AI 기반 SDN 구현 연구 동향 분석

문수빈*, 남대현, 김응수, 조효준, 전형준, 이재욱
국립부경대학교 정보통신공학전공
(subin23*,namdh01,oloae,dhkdlfemqh,jun04292569)@pukyong.ac.kr, jlee0315@pknu.ac.kr

Trend Analysis of AI-based SDN Implementation Research

Subin Moon*, Daehyeon Nam, Eungsu Kim, Hyojun Jo, Hyeongjun Jeon, Jaewook Lee
Department of Information and Communications Engineering, Pukyong National University

요 약

본 논문은 AI 기반 SDN 연구 중 구현이나 실험을 포함한 사례를 중심으로 2020년부터 2025년까지의 동향을 정리하였다. 총 8편의 연구를 선별해 트래픽 분류(서비스 식별), 보안(DDoS 등 이상 트래픽 탐지), 라우팅 및 트래픽 엔지니어링(TE)으로 구분하였으며, 각 연구의 실험 환경, 입력 데이터, AI 기법, 출력/제어를 표로 정리하였다. 트래픽 분류/공격 탐지 분야는 지도학습/딥러닝 기반에 집중되어 있으며, 라우팅/TE 분야는 강화학습 또는 상태 기반 예측형 ML을 통해 경로 선택과 플로우를 갱신으로 연결되는 경향을 보였다. 또한 일부 연구는 데이터, 코드, 실험 절차를 함께 제공하여 재현성을 지원한다. 본 논문은 SDN 애플리케이션 개발 관점에서 데이터 수집 지점, AI 적용 위치, 그리고 성능 검증 방법의 연구 동향을 파악하는 데 목적이 있다.

Ⅰ. 서 론

SDN(Software Defined Networking)은 네트워크를 제어 평면과 데이터 평면으로 분리하여 중앙의 컨트롤러가 정책을 플로우 규칙으로 변환 및 배포하는 구조이다. 이러한 논리적 중앙 집중식 구조는 네트워크 전역의 상태 정보를 실시간으로 수집하고 최적화된 정책을 직접 제어할 수 있어 AI 기술 적용에 용이하다. 최근에는 단순 개념 제시를 넘어, 테스트베드에서 컨트롤러와 OpenFlow 스위치를 연동해 실효성을 검증하는 연구가 증가하고 있다.

본 논문은 AI 기반 SDN 연구 중 데이터 수집, 모델 학습, 컨트롤러 적용, 성능 평가로 이어져 재현 가능성을 높인 최근 연구들을 정리하고, 공통 트렌드와 남은 과제를 살펴본다.

Ⅱ. 본론

A. 문헌 선정 및 분류 기준

참고문헌은 최신 동향 파악을 위해 2020년 이후 연구로 한정하였다. 구현 관점 분석을 위해 AI 모델 출력이 SDN 운영 의사결정 또는 제어 정책에 활용되고 테스트베드 실험을 수행한 사례를 중심으로 선별하되, 제어 연동을 가정한 성능 검증 중심 연구는 비교 대상으로 일부 포함하였다. 선별 문헌은 트래픽 분류, 보안, 라우팅 및 트래픽 엔지니어링 세 분야로 분류하였고, 실험 환경, 입력 특징, AI 기법, 출력 및 제어를 표 1 [1-8]에 정리하였다.

B. 트래픽 분류(서비스 식별)

트래픽 분류는 SDN에서 관측되는 플로우 특성을 바탕으로 애플리케이션 유형을 식별해 네트워크 관리 정책의 근거로 활용한다.

[1]은 Packet_in에서 목적지 IP·포트와 1초 주기 통계의 바이트·패킷 카운트를 입력으로, Ryu 컨트롤러 내 MLP·CNN·SAE로 플로우 단위 7개 라벨을 분류한다. ISCX로 학습하고 TCPreplay 재생 트래픽으로 온라인 에뮬 평가를 수행해 정확도·정밀도·재현율·F1을 보고했으며, 처리 한계와 SkypeAudio - SkypeVideo 오분류로 성능 저하가 나타나 실제 트래픽 검증과 모델·파라미터 최적화가 과제로 남는다.

Ref	연도	과제	구현 환경	입력 데이터(특징)	AI 기법	출력/제어(액션)
[1]	2020	트래픽 분류	TCPreplay, Ryu, OVS	Packet_in IP/포트 + 1초 플로우 통계(바이트/패킷)	MLP, CNN, SAE	서비스 라벨 출력
[2]	2021	라우팅/TE	MLMR 컨트롤러, 휴리스틱 라벨 생성, DNN	트래픽 매트릭스 기반 상태 벡터	DNN 회귀	분배비율 예측 후 룰 설치
[3]	2023	라우팅	Mininet, Ryu, OpenFlow, iperf	링크 상태(가용대역폭 중심, 손실률 포함)	Q-learning	widest-path 선택 후 룰 설치
[4]	2023	보안(DDoS)	Mininet, Ryu, TCP SYN flood	30초 주기 플로우 헤더·통계	SVM, NB, MLP	공격 탐지 후 차단 룰 설치
[5]	2024	트래픽/공격 분류	ISCX VPN - nonVPN, InSDN	플로우 통계 5종(전송률·부하 등)	GRU, BiGRU, LSTM, BiLSTM	분류 결과 보고(제어는 가정)
[6]	2024	보안(DDoS)	Mininet, ONOS, sFlow-RT, REST API	2초 주기 포트·플로우 시계열 + 이벤트	DCA-GRU	DDoS 탐지 및 모니터링
[7]	2025	트래픽 분류 프레임워크	ONOS 기반 SDN-CF, Weka	실시간 플로우 특징	Random Forest	악성 차단 + 라벨 데이터셋 생성
[8]	2025	라우팅/TE	Mininet(NSFNET), Floodlight	RTT/손실률/처리량/사용률 경로 통계	Logistic Regression	저혼잡 경로 선택 후 룰 갱신

표 1. AI 기반 SDN 구현 연구 분석 (2020-2025)

[5]는 공개 데이터셋을 플로우 통계로 변환해 데이터셋을 구성하고, 컨트롤러에서 수집 가능하다고 가정한 5개 플로우 통계 특징만으로 GRU, BiGRU, LSTM, BiLSTM을 비교해 5개 클래스를 분류했다. 학습·검증·테스트 분할과 정확도·정밀도·재현율·F1 평가에서 GRU가 99.65%로 가장 우수했으며, 실제 SDN 환경에서의 온라인 분류와 정책 적용 검증이 향후 과제로 남는다.

[7]은 ONOS 컨트롤러에 통합된 SDN-CF에서 OpenFlow 트래픽을 플로우로 집계해 특징을 추출하고, Weka 기반 Random Forest로 정상·악성을 실시간 분류해 차단·로깅과 라벨 포함 CSV 내보내기까지 지원한다. 데이터셋 자동 생성과 분류기 비교를 함께 제공해 재현 가능한 실험과 비교 평가를 돕는 프레임워크형 접근이며, 여러 지도학습 모델을 정밀도·재현율·F1과 학습시간으로 비교하고 ONOS 통합 후 실시간 성능도 보고한

다. 다만 모델이 메모리에만 유지돼 재사용에 제약이 있고 생성 데이터셋은 재사용 전 검증이 필요하며, 향후 분류기 확장과 온라인 학습, 모델 저장 기능이 과제로 제시된다.

C. 보안(DDoS 등 이상 트래픽 탐지)

SDN은 컨트롤러 단일 지점에 의존하므로 DDoS 공격에 상대적으로 취약하다는 전제를 가진다.

[4]는 Mininet - Ryu 기반 SDN 테스트베드에서 TCP SYN flood를 재현하고, 컨트롤러가 30초 주기로 수집한 OpenFlow 통계로 정상과 공격을 이진 분류한다. flow duration, ip proto, srcport, dstproto, packet count, byte count 특징의 11,545개 샘플로 SVM·Naive Bayes·MLP를 학습했으며, 75% 학습·25% 테스트에서 정확도·정밀도·F1과 혼동행렬로 검증 시 MLP가 99.75%로 가장 높다. 단일 공격과 시뮬레이션 데이터 중심이라 일반화에 한계가 있고, 향후 최적화 기반 분류기 개선을 과제로 제시한다.

[6]은 ONOS - Mininet 가상 SDN에서 DDoS 시나리오를 재현하고 2초 주기로 수집한 트래픽 시계열 통계를 입력으로 DCA-GRU를 적용해, 정확도·정밀도·재현율·F1과 혼동행렬로 성능을 검증했으며 가상 환경과 공격 유형 제한으로 실제 환경 적용과 대응 정책 연동이 과제로 남는다.

전형적인 구현 패턴은 가상 SDN 구성에서 시작해 공격 트래픽 생성과 네트워크 통계 수집을 거친 뒤 ML/DL 기반 분류·탐지로 이어진다.

D. 라우팅 및 트래픽 엔지니어링(TE)

라우팅/TE는 단순 분류를 넘어 경로 선택과 같은 행위 결정이 필요하기 때문에 강화학습이나 예측형 ML을 많이 사용한다.

[2]는 QoS와 룰 공간 제약을 고려한 멀티패스 라우팅에서 컨트롤러가 보유한 트래픽 매트릭스와 휴리스틱 라우팅 해를 학습해, 컨트롤러 애플리케이션의 DNN 회귀로 경로별 트래픽 분배비율을 실시간 예측하고 룰 설치에 활용한다. 성능은 휴리스틱 대비 MSE와 실행시간으로 검증해 계산시간 절감을 보였으나, 휴리스틱 라벨 의존과 제한된 환경 검증이 한계이며 실제 SDN에서의 온라인 적용과 정책 연동 검증이 과제로 남는다.

[3]은 컨트롤러가 링크 대역폭과 손실률을 수집해 정규화하고, Q-learning 에이전트가 병목 가용대역폭을 보상으로 widest-path를 학습해 OpenFlow 플로우 룰에 반영한다. Mininet Ryu iperf에서 Dijkstra 계열과 가용대역폭 오버헤드로 비교했으나 가상 환경 중심이라 실제망과 대규모 토폴로지 온라인 검증이 남는다.

[8]은 Mininet 기반 NSFNET에서 Floodlight가 수집한 RTT·손실률·처리량·대역 사용률 등 경로 통계를 입력으로, 컨트롤러 애플리케이션의 Logistic Regression이 트래픽 레벨을 분류해 여러 최단 후보 경로 중 저혼잡 경로로 플로우 룰을 설치·주기 갱신하는 동적 라우팅을 제안한다. 성능은 홉 기반·QoS 기반 라우팅 대비 RTT·처리량과 PSNR·SSIM로 검증했으며, 가상 환경·시뮬레이션 데이터 기반이라 실제망 일반화와 대규모 토폴로지·컨트롤러 검증이 향후 과제로 남는다.

E. 구현 관점 공통 트렌드 요약

실험 환경은 Mininet 기반 가상 테스트베드가 많이 쓰였고, 컨트롤러는 Ryu와 ONOS 중심이며 일부는 Floodlight나 자체 구성을 썼다.

입력 데이터는 플로우·포트 통계와 Packet_in 기반 헤더, 링크·경로 상태, 트래픽 매트릭스 등 제어 평면에서 수집하거나 측정으로 확보한 정보가 주로 활용된다.

분류·탐지는 지도학습과 딥러닝 중심인 반면, 라우팅·TE는 강화학습과 예측형 ML이 함께 쓰이며 경로 선택과 플로우 룰 갱신으로 연결된다.

성능 검증은 분류·탐지에서 분류 지표를, 라우팅·TE에서 QoS 지표와 함께 실행시간·오버헤드·MSE, 필요 시 QoE 지표까지 사용한다.

재현성은 일부 연구에서 코드·데이터·절차 제공이나 프레임워크 형태로 실험 자동화와 비교 평가를 지원하려는 흐름이 나타난다.

Ⅲ. 결론

본 논문은 2020년부터 2025년까지 발표된 AI 기반 SDN 연구 중 구현 중심의 8개 사례를 분석하였다. 다수 연구는 가상 테스트베드에서 컨트롤러와 스위치로부터 통계 및 상태 정보를 수집해 학습 데이터를 구성하고, 모델의 예측 결과를 경로 선택이나 차단 규칙과 같은 네트워크 제어로 연결해 효과를 평가한다. 트래픽 분류와 보안 분야에서는 특징과 라벨 정의를 포함한 데이터 수집 설계가 성능에 큰 영향을 미쳤고, 라우팅 및 트래픽 엔지니어링 분야에서는 상태 정의와 보상 설계를 바탕으로 QoS 개선과 함께 실행 오버헤드 및 비용 지표를 함께 고려하는 흐름이 나타났다. 향후 과제로는 실제 망과 대규모 환경에서의 온라인 검증과 오버헤드 평가, 코드·데이터·절차 공유를 통한 재현성 강화, 정책 연동 시 충돌과 안정성 검증이 중요할 것으로 보인다.

ACKNOWLEDGMENT

이 논문은 2025 년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구입니다. (No. RS-2025-00558169)

참 고 문 헌

[1] Chang, L.-H., Lee, T.-H., Chu, H.-C., and Su, C.-W. “Application-Based Online Traffic Classification with Deep Learning Models on SDN Networks,” Advances in Technology Innovation, vol. 5, no. 4, pp. 216 - 229, Sep. 2020.

[2] Awad, M. K., et al. “Machine Learning-Based Multipath Routing for Software Defined Networks,” Journal of Network and Systems Management, vol. 29, Art. no. 18, Jan. 2021.

[3] Ke, C.-H., Tu, Y.-H., and Ma, Y.-W. “A reinforcement learning approach for widest path routing in software-defined networks,” ICT Express, vol. 9, no. 5, pp. 882 - 889, Oct. 2023.

[4] Karthika, P., and Arockiasamy, K. “Simulation of SDN in mininet and detection of DDoS attack using machine learning,” Bulletin of Electrical Engineering and Informatics, vol. 12, no. 3, pp. 1797 - 1805, Jun. 2023.

[5] Nuñez-Agurto, D., et al. “A Novel Traffic Classification Approach by Employing Deep Learning on Software-Defined Networking,” Future Internet, vol. 16, no. 5, Art. no. 153, Apr. 2024.

[6] Yoon, N., and Kim, H. “Detecting DDoS based on attention mechanism for Software-Defined Networks,” Journal of Network and Computer Applications, vol. 230, Art. no. 103928, Oct. 2024.

[7] Carneiro-Diaz, V., Álvarez-González, M., and Cacheda-Seijo, F. “SDN-CF: Traffic classification in SDN ONOS controller using machine learning models,” SoftwareX, vol. 32, Art. no. 102382, Dec. 2025.

[8] İpek, A. D., Cicioğlu, M., and Çalhan, A. “AIRSDN: AI based routing in software-defined networks for multimedia traffic transmission,” Computer Communications, vol. 240, Art. no. 108222, Aug. 2025.