 한계점이 나타나고 있다.

클라우드 서비스 (Cloud Service)를 위한 자원 할당 최적화 문제를 다룬 연구들의 경우, 클라우드 환경이나 데이터센터에서 워크로드 및 VNF (Virtual Network Function) 데이터를 주로 수집하여 지능화를 위한 AI/ML 모델의 학습에 사용하였다[14-26].

그 외에, 라우터, 스위치, 게이트웨이 등의 네트워크 장비 내에서 획득할 수 있는 데이터를 수집하여 활용하는 연구들과[18,27-33] 네트워크 장비 이외에 웹서버로부터 획득한 데이터를 활용하는 경우들이 존재한다. 추가적으로, 무선통신 시스템의 사용자 단말에서 생성되는 데이터를 사용한 사례들도 있다[27,33,34].

2.1.2 원시 데이터 (Raw Data)

데이터 소스가 결정되었다면 각 소스에서 어떤 원시 데이터를 수집할 것인가를 결정해야 한다. 본 고에서는 추가의 가공 없이 데이터 소스에서 수집된 상태 그대로의 데이터를 원시 데이터로 지칭한다. 각 데이터 소스에서 수집할 수 있는 원시 데이터의 종류는 다음과 같다.

- 네트워크 트래픽 (Network Traffic)
  - 헤더 (Headers)
  - 페이로드 (Payloads)
- 장비 운용 (Device Operation) 데이터
  - 로그 (Logs)
  - 자원 (CPU, Memory, Storage 등) 사용 상태 (Resource Utilization Status)
- 운용 정책 (Operation Policy)
  - 자원 할당 상태 (Resource Allocation Status)
  - 라우팅 정보 (Routing Information)
- 기타
  - 채널 상태 정보 (Channel State Information)
  - 무선 신호 (Signals)

근래 상당수의 네트워크 지능화 시스템 연구들이 트래픽 분류 또는 수요예측 문제를 다루고 있으며, 네트워크 트래픽 자체를 학습 데이터로 활용하여 이러한 문제들을 위한 AI/ML 모델을 구축한다. 다수의 연구에서 트래픽 패킷 헤더를 활용하고 있으며, 페이로

드 (Payload) 일부를 활용한 사례도 존재한다[35]. 페이로드에 유용한 내용과 다양한 형태의 정보가 포함되어 있음에도 불구하고 활용 사례가 많지 않음은 데이터 보안에 관련된 법적 이슈로 인해 수집, 공개 및 활용이 제약됨을 주된 이유로 추정할 수 있다. 또한, 페이로드가 암호화되는 경우도 많기 때문에 데이터의 정형화 및 특징 추출 시 기술적 어려움이 수반된다는 점도 활용을 어렵게 만드는 원인으로 볼 수 있다.

네트워크 장비에서 획득하는 원시 데이터 사례로는 장비 운용 중에 생성되는 Syslog[36], 침입탐지를 위한 Snort 이벤트 (Event)[37], DNS (Domain Name Server) 및 인증 서버에서 추출한 시스템 컴포넌트 (Component) 로그[38], 등을 들 수 있다. 또한, 클라우드 환경에서 가상 디바이스 (Device)들이 사용하는 CPU, Memory 및 Storage 등의 자원사용 상태[16], 라우터의 자원 활용 상태를 수집해 부하예측에 활용하기도 한다[39].

자원할당 및 네트워크 운용 최적화를 목적으로 한 지능화 연구의 경우, 자원할당 및 운용상태 자체를 원시 데이터로 활용한다[14,15]. 이들의 경우, 각 장비로부터 자원활용 상태를 수집하는데 그치지 않고, 중앙의 관리 개체(예: Controller)가 최적의 자원 할당상태를 유지할 수 있도록 하는 제어문제 해결을 목표로 하고 있다. 이는 기존의 규칙기반 자원관리 방법론에 비해 보다 높은 지능화를 추구하는 기술적 시도로 생각된다.

2.1.3 측정단위 (Measurement Units)

본 절 도입부에 언급한 바와 같이 네트워크 데이터는 시간적 연속성 및 시계열적 특성을 갖기 때문에 데이터셋의 생성 시, 연속된 시계열 데이터를 측정하고 수집하기 위한 단위가 필요하다. 측정단위는 응용 도메인 및 지능화 대상에 따라 차이가 있으며, 동시에 여러 측정단위를 사용하여 데이터를 추출하는 경우도 있다.

- 통신 구성 (Communication Construction)
  - 패킷 (Packet)
  - 플로우 (Flow)
  - 세션 (Session)
- 응용 (Applications)
  - 서비스 (Services)
  - 프로토콜 (Protocol)
- 요청 (Demands)
  - 자원 요청 (Request)
  - 워크로드 (Workload)별 할당자원
- 시공간 (Spatiotemporal)
  - 날짜 (Date)
  - 위치 (Location)

트래픽 데이터를 사용하는 연구들은 패킷, 플로우 (Flow), 세션 (Session) 등을 측정단위로 사용하여 데이터를 생성한다. 패킷 단위로 데이터를 생성하는 경우 타임 윈도우 (Time Window)를 활용하며, 데이터 재조립 속도가 상대적으로 빠른 플로우 단위가 세션 단위 측정보다 많이 사용되는 편이다.

또한 모든 종류의 트래픽을 수집하기보다 특정 서비스 혹은 프로토콜만 지정하여 수집하는 방식도 많이 사용된다. 이들은 응용 도메인 및 지능화의 목적에 맞추어 웹 서비스, 영상 스트리밍 (Streaming), 토르 (ToR)[29,30,40-42] 등 특정 응용을 위한 트래픽만 선별하여 수집한다. 해당 방식은 트래픽 데이터를 AI/ML 모델에 학습시켜 비정상 트래픽을 탐지하기 위한 연구에서 많이 사용된다. 특히, 악성 트래픽을 데이터셋으로 활용하는 사례들도 다수 존재한다[3],43-51].

TCP (Transport Control Protocol)[52,53], UDP (User Datagram Protocol)[54] 등 프로토콜을 특정해서 데이터를 수집하는 사례들 역시 찾아볼 수 있다. 근래에는 암호화된 트래픽을 수집하여 AI/ML 모델을 학습시키는 보다 발전된 형태의 사례들도 등장하고 있다[34,35,42,48,55-57].

클라우드 환경을 대상으로 하는 연구들의 경우, 자원의 요청 (Request)[17,23,26] 및 워크로드 단위의 자원 할당량 데이터를 수집한다[20,21].

사용자 수요 및 비정기적 이벤트에 대한 예측 모델의 경우 시공간 단위 데이터 측정을 사용하며, 일 (Day), 주 (Week), 월 (Month), 계절 (Season) 및 휴일 (Holiday) 등으로 구분하여 데이터를 수집하거나 도심, 교통수단 내부 등 사용자의 위치를 특정해 수집하기도 한다[58].

2.1.4 학습에 사용할 특징값 (Features)

상기 기술한 원시 데이터에서 모델의 훈련 및 추론 과정에 사용될 특징 데이터를 추출하고, 각종 전처리를 적용하여 가공하면, 네트워크 지능화를 위한 학습 데이터셋의 생성이 완료된다. 근래의 네트워크 지능화 연구들이 사용하는 특징값 유형은 다음과 같다.

(1) 메타데이터 (Metadata)

메타데이터 유형은 현재 인터넷 환경에서 널리 사용되는 TCP/IP 프로토콜 모음 (Protocol Suite)을 구

성하는 IP, TCP 및 UDP 패킷의 각 필드 (Field)들을 데이터로 사용하는 사례들을 지칭한다. 이들은 패킷 수집 시 헤더 및 페이로드에서 바로 추출 가능한 정보라는 특징이 있으며, 명목형 (Nominal) 데이터이기 때문에 적절한 전처리를 통해 숫자 형태로 변환하는 과정이 필요하다.

네트워크 트래픽에서 추출하는 대표적인 메타데이터는 IP의 경우 Source Address, Destination Address, Source Port, Destination Port, Service 등이 있다. TCP의 경우 일련번호, 회신번호, 헤더 길이, 플래그 (Flag), 윈도우 크기, 체크섬 (Checksum) 및 페이로드 등을 추출하고, UDP의 경우 패킷 길이, 체크섬, 페이로드 값을 사용하기도 한다. 보안 연결된 트래픽의 경우 TLS/SSL 핸드쉐이크 메시지 (Handshake Message) 필드도 수집 대상이 된다[3,5,7,10,11,25,34,42,43,48-52,55,56,59-70].

본 특징값 유형은 침입/이상탐지, 트래픽 분류, 라우팅, 트래픽 모델링 (Modeling) 최적화 등의 응용을 위한 AI/ML 모델 개발에 주로 활용된다.

(2) 통계 데이터 (Statistical Data)

통계 데이터는 네트워크 시스템으로부터 수집한 원시 데이터에 수학적, 통계학적 처리를 적용하여 생성해내는 가공 데이터를 지칭한다. 특히, TCP/IP 플로우 또는 응용계층 세션별로 추출할 수 있는 다양한 통계적 계산값들이 AI/ML 모델 개발을 위한 특징값으로 사용되고 있다.

대표적인 통계 데이터 특징값의 사례로는 플로우 지속시간, 플로우 지속시간 동안의 데이터 및 응답 (Acknowledge: ACK) 패킷 송수신 총량, 시간에 따른 패킷의 크기 변화, 패킷의 IAT (Inter-Arrival Time), 패킷 송수신시 불안정계수 (Jitter) 등을 들 수 있으며, 상기 특징값들에 대한 기댓값 (Mean), 중심값 (Median), 분산 (Variance), 표준편차 (Standard Deviation), 최대값 (Max), 최소값 (Min), 도수분포표 및 히스토그램 (Histogram) 등 역시 특징값으로 사용되기도 한다[4-8],10,11,30,34,35,40-43],46-49,51,5,55,59,61-63,65,66,68,69-75,76].

이러한 통계 데이터 특징값은 침입/이상 탐지, 트래픽 분류, 라우팅, 트래픽 모델링, 최적화, QoS (Quality of Service) 및 트래픽 분석 등 대부분의 네트워크 지능화 시스템을 위한 AI/ML 모델 생성에 광범위하게 활용되고 있다.

(3) 토폴로지 데이터 (Topological Data)

네트워크는 본질적으로 노드 (Node)와 링크 (Link)로 구성된 그래프 (Graph) 구조로 표현할 수 있기 때문에 토폴로지 상의 인접한 노드들 간의 링크 상태와 경로 (Path) 별 송수신 트래픽량 역시 지능화를 위한 유용한 데이터로 활용될 수 있다. 본 유형의 데이터를 특징값으로 사용하는 경우 지능화 대상 네트워크 시스템의 토폴로지 정보 획득이 필수이며, 수집된 원시 데이터 역시 토폴로지의 구조나 변화에 의존성을 지니게 된다.

본 특징값 유형에 대한 사례로는 노드 간 인접성 및 링크 정보를 포괄하는 토폴로지 데이터, 노드 간 (토폴로지 상) 거리, 라우팅 정보 및 제어 메시지의 송수신 및 오류 현황, 노드 간 조우 (Encounter) 기록과 노드 쌍 (Pair)별 트래픽 요구 행렬 (Demand Matrix), 링크 비용 행렬 (Link Cost Matrix) 등을 들 수 있다[12,13,25,77-85].

이들은 침입/이상 탐지, 라우팅, 트래픽 모델링 및 최적화를 위한 지능화 응용에서 주요 특징값으로 활용된다.

(4) 시계열 데이터 (Time-series Data)

시계열 데이터는 정해진 시간 간격으로 수집, 처리, 정렬된 특징값 유형으로, 클라우드 데이터센터의 컴퓨팅 자원 (CPU, Memory, Storage 등), 네트워크 회선의 대역폭 (Bandwidth) 자원, 기지국 대역폭 자원 등 각종 자원의 요구량 및 사용량에 관련된 데이터에서 많이 나타난다. 시계열 데이터 역시 통계 데이터와 마찬가지로 수학적, 통계적 재처리를 적용하여 사용하는 경우가 많으며, 시계열 데이터 수집의 기준이 되는 시간간격 (Time-scale)은 밀리초 (Millisecond), 초 (Second), 분 (Minute), 시간 (Hour), 일, 주, 월 등에 이르기까지 다양한 단위시간을 사용한다.

본 유형의 사례로는 단위시간 동안 연결된 플로우의 총 개수, 연결된 HTTP (Hyper-Text Transfer Protocol) 세션의 총 개수, 연결된 모든 플로우의 IP 및 포트 주소 분포 및 엔트로피, 지정된 플로우의 SYN, SYNACK, 데이터 패킷 송수신량, IAT, 불안정계수 등을 들 수 있다[14-23,26,27,33,39,86-95].

본 특징값 유형은 침입/이상 탐지, 트래픽 수요예측, 자원관리, QoS를 위한 지능화 응용에서 많이 활용된다.

(5) 내용 기반 데이터 (Content-based Data)

본 유형은 패킷의 페이로드 내부에 포함된 응용계

층 데이터 또는 네트워크 구성요소가 생성하는 각종 로그 메시지에서 추출한 특징값들을 의미한다. 페이로드에 포함된 콘텐츠 (Contents)를 활용하는 경우, 콘텐츠의 템플릿 (Template) 혹은 패턴 (Pattern)을 식별하는 알고리즘을 활용한다. 특히, 특정 이벤트의 유형 또는 발생 빈도를 특징으로 사용하는 경우, 페이로드에 포함된 파일의 타입, 크기, 이름을 기반으로 특징을 추출하기도 한다.

DNS, 인증서버, 스위치 및 UE (User Equipment) 등과 같은 네트워크 구성 요소들이 기록하는 각종 로그 메시지 또한 유용한 특징값으로 활용될 수 있다[36,38,59]. 웹 데이터의 경우 URL 문자열, 웹 문서, 웹 문서별 열람기록 (Page-View) 등에서 특징을 추출한다[18,27-33].

본 특징값 유형은 접속 웹사이트의 판별, 자원관리, 캐시관리, PII (Privacy Identifiable Information) 유출 및 응용계층 보안공격 탐지를 위한 AI/ML 기반 시스템에 폭넓게 활용된다. 특히, 응용계층 보안공격이 시스템에 오동작을 유발하는 특성에 착안하여 응용 계층 센싱 (Sensing)값을 활용해 보안공격을 간접 탐지하는 연구사례도 있다[28]. 이 외에도 트래픽 수요예측, 자원관리, 라우팅, 트래픽 분석, 네트워크 모델링 및 최적화 등의 분야에서 활용된다.

(6) 지리적 데이터 (Geographic Data)

본 특징값 유형의 대표적 사례로는 UE 및 사용자 위치, 서버 위치, BTS (Base Transport Station) 위치 등을 들 수 있다[24,54,58,88,89,95-111].

이들은 트래픽 수요예측, 자원관리, 무선통신추정 및 제어를 위한 네트워크 지능화 응용에서 AI/ML 모델의 입력으로 활용된다.

2.2 공개 네트워크 데이터셋 사례

본 절에서는 네트워크 지능화 연구에서 많이 활용된 공개 데이터셋 중 세 가지 사례를 선정하여 소개한다.

2.2.1 UNSW-NB15 데이터셋

본 데이터셋은 호주 UNSW (Univ. New South Wales, Canberra)의 사이버 보안 연구원 (Institute for Cyber Security)에서 보안 응용을 위한 AI/ML 모델 연구를 위해 구축한 데이터셋이다[112]. 본 데이터셋은 시뮬레이션 네트워크 환경을 구성하고 정상적인 활동에 따른 트래픽과 인위적으로 발생시킨 악의적 (Malicious) 트래픽을 혼합하는 형태로 생성되었다.

그림 2는 UNSW-NB15를 생성하기 위한 테스트베드를 도시한 것이다. IXIA PerfectStorm을 사용하여 정상트래픽을 생성하고, 2번 서버에 배치한 Malware를 통해 악성트래픽을 발생시키도록 했다. 해당 Malware는 Fuzzer, Analysis, Backdoors, DoS, Exploit, Generic, Reconnaissance, Shellcode 및 Worm 공격을 수행하며, 이 과정에서 악성 트래픽이 생성된다.

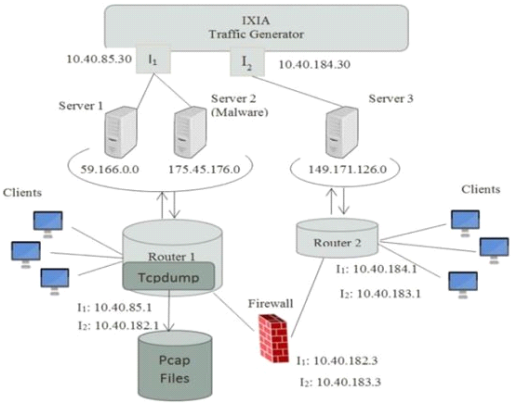


그림 2. UNSW-NB15 데이터셋 생성 테스트베드[112]
Fig. 2. Testbed for generating UNSW-NB15 Dataset

생성된 트래픽의 수집은 1번 라우터에 설치된 TCPdump를 통해 이루어진다. 수집된 트래픽을 PCAP 파일로 저장하고, 이후 Argus 및 Bro-IDS 유틸리티 (Utility)를 통해 학습에 필요한 특징들을 추출한다. 최종적으로는 100GB의 트래픽으로부터 175,341개 레코드 (Record)로 구성된 훈련용 데이터셋과 82,332개 레코드로 구성된 테스트용 데이터셋을 생성하였다.

UNSW-NB15의 특징값들은 자체적으로 개발된 12종의 알고리즘을 활용하여 추출되었으며, 클래스 (Class) 레이블을 포함한 49종의 항목으로 이루어져 있다. 이들은 네트워크 플로우에서 직접 또는 간단한 가공을 거쳐 획득할 수 있는 Flow feature, Basic feature, Content feature, Time feature와 좀 더 복잡한 처리를 거쳐 생성되는 Additional generated feature로 구성된다. Labelled feature로는 상기 언급한 9종의 공격 유형 중 하나를 표시하는 레이블과 해당 트래픽의 악성 여부를 판단하는 True/False 레이블을 포함한다.

2.2.2 MAWI 데이터셋

본 데이터셋은 일본 WIDE 프로젝트 산하의 MAWI 워킹그룹이 트래픽 측정 및 분석을 위해 실제 운용 중인 백본망에서 데이터를 수집한 것으로 PCAP

파일 형태로 제공된다[113]. 트래픽 수집은 TCPdump를 이용해 이루어졌으며, 개인정보보호를 위해 TCPdpriv 유틸리티를 활용한 IP 주소 스크램블링(Scrambling)을 수행하였다.

MAWI 데이터셋 중 미국과 일본을 잇는 링크에서 수집된 트래픽은 MAWILab이라는 데이터베이스로 제공되며, 트래픽 이상 탐지를 위해 개발된 방법들을 평가할 수 있도록 이상 트래픽에 대한 레이블을 포함하고 있다[114]. 해당 레이블은 다수의 탐지 도구를 사용하여 그들 각각의 이상여부 탐지 결과를 조합하는 형태로 생성되었다. MAWILab v1.1 데이터셋은 다음 10종의 특징들로 구성되어 있다.

- anamalyID: anomaly 식별자로 파일에 포함된 다수의 데이터가 동일 anomaly를 참조하는 경우를 식별
- srcIP: 이상 트래픽의 소스 IP 주소 (옵션)
- srcPort: 이상 트래픽의 소스 Port (옵션)
- dstIP: 이상 트래픽의 목적지 IP 주소 (옵션)
- dstPort: 이상 트래픽의 목적지 Port (옵션)
- taxonomy: 백본 상의 이상 트래픽 분류법에 따라 할당된 anomaly 카테고리
- heuristic: Port, TCP Flag, ICMP Code에 기반해 Heuristic에 따라 할당된 Anomaly 코드
- distance: Normal(D_n)과 Anomaly(D_a)로 판단된 값(Distance)의 차(D_n-D_a)
- nbDetectors: 해당 데이터를 이상 트래픽으로 리포팅한 탐지기의 수
- label: 이상 여부에 대한 레이블로 Anomalous, Suspicious, Notice, Benign 중 택일

그림 3은 XML 파일로 제공된 MAWILab 데이터셋의 예시이다. 예시에서 <anomaly> 엘리먼트

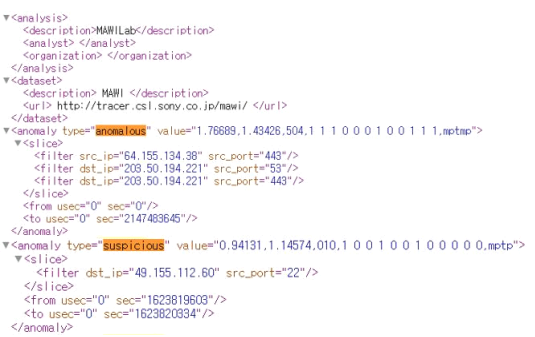


그림 3. MAWILab 데이터셋 예시[114]
Fig. 3. Example of MAWILab Dataset

(Element)는 속성으로 유형 (Type)과 값 (Value)을 갖는데 유형은 해당 데이터의 anomaly 레이블이며 값은 순차적으로 D_n, D_a, Heuristic code, Detector들의 판단 벡터(0: not report, 1: anomaly), 마지막은 Backbone Traffic Anomaly에 대한 Taxonomy를 의미한다.

2.2.3 TOTEM 데이터셋

TOTEM은 네트워크 상에서 라우터 간의 트래픽 양을 측정한 데이터를 활용하여 효율적인 트래픽 엔지니어링 (Traffic Engineering)을 지원하기 위한 도구이다[115,116]. TOTEM 데이터셋은 TOTEM Toolbox를 활용하여 실제 네트워크에서 수집한 데이터로부터 생성한 토폴로지 및 트래픽 행렬 데이터를 지칭한다[117]. TOTEM 데이터셋은 AI/ML 모델 학습을 목적으로 생성된 것이 아니기 때문에 공개된 데이터셋에는 별도의 레이블이나 정형화된 특징값 데이터가 없다. 그러나 근래의 네트워크 지능화 연구에서는 네트워크 트래픽 예측을 위한 학습 데이터로 이들을 활용한 사례가 있다.

TOTEM 데이터셋 중 하나인 GÉANT 데이터셋은 EU의 연구, 교육용 네트워크인 GÉANT 네트워크에서 수집된 데이터셋으로, 23개의 라우터와 38개의 내부 링크 및 53개의 외부 링크로 구성되어 있다[118]. GÉANT의 토폴로지 데이터는 하루 동안의 IS-IS 트레이스 (Trace)를 이용해 생성되었으며 익명화되어 있다. 트래픽 행렬은 매 15분마다 각 노드들 간에 교환된 트래픽의 양을 명세하는 행렬로, 약 4개월 동안 네트워크 상의 모든 링크에서 수집한 데이터를 이용하였다. 이 트래픽 행렬은 GÉANT의 전체 IGP (Interior Gateway Protocol) 라우팅 정보와 샘플링 (Sampling)한 NetFlow 데이터 및 BGP (Border Gateway

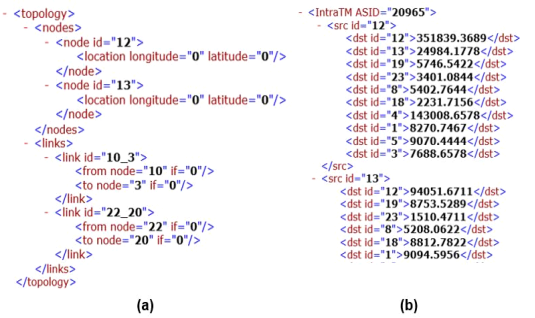


그림 4. TOTEM 데이터셋 사례. (a) 네트워크 토폴로지, (b) 트래픽 행렬[117]
Fig. 4. Example of TOTEM Dataset. (a) Network Topology, (b) Traffic Matrix

Protocol) 라우팅 정보를 사용하여 노드 쌍별로 트래픽 전송량을 계산하는 과정을 통해 만들어진다.

그림 4는 GÉANT 네트워크의 토폴로지와 트래픽 매트릭스 사례 중 일부를 도시한 것이다. (a)의 <topology>는 하위 요소로 <nodes>와 <links>를 갖고 있으며, 이들 각각은 네트워크를 구성하는 노드 및 링크에 대한 정보들을 포함한다. 각 노드의 값은 익명화를 위해 숫자 값으로 대체되어 있다. (b)는 15분 동안 각 노드에서 다른 노드들로 전달된 트래픽 양을 kbps 단위로 명세한 것이다.

지금까지 기술한 공개 네트워크 데이터셋 사례들을 그림 1의 네트워크 학습 데이터 유형에 따라 분류한 결과를 표 1에 제시하였다. 결론적으로 공개 데이터셋들도 앞서의 논문 분석 사례들과 유사하게 백본망과 시뮬레이션 환경에서 수집된 네트워크 트래픽으로부터 플로우 단위로 메타데이터, 통계 데이터 및 내용기반 데이터를 추출하여 학습데이터로 제공함을 확인할 수 있다.

표 1. 데이터 유형 분류에 따른 공개 데이터셋 사례 분석
Table 1. Analysis on public datasets according to data type taxonomy

Datasets	UNSW-NB15	MAWI	TOTEM
Data Sources	Simulation	Backbone	Backbone, Router
Raw Data	Network Traffic (Header)	Network Traffic (Header)	Network Traffic (Header) Operation Policy (Routing Info)
Measurement Units	Flow	Flow	Time
Features	Metadata, Statistical data, Content-based data	Metadata, Content-based data	Metadata, Statistical data
Examples	dur, xproto, xServ, xState, spkts, dpkts, sbytes, dbytes, sloss, dloss	srcip, srcPort, dstIP, dstPort, taxonomy, heuristic, distance	nodeID, linkID, bandwidth btw nodes, network topology

Ⅲ. 네트워크 인공지능 모델 분석

3.1 네트워크 지능화를 위한 AI/ML 모델분류

AI/ML 모델은 네트워크 지능화 시스템에서 추론 및 훈련의 주체가 되는 자료구조 또는 알고리즘 개체를 지칭한다. 본 고에서는 네트워크 지능화 연구에서 활용하고 있는 AI/ML 모델들을 표 2에 제시하였다.

심층신경망 기술의 발달로 인해 최근 널리 사용되는 MLP (Multi-Layer Perceptron), CNN (Convolution Neural Network) 등을 비롯하여, Decision Tree, C4.5, Random Forest, SVM (Support Vector Machine), k-NN (Nearest Neighbor) 등은 트래픽 분류, 침입/이상 탐지, 트래픽 모델링 등 다양한 응용 도메인에 널리 사용되고 있다. 또한 Bayesian Learning, GMM (Gaussian Mixture Model) 등 확률 모형 기반 방법론들도 사용되고 있다.

시계열 패턴의 예측에 적합한 RNN (Recurrent Neural Network), LSTM (Long Short-Term Memory), GRU (Gated Recurrent Unit) 등의 경우 트래픽의 수요 예측, 분석, 침입/이상탐지, 자원관리 등 모든 응용 분야에 걸쳐서 시계열 트래픽의 모델링 및 추론에 활용되고 있다.

표 2. 네트워크 지능화 응용분야별 사용 AI/ML 모델
Table 2. AI/ML Models for Network Intelligence

Application Domains	ML Models
Traffic Classification	Bayesian Learning, C4.5, CNN, Decision Tree, GMM, GNN, GRU, HMM, k-NN, Linear Model, MLP, Naïve Beyesian, Random Forest, RNN, SVM, XGBoost
Traffic Demand Prediction	CNN, DQN, EM, k-means, LASSO, LSTM, MLP, PCA, Random Forest, Ridge, Simulated Annealing
Resource Management	A3C, Bayesian Learning, CNN, DQN, LSTM, RNN, SVM, TD3
Routing	CNN, DDPG, DQN, MLP, Q-Learning, RNN
Intrusion and Anomaly Detection	Autoencoder, MLP, CNN, LSTM, GRU, DT, CART, RF, SVM, k-NN, Ensemble
Traffic Modelling and Optimization	AdaBoost, Autoencoder, CART, CNN, Decision Tree, Ensemble, GRU, k-NN, LDA, Linear Model, LSTM, MLP, Naïve Beyesian, Random Forest, RBM, SVM
Traffic Analysis	GAN, LSTM, MLP

자원 관리 및 라우팅 등 최적화된 솔루션을 탐색하는 문제들에 있어서는 Q-Learning, DQN (Deep Q-Network), DDPG (Deep Deterministic Policy Gradient), TD3 (Twin Delayed DDPG), A3C (Asynchronous Advantage Actor Critic) 등의 강화학습(Reinforcement Learning) 모델들이 많이 활용된다. 근래에는 연합학습(Federated Learning) 및 계층적 학습(Hierarchical Learning)과 같은 향상된 형태의 방법론을 활용함으로써 인공지능 모델의 추론 품질 및 확장성, 경제성, 보안성 등에서 개선을 꾀하는 사례들도 나타나고 있다.

이외에도 RBM (Restricted Boltzmann Machine) 및 Autoencoder, GAN (Generative Adversarial Network)과 같이 생성 모델을 사용하여 침입/이상탐지 및 트래픽 분석에 활용된 사례가 있으나 아직은 전통적인 접근법에 비해 적게 사용되는 편이다.

3.2 네트워크 지능화 응용 사례

본 절에서는 표 2에 제시한 네트워크 지능화 응용분야 중 많은 연구가 진행되고 있는 유형 5종에 관해 기술한다.

3.2.1 트래픽 분류 (Traffic Classification)

트래픽 분류 응용은 네트워크 회선을 통해 인가되는 패킷, 플로우 및 트래픽을 종류, 목적, 응용 등의 특성에 따라 구분하는 것을 목표로 한다. 일반적인 네트워크 트래픽을 대상으로 멀티미디어, 웹 브라우징, 이메일, 파일 전송 등 다양한 응용유형을 구분하기 위한 사례들이 대표적이며[35,65,70], 더 심화된 형태로 암호화된 트래픽의 응용유형을 구분하는 연구들도 등장하고 있다[41,55,56]. 또한, 암호화된 IP 트래픽의 접속 사이트를 분류하기 위한 사례들도 있다[34,68].

기타 응용 사례로는 IP 트래픽에서 ToR 트래픽을 분류하거나[41], TCP의 동작유형(예: BBR (Bottleneck Bandwidth and Round-trip propagation time), Cubic, Reno, Vegas 등)을 분류[69], 트래픽의 부하량 (Mice 또는 Elephant 중에서) 분류[67], 플로우의 전송률 및 지속시간을 예측하는 연구[11] 등을 들 수 있다.

3.2.2 트래픽 수요예측 (Traffic Demand Prediction)

본 응용분야는 유무선 네트워크, 데이터센터, MEC (Mobile Edge Computing) 클라우드 등에 인가되는 트래픽 또는 워크로드의 수요를 사전 예측하는 기술들을 포괄한다.

IP 트래픽 요구량 예측의 경우, 다중 회귀분석에 의해 트래픽 행렬을 완성[8]하거나, 트래픽 인가량[4] 또는 플로우 규모[76]를 예측하는 연구들이 대표적이다. 트래픽 수요를 Low, Medium, High로 단순화하는 대신 예측 정확도를 높이는 접근법도 있다[39].

데이터센터를 대상으로 하는 경우, 워크로드 트래픽의 양을 예측하거나[17,26], CPU, 메모리 및 네트워크 대역폭 등의 자원요구량 및 응답 시간을 예측하는 사례가 있다[18].

이동통신 시스템 및 MEC 환경을 대상으로 하는 경우, 5G-NFV-MEC 환경의 UPF (User Plain Function) 활용률[24] 또는 트래픽 인가량 예측[108], MEC 기반 CDN (Contents Distribution Network)에서 네트워크 캐시 (Cache) 자원관리를 위한 일별 콘텐츠 요청량[27] 또는 Serverless Function의 실행비용 예측[87], 단위 시간 및 단말별 데이터 송수신량 예측[74,103], 데이터센터별 트래픽 할당량 예측[97,98], 기지국별 트래픽 인가량 예측[104,107] 등을 사례로 들 수 있다.

3.2.3 자원 관리 (Resource Management)

본 응용분야는 유무선 네트워크, 데이터센터, MEC 및 가상화 네트워크 등에 인가되는 트래픽 또는 워크로드의 처리를 위한 자원 할당 및 스케줄링 기술들을 지칭한다. 자원은 환경 상세에 따라 CPU 코어, CPU 클럭율 (Clock Rate), VM (Virtual Machine), 서버, 네트워크 대역폭 등 다양한 유형으로 정의될 수 있다. 무선환경의 경우에는 채널 (Channel)화된 시간-주파수 자원 또는 전력의 형태로도 정의가 가능하다.

클라우드 환경을 대상으로 하는 경우, VM 스케일링 (Scaling) 수준[16], 워크로드별 할당할 CPU 코어 개수, CPU 클럭율[33] 등을 결정하는 연구들이 대표적이다. 또한 심층기계학습을 위한 계산 그래프 연산을 수행할 서버 집합을 결정하는 다소 특별한 시나리오 (Scenario)를 가정하는 연구들도 있다[91].

가상 네트워크 환경의 경우, VNF가 실행될 노드를 결정하거나[14], SFC (Service Function Chain)별 대역폭 할당량을 결정하는[22] 연구사례들이 있다.

최근 주목받고 있는 MEC 환경의 경우, AI/ML 모델을 사용한 자원관리 지능화 연구가 활발하게 이루어지고 있다. 주요한 사례로는 워크로드 오프로딩 (Offloading) 여부를 결정하는 연구를 들 수 있다[86,88,89,93,95]. 이들은 Fog-Cloud-IoT 융합 환경에서의 처리시간 최소화[86], QoS 보장을 위한 MEC 워크로드의 허용제어[88], MEC 기반 동적 이동망 및 V2X (Vehicle-to-X) 망에서의 계산, 통신비용[89,93] 및 지연

시간 최소화[95] 등 다양한 동작 시나리오 및 목적을 가정하고 있다. 또한, 사용자 단말별로 할당할 채널, 서버 및 VM 결정[15], 사용자 단말별 전송전력 및 CPU 사이클률 (Cycle Rate) 할당 제어[93] 등과 같이 여러 파라미터들을 한꺼번에 제어하는 결합형 최적화 (Joint Optimization) 사례들도 볼 수 있다.

상기 사례들 가운데 일부는 근래 주목받고 있는 연합학습[15], 계층적 학습[93] 및 강화학습[15,88,89,95] 등을 채택함으로써 지능제어의 수준향상을 꾀한다는 점에서 주목할 만하다.

3.2.4 라우팅 (Routing)

본 응용분야는 IP, 데이터센터, NDN (Named Data Network), 오버레이 (Overlay), IoT (Internet-of-Things), 이동통신망 등과 같이 다양한 네트워크 환경에서의 패킷 포워딩, 라우팅 및 링크 관리 기술들을 포괄한다.

네트워크 지능화를 통한 라우팅을 다룬 사례로는 IP 망의 패킷 포워딩을 위해 다음 패킷 전달지점을 결정하는 사례들이 다수이며[80,82,83], 트래픽 부하량, 버퍼량, 채널 상태와 같이 다수 개의 항목을 예측하는 방식도 있다[12]. 또한, ECMP (Equal Cost Multi-Path) 라우팅의 경로비 (Path Ratio)를 결정하거나[62], 링크별 가중치를 제어하는[85] 기법들도 제안된 바 있다.

그 외에도, 데이터센터[119], 오버레이[78], IoT[84], NDN[31] 등 다양한 시나리오를 고려한 라우팅 지능화 연구사례들이 존재한다.

3.2.5 침입/이상 탐지 (Intrusion/Anomaly Detection)

본 응용분야는 네트워크 회선을 통해 인가되는 패킷, 플로우 및 트래픽에 보안공격을 위한 침입 또는 이상행동을 위한 데이터가 포함되어 있는가를 탐지하는 기술들을 지칭한다.

IP 네트워크상의 보안공격 탐지의 경우, 많은 AI/ML 모델 기반 지능화 연구들이 정상 (Normal, Benign 등으로 지칭) 또는 이상 (Abnormal, Attack, Intrusion, Malicious 등으로 지칭) 중 하나를 판단하는 True/False 탐지 방법론을 택하고 있다[10,38,57,64,66,71,94,120]. 해당 방법론은 구체적인 침입/이상의 내용을 탐지하지는 못하지만, 침입 여부만 판단하는 것만으로도 상당한 실용성이 있으며, AI/ML 모델 기반 탐지 시스템의 정확도를 쉽게 높일 수 있다는 장점이 있기 때문에 많은 연구들에서 채택하고 있는 접근방법이다. 또한 정상, 주목, 의심, 비정상과 같이 탐지 레이블을 4종으로 확장한 사례도 있으며[7], 적게는 5종에서 많게는 15종까지 공격 유형을 보다 세분화해 식별하는 형태로 발전하고 있다[46,51,63].

또한, DPI 회피 공격 탐지[3], DoS 및 DDoS 공격 탐지[43,47,49,60], BGP 이상동작 탐지[121], MEC 보안[46], IoT 보안[53], 무선 센서 네트워크 (Wireless Sensor Network) 상의 악의적 노드 탐지[79], 스마트 공장 보안[28] 및 사용자 기기 상의 개인정보유출 탐지[32] 등과 같이 세부적인 공격 또는 시나리오를 고려한 연구들도 다수 제안된 바 있다.

3.3 미래 네트워크 지능화 응용 사례

본 절에서는 상술한 AI/ML 모델 기반 네트워크 지능화 연구 중 미래 네트워크 인프라를 위한 핵심기술인 SDN (Software-Defined Network), NFV (Network Function Virtualization), NDN, MEC, IoT 등을 목적 시나리오에 고려한 연구사례들을 기술한다.

SDN의 경우, C4.5 및 Hoeffding Decision Tree를 활용한 플로우 전송률 및 지속시간 예측[11], GNN (Graph Neural Network)을 활용한 망의 지연시간, 불안정계수 및 패킷 손실률 예측[13], LSTM 기반의 플로우 규모 예측[76], Random Forest 기반의 SDN-Edge 클라우드 트래픽 인가량 예측[104], 강화학습 기반 데이터센터 라우팅 지능화[119] 등을 사례로 들 수 있다.

NFV의 경우, DAT (Delay-Aware Tree)를 활용한 VNF별 실행위치 지정[14], LSTM 기반의 SFC 별 부하량 예측[22], 5G-NFV-MEC 환경에서 MLP 기반의 SFC 실행위치 지정 및 VNF 스케일링[24], 자연어처리 기반 데이터센터 오류유형 식별[36] 등을 사례로 들 수 있다. 특히 5G-NFV 환경에서 강화학습을 활용하여 자원관리 MANO (Management and Orchestration) 동작을 자동화해 Zero-Touch Slicing 실현을 꾀하는 연구도 제안된 바 있다[92].

NDN의 경우, NDN-MEC 환경에서 강화학습과 Ensemble 학습을 조합한 캐싱 (Caching) 지능화[23], NDN-MEC 환경에서 CNN기반의 Content Chunk 별 요청량 예측[27], MLP 기반의 라우팅 지능화[31] 등을 사례로 들 수 있다.

MEC의 경우, 강화학습과 연합학습을 결합한 단말별 MEC 서버, 채널 및 VM 스케줄링 지능화[15], 5G-NFV-MEC 환경에서 MLP 기반의 SFC 실행 위치 지정 및 VNF 스케일링[24], NDN-MEC 환경에서 CNN기반의 Content Chunk별 요청량 예측[27], GBDT (Gradient Boosting Decision Tree)를 활용한 MEC 보안공격 탐지[46], Fog-Cloud-IoT 융합 환경을 위한

LCS (Learning Classifier System) 기반 워크로드 스케줄링[86], MEC 환경에서 Bayesian 최적화 모델을 활용한 Serverless Function의 실행비용 예측[87], QoS 보장을 위한 MEC 워크로드의 강화학습 기반 허용제어[88], MEC 기반 V2X 망에서 강화학습을 활용하여 차량별로 연결할 기지국과 워크로드의 오프로딩 여부 결정[89], 계층적 학습 (Hierarchical Learning)을 활용한 오프로딩 제어[93], MEC 환경에서 강화학습 기반의 지연시간 최소화를 위한 오프로딩 제어[95], Random Forest 기반의 SDN-Edge 클라우드 트래픽 인가량 예측[104] 등을 사례로 들 수 있다.

IoT의 경우, CART (Classification And Regression Tree)를 이용한 산업용 IoT 보안공격 탐지 및 방어[37], CNN과 RNN을 조합한 암호화된 IoT 트래픽 분류[41], 산업용 제어망을 위한 MODBUS 프로토콜 상에서 LSTM 및 Ensemble 학습을 조합한 보안공격 탐지[53], Decision Tree와 준지도학습 (Semi-supervised Learning)을 조합한 IoT 환경 침입탐지[64], Autoencoder 기반의 비지도학습을 활용한 IoT 보안공격 탐지[71], 무선 IoT 망에서의 GMM 기반 기회포착형 라우팅 (Opportunistic Routing)[84], Fog-Cloud-IoT 융합 환경을 위한 LCS 기반 워크로드 스케줄링[86] 등을 사례로 들 수 있다.

Ⅳ. 결 론

본 고에서는 2016년부터 2021년까지 최근 5년간 통신 및 네트워크 분야를 다루는 저명 학술지 및 학술대회에 발표된 112편의 논문을 선정하여 분석하고, 네트워크 지능화 연구 시 사용할 데이터들을 데이터 소스, 원시 데이터, 측정단위 및 특징값이라는 4가지 기준을 사용하여 분류하였다. 또한 네트워크 지능화의 응용 도메인 및 활용되는 AI/ML 모델들을 사례 중심으로 분석하였다.

분석한 결과에 따르면, 네트워크 지능화를 위한 데이터셋은 시험 목적으로 구성된 테스트베드 또는 시뮬레이션 환경 상에서 목적에 맞는 트래픽을 생성하고, Wireshark, TCPdump 등의 트래픽 수집 유틸리티를 이용해 트래픽을 수집, 가공하는 형태로 생성하는 경우가 많았다. 시험 목적의 테스트베드 또는 시뮬레이션 기반의 데이터셋은 실제 운영되는 네트워크 상에서 나타나는 트래픽의 패턴 또는 분포를 모두 반영할 수 없다는 한계점이 있다. 다시 말해, 해당 데이터셋을 통해 학습한 AI/ML 모델을 실제 운영되는 망의 지능화에 적용하는 경우, 훈련환경과 적용환경의 상이성으로 인해 지능화 성능의 저하가 발생한다.

실제 운용 중인 망에서 수집한 트래픽으로 생성한 데이터셋의 경우, 테스트베드 또는 시뮬레이션 환경에서 합성된 데이터셋에 비해, 현실성 면에서 장점이 있지만, 적절한 데이터 수집 소스의 확보, 개인정보 이슈와 관련된 법적, 제도적 어려움이 존재한다. 또한, 암호화의 사용과 대용량 특성에 의해 재처리 및 특징값 추출이 어렵고, 각 데이터 샘플에 대한 정확한 레이블을 지정하는 작업에도 상당한 비용을 필요로 한다. 특히, 보안응용에 대한 지능화의 경우, 실제 운용중인 네트워크에서 악성 트래픽을 수집하는 것이 쉽지 않기 때문에, 합성된 데이터셋을 많이 사용한다.

네트워크 지능화를 위한 AI/ML 모델 연구들은 이상상황감지, 어플리케이션 식별, 트래픽 수요예측, 경로 관리 및 제어, 자원 계획 등을 목표로 한 연구결과들이 많은 비중을 차지하고 있다. 특히, 근래에는 MEC 기술이 각광을 받게 되면서, 해당 환경을 고려한 오프로딩 및 스케줄링 연구사례도 다수 존재한다.

현재까지의 연구동향에 따르면 네트워크 지능화 연구들은 침입/이상 탐지 및 네트워크 트래픽 분류 등의 특정 응용분야에 많이 분포되어 있으나, 향후에는 네트워크 사업자가 관심을 갖는 주제들인 장애원인 분석 및 장애영향 수량화, 오류정정 등의 응용과 전달망을 위한 인프라 지능제어 분야까지 연구영역의 확대가 필요할 것으로 생각된다.

상기 언급한 한계점들을 해결하고 효과적인 네트워크 지능화를 위한 연구개발이 지속적으로 진행되기 위해서는 다음과 같은 이슈들이 선결되어야 한다. 첫째, 네트워크 관리 및 운용자들이 도입하고자 하는 AI/ML 모델에 적합한 데이터셋을 손쉽게 확보할 수 있는 방안이 마련되어야 한다. 데이터 수집을 위해 네트워크 관리 및 운용 인력들이 데이터의 소스 및 종류를 직접 지정할 수 있고, 장기간 혹은 주기적으로 데이터를 수집할 수 있는 개방형 API (Application Programming Interface)를 제공하는 것이 한 가지 방안이 될 수 있다. 둘째로, 다양한 소스에서 수집된 대규모 원시데이터를 통합 가공하고 학습에 필요한 특징 데이터를 추출해 AI/ML 모델 학습에 바로 사용할 수 있는 데이터셋의 생성을 지원할 수 있는 프레임워크 (Framework)가 필요하다. 특히 현재의 노동집약적인 학습 레이블 생성과정을 자동화 혹은 준자동화할 수 있는 다양한 기능 및 도구의 개발이 시급하다. 셋째, 네트워크 지능화를 위한 다방면의 AI/ML 모델 개발을 효율적으로 진행할 수 있도록 최적화된 학습 환경을 제공할 필요가 있다. 이를 위해서 기존의 AI/ML

모델 연구들을 기반으로 특정 응용에 대해 효과적인 학습 알고리즘과 모델 아키텍쳐 (Architecture) 등을 선정해서 사용자에게 필요한 참조 모델을 제안하고, 기계학습에 필요한 환경을 제공하는 것이 필요하다. 또한, 이미 학습된 모델을 네트워크 환경의 변화를 감지하여 재학습을 수행하는 절차를 제공하는 것도 유용한 서비스로 고려해볼 수 있다.

AI/ML 모델 기반의 지능화는 네트워크의 성능 및 운용 품질 향상에 상당한 효과를 가져올 수 있는 가능성이 있지만 서비스 가용성 및 품질저하의 위험성으로 인해 실제 운용되는 시스템에서는 쉽게 도입되지 못하고 있는 상황이다. 따라서, 네트워크 지능화를 위한 기술적 시도 시 필요로 하는 요소 기술들을 통합적으로 제공하는 라이브러리 (Library) 및 프레임워크의 출현이 기대되는 시점이다. 또한, 이미 획득한 데이터 셋 및 개발된 AI/ML 모델을 쉽게 공유하기 위한 데이터 규격, 프로토콜 및 플랫폼 (Platform)의 구현을 위한 다각적 노력들이 병행되어야 할 것이다.

References

[1] T. Kim, N. Ko, S. Yang, and S. M. Kim, "Trends in network and AI technologies," *Electron. and Telecommun. Trends*, vol. 35, no. 5, pp. 1-13, Oct. 2020.

[2] H. Park, S. Wee, and L. Park, "The application of machine learning and artificial intelligence for beyond 5G and 6G," in *Proc. Symp. KICS*, pp. 994-995, Yongpyong, Korea, Feb. 2021.

[3] S. Zhu, S. Li, Z. Wang, X. Chen, Z. Qian, S. V. Krishnamurthy, K. S. Chan, and A. Swami, "You do (not) belong here: Detecting DPI Evasion attacks with context learning," in *Proc. ACM CoNEXT 2020*, pp. 183-197, Barcelona, Spain, Nov. 2020.

[4] H. Yang, X. Li, W. Qiang, Y. Zhao, W. Zhang, and C. Tang, "A network traffic forecasting method based on SA optimized ARIMA-BP neural network," *Comput. Netw.*, vol. 193, 108102, Jul. 2021.

[5] P. Mulinka and P. Casas, "Adaptive network security through stream machine learning," in *Proc. ACM SIGCOMM 2018* (Demo), pp. 4-5, Budapest, Hungary, Aug. 2018.

[6] Z. Jin, Z. Liang, Y. Wang, and W. Meng, "Mobile network traffic pattern classification with incomplete a priori information," *Comput. Commun.*, vol. 166, pp. 262-270, Jan. 2021.

[7] Y. Zhong, W. Chen, Z. Wang, Y. Chen, K. Wang, Y. Li, X. Yin, X. Shi, J. Yang, and K. Li, "HELAD: A novel network anomaly detection model based on heterogeneous ensemble learning," *Comput. Netw.*, vol. 169, 107049, Mar. 2020.

[8] F. Xiao, L. Chen, H. Zhu, R. Hong, and R. Wang, "Anomaly-tolerant network traffic estimation via noise-immune temporal matrix completion model," *IEEE J. Sel. Commun.*, vol. 37, no. 6, pp. 1192-1204, Jun. 2019.

[9] Y. Sun, G. Li, and B. Ning, "Automatic rule updating based on machine learning in complex event processing," in *Proc. IEEE ICDCS 2020*, pp. 1338-1343, Singapore, Singapore, Nov. 2020.

[10] N. Moustafa and A. Jolfaei, "Autonomous detection of malicious events using machine learning models in drone networks," in *Proc. 2nd ACM MobiCom Wkshp. Drone Assisted Wireless Commun. for 5G and Beyond (DroneCom'20)*, pp. 61-66, London, United Kingdom, Sep. 2020.

[11] S.-C. Chao, K. C.-J. Lin, and M.-S. Chen, "Flow classification for software-defined data centers using stream mining," *IEEE Trans. Serv. Comput.*, vol. 12, no. 1, pp. 105-116, Jan. 2019.

[12] F. Tang, B. Mao, Z. Md. Fadlullah, J. Liu, and N. Kato, "ST-DeLTA: A novel spatial-temporal value network aided deep learning based intelligent network traffic control system," *IEEE Trans. Sustainable Comput.*, vol. 5, no. 4, pp. 568-580, Oct. 2020.

[13] K. Rusek, J. Suárez-Varela, P. Almasan, P. Barlet-Ros, and A. Cabellos-Aparicio, "RouteNet: leveraging graph neural networks for network modeling and optimization in SDN," *IEEE J. Sel. Commun.*, vol. 38, no. 10, pp. 2260-2270, Oct. 2020.

[14] D. M. Manias, M. Jammal, H. Hawilo, A. Shami, P. Heidari, A. Larabi, and R. Brunner, "Machine learning for performance-aware virtual network function placement," in *Proc. IEEE GLOBECOM 2019*, pp. 1-6, Waikoloa, HI, USA, Dec. 2019.

[15] N. Shan, X. Cui, and Z. Gao, ""DRL+ FL": An intelligent resource allocation model based on deep reinforcement learning for mobile edge computing," *Comput. Commun.*, vol. 160, pp. 14-24, Jul. 2020.

[16] S. Kardani-Moghaddam, R. Buyya, and K. Ramamohanarao, "ADRL: A hybrid anomaly-aware deep reinforcement learning-based resource scaling in clouds," *IEEE Trans. Parallel Dist. Syst.*, vol. 32, no. 3, pp. 514-526, Mar. 2021.

[17] X. Zhang, C. Wu. Z. Li, and F. C. M. Lau, "Proactive VNF provisioning with multitime-scale cloud resources: Fusing online learning and online optimization," in *Proc. IEEE INFOCOM 2017*, pp. 1-9, Atlanta, GA, USA, May 2017.

[18] A. Erradi, W. Iqbal, A. Mahmood, and A. Bouguettaya, "Web application resource requirements estimation based on the workload latent features," *IEEE Trans. Serv. Comput.*, vol. 14, no. 6, pp. 1638-1649, 2019.

[19] D. Chen, X. Zhang, L. Wang, and Z. Han, "Prediction of cloud resources demand based on fuzzy deep neural network," in *Proc. IEEE GLOBECOM 2018*, pp. 1-5, Abu Dhabi, United Arab Emirates, Dec. 2018.

[20] Q. Zhou, K. Wang, P. Li, D. Zeng, S. Guo, B. Ye, and M. Guo, "Fast coflow scheduling via traffic compression and stage pipelining in datacenter networks," *IEEE Trans. Comput.*, vol. 68, no. 12, pp. 1755-1771, Dec. 2019.

[21] X. Zeng, S. Garg, M. Barika, S. Bista, D. Puthal, A. Y. Zomaya, and R. Ranjan, "Detection of SLA violation for big data analytics applications in cloud," *IEEE Trans. Comput.*, vol. 70, no. 5, pp. 746-758, May 2021.

[22] V. Eramo, F. G. Lavacca, T. Catena, and P. J. P. Salazar, "Application of a long short term memory neural predictor with asymmetric loss function for the resource allocation in NFV network architectures," *Comput. Netw.*, vol. 193, 108104, Jul. 2021.

[23] T. Zong, C. Li, Y. Lei, G. Li, H. Cao, and Y. Liu, "Cocktail edge caching: Ride dynamic trends of content popularity with ensemble learning," in *Proc. IEEE INFOCOM 2021*, pp. 1-10, Vancouver, BC, Canada, May 2021.

[24] T. Subramanya, D. Harutyunyan, and R. Riggio, "Machine learning-driven service function chain placement and scaling in MEC-enabled 5G networks," *Comput. Netw.*, vol. 166, 106980, Jan. 2020.

[25] J. Lee, P. Sun, and Y. Hu, "Traffic modeling and optimization in datacenters with graph neural network," *Comput. Netw.*, vol. 181, 107528, Nov. 2020.

[26] N. Marie-Magdelaine and T. Ahmed, "Proactive autoscaling for cloud-native applications using machine learning," in *Proc. IEEE GLOBECOM 2020*, pp. 1-7, Taipei, Taiwan, Dec. 2020.

[27] K. H. T. Chiu, J. Zhang, and B. Bensaou, "Cache management in information-centric networks using convolutional neural network," in *Proc. IEEE GLOBECOM 2020*, pp. 1-6, Taipei, Taiwan, Dec. 2020.

[28] A. Elsaeidy, K. S. Munasinghe, D. Sharma, and A. Jamalipour, "Intrusion detection in smart cities using restricted Boltzmann machines," *J. Netw. Comput. Appl.*, vol. 135, pp. 76-83, Jun. 2019.

[29] M. Jiang, Y. Wang, G. Gou, W. Cai, G. Xiong, and J. Shi, "PST: A more practical adversarial learning-based defense against website fingerprinting," in *Proc. IEEE GLOBECOM 2020*, pp. 1-6, Taipei, Taiwan, Dec. 2020.

[30] M. J. Khokhar, N. A. Saber, T. Spetebroot, and C. Barakat, "An intelligent sampling framework for controlled experimentation and QoE modeling," *Comput. Netw.*, vol. 147, pp. 246-261, Dec. 2018.

[31] L. Mekinda and L. Muscariello, "Supervised

machine learning-based routing for named data networking," in *Proc. IEEE GLOBECOM 2016*, pp. 1-6, Washington, DC, USA, Dec. 2016.

[32] J. Ren, A. Rao, M. Lindorfer, A. Legout, and D. Choffnes, "ReCon: Revealing and controlling PII leaks in mobile network traffic," in *Proc. ACM MobiSys 2016*, pp. 361-374, Singapore, Singapore, Jun. 2016.

[33] J. Ren, L. Gao, H. Wang, and Z. Wang, "Optimise web browsing on heterogeneous mobile platforms: A machine learning based approach," in *Proc. IEEE INFOCOM 2017*, pp. 1-9, Atlanta, GA, USA, May 2017.

[34] K. Liang, G. Gou, C. Kang, C. Liu, M. Yang, and Y. Guo, "A multi-view deep learning model for encrypted website service classification," in *Proc. IEEE GLOBECOM 2019*, pp. 1-6, Waikoloa, HI, USA, Dec. 2019.

[35] J. Zhang, F. Li, H. Wu, and F. Ye, "Autonomous model update scheme for deep learning based network traffic classifiers," in *Proc. IEEE GLOBECOM 2019*, pp. 1-6, Waikoloa, HI, USA, Dec. 2019.

[36] S. Satpathi, S. Deb, R. Srikant, and H. Yan, "Learning latent events from network message logs," *IEEE/ACM Trans. Netw.*, vol. 27, no. 4, pp. 1728-1741, Aug. 2019.

[37] M. S. Haghighi, F. Farivar, and A. Jolfaei, "A machine learning-based approach to build zero false-positive IPSs for industrial IoT and CPS with a case study on power grids security," *IEEE Trans. Ind. Appl.*, early access, Jul. 2020.

[38] Y. Yuan, S. Srikant Adhatarao, M. Lin, Y. Yuan, Z. Liu, and X. Fu, "ADA: Adaptive deep log anomaly detector," in *Proc. IEEE INFOCOM 2020*, pp. 2449-2458, Toronto, ON, Canada, Jul. 2020.

[39] C. Shelbourne, L. Linguaglossa, A. Lipani, T. Zhang, and F. Geyer, "On the learnability of software router performance via CPU measurements," in *Proc. ACM CoNEXT 2019*, pp. 23-25, Orlando, Florida, USA, Dec. 2019.

[40] M. Nasr, A. Bahramali, and A. Houmansadr, "Defeating DNN-based traffic analysis systems in real-time with blind adversarial perturbations," in *Proc. USENIX Security 2021*, pp. 1-18, Aug. 2021.

[41] K. Lin, X. Xu, and H. Gao, "TSCRNN: A novel classification scheme of encrypted traffic based on flow spatiotemporal features for efficient management of IIoT," *Comput. Netw.*, vol. 190, 107974, May 2021.

[42] S. Chowdhury, B. Liang, and A. Tizghadam, "Explaining class-of-service oriented network traffic classification with superfeatures," in *Proc. 3rd ACM CoNEXT Wkshp. on Big DAta, Mach. Learn. and Artificial Intell. for Data Commun. Netw. (Big-DAMA'19)*, pp. 23-25, Orlando, Florida, USA, Dec. 2019.

[43] J. P. A. Maranhão, J. P. C. L. da Costa, E. Javidi, C. A. B. de Andrade, and R. T. de Sousa Jr., "Tensor based framework for distributed denial of service attack detection," *J. Netw. Comput. Appl.*, vol. 174, 102894, Jan. 2021.

[44] S. Gamage and J. Samarabandu, "Deep learning methods in network intrusion detection: A survey and an objective comparison," *J. Netw. Comput. Appl.*, vol. 169, 102767, Nov. 2020.

[45] L. Yu, J. Dong, L. Chen, M. Li, B. Xu, Z. Li, L. Qiao, L. Liu, B. Zhao, and C. Zhang, "PBCNN: Packet bytes-based convolutional neural network for network intrusion detection," *Comput. Netw.*, vol. 194, 108117, Jul. 2021.

[46] J.-F. Cui, H. Xia, R. Zhang, B.-X. Hu, and X.-G. Cheng, "Optimization scheme for intrusion detection scheme GBDT in edge computing center," *Comput. Commun.*, vol. 168, pp. 136-145, Feb. 2021.

[47] S. D. Çakmakçı, T. Kemmerich, T. Ahmed, and N. Baykal, "Online DDoS attack detection using Mahalanobis distance and kernel-based learning algorithm," *J. Netw. Comput. Appl.*, vol. 168, 102756, Oct. 2020.

[48] Z. Yao, J. Ge, Y. Wu, X. Lin, R. He, and Y. Ma, "Encrypted traffic classification based on

Gaussian mixture models and Hidden Markov models," *J. Netw. Comput. Appl.*, vol. 166, 102711, Sep. 2020.

[49] Z. Shi, J. Li, and C. Wu, "DeepDDoS: Online DDoS attack detection," in *Proc. IEEE GLOBECOM 2019*, pp. 1-6, Waikoloa, HI, USA, Dec. 2019.

[50] J. Cheng, R. He, E. Yuepeng, Y. Wu, J. You, and T. Li, "Real-time encrypted traffic classification via lightweight neural networks," in *Proc. IEEE GLOBECOM 2020*, pp. 1-6, Taipei, Taiwan, Dec. 2020.

[51] H. Zhang, L. Huang, C. Q. Wu, and Z. Li, "An effective convolutional neural network based on SMOTE and Gaussian mixture model for intrusion detection in imbalanced dataset," *Comput. Netw.*, vol. 177, 107315, Aug. 2020.

[52] H. Yan, H. Li, M. Xiao, R. Dai, X. Zheng, X. Zhao, and F. Li, "PGSM-DPI: Precisely guided signature matching of deep packet inspection for traffic analysis," in *Proc. IEEE GLOBECOM 2019*, pp. 1-6, Waikoloa, HI, USA, Dec. 2019.

[53] M. Saharkhizan, A. Azmoodeh, A. Dehghantanha, K.-K. R. Choo, and R. M. Parizi, "An ensemble of deep recurrent neural networks for detecting IoT cyber attacks using network traffic," *IEEE IoT J.*, vol. 7, no. 9, pp. 8852-8859, Sep. 2020.

[54] J. Lee, S. Lee, J. Lee, S. D. Sathyanarayana, H. Lim, J. Lee, X. Zhu, S. Ramakrishnan, and D. Grunwald, "PERCEIVE: Deep learning-based cellular uplink prediction using real-time scheduling patterns," in *Proc. ACM MobiSys 2020*, pp. 377-390, Toronto, ON, Canada, Jun. 2020.

[55] C. Dong, C. Zhang, Z. Lu, B. Liu, and B. Jiang, "CETAnalytics: Comprehensive effective traffic information analytics for encrypted traffic classification," *Comput. Netw.*, vol. 176, 107258, Jul. 2020.

[56] J. Zhang, F. Li, F. Ye, and H. Wu, "Autonomous unknown-application filtering and labeling for DL-based traffic classifier update," in *Proc. IEEE INFOCOM 2020*, pp. 397-405, Toronto, ON, Canada, Jul. 2020.

[57] M. Injadat, F. Salo, A. B. Nassif, A. Essex, and A. Shami, "Bayesian optimization with machine learning algorithms towards anomaly detection," in *Proc. IEEE GLOBECOM 2018*, pp. 1-6, Abu Dhabi, United Arab Emirates, Dec. 2018.

[58] L. Mei, R. Hu, H. Cao, Y. Liu, Z. Han, F. Li, and J. Li, "Realtime mobile bandwidth prediction using LSTM neural network and Bayesian fusion," *Comput. Netw.*, vol. 182, 107515, Dec. 2020.

[59] D. Li, W. Li, X. Wang, C.-T. Nguyen, and S. Lu, "App trajectory recognition over encrypted internet traffic based on deep neural network," *Comput. Netw.*, vol. 179, 107372, Oct. 2020.

[60] R. K. Deka, D. K. Bhattacharyya, and J. K. Kalita, "Active learning to detect DDoS attack using ranked features," *Comput. Commun.*, vol. 145, pp. 203-222, Sep. 2019.

[61] T. Iwai and A. Nakao, "Progressive slicing for application identification in application-specific network slicing," in *Proc. IEEE GLOBECOM 2020*, pp. 1-6, Taipei, Taiwan, Dec. 2020.

[62] H. Jin, M. Kang, G. Yang, and C. Yoo, "CLEO: Machine learning for ECMP," in *Proc. ACM CoNEXT 2019*, pp. 1-3, Orlando, Florida, USA, Dec. 2019.

[63] R. R. Karn, P. Kudva, and I. A. M. Elfadel, "Dynamic autoselection and autotuning of machine learning models for cloud network analytics," *IEEE Trans. Parallel Dist. Syst.*, vol. 30, no. 5, pp. 1052-1064, May 2019.

[64] W. Li, W. Meng, and M. H. Au, "Enhancing collaborative intrusion detection via disagreement-based semi-supervised learning in IoT environments," *J. Netw. Comput. Appl.*, vol. 161, 102632, Jul. 2020.

[65] Y. Li, B. Liang, and A. Tizghadam, "Robust online learning against malicious manipulation with application to network flow classification," in *Proc. IEEE INFOCOM 2021*, pp. 1-10, Vancouver, BC, Canada, May

2021.

[66] Y. Lin, J. Wang, Y. Tu, L. Chen, and Z. Dou, "Time-related network intrusion detection model: A deep learning method," in *Proc. IEEE GLOBECOM 2019*, pp. 1-6, Waikoloa, HI, USA, Dec. 2019.

[67] A. Majidi, N. Jahanbakhsh, X. Gao, J. Zheng, and G. Chen, "DC-ECN: A machine-learning based dynamic threshold control scheme for ECN marking in DCN," *Comput. Commun.*, vol. 150, pp. 334-345, Jan. 2020.

[68] M. Shen, J. Zhang, S. Chen, Y. Liu, and L. Zhu, "Machine learning classification on traffic of secondary encryption," in *Proc. IEEE GLOBECOM 2019*, pp. 1-6, Waikoloa, HI, USA, Dec. 2019.

[69] K. A. Simpson, R. Cziva, and D. P. Pezaros, "Seiðr: Dataplane assisted flow classification using ML," in *Proc. IEEE GLOBECOM 2020*, pp. 1-6, Taipei, Taiwan, Dec. 2020.

[70] W. Sun, Z. Wang, and G. Zhang, "A QoS-guaranteed intelligent routing mechanism in software-defined networks," *Comput. Netw.*, vol. 185, 107709, Feb. 2021.

[71] R. Bhatia, S. Benno, J. Esteban, T. V. Lakshman, and J. Grogan, "Unsupervised machine learning for network-centric anomaly detection in IoT," in *Proc. 3rd ACM CoNEXT Wkshp. Big DAta, Mach. Learn. and Artificial Intell. for Data Commun. Netw. (Big-DAMA'19)*, pp. 42-48, Orlando, Florida, USA, Dec. 2019.

[72] A. K. Das, P. H. Pathak, C.-N. Chuah, and P. Mohapatra, "Privacy-aware contextual localization using network traffic analysis," *Comput. Netw.*, vol. 118, pp. 24-36, May 2017.

[73] S. Emara, B. Li, and Y. Chen, "Eagle: Refining congestion control by learning from the experts," in *Proc. IEEE INFOCOM 2020*, pp. 676-685, Toronto, ON, Canada, Jul. 2020.

[74] Q. He, A. Moayyedi, G. Dán, G. P. Koudouridis, and P. Tengkvist, "A Meta-learning scheme for adaptive short-term network traffic prediction," *IEEE J. Sel. Commun.*, vol. 38, no. 10, pp. 2271-2283, Oct. 2020.

[75] S. K. Khangura and S. Akın, "Online available bandwidth estimation using multiclass supervised learning techniques," *Comput. Commun.*, vol. 170, pp. 177-189, Mar. 2021.

[76] A. Lazaris and V. K. Prasanna, "DeepFlow: A deep learning framework for software-defined measurement," in *Proc. 2nd Wkshp. CAN'17*, pp. 43-48, Seoul/Incheon, South Korea, Dec. 2017.

[77] A. Badia-Sampera, J. Suárez-Varela, P. Almasan, K. Rusek, P. Barlet-Ros, and A. Cabellos-Aparicio, "Towards more realistic network models based on Graph Neural Networks," in *Proc. ACM CoNEXT 2019*, pp. 14-16, Orlando, Florida, USA, Dec. 2019.

[78] O. Brun, L. Wang, and E. Gelenbe, "Big data for autonomic intercontinental overlays," *IEEE J. Sel. Commun.*, vol. 34, no. 3, pp. 575-583, Mar. 2016.

[79] B. Gao, T. Maekawa, D. Amagata, and T. Hara, "Environment-adaptive malicious node detection in MANETs with ensemble learning," in *Proc. IEEE ICDCS 2018*, pp. 556-566, Vienna, Austria, Jul. 2018.

[80] Z. M. Fadlullah, B. Mao, F. Tang, and N. Kato, "Value iteration architecture based deep learning for intelligent routing exploiting heterogeneous computing platforms," *IEEE Trans. Comput.*, vol. 68, no. 6, pp. 939-950, Jun. 2019.

[81] J. Liu, Q. Wang, C. T. He, K. Jaffrès-Runser, Y. Xu, Z. Li, and Y. J. Xu, "QMR: Q-learning based Multi-objective optimization Routing protocol for flying ad hoc networks," *Comput. Commun.*, vol. 150, pp. 304-316, Jan. 2020.

[82] B. Mao, Z. Md. Fadlullah, F. Tang, N. Kato, O. Akashi, T. Inoue, and K. Mizutani, "Routing or computing? The paradigm shift towards intelligent computer network packet transmission based on deep learning," *IEEE Trans. Comput.*, vol. 66, no. 11, pp. 1946-

1960, Nov. 2017.

[83] B. Mao, Z. Md. Fadlullah, F. Tang, N. Kato, O. Akashi, T. Inoue, and K. Mizutani, "A tensor based deep learning technique for intelligent packet routing," in *Proc. IEEE GLOBECOM 2017*, pp. 1-6, Singapore, Singapore, Dec. 2017.

[84] V. Vashishth, A. Chhabra, and D. K. Sharma, "GMMR: A Gaussian mixture model based unsupervised machine learning approach for optimal routing in opportunistic IoT networks," *Comput. Commun.*, vol. 134, pp. 138-148, Jan. 2019.

[85] Y. Tian, Z. Wang, X. Yin, X. Shi, Y. Guo, H. Geng, and J. Yang, "Traffic engineering in partially deployed segment routing over IPv6 network with deep reinforcement learning," *IEEE/ACM Trans. Netw.*, vol. 28, no. 4, pp. 1573-1586, Aug. 2020.

[86] M. Abbasi, M. Yaghoobikia, M. Rafiee, A. Jolfaei, and M. R. Khosravi, "Efficient resource management and workload allocation in fog–cloud computing paradigm in IoT using learning classifier systems," *Comput. Commun.*, vol. 153, pp. 217-228, Mar. 2020.

[87] N. Akhtar, A. Raza, V. Ishakian, and I. Matta, "COSE: Configuring serverless functions using statistical learning," in *Proc. IEEE INFOCOM 2020*, pp. 129-138, Toronto, ON, Canada, Jul. 2020.

[88] F. Carpio, A. Jukan, R. Sosa, and A. J. Ferrer, "Engineering a QoS provider mechanism for edge computing with deep reinforcement learning," in *Proc. IEEE GLOBECOM 2019*, pp. 1-6, Waikoloa, HI, USA, Dec. 2019.

[89] M. Chen, T. Wang, K. Ota, M. Dong, M. Zhao, and A. Liu, "Intelligent resource allocation management for vehicles network: An A3C learning approach," *Comput. Commun.*, vol. 151, pp. 485-494, Feb. 2020.

[90] W. Guan, H. Zhang, and V. C. M. Leung, "Slice reconfiguration based on demand prediction with dueling deep reinforcement learning," in *Proc. IEEE GLOBECOM 2020*, pp. 1-6, Taipei, Taiwan, Dec. 2020.

[91] Y. Li, Z. Han, Q. Zhang, Z. Li, and H. Tan, "Automating cloud deployment for deep learning inference of real-time online services," in *Proc. IEEE INFOCOM 2020*, pp. 1668-1677, Toronto, ON, Canada, Jul. 2020.

[92] F. Rezazadeh, H. Chergui, L. Alonso, and C. Verikoukis, "Continuous multi-objective zero-touch network slicing via twin delayed DDPG and OpenAI Gym," in *Proc. IEEE GLOBECOM 2020*, pp. 1-6, Taipei, Taiwan, Dec. 2020.

[93] Y.-C. Wu, C. Lin, and T. Q. S. Quek, "A robust hierarchical learning approach for dynamic MEC networks," in *Proc. IEEE GLOBECOM 2020*, pp. 1-6, Taipei, Taiwan, Dec. 2020.

[94] L. Xu, Z. Luan, C. Fung, D. Ye, and D. Qian, "Anomaly detection models based on context-aware sequential long short-term memory learning," in *Proc. IEEE GLOBECOM 2019*, pp. 1-6, Waikoloa, HI, USA, Dec. 2019.

[95] B. Yılmaz, A. Ortiz, and A. Klein, "Delay minimization for edge computing with dynamic server computing capacity: A learning approach," in *Proc. IEEE GLOBECOM 2020*, pp. 1-6, Taipei, Taiwan, Dec. 2020.

[96] A. Bakshi, Y. Mao, K. Srinivasan, and S. Parthasarathy, "Fast and efficient cross band channel prediction using machine learning," in *Proc. ACM MobiCom 2019*, pp. 1-16, Los Cabos, Mexico, Oct. 2019.

[97] D. Bega, M. Gramaglia, M. Fiore, A. Banchs, and X. Costa-Perez, "DeepCog: Cognitive network management in sliced 5G networks with deep learning," in *Proc. IEEE INFOCOM 2019*, pp. 280-288, Paris, France, Apr. 2019.

[98] D. Bega, M. Gramaglia, M. Fiore, A. Banchs, and X. Costa-Pérez, "DeepCog: Optimizing resource provisioning in network slicing with AI-based capacity forecasting," *IEEE J. Sel. Commun.*, vol. 38, no. 2, pp. 361-376, Feb. 2020.

[99] T. Huynh-The, V.-S. Doan, C.-H. Hua, Q.-V. Pham, and D.-S. Kim, "Chain-Net: Learning

deep model for modulation classification under synthetic channel impairment," in *Proc. IEEE GLOBECOM 2020*, pp. 1-6, Taipei, Taiwan, Dec. 2020.

[100] R. Karmakar, S. Chattopadhyay, and S. Chakraborty, "SmartLA: Reinforcement learning-based link adaptation for high throughput wireless access networks," *Comput. Commun.*, vol. 110, pp. 1-25, Sep. 2017.

[101] X. Lyu, W. Feng, and N. Ge, "Deep neural network-based symbol detection for highly dynamic channels," in *Proc. IEEE GLOBECOM 2020*, pp. 1-6, Taipei, Taiwan, Dec. 2020.

[102] C. Saha and H. S. Dhillon, "Machine learning meets stochastic geometry: Determinantal subset selection for wireless networks," in *Proc. IEEE GLOBECOM 2019*, pp. 1-6, Waikoloa, HI, USA, Dec. 2019.

[103] T. Senevirathna, B. Thennakoon, T. Sankalpa, C. Seneviratne, S. Ali, and N. Rajatheva, "Event-driven source traffic prediction in machine-type communications using LSTM networks," in *Proc. IEEE GLOBECOM 2020*, pp. 1-6, Taipei, Taiwan, Dec. 2020.

[104] R. Shinkuma, Y. Yamada, T. Sato, and E. Oki, "Flow control in SDN-Edge-Cloud cooperation system with machine learning," in *Proc. IEEE ICDCS 2020 (NetAI Wkshp.)*, pp. 1304-1309, Singapore, Singapore, Nov. 2020.

[105] C. Sun and C. Yang, "Unsupervised deep learning for ultra-reliable and low-latency communications," in *Proc. IEEE GLOBECOM 2019*, pp. 1-6, Waikoloa, HI, USA, Dec. 2019.

[106] L. Xu, T. Quan, J. Wang, T. A. Gulliver, and K. N. Le, "GR and BP neural network-based performance prediction of dual-antenna mobile communication networks," *Comput. Netw.*, vol. 172, 107172, May 2020.

[107] C. Zhang and P. Patras, "Long-term mobile traffic forecasting using deep spatio-temporal neural networks," in *Proc. ACM MobiHoc 2018*, pp. 231-240, Los Angeles, CA, USA, Jun. 2018.

[108] C. Zhang, H. Zhang, J. Qiao, D. Yuan, and M. Zhang, "Deep transfer learning for intelligent cellular traffic prediction based on cross-domain big data," *IEEE J. Sel. Commun.*, vol. 37, no. 6, pp. 1389-1401, Jun. 2019.

[109] X. Zhang and M. Vaezi, "A DNN-based multi-objective precoding for Gaussian MIMO networks," in *Proc. IEEE GLOBECOM 2020*, pp. 1-6, Taipei, Taiwan, Dec. 2020.

[110] H. Zhou and M. L. Honig, "Deep learning for selecting precoder ranks," in *Proc. IEEE GLOBECOM 2019*, pp. 1-6, Waikoloa, HI, USA, Dec. 2019.

[111] Z. Zhou, J. Yu, Z. Yang, and W. Gong, "MobiFi: Fast deep-learning based localization using mobile WiFi," in *Proc. IEEE GLOBECOM 2020*, pp. 1-6, Taipei, Taiwan, Dec. 2020.

[112] N. Moustafa, *The UNSW-NB15 Dataset*, Retrieved Nov. 28, 2021, from https://research.unsw.edu.au/projects/unsw-nb15-dataset

[113] K. Cho, *MAWI Working Group Traffic Archive*, Retrieved Nov. 28, 2021, from http://mawi.wide.ad.jp/mawi/

[114] R. Fontugne, P. Borgnat, P. Abry, and K. Fukuda, "MAWILab: Combining diverse anomaly detectors for automated anomaly labeling and performance benchmarking," in *Proc. ACM CoNEXT 2010*, pp. 1-12, Philadelphia, USA, Nov. 2010.

[115] S. Balon, J. Lepropre, O. Delcourt, F. Skivee, and G. Leduc, "Traffic engineering an operational network with the TOTEM toolbox," *IEEE Trans. Netw. Serv. Mgmt.*, vol. 4, no. 1, pp. 51-61, Jun. 2007.

[116] S. Balon, J. Lepropre, O. Delcourt, F. Skivee, and G. Leduc, *TOTEM Project: TOolbox for Traffic Engineering Methods*, Retrieved Nov. 28, 2021, from http://totem.run.montefiore.ulg.ac.be/

[117] S. Balon, J. Lepropre, O. Delcourt, F. Skivee, and G. Leduc, *TOTEM Project: TOolbox for Traffic Engineering Methods – Additional Tools and Data*, Retrieved Nov. 28, 2021, from http://totem.run.montefiore.ulg.ac.be/data

tools.html
[118] S. Uhlig, B. Quoitin, J. Lepropre, and S. Balon, “Providing public intradomain traffic matrices to the research community,” *ACM SIGCOMM Comput. Commun. Rev.*, vol. 36, no. 1, pp. 83-86, Jan. 2006.
[119] W.-X. Liu, J. Cai, Q. C. Chen, and Y. Wang, “DRL-R: Deep reinforcement learning approach for intelligent routing in software-defined data-center networks,” *J. Netw. Comput. Appl.*, vol. 177, 102865, Mar. 2021.
[120] E. Viegas, A. Santin, N. Neves, A. Bessani, and V. Abreu, “A resilient stream learning intrusion detection mechanism for real-time analysis of network traffic,” in *Proc. IEEE GLOBECOM 2017*, pp. 1-6, Singapore, Singapore, Dec. 2017.
[121] O. R. Sanchez, S. Ferlin, C. Pelsser, and R. Bush, “Comparing machine learning algorithms for BGP anomaly detection using graph features,” in *Proc. 3rd ACM CoNEXT Wkshp. on Big DAta, Mach. Learn. and Artificial Intell. for Data Commun. Netw. (Big-DAMA’19)*, pp. 35-41, Orlando, Florida, USA, Dec. 2019.

이 주 영 (Jooyoung Lee)

1997년 2월 : 덕성여자대학교 전산학과 학사
1999년 8월 : 연세대학교 컴퓨터과학과 석사
2019년 2월 : 충남대학교 컴퓨터공학과 박사
2000년 3월~현재 : 한국전자통신연구원 책임연구원
<관심분야> 컴퓨터 네트워크, 정보보호, AI/ML
[ORCID:0000-0003-1112-5901]

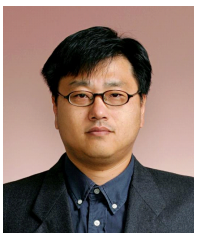
신 승 재 (Seungjae Shin)

2007년 2월 : 충남대학교 전기정보통신공학부 학사
2009년 2월 : 한국과학기술원 전자전산학과 석사
2016년 8월 : 한국과학기술원 전산학부 박사
2016년 10월~현재 : 한국전자통신연구원 선임연구원
<관심분야> 컴퓨터 네트워크, 클라우드 컴퓨팅, 강화학습
[ORCID:0000-0001-8806-0101]

윤 승 현 (Seunghyun Yoon)

1991년 2월 : 성균관대학교 산업공학과 학사
1993년 2월 : 성균관대학교 산업공학과 석사
1997년 2월 : 성균관대학교 산업공학과 박사
1997년 11월~현재 : 한국전자통신연구원 책임연구원
<관심분야> 네트워크, AI, 클라우드, 최적화

김 태 연 (Taeyeon Kim)



1990년 : 중앙대학교 전자계산학과 학사
1992년 : 중앙대학교 전자계산학과 석사
2008년 : 충북대학교 컴퓨터과학과 박사
2019년~현재 : ETRI 지능네트워크연구실 실장
<관심분야> 6G, Network for/by AI