KNOM 2022 Conference Proceeding

2022년 5월 12일~13일

강원대학교

TS1: 학습 기반 네트워크 관리 및 서비스

(1) 강화학습 기반 Live Migration 정책 제어를 통한 MEC 환경에서의 동적 서비스 배치 (POSTECH)
(2) 서비스 유형별 보안 제약이 있는 SDN/NFV 지원네트워크에서 보안 인식된 서비스 요청하기 위한 강화학습 보상 값 기반 라우팅 (전남대학교)
(3) 무인 항공 기지국 환경에서 다중 에이전트 강화 학습 기반 서비스 처리량 최대화 기법 (경희대학교)
(4) Energy Demand Prediction for OCPP-based EV Charging Station: A Federated Learning Framework (경희대학교)
(5) 전기 수요 예측을 위한 연합학습 통신 비용 트레이드 오프 (전남대학교)
(6) 영상회의 관리를 위한 그래프 신경망 활용 방안에 관한 연구 (POSTECH)
(7) 네트워크 관리 시스템을 위한 계층 그래프 학습 모델 (POSTECH)

TS2: 미래 네트워크 서비스 및 관리

(1) 북한군과의 전장상황예측을 기반한 국군에서의 인공지능기술 활용분석 (대전대학교)
(2) ICBM 기반 국방자율무기체계 선진사례 분석 (대전대학교)
(3) 극한자연재해 대비 자율구축/관리 유무선 연합 비상통신망 시스템 (ETRI)
(4) CPU 자원 예측과 SFC의 VNF 그룹 별 Scaling 연구 (POSTECH)
(5) A Decentralized Approach for Virtual Reality-(VR)-based Services in 5G and Beyond Department of Computer Science and Engineering (경희대학교)
(6) A Study on the Digital Twin Technology for Future Network Operations and Managements (KT)
(7) 스마트 실내 서비스를 위한 모바일 로봇 플랫폼 설계 (고려대학교)

TS3: 네트워크 보안 1

(1) 악성코드 분류를 위한 trigram 기반의 BiLSTM 모델 연구 (강원대학교)
(2) Mel-Spectrogram 및 CNN을 활용한 응용 트래픽 (고려대학교)
(3) 필터링 방법 이용한 응용 트래픽 분류의 속도 개선 방안 (고려대학교)
(4) 딥러닝 기반 응용 트래픽 분류에서 데이터셋과 파라미터의 수량적 관계성에 대한 연구 (고려대학교)
(5) 다중 모형 CNN 기반 응용 트랙픽 분류 (고려대학교)
(6) DDoS 탐지를 위한 LSTM 기반 Entropy Threshold 예측 기법 (전남대학교)
(7) VXLAN Tunneling in OpenStack based Multi-site Cloud a secure mechanism for Communication and Data Sharing (제주대학교)

TS4: 블록체인 1 : NFT와 블록체인 응용

(1) 블록체인 기반 대체 불가능 토큰의 메타데이터 연구 (PSTECH)
(2) 대용량 스토리지를 지원하는 블록체인 확장 기법 (계명대학교)
(3) 분산아이디 (DID)를 활용한 트래블룰 준수 개인 암호화폐 지갑 설계 (POSTECH)
(4) 대체 불가능 토큰 (NFT) 거래 특화 블록체인 시스템 분석 (POSTECH)
(5) KOREN에서의 블록체인 기반 계층적 콘텐츠 전달 및 검증 (제주대학교)
(6) 이더리움 노드 탐색 프로토콜/v5의 와이어샤크 해석기 설계 (계명대학교)
(7) 대체 불가능 토큰을 활용한 메타버스 미디어 서비스 플랫폼 디자인 (POSTECH)

TS5: 양자암호통신 및 차세대연구망

(1) 국가과학기술연구망에서의 양자키 분배 기반 하이브리드 TLS 암복호화 방안 연구 (KISTI)
(2) 양자키 관리 네트워크에서의 양자내성암호 기반 데이터 송수신 구조 설계 연구 (KISTI)
(3) 네트워크 보안향상을 위한 QKD 및 PQC를 이용한 KREONET 양자암호통신망 설계 (KISTI)
(4) 양자암호통신망에서의 안전하고 효율적인 양자키 전달 모듈 구현 연구 (KISTI)
(5) 빅데이터 기반 AI 컴퓨팅을 위한 국제간 분산 연구플랫폼 구축 방안 연구 (KISTI)
(6) 과학 연구장비 근거리 무선 연결을 위한 밀리미터파 통신기술 적용방안 (KISTI)
(7) 빅데이터 고속 전송 환경 기반의 인공지능 연구 환경 제공 플랫폼 연구 (KISTI)

TS6: 블록체인2 : 가상자산서비스

(1) 코스모스에서 블록체인 간 메시지 전달 시간 측정 및 분석 (계명대학교)
(2) 블록체인 기반 커뮤니티 서비스 설계 (계명대학교)
(3) P2P 기반 블록체인 메신저 구현 (계명대학교)
(4) 가상자산 시장의 AMM (Automated Market Maker) 서비스 요구사항 및 동향 분석 (POSTECH)
(5) 다중서명과 다자산 계산을 이용한 디지털 자산 커스터디 서비스 설계 (POSTECH)
(6) 이더리움에서 중복 사용 스마트 계약 비용 분석 (계명대학교)

TS7: 네트워크 보안 2

(1) 2D CNN 기반 네트워크 침입 탐지 모델 (강원대학교)
(2) 가상 네트워크 관리를 위한 기계학습 기반 네트워크 공격 및 침입 탐지 시스템 설계 (POSTECH)
(3) CNN 기반 차량용 이더넷 침입 탐지 시스템의 네트워크 패킷 표현 최적화에 관한 연구 (경희대학교)
(4) 딥러닝 기반 익스플로잇 킷 탐지 모델의 입력 데이터 설계에 관한 연구 (고려대학교)
(5) Rule 기반 트래픽 분석을 통한 사용자 행위 탐지 시스템 설계 (고려대학교)
(6) BERT 기반 VM 고장 예측 기법 연구 (POSTECH)

TS1:
학습 기반 네트워크 관리 및 서비스

강화학습 기반 Live Migration 정책 제어를 통한 MEC 환경에서의 동적 서비스 배치

정세연, 유재형, 홍원기
포항공과대학교 컴퓨터공학과

{jsy0906, jhyoo78, jwkhong}@postech.ac.kr

Dynamic Service Placement in Multi-access Edge Computing using Reinforcement Learning-based Live Migration

Seyeon Jeong, Jae-Hyoung Yoo, James Won-Ki Hong
Department of Computer Science and Engineering, POSTECH

요 약

MEC(Multi-access Edge Computing)는 다양한 자원 분포와 서비스 요구사항을 포함하는 5G/6G 를 실현하기 위한 핵심기술의 하나로 주목 받고 있다. 최근에는 일반 기업들도 자체적인 엣지(edge) 데이터센터를 구축하여 빠르고 효과적으로 관제하고, 대량의 자원 및 특수한 네트워크 기능은 통신사업자의 클라우드 데이터센터를 활용하는 형태로 사설 네트워크를 구축하고 있다. 이러한 MEC 환경에서 서비스를 적시적소에 동적으로 배치함으로써 서비스 품질을 향상시키고 자원을 효과적으로 사용할 수 있지만, 동시에 관리 복잡도가 증가한다. 본 논문에서는 부하분산 및 장애완화 등에 사용되는 live migration 기술을 활용한 동적 MEC 서비스 배치 문제를 심층강화학습(Deep Reinforcement Learning) 문제로 모델링하고, 초기 migration 정책이 서비스 요청과 토폴로지에 대한 학습을 통해 서비스 지연시간(latency) 및 가용성(availability)을 향상시키도록 최적화됨을 보인다. 이와 같이 인공지능 기술을 네트워크 관리에 접목하여 관리자의 정책 결정을 지원하거나 MEC 의 관리 복잡도를 낮출 수 있을 것으로 기대된다.

Ⅰ. 서론

MEC (Multi-access Edge Computing) 기술은 다가오는 5G/6G 시대에 발생하는 다양한 서비스 요구사항을 반영하고 구현하는데 핵심적인 기능을 수행할 것으로 기대되고 있다. 특히 private 5G 체계에서는 각 기관별로 독립적인 엣지(edge) 데이터센터를 구축하여 디지털화된 기존 인더스트리 요소(스마트팩토리 등)들을 자체적으로 관제하며 필요에 따라 서비스 프로바이더의 클라우드 자원을 활용함으로써 보다 비용효율적이며 유연한 운영 환경이 제공된다 [1]. 그러나 서비스별 서로 다른 요구사항(URLLC, eMBB 등) 및 데이터센터 간 계층관계(cloud, fog, edge) 등 여러 이종성(heterogeneity)을 내포하고 있기 때문에 MEC 의 관리 복잡도는 크게 증가할 것으로 예상된다.

VM (Virtual Machine) Live Migration은 임의의 서비스 어플리케이션 또는 VNF(Virtualized Network Function)가 동작하는 VM 을 물리적으로 이격된 호스트 서버 간에 이동시키는 기술이며 그 과정에서 발생하는 서비스 단절시간(downtime)을 최소화한다. 클라우드 데이터센터에서는 주로 장비 교체, 주기적인 소프트웨어 업데이트 등의 유지보수 목적으로 Live migration 기술이 활용되고 있으며 [2], 에너지 절감 차원에서 VM consolidation 을 위한 기반 기술로도 활용되고 있다. 또한 MEC 환경에서는 사용자 단말의 이동(mobility)에 따라 서비스 제공 위치를 동적으로 변경해주는 service migration 기술 구현에 live migration 을 활용한다. 본 논문에서는 자원 제약적이고 이중화가 어려운 MEC 환경(hybrid private 5G 등)에서, 자원 효율적이면서 동시에 장애를 완화하도록 서비스를 동적 배치시키기 위한 수단으로 live migration 을 활용한다.

최근 네트워크 관리의 복잡성 문제를 효과적으로 해결하는데 인공지능 기술들이 두루 활용되고 있다. 주어진 정답지 데이터를 학습해 예측 및 분류 문제에 주로 활용되는 지도학습(supervised learning)과 달리, 강화학습(RL, Reinforcement Learning)은 환경(environment)의 현재 상태(state)를 기반으로 에이전트(agent)가 적절한 행동(action)을 취하도록 하고 환경이 피드백해 주는 보상(reward)을 통해 해당 행위의 좋고 나쁨을 판단함으로써, 에이전트로 하여금 누적보상을 최대화하는 일련의 행동 양식을 학습시킨다. 따라서 임의의 최적화 문제를 강화학습 모델로 표현하여 구현할 수 있다면 에이전트와 환경 간에 반복적인 상호작용(학습)을 통해 근사해(approximate solution)를 찾을 수 있다. 최근 딥러닝(Deep Learning) 기술의 발달은 강화학습에 인공 신경망(Artificial Neural Network)을 접목시켜 더 복잡한 문제에 대한 효과적인 학습도 가능케 해주고 있다.

본 논문에서는 서로 다른 요구사항의 서비스들이 여러 엣지 또는 클라우드 데이터센터에 분산 배치된(인스턴스화된) 클라우드 컴퓨팅 환경에서, RL 에이전트가 개별 서비스의 SLA 를 보전하면서 평균 서비스 지연(latency) 및 가용성(availability)을 향상시키는 live migration 정책을 생성하는데 심층강화학습(Deep RL)을 사용한다. 충분히 학습된 migration 정책은 그림 1 과 같은 상황에서 자원 효율적이고 서비스 성능을 향상시키는 동적 서비스 배치를 지원한다.

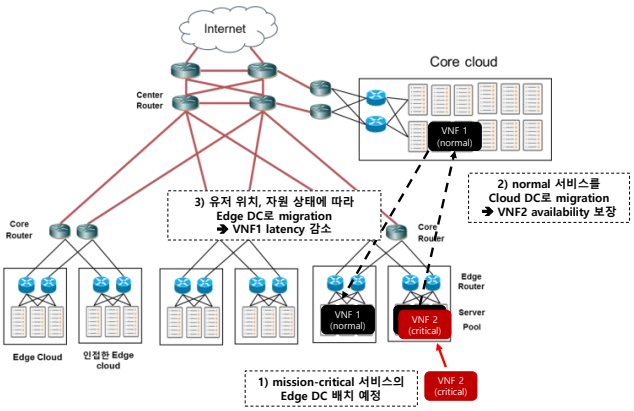


그림 1-a. 동적 서비스 배치 시나리오 1

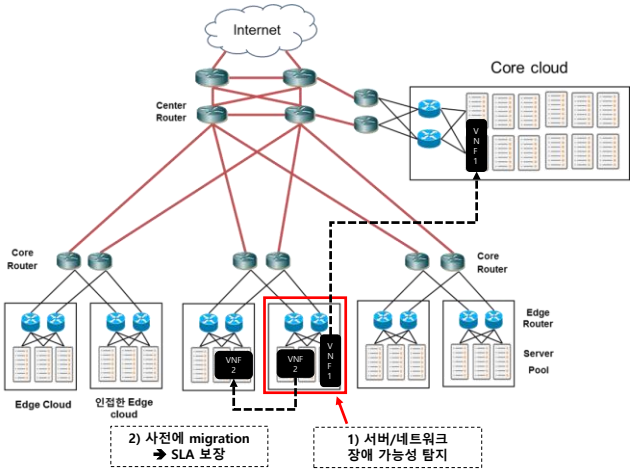


그림 1-b. 동적 서비스 배치 시나리오 2

Ⅱ. 관련 연구

MEC 환경에서는 서비스 성능 향상을 위해 mobile 사용자의 현재 위치에 따라 적절한 엣지 데이터센터로 서비스를 migration 시킬 수 있다. VM 으로 인스턴스화된 서비스에 대한 live migration 은 VM 이미지 파일 전송 등의 비용이 드는 작업이기 때문에 서비스 프로바이더 입장에서는 해당 migration 에 따른 benefit 과 cost 를 고려한 최적화 문제로 접근할 필요가 있다. [3]에서는 심층강화학습의 DQN (Deep Q-Network) 알고리즘을 사용하여 사용자와 서비스 인스턴스가 구동 중인 MEC 서버 간의 거리(distance)를 state, 사용자와 가장 가까운 MEC 서버로의 migration 을 action, best QoS value 와 migration cost 간에 차이를 reward 로 모델링하는 service migration 연구를 진행하였다. [4]는 단일 클라우드 데이터센터와 여러 엣지 데이터센터로 구성된 클라우드 컴퓨팅 환경에서 VNF 를 배치할 때 VNF 의 요구사항(자원, SLA 등), 각 데이터센터의 자원 상태와 각 링크 구간의 대역폭 상태를 state 로 입력 받아 해당 VNF 를 배치하는데 가장 적합한 서버를 출력하는 DDPG (Deep Deterministic Policy Gradient) 모델을 제안하여 평균 service latency 를 최소화하였다. 반면 [5]는 각각의 MEC 서버가 병렬 agent 로 동작하는 multi-agent 모델을 제안하며, single-agent 모델 대비 적은 학습 비용(state 크기, 모니터링 부하 등)으로도 cost 를 최소화하는 migration 정책을 생성한다.

본 연구는 심층강화학습으로 최적 migration 정책을 생성함에 있어서, 관련 연구 [3-5]에서 충분히 다루고 있지 않은 MEC 서버의 고장 상황 및 migration service downtime 과 연계된 SLA availability 를 고려한다.

Ⅲ. 설계

1. 문제 정의

본 연구에서 강화학습을 통해 최적화하려는 동적 서비스 배치 문제는 아래와 같이 정의된다.

- 여러 엣지 데이터센터와 단일 클라우드 데이터센터로 구성된 클라우드 컴퓨팅 토폴로지를 가정함.
- 서로 다른 요구사항(SLAs, 자원 요구량 등), 요청 시간, 사용자 위치를 가진 서비스들이 엣지 또는 클라우드 데이터센터 내부의 서버에 배치됨.
- 서버는 서비스 배치 현황에 따라 점유된 자원 상태가 변하며, 비교적 안정성이 낮은 엣지 데이터센터에 위치한 서버(MEC 호스트)의 경우 특정 조건에 이르면 서비스 장애를 일으킴 [6].
- Migration 컨트롤러는 일정 주기로 서버 별 서비스 배치 상태를 감시하고, migration 이 필요하다고 판단되는 서비스에 대해 migration 목적지 서버를 선정함.
- 해당 migration 으로 인해 서비스의 SLA(latency 및 availability) 위반이 발생되어서는 안됨.
- 상기 조건에 따라 모든 서비스가 종료되는 시점에 목적함수 (1)을 최대화하는 일련의 migration 정책을 도출함.

해당 문제 정의에서 평균 service latency 를 줄이기 위해서는 서비스들이 엣지로 배치(migration)되어야 하는데 이는 엣지 서버들의 부하를 높이기 때문에 service availability 가 감소한다. 반대로 availability 를 증가시키기 위해서는 클라우드 서버로 배치되는 경향을 보여야 하는데 이는 전반적인 latency 를 감소시킨다. 따라서 본 연구에서는 강화학습을 통해 상호 tradeoff 관계에 있는 두 항의 합을 최대화하는 migration 정책을 찾는다 (개별 서비스의 SLA 는 보전).

$$Util. = (-avg.service\ latency) + avg.service\ availability \quad (1)$$

2. 강화학습 모델

그림 2 는 제시된 문제 정의에 대한 강화학습 모델의 구조도이다. 제안하는 DQN 기반 강화학습 모델은 개별 데이터센터가 자체적인 migration 컨트롤러를 가지는 multi-agent 구조로, 각 agent 는 일정 주기 마다 해당 데이터센터에서 동작중인 서비스들에 대해서 일련의 migration 을 수행하고 MEC 환경의 피드백인 reward 를 통해 해당 migration action 의 가치를 평가한다. DQN 알고리즘에서는 인공신경망이 가치 평가 함수의 역할을 수행하므로, 주어진 state 에서 누적 보상(예, 1000 개

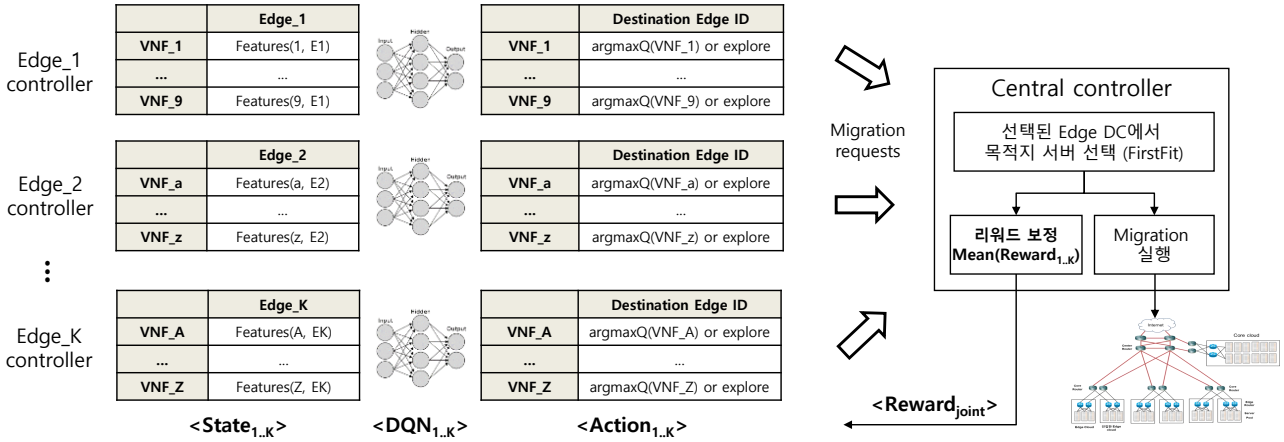


그림 2. Edge-agent 기반 migration 정책 강화학습 모델

서비스를 처리하는 동안 발생하는 모든 action 의 보상 총합)을 최대로하는 action 에 대해 더 높은 가치를 부여하는 방향으로 신경망을 업데이트(학습)한다.

각 agent(Edge controller)는 다른 데이터센터의 자원 상태와 같은 글로벌 정보 없이 해당 데이터센터의 로컬 정보만을 가지고 학습을 진행한다. 따라서 각 $Agent_K$ 의 환경에 대한 관측 정보인 $State_K$ 는 (i)해당 DC 내 서버들의 평균 CPU/memory/disk utilization, (ii)대상 서비스의 자원 요구량 및 SLA 요구사항(예, latency 10ms 이내, availability 99.99% 등)에 관한 수치 데이터(feature vector)를 모든 서비스에 대해 생성한 미니 배치(mini-batch)에 해당된다. 해당 미니 배치를 DQN_K 인공신경망에 입력하면 입력된 순서대로 해당 서비스를 각각의 데이터센터로 migration 할 때 발생하는 action 의 가치가 출력된다. 이 때, 최종 migration 목적지로 현재 가장 높은 가치를 보이는 데이터센터를 선정하거나(Exploitation) 임의의 데이터센터를 선택하며(Exploration), 그 비율은 학습 초기에 90:10 으로 시작하여 99:1 까지 Exploration 비율을 감소시켜 나간다 (decaying epsilon). 각 서비스에 대해 선정된 migration 목적지 리스트가 $Action_K$ 에 해당되며, 현재 위치한 데이터센터가 목적지로 선정되는 경우 기존 배치가 가장 적합하다는 의미이므로 migration 을 수행하지 않는다.

각 agent 별 최종 action set 은 migration request 형태로 Central controller 로 전달되어 해당 목적지 데이터센터(엣지 또는 클라우드) 내에서 수용 자원이 남아있으면서 동시에 해당 서비스의 SLA 를 보전할 수 있는 최종 목적지 서버를 선택한다. 따라서 최종 목적지 서버를 도출하지 못한 migration request 는 거절된다. 각 $Reward_K$ 는 해당 $Action_K$ 에 의한 migration 전/후의 benefit 인 수식 (2)로 정의된다.

$$Reward_k = L_benefit + A_benefit \quad (2)$$

$$L_benefit = \frac{avg.serive\ latency\ before\ -\ after\ migration}{avg.service\ latency\ before}$$

$$A_benefit = \frac{avg.server\ availability\ after\ -\ before\ migration}{avg.server\ availability\ before}$$

$$server.availability = 1 - avg.disk\ util.\ for\ last\ 5\ mon.interval$$

Multi-agent DQN 알고리즘의 기본 구현에서 각 agent 는 자기자신의 reward 를 증가시키는 action 을 선호하도록 greedy 하게 동작하기 때문에, 극단적인 경우 전체 시스템 성능을 저하시킬 수 있다(예, edge DC 1 의 agent 가 동작중인 모든 서비스를 edge DC 2 로 이전시키는 경우). 따라서 각 agent 별 migration 정책이 전체 시스템(MEC 환경) 차원에서 평가되도록 각 $Reward_K$ 를 동기적으로(synchronously) 수신하여 평균값으로 보정하는 모델을 추가하였다. 보정된 $Reward_{joint}$ 는 각 agent 로 반환되어 $State_K$, $Action_K$, migration 이후에 측정되는 $State_K$'(next state)와 함께 replay buffer 에 저장되어 학습 과정에서 샘플링 된다.

3. Migration cost 모델

VM live migration 기술은 사실상의 무중단을 지향하지만 실제 구현에 있어서 가상네트워크 인터페이스의 탈부착, DHCP 지연 등으로 인해 서비스(네트워크) downtime 이 발생하며 그 시간은 해당 VM 의 page fault rate 에 비례한다 [7]. 본 연구에서는 수식 (3)으로 migration service downtime 과 SLA availability 간의 관계를 모델링하여, SLA 를 위반하는 migration request 는 거절한다. *cumulative_downtime* 은 해당 서비스를 migration 할 때 마다 누적되는 service downtime 이며 *hypervisor_constant* 는 OpenStack, KVM 등 VM live migration 구현 방법에 따른 비용 차이를 고려한 상수이다 (예, 100ms).

$$migration\ is\ allowed\ only\ if \quad (3)$$

$$1 - \frac{service.cummulative_downtime\ +\ expected_downtime}{service.duration} \geq service.SLA_availability$$

$$expected_downtime = \frac{service.memory}{service.duration} * hypervisor_constant$$

IV. 구현 및 검증

1. MEC 서버 및 서비스 구성

실험을 위해 1 개 클라우드 데이터센터와 15 개 엣지 데이터센터로 구성되어 배치 위치에 따라 service latency 가 달라지는 MEC 토폴로지를 Python SimPy 기반 시뮬레이터로 구현하였으며 (그림 1), 각 데이터센터 내부의 서버에 대한 설정 값은 표 1 과 같다.

또한 Alibaba 데이터셋[8]을 기반으로 각 서비스에 요청 위치(인접 엣지 ID) 및 SLA latency/availability 를 추가하여 MEC 서비스로 변환하였다 (표 2).

표 1. MEC 서버 구성

구분	CPU (core) / mem / disk	고장 조건	# 서버
클라우드 서버	1000 / 10 / 10	None	1
엣지 서버 (MEC host)	16 / 0.2 / 0.2	>95% disk util. for 10 monitor intervals	15*8

표 2. MEC 서비스 구성

구분	비중 (%)	Latency SLA	Availability SLA	서비스 당 평균 migration (회)
Type 1	20	5ms 이내	Random [None, 99%, 99.9%, 99.99%]	0.2
Type 2	20	10ms 이내		0.56
Type 3	20	50ms 이내		2.3
Type 4	40	None		1.7

2. 성능 평가

제안하는 migration 강화학습 알고리즘을 3000 에피소드에 걸쳐 반복 학습시킨 결과는 그림 3 과 같다. 본 실험에서 하나의 에피소드 동안 서로 다른 자원 요구량을 가진 표 2 의 서비스 1000 개를 표 1 의 서버에 분산하여 최초 배치 후 모든 서비스가 종료될 때까지 10 초 단위로 각 서비스의 migration 정책을 판단한다.

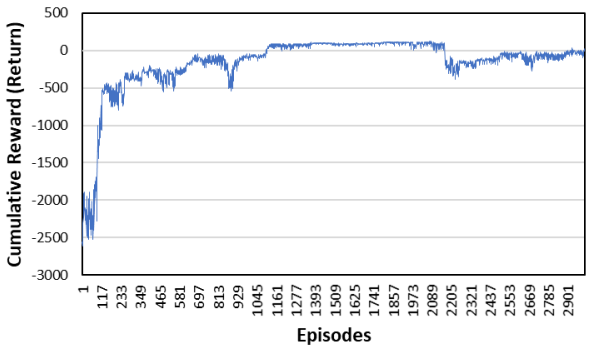


그림 3. 누적 리워드 추이

실험에서 사용한 리워드 계산식(2)은 L_benefit 과 A_benefit 에 각각 1 과 0.5 의 가중치를 부여하였다. 학습 초기에 누적 보상을 크게 증가시키는 정책 방향이 학습되어 꾸준히 증가하다가 1000 에피소드 이후로는 큰 변화없이 일정 수준에 수렴하는 결과를 보였다.

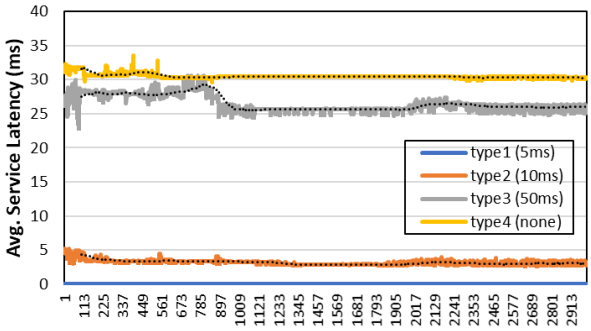


그림 4. 서비스 타입별 평균 latency

그림 4 는 학습된 정책에 의해 각 서비스에 migration 이 수행된 결과를 서비스 타입별 평균 service latency 로 보인다. MEC 서비스(type 1, 2)에 대해 SLA 를 만족시킬 수 있는 migration 목적지 서버군이 한정되어 있으며, migration service downtime 과 SLA availability 간의 관계 모델링(Ⅲ.3 절)으로 인해 서비스 타입별 평균 migration 횟수가 각각 0.2, 0.56, 2.3, 1.7 회(표 2)로 제한됨에도 불구하고 학습이 진행됨에 따라 평균 service latency 가 감소하는 추세를 보였다.

그림 5 는 A_benefit 의 가중치를 1 로 증가시켜 학습했을 때 평균 서비스 중단 횟수가 감소함을 보인다. 본 연구에서 서비스 중단은 엣지 서버의 disk 상태에 따라 발생하기 때문에(표 1 고장조건), migration 정책이 분산 배치를 통해 엣지 서버의 평균 disk 사용률을 낮추거나 클라우드 서버로의 migration 빈도를 높이는 형태로 동작하게 된다.

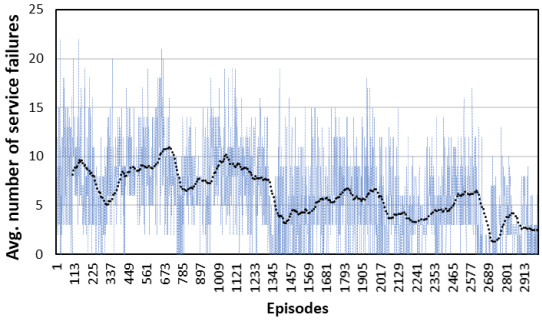


그림 5. 평균 서비스 장애 횟수

V. 결론 및 향후 연구

제안하는 강화학습 알고리즘을 통해 MEC 환경에서 개별 서비스의 SLA 를 보전하면서 보상으로 정의한 성능 지표를 향상시키도록 migration 정책이 개선됨을 보였다.

향후연구로 해당 알고리즘을 OpenStack 과 같은 실제 클라우드 환경에 적용하여 성능을 평가하고 모델을 개선시킬 예정이다.

ACKNOWLEDGMENT

이 논문은 2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원(2018-0-00749, 인공지능 기반 가상 네트워크 관리기술 개발)과 2022년도 정부(산업통상자원부)의 재원으로 산업기술평가관리원의 지원을 받아 수행된 연구임 (No.2009633, 초저지연 네트워크 서비스를 위한 SDN 기반 인공지능 관제 시스템 개발).

참 고 문 헌

[1] 넷매니아즈, “Private 5G Mobile Edge Computing 5G 특화망”, https://www.netmanias.com/ko/private-5g/about-private-5g-portal/1598/.

[2] Google Cloud Platform Blog. “Google Compute Engine uses Live Migration technology to service infrastructure without application downtime”. https://cloudplatform.googleblog.com/2015/03/Google-Compute-Engine-uses-Live-Migration-technology-to-service-infrastructure-without-application-downtime.html.

[3] Zhang, Cheng, and Zixuan Zheng. "Task migration for mobile edge computing using deep reinforcement learning." Future Generation Computer Systems 96 (2019): 111-118.

[4] Dalgkitsis, Anestis, et al. "Dynamic Resource Aware VNF Placement with Deep Reinforcement Learning for 5G Networks." GLOBECOM 2020-2020 IEEE Global Communications Conference. IEEE, 2020.

[5] Dai, Yu, Qiuhong Zhang, and Lei Yang. "Virtual Machine Migration Strategy Based on Multi-Agent Deep Reinforcement Learning." Applied Sciences 11.17 (2021): 7993.

[6] Yala, Louiza, Pantelis A. Frangoudis, and Adlen Ksentini. "Latency and availability driven VNF placement in a MEC-NFV environment." 2018 IEEE Global Communications Conference (GLOBECOM). IEEE, 2018.

[7] Akoush, Sherif, et al. "Predicting the performance of virtual machine migration." 2010 IEEE international symposium on modeling, analysis and simulation of computer and telecommunication systems. IEEE, 2010.

[8] Alibaba cluster trace dataset 2017, https://github.com/alibaba/clusterdata/tree/master/cluster-trace-v2017.

서비스 유형별 보안 제약이 있는 SDN/NFV 지원 네트워크에서 보안 인식된 서비스 요청하기 위한 강화학습 보상 값 기반 라우팅

조현준, 김경백
전남대학교
limdugmin2@gmail.com, kyungbaekkim@jnu.ac.kr

Reinforcement learning reward-based routing for security-aware service requests in SDN/NFV-enabled networks with security constraints by service type

Hyeonjun Jo, Kyungbaek Kim
Chonnam Univ

요 약

SDN/NFV 기술을 이용하여 복잡해지는 네트워크 관리의 용이성, 관리 비용 감소 등 네트워크 환경에서의 효율성을 얻고 있다. 복잡해지는 네트워크 환경속 서비스 기능 체이닝 기술을 이용하여 취약점이 존재하는 애플리케이션 서비스 유형에 따라 보안 기능을 선택적으로 구현함으로써 보안 인식된 서비스 요청을 할 수 있게 된다. 하지만 보안 미들 박스가 서로 다른 위치에 배치될 때 서비스 유형에 맞는 보안 미들 박스를 경유 할 수 있는 효율적인 라우팅 방법이 필요하다. 본 논문에서는 라우팅 문제를 해결하기 위해 Q-Routing 알고리즘의 보상(Reward)을 통해 보안 제약 조건을 만족시킬 수 있는 라우팅 방법을 제안한다.

Ⅰ. 서 론

네트워크 기술은 네트워크 제어 및 관리, 멀티미디어 서비스 기술 등 다양한분야에서 발전하며 혁신적인 개발 연구가 되고 있다[1]. 특히 5G 네트워크에서는 기존 네트워크 환경 하드웨어 중심의 네트워크기능(방화벽, 침입 탐지·방지 시스템, NAT 장비 등)을 소프트웨어로 구현하여, 이들을 상황 변화에 따라 유연하게 제어할 수 있는 기술로서 소프트웨어 정의 네트워킹 기반의 네트워크 기능 가상화 기술을 이용하여 상황 변화에 따라 유연하게 제공되고 있다.

서비스 기능 체이닝은 종단 간 서비스에 유형에 따라 순서적으로 보안 기능을 선택적으로 조합하고 실행하여 서비스 유형별 보안 인식된 서비스 요청을 할 수 있다[2]. 더욱더 앞서 말한 기술의 장점을 사용할 경우 복잡해지는 네트워크 환경에서의 서비스 다변화에 대한 문제와 규모가 커지는 네트워크 환경 속 새로운 위치에 보안 장비를 배치 하지 않고 기존의 보안 장비를 사용하면서 네트워크를 운영할 수 있는 장점이 존재한다. 다양한 서비스 유형별 취약점이 존재하는 서비스 요청에 대한 보안 위협, 대응 방법, 보안 장비의 우선순위를 선정하여 일련의 순서를 구성하는 체이닝 방법에 대해 다양한 연구 방법들이 제안 되었다[3,4].

Q-Learning[5]은 모델 없이 학습하는 강화 학습 기법의 하나며, Q-Routing은 Q-Learning 알고리즘을 변형한 방법을 이용한 방법이다. Q-Routing 알고리즘은 환경(Environment)과 상호작용을 하는 에이전트(Agent)에 대하여 학습시킨다. 에이전트는 상태(state)라고 불리는 네트워크상황에 대한 행동(Action)을수행한다. 먼저 에이전트는 상태와 행동으로 구성된 Q-Table을 최적의 상태로 전환하기 위해 에피소드(Episode)를 정의한다. 에피소드(Episode)에 정의된 단계에 따라 행동 A_t을 선택하고 상태 S_t을 변환하고 최적의 보상(Reward) R_t을 통해 최적의 Q 값 $Q_t(S_t,A_t)$ 을 근사화하는 최상위 정책(Policy)을 설정한다. 따라서 Q-Routing 알고리즘의 시간 복잡도는 네트워크의 전체 노드를 탐색하는 링크 상태 기반 최단 거리 알고리즘의 시간 복잡도에 비해 비교적 낮다.

Ⅱ. 관련 연구

[6]의 저자는 다계층적 SDN 환경에서 강화학습 기반 QoS 인식 적응형 라우팅을 제안하였으며, [7]의 저자는 링크 혼잡을 감지하고 방지하기 위해 강화학습 기반 QoS 인식 라우팅 알고리즘을 제안하였다. [8]의 저자는 사용자별 서비스 요청과 위치 정보를 고려한 여분의 대역폭, 낮은 지연 과 패킷 손실률을 고려한 강화학습 기반 라우팅을 제안하였다. 하지만 노드별 고정된 Q-Routing 방법으로 종단간 거쳐야 하는 네트워크 보안 장비 증가시 알고리즘 수행 시간이 증가되는 문제점이 존재한다. 따라서 노드별 고정된 Q-Routing 방법은 서로 다른 노드에 보안 미들 박스(n)가 배치되었을 때 서비스별 보안 제약 조건을 만족시키기 위한 경로를 찾기 위해 n_i 개의 환경에 따른 에이전트가 수행 하게 되며 종단간 보안제약 조건을 만족하는 경로를 찾기 위해 Q-Routing 알고리즘의 수행시간은 증가하게 된다. 결과적으로 Q-Routing 알고리즘의 낮은 시간 복잡도 장점을 효율적으로 이용하지 못하게 된다. 하지만 Q-Routing 알고리즘의 보상(Reward) R_t 을 통해 최적의 Q값 $Q_t(S_t,A_t)$ 을 근사화하는 최상위 정책(Policy)을 설정 시 보안 미들 박스가 배치된 인접 노드에 특수한 보상값을 통해 Q값을 근사화 시키는 정책을 이용한다면 앞서 말한 보안 제약 조건을 만족시키기 위한 경로를 찾기 위해 Q-Routing 알고리즘의 수행 시간을 줄일 수 있게 된다. 본 논문은 Q-Routing 알고리즘의 보상(Reward)을 통해 보안 제약 조건을 만족시킬 수 있는 라우팅 방법을 제안한다.

Ⅲ. 보안 인식된 서비스 요청하기 위한 강화학습 보상 값 기반 라우팅

SDN의 데이터 평면에 구성된 스위치는 i 는 상태 S_i 로 나타내고 이러한 상태는 상태공간 $S_i \in S$ 에서 관리한다. 상태 공간 S 로 구성된 네트워크 토폴로지는 SDN 데이터 평면의 스위치에 해당하는 그래프로 에이전트에 전달된다. 상태 S_i 의 인접 상태는 해당 스위치의 인접 스위치에

해당한다. 상태 S_i 에서 상태 S_p 전환은 스위치 i 와 스위치 p 을 연결하는 링크에 해당한다. 에이전트는 각 상태 S_i 에 대해 행동 중 하나 A_i 를 수행하고 행동은 행동 공간 $A_i \in A$ 에서 관리 된다. 에이전트의 행동 A_i 은 현재 상태 S_i 를 상태 S_p 로 전환 된다.

본 논문에서 제안하는 정책은 Q 값을 최소화 하기 위해 링크의 전송 속도는 높고 지연, 패킷 손실률, 지터 값이 낮은 링크를 우선순위로 선택한다. 보상 R_t은 네트워크상에서 최적의 경로를 탐색을 위해 지식 평면으로 부터 수집된 링크의 QoS 특성인 지연 d_{link}, 패킷 손실률 p_{link}, 지터 j_{link}, 전송 속도 t_{link} 을 사용하여 링크 QoS 기반 (Q_s) 값을 계산하고 이를 수식 (1)과 같이 나타낸다.

$$Q_s = w_1{}^*(1-d_{link}) + w_2{}^*(1-p_{link}) \downarrow + w_3{}^*(1-j_{link}) + w_4{}^* t_{link} \quad (1)$$

에이전트의 학습 과정에서 각 링크 상태들은 각각 다른 단위 지연 ms, 손실률 %, 지터 ms, 전송 속도 kbps로 구성되어 있기 때문에 각 특징들을 정규화를 시키기 위해 Min-Max 기법을 사용한다. 정규화에 대한 수식 (2)과 같이 나타낸다.

$$x_i = \frac{x_i - X_{\min}}{X_{\max} - X_{\min}},\ x_i \in X, 1,\ 1 \le i \le m \quad (2)$$

Min-Max 기법을 이용하여 링크 상태 기반 보상 R 을 계산하고 이를 수식 (3)과 같이 나타 낸다.

$$R = Q_s = w_1{}^*(1-\bar{d}) + w_2{}^*(1-\bar{p}) \downarrow + w_3{}^*(1-\bar{j}) + w_4{}^* \bar{t} \quad (3)$$

수식 (1)의 w_1, w_2, w_3, w_4 값은 보상 R_t 를 계산 하기 위한 행렬에 대한 가중치를 나타내는 매개 변수이다. 가중치 w_i 는 수식 (4)과 같이 나타낸다.

$$w_1 + w_2 + w_3 + w_4 = 1,\ w_1, w_2, w_3, w_4 \in [0,1] \quad (4)$$

에이전트는 학습률 α, 보상 R_t 및 새로운 상태 S_{t+1} 에서 행동하며 Q 값을 조정한다. 만약 에이전트가 상태-행동 수행시 새로운 상태 S_{t+1}가 보안 미들 박스가 배치된 노드의 인접 위치가 아닌 상태 라면 Q 값에 대한 수식은 (5)과 같이 나타낸다.

$$Q_{t+1}(S_t, A_t) = Q(S_t, A_t) + \alpha^* \downarrow [R_t + \max Q_t(S_{t+1}, A_t) - Q_t(S_t, A_t)] \quad (5)$$

만약 에이전트가 상태-행동 수행시 새로운 상태 S_{t+1} 가 보안 미들 박스가 배치된 노드의 인접 위치 상태 라면 Q 값에 대한 수식은 (6)과 같이 나타낸다.

$$Q_{t+1}(S_t, A_t) = Q(S_t, A_t) + \alpha^* \downarrow [R_t{}^* link\,W_t(S_t, S_{t+1}) \downarrow + \max Q_t(S_{t+1}, A_t) - Q_t(S_t, A_t)] \quad (6)$$

에이전트는 새로운 상태 S_{t+1} 가 보안 미들 박스가 배치된 노드의 인접 위치 상태라면 현재 상태S_t와 새로운 상태S_{t+1} 사이 연결된 링크의 특성인 지연 d_{link}, 지터 j_{link}, 패킷 손실률 p_{link},비율 만큼 가중치를 곱해 보상 값을 업데이트 된다. 링크의 가중치 비율은 $link\,W_t(S_t, S_{t+1})$ 는 수식 (7)과 같이 나타낸다.

$$S_t, S_{t+1}(d_{link} + j_{link} + p_{link}) = 1$$
$$link\,W_t(S_t, S_{t+1}) \in [d_{link}, j_{link}, p_{link}] \quad (7)$$

수식 (7)의 링크의 지연 d_{link}, 지터 j_{link}, 패킷 손실률 p_{link} 값은 상태 S_t 와 보안 노드와 연결된 인접 노드의 새로운 상태 S_{t+1} 사이 링크 상태를 수식(2)를 이용한 정규화된 값이며 해당 링크의 지연, 지터, 패킷 손실률의 대해 비율로 구분하기 위해 Softmax를 사용한다. Softmax 함수에 대한 수식(8)과 같이 나타낸다.

$$Y_k = \frac{\exp(link_k)}{\sum_{i=1}^{n} \exp(link_k)},\quad n = count(k),$$
$$k \in [d_{link}, j_{link}, p_{link}] \quad (8)$$

에이전트는 누적 보상을 최대로 만들기 위해 예상되는 최적의 행동을 선택하는 탐색(Exploration) 및 미래에 더 큰 보상을 얻을 수 있기를 바라면서 다른 행동을 선택하는 이용(Exploitation)을 반복한다. 하지만 에이전트가 탐색하지 않는다면 보상 값을 최대로 만들지 못할 수도 있으며, 탐색만 한다면 기존의 경험을 사용하지 못해 에이전트의 학습 방법에 대하여 비효율적이다. 앞서 말한 비효율적인 탐색과 이용의 트레이드오프(Trade off) 딜레마 현상을 해결하기 위해 에이전트는 학습 프로세스 중 ϵ 확률로 이용을 진행하고 1- ϵ 확률로 탐색을 진행하는 ϵ-greedy를 사용한다. ϵ-greedy를 사용하여 정의된 에이전트의 행동 수식 (9)과 같다.

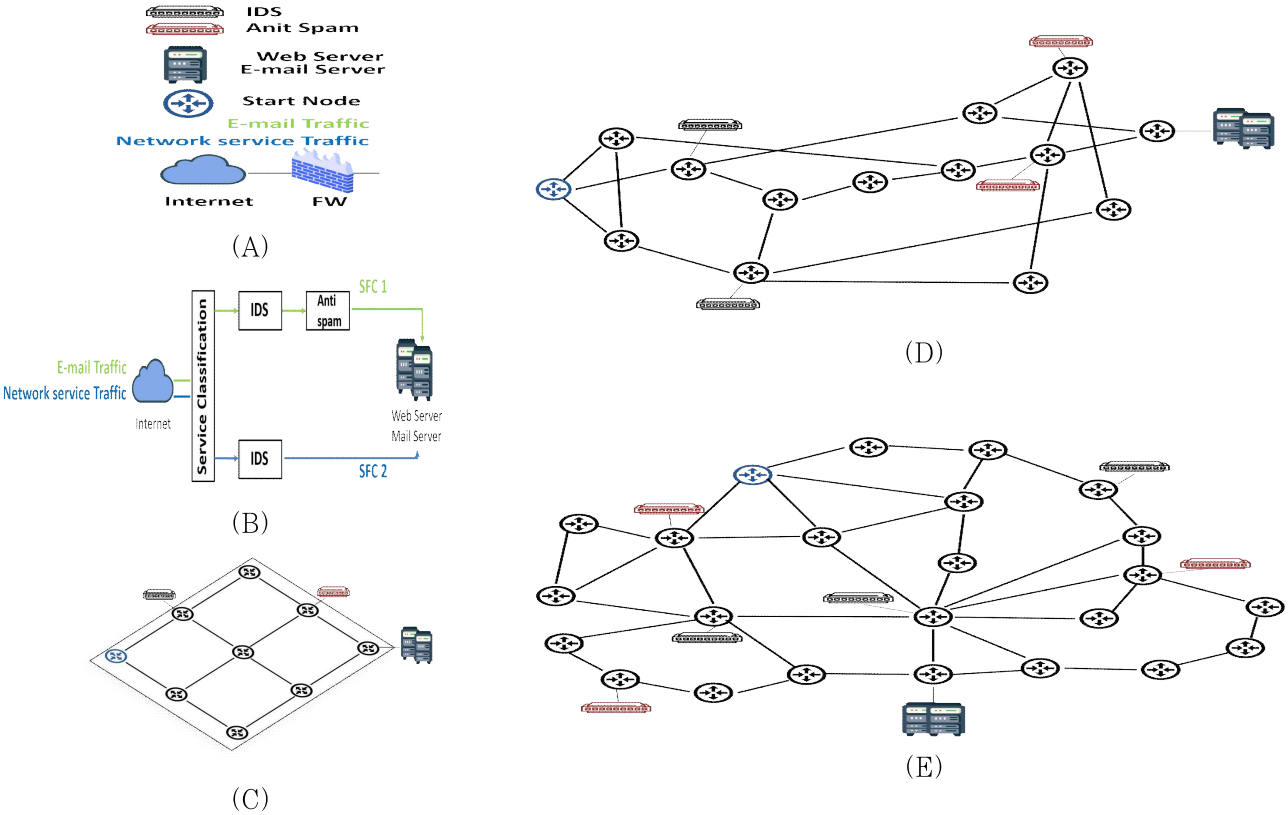
$$A = \begin{cases} \min Q_t(S_t, A), \text{if} < \epsilon \\ another action, otherwise \end{cases} \quad (9)$$

Ⅳ. 실험 및 평가

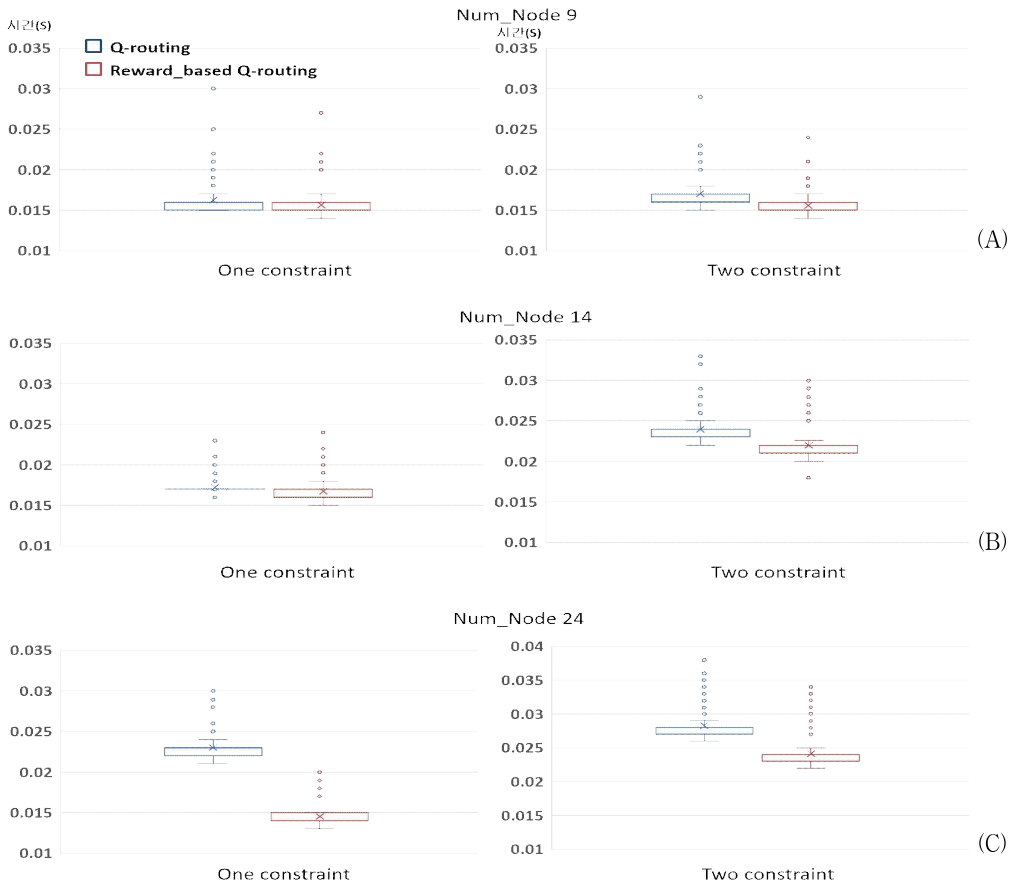
본 장에서는 보안 제약 조건을 만족 하는 경로를 찾기 위해 고정된 노드별 Q-Routing 방법 과 본 논문에서 제안된 방법인 보상 값 기반 Q-Routing 방법의 알고리즘 수행 시간을 비교하며 평가한다.

그림 1은 알고리즘 수행 시간을 비교하기 위해 네트워크에 서로 다른 서비스 요청 트래픽 요청시 서로 다른 보안 제약 조건 구성과 네트워크 규모에 따른 보안 미들 박스가 배치된 네트워크 환경 구성이다.

그림 2은 Q-Routing 알고리즘 수행 시 필요한 모든 매개 변수를 동일하게 설정 후 그림 1처럼 구성된 네트워크 환경에서 하나의 보안 제약 조건과 두 개의 보안 제약 조건을 만족 하는 경로를 찾기 위해 본 논문에서 제안된 보상 값 기반 Q-Routing 알고리즘과 고정된 노드별 Q-Routing 알고리즘[8]의 수행 시간을 비교 하였다. 그림 2의 보안 제약 조건에 따른 알고리즘 수행 시간 비교를 보게 되면 보상 값 기반 Q-routing은 서로 다른 노드에 보안 미들 박스(n)가 배치되었을 때 보안 제약 조건을 만족시키기 위한 경로를 찾기 위해 n 개의 환경에 따른 에이전트가 수행 하게 되며, 노드별 고정된 Q-routing 은 보안 제약 조건을 만족시키기 위한 경로를 찾기 위해 n_i 개의 환경에 따른 에이전트가 수행 하게 됨으로 수행 시간은 $\sum_{i=1}^{T} n_i$ 경유 출발지 - 보안 미들 박스(n), 보안 미들 박스(n), - 목적지 까지 수행된 Q-routing 알고리즘의 수행시간의 총 합으로 얻어진 값이다. 따라서 본 논문에서 제안하는 방법인 보상 값 기반 Q-Routing 알고리즘의 수행 시간은 노드별 고정된 Q-Routing 알고리즘 수행 시간보다 비교적 낮다.



〔그림 1. A : 네트워크 장비 설명, B : 서비스 요청 트래픽 별 구성된 보안 제약 조건
C : 9 node 1 Security middle box, D : 14 node 2 Security middle box, E : 24 node 3 Security middle box〕



〔그림 2. A : 9 node 네트워크 에서 보안 제약 조건 개수에 따른 알고리즘 수행 시간 비교, B : 14 node 네트워크 에서 보안 제약 조건 개수에 따른 알고리즘 수행 시간 비교,C : 14 node 네트워크 에서 보안 제약 조건 개수에 따른 알고리즘 수행 시간 비교 〕

Ⅳ. 결론

네트워크 규모가 커지고, 새로운 위치에 보안 장비를 추가로 배치 시키지 않고, 다른 위치에 운영 중인 보안 장비를 이용하기 위해 종단간 보안 제약 조건을 만족 시킬 수 있는 라우팅 방법이 필요하다. 선행 연구된[6,7,8] 노드별 고정된 Q-Routing 방법은 서로 다른 노드에 보안 미들 박스(n)가 배치되었을 때 서비스별 보안 제약 조건을 만족시키기 위한 경로를 찾기 위해 n_i 개의 환경에 따른 에이전트가 수행 하게 되며 종단간 보안제약 조건을 만족하는 경로를 찾기 위해 Q-Routing 알고리즘의 수행시간은 증가 되는 문제점이 존재 한다.

본 논문에서는 보안 미들 박스가 배치된 인접 노드에 특수한 보상 값을 통해 Q 값을 근사화 시키는 정책을 이용하여 보안 제약 조건을 만족하는 경로를 찾는 방법을 제안 함으로써 알고리즘의 수행 시간을 줄일 수 있는 방법을 제안 한다. 제안된 Q-Routing의 알고리즘 수행 시간을 비교 및 평가하기 위해 노드별 고정된 Q-Routing 방법과 비교 하였다. 실험 결과 네트워크 규모가 커지고, 보안 제약 조건이 많아질수록 제안된 알고리즘의 수행 시간은 노드별 고정된 Q-Routing 기법 보다 비교적 낮은 수행 시간을 얻을 수 있다. 따라서 제안 된 기법은 네트워크가 더욱더 복잡해질수록 다양한 요청 서비스들에 대한 보안 제약 조건을 만족 시킬 라우팅 작업을 수행 시 최소한 네트워크 자원을 사용하며, 빠른 라우팅 결정을 내릴 수 있는데 적합할 수 있다.

CKNOWLEDGMENT

"이 논문은 2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임"(IITP-2019-0-01343)

참 고 문 헌

[1] Ordonez-Lucena, Jose, et al. "Network slicing for 5G with SDN/NFV: Concepts,architectures, and challenges." IEEE Communications Magazine 55.5 (2017): 80-87.

[2] Halpern, Joel, and Carlos Pignataro. "Service function chaining (SFC) architecture." RFC 7665. 2015. 1-32.

[3] Bhamare, Deval, et al. "A survey on service function chaining." Journal of Network and Computer Applications 75 (2016): 138-155.

[4] Hantouti, Hajar, Nabil Benamar, and Tarik Taleb. "Service Function Chaining in 5G& Beyond Networks: Challenges and Open Research Issues." IEEENetwork 34.4 (2020): 320-327.

[5] 13Watkins, Christopher JCH, and Peter Dayan. "Q-learning." Machine learning 8.3-4(1992): 279-292.

[6] T. Uzakgider, C. Cetinkaya and M. Sayit, "Learning-based approach for layered adaptive video streaming over SDN", Comput. Netw., vol. 92, pp. 357-368, Dec. 2015.

[7] S. Sendra, A. Rego, J. Lloret, J. M. Jimenez and O. Romero, "Including artificial intelligence in a routing protocol using software defined networks", Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops), pp. 670-674, 2017.

[8] Quach, Hong-Nam, Sungwoong Yoem, and Kyungbaek Kim. "Dynamic Network Provisioning with Reinforcement Learning based on Link Stability." 2021 22nd Asia-Pacific Network Operations and Management Symposium (APNOMS). IEEE, 2021.

무인 항공 기지국 환경에서 다중 에이전트 강화 학습 기반 서비스 처리량 최대화 기법

박유민, 홍충선*
경희대학교 컴퓨터공학과

yumin0906@khu.ac.kr, *cshong@khu.ac.kr

A Study on the Maximization Throughput based on Multi-Agent Reinforcement Learning in Unmanned Aerial Vehicle-Base Station Environment

Yu Min Park, Choong Seon Hong*
Kyung Hee University

요 약

차세대 이동 통신인 5G 는 밀리미터파를 사용하며 초고속으로 대용량의 서비스 처리를 가능하게 하였다. 하지만 밀리미터파의 한계로 장애물에 의한 통신 손실이 발생하고 안정적인 통신 지원을 위해서 많은 수의 기지국이 필요하게 되었다. 따라서 유동적인 위치 이동이 가능한 무인 항공기 또는 무인 공중 플랫폼과 같이 지상이 아닌 Line-of-Sight (LoS) 확보에 유용한 공중에서 통신 서비스를 지원해주는 새로운 통신 플랫폼이 주목 받고 있다. 이러한 장점에도 불구하고 여전히 무인 항공 기지국은 통신 자원과 위치 이동 등 풀어야 할 최적화 문제들이 존재한다. 이에 본 논문은 무인 항공 기지국의 통신 자원과 위치 이동 문제를 동시에 해결하기 위해 Multi-Agent Reinforcement Learning (MARL) 을 접목하였다. 이 때, 본 논문에서는 MARL 중에서도 Multi-Agent Proximal Policy Optimization (MAPPO) 라는 알고리즘을 사용하며, 각 최적화 변수들이 에이전트가 되어 더욱 협동적으로 최적화를 시행할 수 있는 기법을 제안한다. 결과적으로 본 연구를 통해 제안된 알고리즘은 일반적인 단일 에이전트 기반의 Proximal Policy Optimization (PPO) 에 비해 더욱 빠른 수렴 속도와 높은 보상을 얻을 수 있었다.

1. 서론

차세대 이동 통신인 Fifth-Generation (5G)은 밀리미터파를 사용하며 초고속으로 대용량의 서비스 처리를 가능하게 하였다. 따라서 사용자들은 무선으로 고사양의 콘텐트를 즐길 수 있게 되었다. 하지만 밀리미터파의 한계로 장애물에 쉽게 막혀 통신이 훼손되고 안정적인 통신 지원을 위해서는 많은 수의 기지국이 필요하게 되었다 [1]. 그에 따라 지상 기지국을 대신할 수 있는 새로운 통신 플랫폼에 대한 연구가 활발히 진행 중이다.

많은 새로운 통신 플랫폼이 제안되고 있지만 그 중 무인 항공기를 활용한 통신이 다양한 장점을 가지고 있어 많은 연구가 존재한다 [2]. 무인 항공기를 활용한 통신은 일반 지상 기지국에 비해 Line-of-sight 를 높일 수 있어 안정적인 통신을 보장할 수 있다. 그리고 특정 지역에 사용자 수 또는 서비스 요구량 급증에 따라 무인 항공 기지국은 유동적인 위치 이동으로 효율적으로 대처할 수 있다. 이러한 장점들을 가지고 있음에도 통신 자원, 위치 이동, 그리고 에너지 한계 등 여전히 해결해야 할 문제들이 존재한다.

이를 해결하기 위해 다양한 연구들이 진행 중인데 논문 [3]은 무인 항공 기지국을 통해 다수의 사용자들에 통신을 지원해 주는 상황에서 에너지 한계를 해결하기 위해 최소의 에너지로 최대의 통신 효율을 낼 수 있도록 최적화하였다. 논문 [4]은 무인 항공 기지국에 컴퓨팅 처리를 할 수 있는 엣지 서버를 장착하여 연결된 사용자에게 태스크를 오프로딩 받아 원격으로 컴퓨팅 처리를 할 수 있도록 제안하였다. 하지만 결과적으로 동적으로 변하는 상황에 대처하기 위해서는 최적화를 빠르게 도출할 수 있어야 한다.

이 논문은 2022 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원(No.2019-0-01287, 분산 엣지를 위한 진화형 딥러닝 모델생성 플랫폼)과 과학기술정보통신부 및 정보통신기획평가원의 지역지능화혁신인재양성(Grand ICT 연구센터) 사업의 연구결과로 수행되었음 (IITP-2021-2015-0-00742) *Dr. CS Hong is the corresponding author.

강화 학습은 기계 학습 중 하나로 주어진 환경에서 특정 에이전트가 정해진 행동을 반복하며 최대의 보상을 얻을 수 있게 자율적으로 학습하는 방법이다. 논문 [5]는 강화 학습을 활용하여 최대의 서비스 처리량을 위해 무인 항공 기지국의 위치를 최적화시켰다. 최근에는 여러 에이전트가 협동적으로 학습을 하는 Multi-Agent Reinforcement Learning (MARL) 을 활용하여 다수의 통신 플랫폼을 동시에 학습하는 연구가 진행되고 있다. 논문 [6]은 다수의 무인 항공 기지국을 MARL 을 통해 학습하여 최적화를 진행하였다. 하지만 에이전트를 무인 항공 기지국으로 설정하여 하나의 에이전트가 대역, 전력, 그리고 위치 등 많은 최적화를 함에 따라 느린 수렴 속도, 최적화의 불확실성 등이 문제로 떠오르고 있다. 이에 본 논문에서 주요 제안사항은 다음과 같다.

- 본 논문은 무인 항공 기지국에서 다수의 사용자가 무선 통신을 받는 상황에서 최적의 서비스 처리량을 가질 수 있도록 무인 항공 기지국의 통신 자원 및 위치 이동을 동시에 최적화한다.
- 통신 자원 및 위치에 대한 변수들을 동시에 최적화하기 위해 Multi-Agent Reinforcement Learning (MARL) 기반의 Proximal Policy Optimization (PPO)를 사용한다.
- 마지막으로 단일 에이전트 기반의 강화학습과 제안하는 MARL 기반의 방법을 비교하여 제안하는 MARL 방법이 실제로 얼마나 효율적으로 학습에 효과가 있는지 실험 결과를 보여준다.

2. 시스템 모델

본 논문은 하나의 무인 항공 기지국이 다수의 사용자 $\mathcal{N} = \{1,2,\dots,N\} \in \mathbb{R}^{|N|}$ 에 대해 일정한 시간 $\mathcal{T} = \{1,2,\dots,T\} \in \mathbb{R}^{|T|}$ 동안 무선 통신을 지원한다. 본 논문에서의 무인 항공 기지국은 사용자들에게 Orthogonal Frequency Division Multiple Access (OFDMA) 기반의 다운링크 통신 서비스 지원만이 가능하다. 통신 서비스를 지원할 때 무인 항공 기지국은 위치를 이동할 수 있지만 고도 h_0 를 변화시킬 수는 없다고 가정한다. 다음으로 본 논문에서 사용되는 통신 모델과 해결해야 할 문제 정의에 대해 소개한다.

2.1 통신모델

무인 항공 기지국은 사용자들에게 최적의 무선 통신 지원을 하기 위해 위치를 이동하며 동시에 통신 자원을 최적화 한다. $l_0^t = [x_0^t, y_0^t, h_0]^T$ 와 $l_n^t = [x_n^t, y_n^t]^T$ 는 각각 시간 $t \in \mathcal{T}$ 에서 무인 항공 기지국의 위치, 사용자 $n \in \mathcal{N}$ 의 위치이다. 이 때, 본 논문에서는 무인 항공 기지국은 고정된 높이에서 이동을 가정하였다.

무인 항공기에게 지원 받는 사용자 사용자 $n \in \mathcal{N}$ 의 다운링크 수신되는 Signal to Noise Ratio (SNR) γ_n 은 다음과 같다.

$$\gamma_n(t) = \frac{p_n^t \cdot g_n(t)}{\sigma^2}, \forall n \in \mathcal{N}, \forall t \in \mathcal{T}, \quad (1)$$

$$g_n(t) = \frac{g_0}{(d_n^t)^\alpha}, \forall n \in \mathcal{N}, \forall t \in \mathcal{T}, \quad (2)$$

여기서 p_n^t 과 g_n 은 사용자 $n \in \mathcal{N}$ 에게 할당된 무인 항공 기지국의 송신 전력과 채널 이득이다. σ^2 는 첨가된 가우시안 잡음 세기이다. 그리고 g_0 과 $d_n^t = \sqrt{{h_0}^2 + \|l_0^t - l_n^t\|^2}$ 는 참조 거리 $d_0 = 1\,\mathrm{m}$ 당 채널 이득과 시간 $t \in \mathcal{T}$ 에서 무인 항공 기지국과 사용자 $n \in \mathcal{N}$ 와의 거리이다. α 는 통신의 경로 손실 지수이다. 이렇게 도출된 γ_n 을 통해 Shannon-Hartley 이론에 기반하여 무인 항공 기지국에게 무선 지원을 받는 사용자 $n \in \mathcal{N}$ 의 서비스 처리량은 다음과 같이 도출할 수 있다.

$$R_n(t) = w_n^t \cdot B \cdot log_2\big(1 + \gamma_n(t)\big), \forall n \in \mathcal{N}, \forall t \in \mathcal{T}, \quad (3)$$

이 때, B 와 w_n^t 은 무인 항공 기지국이 사용할 수 있는 전체 대역폭과 시간 $t \in \mathcal{T}$ 에서 사용자 $n \in \mathcal{N}$ 에게 할당되는 대역폭 지수이다.

2.2 문제정의

본 논문은 무인 항공 기지국에게 무선 통신 지원을 받고 있는 사용자들의 서비스 처리량을 최대화하기 위해 무인 항공 기지국의 대역 할당 $\boldsymbol{W} = \{w^1, w^2, \dots, w^T\}$, 전력 할당 $\boldsymbol{P} = \{p^1, p^2, \dots, p^T\}$, 위치 이동 $\boldsymbol{L} = \{l_0^1, l_0^2, \dots, l_0^T\}$ 을 동시에 최적화한다. 이 때, $w^t \in \mathbb{R}^{|N|}$ 과 $p^t \in \mathbb{R}^{|N|}$ 은 시간 t 에서 사용자들에게 할당되는 대역과 전력 벡터이다. 따라서 해결하고자 하는 문제는 다음과 같이 정의할 수 있다.

$$\begin{aligned}
&\text{maximize}_{\boldsymbol{W},\boldsymbol{P},\boldsymbol{L}} && \textstyle\sum_{t=1}^{T}\sum_{n=1}^{N} R_n(t) && && (4)\\
&\text{subject to} && R_n(t) \geq R_{\min}, && \forall n \in \mathcal{N}, \forall t \in \mathcal{T}, && (4a)\\
& && w_n^t \leq 1, && \forall n \in \mathcal{N}, \forall t \in \mathcal{T}, && (4b)\\
& && \textstyle\sum_{n=1}^{N} w_n^t \leq 1, && \forall t \in \mathcal{T}, && (4c)\\
& && p_n^t \leq P_{\max}, && \forall n \in \mathcal{N}, \forall t \in \mathcal{T}, && (4d)\\
& && \textstyle\sum_{n=1}^{N} p_n^t \leq P_{\max}, && \forall t \in \mathcal{T}, && (4e)
\end{aligned}$$

위의 문제에서 제약 사항 (4a) 는 각 사용자들의 최소 서비스 처리량을 보장하며, 제약 사항 (4b) 와 (4c) 는 무인 항공 기지국의 대역 할당은 사용자 전체에 대해 최대 대역폭을 넘을 수 없다는 것을 의미한다. 마지막으로 제약 사항 (4d) 와 (4e) 에서 무인 항공 기지국의 전력 할당은 사용자 전체에 대해 최대 전력을 넘어 할당될 수 없음을 나타낸다.

3. 제안사항

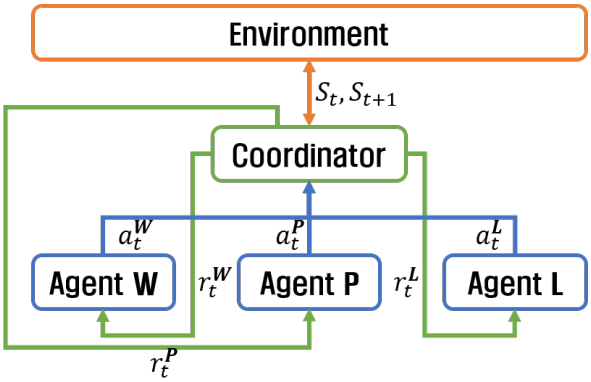


그림 1. 제안하는 MAPPO 학습 과정.

본 논문에서의 해결하고자 하는 문제 (4) 는 각 변수들이 목적 함수에 대해 엮어져 있어 한번에 최적의 근들을 찾는 것은 굉장히 어렵다. 따라서 본 논문에서는 MARL 을 활용한 문제 해결을 제안한다. 본 논문에서 적용하고자 하는 MARL 은 각 최적화 변수 $\boldsymbol{W}, \boldsymbol{P}, \boldsymbol{L}$들이 개별적인 에이전트로 정의되어 각 에이전트들이 목적 함수를 최대화할 수 있게 정의하였다. 그리고 본 논문에서는 MARL 의 알고리즘은 Multi-Agent Proximal Policy Optimization (MAPPO)를 사용하였다. 제안하는 알고리즘은 단일 PPO 에이전트들을 동시에 학습하는 형태로 진행된다. 그림 1 는 제안하는 MARL 알고리즘의 구조를 나타낸다. MAPPO 알고리즘에 대한 설명과 학습 환경에서 사용된 Markov Decision Process (MDP)는 다음과 같다.

Multi-Agent Proximal Policy Optimization (MAPPO): Proximal Policy Optimization (PPO)는 다양한 환경에서 구현과 적용이 간단하며 안정적인 성능을 보여주는 대표적인 강화학습 알고리즘 중 하나이다 [7]. 제안하는 MAPPO 는 다수의 PPO 에이전트들이 동시에 같은 환경에서 학습을 진행한다. 이 때, 각 최적화 변수($\boldsymbol{W}$, $\boldsymbol{P}$, $\boldsymbol{L}$)들이 에이전트가 되어 협동적으로 학습에 참여하게 된다. 이 때, Coordinator 가 에이전트들과 환경 사이에서 동기화 및 상태, 보상, 행동에 대한 전달을 담당한다. 각 에이전트들은 상태는 공유를 하지만 서로 다른 행동, 보상을 가지게 된다. 이렇게 같은 환경에서 서로 다른 보상을 주는 이유는 서로 다른 에이전트들이 학습되는 과정에서 실제 보상에 끼치는 영향을 세밀하게 파악할 수 있기 때문이다. 다음으로 학습에 사용되는 에이전트들의 MDP 를 소개한다.

상태: 시간 $t \in \mathcal{T}$ 에서 각 에이전트들이 공유하는 상태 s_t는 다음과 같이 정의한다.

$$s_t = \{w^t, p^t, l_0^t, \{l_n^t\}_{n\in\mathcal{N}}\}. \tag{7}$$

행동: 시간 $t \in \mathcal{T}$ 에서 각 에이전트의 행동들은 다음과 같이 정의된다.

$$a_t^{\boldsymbol{W}} = \{w^{t+1}\}, \tag{8}$$
$$a_t^{\boldsymbol{P}} = \{p^{t+1}\}, \tag{9}$$
$$a_t^{\boldsymbol{L}} = \{\Delta x_0^{t+1}, \Delta y_0^{t+1}\}, \tag{10}$$

이 때, w^{t+1}와 p^{t+1}의 요소는 모든 $\mathrm{n} \in \mathcal{N}$에 대해 각각 $0 \le w_n^t \le 1$ 과 $0 \le p_n^t \le P_{\max}$ 의 연속적인 공간에서 행동하는 것으로 설정했다. 그리고 식 (10)에서 Δx_0^{t+1}과 Δy_0^{t+1}는 무인 항공 기지국이 시간 t에서 이동한 x, y 축의 거리이다.

보상: 시간 $t \in \mathcal{T}$에서 각 에이전트들의 보상들은 다음과 같이 정의된다.

$$r_t^{\boldsymbol{W}} = \sum_{n=1}^{N} R_n(t) - \zeta \cdot F\left(f\left(a_t^{\boldsymbol{W}}\right)\right) \cdot f^2\left(a_t^{\boldsymbol{W}}\right), \tag{11}$$
$$r_t^{\boldsymbol{P}} = \sum_{n=1}^{N} R_n(t) - \eta \cdot G\left(g\left(a_t^{\boldsymbol{P}}\right)\right) \cdot g^2\left(a_t^{\boldsymbol{P}}\right), \tag{12}$$
$$r_t^{\boldsymbol{L}} = \sum_{n=1}^{N} R_n(t), \tag{13}$$

여기서 $f\left(a_t^{\boldsymbol{W}}\right) = 1 - \sum_{n=1}^{N} w_n^t$ 이고 $F\left(f\left(a_t^{\boldsymbol{W}}\right)\right)$는 $f\left(a_t^{\boldsymbol{W}}\right)$가 0보다 크면 1 이고 그렇지 않다면 0 인 인덱스 함수이다. 비슷하게 $g\left(a_t^{\boldsymbol{P}}\right) = P_{\max} - \sum_{n=1}^{N} p_n^t$ 이고 $G\left(g\left(a_t^{\boldsymbol{P}}\right)\right)$ 는 $g\left(a_t^{\boldsymbol{P}}\right)$가 0보다 크면 1 이고 그렇지 않다면 0 인 인덱스 함수이다. 그리고 ζ과 η는 대역과 전력 할당에 대한 제약 사항의 페널티 변수이다.

4. 실험결과

표 1. 실험에 사용된 변수들의 값

Notion	Value	Notion	Value
σ^2	$-174\ dBm/Hz$	N	10
p_0	$40\ dBm$	T	100
α	0.7	Hidden layer's units	128
B	$100\ kHz$	Hidden layers	2

실험 환경은 $[600\,\mathrm{m}, 600\,\mathrm{m}]$ 공간에서 10 명의 사용자를 무작위로 배치하여 진행했다. 이 때, 무인 항공 기지국은 고정된 고도 $h_0 = 50\,\mathrm{m}$ 에서 움직일 수 있다고 가정하였다. 강화 학습은 총 20 만 번의 에피소드에 걸쳐 진행하였다. 추가로 실험에 사용된 네트워크 모델에 대한 내용과 변수들의 값은 표 1 에 작성하였다. 실험 결과에 앞서 제안하는 알고리즘 MAPPO 의 성능을 평가하기 위해 두 가지 비교 알고리즘을 정의하였다. 먼저, Only_L 은 대역 할당과 전력 할당을 모든 사용자들이 동일하게 설정하고 위치 이동만을 학습한 결과이다. 그리고 PPO 는 하나의 에이전트가 대역, 전력, 그리고 위치 이동 모두를 학습하는 알고리즘이다.

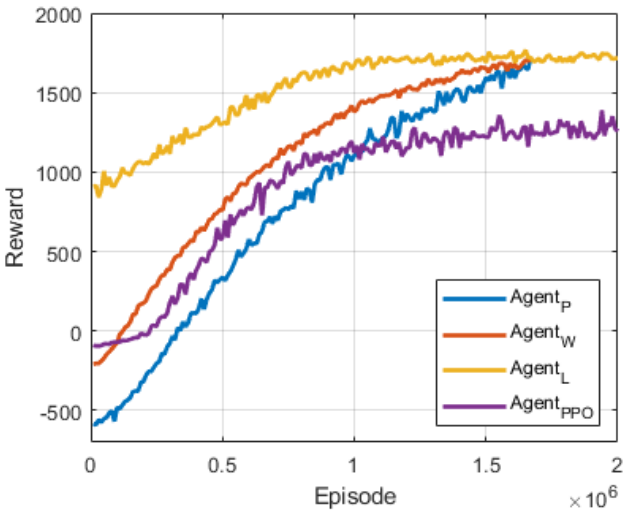


그림 2. 에피소드에 따른 학습 결과.

그림 2 은 에피소드가 진행됨에 따른 최종 보상에 대한 그래프이다. 모두 에피소드가 진행됨에 따라 일정한 보상에 수렴하는 것을 확인할 수 있다. 그 중

Agent_PPO는 비교 알고리즘 PPO에 사용된 에이전트에 대한 학습 내용으로 가장 낮은 최종 보상에 수렴하였다. Agent_W, Agent_P, 그리고 Agent_L은 제안하는 알고리즘 MAPPO에 사용된 에이전트이다. Agent_P, Agent_W, 그리고 Agent_L 순으로 수렴을 하게 되지만 결과적으로 해당 에이전트들이 같은 최종 보상에 도달하는 것을 알 수 있다. 이 결과로 제안하는 MAPPO에서 모든 에이전트들이 동일한 결과를 향해 학습이 잘 이루어진 것으로 판단할 수 있다.

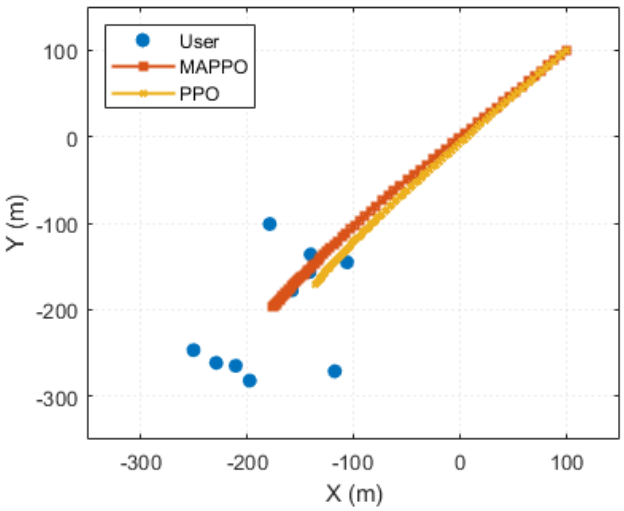


그림 3. 학습 모델을 통한 무인 항공 기지국 위치.

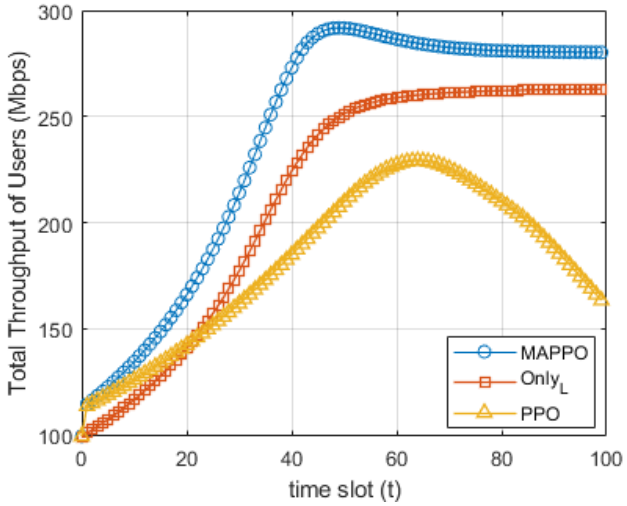


그림 4. 시간에 따른 서비스 처리량 변화.

그림 3는 학습된 모델들을 통해 무인 항공 기지국의 시간에 따른 경로를 나타낸다. 무인 항공 기지국은 모든 사용자들에게 통신이 용이하도록 중앙으로 이동하는 결과를 보여주었다. 하지만 MAPPO와 PPO를 통한 무인 항공 기지국의 최종 위치는 동일하지 않았다. 해당 예시에서의 시간에 따른 서비스 처리량은 그림 4를 통해 확인할 수 있다. 시간이 진행됨에 따라 무인 항공기는 사용자들의 근처로 이동을 하기 때문에 서비스 처리량이 증가하는 것을 알 수 있다. 최종 수렴치 중 제안하는 MAPPO가 가장 높은 성능을 보여주었다. 그리고 단일 에이전트로 학습을 진행한 PPO가 최적화 변수들의 복합된 행동과 보상으로 인해 학습에 실패하여 Only_L보다 낮은 성능을 가지게 되었다.

5. 결론 및 향후 연구

본 논문에서는 무인 항공 기지국이 다수의 사용자들에게 무선 통신 서비스를 제공할 때 통신 자원 및 위치를 최적화하는 방안에 대해 연구하였다. 최적화 방법으로 다수의 에이전트들이 협력을 하며 학습을 하는 MARL 기반의 MAPPO를 제안하였다. 이 때, 각 최적화 변수들이 에이전트로 설정되어 학습에 참여하였다. 결과적으로 제안한 방법을 통해 각 에이전트들이 자신의 행동과 보상에 더욱 집중할 수 있었고 일반적인 단일 에이전트 기반의 강화학습보다 더욱 빠르고 정확하게 모델을 학습시킬 수 있었다. 추후 본 논문에서 다루지 않았던 다수의 무인 항공 기지국, Terahertz (THz) 통신, 그리고 에너지 최적화 등을 고려하여 본 논문을 발전시킬 수 있을 것이다.

참 고 문 헌

[1] Bin, Zesong Fei, and Yan Zhang, "UAV communications for 5G and beyond: Recent advances and future trends," IEEE Internet of Things Journal, Vol. 6, No. 2, pp. 2241-2263, Dec. 2018.

[2] Yu Min Park, Min Kyung Lee, and Choong Seon Hong. "Multi-UAVs Collaboration System based on Machine Learning for Throughput Maximization." 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS). IEEE, 2019.

[3] Zeng, Yong, Jie Xu, and Rui Zhang. "Energy minimization for wireless communication with rotary-wing UAV." IEEE Transactions on Wireless Communications, Vol. 18, No. 4, pp. 2329-2345, Mar. 2019.

[4] Yan Kyaw Tun, Yu Min Park, Nguyen H Tran, Walid Saad, Shashi Raj Pandey, Choong Seon Hong, "Energy-efficient resource management in UAV-assisted mobile edge computing", Vol. 25, No. 1, pp. 249-253, Sep. 2020.

[5] 박유민, 홍충선, "UAV-BS 환경에서 서비스 처리량 최대화를 위한 강화학습 기반의 UAV 배치 연구", 정보과학회논문지, Vol. 47, No. 7, pp. 700-706, Jul. 2020.

[6] Peng, Haixia, and Xuemin Shen. "Multi-agent reinforcement learning based resource management in MEC-and UAV-assisted vehicular networks." IEEE Journal on Selected Areas in Communications, Vol. 39, No. 1, pp. 131-141, Jan. 2021.

[7] Schulman, John, Filip Wolski, Prafulla Dhariwal, Alec Radford, and Oleg Klimov. "Proximal policy optimization algorithms." arXiv preprint arXiv:1707.06347, 2017.

Energy Demand Prediction for OCPP-based EV Charging Station: A Federated Learning Framework

Luyao Zou, Young Woo Kim and Choong Seon Hong
Department of Computer Science and Engineering, Kyung Hee University, Yongin-si, Gyeonggi-do 17104, Korea
email:{zouluyao, ywkim1587, cshong}@khu.ac.kr

Abstract

The rapid penetration of electric vehicles (EVs) has the potential of causing new concerns for the power grid due to the increasing energy demand and the change in load profile. To this end, this article concentrates on predicting the energy demand of the OCPP-based EV charging stations (CSs). However, since the energy usage information is privacy-sensitive, collecting data from each distributed CS is not feasible for centralized prediction. Besides, it is expensive to train a model based on centralized data collection because of communication resource consumption. In this regard, in this article, a long short-term memory (LSTM)-adopted federated learning (FL) framework is proposed for the OCPP-based EV charging station's energy demand prediction, which is helpful for reducing the risk of privacy leakage since only model parameters need to be exchanged without the need of centralized local data. The simulation results demonstrate the effectiveness of the proposed LSTM-adopted FL.

I. Introduction

Electric vehicles currently have enlarged rapidly since they can be beneficial for reducing greenhouse gas emissions so as to protect the environment [1]. However, as EVs continue to penetrate, it becomes difficult for the power grid to manage the energy [2]. Thus, accurate energy demand prediction becomes of paramount importance from the perspective of the power grid. In this work, a long short-term memory (LSTM)-adopted federated learning (FL) framework is presented to forecast the energy demand of the OCPP (Open Charge Point Protocol [3]) adopted EV charging stations (CSs), which are distributed in an urban area. The proposed LSTM-adopted FL is advantageous in addressing the challenges resulting from centralized training. In particular, due to the energy data of each CS having privacy-sensitive phenomena, it is not realistic to train a centralized model by collecting data centralized. Moreover, training a centralized model is a costly task because of the consumption of communication resources for collecting energy data from the numerous distributed CSs. Thus, we introduce the LSTM-adopted FL in this paper since it does not need to centralized gather each charging station's energy data.

Federated learning has been applied for various applications, for instance, CNN with FL setting is utilized in [4] for image classification, which is different from this work. In [5] and [6], the RNN-utilized FL is leveraged for predicting the energy demand for the individual household. However, neither of these two papers considered EV charging nor charging stations. Unlike the aforementioned researches, in this work, we focus on forecasting energy demand of the OCPP-based EV charging stations. The key contributions of this paper are stated as follows:

- We propose a system model for OCPP-based EV charging stations in a considered urban area, where each EV charging station is taken into account using the unified communication protocol, named OCPP. Particularly, adopting OCPP can enable each charging station communicate with central system [7]. Besides, to some extent, using OCPP can make it easy to manage all the charging stations since the inconvenience caused by inconsistent communication protocols can be eliminated.
- Considering the energy data exists time-varying phenomenon and has a privacy-sensitive characteristic, an LSTM-adopted FL framework is presented to predict the energy demand of the considered OCPP-based EV charging stations.
- We evaluate the proposed method with a real-world EV charging demand dataset from [8]. The simulation results show the trend of the average Huber loss for both the training dataset and test dataset across all the CSs, and the error of the overall test dataset regarding various neuron numbers of each LSTM layer. In addition, we also show the overall Huber loss achieved by the proposed LSTM-adopted FL is 0.0359, which is lower than that of FedSGD approach.

II. System Model

Considering an urban area contains a central system and multiple EV charging stations, where central system is considered to manage each charging station. In particular, each charging station consists of multiple EVSEs for charging EVs. In addition, OCPP is adopted as the communication standard between each CS and central system. Further, in order to satisfy the energy requirement of each CS, we assume each CS connects with the power grid so that it can receive on-demand energy from the power grid. The corresponding system model is shown in Fig. 1.

This work was partially supported by the Korea Institute of Energy Technology Evaluation and Planning (KETEP) and the Ministry of Trade, Industry & Energy (MOTIE) of the Republic of Korea (No. 20199810100050), and the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2020R1A4A1018607) *Dr. CS Hong is the corresponding author.

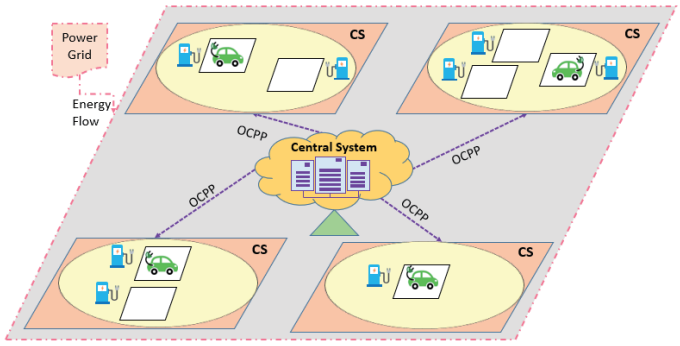


Fig. 1: System model of the proposed OCPP-based EV charging stations in the considered urban area.

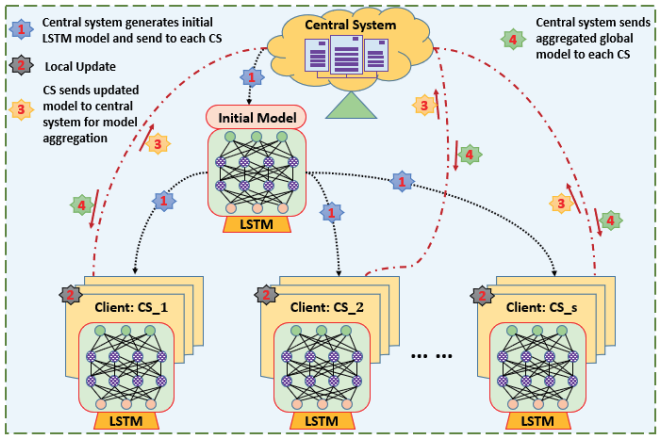


Fig. 2: Energy demand prediction for OCPP-based EV charging station via the proposed LSTM-adopted FL framework.

Let $\mathcal{S} = \{1, 2, ..., S\}$ denote a set of the charging station in the considered urban area. Besides, let $\mathcal{V} = \{1, 2, ...V\}$ indicate the EVs that are required to be charged. Additionally, a discrete charging time-slot is considered in this work, denoted as $\mathcal{T} = \{1, 2, ..., T\}$, where each time-slot is indexed by t and it lasts 6 hours [1].

In the case of EV, we represent the charging period of EV v as τ. In practice, during the EV charging process, there exists charging loss. Thus, it is necessary to consider the charging efficiency, λ. Based on [9], the actual charging of EV $v \in \mathcal{V}$, Γ_v, can be given as follows:

$$\Gamma_v = \int_0^{\tau} \lambda \Psi_v \, d\tau, \tag{1}$$

where Ψ_v denotes the EV v's charging power. Accordingly, denoting the time to start charging as t_{start} and the time to complete charging as t_{end}, we can get the battery energy of EV v after charging, $\eta(t_{end})$, as below:

$$\eta(t_{end}) = \eta(t_{start}) + \int_{t_{start}}^{t_{end}} \lambda \Psi_v \, d\tau, \tag{2}$$

where $\eta(t_{start})$ means the battery energy capacity of EV at t_{start} time.

For each CS $s \in \mathcal{S}$, we assume it can provide $\mathcal{E}_{sv}(t)$ at each time slot t to EV v. To indicate whether EV v is charged by CS s, a binary variable decision, $\beta_{sv}(t)$, is introduced as follows,

$$\beta_{sv}(t) = \begin{cases} 1, & \text{EV } v \text{ is charged by CS } s, \\ 0, & \text{otherwise.} \end{cases} \tag{3}$$

Therefore, the energy demand of each CS, $\mathcal{E}_s^{\text{dem}}(t)$, can be given as below:

$$\mathcal{E}_s^{dem}(t) = \sum_{v}^{|\mathcal{V}|} \beta_{sv}(t) \mathcal{E}_{sv}(t), \tag{4}$$

III. Energy Demand Prediction with the Proposed LSTM-adopted FL

In this work, the objective is to predict the energy demand of each distributed CS. Considering the demand data of each CS is time-varying and privacy-sensitive, LSTM-adopted FL is used since it does not need to collect data centralized, as shown in Fig. 2. In particular, *FedAvg* [10] is adopted in this work. Moreover, each CS is considered as a client in FL setting and the central system is taken into account playing the role of model aggregation.

The procedure of the proposed LSTM-adopted FL approach can be summarized as follows: the central system generates an initial LSTM model (i.e., global model ω), which is initialized by a random value. Then this initial global model will be distributed to each cs $s \in \mathcal{S}$. With the received model, each CS will train its own dataset $\mathcal{D}^s = \{\mathcal{E}_s^{dem}(t), t \in \mathcal{T}\}$. Afterward, the updated model weight of each CS will be submitted to the central system for model aggregation. It is worth nothing that the goal of the proposed method is to minimize the following function [10]:

$$\min_{\boldsymbol{\omega}} \quad f(\omega) = \sum_{s=1}^{|\mathcal{S}|} \frac{|\mathcal{D}^s|}{|\mathcal{D}|} F_s(\omega), \tag{5}$$

where, $F_s(\omega) = \frac{1}{|\mathcal{D}^s|} \Sigma_{\forall i \in \mathcal{D}^s} f_i(\omega)$, here, $f_i(\omega)$ is the user-specified loss function of ith data sample of CS s. Besides, $\mathcal{D}$ is the data of all the CSs. As for the global model ω, it can be defined as the following equation [11]:

$$\omega = \sum_{s=1}^{|\mathcal{S}|} \frac{|\mathcal{D}^s|}{|\mathcal{D}|} \omega_s, \tag{24}$$

where ω_s indicates the model weight of each CS.

IV. Simulation Result and Analysis

In this section, we illustrate the simulation results and analysis for the proposed LSTM-adopted FL framework, where Python and Tensorflow APIs are adopted to implement the proposed framework. Besides, as a case study, we consider 7 CSs, where each CS has two layers of LSTM. To evaluate the proposed framework, we leverage the real-world EV energy charging dataset which is gathered from [8]. In particular, for simplicity, we assume the maximum number of EVs at each time slot t is 300. Besides, we randomly assign these EVs for each CS. Further, we split the original EV energy demand data into a training dataset and a test dataset with a ratio of 7 : 3.

TABLE I: Error for Overall Test Dataset via the proposed LSTM-adopted FL

Error for Overall Test Dataset	Neuron Number of Each Layer	
	128	256
Huber Loss	0.0412	0.0359
MSE	0.0825	0.0717
RMSE	0.2872	0.2678
MAE	0.2510	0.2373

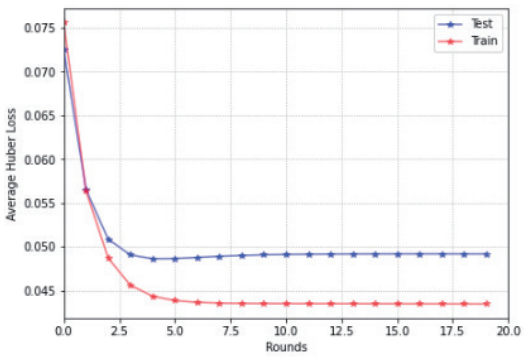


Fig. 3: Average huber loss for both training dataset and test dataset.

In Table I, we list the error for the overall dataset under different neuron number setting. In particular, when the neuron number of each LSTM layer is 128, the Huber loss, mean squared error (MSE), root mean squared error (RMSE) and mean absolute error (MAE) are 0.0412, 0.0825, 0.2872 and 0.2510, respectively. When the number of neurons is increased to 256, those error separately decreases to 0.0359, 0.0717, 0.2678 and 0.2373. Thus, we can infer the proposed LSTM-adopted FL with neuron number 256 for each layer outperforms the one with 128 neurons per layer.

Fig. 3 shows the average Huber loss for both the training dataset and test dataset accross all the CSs. It can be observed that the average huber loss is in decreasing trend. Specifically, in the beginning, the average huber loss is dramatically diminished. After training several round, the average huber loss is slowly declined.

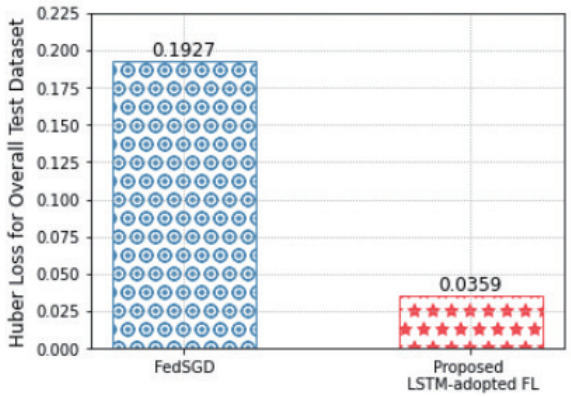


Fig. 4: Huber loss for the overall test dataset separately achieved by the FedSGD algorithm and the proposed LSTM-adopted FL approach.

Fig. 4 shows the Huber loss for the overall test dataset achieved by the FedSGD algorithm and the proposed LSTM-adopted FL method, respectively. Through this figure, it can be seen that the Huber loss achieved by the proposed LSTM-adopted FL method is lower than the FedSGD approach. Thus, we can draw a conclusion that the proposed LSTM-adopted FL outperforms the FedSGD.

V. Conclusion

In this paper, a system model of EV charging stations has been presented. The OCPP as the communication standard is taken into account by each charging station to eliminate the challenges resulting from the inconsistent communication protocols. In addition, the objective of this work is to predict the energy demand of each distributed charging station. To this end, a LSTM-adopted federated learning framework has been proposed, which is helpful for maintaining the data privacy and mitigating the communication cost since it does not need to collect the energy demand data of each charging station to the central system side. The simulation results indicate the proposed LSTM-adopted FL with 256 neurons for each layer is better than the one with 128 neurons per layer. In addition, the proposed LSTM-adopted FL is superior to the FedSGD algorithm since the Huber loss for the overall test dataset obtained by the proposed LSTM-adopted FL is smaller than the FedSGD algorithm.

References

[1] L. Zou, M. S. Munir, Y. K. Tun, S. Kang and C. S. Hong, "Intelligent EV Charging for Urban Prosumer Communities: An Auction and Multi-Agent Deep Reinforcement Learning Approach," *IEEE Transactions on Network and Service Management (Early Access)*, Mar. 2022, doi: 10.1109/TNSM.2022.3160210.

[2] M. Dabbaghjamanesh, A. Moeini and A. Kavousi-Fard, "Reinforcement Learning-Based Load Forecasting of Electric Vehicle Charging Station Using Q-Learning Technique," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 6, pp. 4229-4237, Jun. 2021.

[3] Open Charge Alliance, "OPEN CHARGE POINT PROTOCOL," [Online] https://www.openchargealliance.org/ (Visited on 12 Apr. 2022).

[4] H. Q. Le, M. N. H. Nguyen and C. S. Hong, "A Federated Learning for Image Classification with Heterogeneous Data," *Korea Software Congress 2020*, pp. 352-354, Dec. 2020 (in Korea).

[5] Y. L. Tun, K. Thar, C. M. Thwal and C. S. Hong, "Federated Learning Based Energy Demand Prediction of Individual Households," *Korea Computer Congress 2020*, pp. 299-301, Jul. 2020.

[6] Y. L. Tun, K. Thar, C. M. Thwal and C. S. Hong, "Federated Learning based Energy Demand Prediction with Clustered Aggregation," *2021 IEEE International Conference on Big Data and Smart Computing (BigComp)*, pp. 164-167, Jan. 2021.

[7] S. Orcioni and M. Conti, "EV Smart Charging with Advance Reservation Extension to the OCPP Standard," *Journal of Energies*, vol. 13, Jun. 2020.

[8] NREL Transforming ENERGY, "Impact of uncoordinated plug-in electric vehicle charging on residential power demand - supplementary data," https://data.nrel.gov/submissions/69 (Visited on 11 Apr. 2022).

[9] L. Zou and C. S. Hong, "Smart Energy Scheduling of B2V-enabled Prosumer Community as EVSE Based on SDN Network: A Deep Reinforcement Learning Approach," *Korea Software Congress 2020*, pp. 234-236, Dec. 2020 (in Korea).

[10] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," *Artificial Intelligence and Statistics*, pp. 1273–1282, 2017.

[11] S. Wang, T. Tuor, T. Salonidis, K. K. Leung, C. Makaya, T. He and K. Chan, "Adaptive Federated Learning in Resource Constrained Edge Computing Systems," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 6, pp. 1205-1221, Jun. 2019.

전기 수요 예측을 위한 연합학습 통신 비용 트레이드 오프

염성웅, 이미리내, 쉬바니, 김경백
전남대학교
yeomsw0421@gmail.com, alflsoquf1207@gmail.com, shivanikolekar@gmail.com,
kyungbaekkim@jnu.ac.kr

Communication Cost Trade-off in Federated Learning for Electrical Demand Prediction

Sungwoong Yeom, Mirinae Lee, Shivani Sanjay Kolekar, Kyungbaek Kim
Dept. Artificial Intelligence Convergence, Chonnam National University

요 약

사물 인터넷의 활성화로 인해 빌딩에서의 단기 에너지 소비 예측은 현대의 분산형 전력 시스템에 필수적인 역할을 한다. 사용자의 불규칙한 에너지 소비 패턴에 의한 높은 변동성을 예측하기 위해 시계열 딥러닝 신경망을 사용하는 혁신적인 전기 수요 예측 기법이 등장하였다. 그러나 각 빌딩에서 수집되는 데이터의 양이 다르기 때문에 특정 빌딩에 위치한 모델은 데이터의 양이 부족할 수 있다. 중앙 집중식 시스템은 불균등한 데이터를 가진 빌딩의 모델을 적절하게 학습하기 위해 에너지 소비 샘플 데이터들을 중앙 서버에서 수집하여 모델을 일반화시킨다. 하지만, 이 시스템은 클라이언트에서 서버로 송신되는 민감한 소비 이력 데이터로부터 개인 정보 보호가 보장되지 않을 수 있다. 또한, 이 시스템은 클라이언트의 네트워크 및 에너지 자원이 모두 제한되기 때문에 장기적 관점에서 네트워크의 대역폭에 악영향을 미칠 수 있다. 이 논문에서는 연합학습 프레임워크 환경의 중앙 서버와 클라이언트 사이에서 발생하는 통신 오버헤드와 전기 수요 예측 모델 성능에 대한 트레이드 오프를 연구한다. 제안된 연합학습 프레임워크는 모델 학습 시간 및 개인 정보 보호 측면에서 중앙 집중식 프레임워크를 능가할 수 있음을 보여준다.

Ⅰ. 서 론

재생 가능한 전력 생산 및 시장의 분산화가 증가함에 따라 빌딩 에너지 관리 시스템에서 지속 가능한 에너지 계획 및 생산을 위한 단기 에너지 소비 예측 연구가 활성화되고 있다 [1]. 하지만 빌딩 거주자들의 수와 이들이 사용하는 IoT(Internet of Things) 장치들의 수가 증가함에 따라 빌딩 내 에너지 수요가 불규칙해지고 있다 [2]. 최근 비선형적인 에너지 수요 예측 성능을 증가시키기 위해 시계열 딥러닝 기법을 사용하는 연구가 활성화되고 있다 [3]. 스마트 빌딩은 시계열 딥러닝 모델의 학습을 위해 구내 고급 계량 인프라(Advanced Metering Infrastructure)를 설치하여 상당한 양의 전기 소비 이력 데이터를 수집하지만 이는 모델을 학습하기에 충분하지 않을 수 있다. 빌딩 관리자는 충분하지 않은 데이터 양을 소유한 빌딩들을 위해 에너지 소비 이력 데이터를 다수의 빌딩들로부터 클라우드로 집계하는 중앙 집중식 접근 방식을 채택해왔다 [4][8]. 하지만, 수백만 개의 스마트 미터에서 수집되는 데이터가 모델 학습에 사용되는 경우 모델을 일반화하기 어렵고 계산 집약적이며 확장이 어려울 수 있다. 또한, 수백만 개의 스마트 미터로부터 수집되는 데이터에 의해 발생하는 대역폭으로 인해 상당한 통신 비용이 든다.

에지 컴퓨팅은 IoT와 같은 엔드 서비스 유저에게 보다 더 가까운 원격지 컴퓨터에 계산을 오프로딩(Offloading)하기 위해 도입된 분산 패러다임으로 클라우드 컴퓨팅을 네트워크 에지로 확장하여 속도, 효율성, 안정성, 개인정보 보호, 보안 및 확장성 측면에서 다양한 이점을 제공한다 [5]. 에지 컴퓨팅은 다수의 빌딩들의 AMI로부터 데이터 수집 및 확장할 때 발생하는 개인 정보 보호 및 확장성 문제를 효율적으로 극복하기 위한 훌륭한 솔루션이다. 그러나 딥러닝 기반 에너지 수요 예측 모델은 여러 빌딩 거주자로부터 데이터를 중앙 서버에서 수집하여 학습되는 경우에만 모델의 일반화를 보장하기 때문에 이는 데이터들이 분산된 상태로 유지되고 로컬에서 처리되어야 하는 엣지 컴퓨팅의 사례와 대조된다.

이러한 딥러닝과 엣지 컴퓨팅 사이의 간극을 해소하기 위해 연합학습이 제안되었다 [6]. 연합학습은 중앙 엔티티의 조정하에 모델 학습에 참여하는 장치들의 연합하에 글로벌 모델을 학습하는 분산 머신러닝 기법이다. 중앙 서버는 집계된 모델의 가중치를 통해 글로벌 딥러닝 모델(예: 전기 수요 예측을 위한 시계열 딥러닝 신경망)을 초기화하고 K개의 클라이언트와 공유한다. 즉, 중앙 서버는 각 클라이언트(빌딩 거주자 또는 빌딩)에게 글로벌 모델의 사본을 호스팅 한다. 이후 각 클라이언트는 로컬에서 모델을 학습시킨다. 이때, 로컬에 호스팅 되는 딥러닝 모델은 자체 데이터 세트를 사용한다. 이제 클라이언트는 원시 데이터를 송신하는 대신 로컬에서 업데이트된 모델의 가중치를 중앙 서버로 송신한다. 중앙 서버는 집계 단계에서 수신된 모델들의 가중치를 FedAVG[7]를 통해 평균화하여 글로벌 모델을 업데이트한다. 이 프로세스는 글로벌 모델의 손실이 수렴될 때까지 여러 라운드에 걸쳐 학습을 수행한다.

연합학습은 원시 데이터 대신 로컬에서 업데이트된 모델의 가중치를 송신함으로써 개인 정보를 보호하고 클라이언트 통신 비용을 줄일 수 있지만, 연합학습에 참여하는 클라이언트의 수가 증가한다면 모델의 가중치를 송수신하기 위해 발생하는 상당한 양의 링크 대역폭을 소비하기 때문에 통신 비용과 글로벌 모델의 최종 손실 값 사이의 균형을 완전히 이해하는 데 여전히 격차 있다. 또한, 링크 대역폭이 유한하기 때문에 연합학습은 각 라운드 수를 조정함으로써 리소스 제약을 설정해야 한다.

이 논문에서는 스마트 빌딩 환경을 위한 클라이언트에서 서버로 로컬 업데이트된 매개변수를 공유할 때 발생하는 통신 비용과 글로벌 모델을 최종 테스트 손실 간의 균형을 맞추기 위한 트레이드 오프를 제안한다. 우

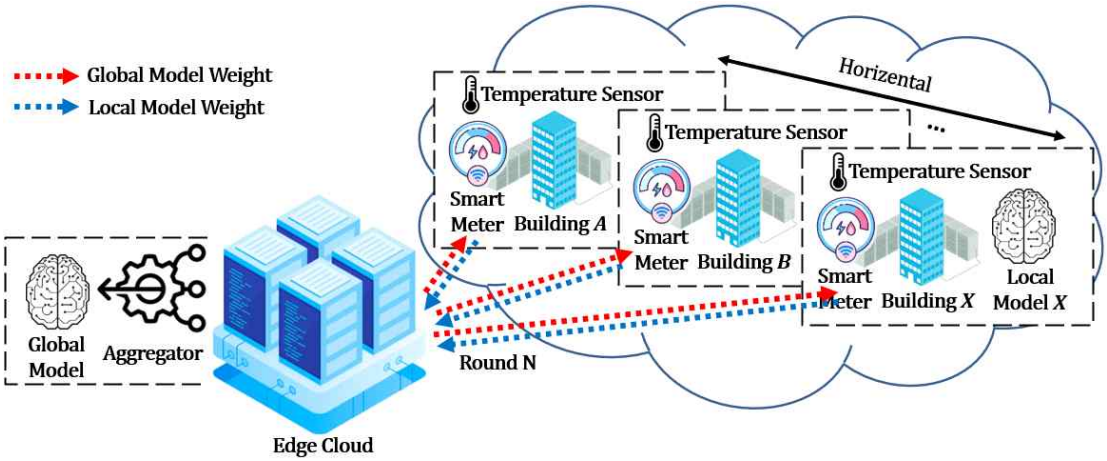


그림 1. 빌딩 에너지 수요 예측을 위한 연합학습 아키텍처

리는 연합학습에 참여하는 클라이언트 수, 모델의 정확도, 학습 시간 간의 균형을 고려하여 다양한 실험을 수행한다.

Ⅱ. 빌딩 에너지 수요 예측을 위한 연합학습 프레임워크

그림 1은 제안하는 빌딩 에너지 소비 예측을 위한 연합학습 프레임워크를 보여준다. 제안하는 아키텍처는 시계열 딥러닝 신경망 중 하나인 LSTM(Long Short-Term Memory) 모델을 각 빌딩에 위치시키고 이를 분산학습하여 빌딩의 에너지 소비를 정확하게 예측한다. 제안하는 아키텍처는 5가지로 구성된다. 먼저, 제로 에너지 빌딩은 태양열 패널 등을 통해 재생에너지를 생산 및 저장하고 빌딩 주거자들에게 에너지를 공급해준다. 부족한 에너지는 스마트 그리드에 의존할 수 있다. 빌딩 거주자들은 빌딩에서 다양한 IoT 장치들을 통해 전기를 소비하며 제로 에너지 빌딩에 요금을 청구한다. 스마트 미터는 빌딩 구내에 설치되어 단위시간당 소비되는 전기의 양을 측정하고 기록한다. 빌딩 에너지 예측 시스템은 제로 에너지 빌딩에 설치되며 이더넷 네트워크 연결을 통해 스마트 미터과 상대 습도, 온도를 캡처할 수 있는 실내 센서에 연결되어 캡처한 에너지 소비 이력 및 기후 데이터를 저장하는 역할을 한다. 또한, 이 시스템은 수집한 데이터를 LSTM 모델을 학습한다. 에지 컴퓨팅 노드는 제로 에너지 빌딩들을 관리하는 중앙 서버이다. 주요 역할은 여러 빌딩 에너지 예측 시스템에서 LSTM 모델이 학습된 대로 각 라운드가 끝날 때 로컬 모델을 수집하고 집계하는 것이다. 이 작업은 글로벌 모델 출력하며, 이 모델은 제로 에너지 빌딩들에게 다시 배포된다.

1. LSTM 기반 빌딩 에너지 수요 예측 기법

에너지 수요 예측 성능의 중요한 점은 에너지 수요 패턴에서 일별 계절성이 나타나는 것이다. 제안된 접근 방식은 에너지 수요를 추정하기 위해 시계열 신경망 모델인 LSTM을 사용한다. 그림 2는 제안된 LSTM 기반 전기 수요 예측 모델 아키텍처를 나타낸다. 이 모델은 3개의 LSTM 레이어와 3개의 Dense 레이어로 구성된다. 이 세 개의 Dense 계층 중 처음 두 계층은 ReLU(Recified Linear Unit) 활성화 함수를 사용하고 마지막 계층은 선형 활성화 함수를 사용한다. 각 레이어는 10개의 노드를 포함한다. 에너지 수요는 하루 동안 일정한 시간 간격으로 관찰된다. 관찰된 에너지 수요에 대한 예측의 안정성을 보장하기 위해 제안된 LSTM 모델에 대한 입력 벡터가 생성된다. 입력 벡터는 시별로 관찰되는 전기 수요, 실내 온도, 실내 습도, 월별 인덱스, 시별 인덱스, 요일 유형 세 가지 특성으로 구성된다. 제안하는 LSTM 모델은전기 수요를 예측하기 위해 입력

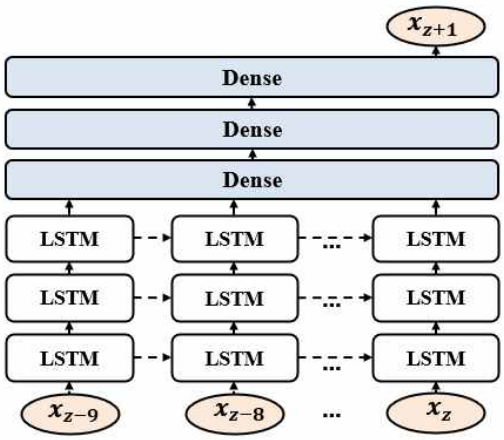


그림 2. LSTM 기반 빌딩 에너지 수요 예측 모델 아키텍처

벡터로 학습한다. 구체적으로 제안하는 LSTM 모델은 특정 시간부터 9시간 전까지 10개의 연속된 에너지 수요 정보를 사용하여 다음 1시간 후에 대한 에너지 수요를 예측한다.

제안하는 모델의 입력 벡터는 6가지 도메인으로 구성된다. 입력 벡터의 첫 번째 도메인은 전기 수요이다. 전기 수요 패턴은 사람의 행동에 영향을 받는다. 예를 들어, 사람에게 쾌적한 실내의 온도 및 습도를 맞추기 위해 에너지를 사용할 수 있다. 즉, 전기 수요는 일별, 주별, 월별 등 복잡한 계절성이 나타난다. 입력 벡터의 두 번째 및 세 번째 도메인은 실내 온도 및 상대 습도이다. 실내 온도 및 상대 습도 또한 복잡한 계절성이 나타난다. 복잡한 계절성 중 일별 및 주별 계절성은 단기 전기 예측에 큰 영향을 미칠 수 있다. 우리는 STL 분해 기법[11]을 통해 전기 수요, 실내 온도 및 상대 습도로부터 일별 및 주별 계절성을 분해하고 이를 입력 벡터로 사용한다. 입력 벡터의 네 번째 도메인은 월별 인덱스이다. 월별 인덱스는 1에서 12 사이의 값을 갖는다. 입력 벡터의 다섯 번째 도메인은 시별 인덱스이다. 1에서 24 사이의 값을 갖는다. 마지막으로, 입력 벡터의 여섯 번째 도메인은 요일 유형이다. 요일 유형은 요일별 전기 수요 간의 관계를 표현하기 위해 공휴일을 포함한 8가지의 범주를 고려하여 원-핫 인코딩을 통해 임베딩한다. 결과적으로 전기 수요 예측을 위한 LSTM 모델의 입력벡터의 길이는 19이다. 제안하는 LSTM 모델은 빌딩 에너지 관리 시스템에 설치된다.

2. 빌딩 에너지 수요 예측을 위한 FedAvg

연합학습은 각 빌딩의 데이터 샘플 수와 관계없이 모델을 공동으로 학습할 수 있도록 제안되었다. 에지 컴퓨팅 노드은 글로벌 모델을 초기화하고 연합학습에 참여할 빌딩들 S에게 초기화된 글로벌 모델의 가중치 w_0를 보낸다. 각 빌딩의 에너지 예측 시스템은 모델을 학습하기 위해 학습률 η 및 배치크기 b와 같은 하이퍼파라미터를 초기화하고 전달받은 모델 가중치를 업데이트한다. 라운드 t에서 학습률 η 및 배치크기 b를 사용하여 학습한 빌딩 i 의 모델 가중치 업데이트에 대한 수식은 아래와 같다.

$$w_t^{s_i} = w_t^g - \eta \nabla loss(w;b) \quad (1)$$

학습된 빌딩 i의 모델 가중치 $w_t^{s_i}$는 엣지 컴퓨팅 노드로 전송된다. 엣지 컴퓨팅 노드에서는 n개의 빌딩들로부터 업데이트된 가중치들 $w_t^{s_1},\ldots,w_t^{s_n}$을 집계하고 이를 FedAvg 알고리즘[7]을 통해 학습한다.

$$w_t^g = \sum_{s_i \in S} \frac{|x_{s_i}|}{\sum_{s_j \in S} |x_{s_j}|} w_t^{s_i} \quad (2)$$

이때, x_{s_i}는 빌딩 i에 데이터 셋의 크기를 의미하며 글로벌 모델의 가중치 w_t^g를 FedAvg 사용하여 평균화한다.

Ⅲ. 검증

1. 실험 설정

이 장에서는 제안된 빌딩 수요 예측을 위한 연합학습(Federated Learning)의 성능을 검증하기 위해 중앙 집중식 학습(Centralized Learning)을 비교한다. 우리는 건물 에너지 시뮬레이터인 CitySim[0]에 의해 미리 계산된 CityLearn[10]의 빌딩 전기 수요 데이터 셋을 실험에 사용한다. CityLearn 환경은 4개의 익명화된 기후 구역과 기후 구역별로 9개의 건물 클러스터로 구성되어 있다. 각 빌딩 데이터 셋은 1년동안 1시간 단위로 측정된 전기 수요 데이터로 구성된다. 우리는 이중 첫 번째 기후 구역에 위치한 7개의 빌딩 데이터 셋을 사용하여 테스트베드 실험을 수행한다. 이 실험은 2개의 NVIDIA GeForce RTX 2080 SUPER가 설치된 머신에서 도커 컨테이너를 기반으로 1개의 MongoDB 서버, 1개의 Chief 노드, 그리고 7개의 Worker 노드로 구성된 클러스터를 통해 수행된다. 표 1은 각 빌딩 데이터에 대한 평균 전기 수요, 평균 실내온도, 평균 상대 습도를 보여준다. 이 빌딩의 전기 수요는 실내 습도 및 온도에 따라 달라질 수 있으며 빌딩별로 위치한 LSTM 모델은 서로 다른 기후 및 전기 수요의 패턴을 학습하여 연합학습에 영향을 미칠 수 있다. 각 데이터 셋의 첫 10개월은 LSTM 모델을 학습하는데 사용하고 다음 2개월은 테스트를 위해 사용한다. LSTM 모델 학습을 위해 Adam Optimizer와 크기가 70인 배치를 사용하였다. 우리는 RMSE(Root Mean Square Error)를 사용하여 연합학습과 중앙 집중식 학습의 성능을 비교하였다.

2. 평가결과

그림 5는 중앙 집중식 학습에서 주기별로 전송되는 데이터에 의해 소요되는 파일 크기와 연합학습에서 LSTM 모델의 가중치가 송수신에 소요되는 파일 크기에 대한 비교를 보여준다. 이때, 이 실험은 단일 Worker 노드에서 수행되었다. 중앙 접근식 학습에서 1년 동안 1시간 단위로 클라이언트에서 중앙 서버로 보내지는 데이터의 총 양은 약 1478KB이고 이는 연합학습에서 약 20 라운드 동안 소요되는 데이터의 총 양과 같다. 따라서,

	Avg. Equipment Electric Power [kWh]	Avg. Indoor Temperature [C]	Avg. Relative Humidity [%]
Building_1	24.83	23.34	46.66
Building_2	24.89	40.81	8.83
Building_3	23.09	54.85	6.42
Building_4	23.01	58.22	4.22
Building_5	23.13	52.32	11.34
Building_6	22.54	52.29	10.83
Building_7	23.67	50.46	11.49

표 1. 빌딩의 전기 수요 데이터 셋

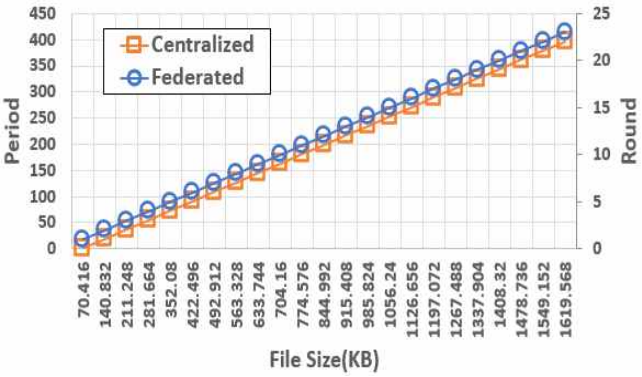


그림 5. 중앙 집중식 학습의 주기별로 전송되는 전기 수요 데이터에 대한 파일 크기와 연합학습의 라운드별로 공유되는 LSTM 모델의 가중치에 해한 파일 크기 비교

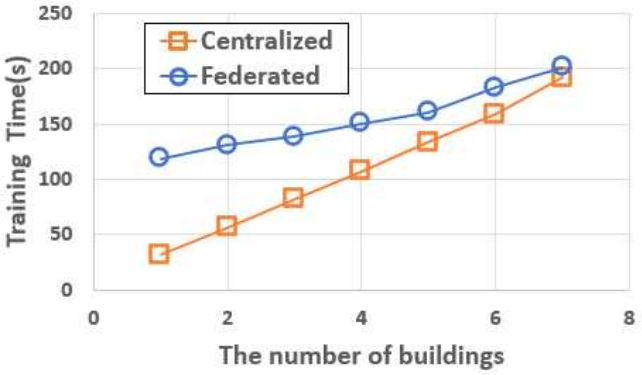


그림 6. 빌딩 수에 따른 중앙 집중식 학습과 연합학습에 소요되는 학습 시간 비교

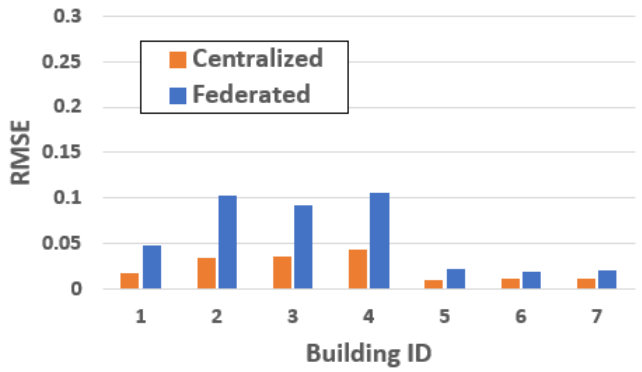


그림 7. 빌딩 에너지 수요 예측을 위한 중앙 집중식 학습 모델과 연합학습 모델의 빌딩별 RMSE 비교

이 실험에서 연합학습의 라운드는 20으로 설정한다. 하지만, 중앙 집중식 학습과 연합학습은 참여하는 Worker 노드의 개수가 증가함에 따라 학습 시간이 길어질 수 있다.

그림 6은 각 모델 학습에 참여하는 빌딩의 수가 증가함에 따라 소요되는 학습 시간을 비교한다. 연합학습에 소요되는 학습 시간은 참여하는 Worker 노드의 수가 적을수록 중앙 집중식 학습에 소요되는 학습 시간에 비해 크다. 하지만 빌딩 수에 따른 연합학습에 소요되는 시간의 증가율은 중앙 집중식 학습에 소요되는 시간의 증가율에 비해 적기 때문에 빌딩의 수가 증가할수록 연합학습의 총 소요시간은 중앙 집중식 학습의 총 소요시간에 비해 적다. 제안하는 실험환경에서는 학습에 참여하는 빌딩의 수가 7개 일 때 두 그래프가 교차한다. 따라서, 이 실험에서 연합학습에 참여하는 Worker 노드 수는 7개로 설정한다. 우리는 이러한 환경에서 중앙 집중식 학습의 RMSE와 연합학습의 RMSE를 통해 성능을 비교한다.

그림 7은 빌딩 에너지 수요 예측을 위해 학습된 중앙 집중식 학습 모델과 연합학습 모델의 RMSE를 비교한다. 중앙 집중식 학습 모델은 학습에 참여한 빌딩의 기후 및 전기 수요 데이터들을 집계하고 다양한 패턴을 학습하기 때문에 각 빌딩에서 낮은 RMSE를 보여준다. 반면에 연합학습 모델은 로컬에서 학습된 모델들의 가중치를 평균화하기 때문에 다른 패턴의 데이터를 학습한 모델의 가중치가 연합학습에 참여한다면 일부 빌딩에 위치한 모델의 RMSE가 높아진다. 빌딩 1,2,3,4에서 연합학습 모델의 RMSE는 중앙 집중식 학습 모델의 RMSE가 낮다. 하지만, 빌딩 5,6,7에서 연합학습 모델의 RMSE와 중앙 집중식 학습 모델의 RMSE는 비슷하다. 즉, 빌딩 1,2,3,4의 데이터 소비 패턴과 빌딩 5.6,7의 데이터 소비 패턴이 다름을 알 수 있다. 이 두 군집은 서로의 학습을 방해할 수 있다.

V. 결론

이 논문에서 빌딩에서 효과적인 단기 전기 수요 예측을 위해 연합학습 프레임워크를 제안하였다. 우리는 제안된 프레임워크의 성능을 평가하기 위해 수집된 방대한 양의 데이터를 사용하여 LSTM 모델이 중앙 서버에서 학습되는 중앙 집중식 프레임워크와 비교하였다. 결과적으로 우리의 제안하는 프레임워크가 중앙 집중식 프레임워크와 부분적으로 비슷한 성능을 보여주지만 모델 학습 시간 및 개인 정보 보호 측면에서 중앙 집중식 프레임워크를 능가할 수 있음을 보여준다. 더욱이 전기 소비 이력이 1시간 이하의 단위로 측정한다면 통신 오버헤드 또한 줄일 수 있음을 보여준다. 하지만, 다른 소비 패턴을 가진 빌딩 데이터를 학습한 모델의 가중치를 연합학습에 참여시키면 모델의 성능이 낮아질 수 있다. 차후에 전기 수요 예측을 위한 연합학습의 성능을 향상시키기 위한 연합 클러스터링에 대한 연구를 진행하고자 한다.

ACKNOWLEDGMENT

이 논문은 2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임"(IITP-2019-0-01343).

참 고 문 헌

[1] A. R. Khan, A. Mahmood, A. Safdar, Z. A. Khan and N. A. Khan, "Load forecasting dynamic pricing and DSM in smart grid: A review", Renew. Sustain. Energy Rev., vol. 54, pp. 1311-1322, Feb. 2016.

[2] Y. Peng, Y. Wang, X. Lu, H. Li, D. Shi, Z. Wang, et al., "Short-term load forecasting at different aggregation levels with predictability analysis", Proc. IEEE Innov. Smart Grid Technol. Asia (ISGT Asia), pp. 3385-3390, May 2019.

[3] Wang, Jian Qi, Yu Du, and Jing Wang. "LSTM based long-term energy consumption prediction with periodicity." Energy 197 (2020): 117197.

[4] P. Zhang, X. Wu, X. Wang and S. Bi, "Short-term load forecasting based on big data technologies", CSEE J. Power Energy Syst., vol. 1, no. 3, pp. 59-67, Sep. 2015.

[5] W. Z. Khan, E. Ahmed, S. Hakak, I. Yaqoob and A. Ahmed, "Edge computing: A survey", Future Gener. Comput. Syst., vol. 97, pp. 219-235, Aug. 2019.

[6] B. McMahan, E. Moore, D. Ramage, S. Hampson and B. A. Y. Arcas, "Communication-efficient learning of deep networks from decentralized data", Proc. Int. Conf. Artif. Intell. Statist., pp. 1273-1282, 2017.

[7] Li, Xiang, et al. "On the convergence of fedavg on non-iid data." arXiv preprint arXiv:1907.02189 (2019).

[8] Global Smart Meters Market－Growth Trends Forecasts (2020－2025), Jan. 2021, [online] Available: https://tinyurl.com/y4ujl8f3

[9] Vázquez-Canteli, José R., et al. "CityLearn v1. 0: An OpenAI gym environment for demand response with deep reinforcement learning." Proceedings of the 6th ACM International Conference on Systems for Energy-Efficient Buildings, Cities, and Transportation. 2019.

[10] Robinson, Darren, et al. "CitySim: Comprehensive micro-simulation of resource flows for sustainable urban planning." Proceedings of the Eleventh International IBPSA Conference. No. CONF. 2009.

[11] Cleveland, Robert B., et al. "STL: A seasonal-trend decomposition." J. Off. Stat 6.1 (1990): 3-73.

영상회의 관리를 위한 그래프 신경망 활용 방안에 관한 연구

유상우 [1], 고경찬 [2], 홍원기 [2]

포항공과대학교 인공지능대학원 [1]
포항공과대학교 컴퓨터공학과 [2]

{rswoo, kkc90, jwkhong}@postech.ac.kr

A Study on the Application Method of Graph Neural Network for Video Conferencing Management

Sangwoo Ryu[1], Kyungchan Ko[2], James Wonk-Ki Hong[2]
Graduate School of Artificial Intelligence, POSTECH[1]
Department of Computer Science and Engineering, POSTECH[2]

요 약

안정적인 영상 회의 제공을 위해 인공지능을 이용한 영상 회의 관리 기술이 다양하게 연구되고 있다. 인공지능 모델에서 높은 성능을 끌어내기 위해서는 수행하려고 하는 작업에 맞도록 적절한 표현 방식을 선택해 모델을 학습을 시키는 것이 중요하다. 따라서 영상 회의 관리를 위해서는 영상 회의의 특성을 고려해 이 특성들을 반영할 수 있는 적절한 표현 방식을 선택할 필요가 있다. 본 논문에서는 영상 회의의 표현 방식으로 그래프를 선택하고 왜 그래프가 적절한 표현 방식인지를 설명한다. 또한 그래프를 이용해 영상 회의를 표현하는 모델링 방법을 소개하고, 이를 어떻게 활용할 수 있을지에 관한 활용 방안을 제시한다. 마지막으로 이를 증명, 이용, 개선할 수 있는 연구 방향을 제시한다.

Ⅰ. 서 론

영상 회의는 서로 다른 지역, 시간대의 사람들 간 효율적인 업무를 할 수 있도록 도와준다. 이런 영상 회의 서비스는 코로나-19 이후 비대면 업무가 늘어나며 사용량이 급증하였다. 대표적인 영상 회의 플랫폼으로는 Zoom [1], Webex [2], Google Meet [3], Vmeeting [14] 등이 있으며, 이런 영상 회의 서비스 제공자는 고객들에게 안정적이고 높은 품질의 서비스를 제공하여 고객을 확보하기 위해 다양한 관리 기술들을 연구하고 부가 기능들을 개발한다.

이와 같은 관리 기술, 기능들은 더 좋은 성능을 내기 위해 인공지능을 이용한 알고리즘을 사용하기도 한다. 인공지능을 이용해서 영상 회의를 개선하기 위해서는 인공지능 모델에 입력으로 들어가는 영상 회의를 어떻게 표현하고 모델링할 지가 중요한 이슈가 된다. 이를 위해서는 영상 회의의 특징을 파악할 필요가 있다. 영상 회의에서는 비디오 스트리밍 서비스와 달리 영상/음성 트래픽이 단방향으로 전달되는 것이 아닌 한 사용자에서 다른 다수의 사용자로 직접 전달되거나, 한 사용자의 트래픽이 중앙 서버를 거쳐 다른 사용자들로 분배되기도 한다. 또한 사용자의 수가 시간에 따라서 달라질 수 있으며, 적으면 2 명부터, 많으면 수백, 수천명까지 존재할 수 있다. 따라서 영상 회의의 상태를 이해하기 위해서는 사용자들, 서버들과의 관계와 그 사이에 전달되는 메시지들을 명확하게 파악할 필요가 있다. 또한 적절한 대역폭 배분을 위해 서버 전체의 상태를 판단할 필요성도 생긴다.

N 차원 배열을 이용하는 이미지와 같은 표현 방식은 이미 많이 연구가 된 표현 방식 중 하나이다. 이미지를 주로 입력으로 사용하는 컨볼루션 신경망 (Convolutional Neural Network, CNN) [4]의 경우에는 주로 일정한 이미지 크기를 이용해 훈련, 추론을 수행하며, 다른 크기의 이미지를 사용하고자 할 때는 이미지의 크기를 조정하거나, 패딩 (padding)을 이용해 크기를 맞춰준다. 하지만 영상회의를 이미지와 유사한 형태로 표현하려는 경우, 사용자 수에 따라 크기가 쉽게 달라질 수 있어 크기를 미리 정해 놓기 힘들기 때문에 영상 회의를 표현하기 위해서는 이 방법들이 적합하지 않다.

그래프는 노드들과 해당 노드들 사이의 관계를 표현할 수 있는 데이터 구조로, 복잡한 관계를 표현할 필요성이 있는 소셜 네트워크, 자연과학 등 여러 분야에서 사용되고 있다 [15]. 따라서 이 연구에서는 그래프를 이용해 영상 회의를 표현하는 방식을 제시한다. 그래프를 이용했을 때의 장점은 다음과 같다. 1) 사용자-사용자, 사용자-서버 등 영상 회의를 구성하는 구성 요소들 간 관계를 표현하기가 쉽다. 2) 사용자 수가 자주 변하는 영상 회의의 특성에 맞게 그래프의 구조를 쉽게 변화시킬 수 있다.

본 논문에서는 먼저 영상 회의 관리를 위해 기계학습을 사용한 연구들과 그래프 신경망에 대해

소개하고, 영상 회의에 그래프 신경망을 사용할 수 있도록 영상 회의를 그래프로 표현하는 모델링 방안을 제시한다. 다음으로 그래프로 표현된 영상 회의를 어떤 문제를 해결하기 위해 사용할 수 있을지에 관한 활용 방안들과 관련된 아이디어 및 연구들을 제시한다. 마지막으로 이 논문의 한계점과 이를 개선하기 위한 향후 연구를 제시한다.

Ⅱ. 배경

이 장에서는 기존 연구에서 영상 회의에 기계 학습을 사용한 사례들과 어떤 방식으로 사용했는지, 이 논문과 어떻게 다른지 알아보고, 이 논문에서 사용하려는 그래프 신경망에 대한 선행 연구들을 설명한다.

1) 영상회의에서의 기계 학습

영상 회의 관리를 위해 기계 학습을 사용하는 연구가 많이 이루어졌다. Concerto [5]는 1 대 1 영상통화에서 최적 전송 비트레이트를 선택하기 위해 모방 학습(Imitation Learning)을 사용하였다. 손실률, 지연 시간 등 현재 네트워크 및 이전 상태를 표현하기 위해 각 상태 별로 고정된 크기의 1 차원 배열을 만들어 신경망의 입력으로 사용하였다. Concerto 의 후속 연구인 OnRL [6]에서는 같은 문제를 해결하기 위해 강화 학습을 사용하였으며, 각 상태 배열을 하나의 배열로 합쳐서 신경망의 입력으로 사용하였다. Concerto 와 OnRL 은 1 대 1 영상통화의 상황을 가정하고 개개인에 대한 전송 비트레이트를 선택하기 때문에 개인의 상태만 이용하여 고정된 크기의 입력을 만들 수 있었다. 하지만 본 논문에서는 다대다 영상회의 사용을 가정하고, 영상 회의 전체, 또는 사용자 간 관계를 고려하는 것을 목적으로 하기 때문에 해당 논문에서 사용한 방법을 사용할 수 없었다.

2) 그래프 및 그래프 신경망

그래프 신경망에 관한 연구는 지난 20 년 동안 다양한 연구가 이루어졌으며, Wu 등[7]은 기계 학습에서 그래프 신경망에 대해서 역사, 분류, 활용 분야 등을 모두 포함하는 포괄적인 리뷰를 작성하였다. 해당 논문에서는 사용 목적 및 방식에 따라 그래프 신경망을 RecGNN (순환 그래프 신경망), ConvGNN (컨볼루션 그래프 신경망), GAE (그래프 오토 인코더), STGNN (공간-시간 그래프 신경망)으로 분류하여 관련 연구를 소개하였다. 또한 그래프를 노드, 엣지, 그래프 중 어떤 단위로 분석할 수 있는지, 지도/비지도학습 각각을 이용한 그래프 모델 훈련에 관해서도 설명한다. 이처럼 그래프에 기계 학습 기법을 효율적이고 쉽게 적용하기 위해 임베딩 (Embedding) 방법을 이용해 벡터로 변환하여 사용하는데, 그래프의 각 노드를 변환하는 노드 임베딩과 그래프 전체를 벡터로 변환하는 그래프 임베딩과 같은 그래프 표현 방식 자체에 관한 연구들도 이루어졌다. 그래프는 다양한 분야에서 활용될 수 있다. 컴퓨터 비전에서는 이미지에 존재하는 물체들의 관계를 나타내기 위해 장면 그래프(Scene Graph)를 만들거나 [8], 행동 인지를 위해 사람의 골격을 그래프로 모델링하기도 한다 [9]. 자연어 처리에서는 단어 간 상호 관계를 표현하기 위해 그래프를 사용한다. 컴퓨터과학/공학 이외의 분야에서도 교통량 예측을 위해 도로 네트워크를 그래프로 표현하는 방법 [10], 신약 개발, 분자 특성 예측 등을 위해 분자 구조를 그래프로 모델링하는 방법 [11] 등이 연구되었다.

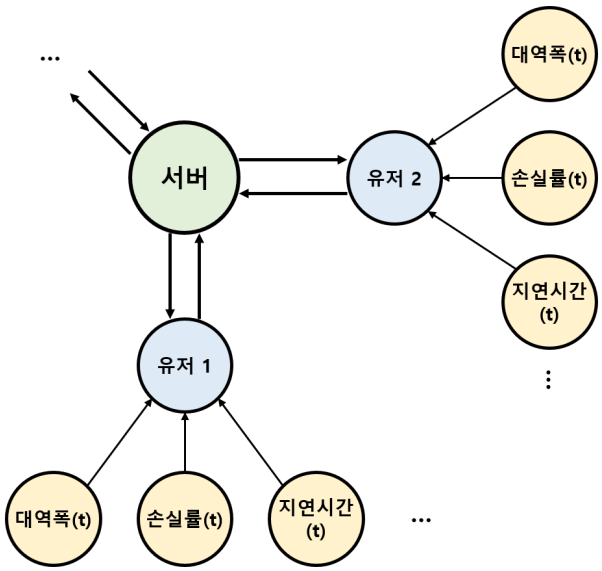


그림 1. 영상 회의 그래프 모델링. 영상 회의 상태를 노드로 표현하는 경우.

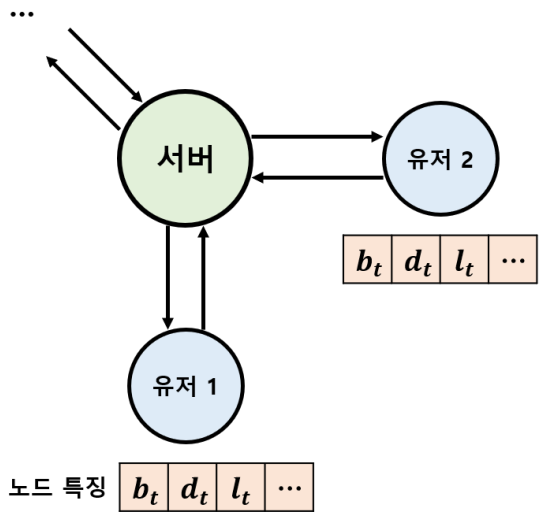


그림 2. 영상 회의 그래프 모델링. 영상 회의 상태를 노드 특징으로 표현하는 경우.

Ⅲ. 그래프 모델링 방안

영상 회의의 상태를 그래프로 표현하는 방법은 사용 목적에 따라 다양하다. 그림 1 은 대표적인 영상 회의 그래프 표현 예시를 보여준다. 먼저 하나의 회의실을 관리하는 서버 노드가 존재하고, 영상 회의에 참가하는 참가자들이 각각을 노드로 설정할 수 있다. 영상 회의의 모든 트래픽이 서버를 통해 전달되는 방식의 경우, 그림 n 과 같이 서버 노드와 유저 노드가 엣지로 연결되어 있으며, 대역폭과 같은 정보를 가질 수 있다. 방향성을 가진 엣지 (Directed Edge)를 사용할 경우, 업로드/다운로드 대역폭을 각각 표현할 수 있다. 영상 회의의 트래픽이 서버를 거치지 않고 P2P (Peer-to-Peer)를 기반으로 전달되는 경우, 서버 노드와 연결되지 않고, 다른 사용자 노드와 직접 연결될 수 있다. 사용자의 상태는 사용자와 연결되는 새로운 상태 노드를

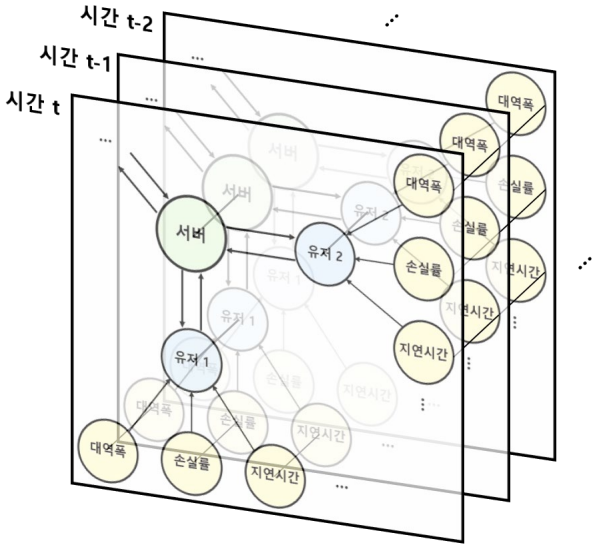


그림 3. STGNN 사용을 위한 그래프 모델링

만들어 표현하거나, 그림 2 와 같이 노드 특징 (node feature)의 형태로 갖도록 설계할 수도 있다. 유저의 상태의 예시로는 현재 대역폭, 손실률, 지연시간, 대역폭 변동 정도 등이 있다. 그림 1 과 같이 새로운 노드를 이용해 표현하는 경우, 해당 노드가 다른 노드들과 메시지를 주고받을 수 있게 되어 유저들의 상태와 해당 특징들의 관계를 더 명확하게 파악할 수 있다는 장점이 있다. 그림 2 와 같이 표현하는 경우, 해당 특징들이 유저 노드를 표현하기 위한 수단으로 사용된다. 또한 두 경우에 실제로 인공지능 모델의 입력으로 사용되는 방식이 달라 (각각 인접 행렬, 특징 행렬의 형태로 사용), 이에 따라 다른 결과를 보여줄 것이다. 이와 같은 기본 형태의 그래프를 기반으로 필요에 따라 다양한 형태로 변형을 할 수 있다. 먼저 영상 회의 서버에서 여러 회의를 관리하는 경우 여러 개의 서버 노드와 전체 관리 노드를 생성해 연결하는 것이 가능하다. 또한 시간적 정보가 필요하다면 그림 3 과 같이 일정 시간 간격마다 해당 시간에서의 상태를 나타내는 그래프들을 그리고, 각 그래프들의 같은 정보를 나타내는 노드들끼리 연결하는 STGNN[9, 10]와 같은 형태의 네트워크를 사용할 수 있다.

서버 노드, 유저 노드, 상태 노드 등 여러 종류의 노드를 제시했는데, 각 노드들을 모두 같은 종류로 생각하는 동종 (Homogeneous) 그래프로 표현할 수도 있고, 각 노드들을 역할에 따라 다른 종류로 생각하는 이종 (Heterogeneous) 그래프로 표현하는 것도 선택할 수 있다.

이런 방식으로 영상 회의를 그래프로 모델링하는 경우, 다른 유저와의 상호작용으로 이루어진다는 영상 회의의 특징을 반영할 수 있다. 본인의 영상을 다른 유저들에게 보냄과 동시에, 다른 유저의 영상을 지속적으로 받아야 하기 때문에, 이 과정은 자신의 네트워크 뿐만 아니라 타인의 네트워크 상황에도 함께 영향을 받는다. 따라서 유저 간 유기적인 연결 관계와 그 특성들을 파악하는 것이 중요하고, 이를 잘 표현할 수 있는 그래프를 한 가지 표현 방식으로 고려할 수 있는 것이다.

Ⅳ. 활용 방안

이 장에서는 그래프로 표현한 영상 회의를 활용할 수 있는 방안을 설명한다. 또한 각 예시에 대해 사용할 수 있는 그래프 표현 방식의 예시를 소개한다.

1) 영상 회의 이상 탐지

영상 회의 이상을 탐지하는 작업은 두 가지 단위로로 구분을 할 수 있다. 먼저 회의실 단위로 보았을 때는, 어떤 회의실에서 진행되는 영상 회의의 현재 상태가 이상이 있는지를 판단하는 작업이다. 예를 들어 특정 회의실에 트래픽이 몰리거나, 다수 사용자들의 연결이 끊어지는 등의 이상 상태들이 가능하며, 그래프 분류 (Graph Classification)를 통해서 탐지하는 것이 가능하다. 이 경우 한 회의실에 대한 그래프 전체를 임베딩하여 사용할 수 있다. 다음으로 한 회의실 내에서 사용자 단위로 볼 수도 있다. 특정 사용자의 네트워크가 불안정하여 트래픽을 제대로 전송하지 못하거나, 다른 사용자의 트래픽을 제대로 받지 못하는 등 사용자 단위의 이상 여부를 탐지할 수 있다. 이 경우 사용자 노드와 다른 이웃 노드들과의 관계를 노드 임베딩을 이용해 변환하여 노드 분류 (Node Classification)를 수행할 수 있다.

이런 방식으로 영상 회의의 이상 상태를 미리 탐지한다면 서버 측면에서는 대역폭을 재분배하거나 서버 자원을 더 할당하는 등 필요한 조치를 미리 마련할 수 있다. 이에 따라 사용자는 안정적인 서비스를 제공받을 수 있게 된다.

2) 상황 별 맞춤 시스템

사용자들을 사용하는 네트워크 환경, 주 사용 패턴, 회의실의 유형 등을 이용해 사용자 및 회의실을 자동으로 분류해 상황 별로 맞춤 시스템을 제공할 수 있다. 예를 들어, 영상 회의를 학교 수업을 위해 이용하는 경우 주로 교수자의 영상 및 화면이 중요한 트래픽이 되고, 다른 사용자들의 트래픽은 상대적으로 낮은 트래픽과 중요도를 가진다. 마찬가지로 세미나 혹은 컨퍼런스로 이용할 경우에도 발표자와 질문자의 영상이 가장 중요하다고 볼 수 있다. 모든 사람의 카메라가 켜진 상태에서 진행되는 회의는 모든 사람이 비슷한 중요도를 가진다고 할 수 있다. 또한 어떤 사용자는 실외에서 무선 네트워크를 이용해 접속을 할 수 있고, 어떤 사람은 실내에서 유선 네트워크를 이용해 접속할 수 있는데, 이러한 주 사용 환경들을 그래프에서 노드 분석, 노드 간 메시지 흐름 분석 등을 통해 분류할 수 있다는 특징을 가진다. 이 작업은 첫 번째 예시인 영상회의 이상 탐지와 유사하게 구현이 가능하며, 사용자 별 시스템을 구축하려는 경우 사용자 노드 임베딩 및 분류를, 회의실 별 시스템을 구축하려는 경우 그래프 임베딩 및 분류를 사용할 수 있다.

3) 영상 회의 SFU 관리

영상 회의의 이상 상태를 탐지하는 것 이외에도 현재 상태를 파악하는 것 만으로도 의미 있는 작업들을 수행할 수 있다. 영상 회의의 트래픽이 중앙 서버를 경유해 전달되는 SFU (Selective Forwarding Unit) 방식 [12, 13]에서는 다른 사용자에게 영상을 전송할 때 해당 사용자의 네트워크 상태를 고려해 전송 비트레이트를 조정한다. 사용자가 끊김 없이 영상을 보기 위해서는 지연 시간이 적고 손실되는 데이터가 없어야 한다. 따라서 현재 상태에 따라 적절한 비트레이트의 영상을 보낼 필요가 있다. 영상 회의 그래프에서는 현재 어떤 사용자들에게 영상을 받거나 보내고 있는지, 현재

네트워크 상태는 어떤 지를 모두 파악할 수 있기 때문에 이를 이용하여 비트레이트를 선택하는 알고리즘을 디자인할 수 있다. 기계 학습을 이용해 비트레이트를 선택하는 이전 연구들[5, 6]과 유사하게, 현재 상태와 이전 상태들을 함께 볼 수 있도록 설계하여 시간의 흐름에 따른 변화 정보도 반영할 수 있으며, 그래프 모델링 방안에서 언급한 내용처럼 STGNN 을 사용하는 것이 한 예시가 될 수 있다.

Ⅴ. 결론 및 향후 연구

이 논문에서는 그래프의 특성이 영상 회의 관리에 왜 적합한지를 설명하고, 영상 회의의 개별 회의 및 전체 서버 상태를 그래프로 표현하기 위한 모델링 방법을 제시하였다. 또한 이렇게 그래프로 표현한 영상 회의를 어떻게 활용할 수 있는지에 대해 가능한 활용 방안들과 예시 표현 방법들을 제시하였다. 이를 통해 앞으로의 영상 회의 관리를 위한 기계 학습 사용 연구의 한 가지 방향을 제시할 것으로 기대한다.

다만 이를 위해서 해결해야하는 한계점이 몇 가지 존재한다. 먼저 영상 회의와 관련된 데이터가 부족하다는 점이다. 영상 회의의 네트워크는 열린 데이터가 많지 않고, 합성/재현 데이터를 만들기 위해서도 많은 노력이 필요해 사용할 수 있는 데이터셋이 많지 않다. 따라서 인공지능 모델을 학습시키기 위해 부족한 점이 많다고 볼 수 있다. 두 번째로 이 연구에서 제시하는 표현 방식을 실제로 인공지능 모델에 적용했을 때 어느 정도의 성능 변화를 이끌어낼 수 있을지 평가가 이루어져야 한다는 것이다. 이를 위해서는 이미 영상 회의를 타겟으로 구현된 인공지능 모델과 이를 재구현 할 수 있는 데이터셋 및 시뮬레이션 플랫폼이 모두 필요하여, 이와 관련된 연구가 모두 선행되어야 한다. 따라서 향후 연구로는 그래프 표현 방식의 성능을 평가하기 위하여 필요한 연구들을 순차적으로 수행하는 것을 계획하고 있으며, 또한 이 논문에서 제시한 표현 방식에서 나아가 이를 고도화하기 위해 영상회의 그래프 임베딩 방법을 연구하거나, 이를 위한 데이터 수집도 연구할 가치가 있다.

ACKNOWLEDGMENT

이 논문은 2022 년도 정부 (과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원 (2018-0-00749, 인공지능 기반 가상 네트워크 관리기술 개발)과 대학 ICT 연구센터육성지원사업의 연구결과로 수행되었음 (IITP-2022-2017-0-01633).

참 고 문 헌

[1] Zoom, https://zoom.us

[2] Webex, https://www.webex.com

[3] Google meet, https://meet.google.com

[4] Y. LeCun et al., “Convolutional networks for images, speech, and time series,” The handbook of brain theory and neural networks, vol. 3361, no. 10, p. 1995, 1995.

[5] Zhou, Anfu et al. "Learning to Coordinate Video Codec with Transport Protocol for Mobile Video Telephony." The 25th Annual International Conference on Mobile Computing and Networking. Association for Computing Machinery, 2019.

[6] H. Zhang et al., “Onrl: improving mobile video telephony via online reinforcement learning,” Proceedings of the 26th Annual International Conference on Mobile Computing and Networking, 2020, pp. 1– 14.

[7] Zonghan Wu, et al. "A Comprehensive Survey on Graph Neural Networks". IEEE Transactions on Neural Networks and Learning Systems 32. 1(2021): 4– 24.

[8] Xu, Danfei et al. "Scene Graph Generation by Iterative Message Passing." Computer Vision and Pattern Recognition (CVPR). 2017.

[9] Yan, Sijie et al., "Spatial temporal graph convolutional networks for skeleton-based action recognition," Thirty-Second AAAI Conference on Artificial Intelligence, 2018.

[10] Yu, Bing et al. "Spatio-Temporal Graph Convolutional Networks: A Deep Learning Framework for Traffic Forecasting." Proceedings of the 27th International Joint Conference on Artificial Intelligence. AAAI Press, 2018.

[11] Gilmer, Justin et al. "Neural Message Passing for Quantum Chemistry." Proceedings of the 34th International Conference on Machine Learning - Volume 70. JMLR.org, 2017.

[12] Petrangeli, Stefano et al. "Improving Quality and Scalability of WebRTC Video Collaboration Applications." Proceedings of the 9th ACM Multimedia Systems Conference. Association for Computing Machinery, 2018.

[13] Xhagjika, Vamis et al. "Load and Video Performance Patterns of a Cloud Based WebRTC Architecture." 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID). 2017.

[14] Vmeeting, https://vmeeting.io

[15] Zhou, Jie et al. "Graph Neural Networks: A Review of Methods and Applications." (2018).

네트워크 관리 시스템을 위한 계층 그래프 학습 모델

김희곤, 유재형, 홍원기
포항공과대학교 컴퓨터공학과

{sinjint, jihyoo78, jwkhong}@postech.ac.kr

The Hierarchical Graph Learning Model for Network Management

Hee Gon Kim, Jae Hyung Yoo, James Won Ki Hong
Department of Computer Science and Engineering, POSTECH

요 약

가상 네트워크 환경은 네트워크의 확장성을 증가시키고 유연한 변화가 가능하게 하였다. 이러한 변화에 힘입어 최근에는 가상 네트워크 환경에서 기계 학습을 이용한 네트워크 관리 방법이 주목받고 있다. 하지만 높은 주목에도 불구하고 큰 성과를 이루지 못하고 있어 본 논문에서는 해당 이유에 대해서 분석을 진행하고 해결 방안을 제시하였다. 본 논문은 기계 학습을 이용한 네트워크 관리 방법에 대해서 서술하고 규모가 큰 네트워크에서의 학습 난이도 증가를 지적하였다. 또한, 계층 그래프 학습 모델을 제안하여 네트워크 관리 모델의 학습 난이도를 낮추는 동시에 다양한 토폴로지에서 범용성을 가질 수 있는 기계 학습 모델을 제안하였다. 제안한 방법을 이용하면 네트워크 규모와 상관없이 기계 학습 모델이 높은 학습 성능을 가질 수 있다.

Ⅰ. 서 론

Software-Defined Networking (SDN) 과 Network Function Virtualization (NFV) 는 네트워크의 확장성을 증가시키고 유연한 변화가 가능하게 하였다[1]. SDN 컨트롤러와 NFV 관리 시스템을 통해서 네트워크 관리자는 네트워크 Orchestration 을 수행할 수 있게 되었으며 효율적인 자원 관리 및 높은 품질의 서비스를 제공할 수 있게 되었다.

기존의 네트워크 관리 모델은 네트워크 관리자의 오랜 경험에 의존하거나 Integer Linear Programming 혹은 휴리스틱 알고리즘을 이용하여 최적화를 시도하였다. 하지만 SDN/NFV 의 도입과 5G 네트워크와 같은 차세대 네트워크의 도입으로 네트워크는 규모가 더 거대해지고 더 빠른 시간 내에 관리 판단을 요구하게 되어 전통적인 관리 모델의 한계점이 드러나게 되었다.

기계학습(Machine Learning)은 차세대 네트워크 관리 모델로 주목을 받고 있다. 전통적인 관리 모델들은 관리 정책을 최적으로 생성하기 힘들거나 계산에 오랜 시간이 걸린다. 하지만, 기계 학습은 빠른 시간 내에 최적의 관리 정책을 생성할 수가 있다. 또한 기계 학습을 이용하는 것으로 사람의 개입이 필요 없는 자율 네트워크(Automated Network)를 도입할 수 있게 되었다[2].

기계 학습의 높은 주목에도 불구하고 실제 네트워크 관리에서의 기계 학습 모델의 도입은 매우 미미하다. 이것은 네트워크 관리라는 분야가 가지는 특수성에 의해서 발생한 결과이다[3]. 기계 학습 모델은 주어진 데이터를 바탕으로 데이터 간의 관계성을 학습하여 모델을 생성하게 되는데, 이때 데이터의 수 또는 관계성이 복잡하면 할수록 모델은 학습에 어려움을 겪게 된다. 네트워크 관리의 경우, 수많은 네트워크 데이터들을 이용하여 관리 모델을 학습하게 되는데, 이때 네트워크 규모가 증가하면 할수록 학습이 필요한 데이터가 기하급수적으로 증가하게 되어 기계 학습 모델이 학습을 하는데 어려움을 겪게 된다.

본 논문에서는 기계학습으로 네트워크 관리 모델을 학습할 때 고려해야할 요구사항들을 명시하며, 계층 그래프 모델을 이용하여 네트워크 관리 학습에서의 난이도를 대폭 낮추는 방법에 대하여 제안한다. 계층 그래프 학습 방법은 네트워크 관리 모델을 학습할 때, 전체 네트워크에 대해서 한번에 학습을 하지 않고, 네트워크를 계층별로 압축하여 학습을 진행하는 것을 의미한다.

Ⅱ. 본론

1) 기계 학습 기반 네트워크 관리

그림 1 은 네트워크 관리 학습 모델의 개념도이다.

네트워크 관리에 사용되는 데이터는 크게 네트워크 데이터와 트래픽 데이터로 구분할 수 있으며 주기적으로 수집되어 저장된다(①). 각 데이터는 아래와 같이 정의될 수 있다[4].

▶ 네트워크 정보
- 토폴로지 구조
- 개별 노드의 정보(CPU Cores, Memory 등)
- 개별 링크의 정보(최대 대역폭 등)
- 기타 비용(노드 운용 비용, 전력 소모 비용 등)

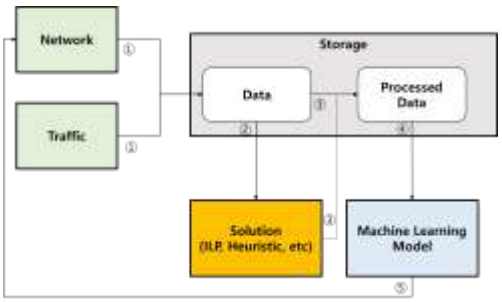


그림 1 학습 모델 개념도

▶ 트래픽 정보
- 트래픽의 출발지, 도착지 노드
- 트래픽의 요구 대역폭
- 트래픽의 최대 허용 지연 시간
- 트래픽 타입(서비스 종류, 정상/비정상 트래픽)

수집된 데이터들은 기계 학습이 모방할 관리 솔루션(ILP 또는 Heuristic 모델)에 입력되어 최적의 관리 정책을 생성하게 된다(②). 생성된 관리 정책은 정책 생성에 사용된 데이터와 쌍을 이루어 학습 데이터로 저장되며(③), 네트워크와 트래픽 데이터는 특성 데이터(Feature Data)가 되며 관리 정책은 라벨링 데이터 (Labeling Data)로 구성이 된다. 일련의 해당 과정(①~③)은 네트워크와 트래픽 데이터가 수집될 때 마다 반복한다. 만약, 관리 솔루션이 네트워크와 트래픽 데이터를 수집하는 것 보다 정책을 생성하는데 시간이 많이 소모되어 저장된 데이터가 많이 존재할 경우에는 가장 최근의 데이터에 대해서 관리 정책을 생성하도록 한다. 만약 기계 학습 모델이 시계열 학습 모델을 사용한다면 학습 데이터가 시계열 정보를 내포할 수 있도록 적절한 간격마다 데이터를 수집하고 관리정책을 생성할 수 있도록 한다. 학습데이터가 충분히 모아졌다면 기계학습 모델이 학습을 하여 관리 솔루션을 모방하게 된다(④). 기계 학습 모델이 성공적으로 관리 솔루션을 모방하게 된다면, ③번 과정을 거치지 않은 채 즉각적으로 네트워크와 트래픽 데이터에 대해 관리 정책을 생성하고 이를 네트워크에 반영시킨다(⑤). 만약, 기계 학습 모델의 성능이 감소하게 된다면 ①~③의 과정을 반복하여 학습 데이터를 수집하고 ④번 과정을 통해 기계 학습 모델을 재 학습시킨다.

2) 계층 그래프 학습 모델

기계 학습을 이용하여 네트워크 관리 모델을 학습할 때 존재하는 가장 큰 문제점은 관리 모델의 높은 학습 난이도 및 데이터의 비효율성이다. 가상 네트워크 장치(VNF: Virtual Network Function) 설치 문제를 네트워크 관리 문제의 예시로 든다면 해당 문제는 일반적인 기계학습 모델처럼 단순한 분류 모델 또는 예측 모델이 아니다[5]. VNF 설치 문제는 네트워크와 트래픽 데이터를 모두 고려하여 네트워크 상의 특정한 노드들에 특정한 VNF 들을 설치해야 한다. 예를 들어 네트워크 노드 수를 m, VNF 종류를 n 이라 하고 VNF 의 설치 여부만을 고려한다고 하면, VNF 설치 문제는 총 $2^{n}m$ 개의 결과를 가질 수가 있다. 여기에서 실제로 존재하는 제약조건(노드 별 존재하는 자원 제약조건, 설치할 VNF 의 개수)을 고려하면 문제는 더 복잡해진다.

기계 학습 모델은 네트워크에 존재하는 각 노드들의 상관관계 정보를 모두 파악하여야 한다. 해당 데이터는 인접 행렬(Adjacency Matrix)를 통해 표현할 수 있으나 희소 행렬로 표현이 되며 비효율적으로 학습이 수행되게 된다. 이러한 문제를 해결하기 위해서 최근에는 그래프 신경망 네트워크 (GNN: Graph Neural Network)을 이용하여 네트워크 데이터를 학습하는 방법들이 시도되고 있다. 이미지 탐색 문제에서 합성 곱 신경망 네트워크(CNN: Convolutional Neural Network)들이 데이터의 특징만을 추출하여 학습하는 방법과 같이 GNN 은 그래프 데이터의 특징을 추출하여 학습하도록 도와준다[6]. 네트워크 규모가 클 경우, GNN 을 사용하는 것으로 학습 데이터를 효율적으로 사용하고 학습 성능의 향상을 기대할 수 있다. 하지만, 관리 모델의 난이도는 줄일 수가 없는데, 이를 해결하기 위해 본 논문에서는 계층 그래프 학습 모델의 도입을 제시한다.

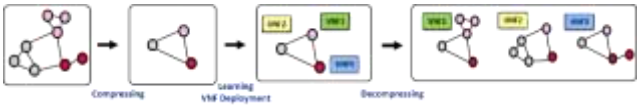


그림 2 그래프 학습 모델

그림 2 는 계층 그래프 학습 모델의 예시로 VNF 설치 문제를 학습하고 있는 과정을 묘사하였다. 계층 그래프 학습 모델은 총 세 단계(①~③)의 학습 프로세스를 가지고 있다. 먼저 그래프로 표현된 네트워크를 압축하는 과정을 거친다(①) 이때, 압축 과정에서는 Graph Theory, GNN 등의 모델을 이용하여 압축을 진행할 수 있다. 압축되는 노드의 기준은 기본적으로 노드 간의 거리 및 차수(Degree)를 통해 결정이 된다. 만약 압축을 하고도 그래프의 규모가 클 경우에는 여러 번 재 압축을 통하여 크기를 줄인다. 이때, 네트워크 규모와 형태에 따라서 압축의 범위(압축되는 노드의 개수 또는 범우)와 압축의 횟수가 다르게 결정될 수 있다. 충분히 그래프가 압축되었을 경우 해당 그래프의 데이터를 이용하여 최적의 정책을 학습한다(②). 또한 압축된 그래프를 분리한 뒤 각 그래프에서 최적의 관리 정책을 학습한다(③). 분리된 그래프들은 네트워크 규모가 작기 때문에 훨씬 더 쉬운 관리 문제를 학습할 수 있게 된다. 이때, 학습 모델은 분리된 각 그래프 별로 존재할 수 있으며, 하나의 학습 모델로 모든 그래프를 학습할 수도 있다. 만약, 네트워크의 토폴로지가 변하지 않는다면 여러 개의 학습 모델로 각각의 그래프를 지역적으로 학습하여 성능을 향상시킬 수 있으며, 토폴로지가 변하는 경우에는 하나의 모델로 전체 그래프를 학습하는 것으로 범용성을 갖출 수 있다.

III. 결론 및 토론

본 논문은 기계 학습을 이용한 네트워크 관리 모델을 제시하고 있으며 계층 그래프 학습 모델을 통하여 네트워크 관리 문제의 난이도를 낮추어 학습 모델의 성능을 향상시키는 것을 제안하고 있다. 제시한 학습 모델을 이용하면 네트워크 규모의 제약 없이 관리 모델을 높은 학습 성능을 가질 수 있다.

ACKNOWLEDGMENT

이 논문은 2022 년도 정부 (과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원 (2018-0-00749, 인공지능 기반 가상 네트워크 관리기술 개발)과 대학 ICT 연구센터육성지원사업의 연구결과로 수행되었음 (IITP-2022-2017-0-01633).

참 고 문 헌

[1] Lange, Stanislav, et al. "Predicting VNF Deployment Decisions under Dynamically Changing Network Conditions." *2019 15th International Conference on Network and Service Management (CNSM)*. IEEE, 2019.

[2] Cheng, Yang, et al. "Bridging machine learning and computer network research: a survey." CCF Transactions on Networking 1.1 (2019): 1-15.

[3] Boutaba, Raouf, et al. "A comprehensive survey on machine learning for networking: evolution, applications and research opportunities." Journal of Internet Services and Applications 9.1 (2018): 1-99.

[4] Bari, Md Faizul, et al. "On orchestrating virtual network functions." 2015 11th International Conference on Network and Service Management (CNSM). IEEE, 2015.

[5] Lange, Stanislav, et al. "Predicting vnf deployment decisions under dynamically changing network conditions." 2019 15th International Conference on Network and Service Management (CNSM). IEEE, 2019.

[6] Gori, Marco, Gabriele Monfardini, and Franco Scarselli. "A new model for learning in graph domains." *Proceedings. 2005 IEEE International Joint Conference on Neural Networks, 2005.*. Vol. 2. IEEE, 2005.



TS2:
미래 네트워크 서비스 및 관리

북한군과의 전장상황예측을 기반한 국군에서의 인공지능기술 활용분석

장아람[1]*, 최예지*, 석우진[2]**
*대전대학교(aram000317@daum.net, elido1450@naver.com)
**한국과학기술정보연구원(wjseok@kist.re.kr)

Analysis of AI Technologies in the Korean Army based on the Battlefield Prediction against the North Korean Army

Jang A Ram*, Choi Ye Ji*, Seok Woo Jin**
Daejeon Univ.*, KISTI**

요 약

최근 4 차산업혁명을 통해 발전한 국방의 과학기술은 북한의 기존 재래식 무기와 신무기의 위협으로부터 대응할 미래전장의 국방능력을 극대화시키고 있다. 북한은 다양한 비대칭 전력의 사용과 더불어 기습공격을 통해 전장을 장악하기 위한 전략을 수립하고 있다. 이에 우리 군은 네트워크 중심전에서 인공지능중심전으로 발전하고 있는 전장에 대비해 국방 AI 기술 로드맵을 구축하여 인공지능 기술의 활용 증대를 위한 노력을 기울이고 있다. 하지만 여전히 인공지능기술의 적용은 인간운용자에 의해 의존하는 형태이며 지휘통제체계가 마비될 시 지휘관의 능력이 중요하게 여겨져 지휘관의 지휘부담이 높다는 문제가 발생한다. 지휘관과 전투원들 사이에 복합적으로 상황을 인식하고, 인공지능의 기술력과 인간의 통찰력이 결합된 지휘통제체계를 구축함으로써 북한의 위협에 효과적으로 대응하는 방안이 필요하다. 이에 본 논문에서는 전장상황을 실시간으로 공유해 감시정찰-지휘통제로 이어지는 국내 인공지능기술 현황분석과 북한군과의 전장상황예측을 기반으로 인공지능 기술의 활용가능성을 제시한다.

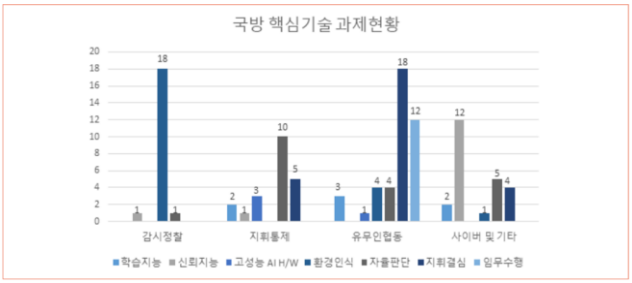
Ⅰ. 서 론

4차 산업혁명은 인공지능기술을 통해 군의 작전개념 및 구조를 완전하게 변화시키고 있다. 북한군은 최근 국지도발에서와 같이 치명적이고 다양한 비대칭수단과 산악지형의 이점을 활용한 비정규적 방법을 배합하여 우리 군이 예상치 못한 기습공격을 감행할 가능성이 높다 [5]. 이에 우리 군은 미래 전장에 대비하여 군 전력을 획기적으로 증강시킬 수 있는 인공지능기술에 주목해야 할 필요성이 있다.

인공지능 기술은 여전히 인간운용자에 의해 의존하는 형태이며 지휘통제체계가 마비될 상황의 대비능력이 완전히 갖춰지지 않은 실정이다. 이에 북한군의 전투양상을 예측하고, 지휘관과 전투원 사이의 복합적 상황인식과 지휘소와의 실시간연결을 통해 지휘관의 부담을 줄이는 방안을 찾아야 한다. 전투상황을 판단하고 학습된 데이터를 바탕으로 능동적으로 최적의 지휘결심을 도출하기 위해서는 지능형 전장관리체계의 구축과 군사용 인공지능 플랫폼 전력화에 힘을 쏟아야 한다. 또한, 4세대 전쟁의 초국가적 위협과 북한의 핵에 방어하기 위한 방어전력은 첨단과학화된 기술을 바탕으로 발전시켜 나갈 수 있다.

따라서 본 논문에서는 전장상황을 실시간으로 공유하고, 감시정찰-지휘통제로 이어지는 국내 인공지능기술의 현황분석과 북한군과의 전장상황예측을 통해 우리 군의 인공지능 기술의 활용가능성을 제시하고자 한다

Ⅱ. 감시정찰-지휘통제 분야 인공지능기술현황



[그림1] 국방 핵심기술 과제현황 [3]

감시정찰을 통해 객체를 탐지하는 전장인식, 탐지한 객체를 분석하는 자율판단, 분석결과를 이용하여 임무를 부여하는 지휘결심을 통해 임무달성을 위한 전략결정을 보조하는 역할을 한다. [그림1]을 보면 감시정찰, 지휘통제체계에서 전장인식기술과 자율판단기술분야의 연구가 중요하게 이루어지고 있는 것으로 볼 수 있다 [3].

1. 감시정찰 인공지능기술현황

감시정찰이란, 적과 지형 또는 날씨에 대한 자료를 알아내기 위하여 각종 정찰자산들을 운용하는 분야로 국방 AI 기능 발전단계에서 1단계인 인식지능이 주로 사용되는 분야이다 [3].

1 주저자(발표자)
2 교신저자

[표 1] 국·내외 개발동향[3]

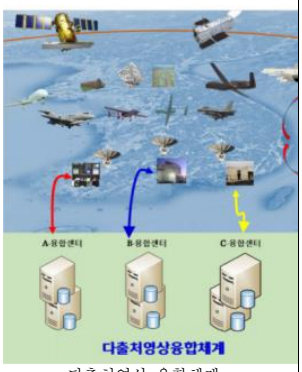
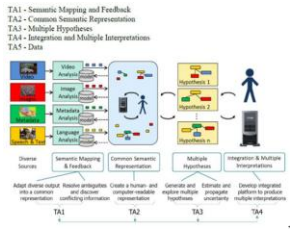
체계명	기관	주요특성
Project MAVEN	/D(미) Amazon MS	- 드론이 수집하는 영상 데이터 내 물체들을 식별/판독하는 알고리즘 - 영상데이터 내 물체학습을 통한 객체인식 및 분류, 타격/비타격 표적 여부 판단
 감정인식시스템	KAIST	- 뇌파와 심박 모니터링을 통한 감정인식시스템 - 정서, 각성도의 2차원에서 감성값을 예측하는 학습모델
 소형 드론용 영상분석 장비	육군교육사령부	- AI 영상분석, 표적추적 - 표적정보 실시간 공유 - 다중 드론 통제/모니터링 - 지형정보 처리(3D 지도 생성)

감시정찰체계의 경우 [표 1]과 같이 전장인식분야의 AI 기술이 중점적으로 사용되고, 드론을 이용한 영상인식과 음성인식, 감정인식의 분야에서 각각의 경우에 따라 다른 객체데이터의 구축을 통해 AI 기술을 적용시켜 나가려는 노력을 기울이고 있다.

2. 지휘통제 인공지능기술현황

지휘통제란, 지휘관이 부대의 임무 달성을 위하여 예속 및 배속된 전력에 대해 권한을 행사하는 것으로 결심하고 지시하고 지시사항의 이행을 감시하고 교정하는 것을 의미한다. 국방 AI 기능 발전단계에서 2~3 단계인 판단, 결심지능 주로 사용되는 분야이다[3].

[표 2] 국·내외 개발동향[3]

체계명	기관	주요특성
 DIAMON D Shield	Lock-heed Martine	- 항공, 해상 및 우주 전반에 걸쳐 시스템과 플랫폼을 연결하여 지휘하고 통제하는 다중 도메인 전투관리 시스템
 JADC2	국방부 (미)	- 현재 미국 각 군 사령부별로 운용되고 있는 정보수집센서와 전술통제망을 단일화하기 위한 지휘통제 네트워크 구축 사업 - 글로벌 네트워크 상의 센서 및 소스를 통합하여 데이터 내의 중요한 추세를 식별하고 지휘관이 현재 및 예측정보를 모두 사용할 수 있도록 함
 다출처영상 융합체계	ADD	- 주요 핵심표적에 대한 적시 징후감시와 전략표적 타격작전 수행 시 신속, 정확한 표적 영상정보를 제공하는 합동전력 지휘통제 체계 - 다출처에서 운용되는 다양한 영상센서를 탑재한 다수의 정찰자산으로부터 수집되는 영상을 융합하여 영상정보를 생성하고 지휘통제체계로 전파할 수 있는 체계
 AIDA	DARPA	- 다양한 소스로부터 입력되는 데이터를 해석하여 이를 공통 의미표현으로 지식화하고 이를 이용하여 복수의 가설을 제시하여 사용자의 의사결정지원

지휘통제체계는 감시정찰체계보다 더 높은 수준의 인공지능 기술이 요구되며 감시정찰무기체계를 통해 수집한 정보를 분석하고 그에 따라 지휘관이 부대의 임무달성을 위해 지시하는 임무를 수행하므로 [표 2]와 같이 자율판단과 지휘결심 분야의 AI 기술이 중점적으로 사용된다.

Ⅲ. 북한군 전장상황예측 기반의 인공지능 활용분석

4세대 전장에 대비한 인공지능기술을 북한군과의 전장상황예측을 통해 어떤 방면으로 적용시킬 수 있을 지 살펴보고자 한다.

1. 북한군의 군사전략

4세대전쟁은, 가용한 모든 네트워크로 적의 전쟁의지를 굴복시키기 위한 정기전이며 비대칭적인 전력에 의존하고, 장기적인 정치 투쟁 성격을 가진다. 4세대전쟁에서의 네트워크는 단순히 군사적인 부문에 제한되지 않고 정치 경제 문화의 모든 네트워크가 목표를 위해 동원된다.

북한은 군사적 목표를 달성하기 위해 정치전, 외교전, 심리전 등과 연계한 군사전략을 전개하는 총력전을 펼치고 있다. 따라서 북한의 전략수립과 군사력 운용을 종합적으로 분석할 필요가 있다. 북한군 군사전략의 특징은 기습전략, 속전속결전략, 배합전략이며, 전선을 구축한 다음 그 전선을 밀고 나가는 전투가 아닌 독립된 부대가 목표점령을 위해 고속기동을 하는 전략에 비중을 두고 있다.

이에 우리는 첫 번째로 짧은 시간 내 기동하는 북한군을 감시정찰체계를 통해 빠르게 식별해야 할 필요가 있다. 북한과의 제4세대 전쟁에서는 북한과 연결된 비국가적 행위자들을 추적하고 이들이 이용하는 네트워크를 탐지하여 차단해야 한다. 이를 위해서는 먼저 비국가적 행위자들의 정확한 실체를 파악해야 한다. 두 번째로 비국가적 행위자들을 추적, 탐지하기 위해서는 많은 인력이 소

요되며 군사적차원 뿐만 아니라 국가적 차원에서의 대응이 요망된다. 이를 통해 자금원을 차단하여 장기적인 활동과 세력의 확장을 봉쇄해야 한다 [2].

북한의 제4세대 전쟁에 대응하기 위해서는 스워밍(Swarming) 개념 적용이 필요하다. 스워밍(Swarming)은 짧은 시간 내에 특정한 지점에서 집중을 달성하는 방식을 강조하는 용어로 벌이나 파리 등이 일순간에 모여들듯이 부대나 전투원들이 짧은 시간에 일정 지점에 집중하여 순간적인 전투력의 우세를 달성하는 방식이다. 세 번째로 이를 위해 우리 군은 네트워크로 연결되고 지휘의 분권화가 이루어져야 한다 [2].

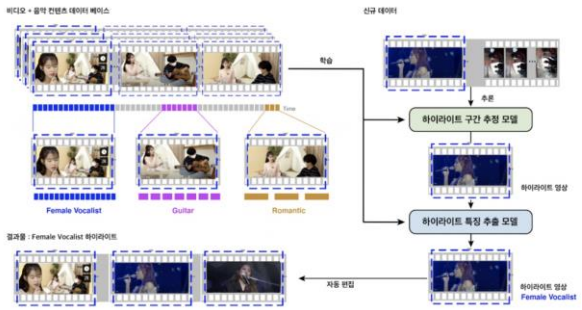
2. 인공지능 기술 활용방안

앞서 기술한 북한군의 군사전략인 속전속결전, 배합전, 기습전의 형태의 전통적 군사전략을 바탕으로 비대칭적이고, 비군사적인 요소를 고려하여 4세대전쟁에 대비할 필요가 있으며 세 가지 문제점에 대한 인공지능 기술의 활용방안을 제시한다.

1) 짧은 시간 내 기동하는 북한군 식별(소형드론용 영상분석 장비 활용/Project MAVEN)

비정규전에 능숙한 북한군은 우리 군이 예상하지 못한 지역이나 방법을 통해 작전을 수행할 가능성이 높다. 우리나라 국토의 70%가 산악지형으로 이루어져 지상의 감시정찰체계로 적을 파악하기 제한되는 부분이 있다. 우리는 적을 빠르게 식별하기 위해 드론으로 수집한 영상데이터 내 물체가 사물인지 사람인지 식별 후 타격의 대상인지 아닌지를 판독하여 빠르게 공격에 대응할 수 있다. 레이더, LIDAR와 같은 정찰센서로 환경인지, 상황인지를 통해 정보를 분석하여 정찰 무인기를 무인기 플랫폼 통제장치를 이용해 무인기를 단일/편대/군집으로 지휘통제한다.

2) 비국가적 행위자에 대한 추적 및 탐지(감정인식 시스템)



[그림2] 동영상에서 하이라이트 영상을 자동으로 추출 및 생성하는 서비스 [4]

인간의 감정을 이해하는 미래 인공지능 기술발전을 위해서 고품격 공공데이터 확보가 필수적이며 [그림2]와 같이 성별, 연령, 환경 등 다양한 수집대상의 감정을 수집하여 분류한다. 이러한 방법으로 축적된 데이터를 바탕으로 비국가적 행위자들을 파악하고, 이들이 사용하는 네트워크를 추적해 장기적인 활동과 세력확장을 막아야 한다.

3) 네트워크의 연결과 지휘분권화(AIDA/다출처영상융합체계)

적에 대한 적시 징후감시와 전략표적 타격작전 수행 시 신속, 정확한 표적 영상정보 제공을 위한 지휘통제체계를 정립하여 네트워크의 연결이 필요하다 [1]. 4세대 전장에서는 비교적 짧은 시간에 화력을 집중하여 공격을 전개해야 하므로 데이터를 수집, 분석하여 지휘통제체계와 연계시키는 것이 중요하다
감시정찰체계와 통합DB서버, 네트워크체계의 연결로 실시간으로 대용량의 정보를 공유하며 머신러닝을 통한 지휘결심정보를 생성한다. 생성된 복수의 지휘결심정보는 AI지휘결심체계에 의해 다영역에 걸친 전장상황의 지휘관 의사결정을 돕고, 기동전력으로 임무를 수행한다.
추후 진행될 자체 의사결정이 가능한 인공지능 기술이 적용된 지휘통제연구에는 자체적 통제와 자체적 규율을 정립하여 운용할 필요성이 있다.

Ⅳ. 결론

본 논문에서는 인간운용자의 의존도를 축소하고, 지휘관의 부담을 감소시켜줄 군에서의 감시정찰-지휘통제 분야 국내외 인공지능 기술현황에 대해 살펴보았다. 또한, 북한군의 전장상황예측양상을 바탕으로 기존의 재래식 전투방식과 더불어 전개될 4 세대 전쟁에서의 대응방안을 인공지능 기술을 활용하여 제시하였다.
전장이 계속해서 확대되는 시점에서 인간의 능력을 대체하고 그 이상의 효율을 이끌어 내기 위한 인공지능 기술은 군 자체적 기술 개발 뿐만 아니라 민간기업과의 협력을 통해 군으로 신속하게 도입해야 할 필요가 있다. 이러한 기술 도입을 통해 우리 군에게 실질적 위협이 되는 존재들을 식별하고 대응하는 전략을 발빠르게 개선시켜 나가야 한다. 이에 향후 진행될 연구에서는 감시정찰, 지휘 통제 등 다양한 상황에 대해 AI 기반으로 시뮬레이션 할 수 있는 디지털 트윈 기술이 더욱 증대되기를 기대한다.

참 고 문 헌

[1] 김대호, "AI 적용 전장정보융합 지휘통제체계 국내외 개발동향 및 발전방향", 2021, pp. 4-6.

[2] 신종필, "북한의 제 4 세대 전쟁에 대한 한국군 대응방안 - 북한의 무력도발 후 수세로 전환 시를 중심으로 -", 2021 , pp.127-129.

[3] 국방기술진흥연구소, "미래국방 2030 기술전략", 2022, pp.9, pp 42-68.

[4] 카이스트, "한국인의 자연스러운 감성 인식 인공지능을 위한 공공 DB 구축", http://kaist.ac.kr

[5] 조상근; 차도완, “북한군 미래전투양상을 고려한 인공지능과 로봇 기술의 적용방안”, 2019

ICBM 기반 국방자율무기체계 선진사례 분석

최예지[1]*, 장아람*, 석우진**[2]

* 대전대학교(elido1450@naver.com, aram000317@daum.net)
** 한국과학기술정보연구원(wjseok@kisti.re.kr)

Analysis of Advanced Cases on ICBM based Military Autonomous Weapon Systems

Choi Ye Ji*, Jang A Ram*, Seok Woo Jin**
Daejeon Univ.*, KISTI**

요 약

4 차 산업혁명과 IT 기술의 발전으로 미래전은 가능한 인명피해를 최소화하면서 적의 전쟁의지를 말살시키는 방향으로 변화될 것이다. 최근 발전하고 있는 클라우딩 기술을 포함한 ICBM 기술들이 육군에서 추구하는 네트워크 중심 작전환경에서 결정적 승리를 달성하기 위해서 필요하다. 본논문에서는 ICBM 기술에 중점을 두고 이를 기반으로 하는 자율무기체계를 분석하며 여러 나라의 사례를 분석하고자 한다. 또한, IoT 기술뿐 아니라 사람의 몸이 네트워크가 되는 YOT(You Of Things) 기술을 이용한 '슈퍼솔저'를 구현하기 위하여 필요한 클라우드 컴퓨팅 기술도 분석하고자 한다.

Ⅰ. 서 론

4 차 산업혁명과 IT 기술의 발전으로 미래전은 가능한 인명피해를 최소화하고, 적의 전쟁의지를 말살시키는 방향으로 변화할 것이다. 정보기술의 지속적인 발전과 인공지능의 도약에 기초하여 기술 혁신뿐만 아니라 군사 혁신이 가속화되고 있으며, 이를 통해 자율무기체계의 중요성도 커지고 있다.

또한, ICBM 기술은 기본적으로 사물인터넷(IoT) 센서가 수집한 데이터를 클라우드(Cloud)에 저장하고, 이를 빅데이터(Big Data) 분석 기술로 분석하여 적절한 서비스를 모바일 기기 서비스(Mobile) 형태로 제공하는 것이다. 특히, 클라우딩 기술은 빅데이터를 분석하여 여러 곳에서 동시에 이용할 수 있기 때문에 국방분야에서도 널리 활용될 것이다.

이 외에도 사람의 몸이 네트워크가 되는 YoT(You of Things) 기술을 이용한 '슈퍼솔저' 구현을 위해 필요한 클라우드 컴퓨팅 기술을 분석하고, '육군의 8 대 게임 체인저'를 소개하며 우리나라에서의 신개념 무기체계에 대한 분석을 진행할 것이다. IT 기술과 함께 발전한 자율무기체계에 대해 분석하고 우리나라 뿐만 아니라 세계 각국에서 미래전에 어떻게 대응하고 있는지도 알아볼 것이다.

국방부에서 2012 년부터 클라우드 컴퓨팅을 시범적으로 도입하고자 계획하고 추진하고 있으며, 클라우드 컴퓨팅의 초연결, 분산화, 민첩성, 비용 절감 등의 특징을 활용하여 변화하는 미래전 적응에 활용될 것이다 [1].

Ⅱ. 국방자율무기체계 선진사례 분석

4 차 산업혁명으로 인한 과학기술의 발전을 통해 미래전의 모습이 변화하고 있다. 흔히 알고 있는 로봇이나 드론 등을 활용한 원거리, 원격 정밀 타격 혹은 네트워크 기반의 전쟁이 발전하고 있다. 이러한 변화로 인해 전쟁의 공간 자체가 지상, 해상, 공중이 아닌 우주와 사이버 공간으로 확대되기도 한다. 전쟁의 공간 확대뿐만 아니라 무기체계도 재래식 무기에서 자율무기체계로 변화하게 되었다. 무기체계가 자체 판단에 의해 인간이 선정한 목표물을 공격한다면 이를 자율무기체계로 볼 수 있는데, 교전에 있어 인간이 개입하지 않는다는 것이 자율무기체계로 인정되기 위한 최소한의 개념 요소이다. 인간 개입이 이루어져도 교전 기능에 있어 자율성이 인정된다면 자율무기체계로 인정한다 [2]. 이러한 사실을 바탕으로 여러 나라의 자율무기체계 선진사례를 분석하고 우리나라의 신개념 무기체계에 ICBM 기술과 관련된 사항을 분석 및 재고하고자 한다.

1. 자율무기체계 선진 사례 분석

자율무기체계는 무기의 정밀도를 높이고 비용을 절감하며 정확한 타격으로 전체 피해를 줄이는 것을 목적으로 한다. 또한, 군사적인 목표 달성뿐만 아니라 병력의 인명피해를 최소화하고자 한다. 재래식 군사력에 기반한 전통 안보와 군사전략에 자율무기체계가 등장하면서 큰 영향을 끼쳤다. 이러한 자율무기체계를 운용하고 있는 전세계 여러 나라들의 사례를 분석해보았다 [3].

[1] 주저자(발표자)
[2] 교신저자

(1) 미국

JADC2(Joint All Domain Command and Control)은 합동전지휘통제로, 다영역에서 생성되는 여러가지 데이터를 통합하는 개념이다. 육, 해, 공 등의 각 군은 자신만의 데이터 소통 체계를 구축하고 있지만, 완벽한 통합체계가 구축되어 있지 않다. 이런 문제점을 해소하고, 각 군이 가지고 있는 무기체계를 각 센서와 AI 알고리즘 등을 연동시켜 의사결정 체계를 향상할 수 있습니다. 진보된 전투 관리체계(ABMS : Advanced Battle Management System)는 이러한 JADC2 능력을 구현하기 위해 항공기, 드론, 함정 등 무기체계의 센서를 연결하는 네트워크를 구축하여 모든 영역에서의 위협과 실시간 작전상황을 제공하는 미 공군의 차세대 지휘통제 체계이다. 자동화, 인공지능 기술, 클라우드 환경, 5G 기반 기술을 핵심기술로 삼는다. 각 센서들을 이용한 IoT, 그로 인해 발생하는 데이터를 분석하는 클라우드, 각 군마다 생성되는 데이터, 어디서든 확인할 수 있는 모바일 등 ABMS 에서도 ICBM 이 사용된다.

(2) 러시아

2017 년 푸틴 대통령이 “AI 리더가 세계를 지배할 것”이라고 언급하였고, 2030 년까지 군대의 30%를 원격통제 또는 자율화된 로봇으로 대체할 계획입니다. 특히 무인전투차량인 ‘비카르’와 소형 무인전차인 ‘우란’을 개발하여 시험 운영하였습니다.

(3) 터키

KARGU-2 는 목표물 주변에서 자폭하는 방식으로 공격하는 드론 병기이며, 인공지능을 기반으로 작동하는 ‘치명적자율무기(LAWs, Lenthal Autonomous Weapons)’이다. 자율적 행동, 혹은 원격 제어로 작동이 가능한 드론으로, 전쟁 또는 반테러 지역에서 사용하기 위해 제작된 자율의지 드론이다. 플랫폼에 내장된 이미지와 딥러닝 알고리즘을 통해 대상을 추적 혹은 효과적으로 사용할 수 있다. 이 외에도 ‘바이락타르 TB-2’라는 대전차 드론을 개발하여 주변국에 수출하고 있다.

[표 1] 선진사례 분석: 주요점 및 핵심기술 분석

선진 사례	주요점	핵심기술
미국	무기체계의 센서를 연결하는 네트워크 구축	자동화, 인공지능 기술, 클라우드 환경, 5G 기반 기술
러시아	원격통제 혹은 자율화된 로봇	IoT, 원격통제, 빅데이터
터키	인공지능을 기반으로 작동하는 ‘치명적 자율무기’	인공지능, 자율화, 클라우드 환경

2. 국방분야에 활용될 ICBM 기술 국내현황

ICBM 은 사물인터넷(IoT), 클라우드(Cloud), 빅데이터(Big Data), 모바일 기기 서비스(Mobile) 형태로 데이터를 제공하는 것이다. 이 기술들을 각각의 기술들로 분리해서 보는 것이 아니라 하나의 통합된 기술로 보며, 서로 상호 보완적인 관계를 형성하고 있으므로 융합된 형태로 발전될 것이다. 지금과 같은 정보화 시대에 자원고갈, 환경문제 등의 문제들을 단순히 생산성을 늘려서 해결하는 것이 아니라 수요적인 접근으로 해결하고자 하는데, 이러한 과정에서 ICBM 기술이 매우 중요하다. 이러한 중요성을 인지하고 사회적 측면에서뿐만 아니라 국방 차원에서도 영향력이 더욱 확대되고 있다 [4].

IoT, 즉 사물인터넷은 사물에 센서를 부착해 실시간으로 데이터를 인터넷으로 주고받는 기술이나 환경을 일컫는다. 이러한 연결된 기기 조차도 사람의 도움 없이 서로 알아서 정보를 주고받으며 대화를 나눌 수 있다. 사물 간 센싱, 정보교환 및 처리가 가능한 M2M(Machine to Machine)과 비슷한 개념이지만 사람의 개입 유무로 개념적 차이가 난다. M2M 의 경우 사람의 개입이 필요하지 않는 통신 혹은 정보교환으로 정의되며 그 범위를 사물로 한정하지만, IoT 는 사람의 개입 없이 기존의 컴퓨터 화면을 통해서만 정보를 전달하는 기술이다. 미시적인 접근 차원에서 거시적인 접근 차원으로 확대되었다고 볼 수 있으며 사람뿐만 아니라 사물까지도 인터넷을 통해 정보를 주고받을 수 있도록 지원해 주기도 한다 [5].

클라우드(Cloud)는 데이터를 인터넷과 연결된 중앙컴퓨터에 저장해서 인터넷에 접속하기만 하면 언제 어디서든 데이터를 이용할 수 있는 기술을 말하며, 네이버, 구글, 마이크로소프트 등 다양한 곳에서 사용되고 있다. 가장 큰 장점은 하나의 데이터를 가지고 여러 사용자가 동시에 이용할 수 있다는 것이다.

빅데이터(Big Data)는 대량의 데이터로부터 가치를 추출하고 결과를 분석하는 IT 기술로서 제조, 통신 등의 다양한 분야에 적용되고 있다. 단순히 대량의 데이터를 의미하는 것이 아니라 비정형화된 데이터들을 처리하고 분석하는 기술 자체를 정의한다. 이러한 빅데이터의 특성은 볼륨(Volume), 다양성(Variety), 속도(Velocity)이며, 가치(Value)나 진실성(Veracity)이 추가되기도 한다 [6].

마지막으로 모바일 기기 서비스(Mobile)는 스마트폰과 태블릿 PC 를 지칭하는 용어이며, 최종 사용자에게 서비스를 전달하는 수단이다. 모바일 기술이 PC 와 같은 작업환경들을 제공함으로써 클라우드가 제공하는 의미 있는 정보들도 모바일을 통해 전달된다. 이로써 모바일 기기도 PC 와 같이 모바일 클라우드 기술개발의 중요성을 부각시키기도 한다.

‘육군비전 2050’에서는 이러한 자율무기체계에 ICBM 기술을 도입하여 신개념 무기체계인 ‘8 대 게임 체인저‘를 발표하였으며, 미래 전장을 예측하고 시간과 공간을 주도하는 초일류 육군으로 거듭나고자 한다. 미래 전장의 판도를 바꾸기 위해 ICBM 기술의 중요성은 나날이 증가하고 있다.

Ⅲ. 육군의 8 대 게임 체인저 분석

군사분야에 있어서 과학기술의 발전에 맞춰 무기체계를 발전시키지 못하면 국가적 생존을 보장하기 어렵다. 그렇기에 우리나라 육군에서는 사회의 변화에 따른 새로운 무기체계를 발표하였다. 슈퍼 솔저는 언제, 어디로든 신속하게 전개할 수 있는 기동력과 스텔스 능력을 지닌 증강된 트랜스 인간전투원으로, IoT 가 아닌 인간의 몸이 네트워크가 되는 YoT 기술을 응용한다.

지능형 자율 전투로봇은 휴머노이드 로봇, 생체 모방형 로봇, 군집드론 등으로 구분할 수 있는데, ‘휴머노이드 로봇’은 사람이 느끼고 판단하는 것처럼 센서를 통해 주변정보를 수집하고 인공지능을 통해 스스로 결정하며, 행동할 수 있는 로봇이다. ‘생체 모방형 로봇’은 동, 식물 등이 가지고 있는 특성을 이용하여 만든 로봇으로,

인공지능을 탑재하여 자율임무를 수행한다. 마지막으로 '군집드론'인데, 무리지어 활동하는 드론군으로, 대형 또는 다량의 특정 목표물에 대해 집단적으로 동시다발적인 공격을 할 수 있다. '초소형 스마트 먼지'도 군집 드론의 일종으로 나노기술을 활용하고, 송수신기나 에너지원 등을 넣어서 네트워크를 형성하기도 한다.

에너지 무기는 기존의 화약무기를 대체할 수 있으며, '레이저 무기'와 '레일건'이 있다. '레이저 무기'는 레이저 빔으로 표적의 동체 파괴 혹은 탑재 전자센서를 무력화시키는 무기이고, '레일건'은 전자기력을 이용해 초고속으로 탄체를 발사하는 무기이다. 둘 다 센서를 이용하여 표적을 탐색할 수 있으며, 첨단과학기술력을 바탕으로 미래 무기체계의 핵심기술이 될 수 있다.

극초음속 무기는 적의 전략적 중심을 타격할 수 있는 무기로, 마하 5 이상의 속도로 일정한 포물선 형태가 아닌 자유자재로 기동하기 때문에 기존의 방어체계로 막을 수 없는 무기로 여겨진다. 고속 고기동성, 시간의 압박과 모호성 등의 특징을 가지고 있으며, 계속된 극초음속 무기 개발을 빅데이터를 활용하여 더 실용적인 무기로 발전하게 될 것이다.

사람이나 물자를 무력화시키고 인체에 치명상이나 영구적 부상을 최소화하면서 재산 및 환경에 불필요한 손상을 주지 않도록 설계된 비살상무기는 인명 살상이나 물자의 파괴를 지양하고 재산 및 환경에 대한 피해를 최소화하는 동시에, 군사작전에 다양한 융통성을 제공하며 적의 전투의지를 마비시키는 수단이다. 대표적으로 사이버전자전 무기가 있는데, 이는 네트워크 환경과 관련된 빅데이터 등의 중요성이 대두된다.

지, 해, 공에 구애받지 않고 어디든지 자유자재로 신속하게 병력을 투사하고 공격과 방어를 자율적으로 할 수 있는 무인자율이동체(Autonomous vehicle)는 첨단과기술을 기반으로 초지능, 초연결 및 무인화 등을 통해 발전되며 재래식 무기와의 융합을 통한 기술혁신이 필요하다.

신개념 무기체계가 발전하면서 그 능력을 최대로 발휘하기 위한 감시정찰 및 지휘통제체계 발전도 필요하다. 그렇기 때문에 전장과 전투수단들의 통합을 보장하는 초연결 네트워크 체계 구축이 필요한데, 감시정찰, 통신, 지능형 지휘결심체계가 있으며 각 체계는 AI 기술을 적용하여 선견, 선결, 선타를 효율적으로 처리한다. 대부분의 무기체계에서 반드시 필요로 하는 에너지원 중 시간 및 장소를 구애받지 않고 지속적인 공급이 가능한 에너지 지원체계가 필요한데, 화석연료 대신 수소, 태양광, 풍력 등 신재생에너지로 대체될 것이다.

이렇듯 변화하는 사회에 맞추어 육군에서도 다양한 변화를 보여준다. 특히, 신개념 무기체계를 발표하여 첨단과학기술군을 건설하고자 하며, 4 차 산업혁명의 물결을 따라 시간과 공간을 주도하는 초일류 육군으로 거듭날 것이다.

Ⅳ. 결론

4 차 산업혁명을 통해 정보화사회로 변화하고, 그와 동시에 육군에서도 무기체계를 발전시켰다. '육군의 8 대 게임 체인저'를 통해 우리 육군에서는 기술의 발전에 따라 어떤 무기체계를 준비하고 있고, ICBM 기술은 어떻게 적용되고 있는지를 분석하였다. 이를 통해 최소한의 살상과 전쟁의지 말살을 목표로 하는 미래전에 우리 육군은 새로운 무기체계를 발전시키고자 한다. 우선 ICBM 기술 중 클라우드, 빅데이터 기술을 중심으로 신개념 무기체계를 분석하고 변화하는 사회에 발맞추어 계속해서 무기체계를 변화시켜야 한다. 특히, 빅데이터 기술은 4 차 산업혁명으로 인해 중요해진 데이터 관리에 관한 기술로 ICBM 기술 중에서도 가장 중요하다고 볼 수 있기 때문에 정보가 중요한 군사분야에서 보안성과 안정성을 더욱 강화시키면서 새로운 무기체계를 적용해야 한다.

참 고 문 헌

[1] 장월수, "국방 클라우드 컴퓨팅 도입에 관한 보안체계 연구", 2012

[2] 박문언 , "자율무기체계의 개념과 비례성의 원칙", 2019

[3] 조현석, "인공지능, 자율무기체계와 미래 전쟁의 변화", 2018

[4] 유성민, "ICBM 산업육성 방안 및 기술도입 전략", 2014

[5] 비피기술거래 , "스마트 그리드와 사물인터넷, 빅데이터의 이해", p.18, 2022

[6] 비피기술거래, "스마트 그리드와 사물인터넷, 빅데이터의 이해", p.29, 2022

극한자연재해 대비 자율구축/관리 유무선 연합 비상통신망 시스템

최태상*, 윤상식*, 김융석**, 윤봉요**
*한국전자통신연구원, **한국수력원자력 중앙연구원
e-mail : {choits, ssyoon90}@etri.re.kr, {yoongseok, ybyun0707}@khnp.co.kr,

Autonomic provisioning and management capable emergency communications system for extreme natural disaster

*{Taesang Choi, Sangsik Yoon}, **{Yoongseok Kim, Bongyo Yun}
Electronics Telecommunications Research Institute, KHNP

요약

본 논문에서는 일본 후쿠시마 원전 사태와 같은 지진, 해일 등 극한 자연재해 상황 하에서 원자력발전소 등 산업시설의 기존 유·무선 통신망이 파괴되었을 때, 기존 통신망과는 별개로 통신 비전문가인 산업시설의 운용자가 수십분 이내에 구축 운용 및 관리 할 수 있는 신속성, 편리성, 휴대성, 신뢰성, 안전성을 모두 갖춘 유·무선 연합 통신망 및 음성/데이터 서비스 자율구축 및 관리 기술을 제안한다. 또한 연구 결과로 개발된 PoC (Proof of Concept) 시스템과 기능 검증 및 시험 결과를 소개한다.

I. 서론

지진, 해일, 폭풍 등으로 인한 후쿠시마 원자력발전소 등 산업시설 사고가 발생하는 극한의 자연재해 속에서 산업시설 내의 긴급 비상통신망 자율 구축 및 통신서비스의 신속한 음성/데이터 기능 재개는 추가 2차, 3차 피해를 최소화할 수 있으며, 산업시설의 안전을 유지하는데 필수적인 작업이다. 이를 해결하기 위해서 본 연구에서는 지진 등 극한 자연재해 조건에서 원자력 발전소 안이 파괴되어 이용 불가능한 기존 통신망과는 별개로 비전문가도 신속하게 구축 및 운용할 수 있는 신속성, 편리성, 휴대성, 신뢰성, 안전성을 모두 갖춘 유무선 연합 비상통신망 및 응급서비스 자율구축 및 관리 기술개발 연구를 수행하였다. 본 연구개발 대상기술은 정상 운영 상황에는 의료 응급 키트와 같이 관련 장비 및 기능을 보관하다가 극한 재난이 발생하였을 경우, 아래와 같은 기술을 기반으로 비상 네트워크를 빠르게 자율 구축함으로써 원자력 시설 운영자들 간에 긴급 통신서비스를 제공함을 목적으로 한다.

- 휴대형 배터리 지원 유선 및 이동통신 연합망 통신스위치, AP(Access Point), 서버 하드웨어 기술
- 극한 재난용 유무선 연합 통신서비스 자율 제어 및 관리 소프트웨어 기술

또한 최악의 극한 재난상황시 기존의 통신망 및 서비스가 모두 파괴되어 사용이 불가한 상황을 고려하여, 재난 발생 이후에 네트워크를 처음부터 자동 구축 및 운영이 가능하도록 개발하였다. (From Zero-clean Network State) 상기의 목적을 달성하기 위해 본 연구개발에서는 핵심 기술로 SDN (Software Defined Networking) [1], SON (Self-Organizing

Network)[2], SIP (Session Initiation Protocol)[3], Web RTC, 기술을 포함한 Plug-and-Operation, 중앙 네트워크 자율관리, Resilient 다중 경로 제어/복구, 전원/배터리 동시 지원 유선 이동통신 연합 네트워킹 핵심 기술을 연구 개발하였다.

본 논문에서는 국내 원자력발전소 환경의 다양한 요구사항을 분석하여 실제 적용 가능한 극한 자연재해 대비 비상 통신망의 최적 구조를 설계하고, 설계된 구조를 구현하기에 적합한 핵심 요소 기술들을 맞춤형으로 개발하여 Proof of Concept (PoC) 시스템을 개발하였다. 본 PoC 시스템은 1차적으로 실험실 환경에서 기능 검증을 위한 적합성 시험을 완료하였으며 운영 중인 원자력 발전소에 시범 적용하여 현장 적합성도 검증하였다. 본 연구에서는 비상통신망의 제공 서비스로 유무선 음성 통신과 화상 통화를 포함한 데이터 통신을 완료하였다.

본 논문의 나머지 부분은 다음과 같이 구성된다. 2절에는 제안된 극한 자연재해 대비 비상통신망 및 서비스의 구조 설계 결과를 설명한다. 3절에서는 PoC 시스템 구현, 시험 및 검증에 대해 기술하고. 마지막으로 4절에서는 논문의 결론 및 향후 연구에 대한 내용이다.

II. 시스템 구조 연구

원자력발전소의 특수한 환경 및 제약사항으로 인해 발전소 건물 내부는 방화벽 및 방화문으로 구성되어 있어 무선 인터넷, 위성, 및 이동 통신 시스템은 건물 내부에서는 일부 오픈 공간을 제외하고는 기능을 할 수 없다. 따라서 극한 자연재해 하의 외부지원을 배제한 상황에서 통신망 전문가의 도움 없이 간단하면서 미리 준비된 최소한의 휴대 가능한 통신장비를 활용하여 신속하게 최소의 인원으로 긴급히 필요한 원자력발전소 시설의 응급통신서비스를 복구할 수 있는 기술이 필요하다. 특히 다음은 이러한 기술에 필요한 최소한의 요구사항이다.

- 극한 재난상황을 고려하여 전원 공급이 차단된 경우에도 최소한의 일정 시간 (기본 8시간 이상) 동안 동작할 수 있는 비상통신망 구축
- 신속성, 편리성, 휴대성, 신뢰성, 안전성을 모두 갖춘 유무선 통합 통신망을 비전문가도 구축 가능한 비상통신망 구축 및 음성/데이터 서비스 운용 자동화
- 원자력발전소 건물은 내/외벽의 두께가 두껍고, 대부분 방화문으로 항상 닫힘 상태를 유지로 유무선 기술이 통합된 비상통신망 구축
- 원자력발전소의 주 제어실(MCR)은 계측설비들이 모여 있어 무선 통신 시 전파 간섭 영향을 받지 말아야 하며 다수 호기 및 건물 외부와의 통신을 위한 유선과 무선이 유기적으로 연합된 효율적인 통신 체계
- 통신서비스는 기본적으로 음성 서비스를 제공하고, 재난 현장 상황의 정밀한 실시간 보고를 위해 사진 이미지, 동영상 비디오와 같은 멀티미디어 전달 데이터서비스의 제공 필요

상기의 시스템 요구사항에 기반하여 극한 자연 재해 대비 원전 비상통신 네트워크에 최적으로 제안된 구조는 다음과 같다.

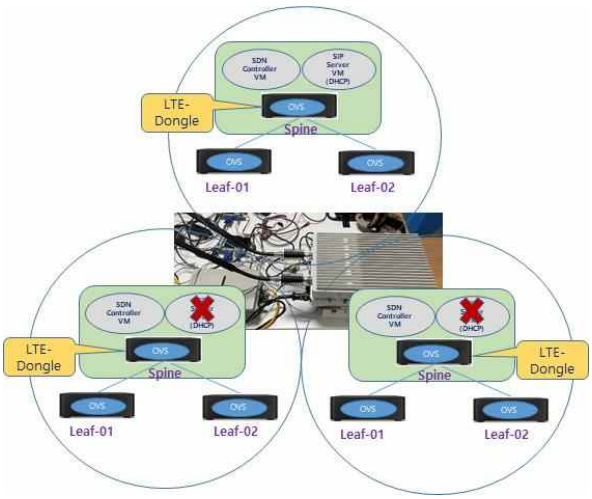


그림 1. 발전소 유무선 연합 비상통신망 구조도

그림 1은 여러 호기로 구성된 발전소 전체에 공통적으로 적용할 수 있는 이동형 LTE 기지국 기반 비상통신망 연합 연결 구조를 도식화하였다. 비상 통신망 구조는 LTE 기지국을 Core Network로 하고 각 건물내부에 구축된 유선네트워크인 Spine-Leaf 구조의 네트워크들을 라우팅 연결 구조로 설계하였다. 이를 위해 각 Spine 스위치에 본 구조를 위해서 개발된 LTE용 모뎀을 연결하고 건물간 무선 구간은 이들 간을 연결하여 라우팅 기능을

제공하는 구조로 설계하였다. 기술한 발전소 환경의 특성상 건물 내부 네트워크의 Spine과 Leaf 스위치 간은 유선으로 연결되며 각 Leaf 스위치에 AP (Access Point) 를 연결하고 유선 단말 혹은 WiFi 무선 단말 (스마트폰 등)을 접속하여 운전원간 비상 통신을 가능하도록 하는 구조로 설계하였다. 단말의 수는 네트워크 throughput과 비례한다. 각 건물내부의 유선 네트워크 구조는 순수한 Spine-Leaf 구조에서 일부 변경되어 Leaf에서 타 Leaf로 확장이 가능한 Hybrid Spine-Leaf 구조로 현장의 요구사항을 반영한 구조로 볼 수 있다.

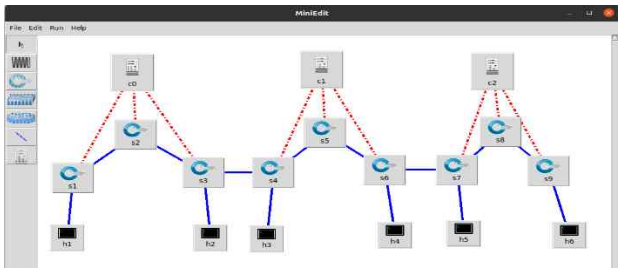


그림 2. 발전소 사이트간 제어를 위한 SDN Clustering 구조도

그림 2는 멀티 사이트를 제어하기 위한 SDN 클러스터링 기능을 적용한 구조이다. 각 사이트는 별도의 SDN controller를 적용하고 이들 간은 클러스터링 기능을 통한 라우팅 기능을 제공하는 구조이다.

멀티 사이트들 간에는 외부 개방 공간이므로 건물 내부의 제약사항과 무관하여 LTE를 이용한 연결을 통해 거리에 제약없이 효율적인 연결 환경을 제공할 수 있다. 그러나 일반 LTE와 달리 본 구조에서 제공되는 LTE 기능은 전원 공급을 가정할 수 없는 상황이고 정상적인 LTE 기능을 모두 사용할 수 없어서 RAN과 Core 기능이 한 장치에 통합된 휴대형 LTE 장비를 사용하였다.

그림 3은 본 비상통신망 구조에서 핵심 기능 중 하나인 Network Reliability and Wireless Mesh Network 기능을 지원하기 위해 SDN Controller에서 제공되는 장애 탐지 및 복구 기능을 도시한다. 그림 3a는 장애가 발생되기 전에 트래픽 흐름이며 그림 3b는 특정 링크에 장애가 발생한 경우 트래픽 흐름이 장애가 발생한 링크에서 복구 경로로 자율적으로 절체하는 기능을 보여준다. 이 때 링크가 무선일 경우도 SDN 기반 WMN 제어 기능이 제공됨으로 물리적 링크의 특성과 무관하게 적용이 가능하다.

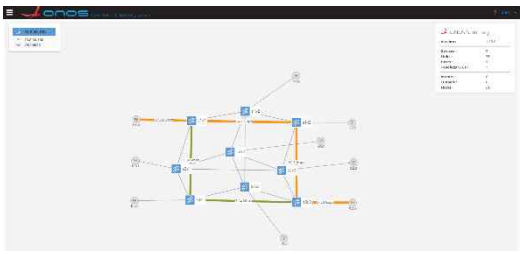


그림 3a. 장애 발생 전 비상통신망 트래픽 흐름도

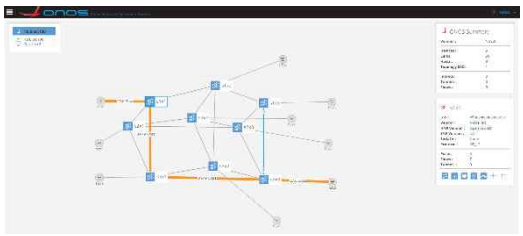


그림 3b. 장애 발생 후 비상통신망 트래픽 흐름도

그리고 그림 4는 본 비상통신망 구조에서 핵심 기능 중 하나인 Traffic Monitoring and Analysis 기능을 지원하기 위해 SDN Controller에서 제공되는 플로우 트래픽 측정 기능을 적용한 예를 도시한다. 이 기능을 적용하면 각 링크별 트래픽 사용량과 링크상의 플로우별 세부 트래픽 세부 통계 정보를 수집 가능하며 이 정보를 기반으로 네트워크의 성능 저하나 장애 여부를 판단할 수 있는 기반 정보가 된다.

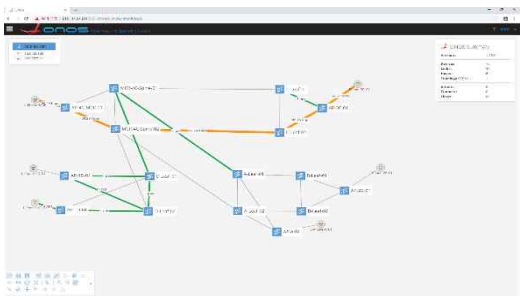


그림 4. 비상통신망 트래픽 모니터링 기능 예시도

Ⅲ. PoC 시스템 구현

3.1 PoC 시스템 구현

본 절에서는 제안된 비상통신망 구조를 PoC 시스템으로 구현하고 기능 검증을 위해 실험실 및 현장 시연을 한 결과를 소개한다. 그림 5는 PoC 시스템 구현 구조도이다.

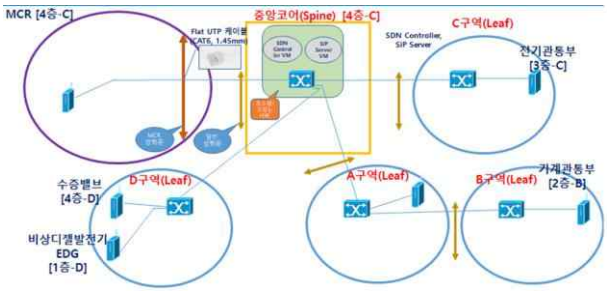


그림 5. 단일 건물용 비상통신망 구현 구조도

Hybrid Spine-Leaf 구조 기반 유무선 통신망구조로 구현되었으며 중앙 코어에 Spine 노드, SDN컨트롤러, SIP/DHCP 서버가 하나의 이동형 패키지에 통합 구현되었으며, C, D, A 구역에 적용될 3개의 Leaf 노드는 스위치 기능만을 이동형 패키지로 각각 개발되었다. 이들 노드들은 중앙 Spine 노드에 연결되었으며, B구역 Leaf 노드는 Spine 노드와 직접 연결할 수 없는 물리적인 제약 조건으로 A Leaf 노드에서 연장되어 연결되어서 Hybrid spine-leaf 구조를 완성하였다. 이들 스위치의 휴대성을 높이기 위해 Controller/Data 네트워크를 하나의 물리 회선에 2개의 논리 회선으로 구분하여, 이더넷 회선 수를 하나로 줄였으며 Spine 노드 소형화/고성능화를 통하여, SDN Controller/SIP Server를 하나의 물리 서버에서 VM 가상화 구조로 설계 변경하였다(VirtualBox). 그리고 각 AP 노드는 Wifi AP와 전화기로 구성된 이동형 패키지로 통합되어 있으며 유선 IP폰과 스마트폰을 AP에 연결하고, 방화문 격벽 간 차폐막 연결은 방화문 아래의 최소 공간을 통과할 수 있는 Flat-UTP 케이블 (CAT6, 1.45mm) 사용하여 연결되었다. 배터리는 8시간 가동을 원칙으로 하며, 배터리는 리튬인산철 배터리를 사용하고 그 이상 운영을 대비하여 보조 배터리를 연결하여 사용하며 이 보조 베터리는 교환 가능하도록 하여 운영의 지속성을 확보하였다.

그리고 이들 단일 건물내부 네트워크는 LTE 네트워크를 통해 연결되어 있으며 그림 6은 3개의 단일 네트워크가 LTE를 통해 연결된 토폴로지를 ONOS SDN controller[4]가 제어/관리하는 GUI 화면을 도시한다.

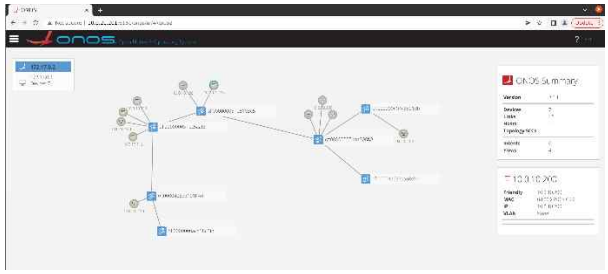


그림 5. ONOS Controller clustering 연동 결과

아래에 각 이동형 패키지에 대한 세부 구현 내용을 정리하였다.

● LTE 이동일체형 패키지



그림 6. LTE 이동일체형 패키지

패키지는 원전 건물 유선 네트워크들 간을 연결하기 위한 이동 코어 네트워크로 eNB, EPC, PTT 서버가 일체형으로 구성되었으며 각 유선네트워크의 Spine 스위치에 이동 모뎀을 설치하여 LTE망을 접속하고 이들 간에 GRE-TAP 터널로 연결하여 동일 서브넷으로 SDN Controller에서는 인식한다. (그림 5 참조)

● Spine/Leaf 스위치 이동형 패키지

본 패키지는 미니 PC(Intel NUC 11 Pro TNKi7) 기반 Spine용 오픈플로우 OVS 스위치, ONOS SDN Controller/SIP/DHCP VM 서버, 배터리로 구성되며 이들을 이동형 패키지로

아래의 그림 7과 같이 제작하였다. 본 패키지 운영자들은 세부 구성 요소와 무관하게 외부로 노출되어 있는 인터페이스를 통한 케이블 연결만으로 간단히 네트워크 구축이 가능하며 크기와 무게를 경량화 하여 쉽게 이동이 가능하도록 제작되었다.



그림 7. Spine/Leaf 노드 이동형 패키지

3.2 PoC 시스템 시험 및 검증

상기에서 제작된 PoC 시스템의 기능 검증을 위해서 그림 8과 같이 실증 시험망을 구성하고 1차적으로 실험실과 2차적으로 현장 시험을 진행하였다. 실험실 시험에서는 패키징 전 단계의 Spine, Leaf 스위치 및 AP 패키지로 구성된 한 개의 호기 건물 유선 네트워크 2개를 LTE 터널로 연결하여 음성 및 데이터 서비스 기능을 시험하였다.



그림 8. PoC 시스템 실증 시험 환경

먼저 연구실/현장 환경에서 네트워크 자율 구축을 위해 Spine과 Leaf 노드 및 이들을 연결하는 링크의 상태, 그리고 AP 노드와 단말의 연결 기능을 ONOS controller를 통해서 확인을 하는 과정과 각 단말간의 음성 통신을 시험하고 이어서 서비스 품질 및 네트워크 트래픽 상태를 모니터링하는 시험을 시행하였으며 마지막으로 장애 발생 시 네트워크 자율 복구 기능이 동작하는 지에 대한 시험을 수행하였으며 모든 기능 시험이 계획 대비 정상적으로 완료되었음을 확인하였다.

Ⅳ. 결론 및 향후 연구 방향

본 논문에서는 후쿠시마 원전 사태와 같은 극한 자연재해로 인해 파괴된 통신 기능을 SDN/SON/LTE 기반 기술을 활용하여 의료 비상 구급상자와 같이 네트워크 구급상자를 제작하여 비상시 통신 비전문가들이 발전소 전구간 필요 장소로 이동 연결만하고 전원만 켜면 음성 및 데이터 통신이 가능하게 하는 독립 네트워크가 자율적으로 구축될 수 있는 기술에 대한 구조 설계 및 구현과 시험 검증에 대해 기술하였다.

서비스 측면에서도 현재 제공되는 음성 및 비교적 단순한 데이터 통신 서비스 뿐만아니라 파괴된 원전 내부의 복잡한 시설들의 복구에 현실감 있게 현장의 상황을 파악하기 위해 필수적인 운전원과 운영 본부와의 증강 현실 기술 기반의 실시간 멀티미디어 통신을 위한 확장이 필요하다. 이를 위해 네트워크 측면에서 지원되어야할 연구 이슈들은 향후 연구를 통해서 해결 방안을 제시할 예정이다.

Acknowledgement

본 논문은 2020년도 한국수력원자력(주)의 재원으로 지원을 받아 수행된 연구결과임. (2021.06~2023.05, 극한 자연재해 대비 발전소 전 구간 및 외부 통신을 지원하는 유무선 비상통신망 구축 기술 개발)

참고문헌

[1] Grag Cross, Open Networking Forum SDN standards, Jan. 2017. Accessed Nov. 15, 2017. https://www.opennetworking.org/ software-defined-standards/overview

[2] 3GPP SON, https://www.3gpp.org/technologies/keywords-acronyms/105-son

[3] Rosenberg, J., et. al, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[4] Grag Cross, ONOS open source project, Jan. 2017. Accessed Nov. 15, 2017., https://www.opennetworking.org/platforms/onos/.

CPU 자원 예측과 SFC 의 VNF 그룹 별 Scaling 연구

최민지, Suman Pandey*, 유재형†, 홍원기†

포항공과대학교 인공지능대학원

*광주과학기술원 전기전자컴퓨터공학부

†포항공과대학교 컴퓨터공학과

minjichoi@postech.ac.kr

*suman17@gist.ac.kr

†{jhyoo78, jwkhong}@postech.ac.kr

CPU resource prediction and VNF group-wise Scaling of SFC

Minji Choi, Suman Pandey*, Jae-Hyoung Yoo†, James Won-Ki Hong†

Graduate School of Artificial Intelligence, POSTECH
*School of Electrical Engineering and Computer Science, GIST
†Department of Computer Science and Engineering, POSTECH

요 약

오늘날 네트워크의 서비스는 많은 양의 트래픽을 생성한다. 이 모든 트래픽은 보안, 침입 탐지, 로드 밸런싱 등의 다양한 네트워크 기능을 제공하기 위해 일련의 네트워크 기능들로 구성된 서비스인 서비스 기능 체이닝(SFC, Service Function Chaining)의 통과를 필요로 한다. 서비스에 대한 요청이 증가함에 따라 서비스 제공자들은 SFC 를 적절히 배치하고 가상 네트워크 기능 스케일링을 진행해야 한다. SFC 의 적절한 배치와 스케일링은 처리량, 종단 간 지연, 그리고 성공적인 요청 처리의 측면에서 서비스 수준 계약(SLA)을 보장한다. SFC 배치와 스케일링은 상관관계가 있지만, 작업은 별도로 모델링 되어야 한다. 서비스 기능 체이닝 배치를 위해서는 CPU, 메모리, 대역폭 그리고 서버의 위치 등을 고려해야 한다. 반면, 스케일링을 위해서는 별도의 매트릭스로서 가상 네트워크 기능(VNF, Virtual Network Function)의 자원 사용량을 고려해야 한다. 스케일링 기능은 새로운 가상 네트워크 기능을 배치하는데 추가적인 비용과 시간이 요구된다. 그렇기 때문에 앞으로 들어올 트래픽이 필요로 하는 가상 네트워크 기능의 필요 자원 요구량을 미리 예측하는 것이 중요하다. 본 논문에서는 지도학습의 한 종류인 RNN(Recurrent Neural Network) 기반 GRU(Gated Recurrent Unit) 모델을 이용하여 VNF 의 CPU 사용량을 예측한다. 예측된 사용량을 기반으로 가상 네트워크 기능의 그룹별 스케일링을 진행하여 스케일링 시 비용과 시간을 최소화하고자 한다. 이후, Q-learning 알고리즘을 엣지 컴퓨팅 환경에 적용한 EdgeQL 알고리즘을 통해 가상 네트워크 기능의 배치를 결정한다.

Ⅰ. 서 론

과거의 방화벽, 침입탐지시스템(IDS), 프록시(proxy) 등의 네트워크 기능(NF, Network Function)들은 미들박스 등의 전용 하드웨어 장치에 내장되어 있었다. 미들박스는 과부하를 효율적으로 처리하도록 설계되었다. 이들은 구입 및 유지 비용이 매우 높으며 탄력 있는 기술 구현이 불가능하다는 단점이 있다. 따라서, 클라우드 서비스 공급자와 운영자들 사이에는 기본 하드웨어에서 네트워크 기능을 분리하고 가상 네트워크 기능(VNF)을 사용하여 상용 서버에서 실행하고자 하는 경향이 있다. 추가적으로 서비스 기능 체이닝은 이후의 트래픽 흐름 조정을 위해 가상 네트워크 기능들을 함께 연결할 수 있도록 체인을 구성한다.

서비스 기능 체이닝은 서비스 요청의 증가와 감소에 따라 자동적인 스케일링 기능을 제공해야 한다. 또한, 서비스 기능 체이닝의 스케일링은 체인의 각기 다른 어플리케이션 그룹에 서로 다른 메커니즘을 제공함으로써 어플리케이션마다 독립적이어야 한다. 서비스 기능 체인 내의 어플리케이션들은 서로 다른 특징을 가지고 있다. 예를 들어 규칙(rule)이 더 많이 추가된 방화벽은 그렇지 않은 방화벽에 비해 CPU 사용량이 더 많다. 어플리케이션 독립적인 스케일링을 통해 네트워크 관리자는 더 이상 가상 네트워크 기능의 서로 다른 자원량 요구 사항을 고려하지 않아도 된다. 자동 스케일링 모듈은 설치된 어플리케이션 특정 요구 사항에 따라 체인의 각 어플리케이션 그룹을 유연하게 확장해야 한다. 더불어 새로 스케일 된 가상 네트워크 기능들은 서비스 기능 체인의 전반적인 종단 간 지연 최소화가 필요한 경우에는 엣지(Edge)에 배치해야 한다.

Ⅱ. 관련 연구

1. 가상 네트워크 기능 자원 기반 자동 스케일링

정책에 기반하여 스케일링 결정을 내리는 것은 가장 널리 사용되는 스케일링 방식이다 [1][2]. 서비스 제공업자들은 CPU 사용량, 메모리 사용량, I/O, 또는 트래픽 요청 등의 입력 임계값을 정의함으로써 1 개 또는 그 이상의 자동 스케일링 정책을 제공할 수 있다. 또 다른 서비스 제공업자들은 스케줄 기반 자동 스케일링을 제공하기도 한다 [3]. 이러한 임계값 기반 스케일링 기술은 오늘날 클라우드 상황에서 잘 작동하지만, 자원 사용량이 임계값을 넘겨야만 스케일링을 진행하기 때문에 여러 차례 과소 공급이 초래될 수 있다.

2. 어플리케이션 매트릭스 기반 자동 스케일링

자동 스케일링은 응답 시간, 연결 오류, 시간 초과 등을 포함하는 어플리케이션 수준의 매트릭스에 기반하기도 한다[4][5]. 이러한 접근 방식은 서버의 스케일링 또는 하나의 가상 네트워크 기능 스케일링에서 잘 작동한다. 서비스 기능 체인 스케일링에서 이 방식은 체인 내 병목현상을 찾기 위해 추가적인 모듈을 필요로 한다. 결국 스케일링 모듈은 가상 네트워크 기능의 자원 사용량 매트릭스를 이용하여 서비스 기능 체인의 어떤 레이어가 SLA 위반의 원인이 되는지 찾아내야 한다.

3. 사전 예방적 기계학습 기반 스케일링

사전 예방적 접근에서 예측 기술은 시스템이 어떤 자동 스케일링 결정을 해야 하는지 자동적으로 미래 수요를 학습하고 예측하도록 한다. 이 문제를 해결하기 위해 다양한 기계학습 방법들이 사용되어 왔는데, 특히 어플리케이션 별 맞춤형 스케일링을 제공을 위한 동적 임계값 예측 방법이 가장 널리 사용되어 왔다[6][7]. 반면, 또 다른 논문들은 과거의 데이터 정보를 기반으로 자원 사용량을 예측하는 시계열 모델을 제안했다[8][9]. [10]은 예측적인 자동 스케일링을 위해 랜덤 포레스트 알고리즘과 같은 지도학습 방법을 제안했으며, [11]은 서버가 없는 구조에서의 요청 기반 강화학습 접근을 연구했다.

최근에는 LSTM 을 기반으로 NFV(Network Function Virtualization) 환경에서 자원을 예측하는 연구가 진행되었으나, 시뮬레이션 상황에서 진행되었으며 스케일링을 위한 실험은 진행되지 않았다 [12]. 더 나아가 지도학습 기반 예측 모델을 통해 예측이 얼만큼 가능한지 증명하고자 한 연구[13]와 각 가상 네트워크 기능 별 미래 자원 요구량을 그래프 신경망 알고리즘을 이용한 연구[14]도 진행되었다.

Ⅲ. 설계 및 구현

동일한 양의 트래픽에 대해 가상 네트워크 기능 별 CPU 사용량은 그림 1 과 같이 다를 수 있다. 들어오는 요청의 수가 같을 때 침입탐지시스템은 방화벽과 프록시보다 더 많은 양의 CPU 사용량을 필요로 한다. 또한, 규칙이 더 많이 추가된 방화벽은 그렇지 못한 방화벽보다 CPU 사용률이 높다. 이것은 동일한 어플리케이션이 버전 및 업데이트에 따라 다른 자원 사용 특정을 가질 수 있음을 보여준다.

가상 네트워크 기능의 자원 사용량은 연속적인 데이터로 모델링 될 수 있다. RNN 은 이러한 연속적인 데이터 또는 시계열 데이터를 모델링하도록 설계되었다. RNN 에서 히든 레이어 h(t)는 입력 레이어 x(t)로부터 현재의 타임스탬프와 이전 타임스탬프의 히든 레이어 h(t-1)을 입력으로 받는다. 이러한 방식을 통해 RNN 은 과거의 정보를 기억하고 그에 따라 새로운 이벤트를 처리할 수 있다. GRU 는 RNN 의 한 종류로, 간단한 구조로 효율적인 계산이 가능하다. GRU 기반 자원 예측 모델은 과거의 자원 사용량을 기반으로 각 VNF 그룹 별 미래 자원 요구량 값을 제공한다.

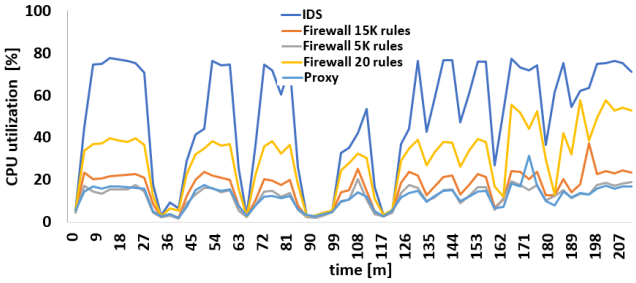


그림 1. VNF 종류에 따른 CPU 사용률 분석

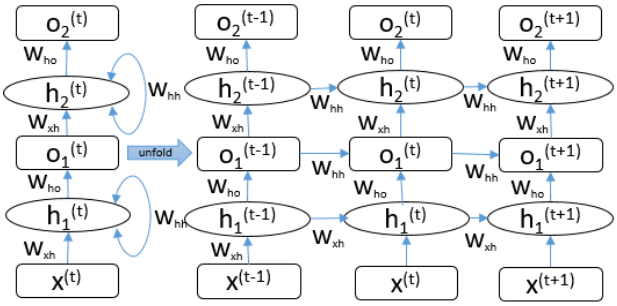


그림 2. RNN 의 다층 구조

GRU 에서 받은 CPU 예측 값과 알고리즘 내에서 설정한 임계값을 기반으로 스케일링이 결정된다. 임계값은 가상 네트워크 기능이 감당할 수 있는 요청의 최대값을 기반으로 정해진다. 실험에서 CPU 사용률의 상한 임계값은 80%이고 하한 임계값은 70%이다. 자동 스케일링 알고리즘은 각 가상 네트워크 기능 별로 스케일링 결정을 포함한 매트릭스를 반환한다. 스케일링 결정이 이루어진 이후에는 가상 네트워크 기능을 실제 서버에 배치하기 위해 Edge Q-Learning (Edge QL)이 사용된다. Scale-in 의 경우에는 단순히 가장 최근에 생성된 가상 네트워크 기능을 삭제한다. 전반적인 프로세스는 그림 3 와 같다.

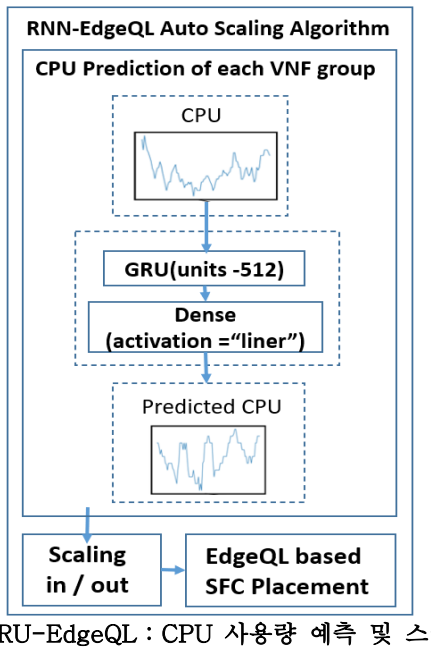


그림 3. GRU-EdgeQL : CPU 사용량 예측 및 스케일링

본 논문에서 EdgeQL 알고리즘은 종단 간 지연과 SLA 위반을 최소화하기 위해 가상 네트워크 기능의 배치에 사용된다. EdgeQL 알고리즘은 Q-learning 알고리즘을 엣지 컴퓨팅 환경에 적용한 것이다. 이 때, Q-learning 액션 공간은 크게 로컬, 이웃, 그리고 데이터센터 서버의 3 가지 계층 구조로 구분되며, 가상 네트워크 기능 사이의 hop 수와 서비스 기능 체인의 길이에 따라 달라지는 보상 함수를 사용한다.

Algorithm 1 Auto-Scaling

Input: $\vec{ut}$, $\vec{lt}$, t_window
for each VNF-Group 1 to n **do**
  Initialize list A and R
  for CPU resource of each VNF-Group **do**
    $T_n = (\sum_{i=0}^{c_n} r_i)$
    $P_n = GRU_pre(T_k^n, t_window)$
    $A_n = \frac{P_n}{c_n}$
    $R_n = \begin{cases} 0 & A_n > ut_k \\ 1 & A_n < lt_k \end{cases}$
    A.append(A_n)
    R.append(R_n)
  end for
  $f(R_n) = \begin{cases} scaleout, & max\left(\left(\frac{P_n}{ut_k}\right) - c_n\right) & \prod R_n = 0 \\ scalein, & -min\left(c_n - \left(\frac{P_n}{lt_k}\right)\right) & \prod R_n = 1 \wedge c_n > 1 \\ maintain \end{cases}$
  O.append(f(R_n))
end for
return O

Ⅳ. 성능 평가

실험은 크게 미래 자원 요구량을 예측과 이를 기반으로 한 스케일링 및 가상 네트워크 기능을 배치로 구분될 수 있다. 본 논문은 GRU 를 이용하여 CPU 요구량을 예측하여 스케일링 결정 후 Edge QL 알고리즘을 이용하여 가상 네트워크 기능을 배치했다.

그림 4 는 GRU 를 이용한 CPU 요구량 예측 결과값과 필요한 서버 개수의 예측 결과값을 보여준다. 본 논문에서 사용한 알고리즘은 워밍업 단계를 30 으로 작게 설정했기 때문에 초반의 예측 정확도는 낮으나, 예측 시작 후 150 분 이상 경과하면 예측 정확도가 어느정도 높아짐을 알 수 있다.

GRU 로 예측한 CPU 사용량을 기반으로 스케일링을 진행하면 스케일링의 변화를 최소화할 수 있다. 이는 곧 새로운 가상 네트워크 기능을 배치하는데 요구되는 추가적인 비용과 시간을 절약할 수 있다.

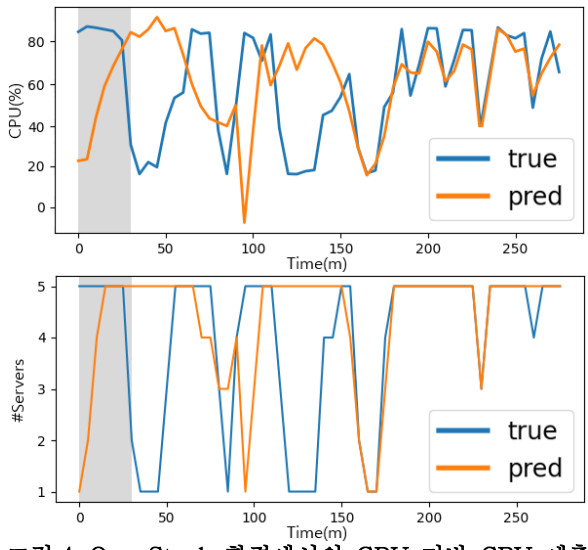


그림 4. OpenStack 환경에서의 GRU 기반 CPU 예측

관련 연구에서는 스케일링 시 단순 임계값 기반 스케일링 방법을 사용한다. 그리고, 가상 네트워크 기능들을 엣지에 배치하지 않는 경우에는 대부분 OpenStack 이 자동적으로 배치하는 방법을 사용한다. 이 두 가지 방법을 본 논문의 GRU 를 이용한 스케일링 방법과 EdgeQL 배치 방법과 조합하면 총 4 가지 경우의 수가 있다.

1) 임계값 기반 스케일링 - OpenStack 기본배치
2) GRU 이용 스케일링 - OpenStack 기본배치
3) 임계값 기반 스케일링 - EdgeQL 배치
4) GRU 이용 스케일링 - EdgeQL 배치

알고리즘의 성능 평가를 위해 각 알고리즘 별 1) 평균 지연 시간, 2) SLA 위반률, 그리고 3) 스케일링 빈도율을 측정하여 비교해보았다. 그림 5 는 본 논문에서 제안하는 GRU-EdgeQL 방식이 다른 방식과 비교하여 평균지연시간, SLA 위반률, 그리고 스케일링의 빈도 측면에서 모두 가장 작은 값을 가짐을 나타낸다.

Ⅴ. 결론 및 향후 연구

본 논문에서는 GRU-EdgeQL 알고리즘을 이용하여 CPU 자원의 사용률 예측과 서비스 기능 체인의 가상 네트워크 기능 그룹 별 스케일링을 설명하였다. GRU-EdgeQL 알고리즘은 RNN 의 한 종류인 GRU 를 이용하여 CPU 요구량을 예측하여 스케일링을 결정한 뒤, EdgeQL 알고리즘을 이용하여 가상 네트워크 기능을 배치한다. 이는 임계값 기반의 OpenStack 기본 배치 방법과 비교하여 현저히 낮은 평균 지연 시간, SLA 위반률, 그리고 스케일링 빈도 값을 가지며 이는 보다 더 적은 비용과 시간으로 같은 일을 처리할 수 있음을 의미한다.

가상 네트워크 기능에는 CPU, 메모리, I/O, 트래픽, 대역폭 등의 많은 자원 요소들이 존재한다. 따라서, 향후 연구에서는 가상 네트워크 기능의 모든 자원 요소들을 고려하여 RNN-EdgeQL 알고리즘을 이용한 자동 스케일링 및 배치를 구현할 계획이다.

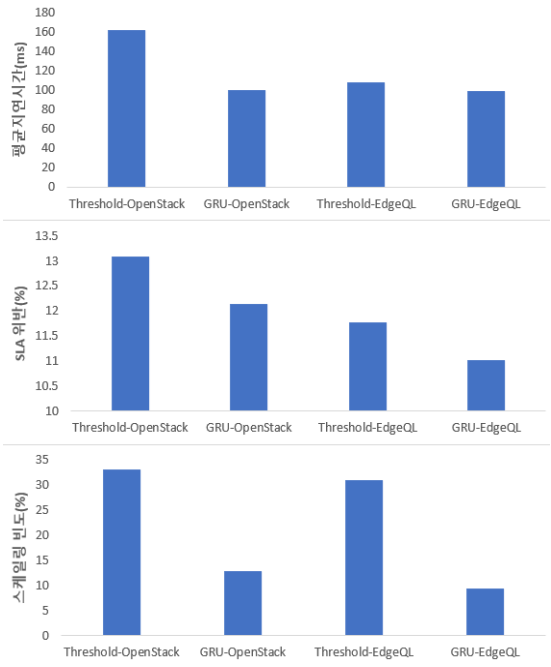


그림 5. SFC 길이 3, Wiki 트래픽 검증 결과

ACKNOWLEDGMENT

이 논문은 2022 년도 정부 (과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원 (2018-0-00749, 인공지능 기반 가상 네트워크 관리기술 개발)과 대학 ICT 연구센터육성지원사업의 연구결과로 수행되었음 (IITP-2022-2017-0-01633).

참 고 문 헌

[1]https://cloud.google.com/compute/docs/autoscaler/scaling-schedules

[2] Singh, P., Kaur, A., Gupta, P. et al. RHAS: robust hybrid auto-scaling for web applications in cloud computing. Cluster Comput 24, 717– 737 (2021). https://doi.org/10.1007/s10586-020-03148-5

[3] X. Wang et al., "Dynamic Resource Scheduling in Mobile Edge Cloud with Cloud Radio Access Network," in IEEE Transactions on Parallel and Distributed Systems, vol. 29, no. 11, pp. 2429-2445, 1 Nov. 2018, doi: 10.1109/TPDS.2018.2832124.

[4] Tang, Pengcheng et al. “Efficient Auto-Scaling Approach in the Telco Cloud Using Self-Learning Algorithm.” 2015 IEEE Global Communications Conference (GLOBECOM) (2014): 1-6. [5(9)]

[5] Wajahat, Muhammad, et al. "Mlscale: A machine learning based application-agnostic autoscaler." Sustainable Computing: Informatics and Systems 22 (2019): 287-299.

[6] K. Thonglek, K. Ichikawa, K. Takahashi, H. Iida and C. Nakasan, "Improving Resource Utilization in Data Centers using an LSTM-based Prediction Model," 2019 IEEE International Conference on Cluster Computing (CLUSTER), 2019, pp. 1-8, doi: 10.1109/CLUSTER.2019.8891022.

[7] A. Bilal, T. Tarik, A. Vajda and B. Miloud, "Dynamic Cloud Resource Scheduling in Virtualized 5G Mobile Systems," 2016 IEEE Global Communications Conference (GLOBECOM), 2016, pp. 1-6, doi: 10.1109/GLOCOM.2016.7841760

[8] W. Iqbal, A. Erradi, M. Abdullah, and A. Mahmood, “Predictive autoscaling of multi-tier applications using performance varying cloud resources,” IEEE Transactions on Cloud Computing, 2019. doi: 10.1109/TCC.2019.2944364.

[9] Schuler, Lucia, Somaya Jamil, and Niklas Kühl. "AI-based resource allocation: Reinforcement learning for adaptive auto-scaling in serverless environments." 2021 IEEE/ACM 21st International Symposium on Cluster, Cloud and Internet Computing (CCGrid). IEEE, 2021

[10] H. Kim, D. Lee, S. Jeong, H. Choi, J. Yoo and J. W. Hong, "Machine Learning-Based Method for Prediction of Virtual Network Function Resource Demands," 2019 IEEE Conference on Network Softwarization (NetSoft), Paris, France, 2019, pp. 405-413, doi: 10.1109/NETSOFT.2019.8806687.

[11] S. Lange, H.-G. Kim, S.-Y. Jeong, H. Choi, J.-H. Yoo, and J. W.- K. Hong, “Machine learning-based prediction of vnf deployment decisions in dynamic networks,” in 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS). IEEE, 2019, pp. 1- 6.

[12] R. Mijumbi, S. Hasija, S. Davy, A. Davy, B. Jennings and R. Boutaba, "Topology-Aware Prediction of Virtual Network Function Resource Requirements," in IEEE Transactions on Network and Service Management, vol. 14, no. 1, pp. 106-120, March 2017, doi: 10.1109/TNSM.2017.2666781

[13] S. Pandey, J. W. -K. Hong and J. -H. Yoo, "Q-Learning based SFC deployment on Edge Computing Environment," 2020 21st Asia-Pacific Network Operations and Management Symposium (APNOMS), Daegu, Korea (South), 2020, pp. 220-226, doi:10.23919/APNOMS50412.2020.9236981.

A Decentralized Approach for Virtual Reality(VR)-based Services in 5G and Beyond

Tri Nguyen Dang, Choong Seon Hong

Department of Computer Science and Engineering
Kyung Hee University, 446-701, Korea
email: {trind, cshong}@khu.ac.kr

Abstract

Augmented and Virtual reality (AR/VR)-based services are proving themselves to be one of the key roles in enabling 5G and beyond services. VR-based services require a significant amount of communication and computational resources. To cope with these requirements, we can use Multi-access Edge Computing (MEC) that bring the resources close to the end-users. However, some of the UEs might not be able to access the MEC due to limitations on physical resources. Therefore, we propose a novel network model that allows UE to share the VRC among themselves if they have the same field-of-view (FoV) via device-to-device communication (D2D). In which, the VRC can be served via a cellular link or D2D links. We then formulate an optimization based on the Linear Programming method to reflect the efficiency of our proposal.

1 Introduction

The tremendous development of 5G has enabled various applications for infotainment services. In which Augmented/Virtual reality (AR/VR)-based services are rising to be one of the main players in future infotainment services[1]. However, these application services require a significant amount of communication and computation resources[2]. Meanwhile, most of the existing AR/VR-based devices have constrained computing capability. To cope with these challenges, we can employ the advantage of MEC which brings the resources close to the end-users[3]. By doing so, we can reduce a significant amount of the data traffic in the network. Moreover, storing the frequently requested content in the MEC cache storage is considered a remarkable solution for reducing redundant computing tasks. The author in [2] proposed a caching strategy for VR-based content via the availability of users based on contract theory. The work in [4] considered the mode selection for VR-based services based on the probabilistic model. Several works have been considered MEC-assisted AR/VR-based services [5], [6], and [7]. In this paper, we propose a network model that allows D2D communication to enabled AR-based infotainment services. In which, VR content can be served via D2D links under some special condition such as the similarity between two user's field-of-views. Next, we present our system model and problem formulation.

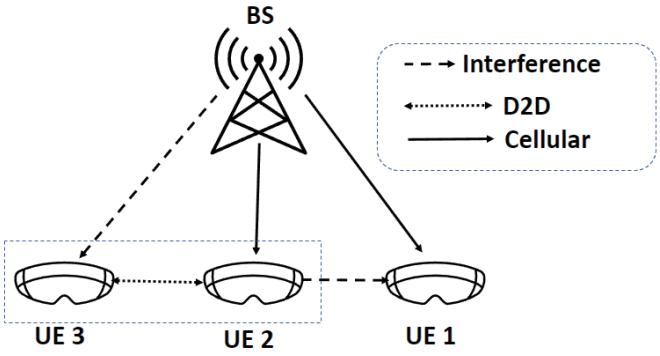


Fig. 1: Illustration of our system model.

2 System model and problem formulation

In this paper, we consider a network services model with a single base station, a set of N users, and a virtual reality content (VRC)(in Fig. 1). Let $\mathcal{C} = \{C_0, C_1, \ldots, C_T\}$ be the set of chunks of VRC, where T is the length of VRC, and C_0 is the initial chunk of the VRC. Each chunk $C_t \in \mathcal{C}$ is also a 360-degree video format. However, each time slot t a user can watch at most 120-degree video which equivalent a part of chunk C_t due to the human eyes perception [4]. Moreover, we assume that UEs are using VR-based services such as watching VRC on Head Mounted Devices (HMDs), Oculus Rift, Samsung GearVR, or Sony PlayStation VR, etc. Each device has a different type of playback format such as: equirectangular (ERP), cubemap (CMP), adjusted

cubemap projection (ACP), adjusted equal-area projection (AEP), Equi-angular projection(EAC)[8]. For instance, the playback format in most of smartphone is EAC projection format. Typically, when UE request for a VRC, the SBS either serve the request immediately if the requested VRC is in its cache storage, otherwise, it needed to fetch the requested VRC from EPC then forward to UEs. However, the size of an VRC is lager than regular video contents. It requires an larger amount of bandwidth to delivery to UEs. Thus, saving system bandwidth is a remain challenges for serving VRC in a wireless manner. Therefore, we investigate the advantage of user's Fidel-of-View to cope with this challenges.It means that each time slot t only the visible part of VRC will be serve at the highest quality which depend on channel condition between UE and BS. Meanwhile the remaining part the chunk C_t will be serve on a lower quality. Moreover, we assume that the VRC is allowed to serve via cellular link, e.g from BS to UE, or D2D link, e.g, from UE to UE. Based on FoV definition, we let f_i^t be the visible part of the VRC of UE i at time slot t, where $f_i^t \subset C_t$. Basically, the BS will use the cellular link to serve the request of UE. However, due to the limitation of physical resources, some of the quest might delayed or drooped if there is a huge amount of request from end-users. Therefore, we proposed a method that allows UE to share the VRC with the other UE via D2D communication if and only if the two UEs have similar visible part. Let ϵ be the threshold for similarity between f_i^t and f_j^t, $i \neq j, i, j \in N$. Let $x_{i,j}$ be the decision variable whether UE i and j able to share the VRC at time slot t or not, and $G(f_i^t, f_j^t) \rightarrow \mathbf{R}_+$ be the function that measurement the similarity between f_i^t and f_j^t.

$$x_{i,j}^t = \begin{cases} 1, & \text{, if } G(f_i^t, f_j^t) \geq \epsilon, \\ 0, & \text{otherwise.} \end{cases} \tag{1}$$

On the other hand, we let $R_{i,0}^t$, and $R_{i,j}^t$ denote the achievable rates between UE i and the BS, and between UE i and UE j at time slot t, respectively. $R_{i,0}^t$ is given by:

$$R_{i,0}^t = B_t \log_2 \left(1 + \frac{p_{i,0}^t g_{0,i}^t}{\sum_{j \in N, i \neq j} p_j^t g_j^t + I_0}\right), \tag{2}$$

where $p_{i,0}^t$ is the transmit power of the BS, $g_{i,0}^t$ is the channel gain of UE i, and $\sum_{j \in N, i \neq j} p_j^t g_j^t$ is the co-tier interference from D2D UEs that use the same channel with UE i, and I_0 is the Additive Gaussian White Noise (AGWN). Similarly, $R_{i,j}^t$ is given by:

$$R_{i,j}^t = B_t \log_2 \left(1 + \frac{p_{i,j}^t g_{i,j}^t}{p_{0,i}^t g_{0,i}^t + \sum_{l \in N, l \neq i, l \neq j} p_{l,j}^t g_{l,j}^t + I_0}\right), \tag{3}$$

where $p_0[t] g_0[t]$ is the interference from cellular link, and $\sum_{l \in N, l \neq i, l \neq j} p_{l,j}^t g_{l,j}^t$ is the interference from D2D links . Consequently, we formulated an optimization as follows:

$$\mathbf{P}: \max_{x_{i,j}} \sum_{t=1}^{T} \sum_{(i,j) \in N, i \neq j} x_{i,j}^t \tag{4a}$$

s.t.:

$$\mathbf{C1}: G(f_i^t, f_j^t) \geq \epsilon, \forall i, j \in N, i \neq j, \forall t \in T, \tag{4b}$$

$$\mathbf{C2}: R_{i,j}^t \geq R_{\min}, \forall i, j \in N, i \neq j, \forall t \in T, \tag{4c}$$

$$\mathbf{C3}: R_{i,0}^t \geq R_{\min}, \forall i \in N, \forall t \in T, \tag{4d}$$

where the objective function is maximize the number of D2D pair that can share the VRC, constraint **C1** guarantee the quality of experience (QoE) by take into account the similarity between two content of UE i and j, constraint **C2** guarantee the quality of service(QoS) for D2D links, and constraint **C3** guarantee the QoS of cellular link. Our optimization is fall linear programming category due either linear or affine constraints. Thus, it is solvable via Linear Programming method. the detail of the algorithm is state in Alg. 1.

Algorithm 1 Algorithm for D2D transmission methodology of VRC in wireless network.

Input: $\mathcal{N}, \mathcal{C}, f(\cdot), G(\cdot), T$
Output: $\boldsymbol{x}$

```
repeat
    t ← t + 1;
    Calculate the similarity between UE i, and j, θ^t_{i,j} ≜ G(f^t_i, f^t_i);
    x_{i,j} = arg max{∑_{j∈N,j≠j} θ^t_{i,j}}
    if x_{i,j} = 1 then
        UE i is served via D2D link;
    else
        UE i is served via cellular link;
    end if
until t=T
```

3 Numerical Results

In order to validate our proposal framework, we used Python3.7 as our simulation tool. Moreover, there is no real data set that is compatible with

TABLE 1: Simulation parameters.

Parameter	Value
Length of content (T)	1000
Number of UEs (N)	100 UEs
White-noise (I_0)	-174 dBm/Hz
System bandwidth(B)	3 MHz
Similarity threshold (ϵ)	$\{0.8, 0.85, 0.9, 0.95\}$
Minimum achievable rate($R_{\min}$)	3.5(Mbps)

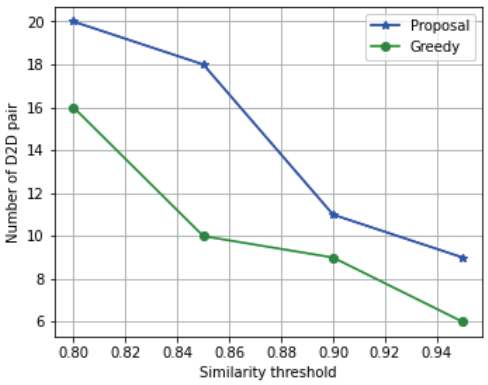


Fig. 2: Number of D2D pairs versus similarity threshold

our system model, thus, we use synthesis data by randomization function in Python. $G(\cdot)$ function is considered as the Kullback–Leibler(KL) divergence function. The main parameters are stated in Table. 1. Fig. 2 shows that when we increase the similarity threshold, the number of D2D pairs that can share VRC is reduced significantly due to the tight protection for QoE. On the other hand, when the number of D2D is reduced, the average achievable of the network is increasing due to the D2D link interference is reduced as shown in Fig. 3. Therefore, we can see that there is a trade-off between the number of D2D pairs in the network and the average achievable data rate. The more D2D pairs the higher the spectrum efficiency and vice versa.

4 Conclusion

In this paper, we proposed a novel framework for AR/VR-based services in the wireless network. In which, we exploit the user's FoV to measure the similarity between FoVs, thus, we can utilize the D2D communication to improve the spectrum efficiency of the network. Our simulation results show that the proposed framework is reasonable and achieve a better performance compare to the Greedy approach.

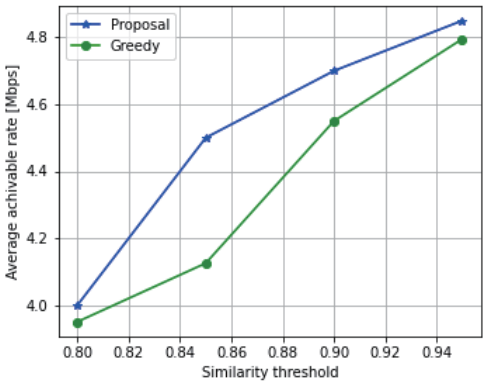


Fig. 3: Average achievable rate of the network

Acknowledgments

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. 2020R1A4A1018607) *Dr. CS Hong is the corresponding author.

References

[1] T. N. Dang, J. M. Jeon, L. U. Khan, A. Manzoor, and C. S. Hong, "Decentralized collaborative caching-based virtual reality for 5g and beyond," in *2021 22nd Asia-Pacific Network Operations and Management Symposium (APNOMS)*, 2021, pp. 394–397.

[2] T. N. Dang, K. Kim, L. U. Khan, S. A. Kazmi, Z. Han, and C. S. Hong, "On-device computational caching-enabled augmented reality for 5g and beyond: A contract theory-based incentive mechanism," *IEEE Internet of Things Journal*, 2021.

[3] Y. Siriwardhana, P. Porambage, M. Liyanage, and M. Ylianttila, "A survey on mobile augmented reality with 5g mobile edge computing: Architectures, applications, and technical aspects," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 1160–1192, 2021.

[4] T. N. Dang and C. S. Hong, "Mode selection for 360-degree video streaming over wireless network," *Journal of Korean Information Science Society*, pp. 1270–1272, 2021.

[5] Y. Cheng, "Edge caching and computing in 5g for mobile augmented reality and haptic internet," *Computer Communications*, vol. 158, pp. 24–31, 2020.

[6] S. Zehtabian, M. Razghandi, L. Bölöni, and D. Turgut, "Predictive caching for ar/vr experiences in a household scenario," in *2020 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 2020, pp. 591–595.

[7] S. Sukhmani, M. Sadeghi, M. Erol-Kantarci, and A. El Saddik, "Edge caching and computing in 5g for mobile ar/vr and tactile internet," *IEEE MultiMedia*, vol. 26, no. 1, pp. 21–30, 2018.

[8] M. Xu, C. Li, S. Zhang, and P. Le Callet, "State-of-the-art in 360 video/image processing: Perception, assessment and compression," *IEEE Journal of Selected Topics in Signal Processing*, vol. 14, no. 1, pp. 5–26, 2020.

미래 네트워크 운영관리를 위한 디지털 트윈 기술 연구

김우태
KT

utae.kim@kt.com

A Study on the Digital Twin Technology For Future Network Operations and Managements

Kim Woo Tae
utae.kim@kt.com

요 약

본 논문은 5G, 디지털전환 등 빠르게 변화하는 초연결 사회의 핵심 인프라로서 점점 중요해지며, 순간의 장애에도 개인 뿐만 아니라, 사회, 국가 전반에 영향을 주는 네트워크 인프라에 대해, 디지털 트윈 기술을 기반으로 기존의 장애 대응·복구 중심 운영관리체계에서 장애예방체계 기술에 대해 연구하였다.

Ⅰ. 서 론

전 지구적으로 모바일, 인터넷 및 사물통신 기기, 서비스 이용의 폭발적 증가로 초연결 네트워크 시대로 진화가 가속화되며, 코로나 19 로 인해 일상생활의 비대면 온라인 전환으로 네트워크에 대한 의존성이 점점 심화되고 있다.

최근 10 년동안 19 건의 통신망 장애사고가 발생하였으며, 이로 인해 건당 수백억원 이상의 피해가 발생하였으며[1], 과기정통부에서는 2021 년 KT 네트워크 사고에 대한 후속대책으로 '네트워크 안정성 확보방안'을 발표하였다. [2]

향 후, 5G 확대, AI 확산과 더불어 XR, 메타버스, 자율자동차 등 초실감·융합 서비스 시대가 도래하면 고품질의 데이터를 안정적으로 전달할 수 있는 네트워크의 중요도는 더 커질 것으로 전망되며, 네트워크 인프라는 공기와 같이 생활의 필수요소가 되어 순간의 장애는 개인 뿐만 아니라, 사회, 국가 전반에 영향을 미치게 된다.

특히, 기존의 이벤트 기반 장애대응과 복구 중심 네트워크 운영관리 체계는 급변하는 시대의 네트워크 관리 요구사항을 충분히 만족하지 못하며, 장애예방 중심의 관리체계에 대한 요구가 점점 증가할 것으로 예상된다.

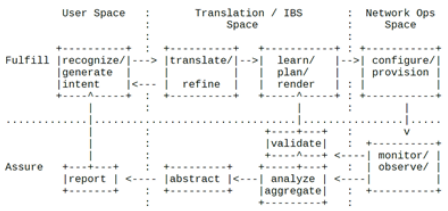
Ⅱ. 본론

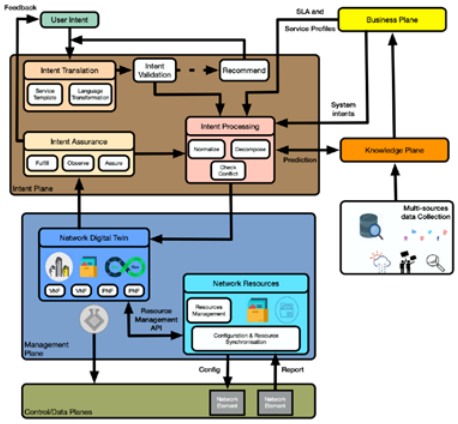
본논문에서는 기존의 장애대응, 복구 중심의 운영관리 체계에서 디지털 트윈기술과 AI, SDN 기술을 연계하여 장애예방 체계 기술에 대해 연구하였다

1. 국내외 기술동향

국내외 통신사업자들은 통신인프라의 운영 효율성 및 지능형 운영관제를 위해, AI 와 SDN 기술을 적용하여 PoC 또는 시범운영 단계에 있다. 하지만, 국내외 텔코 및 벤더 솔루션사 접근방식으로 장애 대응은 가능하지만, 장애 예방을 하기에는 한계가 있는 실정이다.

이러한 한계를 극복하기 위해, IRTF, ITU-T 중심 미래 네트워크 기술, 구조 표준화를 위한 자동화, 지능화 기반 IBN(Intent-Based Networking), Autonomous Network 기술, 구조 연구를 진행하고 있다.

단체	활동
IRTF nmrg[3]	- 네트워크 관리 국제표준화 및 연구활동 - IBN Draft(21.12, Informational) Operational data+ analyticsaction (context-aware+ intended outcome) - SNMP-based → YANG-based management ⇒ 네트워크 인프라 운영데이터와 사용자 의도가 AI, SDN 기술과 연계한 End-to-End 자율운영 네트워크 
ITU-T FG NET2030 [4]	- 2030 미래서비스(HTC, Time-sensitive, multi-sense 등)를 대비한 네트워크 기술, 구조에 대한 표준화 및 연구활동 - Network 2030 시대, 자동화/지능화

	수준의 향상 → Intent 기반, Predictive, Protective automatic management 

그리고, Industry 4.0 관련 스마트시티, 공장 등 산업 영역에서는 디지털 트윈 기술이 활발하게 적용되고 있으나, 네트워크 분야는 아직 초기 단계이며 각 표준 단체에서도 기술, 요구사항을 정의하는 시작단계이다.

2. 연구방향 및 구조

(1) 연구방향

초연결 디지털 대전환을 위해 안전한 네트워크 제공을 위해서는 신속한 장애 복구도 중요하지만, 장애를 미리 예방할 수 있는 기술확보가 선결되어야 한다.

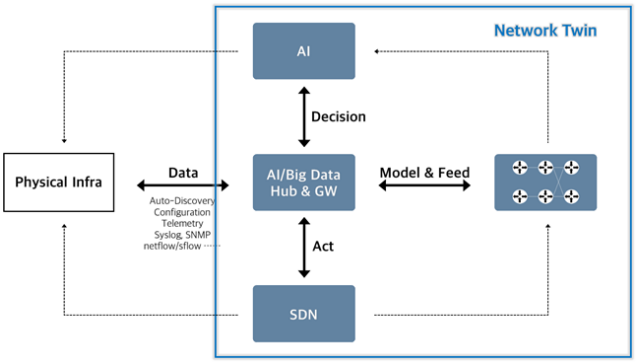


그리고, 이러한 장애예방 기술을 위해 네트워크 분야에도 디지털 트윈 기술 적용이 필요하다. 참고로, 디지털트윈은 현실과 동일한 사물을 가상의 공간에 쌍둥이처럼 똑같이 만들고 현실에서 발생할 수 있는 상황을 가상의 공간에서 시뮬레이션하여 결과를 미리 예측해 보자는 기술이다. 이런 디지털 트윈 기술을 네트워크 분야에 적용하여 다음과 같은 장애예방 체계를 확보할 수 있다.



(2) 디지털 트윈 네트워크 구조

타 산업분야도 마찬가지겠지만, 네트워크 분야에서의 디지털 트윈은 물리적인 네트워크 인프라를 똑같이 복제한 가상의 트윈과 AI 및 SDN 기술이 결합되어야 진정한 네트워크 예방체계를 가질 수 있으며, 전체적인 구조와 요소 기술은 아래와 같다.



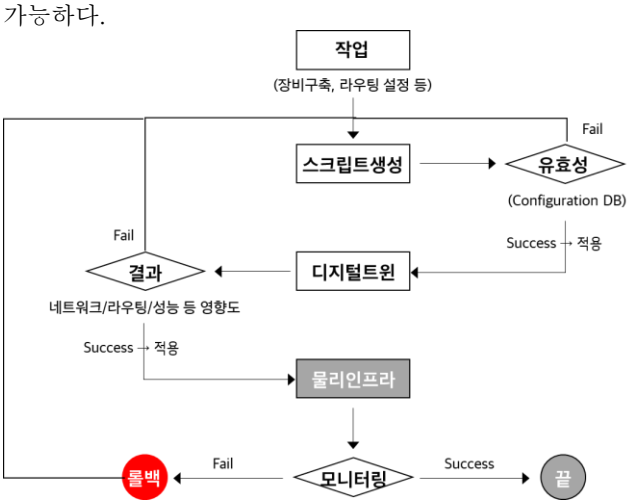
(데이터)모든 산업분야와 마찬가지로, 디지털 트윈 네트워크에서도 물리 인프라에서 발생되는 모든 운영데이터의 실시간 수집 및 시각화, 에뮬레이션 기술이 중요

(모델링)네트워크에서 수집된 물리인프라의 데이터를 디지털 공간으로 동기화하여 네트워크 시각화 및 모의실험을 수행하는 기술

(AI 엔진)네트워크 트윈을 기반으로 물리 네트워크 인프라의 상황을 모니터링하고 트윈을 통해 수행된 노의 결과를 AI/ML 기술을 통해 문제를 예측하고 최적화 작업을 수행하는 기술

(SDN)네트워크 작업에 대한 네트워크 디지털 트윈 대상 사전 적용, 검증 자동화 및 AI가 분석, 진단한 의사결정에 대해 물리 인프라에 자동으로 적용할 수 있는 기술

상기 언급한 디지털 트윈구조와 기술을 네트워크 작업과정에 적용하면 다음 프로세스를 통해 완벽한 네트워크 예방체계를 확보할 수 있게 되며, 유사한 프로세스를 적용하여 네트워크 운영과정에도 적용이 가능하다.



Ⅲ. 결론

본논문에서는 기존의 장애대응, 복구 중심의 운영관리 체계에서 디지털 트윈기술과 AI, SDN 기술을 연계하여 장애예방 체계 기술, 구조 및 프로세스에 대해 제안하였다.

본 제안구조를 통해 디지털 대전환을 뒷받침하는 핵심 인프라로서 안전한 통신망의 구축과 장애예방 실현으로, 네트워크 장애에 의한 경제적, 사회적 손실과 국가적 재난을 예방하며, 향 후 6G, 위성 등 차세대 네트워크의 안정성 보장은 기본으로 미래 자율 네트워크 체계 발전에도 기여할 것으로 기대한다.

참 고 문 헌

[1] 동아일보, “최근 10년 통신장애 사고 19건”(2021)

[2] 과기정통부, “네트워크안정성 확보방안”(2021)

[3] IRTF nmrg, “draft-irtf-nmrg-ibn-intent-classification-06” (2022)

[4] ITU-T FG NET2030, "TR Network2030 - Architecture Framework"(2020)

스마트 실내 서비스를 위한 모바일 로봇 플랫폼 설계

박지태, 이민성, 최정우, 신창의, 김명섭
고려대학교
{pjj5846, min0764, choigoya97, realmine, tmskim}@korea.ac.kr

A Design of Mobile Robot Platform for Smart Indoor Service

Jee-Tae Park, Min-Seong Lee, Jeong-Woo Choi, Chang-Yui Shin, Myung-Sup Kim
Korea Univ.

요 약

최근 과학 기술의 발전으로 다양한 방면에서 로봇에 대한 연구가 활발하게 진행되고 있으며, 머신러닝 및 딥러닝 기술의 발전으로 실내 방역, 안내 등의 여러 가지 서비스를 제공하는 실내 이동 로봇의 수요가 증가하고 있다. 특히 코로나 19 펜데믹으로 인하여, 방역 서비스를 제공하는 로봇에 대한 수요가 급증하였으며, 재택근무로 인하여 실내 생활이 늘어나면서 다른 실내 서비스를 제공하는 로봇에 대한 수요도 증가하고 있다. 하지만 대부분의 실내 서비스는 인력으로 제공되고 있으며, 사용되고 있는 실내 로봇도 개별적으로 동작하여 단순한 기능만을 제공하기 때문에 관리 비용도 많이 든다. 따라서 본 논문에서는 실내 서비스를 제공하는 로봇을 효율적으로 관리하고 제어 할 수 있는 모바일 로봇 플랫폼을 제안한다. 제안하는 모바일 로봇 플랫폼은 인공지능 기반으로 동작하며, 이를 통해 각각의 상황에 대하여 능동적인 대처를 할 수 있다.

Ⅰ. 서 론

최근 과학 기술의 발전으로 다양한 방면에서 로봇에 대한 연구가 활발하게 진행되고 있다. 특히 머신러닝, 딥러닝 기술의 발전으로 방역 로봇, 서비스 로봇과 같이 다양한 분야에서 로봇 기술이 활용되고 있다. 이러한 추세에 따라 실내에서 로봇 스스로 주변 환경을 감지하고, 위치 정보를 얻어 자율 주행이 가능한 이동 로봇의 수요가 증가하고 있다.

로봇 기술의 발전과 수요 증가는 로봇이 인간의 생활 속에 밀접하게 자리 잡도록 하였으며, 코로나 19 펜데믹은 이러한 현상을 더욱 가속화 시켰다. 특히, 비대면 회의, 재택근무 등으로 인하여 실내 생활 비중이 크게 증가 하면서 방역을 포함한 여러 가지 서비스를 제공하는 로봇에 대한 수요도 증가하고 있다. 하지만 실내 서비스는 대부분의 경우 사람이 직접 수행하기 때문에 비효율적이며 많은 시간과 비용이 든다. 이동 로봇을 이용하여 실내 서비스를 제공 할 경우, 정확하고 효율적으로 일을 처리 할 수 있으며, 많은 시간을 단축시킬 수 있다[1-3]. 하지만 실내 서비스를 제공하는 로봇의 경우에도 각각의 로봇이 개별적으로 단순한 업무만을 수행하기 때문에 각각의 로봇들을 체계적으로 관리하기 어렵고, 필요한 서비스에 따라서 다양한 로봇을 배치 할 경우 비용이 많이 든다.

대부분의 관련 연구들은 개별 로봇의 자율 주행, 위치 측정 주변 환경 인식 등의 연구만 수행되어 왔다[1-3]. 이러한 연구들로 인해서 개별 로봇의 성능은 크게 향상시켰으며, 사용자 입장에서 편리한 기능들이 생겼다[4]. 하지만 하나의 개별 로봇이 제공 할 수 있는 기능만으로는 한계가 있으며, 특히 대규모의 실내 환경에서는 효율성이 떨어지는 문제점이 있다. 이를 해결하기 위해서 체계적인 관리 및 제어를 통해 필요한 곳에 로봇을 배치하고, 제어가 필요한 로봇은 신속하고 정확하게 제어 할 수 있는 시스템이 필요하다.

따라서 본 논문에서는 개별적으로 수행하는 로봇을 관리, 제어 할 수 있는 모바일 로봇 플랫폼 설계 방안을 제안한다. 제안하는 모바일 로봇 플랫폼은 기본적으로 인공지능 기반으로 동작하며, 이를 통해 발생 하는 여러 가지 상황에 대하여 능동적으로 대처 할 수 있다. 또한, 각각의 로봇들을 체계적으로 관리하고 제어 할 수 있기 때문에, 효율적으로 일을 처리 할 수 있으며, 불필요한 지출을 줄일 수 있다.

본 논문의 구성은 본 장의 서론에 이어 2장 본론에서 설계한 전체 시스템 구조와 구성되어 있는 각 모듈의 기능 및 행동 시퀀스 알고리즘에 대해 설명하며, 3장에서 결론 및 향후 연구를 제시한다.

Ⅱ. 본론

본 논문에서는 스마트 실내 서비스 제공을 위한 모바일 로봇 플랫폼 설계를 제안한다. 전체 시스템은 로봇, Control Center, 관제 시스템의 세 가지 모듈로 구성되어 있으며, 구조는 그림 1에 나타나있다.

먼저 모든 개별 로봇들은 센서 및 카메라를 통해 정보를 받고, 입력 된 정보를 통해 상황을 판단하고 행동한다. 이 때, 로봇은 인공지능 기반으로 구현되어 있으며, 기본적인 자율 주행과 주변 환경 인식, 상황 판단은 가능 한 것으로 가정하고 상황 판단은 이전에 학습 된 상황을 기준으로 로봇 스스로 판단하고 행동을 수행한다. 인공지능 기반으로 구현 된 행동 시퀀스는 로봇이 특정 상황에 대하여 행동을 수행하는 과정을 나타내며, 그림 2에 나타나있다. 로봇은 지속적으로 주변 환경에 대하여 모니터링을 수행하다가 로봇 내 센서, 카메라를 통해 측정된 정보를 입력으로 받아 드린다. 그 후, 입력으로 들어온 여러 가지 정보를 분석하여 특정 상황 및 환경에 대해 인지하고, 해당 상황에서 어떤 행동을 수행 할지 스스로 결정하여 행동한다. 예를 들어 실내 안내 서비스를 제공하는 로봇의 경우, 실내 출입자가 안내 요청을 하면 센서를 통해 인지된 음성을 분석하여 상황을 인지하고, 인지된 상황에 따라서 로봇은 요청에 대한 대답을 결정하고 제공

본 논문은 2020년도 산업통상자원부 및 한국산업기술평가관리원(KEIT) 연구비 지원에 의한 연구 (No. 20008902, IT비용 최소화를 위한 5채널 탐지기술 기반 SaaS SW Management Platform(SMP) 개발) 이며, 2021년도 교육부의 재원으로 한국연구재단의 지원을 받아 수행된 지자체-대학협력기반 지역혁신 사업의 결과임(2021RIS-004).

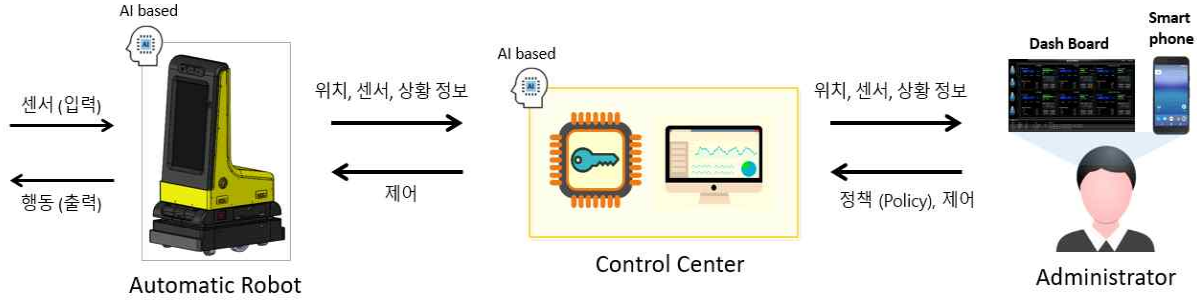


그림 1 모바일 로봇 플랫폼 전체 시스템 구성도

하게 된다.

두 번째 모듈은 Control Center로, 개별 로봇을 제어하고 관리하는 역할을 한다. 로봇이 센서로부터 정보를 입력 받고, 분석 후 해당 상황에 대하여 학습을 기반으로 판단을 할 때, 학습 되지 않은 상황으로 판단 될 경우, Control Center에서 입력 된 정보와 분석 결과를 전달받는다. 이 때, Control Center도 로봇과 마찬가지로 인공지능을 기반으로 동작하며, 개별 로봇의 학습 환경보다 더 큰 환경에 대하여 학습한다. 이를 통해 로봇이 학습 되지 않은 상황일 경우에도 Control Center에서 학습 되어 있는 상황 일 경우, 학습대로 판단하고 행동을 수행한다.

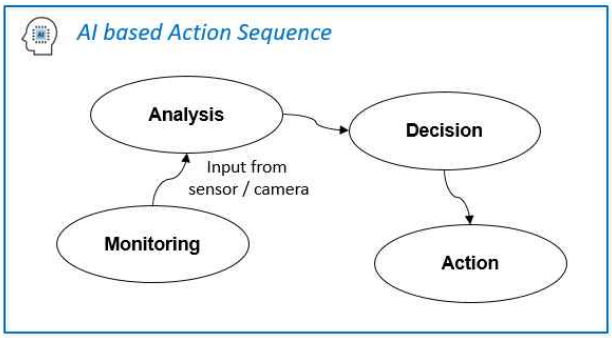


그림 2 인공지능 기반 행동 시퀀스 구조

세 번째 모듈은 관제 시스템으로, 전체 로봇과 Control Center를 제어 및 관리하는 역할을 한다. 관제 시스템은 관리자가 직접 개입하며, 로봇과 Control Center가 학습되지 않은 상황으로 판단 될 경우, 관제 시스템에서 해당 로봇과 Control Center를 직접 제어 한다. 이 후, 로봇과 Control Center는 해당 상황에 대하여 학습을 수행한다. 전체 모듈과 상황에 대해서는 실시간으로 모니터링 되며, 관리자는 대시보드 혹은 스마트 폰을 통해 쉽게 확인 할 수 있다. 또한, 관제 시스템에서는 화재, 무단 침입 등의 긴급 상황이 발생 했을 경우에도 알림, 경고 및 경비 시스템 동작 등의 대처를 할 수 있다.

각 모듈에서 데이터 분석 이후의 행동 시퀀스 알고리즘은 그림 3에 나타나있다. 로봇과 Control Center는 인공지능 기반으로 동작하며, 각 모듈에서 학습 정도에 따라 수행 할 수 있는 기능이 다르다. 관제 시스템에서는 로봇, Control Center를 관리하며, Control Center는 로봇을 관리하며, 로봇은 각각의 기능에 따라 실내 서비스를 제공한다.

Ⅲ. 결론 및 향후 연구

본 논문에서는 기존의 비효율적이고, 많은 시간과 비용이 드는 실내 서비스 제공에서의 문제점을 분석하고, 체계적이고 효율적으로 관리 할 수

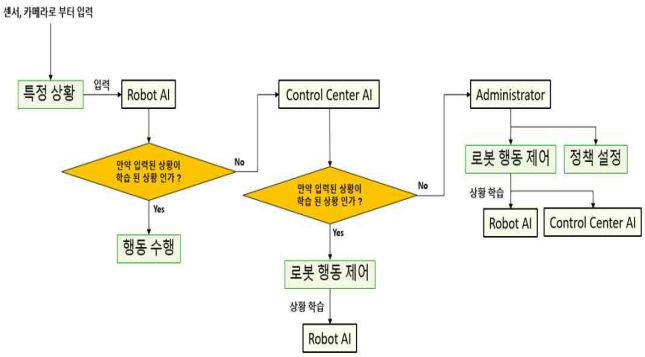


그림 3 행동 시퀀스 알고리즘

있는 모바일 로봇 플랫폼을 제안한다. 제안하는 모바일 로봇 플랫폼은 로봇, Control Center, 관제 시스템으로 구성되어 있으며, 또한, 본 논문에서는 인공지능 기반으로 동작하는 행동 시퀀스를 제시하여 여러 가지 상황에 대해 능동적으로 대처 할 수 있는 방안을 제안한다.

향후 연구로는 방역, 안내, 방범과 같은 실내 서비스를 대상으로 상황별 시나리오를 작성하고, 이에 대한 구체적인 행동 시퀀스를 정의 할 예정이다. 그리고 간단한 기능의 로봇을 활용하여 실제 실험 환경을 구축하고, 실험을 진행 할 예정이다.

참 고 문 헌

[1] 김연태, 김성신. "확장 칼만 필터를 이용한 로봇의 실내 위치 측정." 한국지능시스템 학회 논문지 18.5 pp. 706-711, 2008.

[2] 김현종, 강근택, 이원창. "무선 센서 네트워크와 퍼지모델을 이용한 이동로봇의 실내 위치인식과 주행." 한국지능시스템학회 논문지 18.2 pp. 163-168, 2008

[3] 박성준, 이상민, 김황남. "강화 학습을 통한 센싱 기반 로봇 제어 기술 연구." 한국차세대컴퓨팅학회 학술대회 pp. 101-104, 2021

[4] Chakraborti, T., Kambhampati, S., Scheutz, M., & Zhang, Y, "Ai challenges in human-robot cognitive teaming." arXiv preprint arXiv:1707.04775 2017.

TS3:
네트워크 보안 1

악성코드 분류를 위한 trigram 기반의 BiLSTM 모델 연구

김종욱[1], 최미정[1,2,*]

강원대학교 컴퓨터과학과[1], 강원대학교 빅데이터메디컬융합학과[2]

{jw.kim, *mjchoi}@kangwon.ac.kr

A Trigram Based BiLSTM Model for Classifying Malware

Jong-Wouk Kim, Mi-Jung Choi*

Dept. of Computer Science, Kangwon National Univ.[1]

IGP. in Medical Bigdata Convergence, Kangwon National Univ.[2]

요 약

매일 수 십만 개씩 새롭게 생성되는 악성 파일과 제로데이 공격 및 소프트웨어의 취약점을 악용하여 자산에 많은 손해를 입힌다. 이러한 악성 파일과 공격들을 탐지하기 위해 시그니처를 사용하는 정적 분석과 실행 파일을 직접 실행하는 동적 분석을 사용하고 있지만 많은 수의 새로운 악성 파일에 일일이 대처하기는 어렵다. 이 문제를 극복하기 위해 기계학습 및 딥러닝과 같은 다양한 기술들을 적용하는 연구가 진행되고 있다. 특히, AI 모델을 통한 학습과 의미있는 자질(feature)을 선택하여 악성 파일을 탐지하고 분류하는 AI 모델이 연구되고 있지만, 아직 추가적인 연구가 필요한 상황이다. 본 논문에서는 의미 있는 정적인 자질과 딥러닝 모델을 연구하기 위해 다양한 AI 모델들을 실험한다. 악성 파일을 탐지 및 분류할 수 있는 시스템 구조를 위해 n-gram으로 변환된 opcode 시퀀스 데이터를 학습하는 BiLSTM 모델을 제안한다. 제안하는 모델을 검증하기 위해 대용량의 데이터가 필요하므로 약 23 만개의 악성 및 양성 파일을 수집했으며, 데이터 레이블링을 위해 VirusTotal Academic API를 사용했다. 수집한 데이터로부터 opcode를 추출하고, n-gram으로 변환하여, 최종적으로 BiLSTM 모델이 악성 여부를 판단 및 분류한다. 악성 파일 탐지 실험에서 BiLSTM 모델은 90.9%의 정확도와 89.7%의 F1-Score를 달성했으며, 악성 파일 분류 실험에서 80.4%의 정확도와 80.1%의 F1-Score를 달성했다.

I. 서 론

악성 파일은 컴퓨터, 전자기기, 그리고 네트워크와 같은 조직의 자산에 해를 끼치도록 명시된 컴퓨터 소프트웨어이다. 초기 악성 파일은 원시적이었으며 종종 플로피 디스크를 통해 오프라인으로 확산했으며, 네트워킹과 인터넷이 발전함에 따라 악성 파일은 온라인으로 배포되기 시작했다. 과거 Creeper, Wabbit, 그리고 Elk Cloner와 같은 초기 악성 파일은 명성이나 영광을 위해 제작됐지만, 현재 대부분의 악성 파일은 경제적인 동기나 악의적인 동기를 갖는다 [1]. 1988년에 등장한 Morris Worm은 ARPANET에 연결된 컴퓨터의 상당 부분을 감염시켜 24시간 이내에 네트워크를 무력화시킨 악성 파일로서 개발자인 Robert Morris는 악성 파일 개발 혐의로 법정에서 최초로 유죄 판결을 받았다.

2020년의 팬데믹 상황이 해커들에게 일반인과 기업을 표적으로 삼을 새로운 기회를 제공함에 따라 사이버 범죄로 인한 전 세계 손실 추정치는 1조 달러에 달할 것으로 예견했으며, 전략 및 국제 연구 센터(Center for Strategic and International Studies)와 McAfee는 2020년의 손실이 약 9,450억 달러에 달할 것으로 예상했다 [2]. 이 보고서는 외국 범죄 기업의 랜섬웨어 공격이 미국 산업에 미치는 위협 및 위험이 증가하고 있음을 강조했으며, 의원들은 재정적 부문과 보건의료 부문에 막대한 손실을 끼치고 있다는 사실에 우려를 표명했다. 세계적인 팬데믹 상황에 맞추어 조직과 기업들은 반드시 사용자와 고객의 재정적 손실을 막고, 브랜드 평판의 저하를 차단함과 동시에 정보 구멍, 모니터링 오류 및 자원 오용에 대한 관리의 제어 부재를 방지하는 것이 중요하다.

악성 파일 개발자는 패킹이나 난독화 기술[3]을 사용하여 백신 프로그램을 우회하고 실행 시 실제 동작을 은닉하여 분석의 난이도를 높인다 [4], [5]. 상업용 악성 파일 방지 솔루션은 악성 파일 탐지를 위해 시그니처 데이터베이스를 사용하지만, 새로운 악성 파일을 탐지할 수 없다는 단점이 있다. 전문가들은 이러한 문제를 해결하기 위해 다양한 접근법을 채택하여 계속해서 진화하는 악성 파일을 탐지 및 분류하고자 한다. 특히, 동적 분석이나 디버거를 사용한 연구가 활발히 진행되고 있고 이는 난독화 기법에 강하다는 장점이 있다. 하지만, 일반적으로 가상 머신, 시뮬레이터, 샌드박스 등과 같이 안전하고 완벽히 통제된 환경과 상호 작용 정보를 사용하여 행위 분석을 수행해야 하므로 대규모 데이터셋에 적용할 때 효율성이 많이 떨어진다는 단점이 존재한다 [6].

최근에는 데이터마이닝 등과 같이 여러 기술과 결합한 악성 파일 탐지 방법이 연구되고 있으며, Schultz et. al.은 PE(portable executable) 헤더, 문자열 시퀀스, 바이트 시퀀스를 사용한 데이터 마이닝 기술을 통해 악성 파일을 탐지하는 방법을 제안했다 [7]. 이후, 기계학습, 딥러닝과 같이 인공 신경망을 사용한 악성 파일 탐지 및 분류 방안이 연구되기 시작했다 [8], [9]. 그러나, 많은 논문에서 Microsoft 社가 제공하는 'Microsoft Malware Classification Challenge (BIG 2015)'데이터셋을 사용했다 [10]. 이 데이터셋은 표 1처럼 9개의 서로 다른 family 유형으로 구성되며, 7개의 위협(threat types)이 있지만, 총 10,868개의 샘플들로, 이는 딥러닝 및 기계학습에 적용하여 성능을 평가하기에는 너무 적은 수이다.

따라서, 본 논문에서는 악성 파일의 위협 타입(threat types)을 탐지 및 분류하고자 한다. 총 235,960개의 악성 파일을 수집하여 분석하였다. 대용

표 1. BIG 2015 데이터셋

Family name	# of samples
Ramnit	1,541 (14.2%)
Lollipop	2,478 (22.8%)
Kelihos_ver3	2,942 (27.1%)
Vundo	475 (4.40%)
Simda	42 (0.40%)
Tracur	751 (6.90%)
Kelihos_ver1	398 (3.70%)
Obfuscator.ACY	1,228 (11.3%)
Gatak	1,013 (9.30%)

량의 데이터셋을 수집하기 위해 VirusShare[1]와 VirusTotal[2]에서 제공하는 악성 파일 및 API를 사용하여 데이터셋을 분석하고 레이블링(labeling)한 후 시퀀스(sequences) 기반의 자질과 딥러닝 모델을 가벼운 기계학습 모델부터 CNN, LSTM, BiLSTM 등을 적용하여 총 15개의 위협 타입과 정상 파일(benign files)을 분류했다. 본 논문에서는 각 악성 파일 샘플의 opcode 시퀀스를 추출하고, 특징을 더욱 잘 표현하기 위해 n-gram으로 변환된 opcode 시퀀스를 사용했으며, 위협 타입 별 상관 관계를 분석했다. 그 결과 악성 파일에 대해 90.9% 탐지율과 89.7%의 F1-Score를 달성했으며, 정상 파일을 포함한 16개의 분류 성능은 최대 80.4% 정확도와 80.1%의 F1-Score를 달성했다.

본 논문의 구성은 다음과 같다. 2장에서는 악성 파일을 탐지 및 분류하기 위한 데이터, 전처리 방법, 다양한 기계학습 모델, 그리고 프레임워크를 소개하고, 3장에서는 악성 파일을 탐지 및 분류 실험 결과를 제시하며, 4장에서는 악성 파일을 탐지 및 분류하는 관련 연구를 간략히 소개하며, 마지막 5장에서는 전체 논문을 요약하고 향후 연구를 제시한다.

II. AI 기반 악성 파일 탐지 및 분류 프레임워크

1) 데이터셋 및 전처리 모듈

효과적인 AI 모델을 위해 대용량의 데이터를 VirusShare와 VirusTotal을 통해 악성코드 샘플들을 수집했다. VirusShare의 경우 홈페이지에서 제공하는 토렌트 파일을 사용하여 수집했고, VirusTotal의 경우 Academic Request를 통해 구글 드라이브를 통해 최근 3년간의 악성 파일들을 사용했으며, 데이터 구성은 표 2와 같다. 레이블링(labeling)을 위해 VirusTotal에서 제공하는 Academic API를 제공받아 사용했다. 본 데이터셋은 15개의 위협 타입과 1개의 양성 파일로 구성되며 'Trojan' 위협이 가장 많은 비율을 차지한다.

전처리 모듈에서 각 샘플의 자질을 추출하기 위해 objdump를 사용하여 PE(Portable Executable) 파일의 명령어를 추출하여 다음과 같이 trigram 시퀀스로 변환한다:

{(push, mov, mov), (mov, mov, xor), (mov, xor, mov), (xor, mov, mov), …}

n-gram은 특정 시퀀스의 발생을 예측할 수 있어 서로 다른 위협을 구분할 수 있다는 장점이 있다 [11]. 이것은 단어의 수에 기반한 통계적 접근 방법이며, 모든 단어를 고려하는 것이 아니라 n개의 연속적인 단어들만 고려한다. 이것을 사용할 때 n에 따라 unigram, bigram, trigram, 4-gram 등으로 명명된다. n-gram 기반의 모델에서는 대용량 말뭉치(corpus)에서

1) https://virusshare.com/
2) https://developers.virustotal.com/v3.0/reference

표 2. 수집한 악성코드 데이터셋

Threat type	# of samples
Trojan	90,449 (38.3%)
Backdoor	3,541 (1.50%)
Malware	23,816 (10.1%)
Benign	83,831 (35.5%)
PUP	13,388 (5.70%)
Worm	2,367 (1.00%)
Suspicious	2,831 (1.20%)
Adware	1,589 (0.70%)
Unwanted	2,089 (0.90%)
Virus	312 (0.10%)
Spyware	873 (0.40%)
HEUR	578 (0.20%)
Downloader	439 (0.20%)
Dropper	2,284 (1.00%)
Hacktool	1,261 (0.50%)
Win32	6,312 (2.70%)

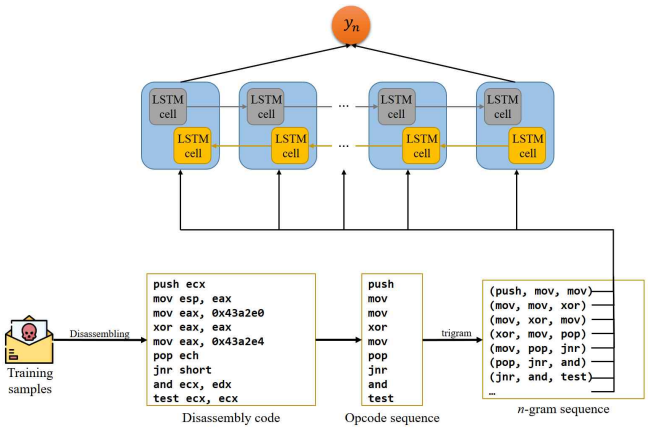


그림 1. Overall architecture of malware detection and classification

효율적인 모델을 구축할 수 있으며, 제한적인 어셈블리 코드에서 매우 효과적으로 탐지 및 분류할 수 있도록 도와준다.

2) 악성 파일 탐지 및 분류 모듈

양방향 LSTM(BiLSTM)은 두 개의 독립적인 LSTM 아키텍처를 함께 사용하는 구조이다. 즉, 기존의 LSTM 계층에 역방향으로 처리하는 LSTM 계층을 추가한 것이며, 최종 은닉 상태는 그림 1처럼 두 LSTM 계층의 은닉 상태를 연결한 벡터를 출력한다. RNN이나 LSTM은 입력 순서를 시간에 따라 입력 및 학습하기 때문에 출력물이 바로 이전의 패턴을 기반으로 결정할 수 있으므로, 이러한 문제를 해결하기 위해 양방향 모델이 등장했다 [12], [13], [14].

BiLSTM은 출력값에 대한 손실을 최소화하는 과정에서 모든 파라미터를 동시에 학습하여 종단간(end-to-end) 학습이 가능하여 출력값에 대한 손실을 최소화하는 과정에서 모든 파라미터를 동시에 학습할 수 있다. 또한, 분산표상(distributed representation)을 사용하기 때문에 입력 데이터 간 유사성을 입력 벡터에 더욱 잘 내재화할 수 있다. 물론, 네트워크를 구성하는 셀이 LSTM이므로 입력 데이터의 길이가 길어져도 성능 저하를 방지할 수 있다.

3) 악성 파일 탐지 및 분류 모듈

표 4. 악성코드 분류 실험 결과

Model	Accuracy	F1-Score
Logistic Regression	64.3%	63.6%
kNN	68.7%	68.1%
Naïve Bayes	27.5%	31.8%
SVM	35.8%	34.9%
Linear SVM	27.0%	24.2%
Decision Tree	75.4%	75.3%
Random Forest	76.8%	76.4%
XGBoost	80.4%	80.0%
DNN	74.6%	74.4%
1DCNN	77.8%	76.8%
LSTM	79.8%	79.2%
BiLSTM	79.9%	79.2%
LSTM (trigram)	80.2%	79.8%
BiLSTM (trigram)	**80.4%**	**80.1%**

표 3. 악성코드 탐지 실험 결과

Model	Accuracy	F1-Score
Logistic Regression	64.9%	63.9%
kNN	79.8%	77.9%
Naïve Bayes	28.9%	25.4%
SVM	39.4%	33.1%
Linear SVM	24.9%	24.3%
Decision Tree	79.5%	77.9%
Random Forest	83.9%	82.1%
XGBoost	85.4%	84.8%
DNN	81.1%	80.6%
1DCNN	82.4%	82.0%
LSTM	84.8%	84.4%
BiLSTM	85.2%	84.7%
LSTM (trigram)	89.9%	89.3%
BiLSTM (trigram)	**90.9%**	**89.7%**

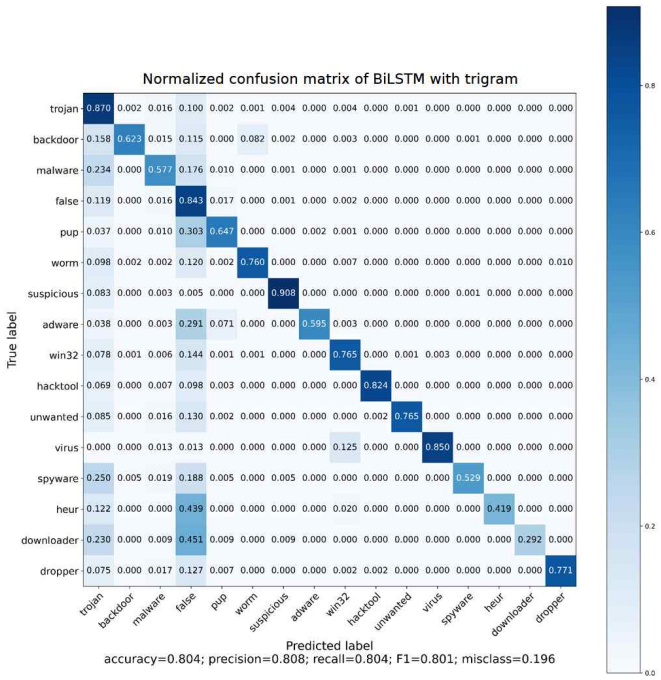


그림 2. BiLSTM-trigram 모델의 혼동 행렬

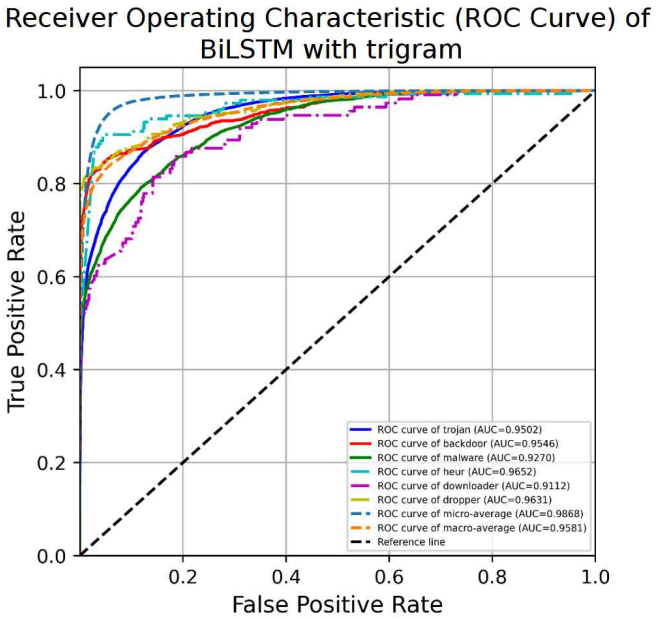


그림 3. BiLSTM-trigram 모델의 ROC 곡선 (receiver operating characteristic)

바이너리 실행 파일은 기계학습에 적합하지 않기 때문에 IDA Pro, objdump, pefile과 같은 디스어셈블러를 사용하여 opcode를 추출한다. 우리가 사용할 부분인 연산자 부분만 사용했다. 단일 opcode는 의미가 없지만 특정 순서의 opcode는 유해한 행위를 나타낼 수 있고, 딥러닝 모델은 사람이 찾아내지 못한 패턴을 찾을 수 있기 때문이다 [15].

추출한 opcode 시퀀스를 n-gram으로 취합한다. 이것은 주어진 텍스트, 음성, 또는 입력값을 n개의 연속적인 나열을 의미한다. {push, mov, mov, xor, mov, ...}와 같은 일련의 opcode가 있는 경우, {(push, mov, mov), (mov, mov, xor), (mov, xor, mov), ...}로 변환할 수 있다. n이 커질수록 딥러닝 모델이 학습하는 데이터의 수와 모델의 사이즈가 기하급수적으로 커지기 때문에 trigram 형식으로 변환한다. 딥러닝 모델은 임베딩 레이어(embedding layer)를 통해 각각의 opcode를 벡터로 변환하여 각각의 셀이 데이터를 학습하고, 악성 파일 탐지 및 분류한다.

III. 실험 결과

악성 파일 탐지 실험은 프레임워크의 악성 파일 탐지에 대한 성능을 보여준다. 대체로 BiLSTM 모델의 성능이 가장 좋았으며, 표 3처럼 다양한 모델들과 비교했다. 기계학습 모델들의 경우 트리 기반의 모델(Decision Tree, XGBoost, Random Forest)들이 높은 성능을 보였고, SVM 기반 모델들이 대체로 낮은 성능을 보였다. 딥러닝 모델들의 경우 BiLSTM이 가장 높은 성능을 보였으며 trigram을 사용할 경우 더 높은 성능을 보였고, DNN의 경우 대체로 낮은 성능을 보였다. Trigram으로 변환된 opcode 시퀀스는 악성 여부를 더욱 잘 표현할 수 있다는 것을 확인했다.

분류 실험은 악성 파일의 위협 분류에 대한 성능을 보여준다. 탐지 실험과 마찬가지로 BiLSTM 모델이 가장 우수한 성능을 달성했으며, 표 4처럼 다양한 모델들과 비교했다. 기계학습 모델들의 경우 트리 기반의 모델(Decision Tree, XGBoost, Random Forest)들이 높은 성능을 보였고, SVM 기반 모델들이 대체로 낮은 성능을 보였다. 그 중 XGBoost만 유일하게 LSTM과 유사한 성능을 달성했는데, XGBoost 모델은 여러 개의 트리를 생성하여 트리를 학습시킬 때 데이터에 가중치를 주기 때문에 학습

에 도움이 된 것으로 보인다. 딥러닝 모델들의 경우 BiLSTM이 가장 높은 성능을 보였으며 trigram을 사용할 경우 조금이지만 더 높은 성능을 보였다. BiLSTM은 시계열 또는 시퀀스 데이터의 양방향 장기 종속성을 학습하기 때문에, LSTM 및 타 모델들 보다 더 높은 성능을 보였다.

그림 2 및 그림 3은 가장 좋은 성능을 보인 trigram 기반의 BiLSTM 모델의 혼동 행렬과 수신기 작동 곡선(receiver operating characteristic curve)을 보여준다. 그림 2에서 확인할 수 있듯이, trigram으로 변환된 opcode를 학습한 BiLSTM은 위협 타입을 잘 분류했다. 하지만, 데이터 수가 적은 그룹들의 경우, 양성 파일 또는 'trojan'으로 오분류했다. 또한, 그림 3처럼 일부 그룹에 대하여 AUC(area under the ROC curve)를 확인해 보면 대체로 0.9 이상을 갖는 것을 확인할 수 있다. 이는 데이터의 불균형으로 인해 대체로 데이터 수가 많은 trojan이나 false(benign)로 분류했다.

표 2와 표 3처럼 악성 파일 탐지 및 분류 실험 결과에서 trigram으로 변환된 opcode를 학습하는 것이 성능 향상에 도움이 됐다. 하지만, *n*-gram을 사용함에 따라 *n*을 선택하는 것이 매우 중요하며 상충 관계(trade-off relationship)가 존재하기 때문에 적절한 *n*을 설정해야 한다.

IV. 결론

해가 지날수록 많은 수의 악성 파일이 증가함에 따라 악성 파일을 탐지하고 그들을 분류하는 것은 점점 더 중요해지고 있다. 본 논문에서는 단계적으로 자질을 추출 및 전처리하여 악성 파일의 위협을 탐지하고 분류하는 것을 돕는다. 본 논문에서는 일정한 시퀀스를 가지고 있는 opcode를 추출하고 trigram으로 전처리하여 BiLSTM 모델에 적용했다. 이를 통해 우리는 파일의 악성 여부를 판단할 수 있었고, 다양한 위협 타입으로 분류할 수 있었다. 이를 위해 실제 악성 파일을 VirusShare와 VirusTotal로부터 제공받았고, VirusTotal의 Academic API를 통해 레이블링했다. 레이블링 된 데이터로 지도 학습(supervised learning) 후 실험 결과, 악성 파일 탐지에서는 90.9%의 정확도와 89.7%의 F1-Score를 달성했고, 분류에서는 80.4%의 정확도와 80.1%의 F1-Score를 달성했다. 이는 데이터의 분포가 편향되어 있으므로, 적은 수의 데이터가 있는 Downloader, Adware, 그리고 HEUR과 같은 그룹은 제대로 분류하지 못했다.

본 연구의 한계는 부족한 데이터와 자질이다. 딥러닝 모델이 대부분 양성 파일 또는 Trojan으로 분류를 했는데, 이것은 다른 그룹에 비해 학습 데이터가 편향되어 있기 때문이다. 또한, opcode 뿐만 아니라 동적 분석과 CFG(control flow graph)와 같은 자질들을 고려할 계획이다. 즉, 딥러닝 모델을 더욱 개선하기 위해 더 많은 데이터를 수집하고 악성 파일의 위협을 탐지 및 분류할 수 있는 의미있는 자질과 기계학습 및 딥러닝이 갖는 적대적 기계학습 공격을 방지할 수 있는 방안을 연구할 계획이다.

ACKNOWLEDGMENT

이 논문은 2020년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임.(NRF-2020R1A2C1012117)

참 고 문 헌

[1] G. Ollman, "The evolution of commercial malware development kits and colour-by-numbers custom malware," *Computer Fraud & Security*, Vol. 2008, No. 9, pp. 4 - 7, Sept. 2008.

[2] Z. M. Smith (McAfee), E. Lostri (McAfee), and J. A. Lewis (McAfee), "The hidden costs of cybercrime [Internet]", Available: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf, 2022.03.18.

[3] N. Kuzurin, A. Shokurov, N. Varnovsky et. al., "On the concept of software obfuscation in computer security", *International Conference on Information Security*, Valparaíso, Chile, Vol. 1, No. 19, pp. 281 - 298, Oct. 2007.

[4] Q. Zhang and D. S. Reeves, "MetaAware: identifying metamorphic malware", in *Proc. of the 23rd Annual Computer Security Applications Conference (ACSAC)*, Miami Beach, FL, pp. 411 - 420, Dec. 2007.

[5] M. R. Chouchane and A. Lakhotia, "Using engine signature to detect metamorphic malware", in *Proc. of the 2006 ACM workshop on Recurring malcode*, New York, NY, pp. 73 - 78, Nov. 2006.

[6] P. LI, L. Liu, D. Gao et. al., "On challenges in evaluating malware clustering", in *Proc. of the International Workshop on Recent Advances in Intrusion Detection (RAID 2010)*, Vol. 6307, Ottawa, Canada, pp. 238 - 255, Sept. 2010.

[7] M. G. Schultz, E. Eskin, F. Zadok et. al., "Data mining methods for detection of new malicious executables", in *Proc. of the 2001 IEEE Symposium on Security and Privacy*, Oakland, CA, pp. 38 - 49, May 2000.

[8] G. E. Dahl, J. W. Stokes, L. Deng et. al., "Large-scale malware classification using random projections and neural networks", in *Proc. of the 2013 IEEE International Conference on Acoustics, Speech and Signal Processing*, Vancouver, Canada, pp. 3422 - 3426, May 2013.

[9] J. Saxe and K. Berlin, "Deep neural network based malware detection using two dimensional binary program features", in *Proc. of the 10th International Conference on Malicious and Unwanted Software (MALWARE)*, Fajardo, Puerto Rico, pp. 11 - 20, Oct. 2015.

[10] R. Ronen (Microsoft), M. Radu (CrowdStrike), C. Feuerstein (Microsoft Research) et. al., "Microsoft malware classification challenge[Internet]", *arXiv preprint arXiv:1802.10135*, Available: https://arxiv.org/abs/1802.10135.

[11] S. Banerjee and T. Pedersen, "The design, implementation, and use of the ngram statistics package", in *Proc. of the International Conference on Intelligent Text Processing and Computational Linguistics*, Mexico City, Mexico, pp. 370 - 381, Feb. 2003.

[12] A. Graves, A. Mohamed, and G. Hinton, "Speech recognition with deep recurrent neural networks", in *Proc. of the 2013 IEEE International Conference on Acoustics, Speech and Signal Processing*, Vancouver, Canada, pp. 6645 - 6649, May 2013.

[13] T. Dozat, P. Qi, and C. D. Manning, "Stanford's graph-based neural dependency parser at the CoNLL 2017 shared task", in *Proc. of the CoNLL 2017 shared task: multilingual parsing from raw text to universal dependencies*, Vancouver, Canada, pp. 20 - 30, Aug. 2017.

[14] M. Schuster and K. K. Paliwal, "Bidirectional recurrent neural networks", *IEEE Transactions on Signal Processing*, Vol. 45, No. 11, pp. 2673 - 2681, Nov. 1997.

[15] E. Raff, R. Zak, R. Cox et. al., "An investigation of byte n-gram features for malware classification", *Journal of Computer Virology and Hacking Techniques*, Vol. 14, pp. 1 - 20, Sept. 2016.

Mel-Spectrogram 및 CNN을 활용한 응용 트래픽 분류

최정우, 김보선, 이정원, 김명섭
고려대학교, 닥터소프트
{choigoya97, boseon12}@korea.ac.kr, ljwbom@doctorsoft.co.kr, tmskim@korea.ac.kr

Classification of Application traffic using Mel-Spectrogram and CNN

Choi Jeong Woo, Kim Boseon, Lee Jeong Weon, Kim Myung-Sup
Korea Univ, Doctorsoft

요 약

네트워크 관리의 기본적인 역할은 QoS (Quality of Service)를 제공하는 것이다. 적합한 QoS를 제공하기 위해서는 효과적인 응용 트래픽 분류가 필수적이다. 그러나 응용 프로그램이 다양해지고 암호화 기술의 광범위한 도입과 포트 난독화 등은 효과적인 트래픽 분류를 방해하고 있다. 이에 본 논문에서는 통계 데이터를 입력으로 사용하는 MLP 모델과 Mel-Spectrogram을 입력 이미지로 사용하는 CNN 모델을 앙상블해 응용 트래픽을 분류하는 방법을 제안한다. 제안하는 방법은 통계 데이터만을 고려한 MLP 모델만 사용한 경우와 비교하여 향상된 성능을 보였다.

Ⅰ. 서 론

인터넷 환경의 성장과 함께 다양한 서비스와 응용이 개발됨에 따라 트래픽이 다양해지고 있다. 이런 상황에 따라 효율적으로 네트워크를 관리하고 사용하기 위한 연구들이 진행되고 있다. 네트워크를 효율적으로 관리하는 것은 사용자에게는 고품질의 서비스를 제공하고, 운영자에게는 서비스의 신뢰성 확보로 이어질 수 있다. 네트워크 관리의 기본적인 역할은 QoS (Quality of Service)를 제공하는 것이다[1]. 적합한 QoS를 제공하기 위해 효과적인 응용 트래픽 분류가 필수적이다.

시간이 지남에 따라 트래픽 분류 기술은 많이 발전해왔다. 전통적인 방법으로는 포트 번호를 사용한 방법이나 DPI(Deep Packet Inspection)과 같은 방법들이 사용되었다. 하지만 이러한 방법들은 각각 응용 프로그램이 잘 알려진 포트 번호를 통해 트래픽을 위장하거나 일반적인 포트 번호를 사용하지 않고, 암호화되지 않은 트래픽에만 적용이 가능하다는 단점을 가진다. 따라서 RF(Random Forest)와 같은 머신러닝 모델, CNN(Convolutional Neural Network)와 같은 딥러닝 모델들이 트래픽 분류에 사용되고 있다. 하지만 머신러닝 모델의 경우 플로우 통계 정보를 사용하기 때문에 트래픽의 특성을 표현하는 것에 있어서 손실이 많다는 단점으로 인해 실용적인 응용 분류에는 적합하지 않다.

기존의 CNN 모델은 패킷 원시데이터를 일차원 또는 이차원 이미지 형태로 입력받아 분류를 수행한다. 본 논문에서는 원본 패킷 데이터로부터 헤더 정보와 통계 데이터에서 특징을 추출해 MLP의 입력으로 사용하고, 음성인식 분야에서 주로 사용되는 Mel-Spectrogram을 사용해서 이미지를 생성하여 CNN 모델의 입력으로 사용해 두 모델을 앙상블하는 응용 트래픽 분류에 대한 방법론을 제안한다. 본 논문은 2장에서 연구에 사용된 주요 기술에 대해 설명한다. 3장에서는 수집한 데이터, 데이터 전처리 과정, 분류 모델에 대해 설명하고 4장에서는 실험 결과를 설명한다. 끝으로 5장에서는 결론과 향후 연구에 대해 설명하는 순으로 진행된다.

Ⅱ. 관련 연구

CNN은 시각적인 영상을 분석하는데 사용되는 다층의 피드-포워드적인 인공신경망의 한 종류이다[2]. CNN은 Feature를 추출하는 Layer와 Activation Function을 통해 결과 값을 도출하는 분류 Layer로 나뉜다. Feature 추출은 이미지의 특성을 판단하는 Convolution Layer와 추출된 Feature를 강화하는 Pooling Layer로 구성된다. 분류 Layer는 Feature 추출 Layer에서 추출된 Feature를 입력으로 받아 분류 결과를 도출한다. CNN 모델의 일반적인 구조는 그림 1과 같다.

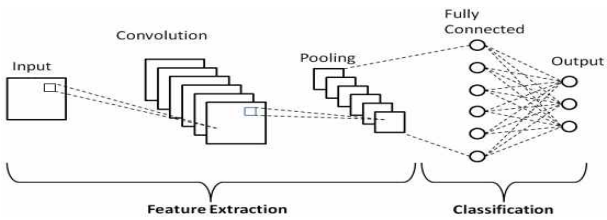


그림 1. CNN 모델 구조

Mel-Spectrogram은 음성 신호를 분석하여 시간에 대한 음성 신호의 주파수 및 강도를 나타낸 특징값이다[3]. 음성 신호를 분석하기 위해 푸리에 변환을 사용하는데, 푸리에 변환을 거친 신호는 주파수(Frequency)와 강도(Amplitude)로 분해되어 각 주파수 별 신호의 강도를 알 수 있게 된다. 시간 정보는 음성에서 매우 중요한 정보 중 하나이기 때문에, 시간 정보를 보존하면서 푸리에 변환이 가능한 단시간 푸리에 변환을 적용한다. 단시간 푸리에 변환은 신호의 처음부터 마지막까지 일정한 크기의 Window를 움직이면서 Window 내부의 신호마다 푸리에 변환을 적용하는 방법이다. 단시간 푸리에 변환의 결과로 시간, 주파수, 강도의 정보를 모두 가진 Mel-Spectrogram을 얻을 수 있다.

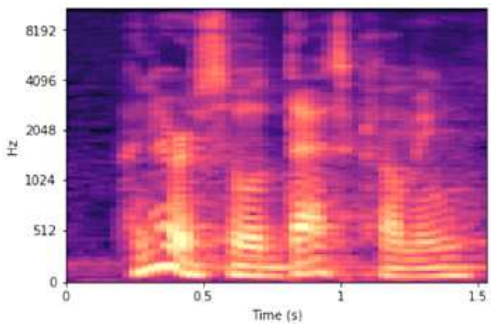


그림 2 Mel-Spectrogram 예시

Ⅲ. 본론

본 장에서는 사용한 데이터셋과 데이터 전처리 과정, 분류모델에 대해 설명한다.

데이터셋은 아래의 표 1의 내용과 같이 총 10개의 응용 트래픽으로 구성되어 있다.

응용명	패킷 개수	플로우 개수
App 1	81735	901
App 2	79360	892
App 3	36481	1013
App 4	74933	936
App 5	97800	964
App 6	102963	1034
App 7	71689	1105
App 8	85215	1020
App 9	94660	881
App 10	102158	802

표 1 응용 별 패킷, 플로우 개수

MLP 모델에 사용할 특징 추출과정은 아래의 그림 3과 같다. 첫 계층에서 IAT와 SIZE로 분할되며 이후 각 특징은 패킷의 방향성에 따라 Packet Direction 단계에서 All, Forward, Backward로 나뉜다. 이후 다음 단계에서는 전체 패킷부터 시작하여 첫 5개 패킷, 첫 10개 패킷 등으로 시작하여 첫 30개까지 분할되어 추출된다. 마지막으로 Statistics 단계에서 총합, 최댓값, 첨도, 왜도 등 13가지 통계 항목으로 추출된다. 최종적으로 플로우 1개당 2(Features) x 3(Direction) x 7(N) x 13 = 546 개의 특징을 추출하여 사용했다.

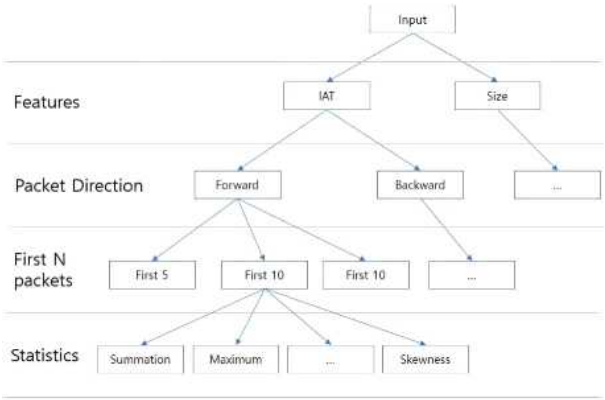


그림 3 계층적 특징 추출과정

CNN 모델의 입력으로 사용할 Mel-Spectrogram 이미지의 예시는 다음 그림 4와 같다.

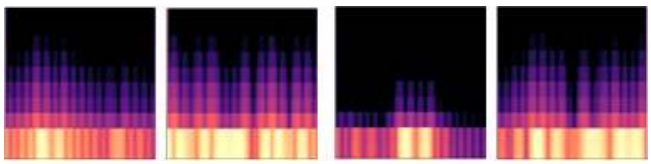


그림 4 Mel-Spectrogram 이미지

그림 4는 두 개의 응용에 대한 Mel-Spectrogram이미지이다. 맨 왼쪽부터 App 3의 처음 20개의 패킷의 패킷 사이즈, 처음 20개의 패킷의 IAT, App 7의 처음 20개의 패킷의 패킷 사이즈, 처음 20개의 패킷의 IAT에 대한 Mel-Spectrogram 이미지이다. 해당 Mel-Spectrogram 이미지의 가로축은 패킷의 개수(1~20), 세로축은 패킷 사이즈 혹은 IAT에 해당한다. 또한 해당 이미지는 패킷 사이즈, IAT와 더불어 첫 패킷부터 20번째 패킷으로 진행되면서 각 특징들의 시간에 따른 변화에 대한 정보도 표현하고 있다.

통계 데이터는 546개의 데이터를 다른 변환없이 사용하며 이때의 Shape는 1x546의 형태를 가진다. MLP 모델은 기본적인 모델을 사용했으며 3개의 Dense(뉴런 개수 64개) Layer를 가진다.



그림 5 통계 데이터 구조 및 MLP 입력 개요

Mel-Spectrogram 이미지가 입력으로 사용되는 CNN모델의 대략적인 구조는 다음 표 2와 같다.

Layer	Parameter
Input	(330, 330, 3)
Conv 2D	(n_filter=64, filter_size=(2, 2))
Pooling Layer 2D	(2, 2)
Conv 2D	(64, (2, 2))
Pooling Layer 2D	(2, 2)
Flatten	-
Dense	(10)

표 2 CNN 모델 하이퍼 파라미터

Ⅳ. 실험결과

아래의 표 3은 수집한 데이터셋에 대한 각 모델별 분류 결과를 나타낸다. 실험은 MLP 모델만 사용해 응용 트래픽을 분류한 경우와 MLP모델과 CNN모델을 Concatenate한 경우의 성능을 비교하는 방식으로 진행했다. 통계 데이터를 입력으로 사용하는 MLP 모델만으로 응용 트래픽을 분류하는 경우에 비해 Mel-Spectrogram을 입력 이미지로 사용하는 CNN 모델을 함께 사용해 응용 트래픽을 분류하는 경우가 좋은 성능을 보이는 것을 알 수 있다.

모델	Accuracy
MLP	89.56
MLP + CNN	92.78

표 3 모델 별 성능 지표

Ⅴ 결론

본 논문은 통계 데이터를 입력으로 사용하는 MLP 모델과 Mel-Spectrogram을 입력 이미지로 사용하는 CNN 모델을 Concatenate하여 응용 트래픽을 분류하는 모델을 제안했으며 3%의 성능이 향상되었음을 확인했다. 향후 연구로는 응용의 종류를 50개 정도로 증가시켰을 때도 효과적으로 응용 트래픽을 분류할 수 있는 모델을 만들기 위한 연구를 수행할 계획이다.

ACKNOWLEDGMENT

본 논문은 2020년도 산업통상자원부 및 한국산업기술평가관리원(KEIT)연구비 지원에 의한 연구 (No. 20008902, IT비용 최소화를 위한 5채널 탐지기술 기반 SaaS SW Management Platform(SMP) 개발) 이고, 2021년도 교육부의 재원으로 한국연구재단의 지원을 받아 수행된 지자체-대학 협력기반 지역혁신 사업의 결과(2021RIS-004)임

참 고 문 헌

[1] 지세현, 백의준, 신무곤, 채병민, 문호원, 김명섭, "합성곱 신경망 기반 웹 응용 트래픽 분류 모델 설계", 통신학회 논문지 Vol.44 No.05, Jun. 2019, pp. 1113-1120

[2] KRIZHEVSKY, Alex; SUTSKEVER, Ilya; HINTON, Geoffrey E. Imagenet classification with deep convolutional neural networks. Advances in neural information processing systems, 2012, 25: 1097-1105.

[3] 이정현, 윤의녕, 조근식 "전이 학습과 어텐션(Attention)을 적용한 합성곱 신경망 기반의 음성 감정 인식 모델" 2020년도 정보과학회논문 Vol.47 No.7, pp. 665-673

필터링 방법을 이용한 응용 트래픽 분류의 속도 개선 방안

이민성, 박지태, 백의준, 홍윤환*, 김명섭

고려대학교, 닥터소프트*

{min0764, pjt5846, pb1069, tmskim}@korea.ac.kr, hond@doctorsoft.co.kr*

Method for Speed Improvement of Application Traffic Classification Using Filtering Method

Min-Seong Lee, Jee-Tae Park, Ui-Jun Baek, Youn-Hwan Hong*, Myung-Sup Kim

Korea Univ. Doctorsoft*

요 약

인터넷의 발전으로 인해 다양한 응용 프로그램들이 등장함에 따라 네트워크 트래픽이 증가하고 있으며 특히 COVID-19로 인한 재택근무가 늘어나고 인터넷 사용이 활발해짐에 따라 가속화되는 추세다. 이에 네트워크 모니터링 및 관리의 중요성이 높아지고 있으며 사용자 품질 보장, 네트워크를 이용한 공격 방어 등을 위한 응용 트래픽 분류는 네트워크 관리 분야의 가장 중요한 기술 중 하나다. 응용 트래픽 분류를 위해 전통적으로 포트 기반, 시그니처 기반 방법, 통계 특징을 이용한 머신러닝 기반 방법들이 사용되었으며 최근에는 딥러닝 기반의 응용 트래픽 분류 방법이 가장 좋은 분류 정확도를 나타내고 있다. 하지만, 딥러닝 기반의 분류 방법은 막대한 계산량을 바탕으로 수행되기에 실제 환경의 대용량 트래픽을 실시간으로 분류하기 어려우며 딥러닝 기반 모델의 경량화를 통한 분류 속도 개선은 응용 트래픽의 복잡성으로 인해 분명한 한계치가 존재한다. 이에 우리는 입력되는 트래픽을 약한 분류기로 먼저 분류하고 분류하기 어려운 나머지 트래픽을 강한 분류기로 분류하는 필터링 방법을 이용한 응용 트래픽 분류 속도 개선 방안을 제안한다. 결과적으로 우리가 제안한 방법은 기존 단일 분류기와 비교하여 분류 정확도는 거의 유지하면서도 분류 속도는 1.5배 증가하였다.

Ⅰ. 서 론

네트워크의 발전으로 인하여 트래픽의 양이 증가하고 있고, 다양한 응용 프로그램들이 등장하고 있다. 특히, COVID-19로 인한 재택근무가 늘어나고 집에서 취미 생활을 즐기는 환경으로 인해 인터넷 사용이 활발해지면서 화상 회의 시스템이나 메신저, 그리고 스트리밍 서비스 등 편의성이 개선된 응용 프로그램들이 사용되고 있다. 이러한 상황에서 트래픽 분석 및 응용 프로그램의 분류는 네트워크의 효율적인 운용과 관리를 위해 필수적이다.

기존 트래픽 분류는 포트 기반 분석, 페이로드 시그니처 기반 분석 등의 방법론들을 사용하였으나, 암호화된 트래픽의 사용으로 인하여 트래픽 분류에 사용되기 어렵다, 이를 보완하기 위하여 트래픽의 플로우 통계 정보를 이용한 머신 러닝 및 딥 러닝 모델을 사용한 응용 트래픽 분류가 연구되고 있다[1].

회사나 학교 등에서는 네트워크 자원을 효율적으로 운용하고 관리하는 것이 필수적이다. 각 장소에서 사용되는 네트워크 상황에 따라서 관리하는 트래픽의 양이 다를 수 있고, 분류해야 하는 응용 트래픽의 종류도 다르다. 이에 따라 응용 트래픽 분류를 가능하게 하는 머신 러닝 및 딥 러닝 모델을 적용 할 때 고려해야 하는 부분이 많아지게 된다.

여러 분야에서 사용되고 있는 딥 러닝 모델은 높은 정확도를 보이면서 지속적인 연구가 진행되고 있다. 응용 트래픽 분류 분야에서도 머신 러닝 및 딥 러닝을 이용한 다양한 연구들이 진행되고 있으며, 높은 정확도를 보이는 모델들도 있다. 지속적인 연구를 통해 정확도가 개선된 모델에서는 IoT 기기나 스마트폰 등 소형 기기에서도 동작 할 수 있도록 소형화되고 있으며, 요구 연산 성능 및 요구 전력을 최소화 하려는 노력을 하고 있다. 이미지 분야에서는 이러한 경량화 모델들이 많이 연구되어 높은 정확도와 함께 실생활에 적용 할 수 있는 모델들이 나타나고 있다. 트래픽 분류 및 분석 분야에서도 높은 정확도를 가진 모델들과 관련된 연구들이 진행되었지만 대용량 트래픽을 처리 할 수 있도록 하는 처리 속도와 관련된 연구는 부족하다. 또한, 경량화를 생각하지 않아도 모델을 처리하는 방법을 적절하게 이용한다면 처리 속도를 개선 할 수 있다.

본 논문에서는 머신 러닝과 딥 러닝 방법을 순차적으로 이용하여 데이터 처리 속도를 개선하는 방안에 대하여 제안한다. 제안하는 방법은 정확도를 유지하면서 전체 처리 속도를 줄이기 위한 방안이다. 데이터 셋에서 분류가 쉬운 데이터 셋은 처리 속도가 약한 분류기로 처리하고 머신 러닝 알고리즘이 처리하지 못하는 분류가 어려운 데이터 셋은 강한 분류기를 사용하여 전체적인 속도를 개선하는 방법을 제안한다.

2장에서는 필터링 방법을 사용한 처리 속도 개선 방법의 구체적인 설명을 기술하고 3장에서는 실험 결과를 기술한다. 마지막으로 4장에서는 결론 및 향후 연구에 대하여 기술하고 논문을 마친다.

Ⅱ. 필터링 방법 이용한 처리 속도 개선 방법

본 장에서는 제안하는 필터링 방법 이용한 처리 속도 개선 방법에 대하여 설명한다.

트래픽 데이터가 모델에 들어가게 되면 약한 분류기에서는 우선적으로 트래픽 데이터의 분류를 진행한다. 분류가 완료되면 약한 분류기에서 확실하게 분류된 데이터는 결과로 도출이 되며, 분류가 확실하지 않다고 판단되는 데이터는 강한 분류기로 보내게 된다. 약한 분류기가 확실하게 분류했다고 판단 할 수 있는 기준을 임계값과 신뢰도로 정한다. 임계값은 머신 러닝이 분류를 진행하였을 때 최소 분류 확률의 기준을 정의하여 확실하게 분류한 데이터라고 판단하는 기준이 된다. 신뢰도는 이를 검증하기 위한 비율이다. 신뢰도는 임계값을 기준으로 분류된 플로우들 중 정확하

※ 본 논문은 2020년도 산업통상자원부 및 한국산업기술평가관리원(KEIT) 연구비 지원에 의한 연구 (No. 20008902, IT비용 최소화를 위한 5채널 탐지기술 기반 SaaS SW Management Platform(SMP) 개발)이고 2021년도 교육부의 재원으로 한국연구재단의 지원을 받아 수행된 지자체-대학 협력기반 지역혁신 사업의 결과 (2021RIS-004)임.

게 분류 된 비율을 계산하였다. 신뢰도가 높을수록 약한 분류기에서 플로우를 확실하게 분류하였다고 판단 할 수 있다.

Random Forest를 사용하여 300개의 플로우 데이터를 분류하였을 때 임계값 별 신뢰도는 표1과 같다. TP_t+FP_t는 임계값을 넘긴 플로우 전체 개수이며 TP_t는 임계값을 넘긴 플로우 중 분류가 정확하게 된 플로우의 개수이다. 이 두 지표를 바탕으로 신뢰도가 결정된다. 임계값을 적절하게 사용한다면 Random Forest에서 71%의 분류 정확도를 가지고도 분류가 가능한 데이터를 100%까지 정확하게 분류 할 수 있다.

표 1. 임계값별 신뢰도

Threshold	0.4	0.5	0.6	0.7
TP_t	119	99	84	45
TP_t+FP_t	127	103	85	45
신뢰도	94%	96%	99%	100%

머신 러닝에서 1차로 분류된 결과를 제외한 나머지 플로우들은 정확도가 더 높은 딥 러닝 모델에서 분류된다. 전체 데이터를 모두 분류하지 않고 어려운 분류 문제만 딥 러닝 모델에서 분류하도록 하여 딥 러닝이 처리하는 데이터의 양을 줄여 처리 속도를 개선한다.

Ⅲ. 실험 결과

본 연구에서 사용되는 데이터 셋은 10가지 응용 트래픽에서 발생한 1000개의 플로우의 원시 데이터를 이용하였다. 1000개의 플로우 중에서 700개의 플로우는 학습 모델, 300개의 플로우는 테스트 모델에 사용되었다.

전체적인 처리 속도를 비교하기 위하여 데이터 셋을 각 알고리즘에 적용하였다. 사용된 머신 러닝 및 딥 러닝 알고리즘은 Random Forest와 CNN[2] 알고리즘을 사용하였다. 먼저 Random Forest 알고리즘은 분류 정확도가 71%이며, CNN 알고리즘은 91%의 분류 정확도를 보였다. 분류 정확도는 딥 러닝 모델인 CNN 알고리즘이 더 높지만, 플로우당 처리 속도는 Random Forest알고리즘이 17배 더 빠른 처리 속도를 보여주고 있다.

표 2. Random Forest와 CNN을 사용한 분류 결과

Model	Random Forest	CNN
Accuracy	71%	91%
처리 속도	33μs/flow	566μs/flow

300개의 테스트 플로우를 기반으로 데이터를 처리할 때 Random Forest는 0.01초의 처리 속도를 보여주고 CNN모델에서는 0.17초의 처리 속도를 보여주고 있다. 제안하는 방법에서는 Random Forest에서 모든 데이터를 먼저 분류하게 된다. CNN 모델은 Random Forest에서 설정한 임계값에 따라서 처리해야 하는 데이터의 양이 달라진다. 임계값이 낮을수록 Random Forest가 처리할 수 있는 데이터가 많아지고, 임계값이 높다면 Random Forest에서 처리 할 수 있는 데이터가 적어지게 된다. 임계값이 높을수록 제안하는 방법의 처리 속도가 늘어나게 되지만 CNN모델을 한 개만 적용하였을 때 발생하는 처리 속도보다는 처리 속도를 줄일 수 있다. 그림 1은 Random Forest와 CNN 모델이 각각 트래픽 데이터를 처리하는 속도와 임계값을 다르게 설정하였을 때 처리 속도가 개선된 것을 보여준다. 제안하는 방법에서 임계값 별 분류 정확도는 평균 90%의 정확도를 보이고 있으며 이는 CNN 모델을 사용하였을 때의 분류 정확도인 91%와 비슷하다.

현재 제안하는 방법에서는 단순하게 두 가지 모델을 사용하였고, 트래픽 플로우도 전체 1000개 중 테스트 플로우는 300개로 적은 양을 사용하였다. 하지만 실제 네트워크 상황에서 적용하게 되면 처리해야 하는 트래픽의 양도 늘어나게 된다. 또한, 딥 러닝 알고리즘을 사용하기 전에 약한 분류기를 여러 개를 사용하여 확실하게 분류 할 수 있는 데이터를 분류해 준다면 처리 속도를 훨씬 더 개선시킬 수 있다. 제안된 방법을 사용하면 빠른 처리 속도를 가지지만 정확도가 낮은 약한 분류기와 높은 정확도를 가지지만 느린 처리 속도를 가진 강한 분류기의 장점을 가지면서 높은 정확도와 빠른 처리 속도를 보일 수 있다.

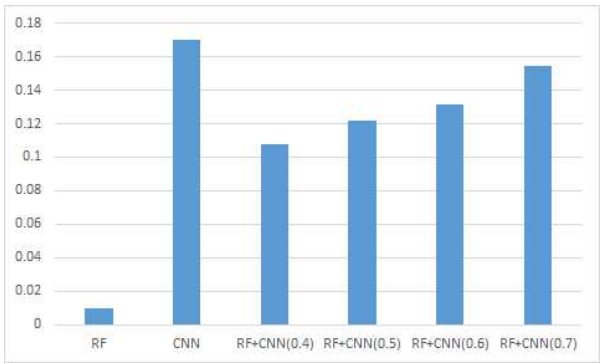


그림 1. 임계값을 적용한 모델 처리 속도

Ⅳ. 결론 및 향후 연구

본 논문은 응용 트래픽 분류에서 머신 러닝 및 딥 러닝 알고리즘을 순차적으로 적용하여 처리 속도를 개선하는 방법을 제안하였다. 사용한 머신 러닝 알고리즘은 Random Forest를 사용하였고 딥 러닝 알고리즘은 CNN 알고리즘을 사용하였다. 분류가 쉬운 데이터들은 머신 러닝 모델에서 빠르게 처리하고 분류가 어려운 데이터들을 딥 러닝 모델에서 처리하여 분류 정확도를 유지하면서 처리 속도를 개선하는 방법이다. 실험 결과 Random Forest는 71%의 분류 정확도를 나타냈지만, Threshold를 이용하여 100%에 해당하는 분류 결과를 나타 낼 수 있다. 또한 정확도를 유지하면서 처리 속도가 개선된 것을 볼 수 있다.

향후 연구로는 앞서 말했던 실제 네트워크 상황에 적용하였을 때를 가정하여 트래픽의 양을 증가시켰을 때 처리 속도의 비교와 파이프라인 형태로 딥 러닝 모델 앞에 여러 개의 머신 러닝 모델을 사용하여 딥 러닝 모델에서 분류 하게 되는 데이터를 줄여 처리 속도를 개선하는 방법에 대하여 연구 할 예정이다.

참 고 문 헌

[1] S. Rezaei and X. Liu, "Deep Learning for Encrypted Traffic Classification: An Overview," in *IEEE Communications Magazine*, vol. 57, no. 5, pp. 76-81, May 2019, doi: 10.1109/MCOM.2019.1800819.

[2] KRIZHEVSKY, Alex; SUTSKEVER, Ilya; HINTON, Geoffrey E.Imagenet classification with deep convolutional neural networks.Advances in neural information processing systems, 2012, 25:1097-1105.

딥러닝 기반 응용 트래픽 분류에서 데이터셋과 파라미터의 수량적 관계성에 대한 연구

신창의*, 최정우**, 백의준**, 박지태**, 김명섭**

국방기술품질원*, 고려대학교**

*superego99@dtaq.re.kr, **{choigoya97, pb1069, pjj5846, tmskim}@korea.ac.kr

A study on the quantitative relationship between datasets and parameters in deep learning-based application traffic classification

Chang-Yui Shin*, Jeong-Woo Choi**, Ui-jun Baek**, Jee-Tae Park**, Myung-Sup Kim**

*Defense Agency for Technology and Quality, **Korea University

요 약

현대 문명의 흐름인 인터넷을 통해 전송되는 데이터의 엄청난 증가와 더불어 여러 가지 보안적 이슈로 인해 트래픽 암호화가 메인흐름이 되었다. 암호화된 트래픽은 동전의 앞뒷면과 같이 개별정보의 보안성을 강화시키기도 하지만 와 실용적인 트래픽분류를 방해하는 효과를 동시에 가져왔다. 이에 따라 유사영역인 트래픽 탐지와 분류는 급속한 관심과 성장을 이루고 있는데, 이전에는 머신러닝 기법을 통해 트래픽 탐지와 분류가 성장했다면 현재는 딥러닝 기법을 활용하는 쪽으로 관심과 성장이 전환되고 있다. 본 논문에서는 딥러닝을 기반으로 하는 트래픽 분류에서 분류의 성능을 높이기 위해 엔지니어 관점에서 추가하는 통계적 정보의 선택이 파라미터의 증가에 영향을 미치는데, 이때 데이터셋이 한정적일때 모델의 적합도에 어떠한 영향을 미치는가에 대해 유추 가능한 이론적 배경을 바탕으로 실험해보았다. 이를 통해 데이터셋의 수 한정적일 때 이를 고려하여, 파라미터가 구성되도록 것이 분류모델의 적합성에 영향을 미치는 요소가 될 수 있음을 확인했다.

Ⅰ. 서 론

IoT(Internet of Things), 즉 인터넷에 연결되어 애플리케이션이나 네트워크에 연결된 장치, 또는 산업 장비 등의 다른 사물들과 데이터를 공유할 수 있는 수 많은 사물들을 통한 헬스케어, 교통, 에너지 등 다양한 서비스 분야의 급격한 성장이 지속되고 있다. 이런 가운데 컴퓨터 네트워크의 QOS, 지능형 네트워크 운영·유지관리 및 네트워크 보안 등 다양한 분야에서 네트워크 트래픽 분류가 활용되고 있다. 최근 네트워크 기술의 발전과 더불어 여러 가지 보안취약성을 뒷받침하고자 암호화 트래픽을 사용하는 추세이다. 암호화된 트래픽으로 인해 개별 정보의 보안성은 강화된 반면 다양한 응용서비스의 실용성을 강화시키는 트래픽분류를 방해하는 효과를 동시에 가져와, 암호화된 트래픽 분류 및 탐지는 중요성이 보다 커지고 있다.

이미지 처리에서 급격히 성장한 딥러닝 기법은 다른 컴퓨팅영역에서의 확장으로 이어지고 있다. AI분야의 진화에 발맞춰 네트워크 트래픽 분류에서도 머신러닝 기법에서 딥러닝 기법으로 관심의 전환이라는 큰 흐름이 지속되고 있다. 머신러닝에 비교했을 때 딥러닝이 보다 높은 성능을 보이기 위해서는 대량의 데이터를 기반으로하는 학습을 통해 가능한데, 실제 환경에서 악성트래픽의 경우 대량의 데이터를 얻기도 어렵고, 대량의 데이터인 경우 연산에 많은 시간과 자원이 소비되는 제한사항이 있다.

본 논문은 2020년도 산업통상자원부 및 한국산업기술평가관리원(KEIT) 연구비 지원에 의한 연구 (No. 20008902, IT비용 최소화를 위한 5채널 탐지기술 기반 SaaS SW Management Platform(SMP) 개발)이고 2021년도 교육부의 재원으로 한국연구재단의 지원을 받아 수행된 지자체-대학 협력기반 지역혁신 사업의 결과 (2021RIS-004)이다.

이에 본 논문에서는 딥러닝기반 응용트래픽 분류에서 데이터셋이 한정적일 때, 분류모델 연산의 중요요소인 파라미터의 증가가 모델의 적합성에 미치는 영향에 대해 접근하였으며, 실험결과를 통해 파라미터와 데이터셋의 수를 연계한 가운데 모델을 설계하고 학습시켜야 함을 확인하였다.

본 논문의 구성은 다음과 같다. 서론에 이어 2장에서는 관련된 주요기술에 대해 제시하고, 3장 본론에서는 이론적 배경, 데이터셋의 구성, 시험환경 등에 대해 설명하고, 4장에서는 이에 대한 실험을 수행한 결과와 분석을 기술하고, 5장에서는 결론과 향후 연구방향을 제시하고자 한다.

Ⅱ. 관련연구

심층 신경망(Deep Neural Networks)은 기존의 머신러닝 모델이 가져올 수 있는 성능을 능가함에 따라 가장 인기있는 방법론 중 하나로 대두되어 지금까지도 급속히 발전되어왔으며 앞으로도 지속될 것으로 전망된다. 심층 신경망 중에서도 가장 널리 사용되는 유형은 LeCun et al.[1][2]에서 역사가 시작되는 CNN(Convolutional Neural Networks)이다. CNN은 특징을 추출하는 Convolutional layer와 데이터크기를 줄이는 Pooling layer로 구성된다.

심층신경망의 정확도를 높이기 위한 다른 추가적인 기법들도 같이 사용되고 있는데, Batch normalization과 Dropout layer가 공통적이다. Ioffe and Szegedy.[3]가 제시하는 Batch normalization은 훈련하는 동안 모든 피처에 대해 배치레벨에서의 정규화를 하고 이어서 전체 훈련데이터 세트레벨에서 크기 재조정을 한다. 이로써 훈련을 통해 얻어진 새로운 평균과 분산은 배치수준에서 습득한 평균과 분산을 대체하게 되는데, 훈련 수렴을 보다 빠르게 이끌어 성능결과를 개선하는데 기여한다.

Srivastava et al.[4]가 제시하는 Dropout layer는 이전 레이어의 출력비율을 0으로 설정하여 보이지 않는 데이터에 대해 일반화시킨다. 이 정규화 기능을 신경망이 특정 입력에 과도하게 의존하지 않게하여 과적합문제를 개선하는데 기여한다.

CNN과 더불어 최근 각광 받고있는 알고리즘이 RNN(Recurrent Neural Networks)인데, RNN은 히든 노드가 방향을 가진 엣지로 연결돼 순환구조를 이루며, 시퀀스 길이에 관계없이 인풋과 아웃풋을 받아들일 수 있는 게 장점이어서 유연하게 구조를 가질 수 있다. 하지만 RNN도 관련 정보와 그 정보를 사용하는 지점 사이 거리가 멀 경우 역전파시 그래디언트가 점차 줄어 학습능력이 크게 저하되는 단점이 있어 이를 개선하여 고안된 것이 LSTM(Long Short Term Memory)과 GRU(Gated Recurrent Unit)[5]이다. 이들은 RNN의 특성을 가지면서 동시에 역전파시 그래디언트가 잘 전파되도록 기능을 개선한 것이다.

최근에는 자연어처리 분야에서 RNN에 기반한 seq2seq 모델이 고정된 크의 벡터에 모든 정보를 압축함에 따른 정보손실과 고질적인 문제인 기울기 소실 문제를 발생시키는 문제에 대한 대안으로, Attention 기법이 등장하면서 텍스트처리 관점에서의 딥러닝 기법의 발전은 지속되고 있다.

Ⅲ. 본론

일반적으로 딥러닝 기법은 머신러닝 기법보다는 학습에 사용되는 파라미터(parameter) 개수가 현저히 많다. 머신러닝 기법은 엔지니어레벨에서 여러 가지 피처(feature)를 선정해 학습에 사용하지만, 딥러닝에서는 피처를 알고리즘 자체에서 추출한다고 이해하면 된다.

응용 트래픽 분류에 있어서 플로우간 관계성을 고려한 모델의 성능이 높다는 것[6]을 기반으로, 패킷 전체의 플로우 통계정보를 기본으로 추가적인 플로우 통계정보(첫번째 패킷으로부터 N번째 패킷까지의 통계정보)를 통한 분류가 뛰어날 것이라는 가정을 하였고, 실험을 통해 확인하려고 한다.

또한 심층신경망을 통해 만들어내는 모델은 히든레이어를 통한 피처의 다양한 선택을 가능하게 하므로, 다중선형회귀 특성의 추정모델이 유사성을 가질 수 있다는 가정을 전제로 하였다. 따라서

$$f(x) \approx \hat{f}(x) \tag{1}$$

$$\hat{f}(x) = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \ldots + \beta_p X_p + \epsilon \tag{2}$$

이므로, RSE(Residual standard error)은

$$RSE = \sqrt{\frac{1}{n-p-1} RSS} \tag{3}$$

이고, 여기서의 RSS(residual sum squares)는

$$\begin{aligned} RSS &= \sum_{i=1}^{n} (y_i - \hat{y}_i)^2 \\ &= \sum_{i=1}^{n} \left(y_i - \hat{\beta_0} - \hat{\beta_1} x_{i1} - \hat{\beta_2} x_{i2} - \ldots - \hat{\beta_p} x_{ip} \right)^2 \end{aligned} \tag{4}$$

이므로, RSS의 감소가 p의 증가에 비해 작으면 더 많은 변수를 가진 모델이 더 높은 RSE를 가질 수 있다는 것을 알 수 있는데, 결론적으로 변수의 개수가 증가할수록 표본의 분산은 커지지만 RSE는 커지므로 언더피팅 또는 오버피팅 문제가 발생하지 않도록 적절한 개수의 변수를 선택하는 것이 필요하다[7]. 본 논문에서의 딥러닝모델을 기반으로 시험할 것이나, 피처의 선택을 모델에 위임하면 파라미터(p)의 수가 통제범위에서 벗어나기 때문에 성능 및 연구목적에 따라 p의 증가량을 통제변수로 넣고, 그 결과에 대해 실험을 통해 확인하는데 목적을 두었다.

본 논문에서는 딥러닝기반 응용트래픽 분류에서 한정된 데이터셋과 파라미터 수와의 관계에 대해 살펴보기 위해, 파라미터에 영향을 줄 수 있는 요소를 입력단계와 처리단계 2가지 경우로 구분해 보았다. 입력단계에는 패킷 헤더정보와 플로우 통계정보가 있으며, 처리단계에는 모델의 하이퍼파라미터가 있다. 처리단계의 하이퍼 파라미터는 입력정보의 피처를 추출하는 단계이므로 앞 단계인 입력단계에 의존적이고, 레이어가 깊을수록 학습효과가 뛰어나므로 모델링과정에서는 고정함으로써 고려사항에서는 제외했다. 딥러닝 기법에서 피처를 선정하지 않는 것이 일반적이나 입력단계의 정보에 변화를 주어, 결과적으로 파라미터의 수에 영향을 줄 수 있도록 하기 위해서 플로우 통계정보를 선택적으로 반영하였다. 사용된 플로우 통계정보는 패킷 길이와 발생 간격(Inter-Arrival Time)에 대한 정보이며, 패킷 전체 또는 첫 N개의 패킷의 길이 및 간격 정보 집계하여 13가지 통계 항목을 추출한 것이다. 통계 항목은 합 · 최댓값 · 최솟값 · 산술평균 · 기하평균 · 1분위 수 · 중앙값 · 3분위수 · 4분범위 · 모표준편차 · 표본표준편차 · 왜도 · 첨도를 포함한다. 패킷 헤더정보는 패킷 헤더정보를 대부분 수정 없이 반영하였으며, 암호화된 패킷이므로 패킷 길이정보로만 부가적으로 변형했다. 아래의 표 1은 수집한 응용 데이터셋의 종류를 나타낸다.

표 1. 수집한 응용 데이터셋

Bithumb	Coineone	Upbit	Excel
Teams	Excel	PPT	Word
Onenote	WEB_Excel	WEB_PPT	WEB_Word
Daum	Gmail	Nate Mail	Naver mail
Naver band	kakaotalk	Skype	Agoda
Airbnb	Goodchoice	Hotels.com	Netflix
Yanolja	11st	Coupang	Gmarket
Musinsa	Tmon	Wemakeprice	Facebook
Instagram	Kakaostroy	Naver blog	Tistory
Twitter	Disney+	Melon Music	Naver TV
Tving	Twitch	Wavve	Naver Series
Youtube Music	Hotels Combined	Kakao webtoon	Naver Webtoon
Kakao page	Youtube		

그리고 아래의 표 2는 전체 통계 정보에 포함된 첫 k개 통계 정보들 중, k를 변화시켜 만든 서브데이터셋을 나타낸다. 표 2의 플로우 통계정보 구성에서 k는 숫자 범위를 의미한다.

표 2. 데이터셋 별 플로우 통계정보와 파라미터 수

데이터셋	플로우 통계정보 구성	특징 수(개)	파라미터 수(개)
Set 1	패킷전체,	78	63,621
Set 2	패킷전체, 1~5	156	83,589
Set 3	패킷전체, 1~5, 1~10	234	103,557
Set 4	패킷전체, 1~5, 1~10, 1~15, 1~20, 1~25, 1~30	546	183,429

심층신경망은 가장 기본적인 MLP(Multi Layer Perceptron)로 선정했으므로, 실험결과에서는 모델의 성능지표 개별 값이 가지는 고저의 의미보다 성능지표별 값의 변화를 통해 p의 증가량 대비 모델의 적합성 변화를 살펴볼 예정이다.

Ⅳ. 실험 및 분석

데이터셋은 각 응용별 플로우 500개로 구성되어 있는데, 실험을 통해 5번째 패킷까지의 통계정보가 응용트래픽 분류모델의 성능을 높이는 정보이고, 다른 통계정보는 상대적으로 그렇지 않음을 우선적으로 확인했다. 물론 모델링에 사용되는 심층신경망의 종류와 형태에 따라 결과는 달라질 수는 있지만, 실험에서는 이것을 기반으로 표 3과 그림 1 같이 수집데이터 Set 1~4 각각에 대해 모델의 성능지표를 확인하는데 중점을 두었다.

아래의 표 3에서는 수집한 응용 데이터셋의 패킷 헤더정보와 플로우 통계정보를 Set 1~4로 구분한 후, MLP를 통해 각 응용별 분류한 결과를 의미하는 성능지표를 나타낸 것이다.

표 3. 데이터셋 별 성능지표

데이터셋	Precision(%)	Recall(%)	Accuracy(%)
Set 1	60.7	29.1	39.0
Set 2	65.6	36.7	45.5
Set 3	63.9	33.3	43.9
Set 4	59.4	33.4	42.2

아래의 그림 1은 표 3에서 살펴본 것을 재해석한 것인데, 데이터 Set 1에서 Set 4로의 순차적 구성은 추가적인 통계정보가 더해지는 추세를 의미한다고 볼 수 있는데, 통계정보가 추가되어도 모델의 성능지표는 감소하는 것을 확인할 수 있다.

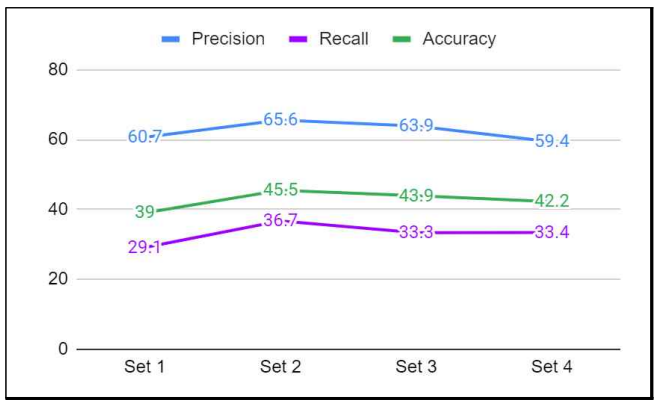


그림 1. 데이터셋 별 성능지표

결과적으로 데이터셋의 수가 한정적일 때, 추가적인 통계정보 중 일부는 정확도를 높이는데 기여했으나, 다른 통계정보들은 추정모델의 파라미터의 수를 늘리기만 할 뿐 오차를 크게 하여, 모델의 적합도를 떨어뜨리는 결과를 나타낸다고 볼 수 있었다.

Ⅴ. 결론 및 향후 연구

본 논문에서는 딥러닝을 기반으로 하는 트래픽 분류에서 데이터셋이 한정적 일때 파라미터의 증가량이 모델의 적합도에 어떠한 영향을 미치는가에 접근하기 위해, 또한 분류의 성능을 높이기 위해 엔지니어 관점에서 추가하는 통계정보(피처)의 선택이 파라미터의 수를 증가시킬 수 있도록 했다. 일부 통계정보는 모델의 적합도를 향상시킬 수 있지만 데이터셋의 수량을 고려치 않고 파라미터의 수(통계정보)를 계속적으로 늘리면 모델의 적합성을 하향시킬 수도 있음을 실험적으로 확인하였다. 나아가 딥러닝 모델이 선택하는 피처의 수가 파라미터의 수를 구성하므로 데이터셋의 수를 고려하여 딥러닝 모델을 모델링하는 것이 중요할 수 있음을 유추해보았다.

향후 연구주제는 다음의 방향으로 확장하려고 한다. 첫째는 고정요소로 판단했던 통계항목을 모델의 적합성 향상에 대한 기여도에 대해 본 논문의 관점에서 딥러닝 모델을 통해 실험해보고자 한다. 둘째로 데이터셋을 한정적 요소로 두고 파라미터의 수에 변화를 주어 결과를 도출한 것에서 나아가, 파라미터를 고정한 가운데 한정적이었던 데이터셋을 단계적으로 증가시켜 보는 것을 딥러닝 모델별로 실험해보고자 한다.

데이터셋의 수가 늘어나면 늘어날수록 분류모델의 정확도가 높아지는 것으로 예측할 수도 있지만 구현된 모델에 따라 정확도의 증가가 둔감해지는 시점이 존재할 것으로 생각되어, 구현하는 모델별 데이터셋과 파라미터의 수는 합리적인 비율이 있음을 찾아보는 주제로 확장하는 것도 의미가 있을 수 있어 연구를 진행하려고 한다.

참 고 문 헌

[1] Y. LeCun et al., “Backpropagation Applied to Handwritten Zip Code Recognition,” Neural Computation, vol. 1, no. 4, pp. 541 - 551, Dec. 1989, doi: 10.1162/neco.1989.1.4.541.

[2] Y. LeCun, Y. Bengio, and G. Hinton, “Deep learning,” Nature, vol. 521, no. 7553, Art. no. 7553, May 2015, doi: 10.1038/nature14539.

[3] S. Ioffe and C. Szegedy, “Batch Normalization: Accelerating Deep Network Training by Reducing Internal Covariate Shift,” p. 9.

[4] N. Srivastava, G. Hinton, A. Krizhevsky, I. Sutskever, and R. Salakhutdinov, “Dropout: A Simple Way to Prevent Neural Networks from Overfitting,” p. 30.

[5] J. Chung, C. Gulcehre, K. Cho, and Y. Bengio, “Empirical Evaluation of Gated Recurrent Neural Networks on Sequence Modeling,” arXiv:1412.3555 [cs], Dec. 2014, Accessed: Mar. 26, 2022. [Online]. Available: http://arxiv.org/abs/1412.3555

[6] Ui-jun Baek et al, “DL-based Traffic Classification considering Relationship between Flows”, KICS 2022 Winter

[7] F. Sohil, M. U. Sohali, and J. Shabbir, “An introduction to statistical learning with applications in R: by Gareth James, Daniela Witten, Trevor Hastie, and Robert Tibshirani, New York, Springer Science and Business Media, 2013, $41.98, eISBN: 978-1-4614-7137-7,” Statistical Theory and Related Fields, vol. 6, no. 1, pp. 87 - 87, Jan. 2022, doi: 10.1080/24754269.2021.1980261.

다중 모형 CNN 기반 응용 트래픽 분류

백의준, 김보선, 박지태, 신창의*, 김명섭
고려대학교, *국방기술품질원
{pb1069, boseon12, pjj5846, tmskim}@korea.ac.kr, superego99@dtaq.re.kr*

Multi-Shape CNN based Application Traffic Classification

Ui-jun Baek, Boseon Kim, Jee-Tae Park, Chang-Yui Shin*, Myung-Sup Kim
Korea University, *Defense Agency for Technology and Quality

요 약

인터넷 사용자의 수가 나날이 증가하고 점점 더 다양하고 복잡한 유형의 응용 또는 공격이 발생함에 따라 네트워크 트래픽 분류는 네트워크 관리 분야의 중요한 직무로 자리 잡았다. 그러나 가변 포트 번호 방식과 페이로드 암호화 기술의 도입은 전통적인 네트워크 트래픽 분류 기술에 명확한 한계점을 가져다주었다. 이에 통계적인 특징을 학습하여 응용 트래픽을 분류하는 머신러닝 기반 기술이 조명되었으며 최근에는 CNN을 이용한 딥러닝 기반 표현학습 방법이 주로 연구되고 있다. 기존 CNN 기반 응용 트래픽 분류에서는 입력 데이터로 패킷 원본 데이터를 가로와 세로의 비율이 같은 2차원 이미지 형태가 주로 고려되었으나 우리는 패킷 내 필드 값의 연속성과 패킷 데이터가 공간 정보가 없는 1차원 데이터임에 초점을 맞추었다. 우리는 패킷의 입력 벡터를 다양한 모형으로 변환하여 그에 대응하는 분류 모델을 생성하였으며 각 분류 모델의 성능을 비교한 결과 기존의 정사각형 모형의 입력 벡터보다 1차원 형태의 입력 벡터가 입력된 모델이 더 정확하게 응용 트래픽을 분류하였다. 또한 우리는 단일 입력 벡터를 다중 모형 입력 벡터로 변환하여 동시에 학습하고 앙상블 기반 응용 트래픽 분류 모델을 제안하였으며 제안한 모델은 단일 모형이 입력된 분류 모델보다 27% 높은 정확도를 보였다.

Ⅰ. 서 론

인터넷 사용자의 수가 나날이 증가하고 점점 더 다양하고 복잡한 응용 트래픽 또는 공격이 발생함에 따라 네트워크 트래픽 분류는 응용 타입 식별, 비정상 행위 탐지, QoS(Quality of Service) 보장 등 네트워크 관리 분야의 중요한 직무 중 하나로 자리매김하였다. 또한 네트워크 트래픽 암호화 기술이 인터넷 서비스 전 분야에 걸쳐 적용됨에 따라 전통적인 트래픽 분류 방법들을 통해 응용을 분류하는 것이 어려워졌고 이는 컴퓨터 네트워크 분야에서 정확하고 강인한 트래픽 분류 방법이 필요함을 강조하고 있다.

네트워크 트래픽 분류 분야의 대표적인 방법은 크게 포트 기반 분류, 페이로드 기반 분류, 머신러닝 기반 분류로 나눌 수 있다. 포트 기반 분류와 페이로드 기반 분류는 전통적으로 널리 쓰였던 분류 방법이나 가변 포트 번호의 도입과 트래픽 암호화 기술의 도입으로 인해 정확히 트래픽을 분류할 수 없다는 명확한 한계점을 가진다. 머신러닝 기반 분류는 현재 가장 많이 사용되고 있는 분류 방법의 하나며 트래픽 데이터로부터 추출된 통계적 특징을 학습하여 분류 모델을 생성한다. 그러나, 특징 데이터 차원 수가 증가하면 할수록 따라 학습이 제대로 수행되지 않는 한계점을 가지고 있으며 이러한 이유로 머신러닝 기반 분류에서는 분류 성능에 유의미한 영향을 미치는 특징이 무엇인지 선택하는 방법이 중요한 도전 과제로 남아있다. 최근에는 머신러닝 기반 방법 중 딥러닝 기반 방법이 많은 연구에서 고려되고 있으며 특히 컴퓨터 비전, 이미지 인식 분야에서 높은 성능을 발휘하는 CNN(Convolutional Neural Network) 기반 분류 방법이 가장 대표적이며 네트워크 플로우가 패킷의 시계열로 구성된 점을 이용하여 RNN(Recurrent Neural Network) 기반 분류 방법 또한 적용되는 추세이다. 일반적으로 CNN 기반 트래픽 분류에서는 네트워크 패킷 데이터를 2차원 이미지로 변환하여 분류 모델에 입력한다. 입력된 2차원 데이터는 여러 층의 Convolutional Layer와 Pooling Layer를 거치며 패킷의 특성을 포함하고 있는 특징 맵으로 변환된다. 그러나 네트워크 패킷은 1차원 데이터이며 일부 필드 값은 연속성을 지니고 있다는 점에서 2차원 이미지 구조와는 근본적인 차이가 있다. 우리는 입력되는 패킷의 필드 값이 패킷을 2차원으로 변환하는 과정에서 절단되어 해당 필드 값이 본래 가지고 있던 의미가 변형될 수 있다는 점에 주목했다. 그림 1은 패킷 데이터가 2차원 이미지로 변환하는 과정에서 필드 값이 손실되는 예시를 나타낸다.

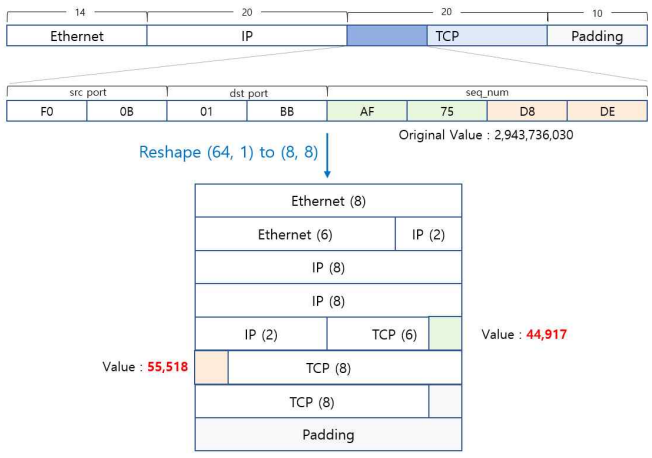


그림 1 패킷 데이터 변환 과정에서 필드 값 의미 손실 예시

본 논문은 2021년도 교육부의 재원으로 한국연구재단의 지원을 받아 수행된 지자체-대학 협력기반 지역혁신 사업의 결과 (2021RIS-004)이고 2021년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구(NRF-2021S1A5C2A03097574)임

그림 1에서는 TCP 헤더의 필드 값의 의미가 손실되는 예시를 나타내었으나 유사하게 TCP 페이로드에서도 연속되는 문자열 중간이 절단되며 본래 의미에 손실이 발생할 수 있다. 또한, 인접한 픽셀값이 주로 유의미한 특징을 가지는 이미지와는 달리 패킷 데이터는 수직적인 관점에서 멀리 떨어진 필드 값과도 유의미한 관계가 있을 수 있다는 점도 고려 대상이다. 본 논문은 입력 데이터인 1차원 패킷 데이터를 다양한 모양의 2차원 데이터로 재구조화하고 이로부터 다양한 특징 맵을 생성하여 응용 트래픽을 분류하는 방법을 제안한다.

본 논문은 1장 서론에 이어 2장에서 관련 연구를 제시하고 3장에서 제안하는 방법을 설명한다. 4장에서는 실험 결과를 설명하고 5장에서 결론 및 향후 연구를 제시하는 것으로 본 논문을 마친다.

Ⅱ. 관련 연구

CNN은 많은 분야에서 사용되고 있는 가장 인기 있는 딥러닝 방법의 하나로 이미지 또는 텍스트 데이터의 지역적 정보 추출에 있어 강점을 가지며 네트워크 트래픽 분류 분야의 많은 연구에 활용되고 있다. [1]은 플로우 내 패킷들의 페이로드를 28*28의 2차원 이미지로 변환하여 CNN 모델에 입력하여 분류 모델을 생성하였다. 또한, 모델 생성에 필요한 하이퍼파라미터를 최적화하는 과정을 통해 10개의 웹 응용을 99.57%의 정확도로 분류하였다. [2]는 패킷을 전체 레이어(ALL)와 TCP 세션의 페이로드인 L7로 구분하여 서브데이터 세트를 생성하고 28x28의 2차원 이미지로 변환하여 분류 모델을 생성하였다. 결과적으로 10개 응용을 평균 99.41%의 정확도로 분류하였다. [3]은 [2]와 마찬가지로 패킷을 ALL과 L7로 구분하여 서브 데이터 세트를 생성하고 이를 784*1 모양으로 변환하고 학습하여 1D CNN 모델을 생성하였으며 28*28 형태의 이미지를 학습하여 2D CNN 모델을 생성하고 두 개 모델의 분류 성능을 비교하였다. 결과적으로 2D CNN 기반 모델의 분류 성능보다 1D CNN 기반 모델이 성능이 좋았으며 저자는 2D CNN의 2차원 공간 특징 학습이 1차원 암호화 트래픽 분류에서 명확하지 않다고 보고했다. [4]는 784*1 모양 데이터를 학습한 1D CNN과 28*28 모양 데이터를 학습한 2D CNN, 784*1 모양 데이터를 학습한 LSTM 모델을 생성하고 각 모델의 분류 성능을 비교하였으며 1D CNN 모델이 가장 좋은 분류 성능을 나타냈다. 또한 저자는 각 모델에서 분류한 결과들을 바탕으로 투표하여 최종 분류 결과를 생성하는 앙상블 방법을 제안했으며 제안한 앙상블 기반 모델의 분류 성능은 1D CNN 기반 분류 모델보다 6% 높은 분류 성능을 보였다. 대다수의 기존 연구들에서 1D CNN기반 분류 모델이 2D CNN 기반 분류 모델보다 트래픽 분류에 적합한 것을 확인할 수 있으나 현재까지도 많은 연구에서 주로 2D CNN 모델이 고려되고 있다. 이는 컴퓨터 비전, 이미지 객체 인식 등의 분야에서 CNN 모델의 발전을 선도하고 있으며 대다수의 첨단 연구가 2D CNN에 기반하고 있기 때문이라고 짐작해볼 수 있다. 컴퓨터 비전 분야의 이미지와 패킷 데이터의 구조 및 특성이 다른 만큼 패킷 데이터에 적합한 입력 모양을 정의하는 것은 필수적이다. 따라서 본 논문에서는 패킷 데이터의 입력 모양이 1차원인지 2차원인지 선택하는 문제를 더 확장하여 패킷 데이터의 어떤 모양이 정확한 분류에 있어 적합한지에 대한 비교실험을 수행하고 다양한 모양에 대응하는 모델의 분류 결과들을 집계하여 학습하는 앙상블 기반 응용 트래픽 분류 모델을 제안한다.

Ⅲ. 실험

A. 데이터 세트

본 실험을 위해 분류 실험을 위하여 50개 종류의 100개 플로우가 포함된 응용 트래픽 데이터 세트를 수집하였으며 수집한 응용의 종류는 표 1에 나타나있다.

표 1. 수집한 응용 리스트

Bithumb	Coineone	Upbit	Excel
Teams	Excel	PPT	Word
Onenote	WEB_Excel	WEB_PPT	WEB_Word
Daum	Gmail	Nate Mail	Navermail
Naver band	kakaotalk	Skype	Agoda
Airbnb	Goodchoice	Hotels.com	Netflix
Yanolja	11st	Coupang	Gmarket
Musinsa	Tmon	Wemakeprice	Facebook
Instagram	Kakaostory	Naverblog	Tistory
Twitter	Disney+	MelonMusic	NaverTV
Tving	Twitch	Wavve	NaverSeries
Youtube Music	Hotels Combined	Kakao webtoon	Naver Webtoon
Kakao page	Youtube		

B. 패킷 데이터 입력 방법

패킷 데이터 입력 방법은 단일 입력과 다중 입력으로 구분할 수 있으며 단일 입력은 분류 모델을 학습할 때 하나의 벡터만이 입력되는 경우를 말한다. 단일 입력은 플로우 내 첫 n bytes를 이어붙여 하나의 벡터로 만드는 것이 일반적이며 헤더 포함 여부를 결정할 수 있다. 우리는 헤더가 포함된 경우(ALL+L7)와 페이로드만 포함된 경우(L7)의 2가지로 나누어 서브 데이터 세트를 생성하였으며 이는 그림 2에 나타나있다.

다중 입력은 분류 모델을 학습할 때 여러 개의 데이터가 입력되는 경우를 말하며 모델은 플로우 내 첫 k개의 패킷 벡터를 동시에 입력받아 학습을 수행한다. [5]에 따르면 14개 이하의 패킷이 입력될 때 가장 좋은 성능

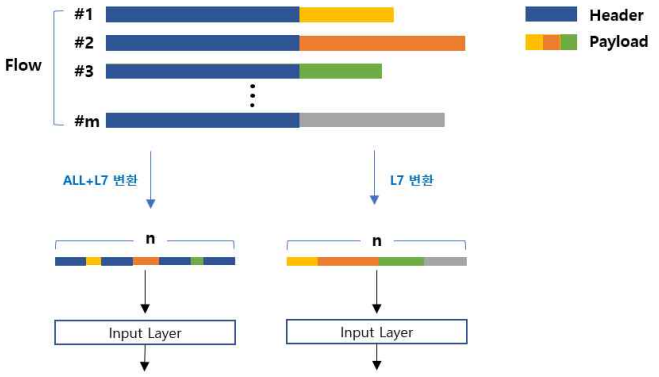


그림 2. 단일 입력 벡터 생성 방법

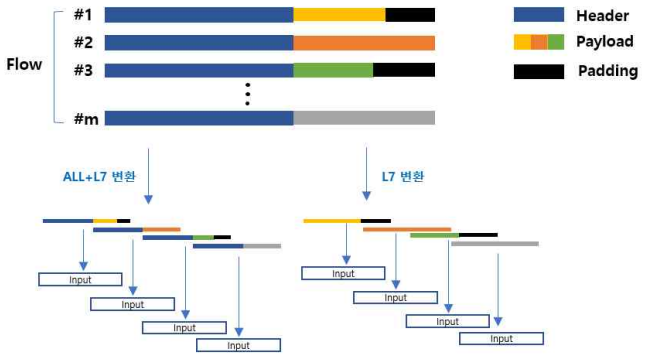


그림 3. 다중 입력 벡터 생성 방법

을 보이며 k에 따른 성능 변화 차이가 크지 않은 것으로 나타났다. 따라서, 우리는 k를 10으로 고정한다. 단일 입력과 마찬가지로 All+L7과 L7의 2가지 경우로 나누어 서브 데이터 세트를 생성하였으며 이는 그림 3에 나타나있다.

B. 입력 벡터 모양

기존 연구에서는 784*1(1D CNN), 28*28(2D CNN)의 2가지 모양이 주로 고려되었으며 이는 392*2, 196*4, 112*7 등의 다른 모양을 가진 입력으로 변환할 수 있다. 이때, 생성할 수 있는 모양의 개수는 입력 벡터의 크기의 약수의 개수와 같으며 784의 경우 15개의 모양을 생성할 수 있지만 마지막 모양은 1*784로서 첫 번째 모양과 동일하게 학습이 수행되므로 마지막 모양은 제외한다.

C. 분류 모델

분류 모델은 LeNet 구조와 유사하게 컨볼루션 레이어 2개와 풀링 레이어 2개로 이루어져 있고 마지막 풀링 레이어 후 2개의 덴스 레이어를 통해 분류 결과를 출력한다. 각 입력 벡터의 모양에 따라 모델의 하이퍼 파라미터를 최적화하기 위하여 Keras Tuner 중 Hyperband를 사용하여 각 모양에 적합한 모델 구조를 결정하였다. 모델 구조를 최적화하는 과정에서는 컨볼루션 레이어와 풀링 레이어의 필터 사이즈와 풀 사이즈만 변경하며 최적화를 수행했으며 고정한 하이퍼 파라미터는 표 2와 같다.

표 2. 모델 최적화 과정에서 고정한 하이퍼 파라미터

고정 하이퍼 파라미터	
컨볼루션 필터 개수	16
덴스 레이어 유닛 수	12

Ⅳ. 실험 결과

본 장에서는 최적의 하이퍼 파라미터가 적용된 분류 모델을 앞서 생성한 서브 데이터 세트에 적용하고 분류 결과를 비교한다.

표3은 L7 데이터 세트의 입력 모형별 최적화된 하이퍼 파라미터를 나타낸다. 주로 추출된 특징 맵을 요약하여 크기를 줄이는데 활용되는 풀링 레이어의 크기가 모두 (1, 1)로 최적화된 것은 패킷의 페이로드 데이터가 2차원 공간 정보가 아닌 1차원 공간 정보를 담고 있는 데이터인 것을 의미한다. 따라서, 2차원 공간 정보 기반 풀링 레이어를 적용하지 않는 것이 적합하다고 판단할 수 있다. 그림 4에서는 L7 데이터 세트의 모형별 분류 모델의 성능을 나타내며 일반적으로 사용했었던 정사각 모형(28*28)은 다른 모형들과 비교하여 높지 않은 것을 확인할 수 있다. 모형 중 패킷의 1차원적 특성을 고려한 392*2, 2*392, 112*7 모형이 가장 높은 성능을 보였다. 표4는 ALL 데이터 세트의 입력 모형별 최적화된 모델 구조를 나타내며 각 모형 별 분류 정확도는 그림 5에 나타나있다. L7 데이터 세트의 결과에서는 정사각 모형(28*28)이 평균적인 정확도를 나타냈으나 ALL 데이터 세트에서는 정사각 모형이 가장 낮은 정확도를 나타냈다. 또한, L7 데이터 세트와는 달리 ALL 데이터 세트에서 제일 높은 정확도를 나타냈던 모형의 경우 풀 사이즈를 (1, 2)를 적용하고 있으며 이는 패킷의 전체 데이터에서는 2차원 공간 정보가 활용되어야 함을 나타낸다. 표 5에서는 데이터 세트와 단일/다중 입력 여부 그리고 단일/다중 모형 여부에 따라 응용 트래픽을 분류한 결과를 나타낸다. L7 데이터 세트와 ALL 데이터 세트를 비교한 결과 ALL 데이터 세트를 적용하는 것이 평균 정확도 측면에서 23% 더 좋은 것을 알 수 있으며 다중입력, 다중모형이 적용된 분류 모델을 사용한 경우에는 27% 정도의 정확도 상승이 있었다. 1D CNN 기

표 3. 입력 모양별 최적화된 모델 구조(L7)

데이터셋	모형	필터 사이즈	풀 사이즈
L7	(784,1)	(43,1)	(1,1)
	(392,2)	(85,1)	(1,1)
	(196,4)	(11,1)	(1,1)
	(112,7)	(13,1)	(1,1)
	(98,8)	(8, 2)	(1,1)
	(56,14)	(7, 3)	(1,1)
	(49,16)	(4, 2)	(1,1)
	(28,28)	(5, 5)	(1,1)
	(16,49)	(2, 4)	(1,1)
	(14,56)	(1, 2)	(1,1)
	(8,98)	(1, 4)	(1,1)
	(7,112)	(1, 5)	(1,1)
	(4,196)	(1, 3)	(1,1)
	(2,392)	(1,43)	(1,1)

표 4. 입력 모양별 최적화된 모델 구조(All)

데이터셋	모양	필터 사이즈	풀 사이즈
ALL	(784,1)	(5, 1)	(1, 1)
	(392,2)	(3, 1)	(1, 1)
	(196,4)	(5, 1)	(1, 1)
	(112,7)	(2, 1)	(1, 1)
	(98,8)	(2, 1)	(1, 1)
	(56,14)	(2, 3)	(1, 2)
	(49,16)	(2, 2)	(1, 2)
	(28,28)	(2, 4)	(2, 1)
	(16,49)	(1, 2)	(1, 2)
	(14,56)	(2, 2)	(1, 2)
	(8,98)	(1, 7)	(1, 1)
	(7,112)	(1, 5)	(1, 1)
	(4,196)	(1, 7)	(1, 1)
	(2,392)	(1, 9)	(1, 1)

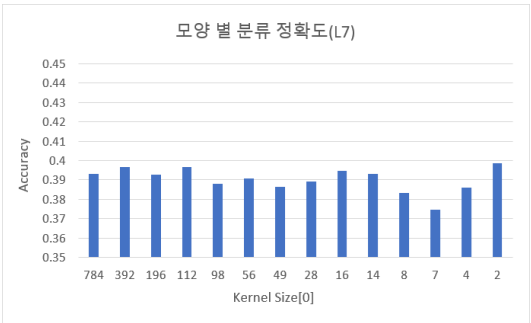


그림 4. 모양별 단일 입력 벡터에 대한 분류 정확도(L7)

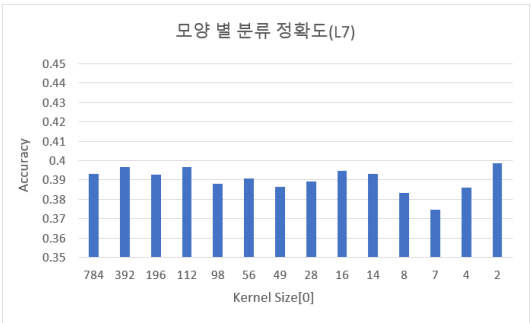


그림 5. 모양별 단일 입력 벡터에 대한 분류 정확도(All)

표 5. 단일/다중 입력, 단일/다중 모형 여부에 따른 분류 정확도

데이터 세트	모델	정확도
L7	단일 입력, 784*1 모형(1D CNN)	0.3933
	단일 입력, 28*28 모형(2D CNN)	0.3893
	단일 입력, 다중(784*1, 28*28) 모형	0.4146
	단일 입력, 다중 모형	0.4160
	다중 입력, 784*1 모형	0.4624
	다중 입력, 28*28 모형	0.4769
	다중 입력, 다중(784*1, 28*28) 모형	0.4792
	다중 입력, 다중 모형	0.4831
ALL	단일 입력, 784*1 모형	0.6047
	단일 입력, 28*28 모형	0.5820
	단일 입력, 다중(784*1, 28*28) 모형	0.6320
	단일 입력, 다중 모형	0.6567
	다중 입력, 784*1 모형	0.7366
	다중 입력, 28*28 모형	0.7158
	다중 입력, 다중(784*1, 28*28) 모형	0.7412
	다중 입력, 다중 모형	0.7526

반 모형(784*1)은 2D CNN 기반 정사각 모형(28*28)보다 모든 경우에서 0.5~2 정확도 상승이 있었으며 [4]에서 제안한 방법과 유사하게 1D CNN 분류 결과와 2D CNN 분류 결과를 앙상블한 분류모데릐 경우 1D CNN 모델보다 평균적으로 2% 정확도 상승이 있었다. 본 논문에서 제안했던 다중 모형별 분류 결과를 앙상블 하는 방법의 경우 L7 데이터 세트에서는 단일 입력일 경우와 다중 입력일 경우 모두 정확도가 소폭 상승했으며 ALL 데이터 세트를 활용한 실험 결과에서는 단일 입력일 때 2.5% 상승했으며 다중 입력일 때는 1.1%가 상승하였고 생성한 모든 분류 모델 중 가장 높은 정확도를 나타냈다.

Ⅳ. 실험 결과

본 논문은 패킷 입력 벡터를 다양한 모형으로 변환하고 각 모형 별 분류 결과를 앙상블하여 응용 트래픽을 분류하는 방법을 제안했다. 우리는 패킷 데이터가 2차원 이미지로 변환되는 과정에서 원래 가지고 있던 1차원 정보가 손실되어 정확히 학습이 되지 않는다는 가정 아래 패킷 데이터를 다양한 모형으로 변환하고 이를 앙상블하는 방법을 적용하여 패킷 데이터 변환 과정에서 발생하는 정보 손실을 최소화하고자 했다. 결과적으로, 제안한 방법은 모든 실험 결과에서 가장 높은 정확도를 나타내었으며 이는 응용 분류 분야뿐만 아니라 공격 탐지 분야에서도 효과적으로 활용할 수 있을것이라고 기대한다. 또한, 우리는 패킷 입력 벡터를 다양한 모형으로 변환하여 개별 분류 모델을 생성하여 분류 결과를 비교하였으며 그 결과 단순히 1차원적 공간정보를 활용하는 입력 벡터 모형(784*1)이나 기존에 주로 활용되었던 정사각 모형(28*28)보다 패킷을 더 잘 표현할 수 있는 모형이 있다는 것을 실험 결과를 통해 증명하였다. 하지만 다양하고 많은 응용 트래픽이 발생하는 환경에서 실용적으로 사용하기에는 정확도가 부족하다는 한계점이 있으며 우리가 변환한 다양한 모형들은 기존 컴퓨터 비전 분야 모델의 정사각 모형과 상이하기 때문에 쉽게 첨단 연구를 적용시키기 어렵다는 점도 큰 한계점으로 작용한다. 따라서 우리는 향후 연구로 기존 CNN 기반의 첨단 분류 모델을 응용 트래픽 분류 분야에 적합하게 변형하여 적용하는 방법에 대해 연구를 수행할 계획이며 본 논문에서 고려하지 않았던 응용 트래픽 플로우 내 패킷들의 시계열 특성을 고려한 분류 모델에 대해서 연구할 계획이다.

참 고 문 헌

[1] L. Xu, X. Zhou, Y. Ren, and Y. Qin, “A Traffic Classification Method Based on Packet Transport Layer Payload by Ensemble Learning,” in 2019 IEEE Symposium on Computers and Communications (ISCC), Jun. 2019, pp. 1–6. doi: 10.1109/ISCC47284.2019.8969702.

[2] S.-H. Ji, U.-J. Baek, M.-G. Shin, B.-M. Chae, H.-W. Moon, and M.-S. Kim, “Design of Web Application Traffic Classification Model Based on Convolution Neural Network,” kics, vol. 44, no. 6, pp. 1113–1120, Jun. 2019, doi: 10.7840/kics.2019.44.6.1113.

[3] W. Wang, M. Zhu, J. Wang, X. Zeng, and Z. Yang, “End-to-end encrypted traffic classification with one-dimensional convolution neural networks,” in 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), Jul. 2017, pp. 43–48. doi: 10.1109/ISI.2017.8004872.

[4] W. Wang et al., “HAST-IDS: Learning Hierarchical Spatial-Temporal Features Using Deep Neural Networks to Improve Intrusion Detection,” IEEE Access, vol. 6, pp. 1792–1806, 2018, doi: 10.1109/ACCESS.2017.2780250.

[5] W. Wang, M. Zhu, X. Zeng, X. Ye, and Y. Sheng, “Malware traffic classification using convolutional neural network for representation learning,” in 2017 International Conference on Information Networking (ICOIN), Jan. 2017, pp. 712–717. doi: 10.1109/ICOIN.2017.7899588.

DDoS 탐지를 위한 LSTM 기반 Entropy Threshold 예측 기법

이지원, 김경백
전남대학교
maum-@hanmail.net, kyungbaekkim@jnu.ac.kr

LSTM-based Entropy Threshold Prediction for DDoS Detection

Jiwon Lee, Kyungbaek Kim
Chonnam National University.

요 약

현재 IoT 장비나 많은 데이터 수요로 인해 거대해진 네트워크를 관리, 제어하기 위해 네트워크 환경이 SDN으로 바뀌고 있다. SDN 환경에서 얻을 수 있는 데이터를 이용해 악성 트래픽을 탐지하기 용이하며, 모델 중에 증가하는 트래픽에 대하여 엔트로피 기반의 탐지 시스템이 주목받고 있다. 하지만 IoT 장비들의 대중화로 사람들의 네트워크 활용성이 높아지고, 공격자는 이러한 IoT 장비를 감염시켜 미라이 봇넷으로 만들어 공격 자원으로 활용하여 다양한 DDoS 공격이 가능해졌다. 이러한 네트워크 환경에 효율적인 Entropy 기반 DDoS 탐지 방법이 대체할 수 있지만, 이러한 Entropy 기반 모델은 Threshold 값을 임의로 설정해야 하며, 모든 네트워크 환경에 적절치 않다. 우리는 Threshold 값을 기계학습을 하여 엔트로피에 대한 적절한 Threshold을 출력하는지 실험하였다.

Ⅰ. 서 론

네트워크 시장 거대화에 따라 네트워크 환경이 SDN으로 바뀌고 있다. SDN은 중앙제어를 이용해 범위 내의 트래픽을 sFlow, NetFlow 등의 방식으로 샘플링이 가능하다. 이를 활용한 기계학습 모델은 좋은 성능의 정확도를 보여주나, 애플리케이션 계층의 DoS 공격이나 Low-Rate DDoS 등 다양한 공격은 탐지하기 힘들며, 해당 공격에 성능이 좋은 시그니처 기반 탐지는 해당 SDN 자원을 더욱 소비하게 된다. 이에 자원 소모에 비해 효율이 좋은 엔트로피 기반 모델이 주목받고 있다. 불확실성에 대한 수치를 사용하는 엔트로피 기반의 탐지 모델은 네트워크 트래픽 탐지에 과거부터 많이 사용되었다. 특정 시간에 대한 Entropy 수치를 뽑고, 정상 범위에 대한 Threshold 값을 설정하여 초과할 경우 해당 시간 내의 DDoS 패킷이 포함된 것으로 판단하는 방법이 대표적이며, 좋은 효율을 위해서는 유동적으로 변화는 트래픽에 대응하여 적절한 Threshold 값과 알고리즘을 결합하는 것이 좋다. 우리는 SDN 같은 거대 네트워크 환경에는 시간별 IP, Port 등의 Entropy가 사용자들의 패턴에 맞춰 시계열 특징을 이용해, 적절한 Threshold 값을 학습하는 LSTM 모델을 만들어 실험했다.

Ⅱ. 관련연구

2.1 Entropy 정의

$$H(X) = -\sum p_x \log p_x \quad (1)$$

Entropy는 무질서함에 대한 수치를 나타낸 것으로, 수식은 아래와 같다. 해당 수식은 예상치 못한 상황에 대한 점수를 높게 평가하여 값을 산출하기에, 새로운 정보에 대한 상황이 들어오면 값이 커지지만, 일정한 정보에 대한 값이 나오면, Entropy 값이 작아지는 특징이 있다. 이러한 특징을 이용하여 정상 패킷의 일정 영역에 대하여 window size로 자르고 그 영역의 Entropy 값을 계산하면 일정한 무질서함의 수치를 기준으로 유지하게 되지만, 반대로 DDoS 공격이 들어오면 무질서함의 수치가 이전과 급격히 바뀌어 DDoS를 탐지할 수 있게 된다.

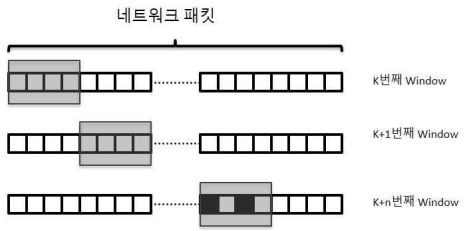


그림 2. window size 만큼 Entropy 측정

2.2 관련 연구

Rui Wang[1]은 SDN 기반에서 작동하는 FLOW 기반 ENTROPY 기반 DDoS 탐지 메커니즘이다. OpenFLow 기반 SDN에서는 스위치에 흐름 테이블이 있으며 이를 이용하여 Entropy를 계산하고 탐지하는 방법을 사용하였다. 하지만 적절한 Threshold를 찾기 위한 데이터 비교 분석으로 끝났다. 노기섭[2]은 Fast Entropy를 활용해 동적 임계치를 내놓는 알고리즘 기반 method를 제안했다. 이 Method를 활용하여 패킷에 대한 DDoS 공격 도입 부분을 탐지하는 연구를 진행하였다. L. D. Tsobdjou [3]는 Entropy 에 대해서 동적 임계치로 이진 분류하는 연구를 진행했다. 역방향과 순방향에 대한 Entropy 값을 따로 계산하는 method로, ICMP, SYN Flooding 공격에 대한 실험을 진행하지만 공격으로 인해 Entropy 수치가 낮아졌을 경우에만 작동하는 method로 인해, 공격하는 IP 대역이 많아졌을 때 탐색하기가 어려워지는 특징을 가지고 있다. 각각 엔트로피 기반을 피쳐로 다양한 Entropy를 사용한 알고리즘 연구가 많지만, 수시로 바뀌는 네트워크 환경에서 적절한 Threshold 값 찾는 것은 힘들다. 이에 우리는 사용자들의 데이터 사용 패턴에 대한 시계열 특징이 있을 것을 가정하여, LSTM 모델로 다음 Entropy 예측하고, 예측된 Entropy 수치에 $\pm\alpha$ 하여 Threshold를 생성하여, DDoS 탐지가 가능한지 실험하였다.

Ⅲ. LSTM 기반 Entropy Threshold 모델

3.1 제안하는 Method 및 전처리 방법

우리는 CIC-IDS 2017[4]의 데이터셋을 사용하여 실험을 진행했다. 패킷에 대한 Source Port, Destination Port와 Protocol 값을 묶은 Port_Flow와 Source IP, Destination IP를 묶은 IP_Flow를 추출하였다. Window size 단위로 Entropy 값을 추출한 후, Sequence Length 길이만큼 Entropy의 이전 n번째 정보까지 shfit한다. 이후 LSTM 모델은 다음 Entropy 수치를 계산한다. 이때 LSTM 모델은 1개의 LSTM 레이어와 3개의 Dense로 구성되며 다음 Entropy 값을 구한다. 그리고 Threshold에 대한 범위는 예측한 Entropy 값 E_{i+1}^{pre} 와 입력값들에 Mean, Min, Max 값을 사용하여 계산한다. 다음 Min, Max의 차이 값인 Difference를 Mean 값에 더하고 빼서 Entropy Threshold Top 값과 Threshold Bottom 값을 생성하였다.

$$
\begin{aligned}
&E_{i-n},\ldots,E_i,E_{i+1}^{pre} \in TW_i \\
&E_i^{mean} = \frac{1}{n+1}\left(\sum_{i=1}^{n} E_i + E_{i+1}^{pre}\right) \\
&d = TW_i^{\max} - TW_i^{\min} \\
&\theta_i^T = E_i^{mean} + d \\
&\theta_i^B = E_i^{mean} - d
\end{aligned}
\tag{2}
$$

3.2 실험 방법 및 평가

우리는 CIC-IDS 2017의 데이터 세트를 이용하여 실험을 진행하였다. 해당 데이터 세트에서는 공격이 없는 평시 데이터만 존재하는 월요일의 데이터와 DDoS 공격이 존재하는 금요일 오후의 데이터를 사용하였으며, 해당 공격에 방화벽 설정을 ON/OFF를 반복하여 만든 데이터셋이다. 정상 데이터인 월요일 데이터 세트를 학습하게 하고, 학습한 모델로 월요일 데이터와 금요일 오후 DDoS 데이터를 테스트하였다. 정상 데이터에 대한 시험 결과 그림3과 같이 처음 부분에는 수치가 불안전하지만, 버스트가 큰 영역이 아니면 대체로 예측한 Threshold 값에 들어왔다. Port Flow 또한 그림 3의 IP Flow 수치와 유사하게 측정되었다.

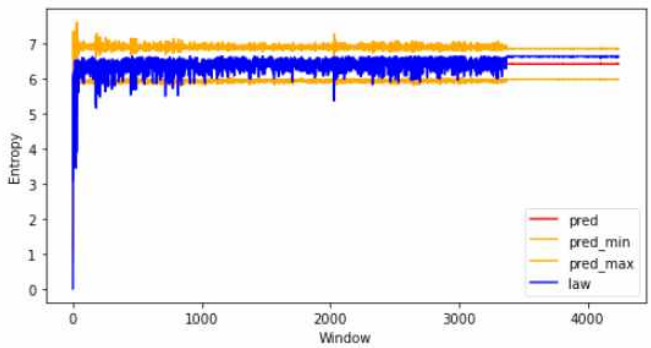


그림 3. 정상데이터의 IP Flow Threshold 예측값

그리고 이후에 DDoS 공격이 포함된 데이터 세트를 시험한 결과 그림 4와 같다. 공격은 윈도우 220부터 시작했다. 그림 4에서 보듯이 DDoS 가 지속 될 경우에 Threshold 값이 적절하게 유지가 힘들었지만, 공격하면서 버스트지점이 생길 때마다 Threshold 값을 넘으면서 공격 도입 부분을 관측 가능하였다. 또 한 Port에 대한 Entropy 값도 예측한 Threshold를 넘어가면서, 이와 유사한 패턴을 확인할 수 있었다.

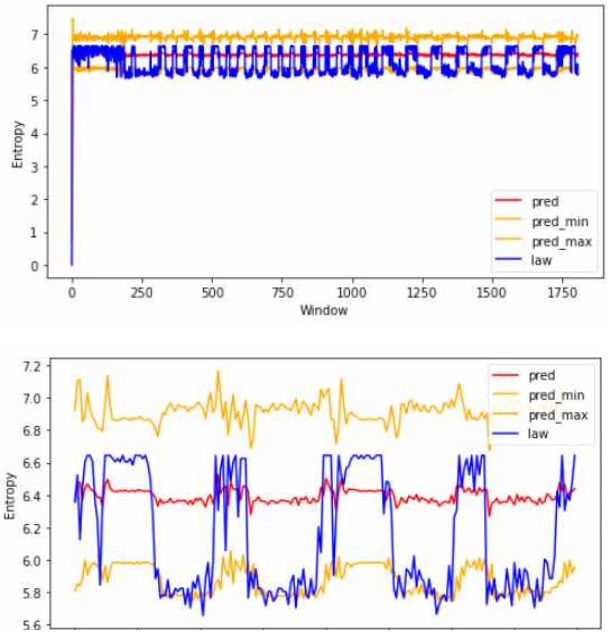


그림 4. 공격 데이터의 IP_Flow Threshold 예측값 400~600 지점 확대

Ⅳ. 결론

본 논문에서는 다음과 같이 Threshold 값에 대한 기계학습을 진행했으며, 공격이 아닌 평시 상황에서도 버스트가 높은 부분에서는 Threshold 값을 넘을 때도 있지만, 네트워크 상황에 적절한 Threshold 값을 뽑았다. 이번 실험에서는 사용한 데이터셋에는 시계열 특징이 없었기에, 공격 데이터의 Entropy 값과 예측한 Threshold를 비교하는 실험을 진행하였으나, 다음 실험에는 사용자들의 데이터 사용 패턴으로 인한 시계열 기반의 특징을 가지는 시나리오를 적용해서, 다양한 환경에서도 Entropy 수치로 DDoS 탐지가 가능한지 이진 분류 모델을 만들어서 모델을 평가하고자 하며, 또한 DDoS 공격이 지속될 경우에 Entropy 값이 DDoS 값과 적응하여 잘못된 Threshold를 계산할 것을 대비해, Exponential Smoothing을 사용해 보완하여 연구를 진행할 예정이다.

ACKNOWLEDGMENT

"이 논문은 2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임"(IITP-2019-0-01343)

참 고 문 헌

[1] R. Wang, Z. Jia and L. Ju, "An Entropy-Based Distributed DDoS Detection Mechanism in Software-Defined Networking," 2015 IEEE Trustcom/BigDataSE/ISPA, 2015, pp. 310-317, doi: 10.1109/Trustcom.2015.389.

[2]K. Kalkan, L. Altay, G. Gür and F. Alagöz, "JESS: Joint Entropy-Based DDoS Defense Scheme in SDN," in IEEE Journal on Selected Areas in Communications, vol. 36, no. 10, pp. 2358-2372, Oct. 2018, doi: 10.1109/JSAC.2018.2869997.

[3]G. No and I. Ra, "Adaptive DDoS Detector Design Using Fast Entropy Computation Method," 2011 Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 2011, pp. 86-93, doi:

[4] Iman Sharafaldin, Arash Habibi Lashkari, and Ali A. Ghorbani"Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization", 4th International Conference on Information Systems Security and Privacy (ICISSP), Portugal, January 2018

OpenStack 기반 멀티 사이트 클라우드의 VXLAN 터널링. 통신 및 데이터 공유를 위한 보안 메커니즘

미르 무함마드 술래만 사르워♦, 디아즈 리베라 하비에르 호세, 아팍 모하마드, 송왕철°
mirsuleman1@gmail.com, shaifvier@gmail.com, afaq24@gmail.com, philo@jejunu.ac.kr

VXLAN Tunneling in OpenStack based Multi-site Cloud a secure mechanism for Communication and Data Sharing

Mir Muhammad Suleman Sarwar, Javier Jose Diaz Rivera, Afaq Muhammad,
Wang-Cheol Song
Department of Computer Engineering, Jeju National University

Abstract

Cloud storage needs to meet several important requirements to maintain tenants data such as data sharing for high availiability, reliability and consistency of data. Cloud tenants need to communicate and share data on an isolated channel to reduce interference and enhance data security. VXLAN provides encapsulated data over an isolated and secure channel. VXLAN allows the creation of a large number of isolated networks, each identified by a unique id. This study presents a secure and isolated communication mechanism between instances of different compute machines in an OpenStack-based cloud using VXLAN tunneling. For this purpose an OpenStack based multi-site cloud is deployed with a control node and two compute nodes. OpenStack network is imlpemented to provide inter connectivity to instances as well as external connectivity. Instances are launched on different compute nodes. Communication between instances is then realized by leveraging advantages of VXLAN.

Ⅰ. Introduction

Previously, VLANs had 12 bits of VLAN ID, allowing a maximum of 4094 isolated networks. VXLAN [7] increases scalability in virtualized cloud environments as the VXLAN ID is 24 bits, enabling you to create up to 16 million isolated networks. VXLAN allows you to use the Layer 3 features of the underlying network. The VXLAN overlay network is abstracted from the underlying physical network infrastructure. The VXLAN overlay network is not visible to the physical network and removes the need for additional physical infrastructure. For example, with an increase in the number of VMs behind the server's physical ports, the forwarding table of the physical switch does not grow. In addition, this reduces the scope of MAC address duplication to VMs that exist in the same VXLAN segment. The MAC address can overlap when the addresses are not a part of the same VXLAN segment. In a VXLAN, only the MAC address of the data link belonging to the same VXLAN segment or VNI must be unique. The VXLAN is similar to a VLAN, where the VLAN ID and the MAC address must have a unique combination. This study shows a secure mechanism for data sharing through VXLAN tunneling among instances on multiple sites of a Cloud.

This manuscript is organized as follows. Section II describes the related work and motivation, Section III details architecture and deployment of system. This section also illustrtaes traffic passing through VXLAN tunnel. Section IV concludes the manuscript.

Ⅱ. Motivation and Related Work

To take advantage of virtualization technology [1], Data Centers (DC) have shifted towards the cloud [2][3]. Cloud provides data Storage as a Service (SaaS) [2][3]. Cloud contains Control and Compute nodes. The control node controls the networking, and compute node stores the data in the cloud [4]. Compute nodes can be in geographically diverse locations in the cloud, leveraging virtualization's true essence. Data stored on compute nodes sometimes needs to be shared for various reasons, such as the nearest access location to reduce bandwidth utilization, security, load balancing, etc. There are multiple types of data sharing in clouds, such as direct access or copying

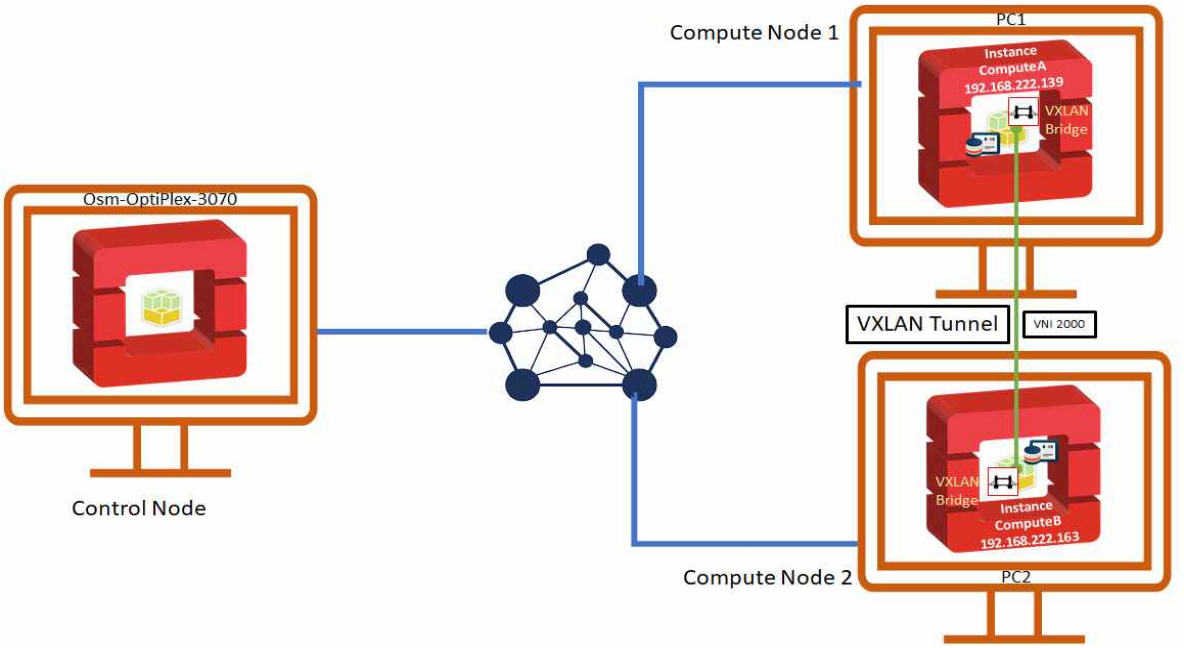


Figure 1 : VXLAN tunneling in OpenStack based multi-site cloud

Table 1 : System Details of each node in cloud

SNo.	Name of Host Machine	Type	Instance	Image	IP of Instance
1	Osm-OptiPlex-3070	Control	NA	NA	NA
2	PC1	Compute	ComputeA	Xenial-ubuntu	192.168.222.139
3	PC2	Compute	ComputeB	Xenial-ubuntu	192.168.222.163

data, also known as data replication. Data replication can be between instances of the same compute, or different computes [5]. A study comprehensively presented data replication patterns in cloud [6].

III. System Architecture

The implemented system contains a MicroStack [8] based deployment of OpenStack [4]. MicroStack is installed on three computers with linux operating system. These host machines are connected to the same network so that they can access each other. One of the MicroStack deployments is initialized as the control node, and the other two as compute nodes. Instances are launched on the Compute nodes, as shown in figure 1, using a xenial ubuntu image. Table 1 shows details of physical hosts and instances.

Once the cloud is deployed and all compute nodes are successfully integrated with the control node the next step is to configure images for instances. The default image Cirros is merely a test image to check creation of instances, and cannot install anything Due to this reason, we need images in which we can install packages such as Open vSwitch (OVS) [9] for our deployment. A xenial-ubuntu image is used to launch instances.

OVS is an OpenFlow-based virtual switch. OVS of instances "computeA" and "computeB" are used to create a point-to-point VXLAN tunnel. OpenStack uses UDP port 4789 by default for VXLAN. Therefore, the UDP port should be added as a rule in the security group.

An OVS bridge is required on both instances for VXLAN tunneling. At each bridge, two ports are created, an internal interface and a VXLAN interface. The remote IP for the VXLAN interface is set to the internal IP of the other instance with VNI equal to 2000. The internal interface serves as access to the overlay network. An IP to the internal interface is added, and MTU is set to 1450 for VXLAN overhead. To test that VXLAN tunnel has been successfully created the internal interface of an instance is pinged from the other instance.

Figure 2 shows traffic passing through VXLAN tunnel with VNI equal to 2000, when instance "ComputeB" pings instance "ComputeA". Using the tcpdump command on interface of instance "ComputeA" we can see that traffic is flowing from instance "ComputeB" that has an IP equal to "192.168.222.163" to instance "ComputeA" that has an IP equal to "192.168.222." Figure 3 shows traffic passing through VXLAN tunnel with VNI equal to 2000, when



Figure 2 : Traffic passing through VXLAN from instance "ComputeA" to "ComputeB"

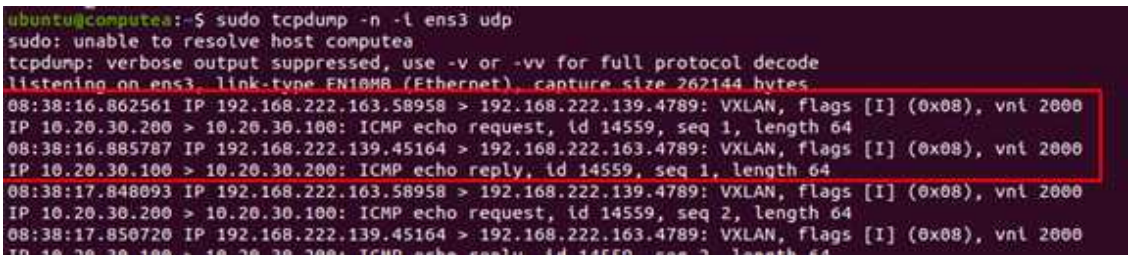


Figure 3 : Traffic passing through VXLAN from instance "ComputeB" to "ComputeA"

instance "ComputeA" pings instance "ComputeB". Using the tcpdump command on interface of instance "ComputeB" we can see that traffic is flowing from instance "ComputeA" that has an IP equal to "192.168.222.133" to instance "ComputeB" that has an IP equal to "192.168.222.163"

IV. Conclusion

Instances on multiple sites can now communicate over a secure and isolated channel through VXLAN with a unique VNI. This VXLAN is dedicated for the two instances to communicate. If other instances want to communicate using their own isolated channel, a VXLAN tunnel with distinct VNI needs to be created. Our future work includes three scenarios. First of all, host-to-host VXLAN tunneling allows all instances to use a single underlying VXLAN tunnel. This scenario will require adding tap ports of instances to the bridges. In the second scenario, a VXLAN tunnel can be created to deploy a compute node where the control node does not have direct access. VXLAN tunnel can be used to extend the access of network. Finally, the VXLAN tunnel can also be used for communication between instances of different OpenStack-based Clouds.

ACKNOWLEDGMENT

This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2022-2017- 0-01683) supervised by the IITP (Institute for Information & communications Technology Planning & Evaluation). This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2016R1D1A1B01016322).

REFERENCES

[1] Chayapathi, Rajendra, Syed F. Hassan, and Paresh Shah. "Network Functions Virtualization (NFV) with a Touch of SDN" ePub_1.Addison-Wesley Professional, 2016.

[2] Mell, P. and T. Grance, "The NIST Definition of Cloud Computing", Special Publication 800- 145, September, 2011.

[3] Tangari, Wang, L., Ranjan, R., Chen, J., Benatallah,B.(eds.):"CloudComputing: Methodology, Systems and Applications." CRC Press, BocaRaton (2017).

[4] https://www.openstack.org. Accessed on 02-02-2022.

[5] https://acloudguru.com/blog/business/sharing-data -in-the-cloud-four-patterns-everyone-should-know Accessed on 02-02-2022.

[6] Gopinath, Suji, and Elizabeth Sherly. "A comprehensive survey on datar eplication techniques in cloudstoragesystems."Int.J.Appl.Eng.Res13,no.22(2018) :15926-15932.

[7] https://docs.oracle.com/cd/E36784_01/html/E36813/gnngz.html Accessed on 22-02-2022.

[8] https://microstack.run/ Accessed on 22-02-2022.

[9] https://www.openvswitch.org/Accessed on 22-02-2022.

TS4:
블록체인 1 : NFT와 블록체인 응용

블록체인 기반 대체 불가능 토큰의 메타데이터 연구

고경찬[O*], 유상우[**], 홍원기[*]

[*]포항공과대학교 컴퓨터공학과

[**]포항공과대학교 인공지능대학원

{kkc90, rswoo, jwkhong}@postech.ac.kr

A Study on Metadata used in Blockchain-based Non-Fungible Token

Kyungchan Ko[O*], Sangwoo Ryu[**], James Won-Ki Hong[*]

[*]Department of Computer Science and Engineering, POSTECH

[**]Graduate School of Artificial Intelligence, POSTECH

요 약

자산의 소유권을 주장하기 위한 방법으로서 블록체인 기반의 대체 불가능 토큰(NFT)이 활발히 활용되고 있다. NFT 의 인기는 날이 갈수록 커져가고 있고, 이에 따라 NFT 를 거래할 수 있는 마켓플레이스가 많이 생겨나고 있다. 앞으로 건전한 NFT 생태계를 만들기 위해서 NFT 에 대한 이해도가 필수적이기 때문에, 본 연구에서는 NFT 의 구현을 위한 표준들과 NFT 발행을 위한 절차에 대해서 조사한다. 이뿐만 아니라 NFT 플랫폼들에서 지원하는 NFT 메타데이터에 대해서 조사를 하고, 각 플랫폼들 마다 다른 메타데이터들을 분석한다.

I. 서 론

대체불가토큰(NFT: Non-Fungible Token) [1]은 블록체인 기술을 기반으로 실물 및 디지털 자산의 소유주를 증명할 수 있도록 하는 크립토 토큰이다. NFT 를 활용하면 원작자들이 영상, 이미지, 예술품 등의 디지털 자산들에 대한 소유권을 쉽게 증명할 수 있다. 이같은 이유로 NFT 는 디지털 소유권에 기반한 다양한 분야로 확장가능하고, 현재는 엔터테인먼트, 부동산(실제/가상), 게임, 스포츠, 미디어 컨텐츠(영화, 음악, 영상 등), 예술품(미술품, 디지털 아트 등) [2] 등 다양한 곳에서 활용되고 있다.

NFT 의 역사를 살펴보자면, 세계 최초의 NFT [3] 는 2014 년 디지털 아티스트 케빈 맥코이가 만든 '퀀텀'이다. 퀀텀을 통하여 처음으로 트랜잭션에 디지털 아트의 실제 파일이 저장된 URL 을 첨가하여 블록체인에 영원히 기록하는 방식이 사용되었으며, 해당 트랜잭션은 네임코인(NameCoin) 블록체인의 174,923 째 블록 [4]에 기록되어 있다. 이후로 스마트 컨트랙트(Smart contract) [5] 기능이 탑재된 블록체인 플랫폼인 이더리움(Ethereum) [6]이 출시되고 나서, 수많은 NFT 기반의 탈중앙화 어플리케이션(DApp: Decentralized Application) 혹은 프로젝트들이 생겨났다. 대표적으로, 디지털 수집품 NFT 프로젝트인 크립토펑크(Cryptopunks) [7], 고양이 육성 게임 DApp 크립토키티(CryptoKitties) [8], 가상 현실 세계 속 토지 소유를 NFT 를 활용해서 구현한 디센트럴랜드(Decentraland) [9]와 NFT 기반 P2E(Pay-to-Earn) 게임으로 유명세를 얻은 엑시인피티니(Axie Infinity) [10] 등이 있다.

위와 같이 NFT 의 활용 사례가 많아지고 수많은 NFT 기반 DApp 들이 출현함에 따라서, 이를 편리하게 관리하고 쉽게 매매할 수 있도록 NFT 관련 표준이 필요하게 되었다. 따라서, 이더리움에서 처음으로 ERC-721 [11]을 통해서 스마트 컨트랙트에서 NFT 를 구현하기 위한 인터페이스들을 정의한 표준을 제안했다.

NFT 가 다양한 분야에서 활용되면서 시장 규모가 커지기 시작했고, 이에 따라 NFT 를 거래할 수 있는 플랫폼들이 등장했다. 대표적으로, OpenSea [12], SuperRare [13], Rarible [14], Nifty Gateway [15] 등의 NFT 마켓플레이스(Marketplace) 플랫폼들이 있으며, NFT 를 발행, 판매, 구매할 수 있는 서비스를 제공한다. 현재는 NFT 에 대한 인기가 많아지면서 NFT 거래관련 사기 [16]와 가짜/표절 NFT [17]도 많이 생겨나고 있는 실정이다. 사용자들은 NFT

마켓플레이스를 통해서 NFT 를 거래하기 때문에 이를 조심할 필요가 있다. 더 건강한 NFT 생태계를 만들기 위해서는 사용자들이 NFT 의 실체가 무엇이고 어떤 데이터들로 이루어졌는지 이해하는 것이 중요하다.

NFT 는 기술적으로 실물/디지털 자산에 대한 정보를 블록체인에 저장하여, 블록체인의 불가변성을 기반으로 해당 자산의 소유권을 주장 가능하도록 만든 것이다. 본 연구에서는 NFT 는 어떤 구조로 이루어져 있는지 분석해보고, 개선할 것이 있는지 파악한다.

II. Non-Fungible Token 조사

현재 가장 널리 사용되고 있는 NFT 표준은 이더리움에서 EIP 로 제안되어서 표준으로 채택된 ERC-721 [12]과 ERC-1155 [18]가 있다. 이더리움에서 제안했던 내용이지만 다른 블록체인 플랫폼도 대부분 해당 표준들을 따르고 있다. 예를 들어서 클레이튼(Klaytn) [19]은 KIP-17 [20]에서 NFT 표준을 정의하고 있는데 이는 ERC-721 과 동일한 내용이다.

NFT 들은 각자 고유하고 대체 불가능하며 1:1 교환이 안되는 특징이 있어서, ERC-20 [21]으로는 NFT 들을 관리하기 것이 불가능했다. 이러한 이유로 NFT 를 위해서 새롭게 ERC-721 이 제안되었다. ERC-721 은 NFT 에 대한 표준 인터페이스를 정의하며, 스마트 컨트랙트에서 NFT 를 다루기 위한 API 들을 표준에 맞춰서 구현할 수 있도록 허용한다. 해당 표준은 개인이 NFT 를 소유하거나 거래할 수 있는 기능뿐만 아니라, 제 3 자(Third party)의 중개인/경매인/지갑에 NFT 를 전송할 수 있도록 위탁하는 기능들도 포함한다.

Method	Description
function **balanceOf**(address _owner) external view returns (uint256);	주소(소유자)에 할당된 NFT 의 개수 반환
function **ownerOf**(uint256 _tokenId) external view returns (address);	특정 NFT(_tokenId)의 소유자 주소를 반환
function **safeTransferFrom**(address _from, address _to, uint256 _tokenId) external payable;	_from 의 주소에서 _to 주소로 NFT 의 소유권을 이전 (_to 주소가 ERC-721 토큰을 받을 수 있는지 검사하고 전달 수행)
function **transferFrom**(address _from, address _to, uint256 _tokenId) external payable;	_from 의 주소에서 _to 주소로 NFT 의 소유권을 이전
function **approve**(address _approved, uint256 _tokenId) external payable;	_approved 주소에 NFT 전송 권한을 부여
function **setApprovalForAll**(address _operator, bool _approved) external;	NFT 소유자가 _operator 주소에 모든 NFT token 들에 대한 전송 권한을 부여/해제
function **getApproved**(uint256 _tokenId) external view returns (address);	_tokenId 에 해당하는 토큰의 전송 권한을 가지고 있는 주소들 반환
function **isApprovedForAll**(address _owner, address _operator) external view returns (bool);	ApprovalForAll 권한이 있는지 여부를 확인

표 1. ERC-721 표준 인터페이스 - Methods

표 1 에 포함된 인터페이스를 모두 포함시켜서 NFT 스마트 컨트랙트를 구현해야 한다. 위 함수들은 필수적으로 구현되어야 하고, Mint, SetTokenURL 등의 Method 를 추가적으로 구현할 수 있다. Mint 는 NFT 를 발행해주는 기능이고, SetTokenURL 은 NFT 의 메타데이터(Metadata)가 저장된 URL 을 설정해주는 기능을 한다. OpenZeppelin [22]에서는 이런 추가적인 기능들이 구현된 Burnable, Pausable, URIStorage, Metadata 등의 확장(Extension) 스마트 컨트랙트들을 제공한다.

ERC-1155 는 ERC-721 의 비효율적인 전송문제 때문에 제안된 Multi Token 에 대한 표준이다.

Method	Description
function **safeTransferFrom**(address _from, address _to, uint256 _id, uint256 _value, bytes calldata _data) external;	_from 주소에서 _value 개수 만큼의 _id 의 NFT 를 _to 주소로 전송
function **safeBatchTransferFrom**(address _from, address _to, uint256[] calldata _ids, uint256[] calldata _values, bytes calldata _data) external;	_from 주소에서 _value 개수 만큼의 _id 의 NFT 를 _to 주소로 전송 (_value 와 _id 배열의 인덱스를 매핑하여 safeTransferFrom 수행)

function **balanceOf**(address _owner, uint256 _id) external view returns (uint256);	_owner 주소가 소유하고 있는 _id 의 NFT 개수를 반환
function **balanceOfBatch**(address[] calldata _owners, uint256[] calldata _ids) external view returns (uint256[] memory);	_owner 와 _id 배열의 인덱스를 매핑하여 balanceOf 수행
function **setApprovalForAll**(address _operator, bool _approved) external;	NFT 소유자가 _operator 주소에 모든 NFT token 들에 대한 전송 권한을 부여/해제
function **isApprovedForAll**(address _owner, address _operator) external view returns (bool);	_owener 가 ApprovalForAll 권한이 있는지 여부를 확인

표 2. ERC-1155 표준 인터페이스 – Methods

NFT 스마트 컨트랙트는 위 두개의 표준을 이용해서 구현할 수 있고, Cryptopunks 와 같은 디지털 이미지를 발행한다고 가정했을 때 NFT 생성 절차는 다음과 같다.

(1) NFT 로 발행할 이미지들 생성(~.jpg)
(2) 생성한 이미지 IPFS [23] 혹은 중앙화 서버에 저장
(3) 각 이미지에 대한 메타데이터(Metadata) 생성(~.json)
(4) 생성한 메타데이터 파일을 IPFS 혹은 중앙화 서버에 저장
  - (2)의 이미지가 저장된 URL 을 메타데이터 파일에서 참조할 수 있도록 추가함
(5) NFT 에 대한 스마트 컨트랙트 작성(ERC-721, ERC-1155)
  - 메타데이터를 나타내는 파일이 저장된 URL 을 블록체인에 기록함
(6) 구현한 스마트 컨트랙트 생성 트랜잭션을 만들어서 블록체인 네트워크에 배치
(7) NFT 를 발행하기 위해서 스마트 컨트랙트의 함수를 호출하는 Minting 트랜잭션을 블록체인 네트워크로 브로드캐스팅
(8) Etherscan [24]혹은 트랜잭션 생성에 사용된 지갑을 통해서 발행한 NFT 들을 확인

III. NFT 메타데이터(Metadata) 분석

NFT 를 생성하기 위해서는 이전 섹션에 설명한 내용과 유사한 절차를 거치게 된다. 그렇다면 실제로 NFT 에 대해서 블록체인에 저장되는 데이터는 무엇일까? NFT 생성 절차를 보면 NFT 를 표현하기 위한 실제 파일과 해당 파일을 설명하는 메타데이터를 생성하는 것을 확인할 수 있다. 따라서, NFT 의 실제 대상을 연결하는 참조가 메타데이터에 포함되어 있고, 해당 메타데이터를 참조하는 URL 이 NFT 스마트 컨트랙트에 포함되어 블록체인에 기록되는 구조를 가지고 있다. 그렇다면 NFT 를 설명하는 메타데이터에 대한 표준이 정해져 있을까? 현재 NFT 메타데이터에 대한 표준 엄격하지는 않고, 자유롭게 정할 수 있지만 Optional 하게 가이드라인을 주는 정도이다. 표준으로 정해진 것이 없기 때문에 NFT 관련 서비스를 제공하는 플랫폼 마다 다르다. 아래 표 3, 4, 5 에서 유명한 NFT 플랫폼들의 메타데이터 가이드 라인을 소개한다.

Field	Description
image	Image 가 저장된 중앙화 서버의 URL 혹은 IPFS URL
image_data	SVG image 데이터
external_url	사용자들이 OpenSea. 플랫폼 말고, 외부에서 접근할 수 있는 URL
description	해당 NFT 에 대한 설명(Markdown 지원)
name	NFT 의 이름
attributes	NFT 이 특징을 설명하는 필드로서, NFT 의 디테일과 희귀도 등을 내포함
background_color	OpenSea NFT 페이지에서 보여질 해당 NFT 의 배경색
animation_url	멀티미디어 첨부파일이 저장된 URL. 영상에 대해서 GLTF, GLB, WEBM, MP4, M4V, OVG, OGG 등의 확장자가 지원되며 음성을 위해서 MP3, WAV, OGA 가 지원됨 (HTML 페이지도 지원됨)
youtube_url	Youtube Video URL

표 3. OpenSea 에서 지원하는 메타데이터 구조[25]

Field	Description
image	Image 가 저장된 중앙화 서버의 URL 혹은 IPFS URL
external_url	사용자들이 Nftify 플랫폼 말고, 외부에서 접근할 수

	있는 URL
description	해당 NFT에 대한 설명(Markdown 지원)
name	NFT의 이름
attributes	NFT이 특징을 설명하는 필드로서, NFT의 디테일과 희귀도 등을 내포함
animation_url	멀티미디어 첨부파일이 저장된 URL. 영상에 대해서, GLB, WEBM, MP4, OGG 등의 확장자가 지원되며 음성을 위해서 MP3, WAV가 지원됨 (HTML 페이지도 지원됨)

표 4. Nftify에서 지원하는 메타데이터 구조 [26]

Field	Description
name	NFT의 이름(최대 200자)
description	해당 NFT에 대한 설명(Markdown 지원)
image	Image가 저장된 중앙화 서버의 URL 혹은 IPFS URL
animation_url	멀티미디어 첨부파일이 저장된 URL. 영상에 대해서 GLTF, GLB, WEBM, MP4, M4V, OVG, OGG 등의 확장자가 지원되며 음성을 위해서 MP3, WAV, OGA가 지원됨
animation_type	animation_url에서 제공되는 멀티미디어 첨부파일의 파일 형식
external_url	사용자들이 binance chain 플랫폼 말고, 외부에서 접근할 수 있는 URL
attributes	NFT이 특징을 설명하는 필드로서, NFT의 디테일과 희귀도 등을 내포함

표 5. Binance Chain에서 지원하는 메타데이터 구조 [27]

그림 1을 통해서 OpenSea에서 확인 가능한 NFT 하나를 예시로 실제 메타데이터 파일이 어떤 형식으로 작성되어 있는지 살펴본다. 그림 1(a)는 CryptoRayRays의 token id가 7330인 NFT [28]의 실제 image이다. OpenSea에서 해당 NFT에 대한 Properties로서 그림 1(b)와 같이 소개하고 있다. OpenSea에서는 NFT 스마트 컨트랙트에 저장된 각 token id에 해당되는 메타데이터 파일의 URL을 읽어 들인다. 해당 메타데이터 파일을 분석하여, 표 3에 표기된 이름의 필드 정보들을 스크래핑한다. 따라서, 메타데이터를 통해서 그림 1(b) 처럼 해당하는 NFT의 Properties 정보를 표시해준다.

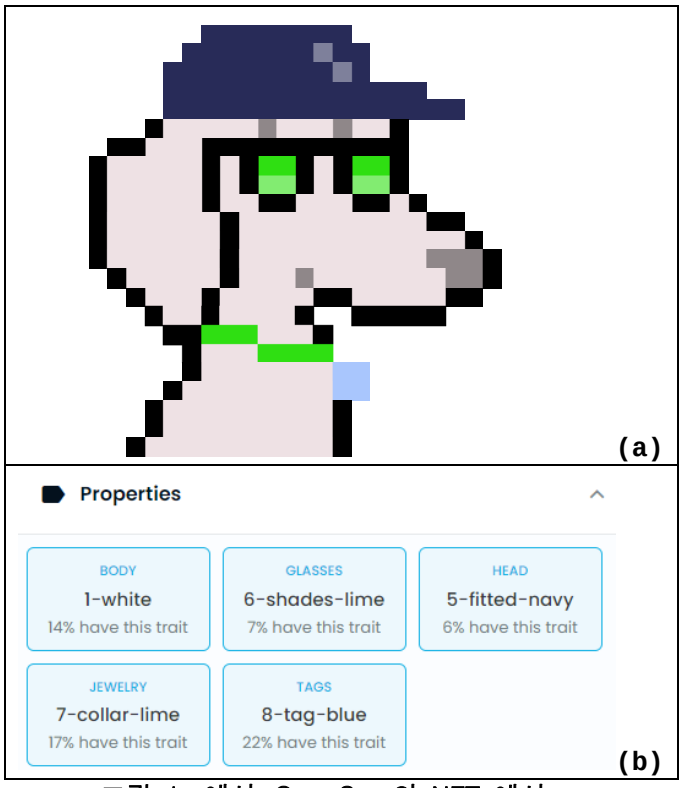


그림 1. 예시: OpenSea의 NFT 예시 – CryptoRayRays #7330

그림 2는 CryptoRayRays #7330의 실제 메타데이터 파일이며, name, description, image, attributes 필드들이 포함된 JSON 파일이다. OpenSea에서는 해당 메타데이터를 통해서 NFT 이름과 설명을 사이트에 표시할 수 있으며, image에 있는 실제 이미지가 저장된 url을 통해서 사이트에 이미지를 게시할 수 있다. 또한, attributes 안에 body, head, glasses, jewelry, tags가 포함되어 있는데, 이를 이용해서 Properties에 해당 NFT에 대한 디테일 정보를 표시해준다.

```
{
  "name": "CryptoRayRays #7330",
  "description": "I always wanted a punk, but
there weren't any for dogs like me. This
inspired me to design & develop CryptoRayRays -
10,000 unique collectible tokens with proof of
ownership stored on the Ethereum blockchain. Your
token allows unlimited cuddles and belly rubs.
<br> CryptoRayRays are not affiliated with
CryptoPunks or Larva Labs. Woof.",
  "image":
"https://gateway.pinata.cloud/ipfs/QmNkxawwVc8Ewg
8sCsvev6ewAVmV9oS9487DZBhzXQLwgz/7330.png",
  "attributes": {
    "id_hash": 7330,
    "body": "1-white",
    "head": "5-fitted-navy",
    "glasses": "6-shades-lime",
    "jewelry": "7-collar-lime",
    "tags": "8-tag-blue"
  }
}
```


그림 2. 예시: OpenSea 에 등록된 NFT 의 메타데이터 예시 [29]

현재 NFT 플랫폼에서 지원하는 메타데이터들의 획일화된 표준이 존재하지 않는다. 따라서, 각 NFT 플랫폼에서 지원하는 메타데이터들은 동일하지 않다. 예를 들어서, image, name, description, animation_url 등 공통적으로 포함되는 필드가 있기 때문에 어느정도 플랫폼 간에 호환성이 있다. 하지만 OpenSea 에서는 background_color 가 메타데이터로 포함되어 있지만, Nftify 와 Binance Chain 에서는 지원하지 않는다. 각 플랫폼들에서는 해당 필들을 읽어 들어서 프론트앤드에 출력해주기 때문에, 해석할 수 없는 필드들에 대해서는 정보를 노출해주지 않는다. NFT 를 구현하기 위한 표준 뿐만 아니라 NFT 를 표현하기 위한 메타데이터에 대해서도 표준이 존재한다면, 각 플랫폼마다 메타데이터 형식이 일치하지 않는 문제를 해결할 수 있을 것이다. 이러한 이유 때문에 카르다노(Cardano) [30]에서는 CIP-0025 [31]에서 NFT 메타데이터 표준에 대한 정의를 제안하고 있다.

Ⅳ. 결론

본 연구에서는 현재 많은 인기를 얻고 있는 NFT 의 실체에 대해서 조사 및 분석을 수행한다. NFT 구현을 위한 표준들과 NFT 를 생성하는 프로세스에 대해서 소개했다. NFT 는 자산의 실제 정보와 해당 NFT 에 대한 정보를 나타내는 메타데이터로 이루어져있고, 해당 메타데이터의 참조 링크가 블록체인에 기록된다. 그래서 NFT 를 정확히 이해하기 위해서는 여러 NFT 플랫폼에서 지원하는 메타데이터들을 조사했다. 그 결과 현재 NFT 를 위한 메타데이터에 대한 표준이 없기 때문에, 각 플랫폼마다 메타데이터가 다르다는 것을 발견했다. NFT 메타데이터를 표준화하면, 모든 플랫폼에서 데이터를 완전히 사용할 수 있을 것이다. 향후 연구로서 본 연구를 기반으로 NFT 메타데이터 표준화에 대한 연구를 진행할 예정이다.

ACKNOWLEDGMENT

본 연구는 (주)코인원의 지원과 과학기술정보통신부 및 정보통신기획평가원의 대학 ICT 연구센터육성지원사업의 연구결과로 수행되었음 (IITP-2022-2017-0-01633).

참 고 문 헌

[1] Wang, Qin, et al. "Non-fungible token (NFT): Overview, evaluation, opportunities and challenges." arXiv preprint arXiv:2105.07447.
[2] 민경식, 김관영, 박진상, "NFT 기술의 이해와 활용, 한계점 분석", KISA Insight 2021 VOL.03
[3] CoinDesk Korea, https://www.coindeskkorea.com/news/articleView.html?idxno=77648
[4] NameCoin Explorer (174923 block), https://nmc.tokenview.com/kr/block/174923
[5] Szabo, Nick. "Formalizing and securing relationships on public networks." First monday.
[6] Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." Ethereum project yellow paper 151.2014
[7] CryptoPunks, https://www.larvalabs.com/cryptopunks/
[8] CryptoKitties, https://www.cryptokitties.co/
[9] Decentraland, https://decentraland.org/
[10] Axie Infinity https://axieinfinity.com/
[11] ERC-721, https://eips.ethereum.org/EIPS/eip-721
[12] OpenSea, https://opensea.io/
[13] SuperRare, https://superrare.com/
[14] Rarible, https://rarible.com/
[15] Nifty Gateway, https://niftygateway.com/
[16] IT 조선, http://it.chosun.com/site/data/html_dir/2021/09/02/2021090201202.html
[17] 매일경제, https://www.mk.co.kr/news/world/view/2022/02/136600/

[18] ERC-1155,
https://eips.ethereum.org/EIPS/eip-1155
[19] Klaytn, https://www.klaytn.com/
[20] KIP-17, https://kips.klaytn.com/KIPs/kip-17
[21] ERC-20, https://eips.ethereum.org/EIPS/eip-20
[22] OpenZeppelin,
https://github.com/OpenZeppelin/openzeppelin-contracts
[23] IPFS, https://ipfs.io/
[24], Etherscan, https://etherscan.io/
[25] OpenSea Metadata Standards,
https://docs.opensea.io/docs/metadata-standards
[26] NFTIFY Metadata Standards,
https://support.nftify.network/hc/en-us/articles/4409618795417-Metadata-Standards
[27] Binance Chain Docs,
https://docs.binance.org/smart-chain/developer/nft-metadata-standard.html
[28] CryptoRayRays #7330,
https://opensea.io/assets/0x8d4e2435c262eb6df10e5e4672a8f07e42d8d67e/7330
[29] CryptoRayRays 7330 Metadata,
https://opensea.mypinata.cloud/ipfs/QmRC3nwNmE5ezFMJKcZCJNCYp2SHfzBSkK9SY782LewRVn/7330
[30] Cardano, https://cardano.org/
[31] CIP-0025, https://github.com/cardano-foundation/CIPs/blob/master/CIP-0025/README.md

대용량 스토리지를 지원하는 블록체인 확장 기법

나동준, 박세진*
계명대학교

nadongjun@kmu.kr, *baksejin@kmu.ac.kr

Blockchain expansion technique that supports large-capacity storage

Dongjun Na, Sejin Park*
Keimyung University

요 약

블록체인 기술은 합의 알고리즘과 분산 원장 기법을 통해 탈중앙화된 데이터 저장으로 데이터의 무결성을 보장하며 데이터 위변조를 방지할 수 있다. 하지만 기존 블록체인 기술은 높은 스토리지 용량 요구와 트랜잭션 전파 속도 문제 해결을 위해 대용량 데이터를 외부 저장소인 오프체인에 저장하는 방식을 사용한다. 블록체인 기술은 저장된 데이터에 대한 위변조 방지는 가능하지만 외부 데이터의 위변조는 방지할 수 없으므로 서비스를 지원하기 위한 대용량 데이터(사진, 영상)에 대한 신뢰성은 보장할 수 없으며 외부 네트워크로 데이터를 저장 및 다운로드 하는 과정의 지연시간이 존재한다. 본 논문에서는 이러한 한계점을 해결하기 위해 대용량 데이터를 블록체인 네트워크의 노드만으로 유지할 수 있는 기법을 제안하였으며 제안된 구조의 실험 결과 기존 퍼블릭 오프체인 기술과 비교하여 제안한 구조의 데이터 Insert 처리 지연시간이 10-50 배 가량 낮았으며 Download 의 경우 지연시간이 최대 100 배 차이가 존재하여 높은 성능을 보이는 것을 확인하였다.

Ⅰ. 서 론

기존 인터넷 서비스는 중앙 서버-클라이언트 구조[1]를 사용하여 서비스를 사용하는 사용자가 데이터를 생산하고 중앙 데이터베이스에서 데이터를 관리하는 방법을 사용한다. 하지만 중앙화된 구조를 사용하여 디도스 공격과 랜섬웨어[2]의 공격이 발생할 경우 모든 사용자의 데이터가 위변조 및 손실될 가능성이 존재하며 서비스가 동작되지 않는 취약점이 존재한다. 이러한 구조는 블록체인[3]을 기반으로 데이터를 관리하는 방법으로 해결할 수 있다.

블록체인 기술은 P2P(Peer to Peer) 네트워크[4]를 기반으로 데이터를 중앙 서버가 아닌 같은 원장을 네트워크의 노드들이 분산 저장하며 합의를 통해 데이터를 저장한다. 이 방법으로 데이터 저장 서비스에 대한 안정성과 신뢰성을 보장할 수 있다.

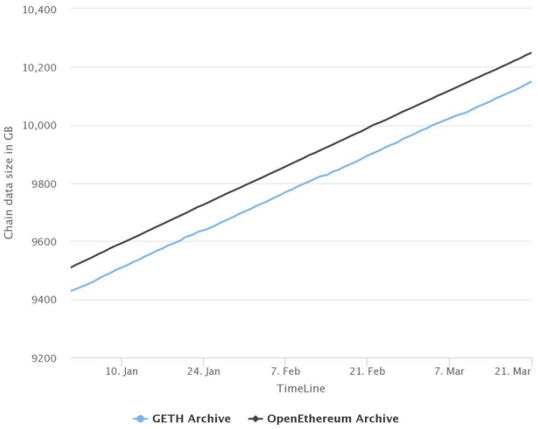


Fig 1. 이더리움 크기 그래프

블록체인 기술의 장점으로 인해 Grand View Research[5]에 따르면 글로벌 블록체인 기술 시장 규모는 2021 년 59 억 2000 만 달러로 2022 년부터 2030 년까지 85.9% 성장이 예상된다.

또한 블록체인 기술의 적용이 금융, 물류, 유통, 제조, 공공 서비스, 사회, 문화 등 전영역으로 확장되었으며 최근에는 기존의 '월드 와이드 웹'(World Wide Web, WWW)의 중앙화 한계를 해결하기 위해 검열, 신원 정보 및 데이터 지배를 막고 데이터의 권한을 탈중앙화 한 인터넷 서비스 제공을 의미하는 Web3.0 의 기반이 되며 기술의 안정적인 서비스 제공을 위해 성능 또한 중요해지고 있다.

하지만 블록체인 기술의 데이터 저장 용량 한계점[6]이 존재한다. Fig 1.의 명시된 EtherScan[7]의 조사 결과에 따르면 현재 스마트 컨트랙트 기능을 제공하여 dApp(Decentralize Application)의 기반이 되는 이더리움의 경우 전체 블록체인을 백업하는 Archive Node 의 스토리지 요구량이 10,000 GB 이상이다.

따라서 블록체인 기술에서 용량에 대한 최적화 솔루션 적용은 필수적이며 이더리움의 경우 데이터 저장을 위해서는 Gas 를 소모해야하며 데이터의 크기 및 스마트 컨트랙트에 연산량에 따라 많은 비용이 든다.

기존 블록체인 기술에서 대용량 데이터의 저장의 경우 많은 비용이 요구되기 때문에 블록체인 네트워크 노드가 아닌 외부의 오프체인[8] 또는 클라우드 서버에 데이터를 저장하고 데이터의 버전과 메타데이터만을 블록체인에 기록하는 방법을 사용한다.

이러한 방법을 통해 메타데이터로 외부 데이터의 위변조를 판단할 수 있지만 외부 네트워크에 저장된 데이터에 대한 손실과 위변조를 방지할 수 없으며 외부 네트워크에 데이터를 요청하고 저장할 경우 지연시간이 존재한다.

분산 파일 시스템인 IPFS(InterPlanetFileSystem)[9]의 경우 파일의 저장을 위해 퍼블릭 네트워크에 파일을 Chunk 단위로 분산 저장하여 Content Name 으로 분산 저장된 파일을 복원하여 사용할 수 있다. 이러한 방법은 전체 네트워크로 파일을 저장할 경우 데이터를 분산하고 여러 노드로 저장하고 저장한 파일을 다운로드할 경우 다시 분산된 조각을 모아야 하므로 지연시간이 존재한다.

또한 파일의 저장을 위해 파일에 대한 Pin 을 하여 비용이 소모되며 블록체인 외부 네트워크에서 유지되는 파일이므로 노드가 유지된다는 보장을 할 수 없어 신뢰성을 보장할 수 없다.

따라서 파일의 신뢰성과 안정성 및 성능 유지를 위해 외부 네트워크가 아닌 블록체인 네트워크의 노드에서 대용량 파일 및 서비스 데이터 저장과 낮은 지연시간을 유지하는 스토리지가 요구된다.

Ⅱ. 본론

본 논문에서는 블록체인 외부 네트워크에 사용자 데이터를 저장하는 방법의 신뢰성과 지연시간의 한계점을 해결하기 위해 블록체인 네트워크 노드의 로컬 스토리지에 서비스 데이터를 저장하여 블록체인을 네트워크 노드만으로 데이터를 관리하는 방법을 제안한다.

블록체인 노드만으로 데이터 스토리지를 구성하기 위해 데이터를 서비스 단위의 클러스터를 구성하여 같은 서비스 데이터베이스에 유지하는 방법을 사용한다.

데이터의 저장을 위해 In-memory 데이터베이스인 MongoDB[10]를 활용하였다.

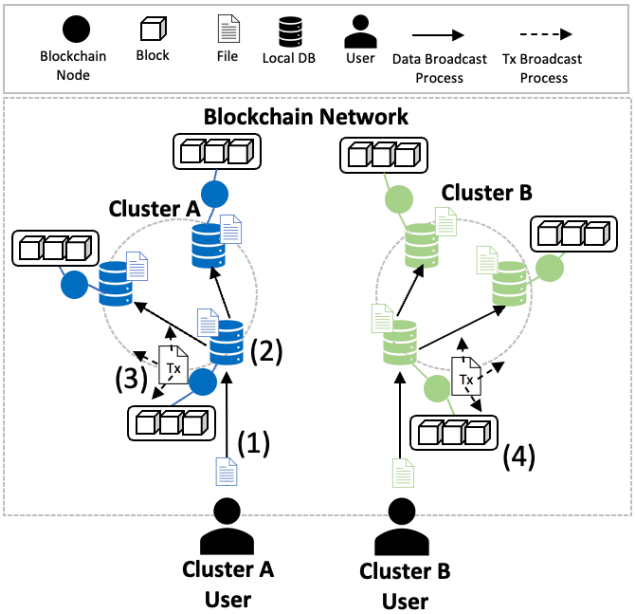


Fig 2. 시스템 아키텍처

Fig 2.는 본 논문에서 제안하는 아키텍처이다. 블록체인 네트워크를 구성하는 블록체인 노드, 클러스터에서 생성된 메타데이터 트랜잭션이 포함된 블록, 사용자가 생성하는 파일, 블록체인 네트워크 노드가 데이터를 저장하기 위해 유지하는 로컬 데이터베이스로 구성되며 클러스터에 데이터를 저장하는 사용자가 존재한다. 로컬 데이터베이스 및 트랜잭션을 블록에 기록하기 위한 2 가지 과정으로 구성된다.

블록체인 네트워크 내 데이터를 저장하기 위해 데이터베이스를 유지하는 클러스터를 구성하였다. 사용자는 속한 서비스 클러스터로 데이터를 저장하고 메타데이터를 클러스터 내 노드가 생성하여 블록체인 네트워크에 브로드캐스트 하며 동작 순서는 다음과 같다.

(1) 클러스터의 유저는 본인이 속한 클러스터 노드에 저장할 파일을 전송한다.
(2) 클러스터 노드 중 리더 노드 역할을 하는 노드가 파일을 저장하고 클러스터 내 모든 노드에 데이터를 복제한다.
(3) 리더 노드는 데이터를 저장 및 복제하고 메타데이터가 포함된 트랜잭션을 브로드캐스트한다.
(4) 블록체인 네트워크에 배포된 트랜잭션이 블록체인에 기록된다. 메타데이터가 포함된 트랜잭션은 클러스터 단위가 아닌 모든 블록체인 네트워크에 배포가 된다.

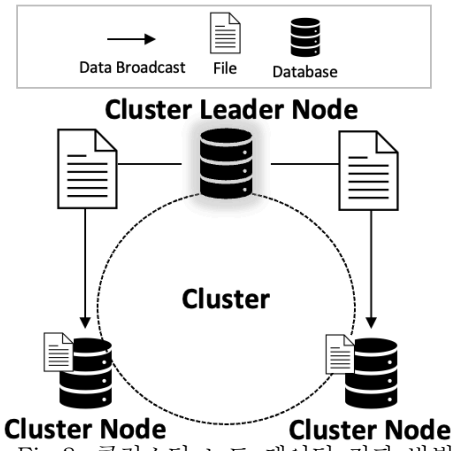


Fig 3. 클러스터 노드 데이터 전파 방법

Fig 3.은 서비스 데이터를 저장하기 위해 구성된 클러스터 네트워크이다. 데이터의 Write 요청을 수행하는 노드 1 개와 Read 요청을 수행하는 2 개 이상의 노드로 구성된다.

리더 노드 : 데이터를 데이터베이스에 저장하는 Write 요청과 데이터의 요청을 수행하는 Read 요청을 모두 처리 가능하지만 write 요청을 주로 수행한다.

클러스터 노드 : 리더 노드에 저장된 데이터를 주기적으로 복제하여 데이터를 저장하며 Read 요청을 수행한다.

동작 과정은 리더 노드가 유저로부터 Base64 형식의 파일 데이터 Write 요청을 수행하고 클러스터 노드에서 주기적으로 데이터를 복제하여 로컬에 저장한다.

제안한 아키텍처 구현을 위해 MacBook Pro (Processor : M1, RAM : 16GB)에 3 개의 노드를 구성하였으며 각각 분리된 컨테이너로 동작한다. 기존 블록체인 대용량 데이터에 사용되는 가장 대표적인 오프체인인 Public IPFS 와 비교한다.

실험을 위해 인터넷 서비스에서 사용되는 가장 대표적인 데이터인 이미지(JPG, GIF, PNG)와 PDF, MP3 형식 파일의 데이터 평균 크기[11]를 기존 오프체인인

IPFS 와 구현된 시스템에서 업로드와 다운로드 지연시간을 비교하였다.

Table 1. 웹 서비스에 사용되는 데이터 형식과 평균 크기

데이터 타입	PNG	GIF	JPG	PDF	MP3
크기	4 KB	8 KB	12 KB	20 KB	4 MB

Table 1.은 실험에 사용된 데이터를 나타낸다. 인터넷 서비스에서 사용되는 대표적인 데이터 형식과 데이터들의 평균 크기에 맞게 Dummy 파일을 생성하여 Docker Network 로 구성한 MongoDB 클러스터 노드와 Public IPFS Network 에 업로드 및 다운로드 지연시간을 비교하는 실험을 진행하였다.

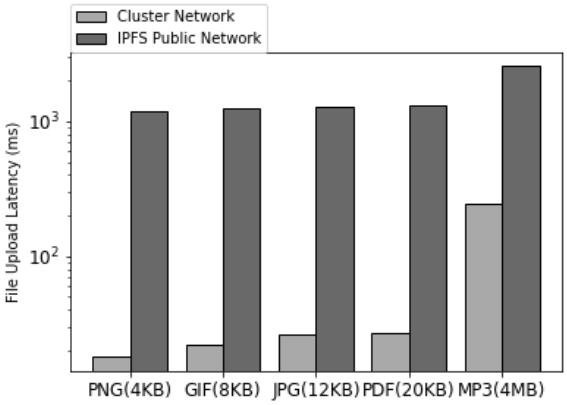


Fig 4. 기존 오프체인 기술과 데이터 저장 지연시간 비교

Fig 4.는 기존 오프체인 기술인 IPFS Public Network 와 아키텍처 구현에 사용된 MongoDB 클러스터 노드 간에 데이터 저장 지연시간을 비교한 Log Scale 그래프이다. Dummy 데이터(4KB, 8KB, 12KB, 20KB, 4MB)를 순차적으로 IPFS 와 클러스터 네트워크에 저장할 경우 지연시간을 측정하였으며 IPFS 네트워크, 클러스터 네트워크에서 모두 데이터 크기가 4KB – 20KB 간에는 큰 차이가 존재하지 않았다. 클러스터 네트워크와 IPFS 간에는 최대 50, 최소 10 배 가량의 저장 지연시간 차이가 존재하여 클러스터 네트워크에서 저장에 소요되는 시간이 더 적은것을 확인하였다.

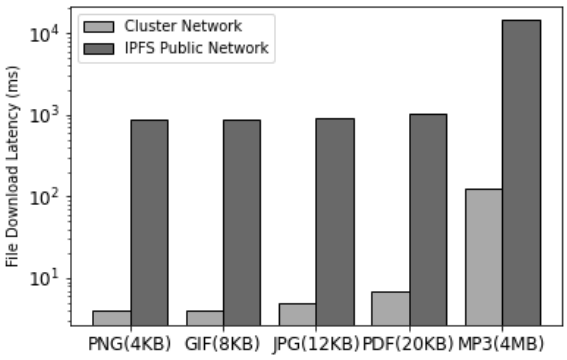


Fig 5. 기존 오프체인 기술과 데이터 다운로드 지연시간 비교

Fig 5.는 Fig 4. 실험에서 진행한 Dummy 데이터(4KB, 8KB, 12KB, 20KB, 4MB)를 IPFS 와 클러스터 노드에 저장한 데이터를 다운로드 할 경우 발생하는 지연시간을 비교한 그래프이다.

실험을 위해 IPFS 의 경우 반환된 IPFS hash 값을 통해 ipfs.files.get() 함수로 파일을 다운로드 받을 경우 지연시간을 측정하였으며 클러스터 네트워크의 경우 업로드한 파일의 Base64 형식 데이터에 대한 Object Id 로 쿼리하여 다운로드 받을 경우 발생하는 지연시간을 측정하였다.

측정 결과 다운로드의 경우도 IPFS 와 클러스터 네트워크에서 데이터의 크기가 4KB-20KB 간에는 큰 차이 존재하지 않았지만 IPFS-클러스터 네트워크 간 같은 크기의 데이터 다운로드의 경우 큰 지연시간이 존재하였으며 IPFS 에서 4MB 의 경우 클러스터 네트워크에 비해 100 배 가량 큰 지연시간이 발생하여 다운로드 시간 또한 제안한 아키텍처에서 낮은 지연시간이 발생하는 것을 확인하였다.

Ⅲ. 결론

본 논문에서는 블록체인의 용량 증가 한계점을 해결하기 위한 솔루션인 기존 오프체인 방식의 신뢰성 및 데이터 복구, 네트워크 지연시간 문제 해결을 위해 블록체인 노드의 로컬 스토리지를 사용하여 클러스터 네트워크를 형성하여 데이터를 저장하는 방식을 제안하였다. 실험 결과 인터넷 서비스에서 사용되는 대표적인 파일 형식을 저장 및 다운로드 하였을 때 대표적인 오프체인 기술인 IPFS 와 비교하여 지연시간이 낮은 것을 확인하였다. 추후 연구에서는 MongoDB 의 경우 최대 16MB 의 파일만을 저장할 수 있다는 한계가 존재하여 데이터 저장 용량의 제한이 존재하지 않는 기법을 연구할 예정이다.

ACKNOWLEDGMENT

이 논문은 2022 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2021-0-00484-002, 노드 간 메시지 전달과 합의를 위한 최적 경로 네트워크 프로토콜 기술개발)

참 고 문 헌

[1] Norrie, Moira C. "Client-Server Database Architectures for the Web." Advances in Multimedia and Databases for the New Century, A Swiss/Japanese Perspective (2000).

[2] Richardson, Ronny, and Max M. North. "Ransomware: Evolution, mitigation and prevention." International Management Review 13.1 (2017): 10.

[3] Zheng, Zibin, et al. "Blockchain challenges and opportunities: A survey." International Journal of Web and Grid Services 14.4 (2018): 352-375.

[4] Ripeanu, Matei. "Peer-to-peer architecture case study: Gnutella network." Proceedings first international conference on peer-to-peer computing. IEEE, 2001.

[5] Blockchain Technology Market Size, Share & Trends Analysis Report By Type (Private Cloud, Public Cloud), By Application (Digital Identity, Payments), By Enterprise

Size, By Component, By End Use, And Segment Forecasts, 2022 - 2030 (https://www.grandviewresearch.com/industry-analysis/blockchain-technology-market).

[6] Zhou, Qiheng, et al. "Solutions to scalability of blockchain: A survey." Ieee Access 8 (2020): 16440-16455.

[7] etherscan, https://etherscan.io/chartsync/chaindefault

[8] Kim, Soohyeong, Yongseok Kwon, and Sunghyun Cho. "A survey of scalability solutions on blockchain." 2018 International Conference on Information and Communication Technology Convergence (ICTC). IEEE, 2018.

[9] Benet, Juan. "Ipfs-content addressed, versioned, p2p file system." arXiv preprint arXiv:1407.3561 (2014).

[10] MongoDB, https://www.mongodb.com/

[11] New facts and figures about image format use on websites, https://www.pingdom.com/blog/new-facts-and-figures-about-image-format-use-on-websites/

분산아이디 (DID)를 활용한 트래블룰 준수 개인 암호화폐 지갑 설계

강창훈, 최원석, 이채현, 우종수*, 홍원기
포항공과대학교 컴퓨터공학과, *포항공과대학교 정보통신대학원

{chkang, ws4583, chlee0211, woojs, jwkhong}@postech.ac.kr

Design of Travel Rule Compliance Private Cryptocurrency Wallet Using Decentralized Identity (DID)

Changhoon Kang, Wonseok Choi, Chaehyeon Lee, Jongsoo Woo*, James Won-Ki Hong
Department of Computer Science and Engineering, POSTECH
*Graduate School of Information Technology, POSTECH

요 약

국제자금세탁방지기구 (FATF)에서는 자금세탁과 테러단체로의 자금 지원을 막기위해 암호화폐 규제에 대한 권고안을 2019년 발표했다. 이 권고안에는 해당 목적 달성을 위해 가상자산사업자 (VASP)가 따라야하는 권고사항들이 담겨있다. 트래블룰은 그 권고사항들 중 하나로서, 모든 가상자산 송금에 대해 송신인과 수신인의 신원정보를 수집 및 보관하여 테러리스트나 범죄조직이 자신들의 자금을 자유롭게 이동시키는 것을 막는 목적을 갖고 있다. 이에 따라 한국에서는 특정 금융거래정보의 보고 및 이용 등에 관련 법률 (특금법) 제정을 통해 국내 암호화폐 거래소들이 트래블룰을 준수하도록 하였다. 하지만 FATF 의 권고안이 개인 암호화폐 지갑과 거래소 지갑 간의 거래시 거래소가 개인지갑 소유자의 신원정보를 수집하는 경우 송금을 허용하고 있는 반면에, 특금법에서는 거래소 지갑 간의 거래에 대한 규제만을 포함하고 있다. 따라서 국내 4대 암호화폐 거래소 (업비트, 빗썸, 코인원, 코빗)들은 트래블룰 시행일 (2022.03.25)을 기준으로 고객이 각 거래소에 증빙을 통해 본인 소유의 개인지갑 주소를 등록하도록 하여 해당 주소로의 입출금만 허용하고 있다. 대부분 고객이 제출한 증빙 이미지를 활용해 심사를 거치는 방식으로 등록 여부가 결정되며, 거래하고자 하는 거래소들마다 각각 따로 등록이 필요하다. 본 논문에서는 World Wide Web Consortium (W3C)에서 표준화하고 있는 분산아이디 (Decentralized Identity, DID) 기술을 활용하여 트래블룰을 준수하면서 거래소로 암호화폐를 입출금 할 수 있는 개인지갑의 설계를 제안한다. 해당 설계에서는 개인지갑 주소가 본인의 소유라는 증명과 자신의 신원정보 데이터를 DID 형태로 발행해 직접 보관한다. 이에 따라 번거롭고 긴 시간이 소요되는 심사 및 등록 과정을 없애고, 거래소로의 입출금시 필수적인 정보만을 본인이 직접 제공하여 개인정보에 대한 자기주권을 행사할 수 있도록 한다.

Ⅰ. 서론

비트코인 [1]을 시작으로 탄생한 수많은 암호화폐들은 기본적으로 거래 당사자들의 신원에 대한 익명성을 제공한다. 거래 내역이 모두 블록체인에 기록되어 투명하게 공개되지만, 거래에 관여된 주소만을 알 수 있고 해당 주소를 소유한 사람의 신원정보는 전혀 알 수 없다. 이런 특징을 악용한다면 자금세탁이나 테러단체로의 자금 지원 등 불법적인 용도로 암호화폐가 활용될 수 있는 문제점이 존재한다. 해당 문제에 대응하기 위해 국제자금세탁방지기구 (Financial Action Task Force, FATF)에서는 2019년부터 암호화폐 규제에 대한 권고안을 발표하고 지속적으로 업데이트하고 있다 [2-7]. 이 기구에 가입되어 있는 각 국가들은 해당 권고안을 바탕으로 입법을 통해 암호화폐에 대한 규제를 실시해야 한다. 권고안에는 암호화폐의 불법적인 활용을 막기 위해 가상자산사업자 (Virtual Asset Service Provider, VASP)들이 따르도록 해야 하는 권고사항들이 담겨있다. 트래블룰은 그것들 중 하나로, 모든 가상자산 송금 건에 대해 자금의 송신인과 수신인의 신원정보를 수집 및 보관하도록 규정하고 있다. 트래블룰이라는 개념은 기존 금융권에서도 해외은행으로 송금할 때 은행이 해외은행 및 계좌정보를 수집, 기록해 두는 것으로 이미 사용 중이며, 이를 가상자산에도 적용하려는 것이다. 가상자산 송금에서 트래블룰 관련 정보의 수집, 보관에 대한 책임은 송신인과 수신인이 속한 VASP 인 각 암호화폐 거래소가 갖게 된다. 거래소들은 기존 자신의 고객들에 대해 확인이 완료된 신원정보를 갖고 있기 때문에 거래소 간 송금이 발생할 때 해당 정보를 서로 교환하여 보관하게 된다. 거래소와 개인지갑 간의 송금일 경우에는 거래소만 개인지갑 소유자의 신원정보를 수집하여 보관하도록 되어있다.

FATF 권고안의 트래블룰에 대응하기 위해 한국에서는 특정 금융거래정보의 보고 및 이용 등에 관련 법률 (특금법) [8]을 제정하여 관련 조항을 포함시켰다. 특금법에 따르면 원화로 환산했을 때 100만원 이상 상당의 송금으로 거래소 간 자금 이동이 발생하는 경우, 송신인과 수신인의 이름 및 가상자산 주소를 송수신 거래소들이 교환, 저장해야 한다. 하지만 FATF 권고안과는 달리,

거래소와 개인지갑 간의 송금에 대해서는 규제가 만들어지지 않았다. 최근 DeFi [9]와 NFT [10] 열풍이 불면서 많은 사람들이 개인지갑을 사용하고 있기 때문에 거래소와 개인지갑 간 송금을 막는 것은 현실적이지 못한 방법이다. 따라서 국내 트래블룰 시행일 (2022.03.25)을 기준으로 원화 거래가 가능한 국내 4대 암호화폐 거래소 (업비트, 빗썸, 코인원, 코빗) [11-14]들은 FATF 권고사항을 참고하여, 본인 소유가 증명된 개인지갑으로만 출금이 가능하도록 하는 화이트리스트 제도를 적용하고 있다 [15-18]. 업비트의 경우 입금 역시 본인 소유가 증명된 개인지갑으로만 가능하며, 메타마스크 [19] 개인지갑만 등록 가능하고 본인인증과 함께 메타마스크의 서명기능을 이용해 본인 소유임을 증명하도록 하고 있다. 이외의 거래소들은 메타마스크, 카카오클립 [20], 카이카스 [21] 등 여러 개인지갑들에 대해 거래소별로 상이하게 등록을 허용하고 있으며, 지갑주소와 신원정보가 함께 담긴 스크린샷이나 영상을 증빙자료로 제출해 심사에 의해 등록여부를 결정한다. 특히 빗썸의 경우 메타마스크 지갑에 대해서는 등록을 원하면 직접 고객센터로 방문해 대면심사를 진행해야 한다. 이러한 방식은 개인지갑 등록과정이 복잡하고 많은 시간 소요가 발생할 뿐만 아니라 거래하고자 하는 거래소마다 모두 따로 등록을 진행해야 하는 불편함이 있다. 또한 본인 소유의 개인지갑만 등록이 가능하기 때문에 타인의 개인지갑으로 직접 송금하는 것이 불가능하다.

본 논문에서는 분산아이디 (Decentralized Identity, DID) [22]를 활용해 별도의 개인지갑 등록과정 없이도 트래블룰을 준수하면서 거래소로 암호화폐를 입출금 할 수 있는 개인지갑의 설계를 제안한다. 해당 설계에서 개인지갑은 지갑주소가 지갑 소유자의 것이라는 증명과 함께 해당 지갑 소유자의 신원정보 데이터를 DID 형태로 발급받아 직접 보관한다. 해당 지갑 사용자는 지갑정보를 미리 거래소에 등록해두지 않고, 거래소와의 입출금 거래가 발생할 때만 지갑 소유에 대한 증명과 거래소가 요구하는 신원정보를 선택적으로 제공할 수 있다. 따라서 기존에 거래소로의 개인지갑 등록과정에서 발생했던 문제점들을 해소하면서, 지갑 소유자가 자신의 개인정보에 대한 자기주권을 행사할 수 있도록 한다. 매 거래마다 정보를 제공해야 한다는 단점이 발생하지만, 이를 통해 중앙화된 저장공간에 수많은 신원정보를 저장함으로써 발생할 수 있는 보안 위협을 줄일 수 있다. 또한 이미 지갑 소유와 신원정보에 대한 분산증명을 갖고 있기 때문에 해당 설계의 개인지갑을 소유한 타인에게 직접 송금하는 과정도 용이해질 수 있다.

Ⅱ. 배경

1. 암호화폐 지갑

암호화폐 지갑 [23]은 해당 지갑이 지원하는 암호화폐를 입출금 및 보관할 수 있는 하나의 장치 또는 프로그램이다. 공개키-개인키 쌍을 저장하고 있으며 이를 이용해 입출금이나 해당 지갑이 소유하고 있는 암호화폐의 종류와 양에 대한 정보를 얻을 수 있다. 암호화폐 지갑은 기준에 따라 다양한 방식으로 분류할 수 있는데, 개인키를 사용자 본인이 직접 보관하는지 또는 개인키는 암호화폐 거래소에서 보관하고 이에 대한 접근권한을 거래소 계정을 통해 얻는지 여부에 따라 개인지갑과 거래소지갑으로 구분할 수 있다.

개인지갑은 지원하는 암호화폐나 주요 목적에 따라 수많은 종류가 존재한다. 일반적으로 특정 지갑 소프트웨어를 설치함으로써 해당 지갑을 사용할 수 있고, 지갑의 생성과정에서 사용자의 신원과 관련한 개인정보는 전혀 포함되지 않는다. 외부에서 해당 지갑을 특정할 수 있는 것은 지갑의 주소 뿐이기 때문에, 암호화폐 거래소에서는 지갑 소유자에 대한 추가적인 정보와 검증없이 트래블룰을 준수하면서 입출금을 지원하는 것이 불가능하다.

2. 분산아이디 (DID)

DID [22]는 블록체인을 이용해 중앙화된 기관이 아닌 자신이 직접 본인의 신원을 관리하는 개념인 자기주권신원 (Self-Sovereign Identity, SSI) [24]을 구현하는 기술이다. 사용자가 신뢰할 수 있는 기관으로부터 최초로 신원정보를 검증 후 증명을 발급받게 되면, 해당 증명을 직접 관리하고 특정 서비스를 이용할 때 필수적인 정보만 선택하여 직접 제공할 수 있게 된다. 현재 많은 기관들이 DID 기술을 개발하고 있으며, 표준화를 위한 연구도 함께 진행되고 있다. 본 연구에서는 World Wide Web Consortium (W3C)에서 표준화를 진행중인 DID 기술을 기준으로 하여 개념 소개 및 설계 제안을 진행한다 [25]. 해당 DID 기술을 이해하기 위해서는 Claim, Credential, Presentation, 그리고 Decentralized Identifier 라는 개념에 대해 알아야 한다.

Claim 은 정보를 담는 가장 기본 단위로써 특정 주체에 대한 속성과 값으로 이루어진다. 예를 들어 Alice 라는 주체의 나이라는 속성이 30세 라는 값을 가진다는 정보가 하나의 claim 이 될 수 있다. Claim 들은 사용자의 신원정보를 직접 검증한 DID 의 발행자가 생성한다. 발행자는 하나 이상의 claim 을 생성하여 모두 자신이 발행한 claim 이라면 하나의 credential 이라는 단위로 묶을 수 있다. Credential 에는 해당 발행자가 생성한 하나 이상의 claim 뿐만 아니라, 추후 서비스 제공자 (검증자)들이 사용자로부터 제공받은 신원정보를 검증할 때 포함된 claim 들이 해당 발행자로부터 검증받은 것임을 증명하기 위해 발행자의 개인키로 암호화된 전자서명이 포함된다. 또한 검증과정에서 검증자는 블록체인 상에서 발행자의 공개키를 찾아 사용해야하기 때문에 이것이 저장된 장소를 알려주는 발행자의 식별자 (Decentralized Identifier, DID) 역시 credential 내에 포함된다. 이러한 정보들이 모두 포함된 credential 을 verifiable credential 이라고 하며, 일반적으로 발행자는 사용자의 요청에 의해 사용자 신원정보를 검증한 뒤 해당 정보를 verifiable credential 로 발급하여 전달해주고 사용자는 이를 보관하게 된다.

이후 사용자는 어떤 서비스를 이용하기 위해 서비스 제공자 (검증자)에게 요구받은 신원정보가 포함된 verifiable credential 들을 제출해야 한다. 이때 사용자 자신에 대한 하나 이상의 verifiable credential 을 하나의 presentation 이라는 형태로 묶어 제출한다. Presentation 에는 포함된 verifiable credential 들이 모두 해당 사용자에 대한 것임을 증명하기 위해 사용자의 서명과 식별자를 함께 갖고 있게 되고, 이런 데이터가 모두 포함된 presentation 을 verifiable presentation 이라고 한다. 최종적으로 verifiable presentation 을 제공받은 검증자는 사용자의 서명과 식별자를 이용해 그 안에 포함된 모든 verifiable credential 들이 해당 사용자에 대한 것임을 확인하고, 각 verifiable credential 내에 포함된 발행자의 서명과 식별자를 이용해 신원정보가 해당 발행자에 의해 검증된 것임을 확인할 수 있다. 앞선 설명대로 DID 시스템이 동작하기 위해서는 사전에 발행자와 사용자가 자신의 공개키-개인키 쌍을 생성하고, 공개키를 자신의 식별자와 함께 블록체인에 등록하는 과정이 필요하다.

Ⅲ. 본론

본 연구에서는 앞서 설명한 기존 개인지갑들이 사용

자의 신원정보를 포함하고 있지 않아 트래블룰을 준수하면서 거래소로 입출금을 직접 진행할 수 없다는 문제를 해결하기 위해 새로운 개인지갑의 설계를 제안한다. 본 연구에서 제안하는 개인지갑의 설계는 DID 기술을 활용해 신원인증기관으로부터 신원정보를 검증받고, 발급받은 verifiable credential 을 개인지갑에서 직접 저장하고 있도록 한다. 또한 지갑주소가 사용자의 소유라는 것을 DID 블록체인의 스마트 컨트랙트 [26]로부터 검증받고 이에 대한 verifiable credential 역시 발급받아 저장한다. 스마트 컨트랙트는 사전에 프로그래밍 된 내용에 따라 조건이 충족되면 자동으로 그 내용이 실행되도록 하는 기능으로, 사용자가 지갑주소에 대한 소유권을 증명할 경우에만 verifiable credential 을 발급해주도록 한다. 이후 거래소로 입출금을 진행할 때 사용자는 해당 두 verifiable credential 을 하나의 verifiable presentation 에 포함시켜 거래소에 제출함으로써, 자신의 신원정보를 제공하고 해당 개인지갑 주소가 본인 소유라는 사실까지 함께 증명할 수 있다. 전체적인 동작과정은 아래 그림 1 과 같다.

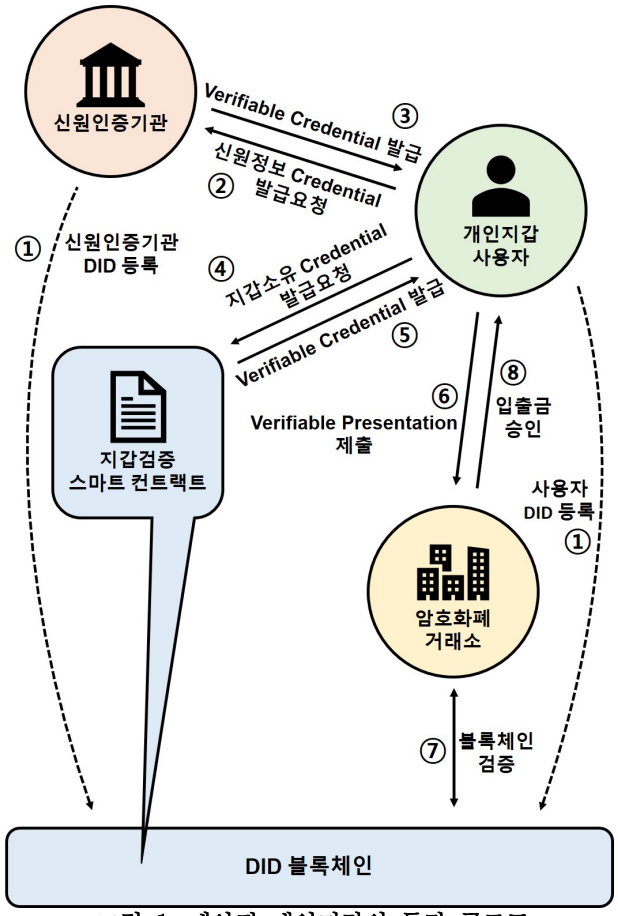


그림 1. 제안된 개인지갑의 동작 구조도

위 그림 1 이 동작하기 위해서는 우선 신원인증기관과 개인지갑 사용자가 자신의 식별자 (Decentralized Identifier, DID) 정보를 DID 블록체인에 등록해야 한다 (①). 이후 개인지갑 사용자는 신원인증기관에게 자신의 신원 검증을 요청하고, 신원인증기관은 검증 후 사용자 신원정보에 대한 verifiable credential 을 발급하여 전달한다 (②, ③). 사용자는 본인의 지갑주소를 본인이 소유하고 있다는 사실도 검증받아야 하는데, 이는 DID 블록체인 상의 지갑검증 스마트 컨트랙트에서 이루어진다. 자신의 지갑주소와 해당 주소와 쌍을 이루는 개인키로 암호화된 서명을 해당 스마트 컨트랙트에 함께 제출하면, 스마트 컨트랙트는 이를 이용해 검증 후 지갑주소에 대한 사용자의 소유권이 확인되는 경우 지갑소유에 대한 verifiable credential 을 발급해 전달한다 (④, ⑤). 이 과정까지 마치게 되면, 사용자는 신뢰할 수 있는 기관으로부터 검증받았다는 것을 증명할 수 있는 신원정보와 개인지갑의 주소가 본인의 소유임을 검증받았다는 증명을 모두 가질 수 있다.

이제부터 위 사용자는 암호화폐 거래소와의 거래가 가능해진다. 먼저, 개인지갑으로부터 거래소로 입금하는 시나리오를 가정한다면, 입금 거래를 생성하는 과정에서 개인지갑은 거래소에 verifiable presentation 을 제출하여 발급받은 입금주소의 입금 승인을 요청한다 (⑥). 요청을 받은 거래소는 전달받은 verifiable presentation 을 DID 블록체인에 접근하여 검증하고 (⑦), 개인지갑 사용자의 신원과 지갑소유에 대한 검증을 통과하였다면 입금을 승인한다 (⑧). 또한 거래소는 해당 요청에서 제공받았던 개인지갑 사용자의 신원정보를 트래블룰 준수를 위해 기록하게 된다.

반대로, 거래소로부터 개인지갑으로 출금하는 시나리오를 가정한다면, 거래소는 일단 고객으로부터 개인지갑으로의 출금요청을 받은 후, 해당 개인지갑으로부터 출금 승인요청이 올 때까지 대기한다. 출금 받을 개인지갑은 거래소에 verifiable presentation 을 제출하여 앞서 생성된 출금 거래의 최종 승인을 요청한다 (⑥). 거래소는 입금 시나리오와 같은 방식으로 DID 블록체인에 접근해 해당 verifiable presentation 의 데이터를 검증하고 (⑦), 문제가 없을 경우 출금을 승인한다 (⑧). 최종적으로 거래소는 verifiable presentation 속 수신인의 신원정보와 최초에 해당 거래를 요청한 고객의 신원정보를 해당 거래 정보와 함께 기록한다. 지금까지의 입금 및 출금 과정은 개인지갑 사용자와 거래소 고객이 동일인이 아니더라도 적용이 가능하다.

암호화폐 거래소마다 입출금시 개인지갑 사용자에게 요구하는 신원정보의 범위는 서로 다를 수 있다. 따라서 특정 거래소의 기준에 부합하는 verifiable credential 을 신원인증기관으로부터 발급받았음에도 다른 거래소와의 입출금 거래시 이를 사용할 수 없고, 다시 적합한 verifiable credential 을 발급받아야 하는 경우가 발생할 수 있다. Credential 은 특수한 서명 기술을 이용해 포함된 claim 들 중 필요한 정보만 선택적으로 공개하는 방법을 제공한다. 본 설계에서는 다양한 거래소들의 요구사항을 포괄하는 신원정보 credential 표준을 구성한다고 가정하고, 사용자는 해당 표준을 기준으로 발급받은 verifiable credential 을 거래소에 제공할 때 필수적인 정보만 선택적으로 제공할 수 있도록 한다.

본 설계에서 사용되는 DID 블록체인은 다음과 같은 최소한의 요구사항이 존재한다. 첫째로, 앞선 설명에서 언급되었던 지갑검증 기능을 수행하기 위해 스마트 컨트랙트를 지원해야한다. 둘째, DID 의 등록이나 스마트 컨트랙트의 실행과정, verifiable presentation 에 대한 블록체인 검증과정에서 요구되는 블록체인 네트워크 수수료가 매우 적거나 없어야 한다. 해당 과정들을 진행할 때마다 매번 수수료가 발생한다면 사용자들이나 거래소를 본 시스템에 참여하도록 유도하기 어려울 것이다. 따라서 예를 들면, 거래소들의 협력을 통해 동일한 목적을 가진 기관들이 하나로 모인 형태의 컨소시엄 블록체인 [27]으로 DID 블록체인을 구성하는 것이 하나의 방법이 될 수 있다. 트래블룰을 준수하는 개인지갑 입출금 활성화 및 거래소의 자체적인 개인지갑 등록 심사과정 삭제가 해당 방안에서 거래소들이 협력을 통해 컨소시엄 블록체인에 참여하려는 공통의 목적이 될 수 있다.

Ⅳ. 결론 및 향후 연구

본 논문에서는 트래블룰을 준수하면서 번거로운 거래소 등록과정 없이 직접 거래소로의 입출금이 가능한 개인 암호화폐 지갑의 설계를 제안했다. 사용자가 DID 기술을 활용해 발급받은 검증된 신원정보를 본인이 직접 관리하고, DID 블록체인 상의 스마트 컨트랙트로부터 개인지갑 주소소유에 대한 증명도 발급받아 보관하게 된다. 개인지갑 사용자는 해당 두 증명을 거래소 입출금시에 거래소에 제공하여 트래블룰을 준수하는 입출금 거래를 진행할 수 있다. 또한 현재 불가능한 타인 명의의 개인지갑으로의 입출금도 지원이 가능하다.

제안된 개인지갑의 설계는 암호화폐 거래소의 협력 없이는 실용이 불가능하다는 한계점이 있다. 본 개인지갑과의 연동을 위해 거래소가 추가적인 개발 작업을 진행하지 않는다면 해당 기능을 모두 구현하더라도 실제로 사용하는 것이 불가능하다. 하지만 지금처럼 개인지갑으로의 입출금이 매우 제한되어 있는 상황에서 거래소의 입장을 생각해보면, 해당 개인지갑을 지원함으로써 개인지갑 입출금이 더 자유로워졌을 때 더 많은 고객이 유입되는 효과를 기대해볼 수 있기 때문에 충분히 도입을 고려해볼 수 있을 것이라 생각된다. 또한 현재 개인지갑 등록 심사를 자체 진행하고 있는 거래소의 경우 직접 증빙자료를 검토하는 과정으로 인해 발생하는 업무부담을 줄일 수 있을 것이다.

사용자가 개인지갑 주소에 대한 소유권을 증명하기 위해서 본 설계에서는 지갑검증 스마트 컨트랙트를 통해 증명을 발급받도록 하고 있다. 해당 과정은 단순히 개인지갑의 개인키 서명 확인만으로 검증이 가능하기 때문에, 본 설계처럼 스마트 컨트랙트를 활용하지 않고 직접 검증자가 해당 서명을 제출받아 확인하는 방법 역시 적용 가능하다. 하지만 검증자 역할을 하는 기존 암호화폐 거래소들의 추가적인 개발 작업을 줄이기 위해 본 논문에서 설명한 것과 같이 설계를 하였다. 또한 본 설계의 방법대로라면 한번의 지갑검증과정으로 발급받은 증명을 지속적으로 사용할 수 있다는 장점이 있다.

향후 연구에서는 본 논문에서 제안한 설계를 기반으로 더 자세한 설계와 구현을 통한 Proof-of-Concept 검증을 진행할 계획이다. 또한 본 설계에서는 거래소로부터 개인지갑으로 출금시에 수신자도 해야 할 일이 발생하는데, 해당 문제를 개선할 수 있는 프로세스 수정 방안에 대한 연구가 필요하다. 마지막으로, 개인 암호화폐 지갑에 자신의 신원정보를 DID 형태로 보관하는 해당 제안의 기본적인 구조를 거래소와의 입출금 외에 또 활용할 수 있는 가능성이 있는지 탐색하여 해당 시스템을 확장시킬 수 있는 방안에 대해서도 연구가 가능할 것이라 생각된다.

ACKNOWLEDGMENT

본 연구는 (주)코인원과 과학기술정보통신부 및 정보통신기획평가원의 대학 ICT 연구센터육성지원사업의 연구결과로 수행되었음 (IITP-2022-2017-0-01633)

참 고 문 헌

[1] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." *Decentralized Business Review* (2008): 21260.
[2] FATF. Outcomes fatf plenary, 16-21 june 2019. Available at https://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-plenary-june-2019.html, Accessed: 2022-04-05.
[3] FATF. Improving global aml/cft compliance: On-going process - 21 june 2019. Available at https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/fatf-compliance-june-2019.html, Accessed: 2022-04-05.
[4] FATF. Public statement on virtual assets and related providers. Available at https://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-statement-virtual-assets.html, Accessed: 2022-04-05.
[5] FATF. Guidance for a risk-based approach to virtual assets and virtual asset service providers. Available at https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html, Accessed: 2022-04-05.
[6] FATF. The fatf recommendations. Available at https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html, Accessed: 2022-04-05.
[7] FATF. Outcomes fatf plenary, 19-21 october 2021. Available at http://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-fatf-plenary-october-2021.html, Accessed: 2022-04-05.
[8] 특정 금융거래정보의 보고 및 이용 등에 관한 법률. Available at https://www.law.go.kr/법령/특정금융거래정보의보고및이용등에관한법률, Accessed: 2022-04-05.
[9] Chen, Yan, and Cristiano Bellavitis. "Blockchain disruption and decentralized finance: The rise of decentralized business models." *Journal of Business Venturing Insights* 13 (2020): e00151.
[10] Wang, Qin, et al. "Non-fungible token (NFT): Overview, evaluation, opportunities and challenges." *arXiv preprint arXiv:2105.07447* (2021).
[11] 업비트. Available at https://upbit.com/home, Accessed: 2022-04-05.
[12] 빗썸. Available at https://www.bithumb.com, Accessed: 2022-04-05.
[13] 코인원. Available at https://coinone.co.kr, Accessed: 2022-04-05.
[14] 코빗. Available at https://www.korbit.co.kr, Accessed: 2022-04-05.
[15] 업비트. 트래블룰 이행에 따른 입출금 방식 변경 시행 및 디지털 자산 입출금 재개 안내. Available at https://upbit.com/service_center/notice?id=2534, Accessed: 2022-04-05.
[16] 빗썸. 화이트리스트 지갑주소 등록 안내. Available at https://cafe.bithumb.com/view/board-contents/1642769, Accessed: 2022-04-05.
[17] 코인원. 트래블룰 시행에 따른 가상자산 이전 방식 안내. Available at https://coinone.co.kr/info/notice/1673, Accessed: 2022-04-05.
[18] 코빗. 개인지갑 주소 등록 가이드. Available at https://exchange.korbit.co.kr/faq/articles/?id=7dWVcdas0GTuwWgLc1hPpV, Accessed: 2022-04-05.
[19] 메타마스크. Available at https://metamask.io, Accessed: 2022-04-05.
[20] 카카오클립. Available at https://www.kakaocorp.com/page/service/service/Klip, Accessed: 2022-04-05.
[21] 카이카스. Available at https://docs.kaikas.io, Accessed: 2022-04-05.
[22] Avellaneda, Oscar, et al. "Decentralized identity: Where did it come from and where is it going?." *IEEE Communications Standards Magazine* 3.4 (2019): 10-13.
[23] Suratkar, Saurabh, Mahesh Shirole, and Sunil Bhirud. "Cryptocurrency wallet: A review." *2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP)*. IEEE, 2020.
[24] Tobin, Andrew, and Drummond Reed. "The inevitable rise of self-sovereign identity." *The Sovrin Foundation* 29.2016 (2016).
[25] W3C. Decentralized Identifiers (DIDs) v1.0. Available at https://www.w3.org/TR/did-core/, Accessed: 2022-04-05.
[26] Mohanta, Bhabendu Kumar, Soumyashree S. Panda, and Debasish Jena. "An overview of smart contract and use cases in blockchain technology." *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. IEEE, 2018.
[27] Dib, Omar, et al. "Consortium blockchains: Overview, applications and challenges." *International Journal On Advances in Telecommunications* 11.1&2 (2018): 51-64.

대체 불가능 토큰 (NFT) 거래를 위한 블록체인 시스템 분석

최원석, 우종수*, 홍원기
포항공과대학교 컴퓨터공학과, *포항공과대학교 정보통신대학원

{ws4583, woojs, jwkhong}@postech.ac.kr

Analysis of Blockchain Systems for Non-Fungible Token (NFT) Trading

Wonseok Choi, Jongsoo Woo*, James Won-Ki Hong
Department of Computer Science and Engineering, POSTECH
*Graduate School of Information Technology, POSTECH

요 약

대체 불가능 토큰 (NFT)은 블록체인 기술을 기반으로 하는 고유하며 복제가 불가능한 가상의 토큰이다. 이러한 특성을 이용해 NFT 는 디지털 자산의 소유권을 증명하는 용도로 사용되며, 미술, 음악, 스포츠, 게임 등 다양한 분야에서 널리 활용되고 있다. 또한, NFT 는 시장을 통한 거래 뿐 아니라 개인 간 거래가 자유롭다는 장점도 있기 때문에 투자의 수단으로도 활용된다. 최근에는 디지털 자산뿐만 아니라 NFT 를 실물 자산에 접목시켜 실물 자산이 정품임을 증명하거나 투자의 목적으로 실물 자산 기반의 NFT 를 발행하는 사례도 등장하고 있다. 특히, 실물 자산을 기반으로 하는 NFT 의 경우 고가의 실물 자산을 여러 개로 분할 하여 적은 금액으로도 투자를 가능하게 하는 조각 투자 시장에서 효과적으로 활용될 수 있다. 하지만 현재 NFT 에도 몇 가지 문제점들이 존재하며 그 중 대부분은 기반 블록체인으로 이더리움을 사용하는 데에서 발생한다. 이더리움의 느린 처리속도와 높은 수수료가 문제가 되며 이를 해결할 수 있는 새로운 블록체인 시스템이 요구되고 있다. 본 논문에서는 이더리움이 가진 문제와 이를 해결하여 NFT 발행 및 거래에 사용되고 있는 기술들에 대해 소개한다. 그리고 다양한 자산을 기반으로 하는 NFT 를 발행 및 거래하기 위해 블록체인 시스템이 가져야할 요건에 대해 분석하고 앞으로 NFT 가 활용되기 위해 진행되어야 할 연구의 방향성을 제시하고자 한다.

Ⅰ. 서론

2세대 블록체인이라 불리는 이더리움 [1]이 이전 세대 블록체인들과 가지는 가장 큰 차이점은 스마트 컨트랙트이다. 스마트 컨트랙트의 도입으로 다양한 디앱 (Decentralized Application, DApp) [2]이 등장하였으며 토큰을 이용하여 사용자들에게 보상을 주어 서비스를 활성화하는 토큰이코노미도 더욱 활성화 되었다. 초기의 토큰 발행은 Ethereum Request for Comment (ERC) 20 [3] 이라 불리는 이더리움 표준을 기반으로 이루어졌다. ERC-20으로 발행된 토큰들은 대체 가능한 토큰 (Fungible Token, FT)으로써 동일한 스마트 컨트랙트에서 생성된 토큰들은 모두 동일한 가치를 지닌다.

한편, 이와 반대로 대체 불가능한 토큰 (Non-Fungible Token, NFT) [4]을 발행할 수 있는 ERC-721 [5] 표준이 정립되었고 이를 기반한 프로젝트들도 다수 생겨났다. NFT를 활용한 대표적인 사례로 크립토키티 [6]가 있다. 크립토키티는 고양이를 기르는 게임으로 이더리움을 기반으로 하는 DApp이다. 크립토키티에서는 고양이를 수집하고 교배시켜 새로운 고양이를 탄생 시킬 수 있다. 크립토키티의 고양이들은 NFT를 기반으로 하고 있기 때문에 모든 고양이들이 서로 다른 외형을 지니고 있어 사람들의 수집 욕구를 자극한다. 크립토키티는 큰 성공을 거두었으며 크립토키티와 유사한 다수의 NFT 프로젝트들이 등장하며 NFT 기술이 대중들에게 더욱 가까워지게 되었다.

NFT 기술이 확산되며 NFT를 수집품뿐만 아니라 다른 용도로도 활용하기 위한 움직임이 생겨났다. NFT의 유일성에 주목하여 NFT를 디지털 자산의 저작권과 소유권을 증명하는 용도로 사용하는 것이 가능함이 여러 사례들로부터 증명되었다. 이는 미술, 음악 등의 예술 업계에서 큰 주목을 받게 되었고 많은 디지털 아트나 음악들이 NFT로 발행되어 판매되기 시작했다. NFT는 시장이나 개인 간 거래가 자유롭다는 장점이 있어 NFT로 게임 아이템과 같은 자산들을 NFT로 발행하는 사례도 있고 NFT 상품을 투자 목적으로 구매하는 사용자들도 많이 생겨났다.

NFT는 디지털 자산뿐만 아니라 실물 자산에도 활용될 수 있다. 명품 브랜드들은 NFT를 활용하여 제품에 대한 설명이 포함된 정품 인증서를 발급할 수 있다. 이를

통해 빠르고 편리하게 제품의 정품 여부를 확인하는 것이 가능하다. 실물 자산 기반의 NFT가 효과적으로 활용될 수 있는 또 다른 사례 중 하나는 조각 투자 시장이다. 조각 투자는 개인이 투자하기 어려운 고가의 자산을 여러 개의 지분으로 쪼개어 다수의 투자자들이 투자 할 수 있는 투자 방식이다. 미술품이나 와인, 명품 시계 등 고가의 상품들에 개인이 투자할 수 있기 때문에 최근 많은 각광을 받고있다. 실물 자산을 여러 개의 지분으로 쪼개는 과정에서 NFT가 효과적으로 활용될 수 있다. 실물 자산을 NFT로 발행하여 나눌 경우 더욱 자유로운 지분에 대한 거래가 가능해지고 거래 과정을 투명하게 확인할 수 있다. 또한, 해당 지분에 해당하는 상품을 쉽게 확인할 수 있다는 장점도 존재한다. 이러한 장점들을 기반으로 조각 투자 시장에 NFT를 적용한 사례 [7]들도 등장하고 있다.

하지만 여전히 NFT 기술에 대한 우려와 불신도 존재한다. 특히, 현재 대부분의 NFT들은 이더리움을 기반으로 하고 있으며 NFT의 문제점 중 상당수는 이더리움 블록체인 네트워크의 자체적인 한계에서 비롯된다. 이더리움의 느린 처리 속도와 높은 수수료가 그 원인이다. 이러한 문제를 해결하기 위해서는 이더리움의 한계점을 해결하고 NFT를 거래하는 데 있어 필요한 기능들이 포함된 새로운 블록체인 시스템이 필요하다. 본 논문에서는 NFT 발행의 기반이 되는 플랫폼 측면에서 이더리움의 문제점과 해당 문제점을 개선한 블록체인들에 대해 소개하고 다양한 자산을 기반으로 하는 NFT를 거래하기 위한 추가적인 요구사항들에 대하여 분석 한다. 이를 통해 NFT를 활용할 수 있는 블록체인에 대한 정보를 제공함과 동시에 앞으로 NFT가 더욱 많이 활용되기 위해 진행되어야 할 연구 방향성에 대해 제시하고자 한다.

Ⅱ. 본론

본 연구에서는 NFT 활용에 있어 이더리움이 갖고 있는 문제점들을 소개하고 해당 문제점을 개선하여 NFT 거래에 활용되고 있는 기술들을 소개한다. 그리고 NFT 거래를 위한 스마트 컨트랙트 요구사항들에 대해 분석한다.

1. 이더리움의 성능과 수수료 문제

이더리움은 2015년 7월 30일 비탈릭 부테린에 의해 만들어진 블록체인이다. 이더리움에서 도입한 스마트 컨트랙트로 인해 이더리움은 비트코인의 뒤를 잇는 블록체인으로 거듭날 수 있었으며 이더리움을 기반으로 다양한 프로젝트들이 탄생했다. 하지만 이더리움에 많은 사용자가 생기면서 이더리움의 문제점 또한 계속해서 제기되어 왔다.

이더리움을 실제 사용하는데 있어 가장 큰 문제가 된 점은 이더리움의 성능 문제이다 [4]. 이더리움의 성능은 약 15 TPS (Transaction Per Second) 정도로 최근에 등장한 블록체인들에 비해 매우 낮은 편이다 [8]. NFT거래가 활발하게 이루어지기 위해서는 많은 양의 트랜잭션들을 처리할 수 있어야 하는데 이 정도의 성능으로는 거래들을 빠르게 처리할 수 없다.

이더리움에서 NFT를 거래할 때 발생하는 높은 가스 수수료 역시 중요한 문제이다 [4]. 스마트 컨트랙트를 통해 NFT를 거래하는 과정에서 적지않은 가스 수수료가 발생하며 이는 잦은 NFT 거래를 불가능하게 만든다. 이로 인해 가스 수수료를 최소화 하기 위한 연구들 [9]도 존재한다. 블록체인의 성능과 수수료 문제는 NFT 거래에 국한된 문제가 아니라 블록체인을 사용하는데 있어 모든 상황에 문제를 야기한다.

이러한 문제들은 합의 알고리즘과 확장성을 개선함으로써 해결할 수 있다. 이더리움 개발자들 역시 이러한 문제를 인식하고 기존의 작업 증명 (Proof of Work, PoW) [10]방식의 합의 알고리즘에서 지분 증명 (Proof of Stake, PoS) [11]방식으로 전환하고자 하며 샤딩 [12]을 통해 확장성을 개선해 나가고자 하고 있다. 하지만 개발 완료 시점이 초기에 계획한 일정에서 많이 늦어져 언제 구현이 완료될 지는 장담할 수 없다.

2. 이더리움 대체 블록체인 기술

솔라나 [12]는 2017 년 출범한 블록체인으로 역사 증명 (Proof of History, PoH) [13]과 지분 증명 방식을 함께 사용하여 성능을 크게 끌어올렸다. 솔라나에서는 지분 증명 방식을 이용해 지분을 기반으로 블록을 생성할 리더를 선정한다. 그리고 거래 내역을 블록에 등록할 때 시간 순서에 대한 정보를 함께 등록하는 역사 증명 방식을 사용하여 블록을 검증하는데 걸리는 시간을 감소시켰다. 솔라나는 50,000 에서 65,000 정도의 TPS 까지도 보일 수 있다고 소개하고 있으며 이더리움을 대체할 NFT 플랫폼으로 주목받고 있다. 솔라나 블록체인을 기반으로 만들어진 NFT 를 거래할 수 있는 NFT 거래 시장 [14]도 등장하고 있다.

한편, 이더리움의 성능 문제를 직접적으로 해결한 방법도 존재한다. 폴리곤 [15]은 이더리움에 적용할 수 있는 레이어 2 네트워크로 별도의 블록체인을 운영하지는 않지만, 트랜잭션을 폴리곤 네트워크에서 빠르게 처리하여 이더리움에 전달하게 된다. 폴리곤에서는 지분 증명 방식을 적용하고 있으며 수수료가 거의 없고 솔라나와 마찬가지로 65,000 TPS의 성능까지 보일 수 있다고 소개하고 있다. 폴리곤은 이더리움을 기반으로 하고 있기 때문에 호환성이 높다는 장점이 있으며 실제로 이러한 특성 때문에 최대 규모의 NFT 거래 플랫폼인 OpenSea [16]에서도 이더리움 다음으로 NFT를 발행하는데 많은 지원을 하고 있다.

	이더리움	솔라나	폴리곤
TPS	20	50,000 ~ 65,000	65,000
합의 알고리즘	작업 증명	역사 증명 + 지분 증명	지분 증명
특징	가장 많은 사용자	이더리움 대체 블록체인	레이어 2 네트워크

표 1. 이더리움, 솔라나, 폴리곤 비교

3. 스마트 컨트랙트 요구사항

NFT 거래를 지원하는 데 있어 가장 중요한 요소는 스마트 컨트랙트로 이를 통해 NFT를 발행할 수 있어야 한다. 현재 가장 많은 NFT가 발행되고 있는 이더리움에서는 토큰과 관련하여 그림 1 과 같이 크게 3 개의 표준이 존재한다. ERC-20 은 FT를 여러 개 발행할 수 있으며 ERC-721 에서는 NFT를 발행할 수 있다. ERC-1155 [17]에서는 ERC-20 과 ERC-721 에서 지원하는 토큰들을 동시에 발행할 수 있으며 Semi-Fungible Token이라 불리는 FT와 NFT 둘 다 될 수 있는 토큰 또한 발행할 수 있다. Semi-Fungible Token 사용법의 예시로는 티켓을 들 수 있다. 티켓은 사용되기 전에 동일한 가치를 갖지만 사용된 이후에는 가치를 잃게 된다. 하지만 사용된 티켓은 추억을 간직하는 용도 등으로 재사용될 수 있다. 이 경우 티켓은 처음에는 FT로 발행되었다가 이후에 NFT로 변환함으로써 활용할 수 있다. 이러한 표준들을 기반으로 현재 이더리움에서 NFT를 여러 개로 조각화 하는 방법에는 크게 두 가지가

존재한다. 하나는 ERC-721 기반의 토큰을 ERC-20 기반의 토큰으로 나누는 것이고 다른 하나는 ERC-1155 표준을 이용해 다수의 NFT를 생성해 내는 것이다.

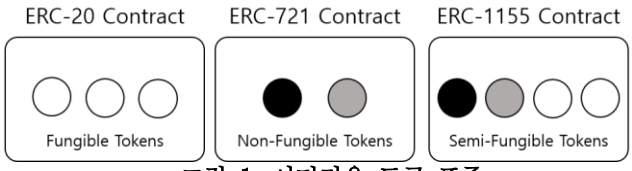


그림 1. 이더리움 토큰 표준

NFT거래를 위한 블록체인 시스템에서는 고가의 상품을 여러 개의 조각으로 분배하는 조각 투자를 지원하기 위해 이더리움의 토큰 표준들과 같이 하나의 NFT를 여러 개로 조각화 할 수 있는 기능이 필요하다. 이 때 나누어진 조각들이 모두 같은 가치를 지니는 것이 일반적이나 때에 따라 각 조각들의 가치가 다르게 되어야 할 필요성도 존재할 것이다. 또한, 게임 아이템과 같은 자산의 경우 동일한 자산에 대한 여러 개의 NFT가 발행될 필요성이 있다. 즉, 여러 개의 NFT를 동시에 발행하는 기능 역시 필요하다. 대부분의 실물 자산이나 일회성으로 사용되는 디지털 자산의 경우 NFT로 발행된 이후 자산이 사라지게 될 가능성도 있다. 이 경우 가치가 없는 토큰들이 시장에서 거래되는 것을 막기 위하여 해당 토큰들을 소각하는 기능 역시 필요하다.

토큰 외에 NFT를 거래할 때 스마트 컨트랙트에서 추가적으로 고려되어야 할 요소들도 존재한다. 실물 자산을 기반으로 한 조각 투자에서는 조각을 소유하고 있는 소유자들의 합의를 통해 실물 자산의 판매가 이루어 질 수 있다. 예를 들어 고가의 명품에 대한 조각 투자에서는 해당 명품이 일정 가격 이상으로 올랐을 때 투자자들에게 명품의 판매 여부를 조사하게 될 수 있다. 이때 스마트 컨트랙트를 통해 토큰 소유자들의 합의를 진행하게 된다면 빠르고 신뢰할 수 있는 의사 결정이 가능하다. 또한, 조각 투자에서는 조각 소유자들에게 일정 기간마다 자산으로부터 발생하는 수입을 분배해야 하는 경우도 존재한다. 부동산이나 미술품과 같은 자산의 경우 해당 자산을 대여해 줌으로써 부수적인 수입이 발생할 수 있다. 이러한 수입을 토큰 소유자들에게 분배하는 과정 역시 스마트 컨트랙트를 통해 진행할 경우 이점이 있다. 이처럼 실물 자산에 대한 NFT를 거래 할 때 필요한 부수적인 공정을 스마트 컨트랙트를 통해 처리함으로써 자동화하는 것이 가능하다.

Ⅲ. 결론 및 향후 연구

본 논문에서는 NFT 거래를 위한 블록체인 시스템에 대해 분석하기 위하여 가장 많은 NFT가 발행되고 있는 이더리움의 문제점에 대해 정리하고 이더리움이 가진 문제점을 해결하여 NFT 발행 플랫폼으로 사용되고 있는 솔라나와 폴리곤에 대해 소개하였다. 이더리움은 거래 처리속도와 높은 수수료 문제가 존재하며 솔라나와 폴리곤은 각각 새로운 블록체인 시스템을 개발하거나 이더리움의 레이어 2 네트워크를 통해 이 문제를 해결하였다. 그리고 본 논문에서는 스마트 컨트랙트 내에서 NFT 거래를 위해 필요한 요소를 분석하였다. 토큰 발행 단계에서 다양한 자산을 기반으로 하는 NFT 거래를 위해 NFT 조각화, 다중 NFT 발행 등의 기술이 필요하며 토큰을 소각하는 기능 역시 필요하다. 또한, NFT를 거래할 때 추가적으로 발생할 수 있는 공정 과정을 스마트 컨트랙트를 통해 자동화 하는 방안에 대해서도 제안하였다.

향후 연구에서는 이더리움 외에 다른 블록체인들이 사용하고 있는 서로 다른 스마트 컨트랙트들에 대해서 분석하고 NFT를 발행할 수 있는 블록체인들을 비교 분석할 계획이다. 또한 이를 바탕으로 다양한 자산에 대한 NFT를 거래할 수 있는 자동화된 플랫폼을 설계하고 구축하고자 한다.

ACKNOWLEDGMENT

본 연구는 ㈜코인원과 과학기술정보통신부 및 정보통신기획평가원의 대학 ICT 연구센터육성지원사업의 연구결과로 수행되었음 (IITP-2022-2017-0-01633)

참 고 문 헌

[1] Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." Ethereum project yellow paper 151.2014 (2014): 1-32.

[2] Buterin, Vitalik. "A next-generation smart contract and decentralized application platform." white paper 3.37 (2014).

[3] EIP-20: Token Standard. URL:https://eips.ethereum.org/EIPS/eip-20 (Accessed:04.08.2022).

[4] Wang, Qin, et al. "Non-fungible token (NFT): Overview, evaluation, opportunities and challenges." arXiv preprint arXiv:2105.07447 (2021).

[5] EIP-721: Non-Fungible Token Standard. URL:https://eips.ethereum.org/EIPS/eip-721 (Accessed:04.08.2022).

[6] Evans, Tonya M. "Cryptokitties, cryptography, and copyright." AIPLA QJ 47 (2019): 219.

[7] Tang, Huimin, Yong Shi, and Peiwu Dong. "Public blockchain evaluation using entropy and TOPSIS." Expert Systems with Applications 117 (2019): 204-210.

[8] Ekta Whitepaper. URL: https://whitepaper.ektaworld.io/ (Accessed:04.08.2022).

[9] Marchesi, Lodovica, et al. "Design patterns for gas optimization in ethereum." 2020 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE). IEEE, 2020.

[10] Gervais, Arthur, et al. "On the security and performance of proof of work blockchains." Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. 2016.

[11] King, Sunny, and Scott Nadal. "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake." self-published paper, August 19.1 (2012).

[12] Luu, Loi, et al. "A secure sharding protocol for open blockchains." Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. 2016.

[13] Yakovenko, Anatoly. "Solana: A new architecture for a high performance blockchain v0. 8.13." Whitepaper (2018).

[14] Solsea. URL: https://solsea.io/ (Accessed:04.08.2022).

[15] Polygon Lightpaper. URL:
https://polygon.technology/lightpaper-polygon.pdf
(Accessed:04.08.2022).

[16] OpenSea. URL: https://opensea.io/
(Accessed:04.08.2022).

[17] EIP-1155: Multi Token Standard.
URL:https://eips.ethereum.org/EIPS/eip-1155
(Accessed:04.08.2022).

이더리움 노드 탐색 프로토콜/v5의 와이어샤크 해석기 설계

류준형*, 주홍택

*계명대학교 컴퓨터공학과

*rjh6883@stu.kmu.ac.kr, juht@kmu.ac.kr

Wireshark Analyzer Design of Ethereum Node Discovery Protocol/v5

Junhyeong Ryu*, Hongteak Ju

*Dept. of Computer Engineering, Keimyung Univ.

요 약

본 논문은 이더리움의 P2P 네트워크를 구성하고 관리하는 노드 탐색 프로토콜의 와이어샤크 해석기 개발을 위한 설계 결과를 제시한다. 현재 이더리움의 노드 탐색 프로토콜은 버전 v5가 주로 사용되며 이전 버전인 v4에 비교하여 암호화가 적용된 것이 주요 특징 중의 하나이다. 따라서 기존 v4에서 개발되었던 와이어샤크의 노드 탐색 프로토콜/v4 해석기로는 더 이상 해석할 수 없어졌다. 본 논문은 노드 탐색 프로토콜/v5의 패킷 중 일부를 해석하는 방식과 결과를 제시한다. 본 연구의 결과는 이더리움 노드 탐색 프로토콜/v5의 와이어샤크 해석기 개발을 위한 사전 연구이다.

Ⅰ. 서 론

이더리움(Ethereum)은 Vitalik Buterin에 의해 2013년에 고안된 스마트 계약(smart contracts) 기능을 갖춘 분산형 오픈소스 블록체인이다.[1] 탈중앙화 애플리케이션을 구축하기 위한 대안 프로토콜로 만들어졌으며, 튜링-완전(Turing-complete) 프로그래밍 언어가 내장된 블록체인을 구축하여 누구나 스마트 계약을 작성 할 수 있다. 또한, 소유권과 트랜잭션 형식 및 상태 전환 기능에 대한 자체 임의 규칙을 만들 수 있는 분산 응용 프로그램을 배포할 수 있고, 사용자가 상호 작용할 수 있다.

이더리움은 현재 기술적인 도약을 진행하고 있으며 그 내용이 이더리움 2.0으로 표현되고 있다. 이더리움 2.0의 기술적 도약 중의 하나는 샤딩을 적용한 이더리움 P2P 네트워크의 수평적 확장이다. 이와 같은 이더리움 P2P 네트워크의 확장이 정상적으로 이루어지고 있는지 확인하기 위해서는 이더리움의 P2P 네트워크를 구성하고 관리하는 이더리움 노드 탐색 프로토콜(Ethereum Node Discovery Protocol)에 대한 분석이 이루어져야 하고 이 분석을 통하여 성능을 확인하고 성능 저하 요인이 있으면 이를 개선해야 한다. 프로토콜 분석을 위해서는 네트워크 패킷 데이터 분석 프로그램이 필요하다. 하지만 가장 대중적으로 많이 사용되는 와이어샤크(Wireshark)는 현재 이더리움 노드 탐색 프로토콜/v5를 지원하고 있지 않다. 프로토콜 v5는 이전 버전인 v4에 암호화가 적용되어 이전 버전의 해석기로는 일부분도 해석이 불가능하다.

이처럼 이더리움의 네트워크 확장에 따라 프로토콜을 분석하고 장애 파악이 필요하지만 기존 노드 탐색 프로토콜/v4에 맞춰서 개발된 와이어샤크 해석기는 노드 탐색 프로토콜/v5의 통신 과정 암호화로 인해 더 이상 사용할 수 없다.[2]

본 논문은 와이어샤크의 이더리움 노드 탐색 프로토콜/v5 해석기를 개발하기에 앞서 기술적 검토를 한 내용과 이를 적용하여 와이어샤크 이더리움 노드 탐색 프로토콜 해석기의 설계 결과를 제시한다. 기술적 검토로 이더리움 노드 탐색 프로토콜 패킷을 수집하여 노드 탐색 프로토콜의 규격에 맞게 수집된 패킷을 수작업으로 해석하는 과정과 해석 내용을 보여준다. 그리고 기술적 검토 내용을 기반으로 설계한 와이어샤크 이더리움 노드 탐색 프로토콜/v5의 와이어샤크 해석기 설계 결과를 제시한다.

본 연구는 이더리움 노드 탐색 프로토콜/v5의 해석기 개발에 관한 최초의 연구라는 학술적 가치가 있다. 우리는 본 연구의 결과를 바탕으로 와이어샤크의 이더리움 노드 탐색 프로토콜 해석기를 개발할 계획이다. 이 논문은 2장에서 이더리움 노드 탐색 프로토콜을 소개하고 v4 개발 결과를 제시한 연구 논문도 요약하여 제시한다. 3장에서는 기술 검토로 v5의 패킷을 수집하여 수작업으로 분석한 결과를 제시한다. 4장에서는 3장의 기술 검토와 이전에 개발한 v4의 해석기 개발 연구를 바탕으로 v5의 해석기 설계 결과를 제시한다.

Ⅱ. 관련 연구

2.1. 이더리움 노드 탐색 프로토콜/v5

노드 탐색 알고리즘의 패킷은 일반 메시지 패킷(Ordinary Message Packet), WHOAREYOU 패킷, 핸드셰이크(Handshake) 메시지 패킷으로 나뉜다. 각 패킷의 구조는 그림 1, 2, 3에서 보여준다.

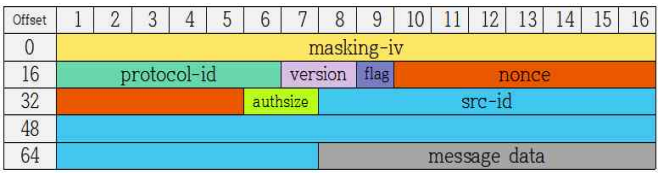


그림 1. Ordinary Message Packet 구조

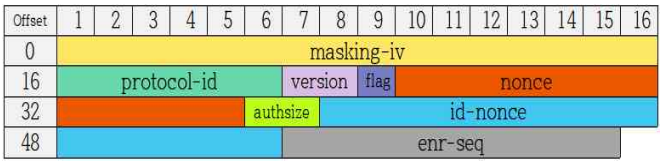


그림 2. WHOAREYOU Packet 구조

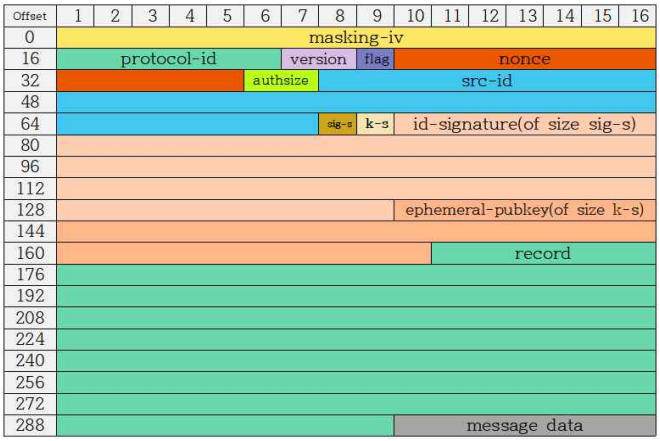


그림 3. Handshake Message Packet 구조

노드 탐색 프로토콜은 P2P(Peer-To-Peer) 네트워크에서 다른 이더리움 노드를 찾기 위한 통신 규약이다. 이더리움에서는 Kademlia기반의 노드 탐색 프로토콜을 사용하지만 일반적으로 사용하는 분산해시테이블(DHT)과 달리 임의의 키와 값을 저장하지 않고 대신 네트워크의 노드에 대한 정보를 제공하는 서명된 문서인 노드 레코드(Node Records)를 저장하고 중계한다. 기존 노드 탐색 프로토콜인 v4와 다른 주요한 특징은 노드 ID 암호화를 확장할 수 있으므로 secp256k1 키를 반드시 사용할 필요는 없어졌다는 점과 통신 과정이 암호화되어 기존 노드 탐색 프로토콜/v4에서 정적인 분석이 가능했던 것과 달리 수동적 관찰자로부터 topic 검색 및 record 조회를 보호한다는 점이다. 이를 위해 패킷의 헤더 부분은 암호화 해석을 위한 masking-iv 부분을 제외하고 AES-128-CTR로 암호화되어 전달되며 메시지 데이터 부분은 AES-128-GCM으로 암호화되어 전달된다. 패킷의 종류는 flag로 구분할 수 있는데 flag=0이면 Ordinary Message Packet이고 flag=1이면 WHOAREYOU Packet, flag=2이면 Handshake Message Packet이다.[3]

2.2 노드 탐색 프로토콜의 통신 과정

이더리움은 P2P(Peer-to-Peer) 네트워크를 통해 통신하며 그림 4와 같이 5단계 과정의 노드 탐색 프로토콜을 사용하여 노드(Node)를 탐색하고 피어(Peer)로 연결한다.

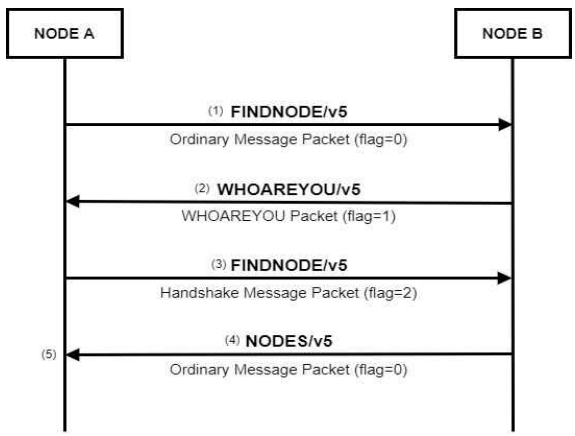


그림 4. 노드 탐색 프로토콜의 통신 과정

1단계는 노드 A가 노드 B와 통신하기 위해서는 노드 A와 노드 B의 노드 레코드의 복사본이 있어야 한다. 이때 노드 A와 B의 이전 통신에서 사용한 세션 키가 있는 경우에는 해당 키를 사용하여 요청을 암호화한다. 하지만 키를 알 수 없는 경우 임의의 메시지 내용이 포함된 일반 메시지 패킷(Ordinary Message Packet)을 전송하여 핸드셰이크(Handshake)를 시작한다.

2단계는 노드 B가 패킷을 수신하고 패킷 헤더에서 소스 노드 ID를 추출한다. 노드 B에 A와의 이전 통신의 세션 키가 있는 경우 메시지 데이터의 암호해독을 시작하고 메시지 복호화 및 인증이 성공하면 단순히 요청에 대한 응답을 보낸다. 노드 B에 세션 키가 없거나 암호해독에 성공하지 못한 경우 WHOAREYOU 패킷으로 응답하여 핸드셰이크를 진행한다.

3단계는 노드 A는 노드 B로부터 WHOAREYOU 패킷을 받고 핸드셰이크 메시지 패킷으로 FINDNODE를 재전송하여 핸드셰이크 과정을 진행한다.

4단계는 노드 B가 자신의 정적 개인 키와 핸드셰이크 패킷을 사용해서 세션 키를 생성하고 해당 키를 이용해서 패킷에 포함된 메시지의 암호를 해독한다. 이때 메시지가 해독되고 인증할 수 있는 경우 새 세션 키가 유효한 것으로 간주하고 NODES 패킷으로 응답한다.

5단계 노드 A는 NODES 패킷을 수신하고 새 세션 키로 이를 인증과 해독을 한 후 인증과 해독에 성공하면 노드 B의 ID가 확인되고 노드 A도 세션 키가 유효한 것으로 판단한 후 핸드셰이크 과정이 마무리된다.[3]

2.3. v4 해석기 개발 논문 요약 및 활용에 관한 의견

노드 탐색 프로토콜/v4에서 사용하는 패킷은 Ping(0x01), Pong(0x02), FindNode(0x03), Neighbors(0x04), ENRRequest(0x05), ENRResponse(0x06)로 총 6가지이다. 노드 탐색 프로토콜의 패킷 헤더는 Hash, Signature, Packet Type으로 구성되어 있다. Packet Type 필드는 메시지의 유형을 정의하는 단일 바이트 패킷이고 Ping 메시지부터 ENRResponse 메시지까지 순서대로 0x01부터 0x06까지의 값으로 필드가 정의되어 있다. 패킷 유형에 따라 메시지의 구조가 다르며 RLP (Recursive Length Prefix) 목록으로 인코딩된다. Neighbors 메시지의 경우 FindNode 메시지의 target ID에 가장 가까운 노드 16개의 정보를 rpcNode 데이터 구조로 응답하는데 rpcNode 필드가 가변적이기 때문에 이더리움의 RLP 디코딩 과정으로 얻은 필드의 길이에 맞게 해석해야 한다. 이후 해당 내용을 기반으로 와이어샤크 플러그인 해석기를 Lua 스크립트로 구현했다. Lua 스크립트에서는 이더리움 RLP 디코딩 과정을 통해 얻은 패킷의 길이에 맞춰서 각 패킷 필드의 길이에 맞춰서 잘라주는 방식으로 와이어샤크 해석기를 개발했다.[2]

노드 탐색 프로토콜/v5의 경우 패킷의 모든 내용이 암호화되어 있는데 암호화만 해석된다면 노드 탐색 프로토콜/v4와 유사한 방식으로 해석기를 만들 수 있다. 따라서 헤더는 AES-128-CTR, 메시지 데이터는 AES-128-GCM을 통해서 암호화를 해석한 후 v4 해석기 개발 방식과 유사하게 Lua 스크립트를 이용해 패킷 필드의 구조에 맞춰서 자르는 방식으로 와이어샤크 해석기를 개발할 수 있을 것이다.

Ⅲ. 노드 탐색 프로토콜 패킷 해석 과정 및 결과

3.1. AES-128-CTR MODE

이더리움 노드 탐색 프로토콜/v5에서는 사용자의 정적인 패킷 분석을 방지하기 위해서 대부분의 패킷의 헤더와 메시지 데이터를 암호화해서 전달한다. 이때 암호화 방식으로 빠른 속도와 보안성을 갖춘 암호화 알고리즘인 AES(Advanced Encryption Standard)를 사용한다. 이더리움의 헤더 부분은 이 중에서도 AES-128-CTR MODE를 사용하고 있다.

AES-128-CTR은 대칭 키 암호화 방식으로 암호화/복호화가 동일한 구조이며, 미리 정해진 IV(Initialization Vector)로 초기화된 카운터(Counter)를 정해진 규칙에 따라 값을 증가시키면서 AES를 통해 암호화하고 암호화된 결과를 평문과 XOR 연산해서 암호문을 생성하는 방식이다.[4]

따라서 패킷 분석을 위해서는 암호문(Ciphertext)과 암호화 시 사용했던 것과 동일한 IV와 Key를 이용하면 평문(Plaintext)을 얻을 수 있다.

3.2. IV(Initiallization Vector) 값 탐색 방법

이더리움의 패킷 암호화 시 사용하는 AES-128-CTR은 IV 값으로 각 패킷의 맨 앞부분 16바이트를 차지하는 masking-iv를 사용한다.

masking-iv는 암호화 해석을 위해서 암호화 없이 전달되기 때문에 와이어샤크를 통해 패킷을 캡처한 후 16바이트에 맞춰서 자른 후 사용하면 된다. 그림 5는 와이어샤크로 WHOAREYOU 패킷을 캡처한 것이다.

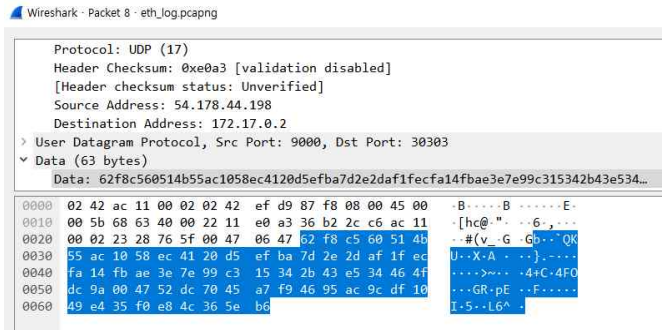


그림 5. 와이어샤크 WHOAREYOU 패킷 캡처본

3.3. KEY 값 탐색 방법

이더리움에서 AES-128-CTR 암호화의 키의 값은 dest-id[:16]으로 표현되어 있다. 이때 dest-id[:16]는 수신자가 자신의 노드 id 중 앞에서부터 16바이트를 dest-id로 사용을 의미한다. 따라서 자신의 노드 ID 파악을 위해 Geth-rpc에 admin.nodeInfo.id를 입력하면 자신의 노드 ID 전체 32바이트가 나오게 된다.[5] 그림 6은 Geth Rpc를 통해 자신의 노드 ID를 탐색한 결과이다.

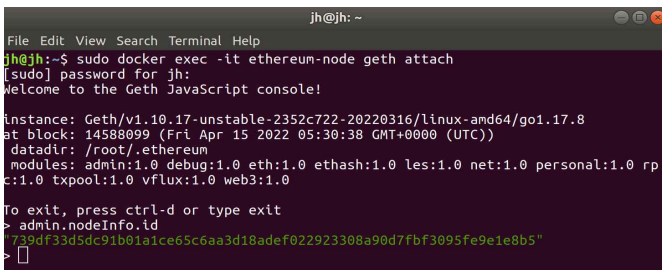


그림 6. Geth Rpc를 통한 자신의 노드 ID 탐색

3.4 구현 결과

이더리움의 노드 탐색 프로토콜 중 WHOAREYOU 패킷을 캡처해서 해당 부분을 분석해 보았다. 해당 방식을 통해 자신에게 들어오는 패킷은 모두 해석이 잘 되었다. 하지만 자신에게서 다른 노드로 보내는 패킷의 경우 해당 노드의 ID를 파악하지 못해서 해석하지 못했다. 그림 7은 그림 5에서 캡처한 WHOAREYOU 패킷의 헤더 부분의 HEX 값을 my.bin에 저장하고 해당 파일을 OpenSSL을 활용해서 해석한 내용이고 그림 8은 해석한 내용을 바탕으로 그림 2의 구조와 같이 분류한 후 출력한 내용이다.



그림 7. WHOAREYOU 패킷 해석 결과

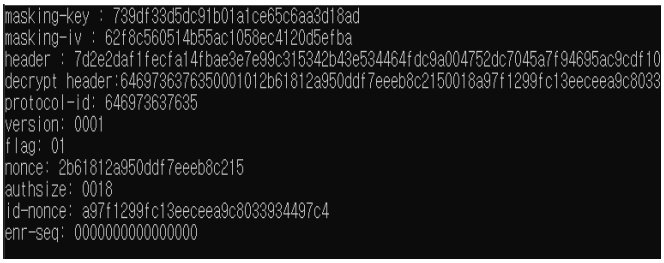


그림 8. WHOAREYOU 패킷 구조에 맞춘 해석 결과

Ⅳ. 와이어샤크 이더리움 노드 탐색 프로토콜/v5 해석기 설계

와이어샤크에서는 AES-128-CTR과 AES-128-GCM에 대해 해석 기능을 제공하고 있다. 해당 암호화를 해석하기 위해서는 와이어샤크의 ESP 프로토콜에 미리 해당 패킷에 대한 KEY, IV, 암호화 종류 등에 대한 정보를 입력해 두면 암호화를 해석할 수 있다. 그림 9는 와이어샤크에서 AES-128-CBC 암호화를 해석하는 방식이다.



그림 9. AES-128-CBC 암호화 해석 방식

AES-128-CTR과 AES-128-GCM의 경우 아직 성공하진 못하였지만 와이어샤크 공식 페이지에 해당 암호화 해석을 지원한다고 작성해 두었기 때문에 AES-128-CBC와 비슷한 방식을 통해 구현하면 해석이 가능할 것으로 판단된다. 이후 노드 탐색 프로토콜/v4와 동일한 방식으로 Lua 스크립트를 이용해 패킷의 필드를 구조에 맞게 자르는 방식으로 와이어샤크 노드 탐색 프로토콜/v5의 해석기를 개발할 수 있다.

Ⅴ. 결론 및 향후 연구

본 논문에서는 P2P 네트워크 향상을 위한 이더리움 노드 탐색 프로토콜/v5의 해석기 개발을 위한 통신 과정의 패킷 분석 과정과 와이어샤크 해석기의 설계를 제시했다.

또한 암호화되어서 볼 수 없었던 자신에게 들어온 패킷을 해석할 수 있게 했다. 하지만 자신이 다른 노드에 보낸 패킷은 dest-id를 파악하지 못해서 해석이 불가했다.

향후 연구로는 본 논문에서 제시한 해석 방식과 노드 탐색 프로토콜/v5

해석기 설계를 활용해서 와이어샤크를 통한 해석기로 개발할 계획이다. 또한 자신이 다른 노드에 보낸 패킷의 dest-id를 파악하지 못했는데 이를 버켓(k-bucket) 내부에 있는 dest-id를 찾은 후 자신이 다른 노드에 보내 패킷에 대한 해석기를 개발할 필요가 있다.

ACKNOWLEDGMENT

이 논문은 2018년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(NRF-2018R1D1A1B07050380).

참 고 문 헌

[1] Buterin, Vitalik,"A next-generation smart contract and decentralized application platform." white paper 3.37, 2014.

[2] 김정연, 주홍택, "이더리움 노드 탐색 프로토콜 분석을 위한 와이어샤크 해석기 개발", 통신망운용관리 학술대회(KNOM Conf. 2021), pp. 84-86, 2021.

[3] Ethereum Foundation, "Ethereum devp2p", 2022, (https://github.com/ethereum/devp2p).

[4] 박진형, 백정하, 이동훈, "모바일 환경을 위한 AES CTR Mode 의 효율적 구현." 정보보호학회논문지 21.5, pp. 47-58, 2011.

[5] Ethereum Foundation, "Ethereum Wiki", 2022, (https://eth.wiki/fundamentals/rlp).

KOREN에서의 블록체인 기반 계층적 콘텐츠 전달 및 검증

왈리드 아크바르, 디아즈 리베라 하비에르 호세, 아팍 모하마드, 칸 탈하 애흐마드, 송 왕 철
{waleedwali786, shaifvier, afaq24, talhajadun}@gmail.com, philo@jejunu.ac.kr

Blockchain-based Hierarchical Content Delivery and Verification in KOREN

Waleed Akbar, Javier Jose Diaz Rivera, Afaq Muhammad, Talha Ahmed Khan,
Wang-Cheol Song
Department of Computer Engineering, Jeju National University

Abstract

With the inception of blockchain technology, the industry utilizes blockchain in multiple domain applications to achieve its goals. The blockchain provides the level of security that most network applications require. Nowadays, blockchain is the backbone of many security applications, from the health care industry to the agriculture industry. In edge computing, distributed processing and storage arises new challenges for operators to validate the same information on distributed resources. One of the primary goals of edge computing is to provide updated content on all the edge servers. That means all users should receive the identical version of the content simultaneously. In this paper, our goal is to ensure that all the edges have similar content through the hash function of the blockchain. The edge device creates the hash of content and sends it to the blockchain to verify the latest version of the content. The smart contract matches the received hash value with the previously stored hash in the blockchain to verify content validity. We created the hierarchal edge content delivery network. The concept is implemented on KOREN-SDI to shows the deployment feasibility of the proposed methodology.

Ⅰ. Introduction

With the advancement of high-speed internet, more end-user applications require ultra-low latency and minor delay in this era. The network should have capabilities to fulfill these requirements. These requirements can be satisfied if the user request is accomplished from the edge. Generally, the edge stores the content copy and updates the content regularly. The problem is when to update the content. There are different possible ways to update the content, update periodically, update on user request, and immediate update. Each option has its advantages; updating periodically means the user gets the content after a specific time interval. If the interval is too small, the network overhead increases, but on the other side, the user delay decreases. Next, the immediate update means when there is an update on the data center, immediately update the content on edge. This option is suitable for fewer updates; otherwise, it will waste network bandwidth. Then, the update on user request means updating the content on edge when there is a request. The option is useful when few users are connected; otherwise, repeated requests are initiated from the edge. The most reasonable choice is based on application type and use-case scenario. The blockchain is a chain of blocks connected in a particular manner to provide the authenticity of data [4]. The critical attribute was the timestamp when block id is added because it can't be modified or removed once it is added; This is the immutable property of blockchain. The blockchain verifies the content version through the smart contract. Generally, it receives the hash of content and data-id to verify the hash already stored on the blockchain.

This manuscript is organized as follows. Section II describes the motivation with related work, section III explains the system design, the blockchain-based content validation with smart contract. The use case envionment with implementation detail is section V and section VI concludes the manuscript.

Ⅱ. Motivation and Related Work

The content update issue worsens in a multi-edge or hierarchical edge environment as there will be more edge devices and multiple data centers. Therefore, some mechanism is needed to ensure all the edge servers and da ta centers have a similar version of the content. Blockchain technology can securely verify the accuracy of

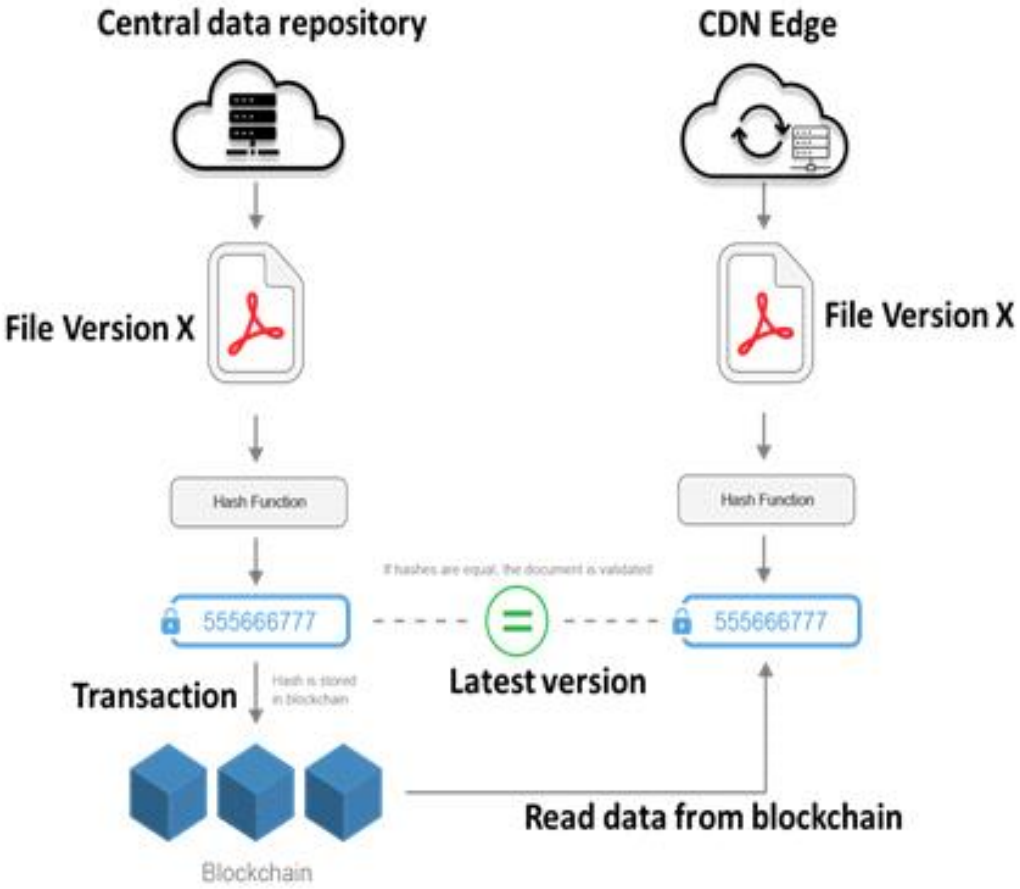


Figure 1: Content Verification using Blockchain

the content. Previously, the blockchain has been implemented in Content Delivey Network (CDN) scenarios for use cases such as DDoS attacks [1], content privacy [2], secure content delivery [3]. We provide a blockchain-based mechanism to ensure that the consumer data is accurate and has the latest version on all the devices. We propose a hash verification method in the blockchain to validate the data. This process assumes that the actual data is stored separately from the blockchain (data center or edge server) and then allows a data identifier and a checksum hash of data to be submitted to the blockchain. The blockchain is a public ledger used to record all the transactions in a decentralized data log rather than a physical ledger or a single database [7].

III. System Design

In the data center, a data repository consists of more than 1300 videos belonging to eight different categories. We build a content delivery environment that provides the capabilities to request content from the data repository. The communication link between user, edge, and data center is provided using File Transfer Protocols (FTP) . The data files stored in the central data repository are checksum hashed using standard methods (e.g., SHA256 checksum). These hashes for specific data files are transmitted to a blockchain (As a transaction). Along with this hash, we can store metadata, such as a timestamp and file size, as part of the transaction contents. This process is re-initiated whenever a change occurs, stowing the new hash on the blockchain. Once all hash is stowed in the blockchain, now the data content on the edge can be verified by sending the hash and data id to a blockchain.

IV. CDN Use Case Scenario

We verify the effectiveness of our proposed model by implementing it on the KOREN testbed [8]. KOREN topology is distributed all over Korea, making it suitable for edge and cloud use cases. As mentioned in the figure below, we can map a CDN Edge-based architecture on KOREN by utilizing distributed servers and arranging them in a central and edge logical manner. Blockchain is implemented using "Besu Hyperledger" tool [9]. When edge receive a request from the user, and if edge has the content, it verifies the version of content through the blockchain by sending the hash and data id. If the verification is successful, the content is provided to user. In case of failed verification or unavailability of content the edge forward the content request towards the data center for fulfillment. The data center provides the new version of content; upon receiving the content, the edge can verify the accuracy of content through the blockchain.

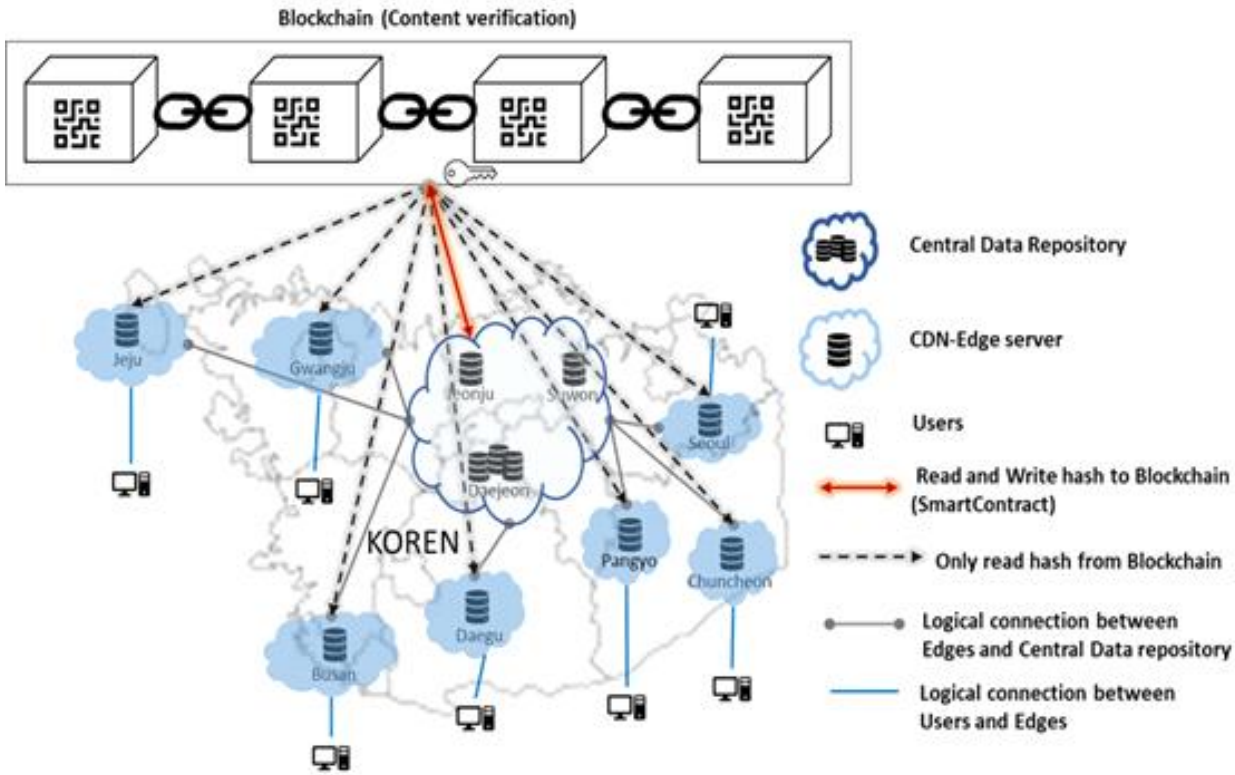


Figure 2: Use case scenario of proposed methodology

V. Conclusion

We design the content version control mechanism in a blockchain-based hierarchal edge environment. The content on edge verifies its validity by sending the hash and data-id to the blockchain. The smart contract on the blockchain is activated and verifies the accuracy of the hash value. When the user requests the content on edge, it proves the content validity through the blockchain. The edge sends the content hash and data-id for validation. This process ensures the validity of data on edge—the implementation on KOREN to verify our proposed system's effectiveness. We are able to achieve data validation and verification using blockchain with a smart contract.

ACKNOWLEDGMENT

This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2022-2017- 0-01683) supervised by the IITP (Institute for Information & communications Technology Planning & Evaluation). This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2016R1D1A1B01016322).

REFERENCES

[1] Kim, Kyoungmin, Youngin You, Mookyu Park, and Kyungho Lee. "Ddos mitigation: Decentralized cdn using private blockchain." In 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN), pp. 693-696. IEEE, 2018.

[2] Vu, Thang X., Symeon Chatzinotas, and Björn Ottersten. "Blockchain-based content delivery networks: Content transparency meets user privacy." In 2019 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1-6. IEEE, 2019.

[3] Conti, Mauro, P. Vinod, and Pier Paolo Tricomi. "Secure Static Content Delivery for CDN Using Blockchain Technology." In Data Privacy Management, Cryptocurrencies and Blockchain Technology, pp. 301-309. Springer, Cham, 2021.

[4] Nofer, Michael, Peter Gomber, Oliver Hinz, and Dirk Schiereck. "Blockchain." Business &Information Systems Engineering 59, no. 3 (2017): 183-187.

[5] Zolfaghari, Behrouz, Gautam Srivastava, Swapnoneel Roy, Hamid R. Nemati, Fatemeh Afghah, Takeshi Koshiba, Abolfazl Razi, Khodakhast Bibak, Pinaki Mitra, and Brijesh Kumar Rai. "Content delivery networks: State of the art, trends, and future roadmap." ACM Computing Surveys (CSUR) 53, no. 2 (2020): 1-34.

[6] Di Pierro, Massimo. "What is the blockchain?." Computing in Science &Engineering 19, no. 5 (2017): 92-95.

[7] Cachin, Christian. "Architecture of the hyperledger blockchain fabric." In Workshop on distributed cryptocurrencies and consensus ledgers, vol. 310, no. 4, pp. 1-4. 2016.

[8]https://www.koren.kr/eng/Intro/intro01.asp Accessed on 20-03-2022

[9] Li, Dongcheng, W. Eric Wong, and Jincui Guo. "A survey on blockchain for enterprise using hyperledger fabric and composer." In 2019 6th International Conference on Dependable Systems and Their Applications (DSA), pp. 71-80. IEEE, 2020.

대체 불가능 토큰을 활용한 메타버스 미디어 서비스 플랫폼 디자인

고경찬[*1], 유상우[2], 김호정[3], 홍원기[1]
[1]포항공과대학교 컴퓨터공학과
{kkc90, jwkhong}@postech.ac.kr
[2]포항공과대학교 인공지능대학원
rswoo@postech.ac.kr
[3]한양대학교 ERICA 글로벌 혁신 클러스터 센터
zczlf94@gmail.com

A Design on Metaverse Media Service Platform using Non-Fungible Token

Kyungchan Ko[*1], Sangwoo Ryu[2], Hojeong Kim[3], James Won-Ki Hong[1]
[1]Department of Computer Science and Engineering, POSTECH
[2]Graduate School of Artificial Intelligence, POSTECH
[3]Global Innovation Cluster Center, Hanyang University ERICA

요 약

새로운 차세대 플랫폼으로 메타버스가 주목받으면서 메타버스 플랫폼 내에서 사회 및 경제 활동이 더욱 활발해질 것으로 예상된다. 비대면 생활이 지속되면서 미디어 서비스에 대한 수요가 늘면서 미디어 콘텐츠 시장 규모도 더욱 커지고 있다. 이러한 흐름에서 앞으로 메타버스 플랫폼 내에서 미디어 서비스 사례들이 많이 생길 것이기 때문에, 메타버스 내에서 불법 미디어 유통 등이 없는 건전한 미디어 서비스 생태계를 구축할 필요가 있다. 본 연구에서는 블록체인 기반 대체 불가능 토큰이 미디어 저작물에 활용될 수 있는지 분석해보고, 이를 활용해서 메타버스 플랫폼 내에서 정당한 소유권이 보장된 미디어 서비스를 제공할 수 있도록 하는 새로운 메타버스 미디어 서비스 플랫폼을 제안한다.

I. 서 론

메타버스 [1]는 가상, 초월을 의미하는 '메타'(Meta)와 세계, 우주를 의미하는 '유니버스'(Universe)를 합성한 명칭이며, 3 차원에서 실제 생활과 법적으로 인정되는 활동인 직업, 금융, 학습 등이 연결된 가상 세계를 의미한다. 즉, 가상세계에서 신뢰가 보장된 체계 위해서 정체성을 가지고 사회적 활동과 경제 활동이 가능함을 의미한다. COVID-19 로 인해서 사람들의 대부분 활동 방식이 비대면으로 바뀌었다. 대면으로 교류하는 것이 힘들어졌기 때문에, 사람들은 온라인에서 현실과 같은 경험을 할 수 있는 대체 서비스에 대한 니즈가 높아졌다. 이러한 흐름이 메타버스가 차세대 플랫폼으로 주목받는 이유이다. 대표적인 메타버스 플랫폼으로 제페토(Zepeto) [3], 이프랜드(ifland) [4], 로블록스(Roblox) [5], 포트나이트(Fortnite) [6], 디센트럴랜드(Decentraland) [7], 샌드박스(Sandbox) [8] 등이 있다.

비대면 시대의 장기화로 미디어 서비스와 엔터테인먼트의 수요가 지속적으로 증가했고, 미디어 컨텐츠 관련 서비스 [9]가 메타버스 플랫폼 안에서 제공되기 시작했다. 향후 수많은 미디어 컨텐츠들이 메타버스 플랫폼으로 유입될 것이 예상되는 가운데, 기존 디지털 콘텐츠에서 발생하는 문제들이 그대로 메타버스에서도 문제가

될 가능성이 높다. 따라서 불법 복제 및 유통 등 기존 디지털 미디어 콘텐츠에서 발생하는 문제들을 유의해야한다. 최근 한국저작권보원에서 조사한 자료 [10]에 따르면, 저작권 보호 10 대 이슈 중에서 13.8%로 1 순위를 차지한 것이 '비대면 환경에서의 저작권 문제'이다.

본 연구에서는 메타버스 플랫폼에서 신뢰가 보장된 미디어 서비스를 제공할 수 있도록, 대체 불가능 토큰(NFT: Non-Fungible Token) [11] 기반의 메타버스 미디어 서비스 플랫폼을 제안한다. 블록체인 기반 대체 불가능 토큰을 이용해서 미디어 콘텐츠들에 대한 소유권을 증명해주고, 이를 통해서 미디어 서비스 제공자는 메타버스 플랫폼에서 콘텐츠에 대한 정당한 권리자임을 인증할 수 있다.

II. NFT 기반 미디어 저작물 관리

NFT 는 블록체인 기술을 기반으로 실물 및 디지털 자산의 소유주를 증명할 수 있는 크립토 토큰이다. NFT 는 자산에 대한 정보를 블록체인에 저장하여, 블록체인의 불가변성과 추적가능성 등의 특징을 통해서 해당 자산의 디지털 소유권을 구현한 것이다. 따라서, NFT 는 디지털 소유권에 기반한 다양한 분야로 확장가능하고, 미디어 저작물에도 적용이 가능하다.

미디어 저작물 자체를 블록체인 상에 직접적으로 저장하는 것이 아니라 저작물에 대한 메타데이터 정보(미디어 파일 설명, 미디어 파일 저장 URL 등)만 블록체인에 저장하고, 실제 파일은 저장소 URL 을 참조하여 얻을 수 있다. 그래서 데이터 크기에 관계없이 대부분의 디지털 파일은 NFT 로 만드는 것이 가능하다.

실제 미디어를 블록체인에 저장하지 않는 이유는 크기가 큰 파일을 블록체인에 저장하는 것이 효율적이지 않고 블록체인 네트워크에 큰 부담이 되기 때문이다. 그래서 실제 디지털 파일(미디어 저작물)과 메타데이터는 중앙 서버나 InternetPlanetary File System(IPFS) [12]에 저장한다. 하지만 중앙 서버와 IPFS 는 데이터의 영속성을 보장하지 않는다는 문제를 가지고 있다. 미디어 저작물을 NFT 기반으로 관리하기 위해서는 미디어 콘텐츠의 영속적인 데이터 저장을 지원해야하며, Filecoin [13], Storj [14], Pinata [15] 등의 플랫폼/서비스들을 활용할 수 있다.

III. NFT 를 활용한 메타버스 미디어 서비스 플랫폼

메타버스 환경에서 건전한 미디어 서비스 생태계를 구축하기 위해서, 제공되는 미디어 컨텐츠에 대한 신뢰가 필요하다. 이를 위해서 미디어 서비스를 제공하는 사용자가 해당 미디어 콘텐츠에 대해서 정당한 권리자라는 것을 증명할 수 있어야 하고, 부정한 서비스 제공자를 식별할 수 있어야 한다. 본 연구에서 제안하는 메타버스 미디어 서비스 플랫폼은 블록체인 기반 NFT 를 활용하여 미디어 콘텐츠에 신뢰를 부여할 수 있다. 그림 1 은 메타버스 미디어 서비스 플랫폼의 개념도를 보여준다. 해당 플랫폼은 여러 메타버스 플랫폼들의 연계를 위해서 중간 허브 역할을 수행한다.

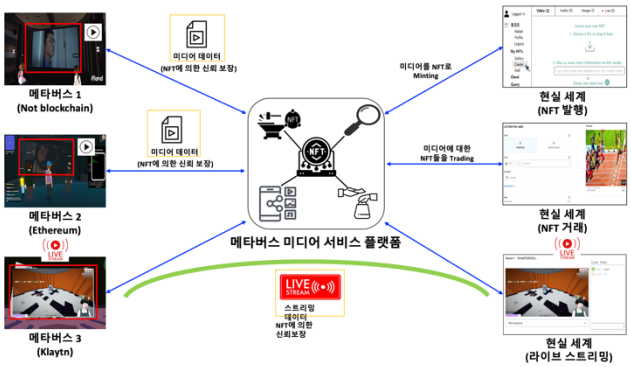


그림 1. 메타버스 미디어 서비스 플랫폼 개념도

본 플랫폼에서 다루는 미디어 유형은 이미지, 비디오, 오디오, 실시간 미디어 스트리밍이며, 제공하는 기능들은 다음과 같다.

① 사용자들이 새로운 미디어 NFT 를 발행할 수 있는 기능을 제공하고, 발행된 NFT 는 신뢰성을 보장함
② 사용자들이 보유하고 있는 신뢰가 보장된 NFT 들을 거래(판매 및 구매)할 수 있는 기능을 제공함
③ 신뢰성이 보장된 미디어 NFT 의 소유자에게 현실/메타버스에서 미디어를 업로드 및 재생할 수 있는 기능을 제공함
④ 실시간 미디어 스트리밍 채널을 NFT 로 관리하고, 어떠한 메타버스 플랫폼에서도 해당 채널에 접근하여 시청 가능함 (단, 채널에서 생성되는 미디어 콘텐츠는 채널 NFT 의 소유자만 NFT 로 발행 가능)

본 플랫폼에서 미디어 콘텐츠의 신뢰를 보장하기 위한 방법으로서 미디어 NFT 를 발행하여 해당 NFT 소유자만 현실 혹은 메타버스에서 실제 미디어 데이터를 요청 및 업로드 할 수 있도록 한다. 미디어 NFT 를 발행할 때 복제된 미디어들을 필터링 해주기 위해서, 해당 미디어 파일과 메타데이터를 '미디어 유사도 검사기'을 통해서 분석하여 현재 등록되어있는 다른 미디어 NFT 와 유사한 것이 있는지 확인한다. 유사도 검사를 수행하기 위해서는 NFT 데이터들이 필요한데, 블록체인 네트워크를 모니터링하여 NFT 관련 데이터를 모두 수집하고 데이터베이스에 저장한다. 이때, 하나의 블록체인만 모니터링하는게 아니라

여러 블록체인들(이더리움 [16], 폴리곤 [17], 클레이튼 [18] 등)을 모니터링한다.

미디어 유사도 검증을 통과하면, NFT 스마트 컨트랙트를 통해서 미디어 NFT 를 발행(Minting)해주게 된다. 이때, 실제 미디어 파일과 메타데이터는 영속 분산 스토리지에 저장하여 영구적으로 미디어 데이터를 보관할 수 있도록 한다.

메타버스 미디어 서비스 플랫폼에서 발행된 미디어 NFT 를 관리하게 되며, NFT 거래(구매/판매)도 지원한다. 사용자는 해당 플랫폼의 프론트앤드를 통해서 NFT 거래 스마트 컨트랙트에 접근할 수 있고, 판매 등록/경매 등록/구매 입찰 등의 기능을 이용할 수 있다. 또한, 메타버스 플랫폼들(Sandbox, Decentraland, Zepto 등)에서 서비스 제공자가 미디어 서비스(예: 메타버스 영화 상영관)를 제공하기 위해서 본 메타버스 미디어 서비스 플랫폼을 이용할 수 있다. 본 플랫폼의 API 게이트웨이를 통해서 미디어를 요청할 수 있는데, 이때 본 플랫폼은 미디어 NFT 인증을 수행하여 통과할 경우 실제 미디어 데이터를 전송해준다.

메타버스 미디어 서비스 플랫폼에서는 일반적인 미디어 뿐만 아니라 실시간 미디어 스트리밍도 제공한다. 본 플랫폼에서 실시간 미디어 스트리밍 채널 정보를 NFT 로 발행할 수 있다. 스트리밍 채널 NFT 의 소유자만 실시간 미디어 스트리밍을 시작할 수 있고, 해당 스트리밍을 통해서 생산된 미디어들을 추가적으로 미디어 NFT 로 제작할 수 있다. 이를 위해서 본 플랫폼은 스트림 키 발행기, NFT 검사기, 스트림 게이트웨이, 트랜스코더(Transcoder) 등의 모듈들이 구현된 실시간 스트리밍 서버를 별도로 운용한다. 그림 2 는 위에서 언급한 기능들이 표현된 NFT 를 활용한 메타버스 미디어 서비스 플랫폼의 아키텍처를 보여준다.

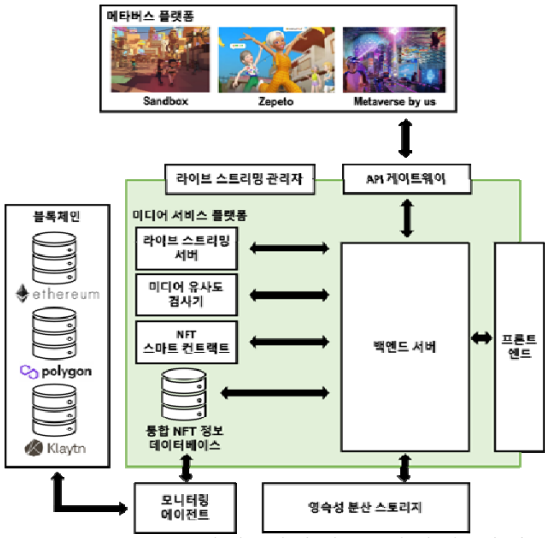


그림 2. NFT 기반 메타버스 미디어 서비스 플랫폼 아키텍처

그림 3 은 본 연구에서 제안하는 메타버스 미디어 서비스 플랫폼의 디자인이다. 해당 디자인 Application layer, Core layer, Storage layer 로 나눠진다. Application layer 는 해당 플랫폼을 이용할 수 있도록 기능을 제공하는 모듈들로 이루어져 있으며, API Gateway, NFT Media Service Front-end, Live Streaming Ingester 가 포함되어있다. Core layer 는 플랫폼에서 제공해야하는 핵심적인 기능을 처리해주는 모듈들로 이루어져 있다. NFT 관리를 위한 NFT smart contract, Media smart contract 가 있고, 신뢰 보장을 위해서 Media Checker 가 있다. 또한, 통합 NFT 데이터베이스 구축을 위한 Crawler 와 실시간 미디어 스트리밍 처리를 위한 Streaming processor 가 있다. Storage layer 에는 미디어 파일의 영구적인 저장을 위한 Permanent DB, 통합 NFT DB 와 여러 블록체인 플랫폼들로 구성된다.

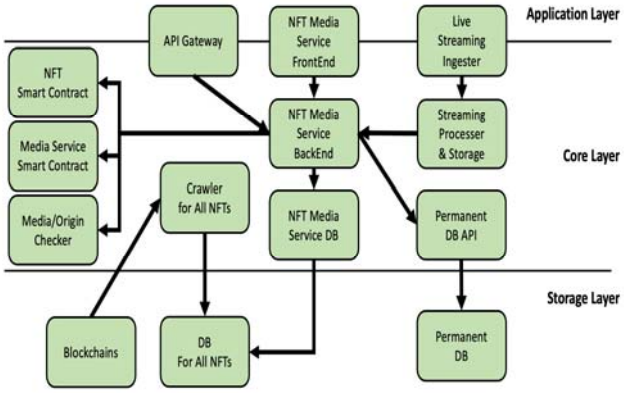


그림 3. NFT 기반 메타버스 미디어 서비스 플랫폼 디자인(High-level Design)

IV. 결론

본 연구에서는 메타버스 플랫폼 내에서 미디어 서비스를 제공할 때 발생할 수 있는 문제를 해결하기 위해서 NFT 를 활용한 메타버스 미디어 서비스 플랫폼을 제안한다. 본 연구를 통해서 NFT 를 활용하여 미디어 저작물을 관리할 수 있는지 그리고 적합한지를 분석하고, 해당 플랫폼에서 제공해야하는 기능들을 정의한다. NFT 기반 메타버스 미디어 서비스 플랫폼의 아키텍처와 디자인을 통해서, 플랫폼의 세부 내용들을 구체화시킨다. 향후 연구는 NFT 기반 메타버스 미디어 서비스 플랫폼을 실제로 개발하여 제안한 내용의 실현가능성을 확인하는 것이다.

ACKNOWLEDGMENT

본 연구는 (주)코인원의 지원과 과학기술정보통신부 및 정보통신기획평가원의 대학 ICT 연구센터육성지원사업의 연구결과로 수행되었음 (IITP-2022-2017-0-01633).

참 고 문 헌

[1] 메타버스 위키, https://en.wikipedia.org/wiki/Metaverse
[2] 한국일보, https://m.hankookilbo.com/News/Read/A2022020210050001429
[3] Zepeto, https://www.naverz-corp.com/
[4] ifland, https://ifland.io/
[5] Roblox, https://www.roblox.com/
[6] Fortnite, https://www.epicgames.com/fortnite/en-US/home
[7] Decentraland, https://decentraland.org/
[8] The SANDBOX, https://www.sandbox.game/ko/
[9] 경일매일, http://www.kmaeil.com/news/articleView.html?idxno=294035
[10] 2021 년 저작권 보호 10 대 이슈 전망, https://www.kcopa.or.kr/download.do?uuid=1347d22d-4bb5-431e-81a3-346ae6f987ce.pdf
[11] Wang, Qin, et al. "Non-fungible token (NFT): Overview, evaluation, opportunities and challenges." arXiv preprint arXiv:2105.07447 (2021).
[12] Benet, Juan. "Ipfs-content addressed, versioned, p2p file system." arXiv preprint arXiv:1407.3561 (2014).
[13] Filecoin, https://github.com/filecoin-project
[14] Storj, https://github.com/storj
[15] Pinata, https://www.pinata.cloud/
[16] Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." Ethereum project yellow paper 151.2014 (2014): 1-32.
[17] Polygon, https://github.com/maticnetwork/
[18] 서상민, et al. "클레이튼 블록체인 플랫폼의 고성능 합의 알고리즘." 한국통신학회지 (정보와통신) 37.3 (2020): 28-36.

TS5:
양자암호통신 및 차세대연구망

국가과학기술연구망에서의 양자키 분배 기반 하이브리드 TLS 암복호화 방안 연구

유기성, 김용환, 이원혁
한국과학기술정보연구원
{ksyu, yh.kim086, livezone}@kisti.re.kr

A hybrid transport layer security encryption and decryption method based on quantum key distribution in KREONET

Gi-Seong Yu, Yong-hwan Kim, Wonhyuk Lee
Korea Institute of Science and Technology Information

요 약

KISTI KREONET에서는 포스트 양자 시대를 대비하여 국가 중요 연구데이터를 물리적 기반의 양자암호기술인 양자키분배(QKD, quantum key distribution)를 이용하여 안전하게 전송・공유할 수 있는 차세대 국가연구망을 구축하고 양자암호키 서비스를 사용자에게 제공하기 위한 연구개발을 추진 중에 있다. 하지만 현재 QKD 시장이 상용화를 목전에 둔 반면 이와 관련된 국내외 표준 및 국내 보안 지침은 수립중인 단계이다. 이에 따라, 본 논문에서는 국가 양자암호통신 인증을 사전 대비하고 국가 중요 연구데이터를 안전하게 전송하기 위하여 QKD 기술을 기존의 국가정보원 검증필 암호 모듈(KCMVP, Korea Cryptographic Module Validation Program) 기반 암호화 알고리즘과 연계하여 하이브리드 형태의 TLS 암복호화 방안에 대하여 제시하고자 한다.

Ⅰ. 서 론

양자 컴퓨터의 발전에 따라 기존의 공개키 알고리즘이 취약해지면 기존 암호체계가 무력화되기 때문에 한국과학기술정보연구원 국가과학기술연구망 KREONET[1]에서는 양자암호기반 차세대 국가연구망 구축 기술개발 계획을 수립하고 국가 중요 연구데이터를 물리적 기반의 양자암호기술을 이용하여 안전하게 전송·공유할 수 있는 차세대 국가연구망 구축을 위한 연구개발을 추진 중에 있다.

KREONET에서 제공하는 양자암호통신 서비스는 공공기관의 정보시스템 안전성을 검증하는 보안적합성 등 당국의 보안 정책 및 제도에 부합해야 하며, 이에 따라 KREONET에서 소통되는 중요 정보인 연구데이터의 보호를 위해 검증필 암호 모듈(KCMVP, Korea Cryptographic Module Validation Program)을 적용할 필요가 있다. 한편, 비대면 환경이 점차 확산됨에 따라 보안을 강화한 양자암호통신 기술을 응용한 보안 서비스를 발굴하여 KREONET을 활용하는 다양한 사용자에게 안전한 데이터 전송을 보장해야 한다.

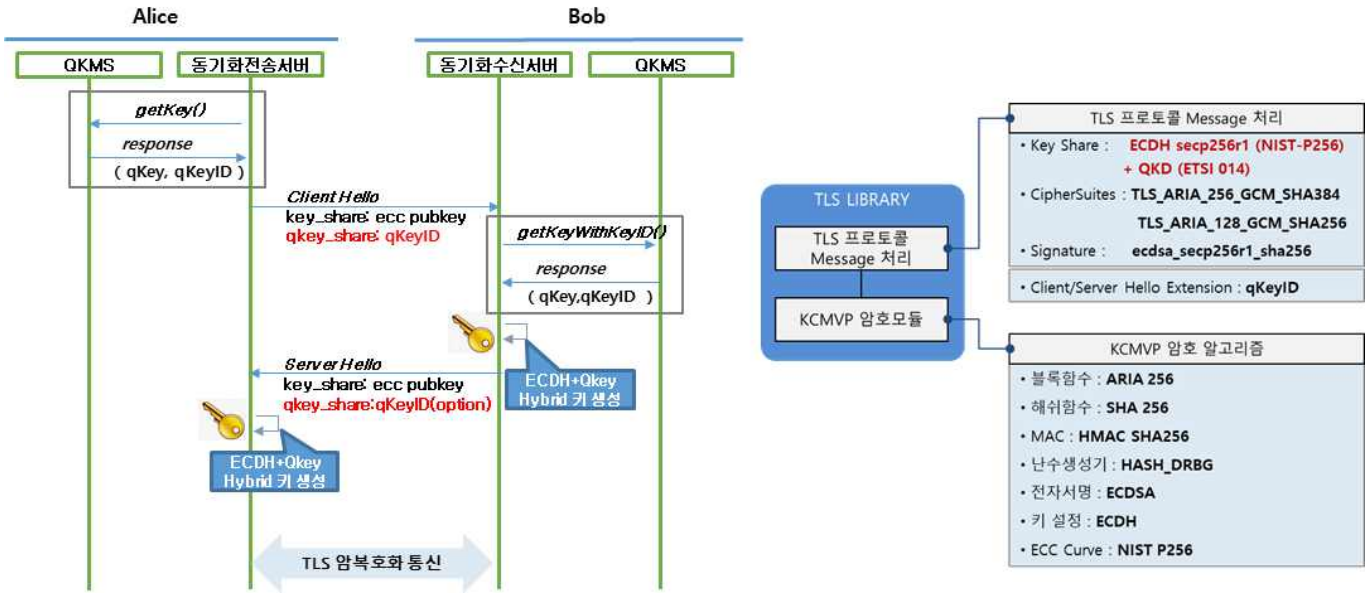
하지만 현재 QKD 시장이 상용화를 목전에 둔 반면 이와 관련된 국내외 표준 및 국내 보안 지침이 수립중인 단계이기 때문에 단번에 QKD 기술 기반의 암호체계를 구축하는데 무리가 있다. 이에 따라, 본 논문에서는 양자키 분배 기술(QKD, Quantum Key Distribution) 기반 양자암호통신망내의 개체 간 데이터 전송 보안 측면에서, 기존 보안 프로토콜을 대체하여 양자암호기술 기반의 고보안성을 보장하기 위하여 KCMVP와 QKD 기술을 결합한 이중 보안 체계의 네트워크 암호 기술인 하이브리드 형태의 전송계층보안(TLS, Transport Layer Security)암복호화 방안을 제안하고자 한다.

Ⅱ. 본론

본 논문에서는 TTA[2]와 ITU-T[3] 표준 문서에 따른 QKD 네트워크 계층, 키 관리 계층, 서비스(사용자) 계층으로 구성된 양자암호통신망 구조를 가정하며, TLS는 2020년에 개정된 1.3 버전의 TLS 프로토콜[4]을 가정한다. 또한 키관리 계층에서 QKD로부터 키를 받아 양자암호키 서비스에게 키를 제공하는 역할을 수행하는 양자키 관리 시스템(QKMS, Quantum Key Management System)과 TLS 사이의 통신은 ETSI 014 표준문서[5]를 따른다.

국가과학기술연구망의 인프라 및 서비스 요구사항에 부합하는 KREONET 양자암호통신망 응용 보안 서비스 환경을 제공하기 위하여 다음의 사항들을 중점적으로 고려할 필요가 있다.

- 표준화/정형화 : KREONET KMS과 연계한 TLS 기반 암호 라이브러리 개발을 위하여 표준문서(ETSI 014 등), 표준 기술 및 도구에 따른 표준화/정형화된 인터페이스/프로토콜 개발이 이뤄져야 함
- 보안성 : TLS v1.3 HandShake 과정에서의 송수신 서버 간, 송수신 서버와 KMS 간 인증 및 데이터 전송 과정에서의 보안이 준수되어야 하며, 국가정보원 검증필 암호모듈(KCMVP) 기반의 암호화 알고리즘 활용 등을 통한 고 수준의 보안성이 제공되어야 함
- 안정성 : 사용자 서비스는 상시 운용되어야 하므로 KMS 장애 혹은 양자 암호키(Q-Key) 부족에 따른 대처 방안이 마련되어야 함
- 확장성 : 양자암호통신 키관리 시스템과 연계한 TLS 기반 암호 라이브러리를 모듈화 형태의 개발을 통하여 이후의 확장성을 보장해야 함
- 호환성 : 상용 리눅스 운영체제 지원하며, 다양한 양자암호 응용서비스들과의 연계를 고려한 인터페이스 개발 및 인증 구성이 이뤄져야 함
- 상호독립성 : 양자암호통신망 구성요소 간의 의존 관계에 따른 기능 제약이 최소화되도록 하이브리드 TLS 암복호화 시스템이 개발되어야 함



(a) 하이브리드 TLS 프로토콜 (b) KCMVP 기반 TLS v1.3 알고리즘

그림 1. 하이브리드(QKD, KCMVP) TLS 암복호화 통신

본 논문에서는 하이브리드(QKD, KCMVP) TLS 암복호화 통신 프로토콜의 구현을 위하여 TLS 상에 동기화 전송 송수신 서버를 구축하였다. 그리고 하이브리드 TLS 암복호화 통신에서 활용하는 양자암호키를 획득하기 위하여 데이터 송수신 도메인에 QKD Alice, Bob을 구성하고 이를 QKMS와 연동한 후에 각각의 TLS 클라이언트/서버와 ETSI 014 표준에 따른 TLS 프로토콜 과정을 추가하였다. 또한 TLS 종단간의 양자암호키 설정을 위해 TLS 클라이언트/서버의 Hello 메시지에 양자키 정보 Extension 필드에 Q-Key Share Extension을 추가하고 해당 키의 식별자 정보(Q KEY SHARE(91) : native defined)를 수록하였다.

그림 1은 제안하는 하이브리드(QKD, KCMVP) TLS 암복호화 통신 과정을 보여준다. 그림 1(a)에서는 상세 TLS 프로토콜을 보여주며, 동기화 전송 서버와 동기화 수신 서버의 처리 절차는 아래와 같다. 그림 1(b)에서는 국내 보안 정책 및 제도에 부합하기 위하여 사용한 부분별 KCMVP 암호 모듈을 보여준다. 키 공유는 ECDH, 암호화 모음은 ARIA, 인증은 SHA에 기반한 KCMVP 암호 모듈을 선정하여 활용하였다.

● 동기화 전송 서버

1) KMS 연동하여 양자 암호키 수신
2) 양자암호키 ID 정보 포함하여 Client Hello 전송
3) Server Hello 수신 후 ECDH+Qkey Hybrid 키 생성
4) 이후 TLS 암복호화 통신 수행

● 동기화 수신 서버

1) Client Hello 에 포함된 양자 암호키 ID수신
2) 양자암호키를 KMS와 연동하여 수신한 양자 암호키 ID 에 해당하는 양자암호키 수신
3) ECDH+Qkey Hybrid 키 생성
4) Server Hello 전송
5) 이후 TLS 암복호화 통신

Ⅲ. 결론

본 논문에서는 양자암호기술 기반의 고보안성을 보장하기 위하여 KCMVP와 QKD 기술을 결합한 이중 보안 체계의 네트워크 암호 기술인 하이브리드 형태의 TLS 암복호화 방안에 대하여 제안하였다. 이를 통하여 포스트 양자 시대에 발맞추어 양자암호기술과 KCMVP 인증 모듈 결합을 통한 국가 양자암호통신 인증을 사전 대비하고 국가 중요 연구데이터를 안전하게 전송하는데 기여할 수 있기를 기대한다.

ACKNOWLEDGMENT

본 연구는 2022년도 한국과학기술정보연구원(KISTI) 주요 사업 과제로 수행한 것입니다

참 고 문 헌

[1] KREONET web site, from https://www.kreonet.net/, Retrieved 2021-04-05.

[2] TTA TTAK.KO-01.0214, “양자암호 전달 네트워크 기능구조”, Approved in 2019-12-11

[3] ITU-T Y.3800, “Overview on networks supporting quantum key,” Approved in 2019-10-25

[4] RFC 8446, “The Transport Layer Security (TLS) Protocol Version 1.3,” Retrieved 2020-03-07.

[5] ETSI GS QKD 014, “Protocol and data format of REST-based key delivery API,” Approved in 2019-02.

양자키 관리 네트워크에서의 양자내성암호 기반 데이터 송수신 구조 설계 연구

김용환, 심규석, 이원혁
한국과학기술정보연구원
{yh.kim086, kusuk007, livezone}@kisti.re.kr

A study on the design of data transmission structure based on post quantum cryptography in a quantum key management network

Yong-hwan Kim, Kyu-Seok Shim, Wonhyuk Lee
Korea Institute of Science and Technology Information

요 약

최근 양자컴퓨터의 발전으로 인해 공개키 기술을 기반으로 하는 암호체계에 대한 우려가 가속화되고 있으며, 이에 따라, 최근 양자키 분배 기술(QKD, Quantum Key Distribution)과 양자내성암호(PQC, Post Quantum Cryptography) 기술이 주목받고 있다. 포스트 양자 시대를 대비하는 QKD에 기반한 양자암호통신망을 구축함에 있어, 양자키 관리 네트워크의 액세스 구간의 통신은 양자 특성에 의하여 보호되는 QKD 계층과는 달리 현재의 통신 체계를 따르고 있으며 이는 보안취약점으로 작용할 수 있다. 본 논문에서는 이러한 QKD 기반의 양자암호통신망의 액세스 구간의 데이터 송수신 방식에 PQC 키 교환 메커니즘(KEM, Key Encapsulation Mechanism)을 양자키 관리 네트워크의 통신 체계에 접목하여 보안성을 강화할 수 있는 데이터 송수신 구조에 대하여 제안한다. 이러한 포스트 양자 시대를 대비하는 QKD와 PQC 기술의 결합을 통하여 각 기술이 지닌 한계를 극복하고 시너지를 낼 수 있기를 기대한다.

Ⅰ. 서 론

최근 양자컴퓨터의 발전으로 인해 공개키 기술을 기반으로 하는 암호체계에 대한 우려가 가속화되고 있다. 이러한 포스트 퀀텀 시대를 대비하기 위하여 대표적인 양자 암호 통신 기술로 양자키 분배 기술(QKD, Quantum Key Distribution), 양자내성암호(PQC, Post Quantum Cryptography) 기술이 등장했다.

QKD는 양자의 불확정성의 원리에 기반 한 양자키 분배 기술로 복제불가능성 원리와 측정 후 붕괴성질로 인해 단일광자를 정확하게 측정할 기회를 한 번으로 제한하여 수신자에게 도달하는 정보를 이용하여 공격자의 유무를 판단할 수 있다[1]. PQC는 양자 컴퓨터의 연산 능력으로 풀기 어려운 수학적 난제에 기반하여 설계되어, 정수를 기반으로 한 문제에 대해 뛰어난 성능을 보이는 양자 컴퓨터에 대해 다항 시간 내에 쉽게 해독되지 않을 것으로 기대되고 있다[2]. PQC는 크게 키 교환 메커니즘(KEM, Key Encapsulation Mechanism)과 전자서명으로 구분되며, 격자 기반(Lattice-based) 암호, 코드 기반(Code-based) 암호, 다변수 기반(Multivariate-based) 암호, 아이소제니 기반(Isogeny-based) 암호, 해시 기반(Hash-based) 서명 등이 있다.

QKD는 정보이론 측면에서 완전한 안전성 제공하나 고가의 전용 장비와 통신채널이 요구되는 등 기존 암호체계에서 전환하는 일이 쉽지 않은 반면, PQC는 기존 암호체계에서의 전환은 QKD에 비하여 용이하나 계산적 안전성 제공, 기반 문제 겨냥 새로운 양자 알고리즘 관련 잠재적 위협이 존재한다. 이에 따라, 최근 2가지 기술을 상호보완적으로 활용하는 연구들이 추진 중에 있다.

본 논문에서는 물리적인 양자 특성에 의하여 절대적인 보안 수준을 제공하는 QKD에 기반 한 양자암호통신망을 구축함에 있어, 네트워크 액세스 구간의 데이터 채널 암복호화에 PQC 기술을 적용하는 구조에 대한 연구이다. 이를 통하여 양자암호통신망 네트워크 오퍼레이터가 관리하지 않는 유저 종단까지 QKD를 배치함에 따른 다양한 관리 및 정책상의 이슈를 해결할 수 있으며, 새로운 양자암호통신망 전환에 소요되는 전반적인 구축비용을 절감할 수 있다.

Ⅱ. 본론

본 논문에서는 QKD 계층, 키 관리 계층, 서비스(사용자) 계층으로 구성된 국내외 QKD 기반 양자암호통신 네트워크 표준 문서[3, 4]를 준용한다. 이에 따르면, QKD 계층에서는 물리적인 양자 특성을 활용하여 양자키를 생성 및 분배하고, 키 관리 계층에서는 양자키 관리 시스템(QKMS, Quantum Key Management System)이 QKD로부터 양자키를 수신 및 관리하며, 암호모듈에 적절한 형태로 서비스 계층에 제공하고, 서비스 계층에서는 키 관리 계층에서 획득한 양자키를 활용하여 암호 서비스를 제공한다.

이 때, 양자키 전달을 위한 QKMS 사이의 코어 네트워크 구간은 QKD로부터 수신한 양자키를 활용하여 안전한 데이터 송수신 환경이 구성된다. 하지만 QKMS와 이를 수신하는 서비스/사용자 사이의 액세스 네트워크 구간은 서비스 대상이 되는 단말이나 서버까지 모두 QKD를 배치할 수 없기 때문에 ETSI 등의 표준문서[5]에서도 일반적인 TLS를 활용하여 데이터 송수신을 하게 된다. 이는 기존의 네트워크 환경에서 발생하는 통신의 보안성 이슈를 야기하기에 본 논문에서는 해당 TLS를 그대로 사용하는 것이 아닌 PQC KEM 기반의 새로운 양자내성 TLS를 구성함으로써 보안 이슈를 해결하고자 한다. 여기서 KEM은 공개키를 사용하여 대칭키를 안전하게 전송하기 위한 키 교환 기술이며, TLS는 최근에 개정된 TLS

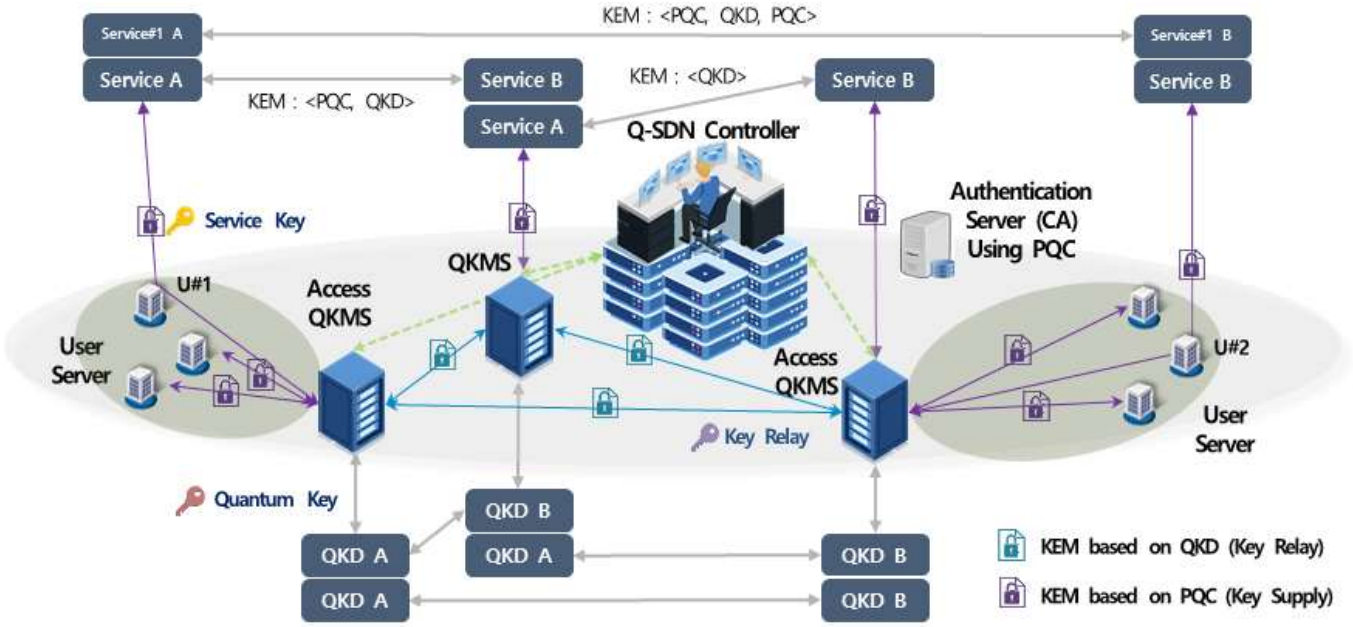


그림 1. 양자키 관리 네트워크 데이터 송수신 구조

1.3 프로토콜[6]을 대상으로 한다.

한편, QKD 기반 양자암호통신망내의 개체 간 데이터 전송 보안 측면에서, 기존 보안 프로토콜을 대체하여 양자암호기술 기반의 고보안성을 보장하기 위하여 현재의 암호 기술과 양자 기반 암호 기술을 결합한 이중 보안 체계의 네트워크 암호 기술 개발이 요구된다. 또한 국가 양자암호통신 인증 측면에서도 TLS에 PQC KEM만을 적용하기 보다는 PQC KEM 알고리즘과 국가정보원 검증필 암호 모듈(KCMVP, Korea Cryptographic Module Validation Program) 기반 암호화 알고리즘 모듈을 결합하여 사용하는 하이브리드 형태의 TLS 프로토콜 구성이 요구된다.

그림 1은 이러한 QKD 기반의 양자암호통신망에서의 양자키 관리 네트워크 데이터 송수신 구조를 보인다. 양자키 전달을 목적으로 한 QKMS 사이의 데이터 송수신은 QKD 기반의 XOR 연산을 통하여 엄밀한 형태의 데이터 안전성을 보장하는 한편, 직접적인 QKD 인프라를 구축하기 어려운 서비스 단말과 Access QKMS 사이의 데이터 송수신은 위에서 제안한 KCMVP 암호화 모듈과 PQC KEM이 결합된 하이브리드 TLS 프로토폴을 활용하여 데이터 안전성을 보장한다.

그리고 이 때, 기존 QKMS의 변경을 최소화하는 양자암호 응용서비스 연계 지원 형태의 양자내성 TLS V1.3 보안 암·복호화를 수행하고 양자암호통신망 구성요소 간 독립성을 보장할 필요가 있다. 이를 위하여, Access QKMS 앞단에 TLS 전송을 위한 프록시를 설정하여 Access QKMS가 QKD 기반의 데이터 송수신과 PQC 기반의 데이터 송수신 요청에 따른 TLS 설정 및 제어를 대행하도록 한다.

Ⅲ. 결론

본 논문에서는 QKD에 기반 한 양자암호통신망을 구축함에 있어, 양자암호통신망의 액세스 구간의 데이터 송수신 방식에 PQC 키 교환 메커니즘을 양자키 관리 네트워크의 통신 체계에 접목하여 보안성을 강화할 수 있는 데이터 송수신 구조에 대하여 제안하였다. 그리고, 이 때 기존 보안 프로토콜을 대체하여 양자기술 기반의 고보안성을 보장하기 위하여 KCMVP 암호 기술과 양자 기반 암호 기술을 결합한 이중 보안 체계의 데이터 송수신 구조를 제안하였다. 이러한 포스트 양자 시대를 대비하는 QKD와 PQC 기술의 결합, 그리고 현재의 KCMVP 인증 암호 기술의 결합 등을 통하여 각 기술이 지닌 한계를 극복하고 상호 시너지를 낼 수 있기를 기대한다.

ACKNOWLEDGMENT

본 연구는 2022년도 한국과학기술정보연구원(KISTI) 주요 사업 과제로 수행한 것입니다.

참 고 문 헌

[1] Scarani, Valerio, et al. "The security of practical quantum key distribution." Reviews of modern physics 81.3 (2009): 1301.

[2] Bernstein, Daniel J., and Tanja Lange. "Post-quantum cryptography." Nature 549.7671 (2017): 188-194.

[3] TTA TTAK.KO-01.0214, “양자암호 전달 네트워크 기능구조”, Approved in 2019-12-11

[4] ITU-T Y.3800, “Overview on networks supporting quantum key,” Approved in 2019-10-25

[5] ETSI GS QKD 014, “Protocol and data format of REST-based key delivery API,” Approved in 2019-02.

[6] RFC 8446, “The Transport Layer Security (TLS) Protocol Version 1.3,” Retrieved 2020-03-07.

네트워크 보안향상을 위한 QKD 및 PQC 를 이용한 KREONET 양자암호통신망 설계

심규석, 김용환, 이원혁
한국과학기술정보연구원

{kusuk007, yh.kim086, livezone}@kisti.re.kr

Design of KREONET Quantum Cryptographic Communication using QKD and PQC for Improving Network Security

Kyu-Seok Shim, Yonghwan Kim, Wonhyuk Lee
Korea Institute of Science and Technology Information

요 약

최근 양자컴퓨터 개발이 활발해지면서 기존 네트워크 암호체계가 위협받고 있다. 대표적으로 양자컴퓨터에서 운영될 수 있는 Shor 알고리즘은 기존 네트워크 공개키 기반 암호체계를 단시간에 풀 수 있다고 증명되었다. 따라서 새로운 암호체계 연구가 활발해지고 있는 가운데 가장 유력한 암호체계는 Quantum Key Distribution(QKD)와 Post Quantum Cryptograph(PQC)이다. 본 논문에서는 QKD 와 PQC 를 중심으로 네트워크망을 구성하고, 이를 효율적으로 운영하기 위한 Quantum Key Management System(QKMS)와 Q-Controller 를 제안한다. 제안하는 양자암호통신망은 QKD 로 백본을 구성하고 유저단은 PQC 로 대체하여 단점을 극복하고, QKMS 와 Q-Controller 를 이용하여 효율적인 네트워크 자원관리를 할 수 있다. 본 논문에서는 QKMS 와 Q-Controller 의 역할 및 기능에 대해 정의하고, 이들로 구성된 양자암호통신망을 제안한다.

Ⅰ. 서 론

오늘날 양자컴퓨터의 개발로 인해 기존 네트워크 보안 방식이 위협받고 있다. 양자컴퓨터로 수행할 수 있는 Shor 알고리즘은 RSA 공개키 암호화방식의 보안을 빠른 시간내에 위협할 수 있다. 따라서 기존 네트워크 보안 방식의 향상 및 양자컴퓨터로 인한 네트워크 위협을 방지하기 위해 QKD 및 PQC 에 대한 연구가 진행되고 있다. QKD 는 양자적 특성을 이용하여 키를 분배하는 과정에서 도청자에 의해 도청이 되는 경우를 탐지할 수 있기 때문에 가장 유력한 보안 방법이다. PQC 는 기존 알고리즘을 향상하여 기존보다 계산복잡도를 증가시켜 양자컴퓨터로 네트워크 보안 위협하는 것을 방지하는 방법이다.

QKD 는 다양한 연구 끝에 양자컴퓨터로부터 안전하다는 것이 증명되었고, 따라서 다양한 프로토콜의 QKD 방안이 연구되고 있다. QKD 는 안정화된 통신을 제공할 수 있지만, 네트워크를 구성하기에는 구축비용이 비싸고, 거리의 한계가 있고, 1:1 통신만 가능하다는 단점이 있다. 이러한 단점으로 인해 전국적인 네트워크망을 QKD 로 구성하는 것은 불가능하다. 이러한 QKD 의 단점을 해결하고, 기존 구축 되어있는 네트워크망을 사용하며 양자컴퓨터의 보안 위협으로부터 예방하기 위해 PQC 분야가 연구되고 있다. PQC 는 기존 알고리즘에서 계산복잡도를 증가시키거나 새로운 암호화 알고리즘을 개발하여 양자컴퓨터에서 수행되는 알고리즘으로 암호화된 데이터를 해독할 수 없도록 연구되고 있다. 그러나 현재까지 PQC 는 계산복잡도를 높이면서 시간복잡도도 높아지기 때문에 암호화 및 복호화에 소요되는 시간이 많이 걸린다는 단점이 있다.

따라서 본 논문에서는 QKD 와 PQC 를 결합한 네트워크망을 설계하여 QKD 의 장점과 PQC 의 장점을 이용한 네트워크 구조를 제안한다. 해당 네트워크 구조는 KREONET 을 모델로 구성하였으며, 향후 적용할 계획이다. 그러나 QKD 와 PQC 만으로 양자컴퓨터에 안전한 네트워크망을 설계하기에는 많은 한계가 있다. 특히 QKD 는 1:1 통신이라는 특성과 통신거리가 짧기 때문에 네트워크망을 설계하는 것은 매우 많은 비용이 소모된다. 따라서 QKMS 및 Q-Controller 시스템을 적용한 QKD 네트워크 구조를 제안한다. QKMS 는 QKD 로부터 대칭키를 수신하여 암호화가 필요한 서비스에 키를 제공하는 역할을 한다. 이 과정에서 QKMS 는 QKD 로부터 수신 받는 대칭키를 효율적으로 사용하기 위해 서비스키를 만들고, 이러한 키들을 관리하기 위해 키의 생애주기를 관리한다. 또한 QKMS 는 키전달을 가능하게 함으로써 거리한계를 극복한다. Q-Controller 는 키 전달 및 QKMS 들을 관리하는 역할을 수행한다.

Ⅱ. 본론

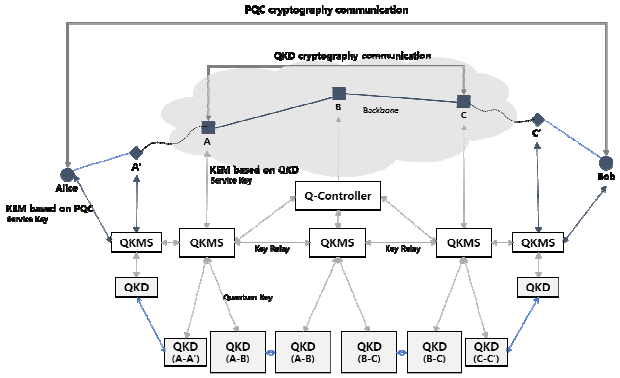
본논문에서 제안하는 양자암호통신망에서 QKMS 와 Q-Controller 는 매우 필수적인 구성요소이다. QKMS 는 QKD 로부터 대칭키를 수신 받아 효율적인 키 사용률을 위해 서비스키를 생성하고, 서비스 보안요구사항에 적합한 키를 제공한다. 또한, QKD 장거리 통신을 위해

키 전달 기능을 수행하고, 안정적인 암호화 서비스를 위한 키 관리 역할을 수행한다. QKMS 의 필수구성요소는 KMA, KSA, KRA 이다. KMA 는 QKD 로부터 대칭키를 수신 받고, 효율적인 키 사용을 위해 키 리포맷을 수행하는 모듈이다. 또한 키의 생애주기 관리를 통해 저장공간 확보 및 키 동기화 시 오류율을 감소시키는 기능을 수행해야한다. KMA 에서 수행하는 기능을 안정적으로 제공하기 위해 QKD Protocol Abstraction Layer 에서는 다양한 종류의 QKD 에서 생성되는 키들을 수신 받기 위해 Adapter 역할을 해야 하고, QKDE Manager 모듈은 QKD 와 관련된 정보를 수신하여 안정적인 네트워크를 유지할 수 있다. 이때 어댑터는 안정적인 키 수신을 위해 ETSI QKD 014 표준 기반 키 수신 프로토콜을 구성해야 한다. KSA 는 서비스 보안요구사항에 적합한 키를 제공하는 모듈이다. 서비스 보안요구사항에 적합한 키를 제공하기 위해서는 NE Protocol abstraction layer 를 통해 다양한 서비스를 지원할 수 있도록 설계되어야 하고, 서비스키와 관련된 모든 작업을 수행해야한다. 마지막으로 KRA 는 장거리 양자암호통신을 위한 키 전달을 위한 모듈이다. 효율적인 키 전달을 위해서 KRA 는 QKMS Manager 를 통해 구성요소 및 토폴로지 상태를 조회하여 키 전달 경로를 설정해야 한다.

Q-Controller 는 QKMS 와 QKD 로 구성되는 양자암호통신망의 전체적인 관리 역할을 수행한다. Q-Controller 는 양자암호통신망 내 QKD 에서 생성되는 양자키 뿐만 아니라 QKMS 에서 생성되는 서비스키를 관리하기 위한 기능을 수행하고, 양자암호통신망을 구성하는 구성장비 및 채널상태를 관리한다. 또한 각 장비의 성능을 모니터링하여 원활한 양자암호통신망을 구성할 수 있는 역할을 수행하며, 각 장비들을 관리하는 만큼 장애가 발생하였을 때 대처 및 알림 역할을 수행한다. Q-Controller 는 QKDN Manager, Key Relay Manager, Topology Manager, State Manager 등 4 가지 모듈로 구성한다. QKDN Manager 모듈은 QKDN 을 구성하는 구성 장비를 관리하고, 실시간 상태 정보 조회를 위해 라이브 업데이트 기능을 수행하며, 상태 정보 조회 시 장애, 성능, 키상태에 대해 조회할 수 있는 기능을 수행한다. 또한, 키 관리망에서 정책을 설정할 수 있고, 현재 상태를 조회하는 기능을 수행한다. Topology Manager 는 양자암호통신망의 토폴로지 상태를 조회 및 관리하여 QKMS 간 키 전달할 때 최적의 경로를 찾아 효율적인 키 전달을 가능하게 한다. 키 전달 기능을 효율적으로 수행하기 위해서 Key Relay Manager 는 QKMS 로부터 키 생성 상태를 조회하여 관리하고, 전달 경로를 탐색하여 생성하고, 전달 경로에서 장애 발생에 대처하기 위해 대체경로를 생성한다. 마지막으로 State Manager 는 양자암호통신망 구성요소에서 장애가 발생하였을 때, 장애에 대한 알림을 수신하고 처리하는 역할을 하고, 키상태 및 성능 정보를 수신한다.

국가 과학기술연구망 기반 양자암호통신망은 앞서 다룬 내용인 QKD, PQC, QKMS, 그리고 Q-Controller 등으로 구성된 암호통신구조를 제안한다. 과학기술연구망은 국내에 17 개의 지역망 센터를 중심으로 Backbone 구간이 설계 되어있다. 또한 각 지역망으로부터 유저까지의 연결이 되어있기 때문에 향후 과학기술연구망 기반 양자암호통신망 구축을 위해 User 간 연결까지의 보안향상을 위한 설계가 진행되어야한다. 따라서 본 논문은 과학기술연구망 기반 양자암호통신망 구축을 위해 QKD, PQC, QKMS, 그리고 Q-Controller 등으로 구성한 네트워크 구조를 설계하였다.

다음 그림은 국가 과학기술연구망 기반 양자암호통신망 설계 내용이다. 다음 그림과 같이 백본구간, 백본과 기관과의 구간 등은 비용은 높지만 안정성은 높인 QKD 로 설계되고, 기관과 유저구간은 안정성은 QKD 보다 낮지만 기존 네트워크를 이용할 수 있고, 설계 비용이 낮은 PQC 로 설계된다. QKD 와 PQC 의 효율적인 연동 및 QKD 에서 분배되는 키들을 효율적으로 관리하기 위해 QKMS 를 구성하고, 양자암호통신망에 전체적인 구성을 위해 Q-Controller 를 구성한다.



Ⅲ. 결론

본논문에서는 QKD, PQC, QKMS, Q-Controller 로 구성된 국가 과학기술연구망 기반 양자암호통신망을 제안하였다. QKD 의 단점을 해결하여 유저와 유저간 양자키로 암호화된 네트워크 통신이 가능하도록 설계하였으며, 안정성을 높이기 위해 PQC 알고리즘을 사용하는 방안을 제안하였다.

향후연구로는 실제 QKD 를 QKMS 와 연동하고, 3 개이상의 도메인에 설치된 QKMS 를 Q-Controller 와 연동하여 실험망을 구성할 예정이다.

ACKNOWLEDGMENT

본 연구는 2022 년도 한국과학기술정보연구원(KISTI) 주요 사업 과제로 수행한 것입니다.

참 고 문 헌

[1] 이원혁, 석우진, 박찬진, 권우창, 손일권, 김승해, 박병연, “양자암호기반의 통신망 구축 및 성능시험 검증연구”. KNOM Review, 2019, vol.22, No.02, pp39-47

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum Cryptography,” Rev. Mod. Phys., Vol.74, No.1, 2002, p.145

[3] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus,“Field test of quantum key distribution in the Tokyo QKD Network”, Optics Express, Vol 19, Issue 11, 2011

양자암호통신망에서의 안전하고 효율적인 양자키 전달 모듈 구현 연구

이원혁

한국과학기술정보연구원

livezone@kisti.re.kr

A Study on the Implementation of Quantum Key Relay based on QKD Network

Wonhyuk lee

Korea Institute of Science & Technology Information

요 약

본 논문은 양자 정보분야에서는 꽤 보편적으로 사용가능한 어플리케이션인 양자키 전달에 대한 연구를 수행하였으며, ETSI나 ITU-T 등의 표준화 문서에서 진행한 표준제안을 활용하여 양자키를 안전하고 효율적으로 전달하기 위한 모듈을 개발 연구하였다.

Ⅰ. 서 론

최근 양자암호통신망이 확대되면서, 국가적으로도 여러 중요 연구분야에서 적용이 이루어지고 있다. 가장 중요한 민감정보 중의 하나인 의료분야에서 특히 많은 적용이 이루어지고 있는데, 블록체인기반의 실손보험청구를 위한 병원간의 진료기록과 보험사간의 전송시에 활용하는 사례가 있다. 또한 의료진의 음성을 인식하여 AI로 자동 저장된 전자진료차트를 데이터센터로 보내는 곳에도 병원과 데이터센터간의 통신에도 활용되는 사례도 있다. 또한 대기업 본사의 IDC센터 업무서버와 스마트오피스간의 주요 기밀업무 수행시에도 산업적으로 활용되는 사례가 있다. 과학기술분야에서도 국가적으로 중요한 연구데이터 및 민감데이터를 전송 공유시에도 활용하기도 하고 있다. 하지만, 현재 양자암호통신망 사례에서 상당부분이 단대단 양자키분배 기반에 기반하고 있으며, 확장성을 위한 효율적인 키 분배가 필요한 시점이다. 본 논문에서는 양자암호통신망에서 3개 이상의 상호 연결된 양자암호통신망 상에서 안전하고, 효율적인 양자키 전달을 위한 양자키 전달 모듈의 구현을 위한 연구를 수행하고자 한다.

Ⅱ. 관련 연구

양자키분배(QKD) 기술은 상용 장비가 출시되어 서비스 구축을 수행하고 있는 상황이며, 양자 정보분야에서는 꽤 보편적으로 사용가능한 어플리케이션이다. ETSI나 ITU-T 등의 표준화 문서에서도 양자키 전달을 위한 표준 제안을 진행하고 있으며, 이를 이용하여 구현하는 사용 장비도 존재한다. 물론 분산된 다중 얽힘을 이용하여 얽힘 스와핑으로 거리를 연장할 수 있는 양자물리학에 기반하는 것이 필요하나, 현재까지 이러한 방식으로 구현가능한 양자키분배 신뢰노드는 전무하다 할 수 있으므로, 현실적으로 적용가능한 양자키 전달을 위한 신뢰노드 연구가 수행되고 있으며, 본 논문에서도 이러한 사례와 표준화 연구를 바탕으로 양자키를 안전하고 효율적으로 전달하기 위한 모듈을 개발 연구하고자 한다.

Ⅲ. 양자키 전달 모듈 설계 연구

3.1. 양자키 전달 모듈 주요 기능 정의

양자키 전달을 위하여 현재 사용하고 있는 양자키분배장비(QKD)는 현재 전송거리에 한계가 존재하기 때문에, 이를 극복하기 위한 키전달 메커니즘을 사용한다. 물론 양자물리학적으로 MDI-QKD등과 같은 중간지의 측정에 무관한 안정성을 유지하기 위한 양자키분배장비가 연구되고는 있으나, 현재 사용되고 있는 DV-QKD는 단대단 동작과정을 거치기 때문에, 중간지에 위치한 곳에서 신뢰노드(Trusted Node)라는 개념으로 키의 전달 연속성을 수행하는 방식으로 진행되고 있다.

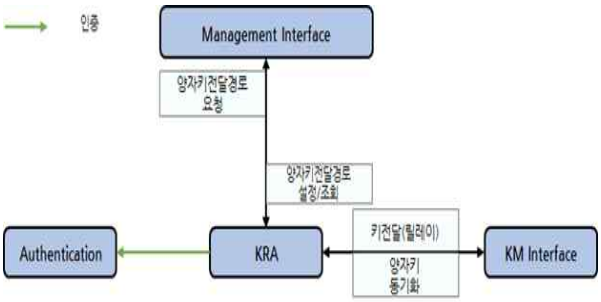
[표 1] 양자키 전달 모듈 주요기능 정의

기능	설명
초기화	KRA 블록 초기화 기능
키 전달경로 설정/조회	QKMS간 키 전달을 위한 경로 설정/조회 및 키 전달 경로 정보 설정/조회/삭제
키 전달 경로 요청	QKMS간 키 전달을 위한 키 전달경로 요청
양자키 생성	RNG에서 양자(대체)키 생성
키 리포멧	RNG에서 생성한 양자(대체)키를 양자키 관리정책에 따라 분할
키 전달 (릴레이)	QKMS간 키 전달(릴레이) 수행
양자키 동기화 (릴레이)	키 전달(릴레이)을 통해 수신한 양자(대체)키에 대해 QKMS간 동기화 수행
양자키 저장	양자키 동기화 후 수신한 양자키 저장
생애주기 관리	양자키에 대한 생애주기 관리

양자키 전달 모듈(KRA)은 해당 기능을 수행하기 위한 모듈이며, 중·장거리 및 다대다 QKD를 제공하기 위한 경로 설정 테이블 설정 기능, 토폴로지 설정 기능, 경로 설정 테이블 설정 기능, 신뢰노드 기반 QKMS간 양자키 전달 기능을 제공하는 양자키전달(KRA) 모듈을 개발하기 위해 주요기능을 정의하고, KRA와의 연계하는 블록을 선정하고 Interface를 구현하였다. 그리고, 각 기능별 동작 개요에 대한 설계를 수행하고, KRA의 주요기능을 정의하였다.

3.2. 양자키 전달 모드별 기능 절차

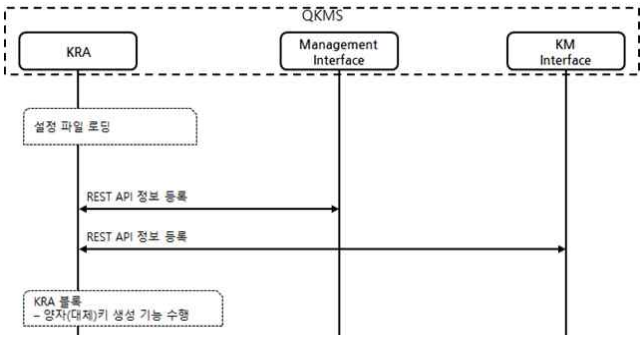
양자키 전달을 위한 블록 기능으로서, 관리 인터페이스, 인증, KM 인터페이스의 기능을 보유하고 있으며, 이는 Management Interface를 통하여, 양자키 전달 경로를 요청하고, 설정 및 조회할 수 있는 기능을 제공하며, KM 인터페이스를 통하여 키 전달 및 양자키 동기화 기능을 수행한다.



[그림 1] 양자키 전달 모듈 연계 블록

(1) 초기화

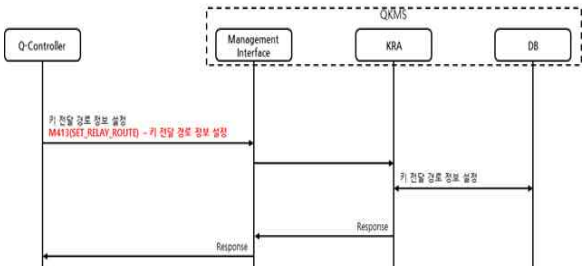
양자키 전달 모듈의 기능에서, 초기화 기능은 KRA 블록을 초기화하는 기능으로 설정 파일에서 QKMS 이름을 가져와 ID로 변환하고 Q-Controller에 대한 정보를 가져오면 Management Interface, KM Interface에 Restful API를 등록한 뒤 주기적으로 양자(대체)키 생성 기능을 수행한다. 다음 그림은 초기화 수행 절차이다.



[그림 2] 양자키 전달 모듈 초기화 기능 절차

(2) 경로설정

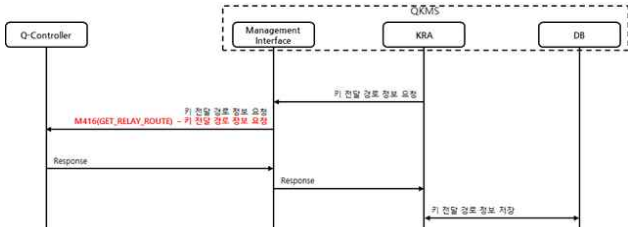
양자키 전달 모듈의 주요 기능은 키 전달(릴레이) 기능을 수행하는 것이다. 이에 앞서 키 전달(릴레이)를 수행하기 위해 필요한 정보를 설정/조회하는 기능이 필요하다. Q-Controller에서 키 전달 경로 정보를 설정하여 Management Interface를 통해 KRA에 전달하고, KRA는 해당 정보를 통해 DB에서 키 전달 경로 정보를 설정한다. 조회 및 삭제도 같은 절차를 수행한다.



[그림 3] 양자키 전달 모듈 경로 설정 기능 절차

(3) 전달경로 요청

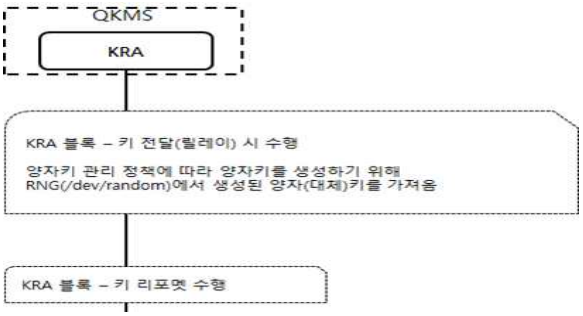
양자키 전달을 할 때, 데이터베이스 정보에 다음 QKMS에 대한 전달 경로가 없을 경우, 상단의 관리정보를 가지고 있는 Q-Controller로 전달 경로를 요청해야 한다. 이때 키전달 에이전트인 KRA가 이 기능을 수행하며, 다음 그림은 키 전달 경로에 대한 정보 요청을 수행하는 절차이다.



[그림 4] 양자키 전달 모듈 키 전달 경로 정보 요청 기능 절차

(4) 양자(대체)키 생성

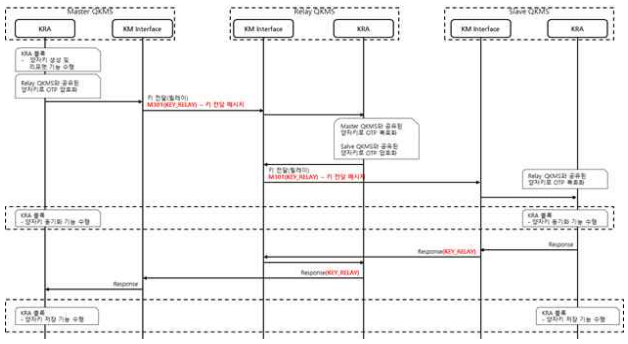
양자키 전달을 통하여 전달되는 양자키는 양자 대체키를 사용한다. 대체키를 전달하여 사용하기 때문에 QKD에서 생성된 양자키를 사용하지 않고, 양자 랜덤넘버 생성기(QRNG)를 통하여 생성된 대체키를 QKD에서 생성한 양자키로 암호화하여 전달하며, 다음 그림은 양자 대체키를 생성하는 기능 절차도이다.



[그림 5] 양자(대체)키 생성 절차

(5) 양자키 전달 절차

양자키 전달 절차는 다음 그림과 같다. Alice QKMS의 KRA 블록은 양자키 생성 및 리포멧 기능을 수행하여 전달할 양자키를 생성하며, 이후 Relay QKMS와 공유된 양자키로 OTP 암호화를 하여 KM Interface를 통해 Relay QKMS로 전달한다. Relay QKMS의 KRA는 Alice QKMS와 공유된 양자키로 전달된 키를 복호화하고, Bob QKMS와 공유된 양자키로 OTP 암호화하여 Bob QKMS로 키를 전달한다. Bob QKMS의 KRA는 Relay QKMS와 공유된 양자키로 OTP 복호화하여 키를 전달받을 수 있다.



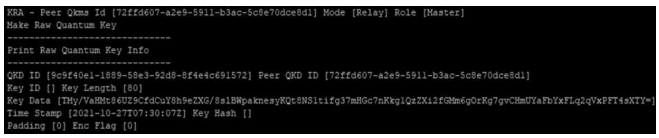
[그림 6] 양자키 전달 절차

IV. 양자키 전달 구현 시뮬레이션 결과

QKMS에 설정된 키 생성 프로파일 및 전달 경로에 따라 양자키 릴레이가 수행되는지 확인을 위하여 양자키 전달모듈의 구현을 수행하였다. 양자키 릴레이를 위해서는 키 생성 프로파일 및 양자키 전달 경로가 설정되어 있어야 하며, 릴레이 수행과정에서 Master QKMS에서 생성된 양자(대체)키를 설정된 키 생성 프로파일에 따라 리포맷을 수행한 뒤, 릴레이 QKMS를 거쳐 Slave QKMS로 전달됨을 확인하였다. 이때 Master와 Slave QKMS 간에 동기화를 수행하여 동일한 양자키를 저장하였는지를 확인하였다.

4.1. 양자키 릴레이 기능 검증

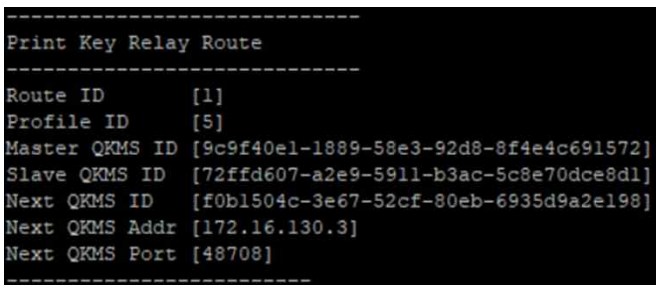
(1) RNG에서 양자(대체)키 생성



(2) 설정된 키생성 프로파일에 따라 리포맷 수행



(3) 전달 경로 수신



(4) 메시지 암호화 송신

전달 경로에 위치한 다음 QKMS와 가지고 있는 양자키를 가져와 메시지를 OTP 암호화 수행하여 전달하고, 양자키 사용상태를 확인한다. 또한 다음 전달 경로에 위치한 QKMS는 양자키 릴레이 메시지를 수신하여 암호화에 사용된 양자키를 확인하여 메시지를 복호화한 뒤, 최종 목적지가 아님을 확인하여, 최종 목적지까지 반복하여 전달을 수행한다.

(5) 최종 전달키 확인

QKMS는 양자키 릴레이 메시지를 수신하여 암호화에 사용된 양자키를 확인하고 메시지를 복호화한 뒤 최종 목적지인 것을 확인하면, 수신 메시지의 키 ID를 사용하여 Master QKMS에 동기화 요청을 수행하고, 여기서 확인 절차 수행하여 성공하면, 최종 응답이 돌아와 양자키 릴레이가 완료되고, Master와 Slave QKMS 모두가 데이터베이스에 최종 상태를 보관하고, 종료된다.

hex(Q_KEY_ID)	TIME	hex(PEER_QKMS_ID)	STATE	Q_KEY
0CAC1A0827DE5ACFB5E1F8A95F5F5604	1635287407	72FFD607A2E95911B3AC5C8E70DCE8D1	0	YcZzucqSDVA=
129CD685A1695031AB71227DAE15DF82	1635287407	72FFD607A2E95911B3AC5C8E70DCE8D1	0	WpaknesyKQs=
15283BE6E2AE57EB980AD50C01AC9B2C	1635287407	72FFD607A2E95911B3AC5C8E70DCE8D1	0	zZXi2fGMm6g=
37D9B26F67CE56D39A9F09B9560F8D7F	1635287407	72FFD607A2E95911B3AC5C8E70DCE8D1	0	qVxPFT4sXTY=
5018D3E85DF557A1A201490EB83610FB	1635287407	72FFD607A2E95911B3AC5C8E70DCE8D1	0	fDUtbYn4N+4=
86368D7BD9A75C13B57EAF26B49766DD	1635287407	72FFD607A2E95911B3AC5C8E70DCE8D1	0	DqyoO4Lwh5k=
91C941DBB0C857FA8EB787BB19A5ABCB	1635287407	72FFD607A2E95911B3AC5C8E70DCE8D1	0	TMy/VaHMt84=
988D4AEAB6F952BA97499AA6230538A1	1635287407	72FFD607A2E95911B3AC5C8E70DCE8D1	0	Hl5lcb/yyUE=
A95146322DB550168D9C8704028735D1	1635287407	72FFD607A2E95911B3AC5C8E70DCE8D1	0	RhoVtjEUurY=
C4DDEC7275555D13A12F4BEBD8B05B95	1635287407	72FFD607A2E95911B3AC5C8E70DCE8D1	0	1GfQn3QrmPI=

[그림7] QKMS1(Master QKMS) K_KEY_INVENTORY Table 정보

hex(Q_KEY_ID)	TIME	hex(PEER_QKMS_ID)	STATE	Q_KEY
0CAC1A0827DE5ACFB5E1F8A95F5F5604	1635287407	9C9F40E1188958E392D88F4E4C691572	0	YcZzucqSDVA=
129CD685A1695031AB71227DAE15DF82	1635287407	9C9F40E1188958E392D88F4E4C691572	0	WpaknesyKQs=
15283BE6E2AE57EB980AD50C01AC9B2C	1635287407	9C9F40E1188958E392D88F4E4C691572	0	zZXi2fGMm6g=
37D9B26F67CE56D39A9F09B9560F8D7F	1635287407	9C9F40E1188958E392D88F4E4C691572	0	qVxPFT4sXTY=
5018D3E85DF557A1A201490EB83610FB	1635287407	9C9F40E1188958E392D88F4E4C691572	0	fDUtbYn4N+4=
86368D7BD9A75C13B57EAF26B49766DD	1635287407	9C9F40E1188958E392D88F4E4C691572	0	DqyoO4Lwh5k=
91C941DBB0C857FA8EB787BB19A5ABCB	1635287407	9C9F40E1188958E392D88F4E4C691572	0	TMy/VaHMt84=
988D4AEAB6F952BA97499AA6230538A1	1635287407	9C9F40E1188958E392D88F4E4C691572	0	Hl5lcb/yyUE=
A95146322DB550168D9C8704028735D1	1635287407	9C9F40E1188958E392D88F4E4C691572	0	RhoVtjEUurY=
C4DDEC7275555D13A12F4BEBD8B05B95	1635287407	9C9F40E1188958E392D88F4E4C691572	0	1GfQn3QrmPI=

[그림 8] QKMS3(Slave QKMS) K_KEY_INVENTORY Table 정보

V. 결론

본 논문에서는 ETSI나 ITU-T 등의 표준화 문서에서 정의한 표준을 준수하면서, 양자암호통신망에서 양자키를 거리의 한계 등의 이유로 제한적인 사이트에 전달하기 위한 양자키 전달 모듈을 설계 연구하고, 구현하여 동작을 검증하였다. 4장에서와 같이 구현된 시스템간에 양자키 업데이트 및 전달이 잘 수행됨을 확인할 수 있었다. 본 논문에서는 양자키를 생성한 이후, KMS가 다른 도메인의 KMS에게 키를 전달하는 기능 위주로 작성하였으나, 전체 시스템은 QKD로부터 키를 받는 South bound, 양자키를 응용단에 전달하기 위한 North bound의 계층간 키 전달 연계기능을 추가로 구현할 예정이다.

향후 양자얽힘 등을 이용한 양자 물리적 기반의 양자키분배 시스템이 나오기 전까지는 신뢰노드를 바탕으로 양자키 전달 매커니즘을 적용하고 활용할 수 있을 것으로 기대된다.

ACKNOWLEDGMENT

본 연구는 2022년도 한국과학기술정보연구원(KISTI) 주요사업 과제로 수행한 것입니다.

참 고 문 헌

[1] H. Bechmann-Pasquinucci, A. Pasquinucci, "Quantum key distribution with trusted quantum relay", Quantum Physics, arXiv:quant-ph/0505089v1, 2005년 5월

[2] S.M. Barnett and S.J.D.Phoenix, "Extending the Reach of QKD Using Relays", IEEE GCC Conference and Exhibition, 2011

[3] 이원혁, 석우진, 손일권,"양자암호기반의 통신망 구축 및 성능시험 검증 연구", KNOM Review 22권 2호, pp39-47, 2019년10월

[4] 김용환, 심규석, 이원혁, "중장거리 양자 암호키 분배를 위한 키 관리 계층 기반 양자키 전달 구조 및 방안", 2021년도 한국통신학회 동계종합학술발표회, p74-75, 2021년 2월

[5] 심규석, 손일권, 김용환, 이은주, 배광일, 김현진, 이원혁, "국가과학기술연구망 기반 양자암호통신 구축을 위한 양자 키 관리 시스템 설계", 2021년도 한국통신학회 동계종합학술발표회, p70-71, 2021년 2월

빅데이터 기반 AI 컴퓨팅을 위한 국제간 분산 연구플랫폼 구축 방안 연구

문정훈, 석우진, 김기현
한국과학기술정보연구원
{jhmoon, wjseok, kkh1258}@kisti.re.kr

A study on the establishment of an international distributed research platform for AI computing based on science big data.

Jeonghoon Moon, Woojin Seok, Kihyeon Kim
Korea Institute of Science and Technology Information(KISTI)

요 약

빅데이터의 출현으로 지난 10년간 과학기술분야는 인공지능 기반의 다양한 응용연구가 활성화 되고 있다. 이런 동향에 반해 현재 IT 인프라 체계는 기존 CPU기반의 클러스터 방식과 대용량 연산이 가능한 HPC 기반으로 구성되어 있으며, 데이터 또한 개별 데이터센터 중심의 저장과 관리가 이루어지고 있어 과학분야의 빅데이터에 대한 효과적인 전송, 저장, 공유가 어려우며, GPU기반의 AI연산을 위한 전산자원도 부족한 실정이다. 따라서 이러한 환경의 개선을 위해 빅데이터 기반의 AI 컴퓨팅을 위한 분산 연구플랫폼 구축을 통해 부족한 AI 컴퓨팅 자원을 해결하고, 초고속연구망 기반의 빅데이터 고속도로 구축을 통해 효과적인 전송과 활용을 위한 방안을 제안하였다.

Ⅰ. 서 론

본 논문에서는 빅데이터의 출현으로 지난 10년간 과학기술분야에서는 인공지능 기반의 폭넓은 응용연구가 진행되고 있다. 이러한 빅데이터 기반의 인공지능 연구는 빅데이터의 저장, 저송, 공유를 위한 특화된 기술을 요구하고 있으며, 특히 컴퓨팅 자원과 스토리지 지원을 중심으로 협업 환경에 대한 수요가 증가하고 있다. 이것은 고성능 장비와 계산자원에 대한 액세스의 증가로 이어지며, 이러한 수요 증가로 인해 IT 자원의 부족과 성능저하를 초래하며 빅데이터 기반의 응용연구 활성화에 여러 가지 제약이 나타나고 있다.

이상과 같은 연구 동향과 기술발전에 의해 빅데이터 생태계의 발전에 따른 IT인프라의 고도화와, 계산자원의 효과적인 지원 등에 대한 해결책으로 다양한 기술과 응용 환경이 고도화 되고 있다. 특히 그 중에서도 미국 에너지국(DoE) 산하 ESnet에서는 수년전부터 이러한 문제를 해결하고 고도화하기 위해 기존 네트워크 체계를 빅데이터를 위한 고속 전송을 위한 기술체계로서 ScienceDMZ를 제안하였고, 이를 기반으로 빅데이터 고속도로 체계를 구축하여 캘로포니아 지역의 주요 대학과 연구소를 연동하는 새로운 형태의 연구플랫폼 환경을 구축 개발하고 있다. 특히 샌디에고 슈퍼컴퓨팅센터 중심의 Calit2와 캘리포니아 연구망인 CENIC에서 주도적으로 추진하고 있다. 먼저ScienceDMZ 환경 을 주요 연구소와 대학에 구축하고 이들을 CENIC의 초고속연구망으로 연동하여 빅데이터의 흐름을 원활히 하고, 주요 대학과 연구소에 구축된 ScienceDMZ 기반의 계산자원들을 연계하여 부족한 계산 환경을 제공하고, 새로운 형태의 연구 환경을 제공한다. 특히 ScienceDMZ 환경에서 데이터 전용 전송 노드인 DTN(Data Transfer Node)의 효과적인 활용을 통해 빅데이터 전송 뿐만아니라 전송 이외의 시간에 컴퓨팅 자원으로 활용이 가능한데 이것은 빅데이터 고속도로 체계와 컴퓨팅 체계를 연계한 플랫폼 형태로 구성하여 제공하게 된다. 현재 미국의 샌디에고 슈퍼컴퓨팅 센터와 샌디에고 대학교 중심의 PRP(Pacific Research Platform) 프로젝트를 통해 빅데이터의 전송과 인공지능 컴퓨팅 작업이 검증되고 있으며, 미국 전역에 대해 연구플랫폼화를 추진하는 NRP(National Research Platform) 프로젝트가 진행 중에 있다. 또한 GLIF(Global Lambda Integrated Facility) 기반의 전세계 연구망을 기반으로 주요 거점 도시에 대한 ScienceDMZ 환경을 연계하는 GRP(Global Research Platform) 프로젝트로 확대되어 추진 중에 있다.

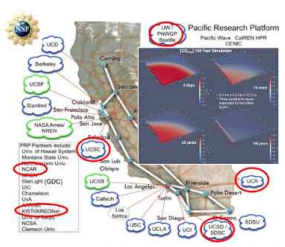


그림1. PRP(NSF 과제) 기반의 분산 컴퓨팅을 활용한 CO2 격리 분석 연구

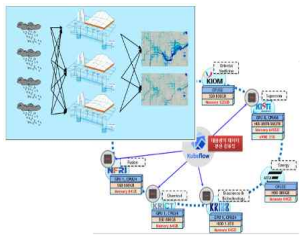


그림2. LSTM 기법을 활용하여 출연연 중심의 KRP(Korea Research Platform) 환경에서 기상데이터 분석

그림1은 PRP 프로젝트 기반의 분산 컴퓨팅을 활용한 CO2 격리 분석 연구사례이며, 캘리포니아에 있는 대학과 연구소를 중심으로 구축된 ScienceDMZ를 활용하여 고대역 분산환경에서의 계산작업을 수행하였고, 그림2는 LSTM 기법을 활용하여 출연연 중심의 KRP(Korea Research Platform) 환경에서 기상데이터 분석 사례이다. HPC 수준의 계산 자원을 확보하지 않아도 ScienceDMZ 기반의 빅데이터 고속도로와 연구플랫폼 기반의 분산 컴퓨팅 자원들을 연동하여 상기와 같은 연구를 수행할 수 있으며, 이러한 연구플랫폼에는 연구데이터의 저장을 위한 스토리지 자원과 HPC급 슈퍼컴퓨터의 연계도 가능하므로 다양한 형태의 컴퓨팅 자원들의 연계를 통해 부족한 컴퓨팅 자원과 빅데이터의 처리를 수행할 수 있다. 이것은 응용연구를 위한 연구자가 HPC, 대용량 스토리지, GPU 등을 보유하지 않아도 필요한 연구를 수행할 수 있다는 의미가 되며, 특히 그림2에서는 기상기후 데

이터를 개선된 LSTM 기법을 적용하고 GPU 컴퓨팅을 활용하여 도시 홍수 모델 개선 연구를 수행하므로 사회현안문제 해결에도 기여한다. 이러한 선행연구와 연구동향에 따라 ScienceDMZ 기반의 연구플랫폼은 국가간 적용이 가능하며, 특히 아시아의 부족한 IT 인프라와 컴퓨팅 자원에 대해서 국제 연구망 기반의 빅데이터 고속도로를 구축하고 참여국의 주요 컴퓨팅 자원을 연계하여 국제간 분산환경에서의 연구플랫폼을 구축 할 수 있다. 따라서 본 론에서는 연구망을 활용하여 빅데이터 기반 인공지능 컴퓨팅을 위한 국제간 분산 연구플랫폼 구축을 위한 요소기술과 구축을 위한 방법론을 제시하고, 결론에서는 본 논문에서 제안한 연구플랫폼의 활용 방안과 향후 연구 방향을 제시한다.

Ⅱ. 본론

빅데이터 기반 AI 컴퓨팅을 위한 국제간 분산 연구플랫폼 구축을 위해 먼저 국제간 빅데이터 고속도로 체계를 ScienceDMZ 환경의 구축을 제안하고, 이를 기반으로 연구플랫폼 구축을 위한 요소기술과 시스템 구성에 대한 방안을 제안한다. 특히 아시아지역 대표 연구망 협의체인 APAN, TEIN, APONET 등을 통해 각국의 연구망에 대해 상호 연동을 추진하고, 연구플랫폼을 기반으로 각국의 컴퓨팅 자원을 연결하여 고성능 네트워킹 기반 분산 컴퓨팅 환경을 구축한다. 따라서 국제간 분산 연구플랫폼은 아시아지역 개발도상국들의 컴퓨팅, 네트워킹 자원에 대해 공유가 가능하다. 이러한 분산 연구플랫폼을 구축하기 위해서는 앞서 언급한대로 ScienceDMZ 환경 구축 기술과 컴퓨팅 자원의 효과적인 관리와 운영을 위한 쿠버네티스 기반의 플랫폼 구축 기술이 필요하며, 이를 통해 컨테이너들의 효과적인 관리와 운영을 할 수 있게 된다. 따라서 본 논문에서 제안하는 분산 연구플랫폼을 구축하기 위해 다음의 구성 단계를 거친다. 1단계, 국제간 빅데이터 고속도로 체계의 구축, 2단계, 분산된 컴퓨팅 자원의 연계를 통한 연구플랫폼의 구축, 3단계, 빅데이터 기반의 인공지능 분야 응용연구 사례의 발굴.

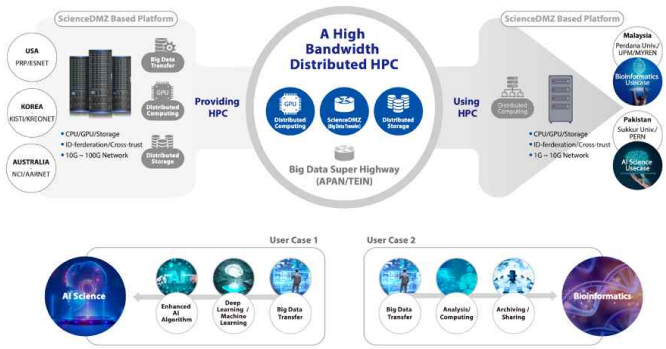


그림3. 빅데이터 기반 AI 컴퓨팅을 위한 국제간 분산 연구플랫폼 구성도

아시아지역 개발도상국의 국제연구망 연동을 통해 ScienceDMZ 간 End-to-end 방식의 빅데이터 고속도로 체계를 구축한다. ScienceDMZ 환경의 구축은 4가지 기본 원리를 통해 구축되는데 1) 비즈니스 트래픽과 과학 트래픽의 분리, 2) 데이터 전송 전용 노드인 DTN의 구축 및 사용자 환경에서 WAN에 가장 가까운 위치에 구축, 3) ScienceDMZ 환경으로 연동된 각각의 DTN의 전송 성능 모니터링을 위한 perfSONAR 구축, 4) 사용자가 소속된 연구망의 빅데이터의 효과적인 전송을 위한 방화벽 우회 정책 수립과 전송 경로 최적화 및 고성능화. 또한 각각의 DTN 노드들은 리눅스를 기준으로 전송 성능 최적화를 위한 TCP 튜닝을 하게되는데 이때, 전송 디바이스의 큐 설정, 전송 소켓 버퍼 튜닝, TCP 크기 조정, 혼잡제어 파라미터와 TCP 알고리즘 선택을 통해 최적의 전송 환경을 구성한다. DTN은 전송 외의 시간에는 CPU, GPU, 메모리 기반의 컴퓨팅 자원으로 활용하게된다. DTN 전송 성능은 통상 기본 구성하에서는 주어진 대역폭의 75% 수준의 전송 성능을 보인다. 위의 그림3은 아시아 지역을 중심으로 ScienceDMZ를 통해 빅데이터 네트워크를 구축하고 쿠버네티스를 통해 분산 CPU, GPU, 메모리, 스토리지 등의 컴퓨팅 자원 관리의 기본 구성도이다. 빅데이터 기반 AI 컴퓨팅을 위한 국제간 분산 연구플랫폼 구축을 위한 단계별 세부사항은 다음과 같다.

1단계 : 국제간 빅데이터 고속도로 체계의 구축

1) 국제간 연구망의 연동과 ScienceDMZ 환경의 구축을 위해 해당국가는 자국의 연구망을 국제연구망에 연동하여 상호 신뢰존(Trust-Zone)을 형성한다. 또한 해당국가의 연구망은 상호간의 비즈니스 트래픽과 과학 트래픽의 분리를 위해 전용망 형태로 구성한다.

2) 사용자 환경에서 데이터 전송 전용 노드인 DTN을 구축하여 ScienceDMZ 환경을 구축한다. 데이터 전송 가속기 역할을 하는 DTN은 컨테이너 기반의 분산 컴퓨팅 자원으로도 활용되며, 따라서 사용자 요구에 따라 CPU, GPU, 메모리 중심의 컴퓨팅 작업에 활용된다.

3) 사용자 환경에서 DTN 간 연동에 대한 네트워크 환경 모니터링은 전송 성능의 보장과 컴퓨팅 자원 간 원활한 운영을 위해 필요하며, 이를 위해 perfSONAR 기반의 Maddash를 통해 상호간 전송 성능을 모니터링 한다. 기본적으로 전송 성능을 모니터링 하기위해 DTN간 throughput, packet loss, RTT 등을 OWAMP(One Way Active Measurement Protocol), BWCTL(Bandwidth Controller) 등의 전송 성능 측정 기능을 통해 모니터링하여 파악한다. 또한 DTN 노드의 상황과 성능을 모니터링하기 위해 각각의 노드에 설치된 프로메테우스를 통해 DTN 노드의 전산자원 상태와 성능을 모니터링하고 그라파나를 통해 사용자에게 정보를 제공한다.

2단계 : 분산된 컴퓨팅 자원의 연계를 통한 연구플랫폼의 구축

ScienceDMZ 환경 구축을 통해 설치된 각각의 DTN은 전송 노드로 활용될 뿐만아니라 컴퓨팅 자원으로도 유용하다. 특히 GPU-Enabled DTN을 통해 인공지능 학습, 추론 작업을 할 수 있으며, 쿠버네티스를 통해 컨테이너 기반의 계산자원으로 사용자에게 제공이 가능하다. 특히, 분산된 DTN의 GPU 뿐만아니라, CPU, 메모리, 스토리지 등도 분산 컴퓨팅 자원으로 활용이 된다. 1) 쿠버네티스 기반의 플랫폼을 통해 DTN을 계산자원의 형태로 제공하고 운영하며, 각각의 DTN은 마스터 노드의 워커로드로 활용되며, 쿠버플로우를 통해 계산자원인 Pod를 구성하여 사용자 요구에 맞는 계산자원으로 제공하게 된다. 이때 계산자원을 할당 받을 때 단일 노드의 작업의 범위를 벗어나는 큰 작업(Big Job)을 수행하기 위해 LSC(Large Single Container)를 구성하여 거대작업을 수행할 수 있으며, 향후 HPC 수준의 작업이 가능한 방향으로 고도화 한다.

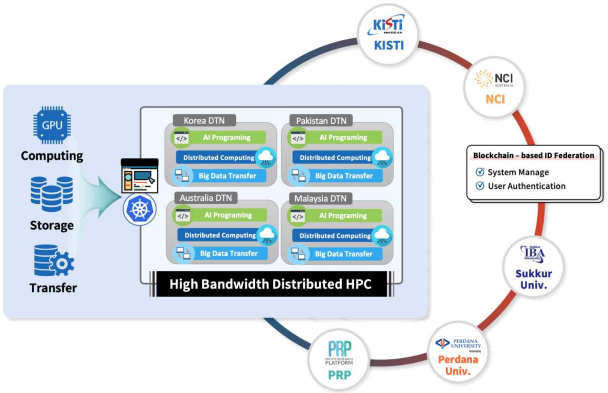


그림4. 인공지능 컴퓨팅을 위한 분산 연구플랫폼 구성도

2) 쿠버네티스 기반의 연구플랫폼은 계산자원 뿐만아니라 스토리지 자원(Ceph)도 연계가 가능하며, 블록/오브젝트 스토리지 형태로 사용자에게 개별 저장 공간을 할당하며, 이때 인공지능 학습과 추론에 필요한 빅데이터 전송과 저장공간으로 활용된다.
3) 쿠버네티스 기반의 연구플랫폼을 활용하기 위해 사용자 포털을 구축하여 비IT 사용자에게도 쉬운 접근과 활용이 가능하게 구축한다. 위의 그림 3은 기본적인 연구플랫폼의 구성도이며, 전송과 컴퓨팅을 위한 DTN의 구성과 쿠버네티스를 통한 관리 환경을 보여준다.

3단계 : 빅데이터 기반의 인공지능 분야 응용연구 사례의 발굴
앞의 1,2단계를 통해 구축한 국제간 분산 연구플랫폼은 GPU 기반의 인공지능 분야 연구에서 부족한 계산자원을 지원하고, 대용량 데이터의 빠른 전송과 공유를 지원하므로 IT 인프라 및 계산자원이 부족한 사용자에게 효과적이다. 향후 HPC급의 고성능 컴퓨팅 자원에 대한 상호 공유 기술 개발과 협력으로 거대 계산자원의 제공이 가능하다. 특히 본 연구는 아시아 지역의 개발도상국을 대상으로 빅데이터 기반의 바이오연구 분야와 인공지능 연구분야의 GPU 컴퓨팅 기반의 응용연구에 부족한 IT인프라 및 계산 자원의 지원과 연구활성화에 활용될 예정이다.

Ⅲ. 결론

본 논문에서는 빅데이터 기반 AI 컴퓨팅을 위한 국제간 분산 연구플랫폼 구축 방안과 활용 분야를 제안하였다. ScienceDMZ 기반의 분산 연구플랫폼의 구축을 통한 빅데이터 고속도로 체계와 컴퓨팅 체계의 연계는 급속히 증가하는 빅데이터와 이를 기반으로 인공지능 연구분야의 응용연구에 대한 부족한 전송 성능과 컴퓨팅 자원의 효과적인 제공을 가능하게 한다. 특히 GPU와 스토리지 기반의 자원에 대한 효과적인 공유와 활용이 가능하며, 사용자 관리를 통해 원격지에 대한 연구플랫폼을 통한 IT 자원의 제공이 가능하다. 향후 연구 방향으로는 HPC 연계를 위한 쿠버네티스 기반의 잡스케줄러의 상호연계 개발과 LSC 기술의 고도화와 안정화를 통한 거대계산 문제 지원, 그리고 인공지능 컴퓨팅 자원을 보다 효율적으로 활용하기 위한 vGPU 스케줄링 기법 등에 대한 연구가 필요하다.

참 고 문 헌

[1] PRP, https://www.pacificresearch-platform.org
[2] NRP, https://pacific-researchplatform.org/NRP/
[3] CHASE-CI, https://nsf.gov/award-search/showAward?AWD_ID=1730158
[4] ESnet ScienceDMZ, https://fasterdata.es.net/science-dmz/DTN/
[4] Dart, Eliet al, “The Science DMZ: A Network Design Pattern for Data-intensive Science”,The International Conference for High Performance Computing, Networking Storageand Analysis (SC13), pp. 173-185, 2014.
[5] P. Xu, S. Shi, and X. Chu, "Performance evaluation of deep learning tools in Docker containers," in 2017 3rd International Conference on Big Data Computing and Communications (BIGCOM), 2017: IEEE, pp. 395-403.
[6] 문정훈, 곽재승, 홍원택, 김기현, 이상권, 김동균, 김용환, and 유기성. "과학빅데이터 고속전송을 위한 ScienceDMZ 구축 방안 연구." KNOM Review 22, no. 2 : 12-21, 2019.

과학 연구장비 근거리 무선 연결을 위한 밀리미터파 통신기술 적용방안

김기욱, 석우진, 곽재승
한국과학기술정보연구원
{wowook, wjseok, jskwak}@kisti.re.kr

Application of mmWave Communication Technology for Short-range Wireless Connection of Scientific Research Equipments

Kiwook Kim, Woojin Seok, Jaeseung Kwak
Korea Institute of Science and Technology Information

요 약

과학 연구장비에 요구되는 고 대역폭의 제공에 더불어 연구장비 내 케이블 감소 및 전송 경로 최적화를 통한 설치비용 감소와 관리 간소화를 위해, 과학 연구장비의 기술과 구조에 적합한 근거리 무선통신 기술을 활용해서 유선연결의 단점을 보완하기 위한 연구가 필요하다. 본 논문은 과학 연구장비의 통신 요구사항을 만족하기 위해 60GHz 이상의 고주파수 대역을 사용하는 밀리미터파 통신 기술을 적용하는 방안을 제시한다. 과학 연구장비를 위한 근거리 통신에서는 고대역 주파수의 짧은 도달범위를 단점이 아닌, 근거리 대용량 무선전송 응용을 위해 주파수 재사용성을 극대화할 수 있는 장점으로서 활용 가능하다. 이를 통해 기존에 국내에서 본격적으로 상용화가 이루어지고 있지 않은 60GHz 이상 고대역 주파수의 과학기술 분야 선제적 적용사례를 발굴할 수 있다.

Ⅰ. 서 론

과학 실험장비의 대형화 및 정밀화에 따른 데이터 전송량의 증가는 장비 간 연결에 점점 더 많은 대역폭을 필요로 하며, 대역폭의 부족은 실험장비의 성능제한을 발생시키므로 요구사항을 만족하기 위한 통신 대역폭의 확보가 중요하다. 일례로, 스위스 CERN의 고광도 입자가속기(HL-LHC)를 활용하는 차세대 화소검출기(ATLAS Phase Ⅱ Inner Tracker Pixel Detector) 연구장비에서 적중 클러스터를 모두 판독하기 위해 필요한 대역폭은 50-100 Tbps이다. 이를 전송하기 위해 실험장비 내에 각각 5 Gbps의 데이터를 전송하는 10,000 여개의 상향링크를 필요로 한다.[1]

그러나 대형연구장비의 점점 높아지는 대역폭 요구사항을 만족하기 위해서 연구장비 내의 유선 연결을 증가시키는 것만으로는 부족하다. 유선연결을 위한 케이블의 증가는 연구장비 내 케이블링 공간으로 인한 측정 불가영역(dead-zone)을 발생시키며, 또한 케이블 주위 공간에도 산란 및 상호작용, 열 발생 등으로 측정 데이터에 영향을 끼친다. 한 예로, 그림 1은 CERN의 CMS 검출기에서 케이블링으로 인해 에너지 검출 모듈(ECAL)의 측정 불가영역(회색 수직선)이 발생한 것을 보여준다.

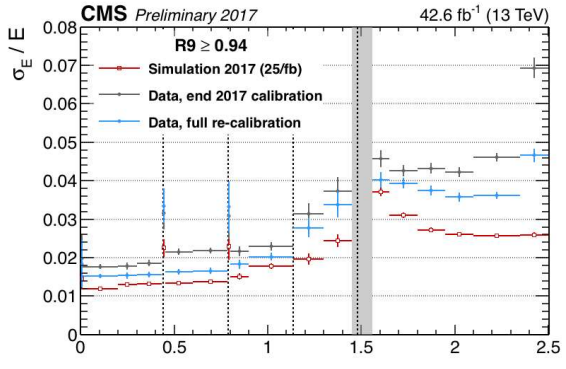


그림 1. 케이블링으로 인한 측정오류 및 측정불가영역 발생 예[2]

또한 케이블 경로로 인해 연구장비의 설계가 제한되어 제작의 효율성에도 영향을 주며, 케이블이나 커넥터의 파손 및 다수의 관리인력 운영 등으로 직접적인 비용 상승 요인이 되기도 한다. 이와 같이 과학 연구장비에 요구되는 고 대역폭의 제공에 더불어 실험장비 내 케이블 감소 및 전송 경로 최적화를 통한 설치비용 감소와 관리 간소화를 위해서는, 과학실험 연구장비의 기술과 구조에 적합한 근거리 무선통신 기술을 활용해서 유선연결의 단점을 보완하기 위한 연구가 필요하다.

근거리의 고속 통신을 지원하기 위해서는 밀리미터파(mmWave) 이상의 높은 주파수 대역을 사용하는 것이 유리하다. 일반적으로 고대역 주파수는 대용량 데이터 전송이 가능하며 직진성이 높은 장점이 있으나 도달범위가 짧은 단점 때문에 무선통신에 활용이 힘들다. 이로 인해 현재 무선통신 분야에서는 28GHz 주파수까지만 활발히 제품 개발이 이루어지고 있으며, 60GHz 이상은 개발 및 상용화 진행이 더딘 상황이다.

그러나 과학 연구장비를 위한 근거리 통신에서는 고대역 주파수의 짧은 도달범위를 단점이 아닌, 근거리 대용량 무선전송 응용을 위해 주파수 재사용성을 극대화할 수 있는 장점으로서 활용 가능하다. 이를 통해 아직 본격적으로 상용화가 이루어지고 있지 않은 60GHz 이상 고대역 주파수의 과학기술 분야 선제적 적용사례를 발굴할 수 있을 것으로 기대된다.

Ⅱ. 대형연구장비 근거리 통신에 적합한 주파수 대역 선정

일반적으로 높은 주파수 대역을 사용 시 다음과 같은 장점들을 활용 가능하다. 먼저 높은 데이터 전송량의 달성이 가능하다. 고주파수 대역은 허용 주파수 대역폭이 수GHz까지도 가능하므로 초고속 데이터 전송에 적합하다. 또한 주파수가 높아질수록 파장이 작아지므로 파장에 비례하여 크기가 작아지는 안테나 및 RF 소자들이 소형화되므로 송수신기의 크기(폼팩터)를 충분히 작게 만들 수 있다. 또한 수십 mW 단위의 저전력을 사용하며 투과력이 약해서 인체에 미치는 영향이 작다.

이런 장점들에도 불구하고, 주파수 대역이 높아질수록 투과력이 낮아지고 높은 신호감쇠에 의해 전파 도달거리가 좁아지는 단점이 있어 기존 이동통신 등의 상용 무선통신에서는 고주파수 영역을 선호하지 않았다. 하지만 연구장비간 근거리 통신 환경에서는 높은 신호감쇠를 오히려 장점으로 활용 가능하므로(주파수 재사용성 및 보안성 측면), 최대한 높은 주파수 대역을 활용하는 것이 유리하다.

그러나 고대역 주파수의 활용에는 기술적인 한계가 있다. 사용하는 주파수가 높아질수록 캐리어 주파수 파장을 만들어주는 오실레이터의 정확도도 높아져야 하고, 또한 잡음을 제거하기 위한 회로설계 난이도가 높아진다. 따라서 기술 활용 가능성(feasibility)을 고려하여 적절한 주파수 대역의 선정이 필요하다. 현재는 주로 5G mmWave에 사용되는 28GHz 장비는 상용화 단계에 들어서 있는 반면, 60GHz 이상은 통신칩이나 모듈 등을 활용한 시제품은 많이 만들어지고 있으나 일반 사용자를 대상으로 하는 완제품으로 출시된 사례는 많지 않으며, 그보다 높은 100GHz 이상에서는 통신기술 자체에 대해 연구실 수준의 연구들이 이루어지고 있는 상황으로 현재로서는 당장 시험구축 가능한 수준은 도달하지 못한 것으로 여겨진다.

Ⅲ. 밀리미터파 주파수 활용 시 고려사항

밀리미터파의 사전적 의미는 30GHz에서 300GHz 사이의 주파수 대역이지만, 무선통신 분야에서는 일반적으로 26GHz, 28GHz, 38GHz, 60GHz, 94GHz 주파수 대역을 밀리미터파 주파수로서 사용한다. 또한 그보다 높은 100GHz 이상의 주파수 대역을 포함하여 지칭하는 경우에는 sub-THz라는 표현을 병행하여 사용한다. 이들 주파수 대역은 기존에는 주로 군사 및 위성 통신 일부 분야에서 한정적으로 사용되었으나, 최근에는 무선통신 기술의 발전에 따라 5G 이동통신에서도 사용되기 시작했다.

국내에서는 삼성전자 및 한국전자통신연구원(ETRI)등을 중심으로 28GHz 밀리미터파의 상용화를 달성하는 것을 목표로 기술 연구들이 활발히 이루어졌으나, 아직은 낮은 통신거리로 인해 다양한 응용에 활용되기 힘들어 본격적인 상용화에 나서지 못하고 있다. 또한 5G에서도 28GHz까지만 활용하며, 60GHz 등의 고주파 대역은 대부분 국가의 전파규정에서 용도미지정 대역으로 비면허 사용이 가능하게 풀어놓은 상태이다. 60GHz 이상 주파수대역은 현재로서는 5G 서비스에 주력한 국내 통신업계의 주요 개발 및 상용화 대상에서 벗어나 있어, 향후 60GHz 이상 고대역 주파수를 활용한 차세대 무선통신 기술개발을 대비하기 위한 측면에서 선제적인 기술 연구를 필요로 하고 있다.

IEEE에서는 근거리 통신이나 측위 등의 목적으로 60GHz 주파수 대역을 활용한 표준을 제정하고 있다. 2012년에 발표되고 2016년에 채택된 IEEE 802.11ad 표준은 WiGig 라는 이름으로도 불린다. 멀티미디어 스트리밍 및 VR 헤드셋 연결 등의 응용을 타깃으로 하며, 약 10미터 거리 내에서 최대 7Gbps 데이터 전송속도를 목표로 제정되었다. 이후 2017년에는 IEEE 802.11ad와 호환되는 개정판으로 IEEE 802.11ay draft가 발표되었다[3][4]. IEEE 802.11ad가 최대 2.16GHz 대역폭을 사용하는 반면, IEEE 802.11ay는 4개의 채널을 결합하여 최대 8.64GHz 대역폭을 사용하여 스트림당 최대 link-rate는 44 Gbps이다. 최대 4개의 스트림을 지원하는 MIMO를 포함하여 이론상 최대 176 Gbps 달성이 가능하며, 이를 통해 사무실이나 가정 내 케이블 대체 및 ISP의 실외 백홀 연결 등의 타겟 응용에 적용하는 것을 목표로 한다. 2021년에 WG으로 승인되며 표준 개발이 활발히 이루어지고 있다.

기타 표준으로, China mmWave라고도 불리는 IEEE 802.11aj는 IEEE 802.11ad의 PHY와 MAC을 수정해 중국의 59-64GHz 대역폭에서 운용하며, 2018년 2월 승인되었다. 또한 60GHz 대역을 통신이 아닌 Positioning 목적으로 사용한 IEEE 802.11az 표준도 있다. 고밀도 AP/STA 및 비가시거리 WLAN 환경에서 Fine Timing Measurement 프로토콜 기반의 초정밀, 저전력 측위 기술을 목표로 하며, 2.4/5/60㎓ 주파수 대역을 사용하여 다중 채널기반 측위 기술을 포함한다.

Ⅳ. 주파수 대역 특성을 활용한 근거리 다중 무선링크 구성방안

60GHz 주파수 대역은 인근 주파수 대역들에 비해 공기 중 신호감쇠가 유독 높은 특징을 가지며(그림 2), 이로 인해 근거리 통신을 위한 전파 도달거리 조절이 용이하다. O_2 감쇠에 영향을 받는 주파수와 아닌 주파수를 비교해보면(그림 3), 똑같이 1km 지점에서 30dB로 수신되도록 송신했을 때 O_2 감쇠에 영향을 받는 경우엔 2.5km 지점까지만 가도 수신 신호세기가 0dB가 되지만, O2 감쇠에 영향을 안 받으면 32km 지점까지 가야 0dB가 된다. 이렇게 전파 도달거리의 조절의 용이함은 무선 링크 간 간섭의 영향을 줄이기 위해 활용 가능하다.

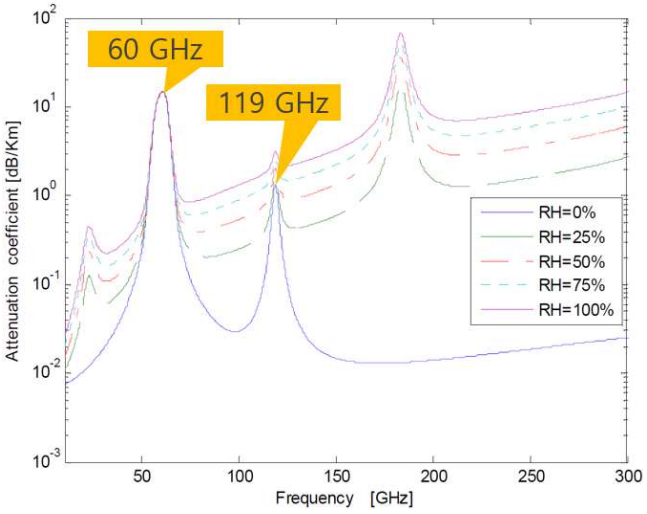


그림 2. 주파수 대역별 공기 중 신호감쇠[5]

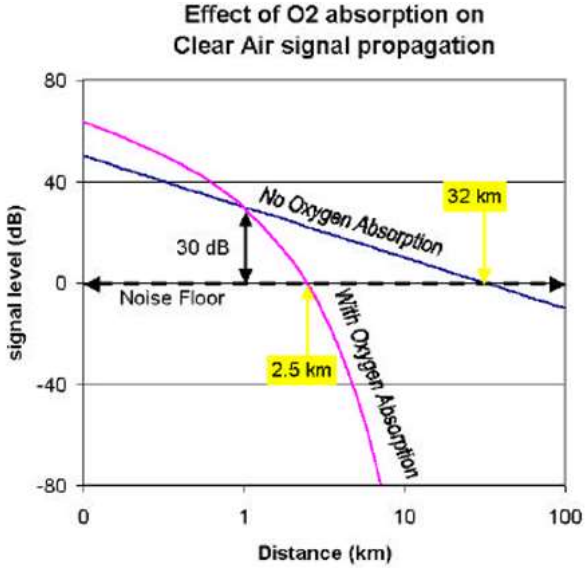


그림 3. 공기 중 신호감쇠에 의한 전파 도달거리 영향[6]

또한 회절 원리에 의해 주파수에 반비례하여 빔 폭이 좁아지며, 이에 의해 높은 주파수를 사용하면 직선에 가까운 빔 형태를 만들어낼 수 있다. 표 1에서 2.4 GHz 주파수 사용 시 117도의 넓은 빔 폭이 형성되는 것에 비해, 60 GHz 주파수 사용 시 4.7도의 직선에 가까운 빔 폭이 형성되는 것을 확인할 수 있다.

주파수	99.9% 빔 폭
2.4 GHz	117°
24 GHz	12°
60 GHz	4.7°

표 1. 주파수별 빔 형태[6]

이와 같이 60GHz 이상의 고주파수를 사용하면 전파의 방향성 및 도달거리의 조절이 용이하며, 따라서 전파범위를 원하는 모양으로 형성해 내기에 유리하다. 우리는 이와 같은 고주파수의 특성을 활용해서 다수의 무선링크를 인접하여 평행 배치하여 좁은 범위 내에서 많은 무선링크가 상호간 간섭을 최소화하며 동시에 전송하도록 구성하기 위한 연구를 추진하고 있다. 예를 들어, 다수의 60 GHz 통신링크를 1m^2 면적 내에 링크 간 3.5cm 거리로 평행 배치 시, 이론적으로 3.7 Tbps/m^2 까지 달성 가능할 것으로 예상되고 있다.

V. 관련연구

입자가속기 및 검출기 기술 발전을 위한 AIDAinnova 프로젝트(EU의 Horizon 2020 프로그램 지원)의 일환으로, WADAPT(Wireless Allowing Data and Power Transmission) 연구그룹에서 비면허대역 주파수를 활용하여 기존 검출기의 유선통신을 대체하기 위한 연구를 진행하고 있다.

이들의 목표는 그림 4와 같이 기존 검출기의 축 방향(Axial) 데이터 전송을 위한 수십 미터의 유선통신 대신, 약 1미터 거리의 무선통신으로 대체하여 전송 경로를 효율적으로 개선하는 것이다.

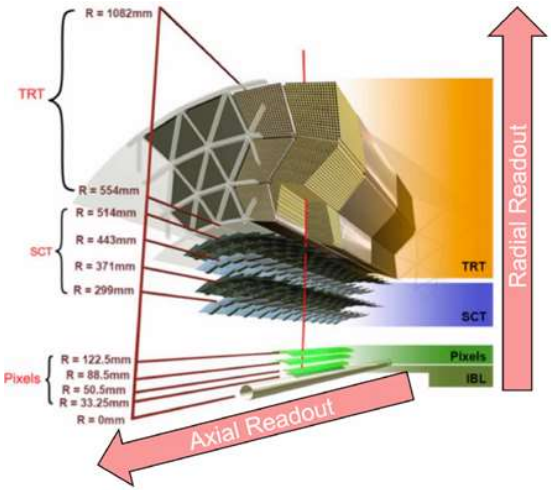


그림 4. 전송 경로의 개선을 통한 효율성 향상[1]

이를 위해서는 무선통신 경로 상에 존재하는 여러 겹의 센서 층을 통과하여 데이터를 전송할 수 있어야 하며, 또한 전송 경로 상에서 각 센서 층에서 수집되는 데이터를 추가적으로 전송해야만 한다. 이들은 그림 5와 같이 각 층마다 송신 및 수신을 번갈아 하여 센서 층을 통과하도록 하였으며, 또한 추가적인 데이터 전송을 위해 일정 면적 내에 60GHz 대역의 통신링크를 다수 사용하여 성능을 높이는 방법으로 연구를 진행하고 있다. 최근 실험을 기반으로 추정되는 성능은 1.2 Tbps/m^2 이다.

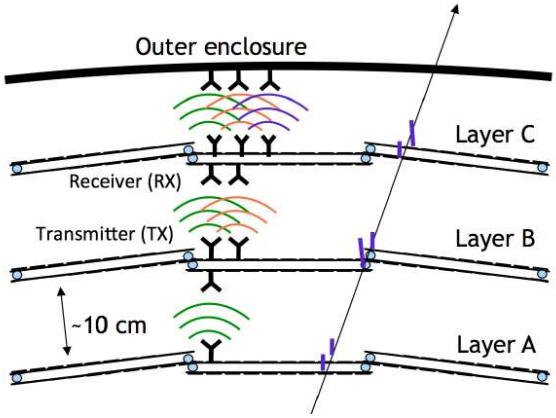


그림 5. WADAPT의 대형연구장비 내 무선 연결 시나리오[9]

VI. 결 론

대형연구장비에 활용 가능한 수준의 높은 대역폭 및 주파수 재사용성을 가진 무선기술 확보는 과학연구장비의 측정 정확도 향상 및 구축·운영비용의 절감을 위해 중요하다. 밀리미터파 기반의 근거리 무선통신을 과학기술 분야에 선제적으로 적용하는 것은 국내 통신 산업계에서 아직 활발히 제품 개발이 이루어지고 있지 않은 60GHz 이상 고대역 주파수 통신의 상용화를 대비한 선도적 역할을 할 수 있을 것으로 기대된다.

참 고 문 헌

[1] The ATLAS Collaboration, “ATLAS Phase-II Upgrade Scoping Document (ver 1.0),” September 2015.

[2] CMS Public Web, “CMS ECAL Performance in 2017,” (https://twiki.cern.ch/twiki/bin/view/CMSPublic/EcalDPGResultsCMSDPS2018015)

[3] Y. Ghasempour, C. R. C. M. da Silva, C. Cordeiro and E. W. Knightly, "IEEE 802.11ay: Next-Generation 60 GHz Communication for 100 Gb/s Wi-Fi," in IEEE Communications Magazine, vol. 55, no. 12, pp. 186-192, Dec. 2017, doi: 10.1109/MCOM.2017.1700393.

[4] IEEE 802.11ay WG, “Status of Project IEEE 802.11ay,” (https://www.ieee802.org/11/Reports/tgay_update.htm)

[5] Y. Pinhasi et al., “Ultra Wideband Wireless Communications in the 60 GHz Band,” WSEAS Transactions on Communications (WTOC) 9, 12 (December 2010), pp. 773-781.

[6] YDI Wireless, “The Benefits of 60 GHz Unlicensed Wireless Communications,” (https://www.fcc.gov/files/ydibenefits60ghzpdf)

[7] S. Pulipati et al., "Xilinx RF-SoC-based Digital Multi-Beam Array Processors for 28/60 GHz Wireless Testbeds," 2020 Moratuwa Engineering Research Conference (MERCon), 2020, pp. 254-259, doi: 10.1109/MERCon50084.2020.9185240.

[8] E. Locci et al., “Development of wireless techniques in data and power transmission - application for particle physics detectors,” e-Print: 1511.05807 [physics.ins-det]

[9] The WADAPT Collaboration, “Multi-Gigabit Wireless Data Transfer for High Energy Physics Applications,” Proceeding of 2017 European Physical Society Conference on High Energy Physics (EPS-HEP 2017), Venice, Italy, July 5-12, 2017.

빅데이터 고속 전송 환경 기반의 인공지능 연구 환경 제공 플랫폼 연구

김기현, 문정훈*, 석우진
한국과학기술정보연구원
{kkh1258, *jhmoon, wjseok}@kisti.re.kr

Platform Research for Providing AI Research Environment based on Bigdata High-speed Transmission Environment

Ki-Hyeon Kim, Jeonghoon Moon*, Woojin Seok
Korea Institution Science Technology Information (KISTI)

요 약

최근 과학기술분야에서 빅데이터를 이용한 다양한 연구들이 이루어지면서, 빅데이터의 중요성이 점점 커져가고 있다. 생명공학, 한의학, 화학, 핵융합, 농업 등의 분야에서는 이미 데이터 제공 및 처리를 위한 기술들을 개발하고 있다. 하지만 빅데이터를 빠르게 전송하기 위한 네트워크 전송 환경의 부재와 빅데이터를 처리하고 인공지능 학습에 사용할 수 있는 플랫폼을 제공하기 위한 정책과 자금의 문제가 존재한다. 이에 따라 KISTI에서는 이러한 문제를 해결하기 위해 R&E Together라는 프로젝트를 통해 출연연을 대상으로 빅데이터 전송과 데이터 처리를 위한 플랫폼을 제공하고 있다. R&E Together 플랫폼은 고속 빅데이터 전송을 위한 네트워크의 구조를 설계한 ScienceDMZ 라는 기술을 이용하여 빅데이터 전용의 고속 네트워크를 구축하고 그 인프라 위에서 동작하는 인공지능 연구 환경 제공 플랫폼을 개발하여 연구자들에게 인공지능 연구 생산성 향상을 목표로 하고 있다. R&E Together 프로젝트를 통한 타 분야의 빅데이터 제공 및 처리를 위한 플랫폼 개발 과제에서 KISTI의 플랫폼을 적용하고자 하는 사례를 통해 이 기술의 우수성을 제시하고자 한다.

Ⅰ. 서 론

과학기술분야에서 최근 수행되는 연구 환경은 다양한 연구 분야의 데이터화 및 정보화이다. 기존 과학기술분야에서는 수행하고 있는 연구의 가시화 또는 시뮬레이션화와 같은 연구 환경 이였다면, 최근 진행되는 연구의 형태는 거대한 장비 또는 실험에서 나오는 데이터를 수집하여 컴퓨팅을 이용하여 결과를 분석 및 예측하는 연구 형태로 변하고 있다. 이를 위해서는 과학기술분야에서는 빅데이터 관리와 컴퓨팅을 활용할 수 있는 플랫폼의 필요성이 대두되고 있다. 시장 조사 기관 IDC의 보고서에 의하면 2021년 국내 빅데이터 분석 시장 규모는 2조 296억 원이며, 2025년 까지 매년 평균 6.9%씩 성장해 매출 규모가 2조 8353억 원에 이를 전망이라고 예상한다[1]. 이와 같이 빅데이터는 국내·외적으로 모든 분야에서 관심이 높다. 또한 과학기술 분야 뿐 만 아니라 기업 연구소등 각계 다양한 분야에서 데이터화를 위해 노력하고 있다.

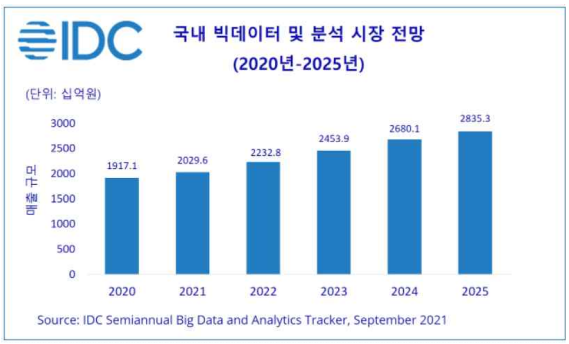


그림 1. 국내 빅데이터 및 분석 시장 전망

과학기술분야에서는 빅데이터 관리 및 컴퓨팅을 활용할 수 있는 플랫폼이 필요하지만, 이러한 플랫폼이 있기 이전에 빅데이터를 빠르게 처리하고 빠르제 전송할 수 있는 인프라가 필요하다. 이를 위해 KISTI에서는 국내 출연연구소를 대상으로 R&E Together라를 프로젝트를 진행 중에 있다. 이 플랫폼은 국내의 빅데이터 전송/관리 및 컴퓨팅 활용을 위한 인프라와 플랫폼을 제공하기 위해 진행하고 있는 프로젝트이다.

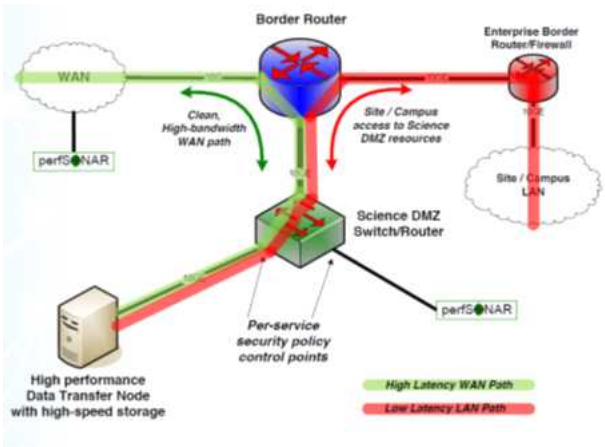


그림 2. ScienceDMZ 구축 환경

빅데이터를 빠르게 처리하고 전송하기 위해서는 ScienceDMZ[2]라는 기술이 필요하다. ScienceDMZ은 빅데이터를 데이터의 손실 없이 빠르게 전송 가능한 네트워크 구조를 변경한 기술이다. ScienceDMZ은 3가지의 중요한 기술을 가지고 있다. 첫 번째는 기존 네트워크의 구조 변경이다. 기존의 네트워크는 사무실에서 사용하는 인터넷망과 연구 데이터를 전송하는 연구망으로 구성되어 있다. 인터넷 망의 패킷로스로 인해 네트워크 성능 저하를 불러온다. 따라서 인터넷 망과 연구망을 분리해야 하며, 데이터 전송 서버의 데이터를 보호하기 위해 다양한 보안장비를 거쳐야 하고, 복잡한 네트워크의 구조를 갖기 때문에 대역폭 대비 전송 성능은 50-60%의

성능을 제공하였다. 하지만 데이터 전송 서버의 네트워크 구조를 다이렉트 또는 VLAN으로 구성하고, 보안 장비를 우회하고 ACL(Access Control List)을 이용하여 보안을 구성할 시 네트워크의 전송 성능은 90% 이상의 성능을 제공한다. 두 번째는 데이터를 전송하는 서버인 Data Transfer Node(DTN) 이다. DTN은 데이터를 전송하는 최적화된 서버로써, 스토리지, 메모리, 네트워크의 빠른 처리를 위해 고성능의 하드웨어로 구성된 서버이다. 고성능 CPU, NVMe, NIC 100GbE 또는 DPU 100GbE을 활용한 서버이다. 세 번째는 모니터링 시스템이다. 모니터링 시스템은 PerfSORNAR(performance Service-Oriented Network monitoring ARchitecture)[3]를 활용하며, 종단 간 사용 예상치를 계산하는데 도움을 주고 네트워크의 연결된 경로의 상태를 제공하도록 설계된 네트워크 측정 도구이다. 세 가지의 구성요소를 통해 ScienceDMZ을 구축할 수 있다.

ScienceDMZ을 구축한 인프라 중에 DTN 서버를 활용하여 빅데이터를 고속으로 전송이 가능하며, 데이터를 전송하는 시간 이외의 유휴시간에는 컴퓨팅을 수행하여 연구 결과를 도출할 수 있도록 구성하기 위한 시스템을 개발한다. ScienceDMZ 구축 과 AI 연구 환경을 제공하는 플랫폼을 같이 구성하기 위한 프로젝트가 R&E Together이다.

본 논문에서는 R&E Together 플랫폼을 활용하여 고속 빅데이터 전송 환경을 제공하며, 컴퓨팅을 수행할 수 있는 기술을 타 분야에 적용하는 사례들을 기술하며, 이 기술의 우수성에 대해 설명하고자 한다.

Ⅱ. R&E Together 프로젝트 구축 및 개발

1) ScienceDMZ 구축

R&E Togehter 프로젝트는 빅데이터를 기관과 기관 간에 고속 데이터 전송을 위한 네트워크를 위해 ScienceDMZ을 구축한다. 각 기관의 ScienceDMZ 네트워크를 구축하기 위해 DTN 서버를 구축하며, ScienceDMZ 구축을 위해서는 Border Router에 DTN 서버를 연결하고 보안 장비들을 우회하여 100G 또는 40G 네트워크 회선을 연결한다. 기관에서 제공할 수 있는 네트워크의 대역폭은 각기 다르지만, 40G 이상의 네트워크를 제공할 때 대역폭 대비 높은 성능을 보장할 수 있다. 그림 3은 각 기관에 구축한 ScienceDMZ 구축 스키마이다.

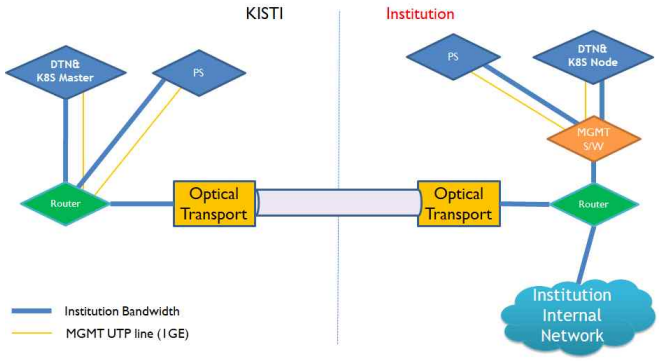


그림 3. ScienceDMZ 구축 스키마

ScienceDMZ 네트워크 구축 또한 중요하지만 DTN 서버의 구성 또한 중요하다. DTN 서버는 데이터 전송을 위한 최적화된 서버로써, CPU를 사용하여 고속 네트워크 전송을 수행하며, 스토리지를 SSD 또는 NVMe를 이용하여 데이터를 전송하게 되면 디스크의 고속 처리가 가능하기 때문에 더 빠르게 디스크 to 디스크 데이터 전송 성능을 향상시킨다. 따라서 DTN 서버의 경우 CPU의 가상화 환경을 구성하지 않고, OS 에서는 데이터의 전달 양을 증가 시킬 수 있는 파라미터들의 설정 값을 최대로 구성한다. 이렇게 구축된 ScienceDMZ 기관과 기관 간에 디스크 to 디스크 전송 성능 결과는 70-80% 정도의 성능 향상을 보인다.

2) AI 연구 환경 제공 플랫폼 개발

출연연구소 기관에 ScienceDMZ구축하고 구축된 기관에 DTN 서버를 설치하였다. 이렇게 설치된 서버들의 구조를 보면 분산 환경을 제공한다. 분산 환경으로 제공되는 이유는 ScienceDMZ의 빅데이터 전송 환경 구축 및 DTN의 데이터를 전송하는 시간 이외의 유휴시간에 컴퓨팅을 수행하기 위함이다. 이러한 인프라 환경에서 AI 연구 환경 제공 플랫폼 개발을 진행하며, 분산된 환경의 서버들을 연계하여 구성하기 위해서 Kubernetes[4] 라는 기술을 이용한다. Kubernetes는 구글에서 개발한 오픈소스로써, Docker 컨테이너 관리를 위해 개발되었으며, 본 시스템은 컨테이너 기반으로 대부분의 서비스를 제공한다. 컨테이너를 사용자들에게 제공하기 위해서는 사용자들이 필요로 하는 인공지능 연구 환경을 위한 이미지를 만들고, 저장하기 위한 공간이 필요하다. 본 시스템에서는 오픈소스 Harbor[5]를 이용하며, Harbor는 프라이빗 이미지 레지스트리로써, 사용자들이 구축한 이미지를 자유롭게 레지스트리에 올리고 사용자간 공유가 가능하며, 그 이미지를 컨테이너로 구성하여 사용할 수 있도록 제공하고 있다.

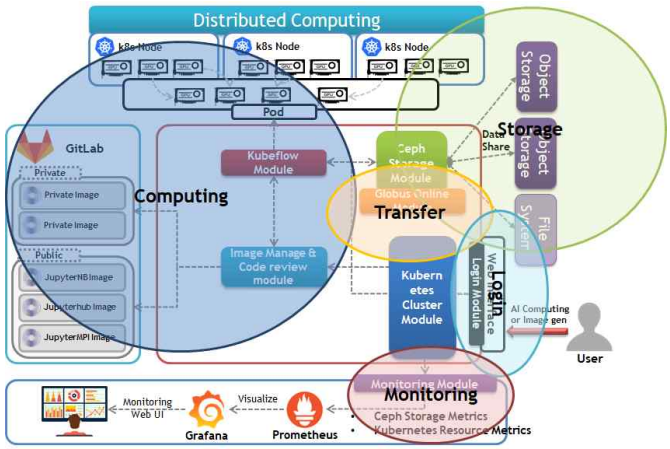


그림 4. AI 연구 환경 제공 플랫폼 구성도

사용자들에게 제공하는 기본적인 이미지는 Jupyter[6]를 제공하고 있으며, Jupyter는 라이브 코드, 등식, 시각화, 설명을 위한 텍스트 등을 포함한 문서를 만들고 공유가 가능한 오픈소스 웹 어플리케이션이다. 최근에는 시뮬레이션, 머신러닝, 통계 분야에서 많이 활용되는 어플리케이션으로 사용자들이 손쉽게 머신러닝을 수행할 수 있도록 웹 UI 기반의 Jupyter Lab을 기본 이미지로 제공하고 있다. 또한 Anaconda 환경을 기본 이미지로 제공하고 있으며, Anaconda는 독립적인 작업환경에서 패키지 관리 및 버전 관리를 위한 가상의 환경을 제공하는 패키지 관리 시스템이다. 두 이미지를 기본으로 제공하며, 사용자는 자신이 원하는 시스템의 환경을 이미지로 구성할 수 있도록 서비스를 제공하고 있다.

Kubernetes에서는 스토리지를 구성할 때, 기본적으로 Local 스토리지를 제공하며, 다른 스토리지 제품들과도 연계가 가능하다. 본 시스템에서는 Ceph[7] 스토리지를 Kubernetes와 연계하여 제공하며, Ceph 스토리지는 단일 분산 컴퓨터 스토리지 환경을 제공하며, 오픈소스 스토리지 플랫폼이다. Ceph은 오브젝트, 블록, 파일 시스템 인터페이스를 제공하지만 본 시스템에서는 오브젝트 스토리지로써 활용된다. Kubernetes에서 컨테이너를 생성하기 이전에 스토리지를 구성하고, 내가 생성한 스토리지를 이용하여 컨테이너를 생성한다. 생성된 스토리지는 오브젝트 스토리지이므로 다른 사용자와 데이터를 교환할 수 있으며, 내가 기존에 사용하던 클라

우드 플랫폼(GCP, AWS, Naver)과 연계하여 데이터를 교환하는 환경 구성 또한 가능하다.

다음으로 모니터링 환경을 제공한다. 모니터링 환경은 Prometheus와 Grafana를 이용하여 리소스 모니터링 환경을 제공한다. 각 사용자는 모니터링 환경을 통해 내가 현재 리소스 사용량을 확인할 수 있고, 지금까지 리소스 총 사용량을 확인할 수 있다. 이를 위해 Namespace로 분류된 컨테이너의 리소스를 모니터링하며, 이를 통해 개인별 사용량의 정도를 확인할 수 있는 구조로 개발하였다.

3) 플랫폼 활용 사례

KISTI에서는 무선 네트워크를 위한 다양한 기술들을 개발하고 있으며, 최근에는 LoRa 기술[8]을 이용하여 센서로 부터 데이터를 모아 연구자들에게 제공하는 연구를 하고 있다. 이와 같이 무선 네트워크 기술과 연계하게 되면, Edge-Computing 구조를 구성할 수 있다. 무선 센서에서 추출된 데이터들을 R&E Together 인프라를 이용하여 AI 인공지능 플랫폼으로 전송하고 전송된 데이터들은 가까운 DTN 서버에서 컴퓨팅을 이용하여 사용자가 결과를 손쉽게 가져갈 수 있는 Edge-Computing 구조의 플랫폼을 추후 사용할 예정이다.

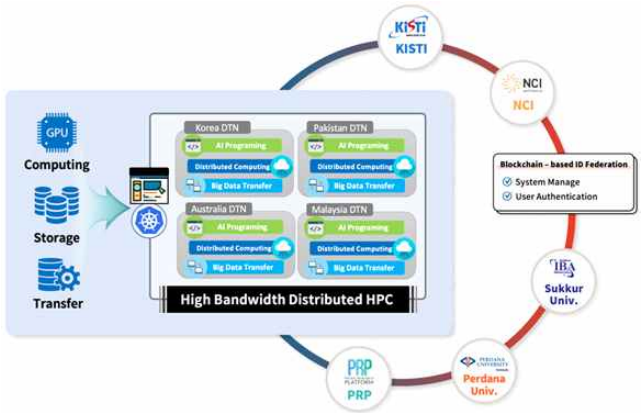


그림 5. Asi@Connect 사업 시스템 구성도

KISTI에서는 아시아 지역의 ScienceDMZ 인프라를 연결하고 KISTI에서 개발한 AI 연구 환경 제공 플랫폼을 제공하여 개발도상국들의 인공지능 연구를 위한 Asi@Connect 사업을 진행하고 있다. 이 사업은 개발도상국에 지원 사업으로 KISTI는 아시아지역의 ScienceDMZ 리딩 역활과 동시에 데이터 전송 플랫폼을 아시아 지역에 구축 및 연계하여 개발도상국에 부족한 인프라를 제공하고 연구자들에게 인공지능을 연구할 수 있는 환경을 제공해주고, 인공지능 연구 생산성 향상을 위해 노력하고자 한다.

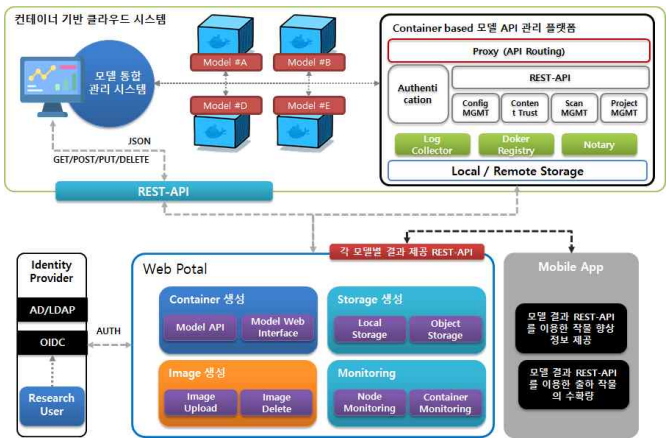


그림 6. 농업 빅데이터 플랫폼 전체 구성도

농업 분야의 지능화를 위해 다양한 농업 품종에 대한 데이터를 수집하고 수집된 데이터들의 인공지능 모델을 적용하여 이번 년도의 다양한 품종들의 출하량 또는 생산량을 확인할 수 있는 시스템을 구축하고자 한다. 이와 관련하여 농진청에서 발주한 과제를 서울대 농대와 함께 진행하고 있으며, 이 과제를 통해 농민들에게 지능화된 정보를 제공할 수 있도록 R&E Together의 플랫폼을 적용 및 개발하여 농업 분야의 빅데이터 관리 및 처리를 위한 플랫폼으로 제공될 예정이다.

Ⅲ. 결론

과학기술분야에서 데이터의 수집 및 처리를 위한 다양한 연구들이 진행되고 있다. 하지만 과학기술분야의 기관들은 빅데이터를 전송하기 위한 인프라의 부족과 컴퓨팅을 제공할 수 있는 시스템의 부재 등의 문제에 직면하여 있다. 이와 같은 문제를 해결하기 위해 KISTI에서는 R&E Together 이라는 프로젝트를 진행하고 있다. 이 프로젝트는 출연연구소를 대상으로 빅데이터 전용의 네트워크인 ScienceDMZ 네트워크 구축과 인공지능 연구 환경을 제공할 수 있는 플랫폼을 개발하여 연구자들에게 제공하기 위한 프로젝트이다. R&E Together 프로젝트는 고성능의 ScienceDMZ 네트워크와 DTN 서버를 이용하여 네트워크 전송 환경을 구성하고, 그 위에 Kubernetes 컨테이너 매니지먼트 시스템을 이용한 컨테이너 기반의 Jupyter, Anaconda 환경의 시스템을 연구자들에게 제공하기 위한 서비스이다.

이 프로젝트를 통해 국내 출연연의 인공지능 연구 생산성을 향상시키고 또한 타 분야의 인공지능 연구 융합을 위해 노력하고 있다. 이 뿐만 아니라 이러한 플랫폼을 활용하여 타 분야에 적용할 수 있다. 그 예로 Edge-Computing, Asi@Connect 사업, 농업 분야의 빅데이터 관리 및 처리를 위한 플랫폼으로 활용될 예정이다.

추후에는 R&E Together 프로젝트와 Asi@Connect 프로젝트를 연계하여 하나의 거대한 아시아 지역의 컴퓨팅을 활용할 수 있는 연계 서비스를 개발하여 거대한 분산 컴퓨팅 환경으로 사용 가능하도록 구성할 예정이다.

ACKNOWLEDGMENT

본 연구는 2022 년도 한국과학기술정보연구원(KISTI) 주요사업 과제로 수행한 것입니다.

참 고 문 헌

[1] IDC Korea."국내 빅데이터 및 분석 시장 전망 , 2021-2025 ," web site, Retrieved, 04, 12, 2022, https://www.idc.com/kr

[2] Dart, Eli, Lauren Rotman, Brian Tierney, Mary Hester, and Jason Zurawski. "The science dmz: A network design pattern for data-intensive science." Scientific Programming 22, no. 2 (2014): 173-185.

[3] PerfSONAR, web site, Retrieved, 04, 12, 2022, https://www.perfsonar.net/

[4] Kubernetes, web site, Retrieved, 04, 12, 2022, https://kubernetes.io/

[5] Jupyter, web site, Retrieved, 04, 12, 2022, https://jupyter.org/

[6] Harbor, web site, Retrieved, 04, 12, 2022, https://goharbor.io/

[7] Ceph, web site, Retrieved, 04, 12, 2022, https://ceph.com

[8] Kim, C.; Kim, J.; Kim,K.H.; Lee, S.K.; Kim, K.; Shah, S.A.R.; Goo,

Y.H. “ScienceIoT: Evolution of the Wireless Infrastructure of KREONET”. Sensors 2021, 21, 5852.

TS6:
블록체인2 : 가상자산서비스

코스모스에서 블록체인 간 메시지 전달 시간 측정 및 분석

김정연*, 주홍택

*계명대학교 컴퓨터공학과

*jungyeonkim@stu.kmu.ac.kr, juht@kmu.ac.kr

Inter-Blockchain Communication Message Relay Time Measurement and Analysis in Cosmos

Jungyeon Kim*, Hongteak Ju

*Dept. of Computer Engineering, Keimyung Univ.

요 약

코스모스는 기존 블록체인의 확장성 문제를 해결하기 위해 블록체인 간 통신 프로토콜을 적용하여 이기종 블록체인을 연결하는 수평적 스케일링을 달성했다. 코스모스는 블록체인 간 트랜잭션 비율이 증가함에 따라 전체 네트워크 초당 거래 처리량이 감소되는 문제가 있다. 이러한 문제 해결 방안은 체인 간 연결에 대한 기초 연구를 바탕으로 도출되어야 한다. 본 논문은 코스모스에서 블록체인 간 메시지 전달 시간 측정 시스템을 제안하고 체인 간 대체 가능 토큰 전송의 경우에 블록체인 간 메시지 전달 시간을 수집 및 분석한다.

Ⅰ. 서 론

코스모스(Cosmos)는 서로 다른 독립 블록체인들이 통신할 수 있도록 연결하는 플랫폼이다[1]. 기존 블록체인은 에너지 비효율, 제한적인 거버넌스 메커니즘과 확장성(Scalability) 문제를 가지고 있다[2, 3]. 이를 해결하기 위해 코스모스는 블록체인 간 통신 프로토콜(Inter-Blockchain Communication, IBC)로 여러 병렬 블록체인을 연결하는 수평적 스케일링(Horizontal Scaling)을 달성했다[4]. 코스모스 네트워크에 연결된 블록체인은 이론적으로 무한히 확장 가능한 성능을 가질 수 있으나, 체인 간 긴 메시지 전달 시간으로 인해 전체 초당 거래 속도(Transactions Per Second, TPS)가 느려지는 문제가 있다. 이러한 문제 해결 방안은 블록체인 간 메시지 전달 시간 측정과 체인 간 연결에 대한 기초 연구를 바탕으로 도출되어야 한다.

본 논문은 코스모스에서 블록체인 간 통신 메시지 전달 시간 측정 방법을 제안한다. 제안하는 블록체인 간 메시지 전달 시간 측정 시스템은 코스모스 허브(Cosmos Hub)와 오스모시스(Osmosis) 메인넷에서의 성능을 측정하고 구간별로 분석한다. 블록체인 간 메시지 전달 과정을 수집·분석하여 블록체인 상호 운용성 성능 개선 연구를 위한 기초 자료로 사용할 수 있다.

본 논문의 2장은 코스모스의 블록체인 간 통신 프로토콜과 기존 블록체인 상호 운용성 솔루션 연구를 제시한다. 3장은 코스모스에서 블록체인 간 메시지 전달 시간 측정 방법에 대해 설명한다. 4장에서 수행한 실험 결과를 분석하고 5장은 본 논문의 결론을 다루며 논문을 마친다.

Ⅱ. 배경 및 관련 연구

코스모스는 독립적인 병렬 블록체인의 분산 네트워크다. 코스모스를 통해 서로 다른 블록체인은 주권을 유지하고 트랜잭션을 빠르게 처리하며, 다른 블록체인과 통신할 수 있어 수평적 스케일링의 이점을 얻을 수 있다. 코스모스는 그림 1과 같이 이종 블록체인인 존(Zone)과 각 존이 상호 작용할 수 있도록 최신 상태를 지속적으로 스트림하는 허브(Hub)로 구성되어 있다[1]. 모든 존은 허브를 통해 토큰과 데이터를 서로 전송할 수 있다. 허브는 모든 존에 걸쳐 각 토큰 총액의 전역적 불변성(Global Invariance)을 보존한다. 블록체인 간 통신 (Inter-Blockchain Communication, IBC) 프로토콜은 이종 블록체인 간 최소한의 필수 공통 인터페이스만 공유하면서 안전하고 자발적으로 상호 작용할 수 있는 메커니즘을 제공한다. 블록체인 간 통신 프로토콜은 코스모스 허브(Cosmos Hub), 오스모시스(Osmosis), 바이낸스 체인(Binance Chain) 등과 같이 텐더민트(Tendermint) 기반인 블록체인과 상호 작용 시에 사용할 수 있다[5]. 비트코인(Bitcoin), 이더리움(Ethereum)과 같이 텐더민트 기반이 아닌 블록체인은 페그존(Peg-zone)이라는 특수한 유형의 존이 사용된다.

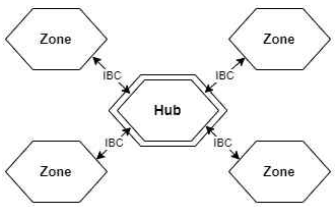


그림 1. 코스모스 네트워크에서 허브와 존

2.1 코스모스의 블록체인 간 통신 프로토콜

코스모스의 블록체인 간 통신 프로토콜은 독립 블록체인에 있는 모듈 간의 신뢰할 수 있고, 인증된 통신을 위한 엔드 투 엔드(End-to-End) 연결 지향 프로토콜이다[6]. 블록체인 간 통신 프로토콜은 알려지지 않은 동적 토폴로지에 배치된 이기종 블록체인 간의 상호 운용을 위해 설계되었으며 다양한 합의 알고리즘과 상태 머신으로 작동한다.

그림 2는 IBC 프로토콜을 사용하여 블록체인 A에서 이기종 블록체인 B로 대체 가능 토큰 전송(Fungible Token Transfer)하는 과정을 보여준다. 블록체인 A 네트워크에 참여하고 있는 송신 노드는 노드 내 애플리케이션 레이어(Application Layer)에서 블록체인 B의 수신 지갑 주소로 IBC

토큰 전송을 요청한다. 요청을 수신한 IBC 레이어는 전달받은 정보로 송신 지갑 주소, 수신 지갑 주소, 토큰의 양, 토큰 단위, 송신 포트, 송신 채널을 입력하고 시간 초과 블록 높이, 타임스탬프와 시퀀스(Sequence)를 추가하여 IBC Transfer 트랜잭션을 발행한다. 시퀀스는 제네시스 블록부터 생성된 특정 채널(Channel)을 통해 생성된 거래 총 수이며, 특정 거래를 가리킨다. 한 건의 거래에 대한 모든 IBC 트랜잭션은 동일한 시퀀스 값을 가지고 있다[7]. IBC Transfer 트랜잭션은 블록체인 레이어를 통해 송신 노드와 연결된 피어로 전파된다. 트랜잭션이 블록에 포함되어 결제의 완결성(Settlement Finality)을 가지게 되면 블록체인 A에서 IBC Transfer 트랜잭션의 토큰은 잠금(Token Lock) 처리된다. IBC 아키텍처에서 블록체인은 네트워킹 인프라를 통해 서로 메시지를 직접 보내는 것이 아니라 보낼 메시지를 생성한 다음 중계자(Relayer)를 통해 송신 블록체인에서 수신 블록체인으로 물리적으로 중계된다. 중계자는 IBC 프로토콜이 구현된 블록체인의 상태를 지속적으로 스캔하고 IBC 트랜잭션이 있을 때 중계해야 한다. 그림 2에서 중계자들은 블록체인 A와 블록체인 B 네트워크에 모두 참여하고 있다. 중계자 운영은 누구나 할 수 있으며, 중계하는 블록체인에 따라 거래 수수료로 보상받을 수 있다[8]. 중계자는 전달할 IBC 트랜잭션을 종합(Bundling)하여 수신 블록체인 B로 보내는 IBC RecvPacket을 포함한 IBC 트랜잭션을 발행 및 중계한다. 수신 블록체인에서 IBC 트랜잭션은 커밋(Commit)되기 전에 IBC 레이어의 라이트 클라이언트(Light Client)를 사용하여 유효성을 확인한다. 블록체인 B에서 IBC RecvPacket 트랜잭션이 완결성을 가지면 수신 지갑 주소로 바우처(Voucher)가 민팅(Minting)된다. 또한, 중계자는 수신 블록체인에서 토큰 전송 완료를 알리는 IBC Acknowledgement 트랜잭션을 구성하여 중계한다. 송신 블록체인 A는 IBC Acknowledgement 트랜잭션을 블록에 포함시켜 토큰 전송이 정상적으로 완료되었음을 증명한다. 위 과정은 그림 2의 과정 1단계부터 12-1, 12-2단계까지 순서대로 볼 수 있다.

IBC는 분산 네트워크를 통해 작동하고 잠재적으로 결함이 있는 중계기에 의존하여 메시지를 중계하므로 트랜잭션이 시간 내에 또는 목적지로 전송되지 않는 경우를 처리해야 한다. 비정상적으로 IBC RecvPacket이 블록에 포함되지 못한 경우, 중계자는 IBC Timeout 트랜잭션을 생성 및 전달한다. 이를 수신한 송신 블록체인이 IBC Transfer 트랜잭션의 토큰 해제(Token Unlock) 프로세스를 실행한다[5].

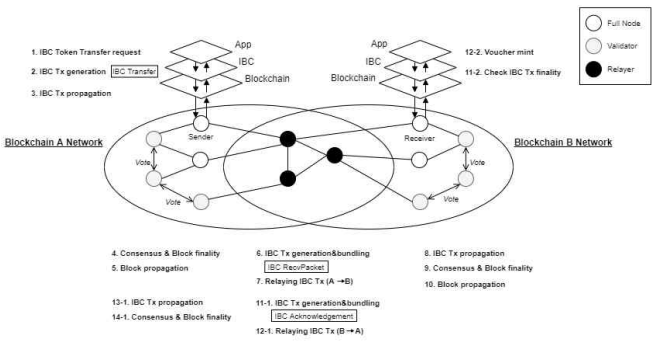


그림 2. 대체 가능 토큰 거래 과정

2.2 관련 연구

J. Han [9]은 CBDC(Central Bank Digital Currency)를 위한 블록체인 상호운용성을 보장하는 Cosmos 블록체인 기반 Cos-CBDC를 제안했다. 네트워크 지연을 고려하지 않기 위해 동일한 네트워크에서 구현 및 실험 결과로 Cos-CBDC의 성능이 블록체인의 수에 따라 향상되는 것으로 나타났다. 체인 간 트랜잭션은 체인 내 트랜잭션보다 네트워크 트래픽 및 대기 시간 측면에서 낮은 성능을 보이고 있으며, 사이드 체인이나 이기종 블록체인 연결이 전체 시스템 성능을 저하시킬 수 있다고 언급했다.

L. Kan [10]은 이종 블록체인 간 통신을 위한 대화형 다중 블록체인 아키텍처(Interactive Multiple Blockchain Architecture)를 제안했다. 제안한 아키텍처에서 체인 간 상호운용성을 위해 노드를 라우터 블록체인(Router Blockchain)으로 사용한다. 라우터 역할을 하는 노드는 동적 블록체인 네트워크를 생성하여 체인 간 트랜잭션을 전달한다. 라우터 블록체인이 주고받는 통합 트랜잭션 형식을 제안하고, 서로 다른 블록체인 간의 일관성을 유지하기 위한 교차 체인 프로토콜은 3단계 커밋 방법을 사용한다. 성능 측정 실험에서 체인 내 트랜잭션은 평균 1520.56TPS인 반면 체인 간 트랜잭션은 최대 899.81TPS로 보다 낮은 성능을 보인다. TPS 감소는 주로 라우터 블록체인 간에 통합 트랜잭션을 확인하는 단계에서 발생하였다.

위 연구에서 사용된 공증인 제도(Notary Scheme) 솔루션, 블록체인 라우터 솔루션과 같은 대부분의 상호운용성 솔루션은 중계자를 사용하여 체인 간 통신을 연결한다[11]. 이러한 아키텍처에서 체인 간 메시지 전달 성능은 전체 트랜잭션 처리 속도에 영향을 줄 수 있다. 이를 위해 상호 운용 가능한 블록체인 네트워크에서 체인 간 통신에 대한 측정 및 분석 연구가 필요하다.

Ⅲ. 블록체인 간 메시지 전달 시간 측정 환경 구성 및 방법

본 연구의 블록체인 간 메시지 전달 시간 측정 시스템의 구조는 그림 3과 같다. 실험을 위해 측정 클라이언트(Measurement Client), SPV 클라이언트를 운영하고 실험값을 추출한 Raw 데이터를 데이터베이스나 Log File로 저장한다. Raw 데이터의 타임스탬프를 기준으로 블록체인 간 메시지 전달 시간을 계산하고 이에 대한 통계 및 구간 분석을 실행한다.

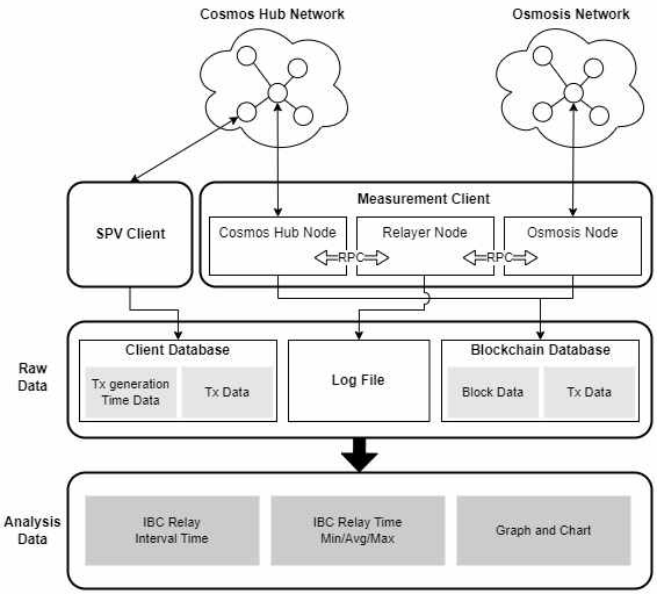


그림 3. 블록체인 간 메시지 전달 시간 측정 시스템 구성

3.1 측정 환경

측정 클라이언트가 설치된 컴퓨터는 intelCore i9-7900X 3.30GHz, 4TB SSD, 64GB RAM을 사용하며 운영체제는 Linux 20.04 버전이다. 측정 클

라이언트를 운영하기 위해 1대의 컴퓨터에 중계자 프로그램과 코스모스 노드, 오스모시스 노드를 설치하고 각 네트워크에 연결하여 블록 동기화 완료 후 진행한다. 중계자 프로그램은 원격 프로시저 호출(RPC)을 사용하여 로컬 호스트(Localhost) 내의 블록체인 최신 상태를 스캔하거나 트랜잭션을 제출할 수 있다. 중계자는 상대 블록체인에 트랜잭션을 제출할 수 있도록 일정 코인을 보유한 지갑을 연결해야 한다. 대체 가능 토큰 거래(Fungible Token Transfer)를 발생시키는 SPV 클라이언트는 Cosmostation을 사용한다. 표 1은 블록체인 간 메시지 전달 시간 측정에 사용된 소프트웨어를 설명한다.

표 1. IBC 메시지 전달 시간 측정 구성 요소

구성 요소	사 양
Go-Language	Ver 1.17.4
Gaia	Ver 7.0.0
Osmosis	Ver 7.0.3
Relayer	Go-Lang Ver 2.0.0
Cosmostation	Ver 1.5.45

3.2 블록체인 간 메시지 전달 시간 측정 방법

본 연구는 코스모스에서 블록체인 간 메시지 전달 시간을 측정하기 위해 코스모스 허브에서 오스모시스로 토큰 전달 트랜잭션을 생성하고 시간 데이터를 수집한다. 코스모스 허브 네트워크와 연결된 SPV 클라이언트는 오스모시스로 보내는 토큰 전달 트랜잭션을 생성한다. 측정 클라이언트는 SPV 클라이언트가 생성한 토큰 전달 트랜잭션을 각각의 블록체인 메인넷(Mainnet)에 중계하기 위해 코스모스 허브 노드와 오스모시스 노드를 운용한다. 측정 클라이언트의 중계자는 코스모스 허브 블록체인과 오스모시스 블록체인을 RPC로 연결하여 최신 상태를 수집하고 IBC 트랜잭션을 제출한다. SPV 클라이언트와 측정 클라이언트에서 대체 가능 토큰 전달을 수행하고 수행 중 생성되는 트랜잭션 생성 및 블록 시간에 대한 데이터를 수집한다. SPV 클라이언트에서 토큰 전달 트랜잭션을 생성하고 해당 트랜잭션 정보와 생성 시간 정보를 Client 데이터베이스에 저장한다. 코스모스 허브와 오스모시스 노드로부터 SPV 클라이언트의 지갑 주소가 포함된 IBC 트랜잭션과 트랜잭션이 포함된 블록 정보를 수집하여 Blockchain 데이터베이스에 저장한다. 중계자는 이종 블록체인 간의 중계 과정을 로그 파일에 저장한다. 중계 과정 로그 파일에서 SPV 클라이언트가 생성한 토큰 전달 트랜잭션의 중계 과정 데이터만 추출하여 Log File로 저장한다. 한 건의 토큰 전달에서 Client 데이터베이스의 IBC Transfer 트랜잭션 정보와 Blockchain 데이터베이스의 IBC RecvPacket과 IBC Acknowledge-ment 트랜잭션의 연결은 채널과 시퀀스 값으로 추적할 수 있다.

전체 블록체인 간 메시지 전달 시간은 IBC Transfer 트랜잭션 생성 시간부터 IBC Acknowledgement 트랜잭션이 포함된 블록 생성 시간까지다. 본 논문에서는 그림 4를 바탕으로 블록체인 간 메시지 전달 과정을 5개의 구간으로 나누어 분석을 진행한다. IBC Transfer 트랜잭션 생성 시간부터 IBC Transfer 트랜잭션이 포함되어 블록이 생성된 시간까지 구간 1로 분류한다. 구간 1에서는 코스모스 허브 네트워크에서 트랜잭션 전파와 블록 합의가 진행된다. IBC Transfer이 포함된 블록 생성 시간부터 IBC RecvPacket 트랜잭션이 생성된 시간까지 구간 2로 분류한다. 구간 2에서는 코스모스 허브의 블록 전파와 중계자의 패킷 생성이 진행된다. 생성된 IBC RecvPacket이 오스모시스 블록체인에 포함되는 시간까지는 구간 3이다. 구간 3에서는 중계자의 IBC 트랜잭션 전달 및 오스모시스 네트워크에서 트랜잭션 전파와 블록 합의가 진행된다. 오스모시스에 블록 생성 후, 중계기가 IBC Acknowledgement 트랜잭션을 생성하는 시간까지는 구간 4이다. 구간 4는 오스모시스 블록 전파 성능과 중계자 알고리즘 성능 지표가 될 수 있다. 생성된 IBC Acknowledgement가 전파되어 코스모스 블록체인에 포함되는 시간까지 구간 5로 나눈다. 사용자가 SPV 클라이언트로부터 IBC 거래를 완료하였다는 안내를 받는 시점은 IBC Acknowledge-ment 트랜잭션이 블록에 포함된 후, 블록 전파와 SPV 클라이언트의 거래 확인 처리 시스템의 영향을 받는다. 이는 코스모스 블록체인의 IBC 거래 과정이 아닌 클라이언트 처리 과정이기 때문에 구간 5는 IBC Acknowledgement가 포함된 블록 생성 시간을 기준으로 측정한다. 위와 같이 블록체인 간 메시지 전달 과정을 구간별로 나누어 전체 전달 시간에 영향을 주는 처리 과정을 더 정확하게 파악한다.

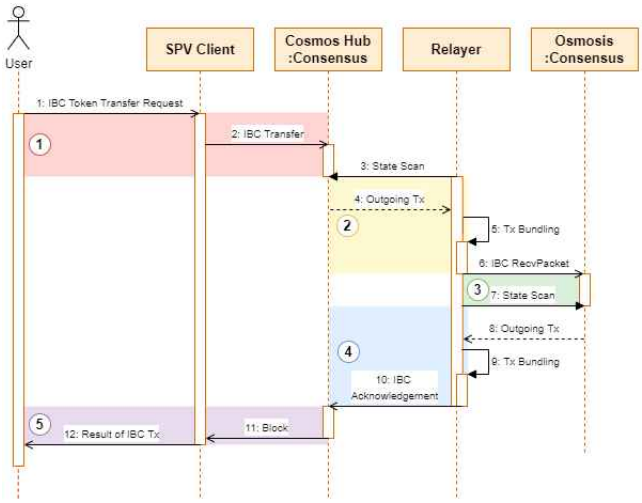


그림 4. 블록체인 간 메시지 전달 과정

Ⅳ. 블록체인 간 메시지 전달 시간 측정 결과

코스모스 허브에서 오스모시스로 대체 가능 토큰 전달을 30회 실시하여 측정한 결과는 표 2와 같다. 블록체인 간 메시지 전달 시간은 평균 69.7초가 걸린다. 최소 전달 시간과 최대 전달 시간은 약 2배 이상 차이를 보인다. 분산은 404.27초 표준편차 20.10초이고 이는 전체 측정값이 평균값으로부터 넓게 퍼져있음을 나타낸다.

표 2. 블록체인 간 메시지 전달 시간 통계

평균	최소	최대	분산	표준편차
69.7초	44초	116초	404.27초	20.10초

블록체인 간 메시지 전달 시간을 측정 지점에 따라 다섯 구간으로 분류한 결과는 표 3과 같다. 구간 1은 IBC Transfer 트랜잭션이 생성 및 전파되고 합의 과정을 거친 시간이다. 텐더민트(Tendermint) 합의 엔진은 검증인이 100명일 때 대략 2초에서 3초 사이에 블록을 생성한다[12]. 실험을 진행한 2022년 4월 기준으로 코스모스 허브의 검증인은 175명이며, 합의 시간은 약 7.4초이다[13]. 이를 참작하여 구간 1의 평균 11.33초 중에서 코스모스 허브에서 트랜잭션 생성 및 전파하는 시간이 약 3.93초가 소요됨을 알 수 있다. 오스모시스의 검증인은 135명이며, 합의 시간은 약 6.53초이다[14]. 구간 3의 12.6초 중 오스모시스에서 트랜잭션 전파 과정의 소요 시간이 약 6.07초로 추측된다.

표 3. 블록체인 간 메시지 전달 시간 구간 별 통계

항목\구간	1	2	3	4	5
평균	11.33초	10.3초	12.6초	11.4초	24.06초
백분율	16%	15%	18%	16%	35%

블록체인 간 메시지 전달 시간 중 구간 1, 3, 5는 체인 내 트랜잭션 전파 및 합의 시간으로 각 블록체인 TPS 성능을 나타낸다. 구간 2와 4는 체인 간 트랜잭션 생성 및 전달 시간으로 체인 내 트랜잭션 소요 시간과 비등한 수준으로 전체 블록체인 간 메시지 전달 속도에 영향을 줄 수 있다. 또한, 전체 블록체인 간 메시지 전달 시간 중 구간 5가 가장 많은 시간을 소요하고 있다. 구간 5는 중계자가 IBC Acknowledgement 트랜잭션을 생성한 시점부터 IBC Acknowledgement 트랜잭션이 포함된 블록 생성 시간까지로 코스모스 허브 네트워크에서 트랜잭션 전파 및 합의가 진행되는 시간이다. 그림 5에서 전달 시간 순으로 정렬하고, 구간에 따라 분류한 결과로 구간 5가 전체 블록체인 간 메시지 전달 과정을 지연시키고 있음을 확인했다.

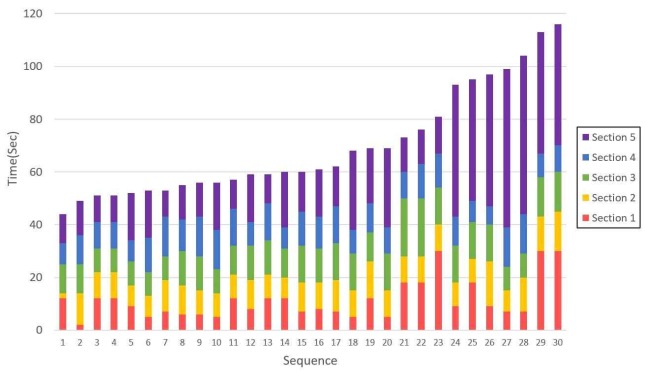


그림 5. 블록체인 간 메시지 전달 시간 정렬 그래프

V. 결 론

본 논문에서는 코스모스에서 블록체인 간 메시지 전달 시간 측정 방법을 제안한다. 제안하는 방법은 메인넷에 IBC 트랜잭션을 실제로 생성 및 전송하여 트랜잭션 전파 시간을 확인한다. 또한, 중계자를 운용하여 체인 간 트랜잭션 전파 시간을 측정한다. 실제 운용을 통해 측정 가능한 지점을 추가하여 블록체인 간 메시지 전달 시간을 구간 별 측정을 수행하였다. 실험을 통해 코스모스에서 오스모시스로의 대체 가능 토큰 전송은 평균 69.7초에 수행 완료하는 것을 보였다. 구간 별 시간 측정으로 중계와 IBC Acknowledgement 트랜잭션 처리 과정이 블록체인 간 메시지 전달 시간에 영향을 주고 있음을 확인했다. 따라서 향후 블록체인 간 메시지 전달에서 성능 지연의 원인 분석에 대한 연구를 진행할 예정이다.

ACKNOWLEDGMENT

이 논문은 2018년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(NRF-2018R1D1A1B07050380).

참 고 문 헌

[1] Kwon, Jae, and Ethan Buchman, "Cosmos whitepaper.", 2019. (https://v1.cosmos.network/resources/whitepaper)

[2] Q. Zhou, H. Huang, Z. Zheng and J. Bian, "Solutions to Scalability of Blockchain: A Survey," in IEEE Access, vol. 8, pp. 16440-16455, 2020.

[3] Surya Viswanathan and Aakash Shah, “The Scalability Trilemma in Blockchain”, 2018. (https://aakash-111.medium.com/the-scalability-trilemma-in-blockchain-75fb57f646df)

[4] Tendermint Inc, “What is Cosmos?”, 2019. (https://v1.cosmos.network/intro)

[5] Interchain GmbH, “IBC Overview”, 2021. (https://ibc.cosmos.network/main/ibc/overview.html)

[6] Goes, Christopher. "The interblockchain communication protocol: An overview." arXiv preprint arXiv:2006.15918 (2020).

[7] Goes, Christopher., “ics-020-fungible-token-transfer”, 2020. (https://github.com/cosmos/ibc/tree/master/spec/app/ics-020-fungible-token-transfer)

[8] Interchain GmbH, “Relayer”, 2021. (https://github.com/cosmos/relayer/tree/v1.0.0)

[9] Han, Jungsu, et al. "Cos-CBDC: Design and Implementation of CBDC on Cosmos Blockchain." 2021 22nd Asia-Pacific Network Operations and Management Symposium (APNOMS). IEEE, pp. 303-308, 2021.

[10] Kan, Luo, et al. "A multiple blockchains architecture on inter-blockchain communication." 2018 IEEE international conference on software quality, reliability and security companion (QRS-C). IEEE, pp. 139-145, 2018.

[11] Qasse, Ilham A., Manar Abu Talib, and Qassim Nasir. "Inter blockchain communication: A survey." Proceedings of the ArabWIC 6th Annual International Conference Research Track, Article 2, pp. 1 - 6, 2019.

[12] Gautier MARIN, “A tour of Cosmos for Developers”, 2017. (https://blog.cosmos.network/a-tour-of-cosmos-for-developers-7517ba1b4045)

[13] Cosmostation, “Mintscan - cosmos chain explorer”, 2022. (https://www.mintscan.io/cosmos/validators)

[14] Cosmostation, “Mintscan - osmosis chain explorer”, 2022. (https://www.mintscan.io/osmosis/validators)

블록체인 기반 커뮤니티 서비스 설계

김다운, 박세진
계명대학교
ekdns990@naver.com, baksejin@kmu.ac.kr

A Design of Community Service based on Blockchain

Daun Kim, Sejin Park
Keimyung Univ.

요 약

인터넷 발전으로 인해 거대한 정보 교류의 장이 된 커뮤니티는 중앙 서버로 서비스되고 있다. 즉, 커뮤니티에 가입한 사용자의 개인정보와 특정 집단을 위해 게시한 게시물의 정보가 모두 중앙 서버에 저장된다. 따라서 중앙 서버가 해커로부터 공격당할 경우 데이터 위변조 가능성이 존재하여 보안 측면에서 문제점이 발생한다. 커뮤니티의 중앙화된 구조로 인한 DDoS 공격 또한 빈번히 발생하는 상황이다. 본 논문에서는 이러한 문제점을 해결하는 탈중앙화 형태의 커뮤니티 서비스를 제안한다. 본 논문이 제시하는 서비스는 블록체인인 Ethereum과 스마트 계약을 활용하여 사용자와 기본 데이터를 블록체인에 저장함으로써 데이터의 무결성을 보장하고 P2P 방식의 분산 저장 기술을 통하여 DDoS 공격을 해결한다. 본 논문에서는 서비스의 설계 내용인 전체 시스템과 데이터 저장 구조, 주요 기능의 동작 과정을 기술하고 블록체인과 외부 스토리지를 연계한 고성능 커뮤니티 서비스를 구상한다. 데이터 저장 구조를 구성하는 블록체인과 외부 스토리지 성능 실험을 진행한 결과 외부 스토리지의 저장 속도가 24배 빨랐다.

1. 서 론

인터넷이 발전하며 사이버 스페이스를 이용한 커뮤니티가 활성화되었다. 이러한 온라인 커뮤니티는 거리의 제약 없이 공통의 관심사를 가진 사용자 간의 정보 공유를 가능하게 한다. MZ세대의 70% 이상이 온라인 커뮤니티를 사용하고 있다는 최근 연구의 조사 결과를 참고하면, MZ세대를 중심으로 커뮤니티에 대한 사용률이 매우 높다[1]. 하지만 대중적으로 이용되는 온라인 커뮤니티는 중앙화 형태의 구조로 이루어져 있어 보안 측면에서 문제점이 발생한다. 즉 사용자의 정보, 커뮤니티 사용자 간 공유하는 정보들로 구성된 중요 데이터가 모두 중앙 서버에 저장되어 해킹으로 인한 데이터 유출 우려가 있으며 데이터 위변조의 위험으로 사용자가 잘못된 정보를 습득할 수 있다. 또한, 사용자가 많은 유명 커뮤니티들은 악의적 의도를 가진 해커에 의한 DDoS 공격에 쉽게 노출된다.

먼저 가장 많은 일일 방문자 수를 보유한 커뮤니티 웹사이트의 경우[2] 중앙 서버가 10차례 이상 DDoS 공격에 노출되어 서비스 이용 장애 피해를 본 바가 있다. 웹호스팅 서비스를 제공한 업체가 지속해서 대응했음에도 DDoS 공격은 5일 동안 이어졌다[3]. 이처럼 예상 불가능한 공격으로 인해 사용자는 간헐적으로 발생하는 접속 장애로 커뮤니티 이용에 불편함을 느낀다.

또한, 실제 커뮤니티 회원 수 260만 명에 달하는 커뮤니티의 경우[4], 중앙화된 형태의 구조로 인해 개인 정보 유출이 발생한 전적이 있다. 이러한 해킹은 사용자의 아이디와 패스워드를 포함한 정보들이 해커에 의해 유출되기에 정보가 유출된 사용자에게 큰 두려움이 따른다.

본 논문에서는 이러한 문제점을 해결하기 위해 블록체인 기반 탈중앙화 형태의 커뮤니티 서비스를 제안한다. 본 논문은 관련 연구로 블록체인과 Ethereum, 스마트 계약을 소개하고 제안하는 시스템의 아키텍처와 데이터 저장구조, 주요 기능의 동작 과정, 실험, 결론으로 구성된다.

2. 관련 연구

본 장에서는 제안하는 서비스와 연관된 블록체인과 Ethereum[5], 스마트 계약 연구를 기술한다.

2.1 블록체인

블록체인[6] 기술은 가상화폐인 비트코인[7] 모델의 바탕이 된다. 전자화폐 따위의 데이터를 중앙 서버에 저장하지 않고 P2P 네트워크 자원을 활용해 네트워크에 참여하는 모든 노드가 개별적 거래를 확인하고 승인하여 거래 내용을 참여 노드가 유지하는 것이 블록체인의 원리이다. 이때 승인된 거래 내용이 저장되는 블록은 부모를 암호화 방식으로 참조하여 서로 연결된 체인의 형태를 띤다. 블록체인은 네트워크상에 존재하므로 모든 노드가 거래 내용을 감독하여 데이터의 신뢰성을 보장하는 동시에 데이터의 위변조 가능성을 차단한다.

2.2 Ethereum

Ethereum은 네트워크의 노드에서 업데이트되고 공유되는 공용 데이터베이스 역할을 수행하는 스마트 계약 플랫폼이다. Ethereum의 기본 암호화폐는 이더(Ether)이며, 트랜잭션 요청을 브로드캐스트하는 노드는 일정의 수수료인 GAS를 지급해야 한다. 이 수수료는 거래를 확인하고 블록에 등록하여 브로드캐스팅하는 작업을 한 노드에게 제공된다. 이러한 메커니즘이 작업 증명 합의이다.

또한 Ethereum은 블록체인 네트워크의 모든 노드가 상태를 저장하고 동의하는 글로벌 가상 컴퓨터인 EVM[5](Ethereum Virtual Machine) 이 존재한다. 참여 노드는 EVM의 상태 사본을 보관하고 EVM에서 임의의 코드 실행을 요청한다. 코드 실행 시 상태가 변경되며 변경된 내용은 전체

네트워크에 전파된다.

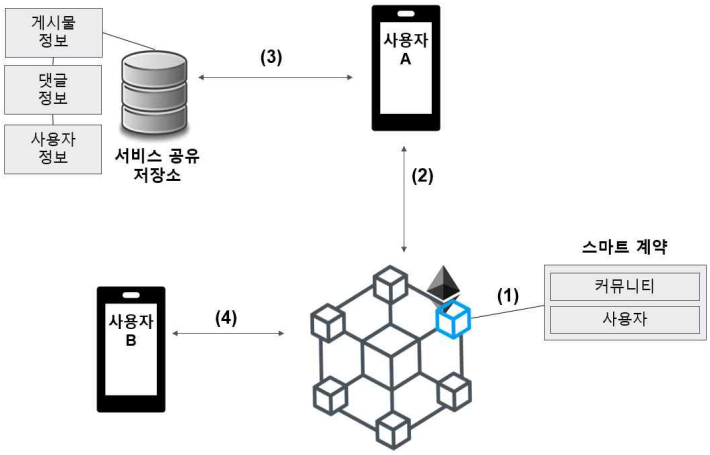
2.3 스마트 계약

스마트 계약[8]은 Ethereum 블록체인에 존재하는 코드와 데이터의 모음이다. 이 스마트 계약은 미리 정해진 조건이 충족될 때 실행되는 코드이다. 이러한 코드는 블록체인에 저장되기 때문에 중개자의 개입 없이 계약 실행이 자동화된다.

계약은 Solidity[8]와 같은 고급언어로 작성된 후 EVM 바이트 코드로 컴파일되어 블록체인에 배포된다. 개발자는 스마트 계약을 활용하여 Dapp[8]을 개발한다. Dapp은 중개자 없이 최종 사용자와 제공자 간의 직접적 상호작용을 가능하게 하는 애플리케이션이다.

3. 제안 시스템

3.1 시스템 아키텍처



[그림1] 커뮤니티 서비스 아키텍처

본 논문에서 제안하는 서비스의 전체적 구조는 [그림1]과 같다. 전체 구조는 클라이언트와 블록체인 네트워크, 서비스 공유 스토리지로 구성된다. 서비스는 사용자가 목적에 부합하는 커뮤니티를 생성하고 참여할 수 있다. [그림1] 은 사용자 A가 커뮤니티를 생성하여 사용자 B가 커뮤니티에 참여하는 과정을 아키텍처를 통해 차례대로 나타낸다. 과정과 서비스 설계에 대한 구체적 내용은 다음과 같다.

(1) 블록체인에 커뮤니티 생성 및 가입과 사용자 등록 및 인증을 수행하는 스마트 계약을 컴파일하여 배포한다. 이때 스마트 계약을 통해 커뮤니티 목록과 사용자 목록이 블록에 저장된다.

(2) 사용자 A는 배포된 스마트 계약 코드를 실행하여 커뮤니티를 생성한다. 하나의 사용자가 여러 개의 커뮤니티를 생성하는 것 또한 가능하다. 생성된 커뮤니티의 ID는 블록체인에 저장되며 커뮤니티를 생성 시 커뮤니티 전용 게시판이 생성된다.

(3) 커뮤니티 생성 시 추가적인 커뮤니티의 정보는 서비스 공유 스토리지에 저장된다. 여기서 서비스 공유 저장소는 오로지 해당 커뮤니티에 참여한 사용자만이 접근 가능한 저장소로 정의한다. 게시판을 구성하는 게시물과 댓글, 사용자의 개인 정보는 모두 블록체인이 아닌 서비스 공유 저장소에 저장된다.

(4) 사용자 B는 스마트 계약 코드를 실행하여 커뮤니티에 가입하여 사용자 A가 생성한 커뮤니티를 이용한다.

3.2 데이터 저장 구조



[그림2] 서비스의 데이터 저장 구조

[그림2]는 서비스 관련 데이터가 어느 저장소에 저장되는지를 나타낸 것이다. 데이터 저장소는 크게 블록체인 저장소와 과 서비스 공유 저장소로 분류된다. 블록체인 저장소엔 그룹 ID의 목록과 사용자 ID의 목록, 그리고 사용자 ID별 가입된 그룹 목록 데이터에 접근할 수 있는 사용자 그룹 목록 ID가 저장된다. 블록체인에 그룹과 사용자, 가입의 정보를 저장함으로써 커뮤니티 서비스를 구성하는 데이터의 무결성이 보장된다.

[그림2]의 서비스 공유 저장소는 같은 커뮤니티를 이용하는 사용자에게 공유되는 저장소로써 사용자 ID에 따른 개인 정보, 그룹 ID에 따른 그룹 정보, 커뮤니티별 게시판을 구성하는 게시물과 댓글의 정보가 저장된다. 블록체인에 저장되는 데이터는 네트워크에 참여한 모든 노드가 열람할 수 있으므로 데이터의 신뢰성을 보장할 수 있지만, 블록체인의 경우 입출력 처리가 비교적 느리기에 세부 정보는 서비스 공유 저장소에 저장한다.

3.3 주요 기능 동작

[표1] 커뮤니티 주요 기능 테이블

	기능	저장소	데이터	계약 기능
로그인	Login(private Key): return bool	스마트 계약	–	checkRegistered User (userAccount) : return bool
회원 가입	signUpNew User(): return privateKey	스마트 계약	userList[]: umap	addUser (userAccount)
	signUpOwns EOA(privateKey): return bool	스마트 계약	userList[]: umap	checkRegistered User (userAccount) :return bool addUser (userAccount)
그룹	addGroup (GroupName)	스마트 계약	GroupID	addGroup (GroupName)
		서비스 공유 저장소	GroupID :GroupInfo	

본 논문이 제안한 서비스의 주요 기능은 [표1]과 같다. [표1]에 표시된 주요 기능은 Ethereum 개인 소유 계정을 활용한 사용자 인증 로그인과 회원가입, 그룹으로 나뉜다. 다음은 각 함수에 대한 동작 과정을 서술한다.

① Login(privateKey) : 사용자는 로그인 시 서비스에 등록된 계정의 개인 키를 입력하여 로그인을 수행한다. web3[9]의 API를 활용하여 사용자의 개인 키로부터 계정을 도출한다. 이때 도출된 계정이 블록체인에 기록된 사용자 목록에 존재하는지 스마트 계약의 함수를 통해 검사하여 그 결과를 반환한다.

② signUpNewUser(): Ethereum 개인 소유 계정(EOA)이 없는 사용자가 가입 요청 시 Ethereum 네트워크의 EOA를 생성한다. 서비스 사용자 인증의 수단이 될 개인 키를 가입 요청을 한 사용자 클라이언트에 출력하고 사용자의 계정의 주소를 블록체인에 기록한다.

③ signUpOwnsEOA(privateKey): Ethereum 개인 소유 계정이 이미 존재하나 서비스에 등록되지 않은 사용자의 회원가입을 수행한다. 사용자가 보유한 EOA의 개인 키를 입력하면, 서비스 사용자 목록에 존재하는지 검사한다. 이후 사용자 목록에 EOA 소유자가 존재하지 않는다면 가입을 진행하여 EOA 주소를 사용자 목록에 추가한다.

④ addGroup(GroupName): 사용자가 커뮤니티의 이름을 입력하여 생성 요청을 하면 커뮤니티 생성을 수행한다. 생성된 커뮤니티 ID는 중복되지 않는 데이터로 블록체인에 저장한다. 이와 동시에 서비스 공유 저장소에는 생성일, 소개말과 같은 커뮤니티의 추가적인 정보를 커뮤니티 ID와 대응하여 저장한다.

Ethereum의 개인 소유 계정은 비대칭 키 알고리즘을 채택한다. 이때 비대칭 키[10]는 공개키와 개인 키를 가진다. 공개키는 타인에게 공개되는 정보이며 개인 키는 공개키로 암호화된 데이터를 복구하기 위해 필요한 정보로 오로지 자신만 소유하고 있어야 하는 정보이다. 본 논문이 제안하는 서비스의 로그인 방식은 이러한 특성을 가진 EOA를 활용하여 계정을 생성하고 블록체인에는 개인 키를 제외한 생성된 공개키의 일부만을 저장함으로써 해킹 위험 없이 사용자 인증이 가능하다. 개인 키의 정보는 사용자 개인을 제외한 어느 곳에도 저장되지 않기 때문에 이러한 로그인과 회원가입 절차는 개인정보 유출로부터 안전을 보장한다.

4. 실험

본 장에서는 서비스 주요 기능의 동작 시간의 평균을 측정한다. 데이터가 각각의 저장소에 저장되는 데에 소요되는 시간을 측정하였다.

[표2] 실험 환경

실험 환경		iPhone 8 Plus
네트워크		IEEE 802.11N
운영체제		iOS 15.0
스펙	CPU	2x Monsoon, 4x Mistral
	RAM	2GB

실험은 [표2]의 환경에서 진행하였다. 실험 기기에서 정보 저장 함수를 호출하면 구축한 Ethereum 프라이빗 네트워크를 통해 블록체인에 정보를 저장한다. 또한 블록체인에 추가된 정보와 부가적인 정보는 서비스 공유 스토리지에 저장될 수 있도록 하며, Firebase[11]가 이 저장소의 역할을 수행토록 하였다.

[표3] 그룹 저장 소요 시간

저장소 / 함수	Ethereum	Firebase
addGroup(msec)	897.17457	36.16578

[표3]은 그룹 저장 기능 수행 시 각 저장소에 정보가 저장되는 시간의 평균을 측정하여 나타낸 것이다. 사용자가 그룹 추가를 요청하면 사용자가 입력한 그룹의 정보를 블록체인 저장소와 서비스 공유 저장소에 각각 저장한다. 블록체인에 저장되는 정보는 그룹 ID이며, 서비스 공유 저장소에 저장되는 정보는 그룹 ID를 포함한 개설날짜, 개설자, 그룹명이다. 이때 정보가 블록체인 저장소인 Ethereum에 저장되는 평균 시간은 897.17457(msec)로 측정되었고, 서비스 공유 저장소의 역할을 하는 Firebase에 저장되는 평균 시간은 36.16578(msec)로 측정되었다. 결과적으로 Ethereum은 약 24배 정도 느린 저장 속도를 보였다.

이러한 실험 결과를 비추어 보았을 때, 이더리움을 활용해 커뮤니티의 모든 데이터를 블록체인에 저장하여 서비스한다면 외부 스토리지만을 사용하는 서비스보다 성능이 매우 떨어진다. 하지만 집단끼리 공유되는 일부 데이터를 외부 스토리지와 연계하여 저장한다면 기존 소요 시간을 단축하여 성능 차이를 극복한다.

5. 결론

본 논문은 중앙 서버 형태의 커뮤니티 문제점과 피해 사례를 지적하고, 기존 중앙 집중식 구조에서 벗어나 블록체인을 활용하여 데이터의 무결성을 보장하는 P2P 커뮤니티 서비스를 제안했다. 이때 블록체인에 데이터를 기록하는 시간이 외부 스토리지에 데이터를 기록하는 시간보다 느린 성능적 문제를 블록체인과 외부 스토리지 연계를 통해 해결하여 높은 성능의 커뮤니티 서비스를 구현할 수 있다. 제안된 서비스는 사용자의 패스워드와 기타 정보를 서비스에 저장하지 않음으로써 개인 정보 유출을 방지하고, P2P 구조로 서비스를 설계하여 중앙 서버에 따른 관리 비용 절감과 더불어 DDoS 공격에 대한 해결책을 제시했다.

ACKNOWLEDGMENT

이 논문은 2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2021-0-00484-002, 노드 간 메시지 전달과 합의를 위한 최적 경로 네트워크 프로토콜 기술개발)

참 고 문 헌

[1] DP2021-no. 2 (2021), Retrieved Mar., 28, 2022 from https://www.20slab.org/Archives/37850.

[2] Dcinside (1999), Retrieved Mar., 28, 2022 from https://www.dcinside.com/.

[3] Net Korea (2019), Retrieved Mar., 28, 2022 from https://zdnet.co.kr/view/?no=20190110110524.

[4] PPOMPPU (2005), Retrieved Mar., 28, 2022 from https://www.ppomppu.co.kr/.

[5] Ethereum Community, Etherum Homestead Docs. (2016)

Retrieved Mar., 25, 2022 from https://www.ethdocs.org/en/latest/.

[6] Don Tapscott and Alex Tapscott. , *Blockchain revolution : how the technology behind bitcoin is changing money, business, and the world,* Portfolio, 2016.

[7] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." Decentralized Business Review, 2008.

[8] Chris Dannen, *Introducing Ethereum and Solidity*, Apress, 2014.

[9] Petr Korolev, web3swift Docs.(2021), Retrieved Mar., 25, 2022 from https://github.com/skywinder/web3swift/blob/master/Documentation/.

[10] C. I. Woo, B. S. Kim, Y. S. Song, J. S. Yoo, I. C. Shin, "A Design of Public Key Encryption Algorithm using RSA", J*ournal of Proceeding of the Design Confernece of The Institute of Electronics and Information Engineers(IEIE)*, vol. 20, no. 1, pp 10-14, Jan. 1998.

[11] Firebase Docs. (2022), Retrieved April, 29, 2022 from https://firebase.google.com/docs/.

가상자산 시장의 AMM (Automated Market Maker) 서비스 요구사항 및 동향 분석

이채현, 우종수*, 홍원기
포항공과대학교 컴퓨터공학과, *포항공과대학교 정보통신대학원

{chlee0211, woojs, jwkhong}@postech.ac.kr

Analysis of AMM (Automated Market Maker) Service Requirements and Trends in Crypto Market

Chaehyeon Lee, Jongsoo Woo*, James Won-Ki Hong
Department of Computer Science and Engineering, POSTECH
*Graduate School of Information Technology, POSTECH

요 약

가상자산을 거래하기 위해 중앙화 거래소가 등장한 이래, 중앙화 거래소의 신뢰 문제를 개선하기 위해 제 3 자의 필요성을 제거한 탈중앙화 거래소가 등장했다. 탈중앙화 거래소는 구현 방식에 따라 호가창 기반의 거래소, AMM 기반의 거래소로 구분할 수 있는데 상위 TVL 을 차지하는 탈중앙화 거래소의 경우 대부분 AMM 기반의 서비스를 제공하고 있다. AMM 서비스는 호가창 없이 유동성 풀을 기반으로 토큰 교환을 가능케 하는 서비스로, 모든 로직이 스마트 컨트랙트 상에 구현되어 있다. 누구든 유동성 공급자가 되어 유동성을 공급할 수 있고, 유동성 풀을 기반으로 투자자는 원하는 토큰을 거래할 수 있다. P2C (Peer to Contract) 매커니즘을 따르기 때문에 토큰은 스마트 컨트랙트 상에 예치되며 유동성 풀에 대한 정보 및 토큰 교환 역시 스마트 컨트랙트를 통해 이루어진다. AMM 서비스를 위한 스마트 컨트랙트를 개발하기 위해서는 AMM 의 요구사항에 대해 분석해야 한다. 본 논문에서는 AMM 이 무엇인지에 대해 설명하고, AMM 을 구성하고 있는 요구사항들에 대해 분석한다. 유동성 풀의 형태와 유동성 예치 형태, AMM 개발을 위해 사용된 기반 블록체인 플랫폼, 가격 알고리즘 등에 따라 다양한 유형의 AMM 이 서비스되고 있다. AMM 서비스를 이용해 거래를 하는 경우, 투자자 및 유동성 공급자가 겪게 되는 리스크에 대해 설명하고, 효과적인 AMM 을 개발하기 위해 고려해야 할 사항들에 대해 제시한다. 또한, 일부 잘 알려진 AMM 기반 거래소에 대해 소개하면서 AMM 서비스의 동향에 대해 분석한다.

Ⅰ. 서론

현 가상자산 시장에는 가상자산 거래를 위한 두 가지 유형의 거래소가 존재한다. 중앙화 거래소[1]는 거래와 관련한 모든 정보를 서비스 제공자가 보관하고, 모든 거래가 중앙 시스템 상에서 일어나기 때문에 여러 취약점을 가진다. 이용자의 개인 정보 및 거래 관련 정보를 보유하고 있는 중앙 서버에 대한 해킹 위험성이 크고, 시스템을 유지, 보수하기 위한 인적, 물적 비용을 동반한다. 또한 상장 비리, 시세 조작, 가격 담합, 장부 거래 등과 같은 부당 행위에 노출될 가능성이 있다. 이러한 중앙화 거래소의 신뢰 문제에 따라 중앙 기관을 제거한 탈중앙화 형태의 거래소가 등장하게 되었다.

탈중앙화 거래소[2-4]는 중앙화 거래소와 구조적, 기술적인 차이점이 존재하며 여러 장단점을 가진다. 탈중앙화 거래소는 블록체인을 기반으로 개발되어 스마트 컨트랙트(자동화된 프로그램 코드)에 명시된 룰에 따라 자동적으로 거래가 이루어지기 때문에 중앙 기관/관리자의 개입없이 가상자산 거래가 가능하다. 모든 거래 내역이 블록체인 상에 저장되기 때문에 해킹과 위변조의 위험으로부터 안전하다. 탈중앙화 거래소는 구현 방식에 따라 호가창(orderbook)[5] 기반의 거래소, AMM (Automated Market Maker) [6-7]기반 거래소 등으로 구분할 수 있다.

중앙화 거래소를 비롯해 호가창(order book) 기반의 탈중앙화 거래소[8-9]에서는 호가창을 기반으로 가상자산의 가격이 결정된다. 호가창은 거래소에서 취급하는 가상자산의 입찰 가격을 표시하는 일종의 주문 기록 장부로, 투자자가 매수 및 매도 주문을 입력하면 호가창에 해당 주문이 실시간으로 표시된다. 호가창은 구매자와 판매자를 연결해주는 역할을 수행하여 주문 (매수/매도) 가격과 같을 경우 거래를 실행한다. 초기의 탈중앙화 거래소는 중앙화 거래소에서 채택하고 있는 호가창 방식으로 설계되었으나, 이 방식은 유동성이 충분하지 않은 경우 슬리피지(Slippage)[10-11]가 발생할 수 있고 거래 체결이 지연되는 문제가 있다. 슬리피지는 매매주문시 발생할 수 있는 체결 오차로, 구매자/판매자가 원하는 매수/매도 희망 가격과 실거래 가격이 차이가 나 원하는 가격에 가상자산을 거래할 수 없는 것을 의미한다. 이처럼 유동성이 확보되지 않은 자산에 대해 원하는 가격에 거래를 하기 어렵다는 점 등 호가창 방식의 거래소가 가지는 문제점을 개선하기 위해 AMM (Automated Market Maker) 방식의 탈중앙화 거래소가 등장하게 되었다[12-21].

AMM 방식의 거래소는 호가창이 없고, 유동성 풀에 예치된 자산을 스왑(교환)하는 방식으로 거래가 이루어진다. 다양한 유형의 탈중앙화 서비스가 여러 블록체인을 기반으로 개발되어 운영되고 있으며, 탈중앙화 거래소를 통해 거래금액이 꾸준히 증가하고 있다[22-23]. 현존하

는 탈중앙화 거래소 중 상위 TVL (Total Value Locked)의 거래소는 대부분 AMM 기반의 거래소로, 탈중앙화 거래소 별 AMM 의 구현 방식에 따라 서로 다른 특성을 가진다. 본 연구에서는 AMM 기반의 거래소에 초점을 두어 AMM 의 특성을 분석한다.

본 논문에서는 가상자산 시장에 적용할 수 있는 효과적인 AMM 서비스를 개발하기에 앞서, AMM 서비스 개발을 위한 요구사항과 서비스 동향에 대해 분석한다. 가상자산 거래를 위한 AMM 서비스가 무엇인지, AMM 을 구성하기 위한 요구사항이 무엇인지에 대해 분석하고, 가상자산 시장에서 활발하게 운영중인 주요 탈중앙화 거래소를 예시로 들어 AMM 동향에 대해 설명하여 개선된 AMM 을 고안하기 위한 방향성을 제시하고자 한다.

Ⅱ. AMM (Automated Market Maker)

호가창 기반의 거래소는 마켓 메이커가 매도/매수 주문을 냄으로써 자산의 가격을 결정하고, 유동성을 공급하게 된다. 즉, 호가창에 등록되는 매수/매도 주문을 통해 원활한 매매를 가능케하는 방식이다. 반면, Automated Market Maker 는 호가창이 아닌 유동성 풀을 기반으로 운영된다. 유동성 공급자가 유동성 풀에 가상자산을 예치하면, 그 유동성 풀을 이용해 누구든 자신이 가진 가상자산을 원하는 다른 가상자산으로 교환할 수 있다. 누구든 유동성 공급자가 되어 유동성을 제공할 수 있으며, 유동성 공급자가 마켓 메이커의 역할을 수행한다. 유동성 공급자는 유동성을 공급하는 대가로 거래 수수료 및 LP 토큰을 보상으로 얻을 수 있다[24].

유동성 풀에 예치된 가상자산의 호가는 AMM 이 채택하는 가격 알고리즘을 기반으로 결정된다. 가격 알고리즘은 사전에 정의되는 일종의 수학 공식으로, AMM 마다 목적에 맞는 다른 가격 알고리즘을 적용할 수 있다.

AMM 서비스는 P2C (Peer to Contract) Scheme 에 따르고 있어, 유동성을 예치하거나 가격 알고리즘에 따라 자산을 교환하는 알고리즘이 스마트 컨트랙트 상에 작성되어 자동으로 수행된다. 모든 과정에서 제 3 자의 중앙 개입자가 존재하지 않기 때문에 누구든 자율적으로 유동성을 제공할 수 있고, 유동성 풀과 풀에 예치된 자산은 모두 스마트 컨트랙트에 보관된다. 또한 컨트랙트 상에 정의된 가격 알고리즘에 따라 자산을 교환하므로 거래 시점, 거래 규모, 유동성에 상관없이 즉각적인 거래 체결이 가능하다.

Ⅲ. AMM 서비스 요구사항

1. 유동성 풀과 유동성 예치 형태

유동성 풀은 스마트 컨트랙트 상에 존재하는 가상자산풀을 의미한다. 유동성 공급자는 누구든 자신이 보유한 토큰을 유동성 풀에 예치할 수 있다. 유동성 풀에 예치하는 형태는 구현에 따라 다르지만, 일반적으로는 두 개의 토큰을 Pair 형태로 묶어 유동성을 공급하게 된다. 스마트 컨트랙트 내에는 공급된 Pair 별로 별도의 유동성 풀이 유지된다. 구현에 따라 유동성 풀을 구성하는 토큰이 Pair 형태가 아닌 하나의 토큰 또는 세 개 이상의 토큰이 될 수도 있다.

유동성 공급자에 의해 유동성 풀에 토큰이 예치되면, 투자자는 자신이 교환하고자 하는 토큰 유형에 맞는 유동성 풀으로부터 토큰을 교환한다. 토큰 교환은 유동성 풀에 예치된 두 토큰 간의 교환 비율에 따라 이루어지며 토큰 교환이 이루어질 수록 교환 비율이 변동된다. 만약 유동성 풀에 예치된 토큰의 수량이 적다면 교환 비율이 크게 변동되기 때문에 실제 시장 가격과의 차이가 많이 나는 슬리피지 문제가 발생할 수 있다. 슬리피지를 최소화하기 위해서는 유동성 풀에 많은 유동성이 공급되어야 하는데 이를 위해 유동성 공급자에게 보상을 제공한다.

유동성 공급자는 유동성을 공급한 행위에 대해 그 풀에서 발생하는 토큰 교환 수수료, 유동성 풀 토큰 등을 보상으로 얻는다. 이때 유동성 풀에 예치한 토큰의 양에 비례하여 수수료를 배분 받는다.

2. 가격 알고리즘

유동성 풀을 기반으로 토큰 거래가 이루어질 때는 가격 알고리즘에 기초해 토큰의 가격이 결정된다. 일반적으로는 Ⅲ-1.에서 설명한 것처럼 유동성 풀 내에 존재하는 두 토큰의 교환 비율에 따라 가격이 결정되는데, 이때 적용되는 가격 알고리즘은 CFMM (Constant Function Market Maker) [25] 공식을 따른다. CFMM 은 변하지 않는 고정된 상수 값을 기반으로 토큰의 수량을 변경시키는 것을 의미하며 토큰 교환 방식에 따라 CPMM (Constant Product Market Makers), CSMM (Constant Sum Market Makers), CMMM (Constant Mean Market Makers) 등이 있다[25].

CPMM 는 x*y = k 의 공식에 따라, 두 토큰 수량의 곱이 일정한 상수 k 를 유지하는 방향으로 토큰의 스왑 양이 결정되는 것을 의미한다. 이 알고리즘의 경우 함수의 공식에 따라 토큰 가격과 수량이 반비례하는 그래프를 띄며 무한히 발산하는 성격을 띠기 때문에 이론상으로 무한의 유동성을 제공한다. 즉, 유동성 풀에 토큰이 예치되어 있기만 하다면 원하는 가격이 아닐지라도 (실제 시장가격과 차이가 나는 슬리피지가 큰 상황) 항상 토큰을 교환할 수 있다. Uniswap 을 비롯한 대부분의 AMM 서비스는 CPMM 유형의 가격 알고리즘을 채택하고 있으며 목적에 따라 다양한 variation 이 존재한다.

CSMM 은 x+ y = k 의 공식에 따라, 두 토큰 수량의 합이 일정한 상수 k 를 유지하는 방향으로 토큰의 스왑 양이 결정되는 것을 의미한다. 공식에 따라 CSMM 은 슬리피지가 발생하지는 않지만, 두 Pair 의 토큰 중 하나의 토큰 수량이 0 이 될 수 있기 때문에 무한 유동성이 제공되지는 않는다.

CMMM 은 토큰의 산술적 평균값이 일정한 상수 k 를 유지하는 것으로 두 개 이상의 토큰을 예치할 수 있고, 토큰 별로 서로 다른 가중치를 부여하는 것이 가능하다. (x*y*z)^(1/3) = k 의 공식을 따른다.

여러 AMM 서비스는 유동성 공급자의 리스크를 줄이고, 투자자들이 겪을 수 있는 슬리피지 문제를 최소화하기 위해 CFMM 에 파라미터를 추가하거나 하이브리드 형태의 CFMM 을 개발하고 있다. CPMM 과 CSMM 을 결합한 형태의 가격 알고리즘을 채택하기도 하고, 오라클 서비스를 이용해 토큰의 가격을 결정하기도 한다.

3. 슬리피지 및 비영구적 손실에 대한 대안

AMM 을 기반으로 토큰을 거래하는 경우, 투자자와 유동성 공급자는 슬리피지 및 비영구적 손실에 대한 리스크를 입을 수 있다.

슬리피지는 거래 희망 가격과 실제 체결 가격 사이의 차이를 의미하는 것으로 투자자가 겪을 수 있는 리스크에 해당한다. 기존의 중앙화 거래소뿐만 아니라 AMM 기반의 거래소에서도 유동성이 충분하지 않다면 슬리피지가 발생할 수 있다. AMM 기반의 거래소에서는 가격 알고리즘의 교환 비에 따라 토큰의 가격이 결정되기 때문에 유동성 풀에 유동성이 충분하지 않다면 원하는 가격보다 더 높거나, 낮은 가격에 거래가 체결될 수 있다.

비영구적 손실은 유동성 공급자가 겪을 수 있는 리

스크로, 자신이 보유한 토큰을 유동성 풀에 예치함으로써 얻을 수 있는 이익이, 토큰의 가격이 상승함으로써 얻을 수 있는 이익보다 작을 때 발생한다. 쉽게 말해, 토큰을 풀에 예치하는 대신, 단순히 지갑에 보유하고 있는 것이 토큰 보유자에게 더 높은 수익을 가져다 줄 수 있다. 유동성 풀에 예치된 토큰은 가격 알고리즘에 따라 교환비가 조정될 뿐 거래 비율을 자동으로 조정하지 않기 때문에 AMM 내에 예치된 토큰이 시장 가격을 벗어나는 경우 비영구적 손실이 발생한다.

효율적인 AMM 서비스를 개발하기 위해서는 슬리피지와 비영구적 손실을 최소화할 수 있는 방안에 대해 고려해야 한다. 일부 AMM 서비스 프로바이더는 오라클 서비스를 이용해 예치된 가격이 시장가격의 예상 범위를 벗어나더라도 일정 환율을 유지하게 하거나, 가격 알고리즘을 개선하는 방식으로 리스크를 줄이기 위해 노력하고 있다.

Ⅳ. AMM 서비스 동향

1. 탈중앙화 거래소의 AMM

현 가상자산 시장에는 많은 수의 탈중앙화 거래소가 존재하며 현존하는 탈중앙화 거래소의 AMM 서비스는 자산의 예치 형태, 예치되는 자산의 유형, 기반 블록체인 플랫폼, 가격 알고리즘 등에 따라 다양한 형태로 구성될 수 있다.

탈중앙화 거래소 중 가장 잘 알려진 Uniswap [12]은 이더리움을 기반으로 개발되었다. 기존의 Uniswap v2는 유동성 풀에 두 토큰을 Pair 형태로 예치하고, 두 토큰의 양이 일정한 상수를 유지하도록 하여 가상자산을 교환할 수 있다. 지난 2021 년 5 월에는 유동성 공급 방식을 개선한 Uniswap v3 가 출시되었다. Uniswap v3 에서는 토큰을 Pair 형태로 등록하지 않아도 하나의 토큰만으로 유동성을 공급할 수 있고, 유동성을 공급할 때 원하는 가격 범위 내에서 토큰 거래가 가능하도록 하는 매커니즘을 추가하였다. 이와 같은 개선 사항을 통해 유동성 공급자는 v2 보다 최대 4000 배 가량 자본 효율적으로 유동성을 공급할 수 있고, 비영구적 손실을 줄일 수 있다.

Curve Finance [13]는 현재 가장 큰 규모의 유동성을 보유한 탈중앙화 거래소로(2022 년 4 월 8 일 기준), 이더리움 네트워크 상에서 스테이블 코인을 교환할 수 있다. USDT, USDC, DAI, BUSD 등 다양한 스테이블 코인을 저렴한 수수료로 토큰 교환이 가능하며 슬리피지가 낮고 최소화된 비영구적 손실을 보장한다는 장점이 있다. Curve Finance 는 두 개 이상의 자산을 하나의 유동성 풀에 공급할 수 있다.

PancakeSwap [14]은 바이낸스 스마트 체인을 기반으로 개발된 서비스로 바이낸스 스마트 체인을 활용하여 상대적으로 저렴한 수수료로 토큰을 교환할 수 있다. AMM 을 기반으로 BEP-20 토큰을 교환할 수 있고 Pair 형태로 유동성을 공급한다.

KLAYswap [15-16]은 Klaytn [26-27] 메인넷에서 운영되는 디파이 서비스로 Klaytn 기반의 서비스 중 가장 유동성이 크고 거래가 활발히 일어나고 있다. 단일 예치, 일반 페어 예치, 플러스 예치 등을 통해 하나의 토큰 또는 두 개의 토큰을 Pair 형태로 예치하고, 예치에 따른 보상을 획득할 수 있다.

본 논문에서 소개된 여러 AMM 서비스 이외에도 Balancer [17], Bancor [18], SushiSwap [19], Kyber network [20], QuickSwap [21] 등의 다양한 탈중앙화 거래소가 AMM 서비스를 기반으로 운영되고 있고, 구현에 따라 서로 다른 기반 블록체인 플랫폼, 유동성 풀 예치 형태, 가격 알고리즘, 교환 수수료 등을 가진다.

2. 중앙화 거래소의 AMM

가상자산 시장에서의 AMM 은 일반적으로 탈중앙화 거래소를 위한 프로토콜로써 적용되어 왔다. 하지만 중앙화 거래소에서도 AMM 을 도입하여 다양한 사용자 경험을 제공할 수 있다. 서비스 이용자는 유동성을 제공함으로써 추가 수익을 창출할 수 있으며, 유동성을 기반으로 빠르게 자산을 스왑할 수 있다.

2013 년 설립된 글로벌 가상자산 거래소 gate.io 는 Liquidity Mining 이라는 서비스를 통해 일종의 AMM 서비스를 제공한다 [28-30]. 두 개의 자산을 Pair 형태로 묶어 유동성을 제공하고, 이에 대한 대가로 수수료를 얻을 수 있다. 게이트아이오의 서비스는 CPMM, 즉, 두 자산의 곱이 일정한 상수를 유지하도록 하는 가격 알고리즘을 이용해 자산의 가격이 결정된다. 중앙화 거래소에서 AMM 을 도입하기 위해서는 어떤 방식으로 서비스를 구현할지, 많은 유동성을 유지하기 위해 유동성 공급자에게 어떻게 보상을 제공할지 등에 대해 고려해야 한다.

Ⅴ. 결론 및 향후 연구

본 논문에서는 탈중앙화 거래소의 등장과 종류에 대해 간략히 설명하고, 탈중앙화 거래소 중 AMM 기반의 거래소에 초점을 맞추어 AMM 의 특징, 요구사항과 동향에 대해 분석하였다. 다양한 AMM 기반의 탈중앙화 거래소 및 디파이 서비스가 등장하고 있고 많은 양의 토큰들이 AMM 기반의 서비스를 통해 거래되고 있음을 확인하였다.

AMM 서비스는 유동성 풀과 가격 알고리즘에 따라 거래가 이루어지며, 특히, 유동성을 예치하고 자산을 거래하기 위한 로직이 모두 스마트 컨트랙트 상에서 구현되어 제 3 자의 기관 개입 없이 자동으로 거래가 이루어진다.

AMM 서비스를 구성하기 위해선 유동성 풀, 가격 알고리즘이 필수적으로 고려되어야 하며 유동성 풀을 어떻게 구성할지, 유동성의 예치 형태, 기반 블록체인 플랫폼, 취급 가장자산의 종류 등에 따라 다양한 유형의 AMM 서비스를 구현할 수 있다. 또한 AMM 기반의 거래소는 호가창 없이 가격 알고리즘을 기반으로 가격을 결정하는데 어떠한 가격 알고리즘을 사용하느냐에 따라, 토큰 가격과 투자자, 유동성 공급자의 수익에 영향을 미친다.

효과적인 AMM 서비스를 개발하기 위해서는 운영하고자 하는 서비스의 목적에 맞는 유동성 풀의 예치 형태와 가격 알고리즘를 설계가 선행되어야 하며 슬리피지와 비영구적 손실을 줄이기 위한 방안이 고려되어야 한다.

향후 연구에서는 본 연구를 바탕으로 효과적인 AMM 서비스를 디자인하고, 개발하고자 한다. 또한, 기존의 AMM 과 비교해 유동성 풀의 효율성, 슬리피지, 비영구적 손실 측면에서 어느 정도의 개선 효과가 있는지 실험해보고자 한다.

ACKNOWLEDGMENT

본 연구는 ㈜코인원과 과학기술정보통신부 및 정보통신기획평가원의 대학 ICT 연구센터육성지원사업의 연구결과로 수행되었음 (IITP-2022-2017-0-01633)

참 고 문 헌

[1] Liu, Y., Vogel, S., & Zhang, Y. (2018, June). Electronic trading in OTC markets vs. centralized exchange. In Paris December 2018 Finance Meeting EUROFIDAI-AFFI.

[2] Caliskan, K. (2020). Platform works as stack economization: cryptocurrency markets and exchanges in perspective. Sociologica, 14(3), 115-142.

[3] Pop, C., Pop, C., Marcel, A., Vesa, A., Petrican, T., Cioara, T., ... & Salomie, I. (2018, September). Decentralizing the stock exchange using blockchain an ethereum-based implementation of the bucharest stock exchange. In 2018 IEEE 14th International Conference on Intelligent Computer Communication and Processing (ICCP) (pp. 459-466). IEEE.

[4] Aspris, A., Foley, S., Svec, J., & Wang, L. (2021). Decentralized exchanges: The "wild west" of cryptocurrency trading. International Review of Financial Analysis, 77, 101845.

[5] Weber, P., & Rosenow*, B. (2005). Order book approach to price impact. Quantitative Finance, 5(4), 357-364.

[6] Aoyagi, Jun and Ito, Yuki, Coexisting Exchange Platforms: Limit Order Books and Automated Market Makers (March 20, 2021). Available at SSRN: https://ssrn.com/abstract=3808755 or http://dx.doi.org/10.2139/ssrn.3808755

[7] Othman, A., Pennock, D. M., Reeves, D. M., & Sandholm, T. (2013). A practical liquidity-sensitive automated market maker. ACM Transactions on Economics and Computation (TEAC), 1(3), 1-25.

[8] RAYDIUM, Available at https://dex.raydium.io/#/market/teE55QrL4a4QSfydR9dnHF97jgCfptpuigbb53Lo95g

[9] dYdX, https://trade.dydx.exchange/

[10] Brown, S. M. (2005). Slippage: The hidden cost of trading. University of South Carolina.

[11] Frino, A., & Oetomo, T. (2005). Slippage in futures markets: Evidence from the Sydney Futures Exchange. Journal of Futures Markets: Futures, Options, and Other Derivative Products, 25(12), 1129-1146.

[12] Introducing Uniswap V3, Uniwap, https://uniswap.org/blog/uniswap-v3, 2021. 05. 23

[13] Curve Finance, Curve, Available at https://curve.fi/

[14] PancakeSwap, Available at https://pancakeswap.finance/

[15] KLAYswap, Available at https://klayswaps.com/?url=https://klayswap.com/

[16] KLAYswap, Available at https://docs.klayswap.com/

[17] Balancer, Available at https://balanccer.net/?url=https%3A%2F%2Fapp.balancer.fi%2F

[18] Bancor, Available at https://app.bancor.network/pools

[19] SushiSwap, Available at https://app.sushi.com/en/swap

[20] Kyber Network, Available at https://kyber.network/

[21] QuickSwap, Available at https://quickswap.exchange/#/swap

[22] https://dune.xyz/hagaetc/dex-metrics

[23] Defi Llima, Available at https://defillama.com/

[24] Uniswap v2 Core, Available at https://uniswap.org/whitepaper.pdf

[25] Angeris, G., & Chitra, T. (2020, October). Improved price oracles: Constant function market makers. In Proceedings of the 2nd ACM Conference on Advances in Financial Technologies (pp. 80-91).

[26] Klaytn, Available at https://www.klaytn.com/

[27] Klaytn Docs, Available at https://ko.docs.klaytn.com/

[28] Liquidity Mining, Gate.io, Available at https://www.gate.io/liquidity

[29] FAQ- Liquidity Mining, Gate.io, Available at https://www.gateio.ch/help/lend/mining/21060/faq-liquidity-mining

[30] What is Liquidity Mining?, Gate.io, Available at https://www.gateio.ch/blog_detail/397/what-is-liquidity-mining

P2P 기반 블록체인 메신저 구현

양현주, 박세진
계명대학교

to123we10@gmail.com, baksejin@kmu.ac.kr

Implementation of P2P-based blockchain messenger

Hyunjoo Yang, Sejin Park
Keimyung Univ.

요 약

본 논문은 기존 중앙 서버를 활용한 모바일 메신저의 문제점을 해결하기 위해 구현한 P2P 기반 블록체인 메신저를 분석한다. 중앙 서버의 문제점으로는 서버 관리 비용, 데이터 유출 및 위변조, 해킹 등 비용 및 보안과 관련된 다양한 문제점이 존재한다. 이러한 기존 모바일 메신저의 문제점 해결을 위해 사용자의 개인 정보를 요구 및 저장하지 않고, 데이터의 무결성을 보장하는 P2P 기반 블록체인 메신저가 필요하다. 따라서 본 논문에서는 블록체인 기술과 P2P protocol 을 활용하여 기존 중앙 서버 구조의 모바일 메신저의 문제점을 해결하는 새로운 방안을 제안하고, 제안 메신저의 성능 실험을 위해 노드 발견 및 메시지 송수신 시간과 블록체인으로부터의 정보 수신 시간의 평균을 측정하였다. 해당 실험을 통해 제안 메신저의 채팅 서비스를 사용하기 위한 평균 시간이 503.5(msec), 블록체인의 정보를 사용하기 위한 정보 수신 평균 시간이 66.47(msec)임을 도출하였다.

Ⅰ. 서 론

모바일 메신저는 스마트폰과 같은 모바일 기기를 통해 실시간으로 메시지 및 사진 등 데이터를 주고받을 수 있도록 모바일 메시징 서비스를 제공하는 플랫폼이다. 대표적인 글로벌 메신저로는 최근 약 20 억명의 사용자를 보유한 WhatsApp 이 있고[1], 국내 대표 메신저로는 2021 년 기준 국내 메신저 시장 점유율 86.5%에 달하는 카카오톡이 있다 [2]. 이러한 기존 메신저들은 시간과 거리의 제약없이 1:1 을 넘어 1:N 의 대화가 가능하도록 만들었지만 서비스가 중앙 서버의 구조로 운영된다는 단점이 있다.

중앙 서버를 활용한 모바일 메신저는 사용자의 데이터를 중앙 서버에서 저장 및 관리하기 때문에 비용과 보안 측면에서 다양한 문제점들이 제기된다. 구체적인 예로는 서버 관리 및 유지 비용, 데이터 유출 및 위변조 등이 있다.

본 논문에서는 이러한 중앙 서버 구조의 모바일 메신저 문제점을 해결하기 위해 블록체인과 P2P protocol 을 활용한 P2P 기반 블록체인 메신저를 제안한다. P2P 기반의 서비스 운영으로 중앙 서버의 문제점에서 근본적인 원인인 서버를 사용하지 않으면서 탈중앙화된 구조의 블록체인을 통해 데이터를 분산 저장하여 데이터의 위변조를 방지한다.

Ⅱ. 본론

1. 관련 연구

본 장에서는 본 논문에서 제안하는 블록체인 메신저와 관련된 연구를 기술한다.

가. Ethereum

Ethereum[3]은 smart contract 라는 애플리케이션 코드를 안전하게 실행하고 검증하여 P2P 네트워크를 구축하는 분산형 블록체인 플랫폼이다. Smart contract[4]는 미리 정해놓은 조건이 충족될 때 자동으로 실행되는 프로그램이다. 즉, 중개인의 개입없이 다양한 형태의 계약의 유효성과 신뢰성을 검증하고 이를 체결할 수 있도록 지원한다.

나. P2P(Peer-to-Peer)

기존 서버-클라이언트 모델의 네트워크와 달리 서버없이 노드 간의 통신을 가능케 하는 모델이 P2P 이다.

1) libp2p Protocol

본 논문에서 제안하는 메신저는 libp2p 를 사용하여 구현했다. libp2p[5]는 IPFS 에서 구축됐지만 이에 의존하지 않고 많은 프로젝트의 전송 계층으로 사용된다.

libp2p 에서는 다른 Peer 에게 메시지를 전송하기 위해 Peer 검색 및 연결을 시도하고 이를 Peer routing 이라 한다. Libp2p 의 Peer Routing System 은 연결을 원하는 Peer 의 정보를 주변 노드들에게 반복적으로 요청하여 얻는 Kademlia [6]routing algorithm 을 사용하여 구현되었다. 본 논문에서는 Peer routing 의 자세한 설명은 생략한다.

다. 출시된 기존 블록체인 메신저

1) Secretum

Secretum[7]은 블록체인 기술을 사용한 메신저로 익명성을 보장한 분산형 애플리케이션(DApp)이다. 전화번호 또는 이메일과 같이 사용자의 개인 정보를 통한 인증과정없이 오로지 지갑 주소를 통해 채팅 서비스를 이용한다.

모든 대화는 네트워크를 통해 이동하지 않는 임의의 키로 시작되는데 이 키가 없으면 어느 누구도 해당 메시지를 읽을 수 없다. 이 때, 노드 간 주고받는 메시지는 종단 간 암호화되어 Secretum Network 의 신뢰할 수 있고 검증된 노드에 저장된다. 또한, Secretum 은 암호 화폐 및 NFT 운영을 위한 특정 모듈을 통합하여 서비스를 제공한다.

2) 제안 메신저와의 차이점

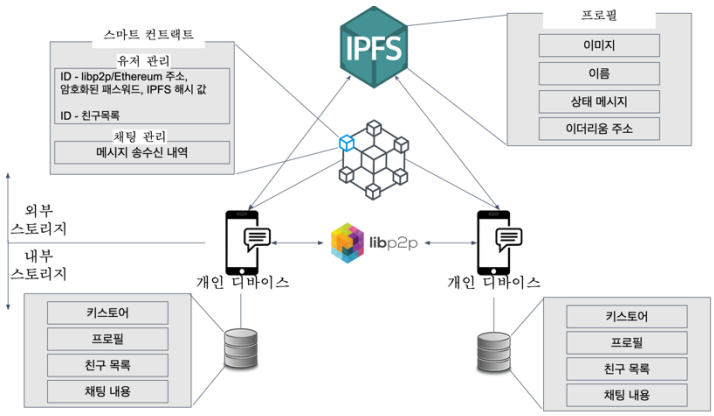
[표 1. Secretum 과 제안 메신저의 차이점]

구분	Secretum(비교 메신저)	제안 메신저
블록체인	솔라나(Solana)	이더리움(Ethereum)
채팅 데이터 저장	블록체인의 검증된 노드	개인 디바이스
채팅 데이터에 대한 가스비 소모	O	X

Secretum 과 본 논문에서 제안하는 메신저의 가장 큰 차이점은 채팅 데이터가 저장되는 위치이다. Secretum 메신저에서는 모든 대화 내용이 암호화되어 검증된 노드에 저장되고, 제안 메신저의 채팅 데이터는 각 사용자 디바이스 내부 DB 에 저장된다.

즉, 비교 메신저의 대화 내용 저장 방식은 대화 데이터의 사이즈가 클수록 많은 가스비를 소모한다. 하지만, 제안 메신저는 채팅 데이터 저장에 있어 가스비를 요구하지 않으며 채팅 데이터를 외부에 노출하지 않고 개인 디바이스에서 관리한다.

2. 제안 메신저 아키텍처



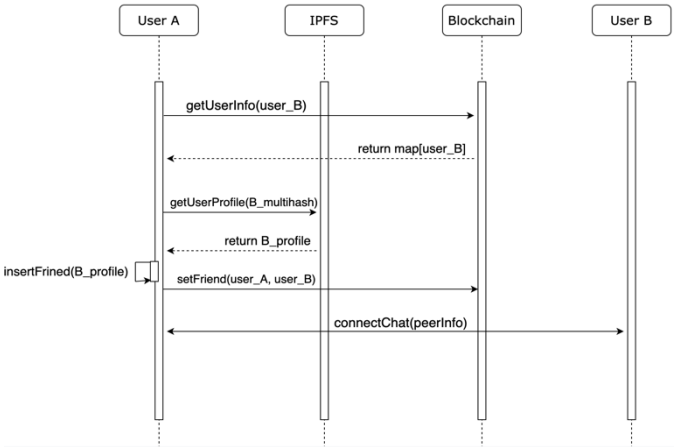
[그림 1. 제안 메신저 아키텍처]

그림 1 은 본 논문에서 제안하는 메신저의 전체 시스템 구조로 각 데이터가 저장되는 위치를 나타낸다.

디바이스 내부 DB 의 Keystore 필드에는 유저의 서비스 ID 및 암호화 된 패스워드, private key 가 저장되어 있다. 해당 Keystore 는 제안 메신저의 서비스에 로그인 할 때 사용된다. Profile 필드에는 유저의 이미지, 이름, 상태메시지가 저장되어 있으며 유저의 프로필을 나타낼 때 사용된다. 해당 Profile Data 는 IPFS 에 업로드 되며 파일의 해시 값은 User Management 컨트랙트에 저장된다. Friends L ist 필드에는 친구의 이미지, 이름, 상태메시지, libp2p/Ethereum Address 가 저장되어 있으며 libp2p Address 는 스마트 컨트랙트를 통해 주기적으로 갱신된다. Chat C ontents 필드는 RoomId, 송신자 ID, 메시지 내용, 시간이 저장되어 각 채팅방의 대화 내용을 담고 있다.

User Management 컨트랙트는 User ID 와 libp2p/Ethereum Address, Password H ash, IPFS Hash 값을 맵핑하여 저장한다. 또한, 각 유저는 친구 목록을 해당 컨트랙트를 통해서 저장 및 관리한다. Chat Management 컨트랙트는 각 유저 간 메시지를 주고받은 시간을 체크하여 주기적으로 트랜잭션을 발생시킨다.

3. 제안 메신저 동작 방식



[그림 2.제안 메신저 채팅 연결 시퀀스 다이어그램]

제안 메신저의 채팅 서비스를 시작하기 위해서는 메신저에 회원 가입 된 유저여야 한다. 사용자는 UserId, 이름, 패스워드, 상태메시지(선택사항)를 입력하여 회원 가입을 완료한다. 이 때, UserId 는 User Management 컨트랙트 통해 중복되지 않게 생성되고, Chathost.peerId 함수를 통해 중복되지 않는 libp2p Address 를 부여 받는다. 다른 유저와의 채팅을 시작하려면 해당 유저의 libp2p Address 를 알고 있어야 한다.

그림 2 는 User A 가 User B 를 친구 추가하고, 채팅을 시작하는 시퀀스 다이어그램이다. User A 는 User B 의 ID 를 통해 User Management 컨트랙트에 저장된 B 의 정보를 가져온다. 반환 받는 정보는 그림 1 에서 표현한 ID 와 맵핑된 libp2p Address 와 같은 값이다. 이 때 IPFS Hash 값을 통해 IPFS 에서 B 의 프로필을 불러와 디바이스 내부 DB Friend L ist 에 저장한다. 또한, User Management 컨트랙트를 통해 친구 목록 필드에 A 의 UserID 와 B 의 UserID 가 Mapping 되어 저장된다. 다음으로 A 가 B 와의 채팅 연결을 위해 앞에서 반환 받은 libp2p Address 를 통해 B 와의 채팅을 시작한다. A 는 User Management 컨트랙트에서 주기적으로 B 의 libp2p Address 를 확인해서 채팅을 유지할 수 있다.

4. 실험

본 장에서는 제안하는 메신저에서 노드 발견 및 메시지 수신 시간과 블록체인으로부터 필요한 정보 수신 시간의 평균을 측정하였다. 실험 환경은 다음과 같다.

[표 2. 실험 환경]

실험 환경		Galaxy S20+	Galaxy Tab S7
네트워크		IEEE 802.11N	
운영체제		Android-12	Android-11
스펙	CPU	**Exynos:** Octa-core (2x2.73 GHz Mongoose M5, 2x2.60 GHz Cortex-A76 and 4x2.0 GHz Cortex-A55) **Snapdragon:** Octa-core (1x2.84 GHz, 3x2.42 GHz and 4x1.8 GHz)	Octa-core (1x3.09 GHz, 3x2.42 GHz, 4x1.8 GHz)
	RAM	12GB RAM	6GB RAM

실험은 표 2 와 같이 동일한 네트워크에 연결된 두 개의 디바이스를 활용하여 진행하였다. 각각의 디바이스는 제안 메신저에 회원 가입 된 상태이며, Galaxy S20+ 를 노드 A, Galaxy Tab S7 을 노드 B 로 지칭한다.

1) 노드 발견 및 메시지 송수신 평균 시간

[표 3. 노드 발견 및 메시지 송수신 평균 시간]

	Node Discovery	Message Recv.	Average
시간(msec)	230.82	776.18	503.5

해당 실험은 각 노드에서 동일한 조건으로 진행되었으며, 각각의 실험 결과를 합산하여 평균을 측정하였다. 노드 A 가 채팅 시작 시 노드 B 를 발견(혹은 반대의 경우)하는 시간을 측정하여 Node Discovery 의 결과를 산출하였다. 또한, Message Recv. 의 결과는 노드 A 가 메시지를 전송하고 노드 B 가 해당 메시지를 수신(혹은 반대의 경우)하는 데까지 걸리는 시간을 측정하여 도출해낸 것이다.

표 3 은 위 실험 결과를 정리한 것으로 메시지를 송수신하는 데 걸리는 시간이 동일한 네트워크에 존재하는 노드를 발견하는데 걸리는 시간보다 평균적으로 545.36(msec) 많은 시간이 소요된다.

위 실험 결과를 통해 제안 메신저에서 채팅 서비스를 사용하는데 평균 503.5(msec)의 시간이 소요됨을 확인하였다.

2) 블록체인으로부터 필요한 정보 수신 평균 시간

[표 4. 블록체인으로부터 정보 수신 평균 시간]

	Login Info.	Friend Info.	Average
시간(msec)	64.56	68.38	66.47

해당 실험은 블록체인으로부터 받아오는 정보를 로그인을 위한 정보(암호화된 패스워드), 친구 추가를 위한 정보(친구의 Ethereum/libp2p Address, profile IPFS hash value) 두 가지로 나누어 각각의 정보 수신 시간의 평균을 측정하였다. 실험을 위한 Ethereum Private network 구축하여 User Management 컨트랙트를 배포하고 실험을 진행하였다. 사용자가 로그인을 위한 아이디와 패스워드를 입력하면, 컨트랙트는 해당 아이디와 Mapping 되어 있는 string 타입의 암호화된 패스워드를 반환한다. 또한, 추가하고 싶은 친구의 UserId 를 입력하면 컨트랙트는 해당 UserId 에 Mapping 된 string/address 타입의 유저 정보를 반환한다.

표 4 는 위 실험 결과를 정리한 것으로 로그인 정보 수신 평균 시간 보다 친구 추가를 위한 정보를 수신하는 시간이 3.82(msec) 길게 소요되지만 큰 차이를 보이지 않는다.

위 실험 결과를 통해 블록체인에서 필요한 정보를 수신하는 평균 시간은 66.47(msec)임을 확인하였다.

5. 구현된 기능 및 한계점

현재 구현된 메신저 기능으로는 Sign-Up, Login, Friend Management, Chat 으로 메신저의 기본적인 기능은 모두 구현되었다. 하지만, 해당 메신저 채팅의 경우 동일한 네트워크 안에서의 메시지 송수신은 가능하지만 서로 다른 private/local network 에서 사설 IP 를 할당받은 클라이언트 간
메시지 전달이 불가능하다.

Ⅲ. 결론

본 논문은 기존 중앙 서버 구조의 모바일 메신저의 문제점을 지적하고, 해결방안으로 P2P 기반의 블록체인 메신저를 제안한다. 현재까지 구현한 모바일 메신저는 libp2p protocol 과 Ethereum 의 Smart Contract 를 사용해 서버 관리 비용을 절약하고, 사용자의 데이터 유출 및 위변조를 방지한다. 현재, 서로 다른 private/local network 에서 사설 IP 를 할당받은 클라이언트 간 채팅이 가능하도록 하는 연구를 진행 중이다.

ACKNOWLEDGMENT

이 논문은 2022 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2021-0-00484-002, 노드 간 메시지 전달과 합의를 위한 최적 경로 네트워크 프로토콜 기술개발)

참 고 문 헌

[1] Statista Research Department, WhatsApp - Statistics & Facts (2022), Retrieved Mar.,20,2022, from https://www.statista.com/topics/2018/whatsapp/#dossierKeyfigures

[2] 최준선, “카톡 지워도 될까요…카카오 안쓰는게 가능?”(2021), Retrieved Mar.,20,2022, from http://mbiz.heraldcorp.com/view.php?ud=20210910000714&a=99

[3] AWS, what is Ethereum?, Retrieved Mar.,20,2022, from https://aws.amazon.com/ko/blockchain/what-is-ethereum/

[4] IBM, What are smart contracts on blockchain?, Retrieved Mar.,20,2022, from https://www.ibm.com/topics/smart-contracts

[5] libp2p, What is libp2p?, Retrieved Mar.,20,2022, from https://docs.libp2p.io/introduction/what-is-libp2p/

[6] WIKIPEDIA, kademlia(2022), Retrieved Mar.,20,2022 from https://en.wikipedia.org/wiki/Kademlia

[7] anshuman, Secretum Blockchain Messaging App: How to Use, Its Features(2021), Retrieved Mar.,20,2022, from https://gadgetstouse.com/blog/2021/12/27/secretum-blockchain-messaging-app-features/

다중서명과 다자산 계산을 이용한 디지털 자산 커스터디 서비스 설계

김정헌, 우종수*, 홍원기
포항공과대학교 컴퓨터공학과, *포항공과대학교 정보통신대학원

{kjheon1118, woojs, jwkhong}@postech.ac.kr

Design of Digital Asset Custody Service using Muti-Signature and Multi-Party Computation

Jeongheon Kim, Jongsoo Woo*, James Won-Ki Hong
Department of Computer Science and Engineering, POSTECH
*Graduate School of Information Technology, POSTECH

요 약

디지털 자산 시장의 폭발적인 성장에 기반하여, 국내에서 「특정금융정보의 보고 및 이용 등에 관한 법률」, 특금법이라고 불리는 법안이 2021년 3월 개정되었다. 개정된 특금법은 국제자금세탁방지기구 (FATF)에서 자금세탁과 테러자금조달 방지를 위해 권고한 내용들을 이행하기 위한 조치이다. 특금법 개정은 디지털 자산 시장이 제도권 안으로 들어오는 시작점이 되었으며, 국내 여러 은행들은 여러 블록체인 기업들과 합작 법인을 설립하여 디지털 자산 커스터디 서비스 (DACS)를 계획하거나 제공하기 시작하였다. 국민은행이 합작한 한국디지털에셋 (KODA) 뿐만 아니라, 신한은행이 합작한 한국디지털자산수탁 (KDAC) 등에서 커스터디 서비스를 제공하고 있다. 이러한 커스터디 서비스는 디지털 자산을 위탁 관리하는 서비스와 개인키를 안전하게 보관하는 서비스로 나눌 수 있다. 본 논문에서는 해당 서비스들을 모두 지원하기 위해, 다중서명과 다자간 계산을 이용한 디지털 자산 커스터디 서비스의 설계를 제안한다. 해당 설계는 4단계 레이어로 구성되어 있으며, 각 단계별 레이어에서는 KYC (Know Your Customer) 인증과 다중서명 스마트 컨트랙트, 신뢰실행환경 (Trusted Execution Environment), 그리고 다자간 계산 기반 키관리 시스템을 통해 커스터디 서비스에 보안을 제공한다. 이를 통해 해당 커스터디 서비스를 사용하는 고객들의 디지털 자산을 안전하게 보관할 수 있도록 한다.

Ⅰ. 서 론

2016년 비트코인으로부터 시작된 디지털 자산 시장의 폭발적인 성장은 현재까지 그 기조가 이어지고 있다 [1]. 특히 2020년 이후에는 시장 규모가 2조 달러를 넘기면서 높은 증가세를 시현하였다. 이러한 최근 디지털 자산 시장의 경향에 따라, 은행권에서도 신규 사업의 일환으로 디지털 자산 커스터디 서비스에 대한 관심이 증가하고 있다. 커스터디 서비스는 은행권의 전통적인 서비스로, 디지털 자산이 등장하기 전의 금융 자산을 보관하거나 위탁 관리하는 수탁업무를 뜻한다. 이처럼 디지털 자산 커스터디 서비스는 디지털 자산 시장의 빠른 성장에 대응하여, 커스터디 서비스의 영역을 디지털 자산으로 확대한 것으로, 주로 기관 투자자를 대신해 디지털 자산을 대신 구매하거나, 디지털 자산의 소유권을 증명하는 개인키 보관 등의 서비스를 제공한다.

이러한 경향에 대응하기 위해, 국내에서는 2021년 3월 「특정금융정보의 보고 및 이용 등에 관한 법률」 (특금법)이 개정되었다 [2]. 이처럼 디지털 자산 사업의 법적 근거가 마련됨에 따라, 라이선스를 취득하면 국내에서 가상자산 사업자로서 디지털 자산 커스터디 서비스를 제공할 수 있게 되었다. 국내 은행들 또한 해당 사업에 참여하고 있는데, KB 국민은행은 여러 기업들과 한국디지털에셋 (KODA)이라는 합작법인을 설립하여, 네트워크가 차단된 환경에서 고객의 디지털 자산을 안전하게 보관해주는 서비스를 제공하고 있다 [3]. 또한 신한은행도 한국디지털자산수탁 (KDAC)이라는 법인을 통해 커스터디 서비스를 제공중에 있다 [4]. 이러한 동향은 국내뿐만 아니라 해외에서도 이어지고 있다. 2020년 7월 미국에서는 국립은행 (National Saving Banks)과 연방저축조합 (Federal Saving Associations)에서 디지털 자산 커스터디 서비스를 제공할 수 있다고 발표하였다 [5]. 이후 씨티그룹, JP 모건, 모건스탠리 등 대형 은행들의 커스터디 서비스 제공 계획을 발표하면서 디지털 자산 커스터디 서비스 시장은 더욱 크게 성장할 것으로 예측된다 [6].

디지털 자산 커스터디 서비스는 두 가지 서비스로 나눌 수 있는데, 첫 번째는 기존에 실물로 존재하는 금융자산을 위탁 관리하는 전통적인 커스터디처럼, 디지털 자산을 위탁 관리해주는 서비스이고, 두 번째는 디지털 자산 (암호화폐, NFT 등)의 소유권을 증명할 수 있는 개인키를 안전하게 보관하는 서비스이다. 디지털 자산은 디지털 환경 (블록체인 등)에 존재하며, 개인키로만 해당 자산의 소유권을 증명할 수 있다. 만약

개인키가 타인에게 노출된다면 타인이 해당 디지털 자산의 소유권을 증명할 수 있게 되므로 자산을 탈취당할 위협에 직면하게 된다. 이러한 위험을 방지하기 위해, 디지털 자산 커스터디 서비스는 고객의 개인키가 노출되지 않게 안전하게 보관하는 서비스를 제공한다. 현재 국내에서 커스터디 서비스를 제공하고 있는 한국디지털에셋과 한국디지털자산수탁은 모두 개인키를 인터넷과 단절된 환경인 콜드월렛 (Cold Wallet)에 안전하게 보관할 수 있도록 다중서명 (Multi Signature) [7] 시스템을 적용하고 있다. 다중서명 방식을 통하면 N 개의 개인키 중 M 개 이상의 서명 (M-of-N)이 필요하게 되며, 하나의 개인키를 분실하거나 유출하여도 자산이 탈취되지 않는 장점이 있다.

개인키를 안전하게 관리하기 위한 기술에는 두 가지가 있는데, 첫 번째는 위에서 소개한 다중서명 방식으로, 블록체인에서 온체인 방식으로 동작한다. 두 번째는 다자간 계산 [8] 방식으로, 온체인 방식이 아닌 오프체인 방식으로 동작한다. 다중서명 방식은 여러 개의 개인키를 통해 관리되기 때문에, 디지털 자산 커스터디 서비스 중 고객의 개인키를 안전하게 보관하는 서비스에 적합하다. 이에 반해 다자간 계산 방식은 디지털 자산을 커스터디 서비스를 제공하는 사업자에 위탁할 때, 해당 사업자의 개인키를 안전하게 보관하는 역할에 적합하다.

따라서 본 논문에서는 다중서명과 다자간 계산을 모두 활용하는 디지털 자산 커스터디 서비스의 설계를 제안한다. 본 설계에서는 다중서명 방식을 통해 디지털 자산을 위탁 관리하는 커스터디 서비스를 제공하고, 다자간 계산 방식을 통해 커스터디 사업자의 개인키를 안전하게 보관하는 서비스를 제공한다. 이 때, 다중서명을 통해 여러 개의 개인키를 생성하여 일부를 가상자산 사업자 측에서 보관함으로써, 개인키를 분실하거나 유출하여도 다시 복원할 수 있게 된다. 또한 다자간 계산을 통해 하나의 개인키가 여러 개의 조각으로 분산되어, 해당 조각들을 인터넷이 단절된 콜드월렛에 보관하게 된다. 이 때, 다자간 계산을 통해 보관된 조각들을 노출시키지 않고도 트랜잭션에 서명하는 것이 가능하므로, 기존 개인키를 노출 시키지 않는다. 뿐만 아니라, 다자간 계산을 통해 개인키를 변경하지 않고도 분산된 조각들을 업데이트하는 것이 가능하여 더욱 보안성을 높일 수 있다.

Ⅱ. 배경

1. 다자간 계산 (Multi-Party Computation, MPC)

다자간 계산은 분산된 여러 노드들이, 개인이 가진 데이터 내용을 공개하지 않고도 필요한 임의의 기능을 공동으로 계산하기 위한 암호화 프로토콜이다. 이는 신뢰할 수 있는 제 3 자가 없는 상황에서 상대방과의 정보를 비교하기 위해 시작되었다. Yao의 백만장자 문제 [9]를 통해 구체화되었는데, 두 명의 백만장자가 서로의 재산에 관한 정보를 노출하지 않고 상대방과 자신의 재산을 비교하고자 하는 것에서 출발하였다. 이를 일반화하면 Alice는 입력으로 x를, Bob은 입력으로 y를 가지고 있을 때, f(x,y)를 계산하되, Alice는 y를, Bob은 x를 알 수 없어야 한다. 이러한 문제를 해결하기 위해 다자간 계산이 사용된다.

이러한 다자간 계산의 개념을 개인키 보안에 적용시킬 수 있다. 원래의 개인키를 노출시키지 않기 위해 개인키를 N개의 조각으로 나누어 분산 저장한다. 이후 블록체인 네트워크에 트랜잭션을 전송하기 위해서는 개인키로 서명된 트랜잭션이 필요하다. 해당 트랜잭션에 서명하기 위해서는 개인키가 필요하지만, 현재 우리가 가지고 있는 것은 온전한 개인키가 아닌 개인키의 조각뿐이다. 서명을 위해 개인키의 조각을 조합하여 온전한 개인키를 재생성 할 수도 있지만, 재생성 과정에서 개인키가 노출될 위협을 배제할 순 없다. 따라서 이 때 사용할 수 있는 방법이 위에서 설명했던 다자간 계산 과정이다. 간략히 서명하는 과정을 f라는 함수로 나타내면, 해당 함수는 N개의 조각들인 x_1, x_2, ... x_n 들과 서명되지 않은 트랜잭션을 입력으로 가지고, 서명된 트랜잭션을 출력으로 가지는 함수가 된다. 즉, $f(x_1, x_2, \dots x_n,$ unsigned transaction) = signed transaction 의 형태를 띄며, 다자간 계산을 적용할 수 있다. 다자간 계산을 적용하면 각 노드 j는 자신이 가지고 있는 조각인 x_j 를 제외한 다른 조각들은 모르는 상태로, 트랜잭션에 서명할 수 있게 된다. 또한 비대화형 영지식 증명에 기반하여, 기존 개인키를 변형하지 않고도 트랜잭션에 사용된 개인키의 조각들을 주기적으로 업데이트하는 것이 가능하게 하여 보안성을 높일 수 있다.

2. 영지식 증명(Zero-Knowledge Proof)

영지식 증명 [10]은 상대방에게 어떠한 사항이 참이라는 것을 증명할 때, 자신이 가지고 있는 어떠한 정보도 제공하지 않은 채 참, 거짓을 판별할 수 있는 절차를 뜻한다. 이 때, 정보를 가지고 해당 정보를 가지고 있다는 것을 증명하려고 하는 쪽을 증명자라고 하며, 해당 증명의 참, 거짓을 판별하려는 쪽을 검증자라고 한다. 영지식 증명은 완전성, 건전성, 영지식성이라고 하는 세가지 성질을 만족시켜야 한다. 완전성은 어떤 조건이 참이라면 신뢰할 수 있는 증명자는 검증자에게 해당 사실을 증명할 수 있어야 하는 성질이다. 건전성은 어떤 조건이 거짓이면 신뢰할 수 없는 증명자는 거짓말을 통해 검증자에게 해당 조건이 참임을 납득시킬 수 없어야 하는 성질이다. 마지막으로 영지식성은 어떤 조건이 참일 때, 증명 과정에서 해당 조건이 참이라는 정보를 제외한 어떠한 정보도 알 수 없어야 하는 성질이다. 영지식 증명은 이러한 세 가지 성질을 만족할 때, 검증자는 증명자가 해당 조건이 참이라는 사실을 확률적으로 확신할 수 있게 된다.

영지식 증명에는 두 가지 종류의 시스템이 존재한다. 첫 번째는 대화형 영지식 증명 시스템 (Interactive Zero-Knowledge Proof System)으로, 증명자와 검증자가 반복적인 대화를 통해 해당 조건이 참이라는 사실을 확률적으로 서서히 증가시켜 나가는 시스템이다. 두 번째는 비대화형 영지식 증명 시스템 (Non-Interactive Zero-Knowledge Proof System, NIZK)으로, 검증 시 증명자가 검증자에게 한 번의 정보 전송으로도 증명이 가능한 시스템이다. 대화형 시스템에서 필요했던 반복적인 대화가 없어져 시간적 효율성이 증가한다는 장점이 있다. 비대화형 영지식 증명의 대표적인 프로토콜로는 zk-SNARK (zero-knowledge Succint Non-Interactive Argument of Knowledge) [11]가 있다. zk-SNARK 프로토콜은 실제로 지캐시 (Zcash) [12] 암호화폐에 적용되어 개인의 거래 정보를 완전히 보호하는데 사용되고 있다. 또한 앞에서 설명한 안전한 다자간 계산의 과정 중, 개인키의 조각을 생성하는 과정과 사용된 개인키를 업데이트하는 과정에서도 해당 비대화형 영지식 증명 과정을 사용하고 있다.

Ⅲ. 본론

본 논문에서는 다중서명과 다자간 계산을 기반으로 한 디지털 자산 커스터디 서비스의 설계를 제안한다. 본 설계에서 전체적인 서비스는 4 단계의 레이어를 통해 구성되는데, 각 레이어를 통해 단계별 보안을 보장함으로써, 최대한 고객의 개인키가 노출되지 않도록 한다. 아래 그림 1 은 전체적인 커스터디 서비스의 구조도를 나타낸 것으로, 가장 위에 존재하는 레이어 0 은 고객과의 상호작용을 담당한다. 레이어 0 은 고객들이 사용할 수 있는 지갑 혹은 대시보드로 구성되어 있으며, 해당 요소들은 모바일 혹은 웹으로 구성된다.

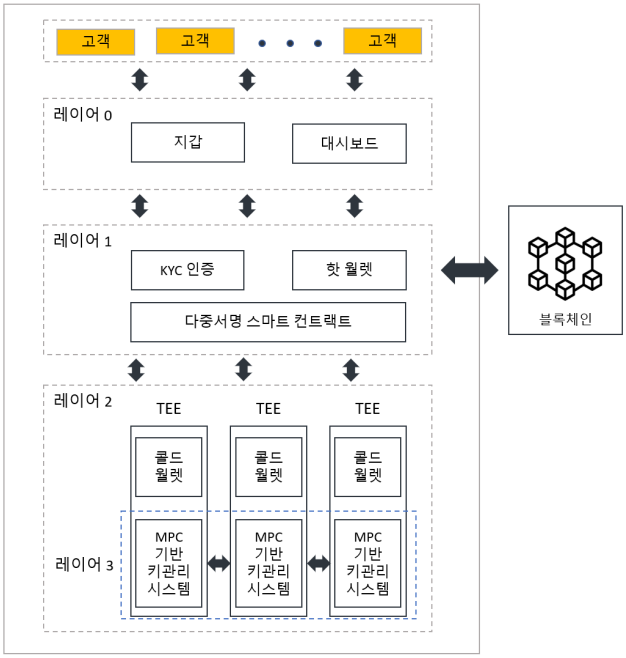


그림 1. 커스터디 서비스의 전체 구조도

레이어 0 에서는 고객들의 요청을 입력받아 해당 요청을 레이어 1 으로 전달해주는 역할을 한다. 이 때, 레이어 1 에서 가장 처음으로 제공하는 보안 요소는 KYC (Know Your Customer) 인증과정이다. 특금법에 의거하여 가상자산 사업자가 법에서 정의하는 금융회사에 포함됨에 따라, 가상자산 사업자는 KYC 인증과정을 통해 고객을 확인해야 할 의무를 가진다. 이에 따라 KYC 인증 과정을 레이어 1 에 위치시켜, 고객이 개인키를 생성하려면 먼저 지갑 소프트웨어나 대시보드를 통해 본인인증을 할 수 있도록 하였다. 또한 레이어 1 에는 KYC 인증과정 뿐만 아니라, 가상자산 사업자가 블록체인 네트워크와 쉽게 거래를 주고 받기 위한 핫 월렛이 위치하며, 고객의 개인키를 안전하게 관리하기 위한 다중서명 스마트 컨트랙트가 위치한다. 해당 스마트 컨트랙트를 통해 고객은 다중서명을 이용할 수 있으며, 생성된 여러 개의 개인키 중 일부를 가상자산 사업자 측에 위탁하여 이후 고객이 가지고 있는 개인키를 잃어버리더라도 복구할 수 있도록 한다.

이후 레이어 2 에서부터는 본격적으로 고객들로부터 위탁받은 자산을 안전하게 보관하기 위해, 가상자산 사업자 측에서 관리하는 개인키를 안전하게 보관하는 역할을 한다. 레이어 2 는 신뢰실행환경 (Trusted Execution Environment, TEE) [13]을 기반으로 동작한다. 신뢰실행환경은 보안성을 높이기 위해 메인 프로세서 내에 일반 영역과는 별도로 독립된 보안 영역을 제공하는 실행환경을 뜻한다. 본 설계에서는 신뢰실행환경을 통해 개인키의 조각들을 보호하기 위한 콜드월렛을 구현한다. 그림 1 에서도 볼 수 있듯이, 레이어 2 내부에는 여러 개의 신뢰실행환경이 존재하는 것을 확인할 수 있는데, 다자간 계산을 통해 생성된 개인키의 조각들을 해당 콜드월렛에 저장하는 구조이다. 이 때, 가상자산 사업자는 개인키를 몇 개의 조각으로 구성할지 유연하게 결정할 수 있는데, 해당 결정에 따라 사용되는 신뢰실행환경의 개수 역시 변화하게 된다.

레이어 3는 레이어 2 내부에서 동작하게 되는데, 신뢰실행환경 내부에 존재하는 MPC 기반 키관리 시스템을 통해 개인키를 관리하게 된다. 해당 시스템은 4가지 단계로 구성되어 있고 다음과 같은 과정으로 진행된다.

1. 개인키 x 를 n 개의 조각 $x_1, x_2, \ldots x_n$ 으로 나눈 후, 각 조각은 각 노드 $p_1, p_2, \ldots p_n$ 에 저장된다. 이 때, 각 노드는 슈노르 비대화형 영지식 증명 [14] 방법을 사용하여 자신의 개인키 조각 x_i 를 가졌다는 것을 전체 노드에 브로드캐스트한다.
2. 트랜잭션에 서명하기 전, 각 노드는 사전서명 과정을 거쳐 서명에 사용될 값들을 계산한다. 이 때, 파일리어 암호체계 [15]를 사용하여 각 노드가 가지고 있는 개인키의 조각에서 서명에 필요한 값들을 계산한다.
3. 서명 과정에서는 사전서명 과정에서 생성했던 값들을 통해 각 노드의 서명인 σ_i 를 생성하고, 생성된 서명을 통해 최종 서명인 σ 를 생성할 수 있다. 생성된 최종 서명을 통해 트랜잭션에 서명한다.
4. 주기적으로 각 노드에 저장된 개인키 조각을 업데이트하여 콜드월렛에 저장한다. 이 때, 비대화형 영지식 증명에 의해 개인키 조각을 업데이트하더라도 기존 개인키에는 영향이 없다.

레이어 3 내의 MPC 기반 키관리 시스템을 통해 온전한 개인키의 노출 없이 트랜잭션에 서명을 진행할 수 있다. 뿐만 아니라, 키관리 시스템을 통해 생성되거나 업데이트 된 개인키의 조각은 레이어 2 내의 신뢰실행환경에 저장되어 더욱 안전하게 보관된다. 이처럼 레이어 1 에서는 다중서명을 통해 고객의 개인키를 안전하게 보관하며, 레이어 2 와 3 에서는 다자간 계산을 통해 가상자산 사업자의 개인키를 안전하게 보관한다.

Ⅳ. 결론

본 논문에서는 다중서명과 다자간 계산을 기반으로 4 단계 레이어를 가지는 디지털 자산 커스터디 서비스의 설계를 제안했다. 다중서명 스마트 컨트랙트를 기반으로 편리하게 고객이 디지털 자산을 사용할 수 있을 뿐만 아니라, 개인키를 잃어버리더라도 찾을 수 있으며, 보안성이 뛰어난 다자간 계산을 기반으로 가상자산 사업자는 안전하게 개인키를 보관함으로써 위탁받은 디지털 자산을 안전하게 보관할 수 있다. 또한 다단 레이어 구조를 통해, KYC 인증과정과 신뢰실행환경을 포함한 3 중 보안을 고객에게 제공할 수 있도록 하였다.

향후 연구에서는 본 논문에서 제안한 설계를 기반으로 하여, 개인키의 조각을 물리적으로 안전하게 보관할 수 있는 하드웨어 보안 모듈 (Hardware Security Module, HSM)까지 포함하여 자세한 설계를 진행할 계획이다. 뿐만 아니라, 해당 설계의 구현을 통한 Proof-of-Concept 검증을 진행하여, 기존의 커스터디 서비스와 함께 정량적 성능을 평가 및 비교하는 연구가 필요하다.

ACKNOWLEDGMENT

본 연구는 ㈜코인원과 과학기술정보통신부 및 정보통신기획평가원의 대학 ICT 연구센터육성지원사업의 연구결과로 수행되었음 (IITP-2022-2017-0-01633)

참 고 문 헌

[1] KAAL, Wulf A. Digital Asset Market Evolution. J. Corp. L., 2020, 46: 909.

[2] 특정 금융거래정보의 보고 및 이용 등에 관한 법률. Available-at https://www.law.go.kr/법령/특정금융거래정보의보고및이용등에관한법률, Accessed: 2022-04-07

[3] 한국디지털에셋. Available at https://kodax.com/ Accessed: 2022-04-14

[4] 한국디지털자산수탁. Available at https://www.kdac.io/ Accessed: 2022-04-14

[5] OCC. Federally Chartered Banks and Thrifts May Provide Custody Services For Crypto Assets. Available at https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-98.html Accessed: 2022-04-14

[6] Coindesk. Goldman Sachs to Enter Crypto Market 'Soon' With Custody Play: Source. Available at https://www.coindesk.com/business/2021/01/15/goldman-sachs-to-enter-crypto-market-soon-with-custody-play-source/ Accessed: 2022-04-14

[7] HARN, Lein. Group-oriented (t, n) threshold digital signature scheme and digital multisignature. IEE Proceedings-Computers and Digital Techniques, 1994, 141.5: 307-313.

[8] CANETTI, Ran; MAKRIYANNIS, Nikolaos; PELED, Udi. Uc non-interactive, proactive, threshold ecdsa. Cryptology ePrint Archive, 2020.

[9] A. C. Yao, "Protocols for secure computations," 2013 IEEE 54th Annual Symposium on Foundations of Computer Science, IEEE, pp. 160-164, Nov 1982.

[10] A. De Santis and G. Persiano, "Zero-knowledge proofs of knowledge without interaction," Proceedings., 33rd Annual Symposium on Foundations of Computer Science, 1992, pp. 427-436, doi: 10.1109/SFCS.1992.267809.

[11] BEN-SASSON, Eli, et al. Succinct {Non-Interactive} Zero Knowledge for a von Neumann Architecture. In: 23rd USENIX Security Symposium (USENIX Security 14). 2014. p. 781-796.

[12] Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, Madars Virza, Zerocash: Decentralized Anonymous Payments from Bitcoin, proceedings of the IEEE Symposium on Security & Privacy (Oakland) 2014, 459-474, IEEE, 2014

[13] SABT, Mohamed; ACHEMLAL, Mohammed; BOUABDALLAH, Abdelmadjid. Trusted execution environment: what it is, and what it is not. In: 2015 IEEE Trustcom/BigDataSE/ISPA. IEEE, 2015. p. 57-64.

[14] HAO, Feng. Schnorr non-interactive zero-knowledge proof. RFC, 2017, 8235: 1-13.

[15] PAILLIER, Pascal. Public-key cryptosystems based on composite degree residuosity classes. In: International conference on the theory and applications of cryptographic techniques. Springer, Berlin, Heidelberg, 1999. p. 223-238.

이더리움에서 중복 사용 스마트 계약 가스 비용 분석

김애리, 주홍택
계명대학교 컴퓨터공학과
AeriKim@stu.kmu.ac.kr, juht@kmu.ac.kr

Analysis of duplicate usage smart contract gas costs in Ethereum

Aeri Kim, Hongtaek Ju
Dept. of Computer Engineering, Keimyung Univ.

요 약

이더리움의 스마트 계약은 블록체인의 특징인 투명성, 익명성, 비가역성 등을 통하여 존재 증명 및 내용 증명에 유리하며, 이를 활용한 디앱(Dapp)의 개발이 활발히 이루어지고 있다. 개발된 디앱은 특정 스마트 계약을 계속해서 사용하게 되는데, 이는 처음 부테린이 의도한 스마트 계약의 논리적 확장이라 할 수 있는 분산형 자율조직(DAOs)의 의의인 장기 스마트 계약과 의도가 상통한다. 이러한 장기적인 이용은 스마트 계약 중복 사용을 야기한다. 스마트 계약은 배포(Deploy)하고, 사용하는 데에 일명 가스(gas)라 부르는 비용이 필요하다. 계약의 중복 사용과 장기 사용을 모두 고려하여 가스 비용이 적게 들게 스마트 계약을 설계하고 디앱을 개발하여야 한다. 가스 비용의 절감은 환경적인 측면에서도, 사용자의 입장에서도 중요하기 때문이다. 본 논문에서는 테스트 넷을 구성하고, 인터넷 모임 내용을 증명하는 디앱의 스마트 계약을 개발 및 배포한다. 해당 스마트 계약에 내용을 담는 방법을 하나의 계약에 하나의 모임 내용을 담는 방식과(다중 배포; Multiple Deploy) 하나의 계약에 여러 모임의 내용을 담는 방식(단일 배포; One-time Deploy)으로 분류한다. 그리고 장기적이고 중복해서 계약을 사용할 때에 어떤 방식이 더 효율적인지 수식과 그래프를 통해 분석한다. 실험 결과는 스마트 계약에 하나의 모임 내용만을 담을 때에는 다중 배포 방식이, 둘 이상의 내용을 담을 때에는 단일 배포 방식이 효율적임을 보여준다. 해당 결론은 이더리움 사용자의 디앱 개발 및 사용에 도움을 줄 수 있다.

Ⅰ. 서 론

이더리움(Ethereum)은 비탈릭 부테린(Vitalik Buterin)에 의해 개발된 블록체인 플랫폼으로 튜링 완전 언어를 내장한다 [1]. 이더리움의 핵심은 임의의 사전 지정된 규칙에 따라 디지털 자산을 자동으로 이동하는 시스템인 스마트 계약(Smart Contract)이다. 스마트 계약은 블록체인의 특징인 투명성, 익명성, 비가역성 등을 통하여 존재 증명 및 내용 증명에 탁월한 이점을 가지고 있으며 [2], 이를 활용한 디앱(Dapp)의 개발이 활발히 이루어지고 있다. 보통 개발된 디앱은 특정 스마트 계약을 계속해서 사용하게 되는데, 이는 처음 부테린이 의도한 스마트 계약의 논리적 확장이라 할 수 있는 분산형 자율조직(DAOs)의 의의인 장기 스마트 계약과 의도가 상통한다. 이러한 장기적인 이용은 스마트 계약 중복 사용을 야기한다. 스마트 계약은 배포(Deploy)하고, 사용하는 데에 일명 가스(gas)라 부르는 비용이 필요하다. 계약의 중복 사용과 장기 사용을 모두 고려하여 가스 비용이 적게 들게 스마트 계약을 설계하고 디앱을 개발하여야 한다. 가스 비용의 절감은 환경적인 측면에서도[3], 사용자의 입장에서도 중요하기 때문이다.

본 논문에서는 이러한 계약의 중복 사용에 대하여 가스 비용을 분석하고 효율적인 가스 비용을 지출하는 방법을 제안한다. 분석에 사용되는 디앱은 햅즈업고(Hands-up-go)의 변형이다[4]. 기존의 핸즈업고는 행사 진행을 위한 블록체인 기반 분산 애플리케이션이며, 본 논문에서 사용할 변형 핸즈업고는 모임에 초점을 둔다. 요즘에는 소셜 네트워크 서비스(SNS)를 통해 사용자 간의 자유로운 의사소통과 정보 공유, 그리고 인맥 확대의 기회가 제공되며 사회적 관계망이 넓어지고 있다 [5]. 이를 통해 사람들은 익명을 바탕으로 자유롭게 모르는 사람들과 거래하고, 소통하며 모임을 갖기도 한다. 인터넷 공동 구매, 중고 거래, 소개팅 앱, 오픈 채팅방 등이 그 예시이다. 하지만 이러한 모임은 익명을 악용한 사기인 경우도 많다. 이에 디앱을 통하여 모임 내용을 기록하여 사기 행각을 막고 더 나아가 법적 증거물로 사용할 수 있게 정보를 제공할 수 있는 것이 핸즈업고이다.

본 논문은 핸즈업고를 사용하여 하나의 계약에 하나의 모임 내용을 담는 것이 좋은지(Multiple Deploy), 하나의 계약에 여러 모임의 내용을 담는 것이 좋은지(One-time Deploy) 분석하고 효율적인 방안을 제시한다. 본 논문의 결과는 이더리움 사용자의 디앱 개발 및 사용에 도움을 줄 수 있다.

Ⅱ. 관련 연구

이기영 등[4]은 이더리움 블록체인 기반으로 행사 진행에 사용하는 분산 애플리케이션인 핸즈업고 개발 내용과 결과를 제시한다. 해당 논문에서 제시하는 핸즈업고를 기반으로 사용 의도와 설계를 구체화하고 변형한 것이 본 논문에서 분석으로 사용할 디앱이다. 이기영 등이 제시한 핸즈업고와 본 논문의 핸즈업고는, 원리는 비슷하나 디앱의 구성과 스마트 컨트랙트의 구조 및 함수가 다르다.

김진영 등[6]은 스마트 컨트랙트의 개발 언어가 가스에 미치는 영향을 분석한다. Solidity, Vyper, Diff 언어에 대해 총 4가지의 함수를 사용하여 가스 비용을 측정하며 Vyper를 사용하는 것이 효과적임을 보여준다.

S. Christopher 등[7]은 가스 비용을 심층적으로 시각화하는 도구인 Visualgas를 제공하여, 스마트 계약의 더 간단하고 가스 효율적인 개발을 지원한다.

김대한 등[8]은 이더리움 네트워크에 트랜잭션 발행 시 발생하는 부하, 즉 비용을 줄이기 위해 스마트 계약을 효율적으로 구성하는 방식을 연구한다. 그 결과로 배포 시 구조체를 활용하거나, 매개 변수를 임시 값으로 받고 반환하는 것이 효율적이라고 밝힌다.

이더리움의 스마트 계약 가스 비용 분석은 언어 및 구조 등 다양한 관점에서 이루어지고 있으며, 효율적인 가스 사용을 위한 도구를 제공하기도 한다. 본 논문에서는 가스 절감을 위하여 계약에 내용을 담는 방법을 제안하여 이더리움 사용자가 디앱을 효율적으로 사용할 수 있게 돕는다.

Ⅲ. 실험 설계 및 환경 구성

3.1. 핸즈업고 설계

핸즈업고는 모임 내용을 기록하는 것을 목적으로 한다. 이때 모임 내용을 어떻게 담아서 스마트 계약을 배포할 것인지에 따라 단일 배포(One-time Deploy)와 다중 배포(Multiple Deploy)로 나뉘며, 이에 따라 엔티티와 함수도 달라진다.

먼저 다중 배포의 경우는 하나의 스마트 계약에 하나의 모임 내용이 담기는 것으로 다음과 같은 시나리오를 갖는다.

1. 모임을 주관하는 모임장(Agent)이 모임 내용을 등록(Constructor)한다. 주관자는 모임 마감 기한(Deadline), 모임 참가비용(Fee), 모집 인원(GoalNum), 모임 내용(contents)을 담아 스마트 계약을 배포하게 되고, 이때 모임 내용은 SHA-256 해시 함수로 해싱한 결과이다. 많은 내용이 담기면 가스 비용이 증가하기 때문에 외부에 데이터베이스를 따로 두고, 내용을 증명할 수 있는 해시 함수를 사용한다.
2. 불특정 다수(Anybody)는 배포된 계약을 통해 현재 모집 인원수(nowNum), 마감기한까지 남은 시간(remain), 모임 내용(getInfo)을 확인한다.
3. 참가하고 싶으면 불특정 다수는 참가자(Participant)가 되어, 일정 참가비용을 계약에 지불함(receive)으로써 참가 등록을 한다.
4. 설정한 마감기한이 끝나면(isdeadline) 더 이상 참가할 수 없으며, 모임장과 참가자는 모임 내용을 수행한다.

다중 배포의 유스 케이스와 컨트랙트 다이어그램은 다음 그림 1이다.

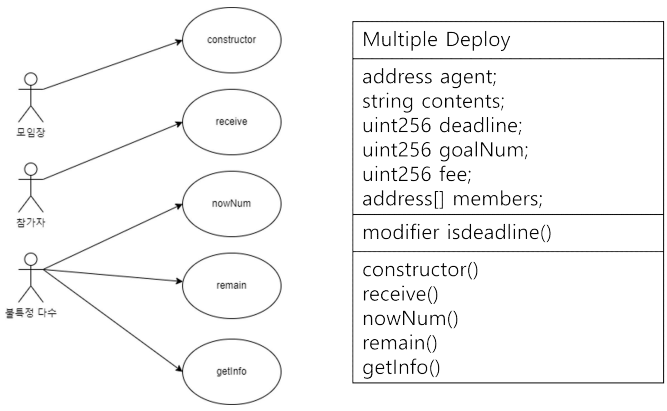


그림 1. 다중 배포의 유스 케이스와 컨트랙트 다이어그램

단일 배포의 경우에는 하나의 스마트 계약에 여러 모임 내용을 담는다. 유스 케이스와 컨트랙트 다이어그램은 그림 2로 표현하고 있으며, 시나리오는 다음과 같다.

1. 모임을 관리하는 관리자(Admin)가 일정한 시간 간격(time)을 두고 계약을 배포한다(Constructor).
2. 모임을 주관하는 모임장(Agent)이 관리자에게 모임 마감 기한(Deadline), 모임 참가비용(Fee), 모집 인원(GoalNum), 모임 내용(contents/SHA-256)을 넘기면, 관리자는 해당 내용을 스마트 계약 리스트(calist)에 넣는다(AddCa). 이때 관리자만이 계약을 추가할 수 있다(isAdmin).
3. 불특정 다수(Anybody)는 배포된 계약을 통해 현재 모집 인원수(nowNum), 마감기한까지 남은 시간(remain), 모임 내용(getInfo)을 확인한다.
4. 참가하고 싶으면 불특정 다수는 참가자(Participant)가 되어, 일정 참가 비용을 계약에 지불함(join)으로써 참가등록을 한다.
5. 설정한 시간 간격이 지나면(isEnd) 더 이상 다른 계약을 추가할 수 없고, 참가할 수 없으며 모임장과 참가자는 모임 내용을 수행한다.

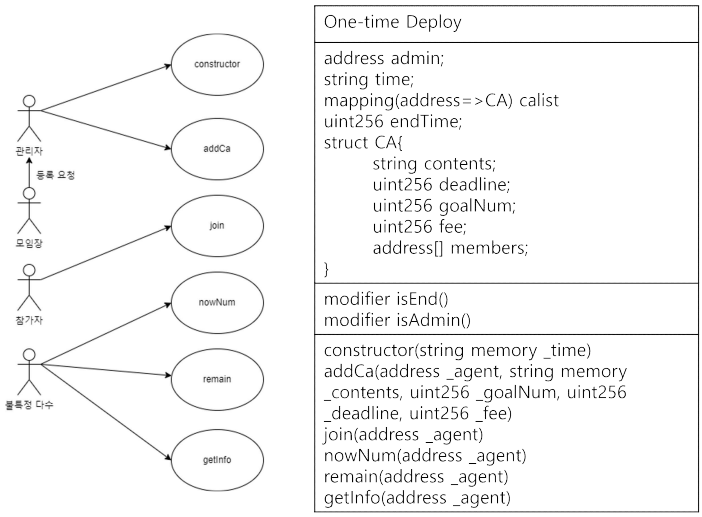


그림 2. 원타임 배포의 유스 케이스와 컨트랙트 다이어그램

3.2. 실험 환경

본 연구에서 사용된 PC는 i5-7500T CPU, 8GB의 메모리를 갖고 있으며, 저장 공간은 SSD 1TB 하드디스크를 사용한다. 운영체제는 리눅스 18.04 LTS 이다. Geth 는 1.10.16 버전, Go는 1.17.1 버전을 이용하며, 솔리디티 언어는 0.8.13+를 사용한다.

Docker를 사용하여 Geth를 설치하고, 독자적인 테스트 넷(private network)을 구성한다. 솔리디티 언어 작성은 Remix IDE 웹 사이트[8]를 사용하고 있으며, 만들어진 스마트 컨트랙트 컴파일과 배포 및 실행은 모두 독자적인 테스트 넷에서 진행한다.

Ⅳ. 스마트 컨트랙트 비용 분석

4.1. 비용 분석 방법

스마트 컨트랙트에 사용되는 가스 비용은 크게 배포(Deploy) 비용, 함수 실행 비용(트랜잭션 발생)으로 나눌 수 있다. 여기서 단일 배포와 다중 배포의 비용을 핸즈업고로 분석하기 위해서 함수 실행비용을 나눠 참가비용까지 고려한다. 참가비용은 payable 함수를 사용할 때 사용되는 가스이고, 그 외의 함수는 함수 실행비용으로 처리한다. 다중 배포의 경우에는 함수 실행비용을 고려하지 않아도 된다. 위의 비용 분류를 통해 다음과 같은 비용 계산 수식을 세울 수 있다.

$$TC_x = DC_x \cdot k + FC_x \cdot n + JC_x \cdot p$$

수식 1. 가스 비용 계산 수식

수식 1에서 TC_x는 총 비용(TotalCost)을 의미하고, 각 DC_x, FC_x, JC_x는 배포 비용(Deploy Cost), 함수 실행비용(Function Cost), 참가비용(Join Cost)이다. k,n,p 값은 각각 배포 횟수, 모임의 수, 참가자의 수를 의미한다. 단일 배포의 경우에는 k의 값이 1로 고정된다. 다중 배포의 경우에는 함수 실행비용이 사라지고, 배포 횟수와 모임의 수가 같은 의미를 갖는다. 이를 고려하여 수식1에서 다음 수식2(x=o)와 수식3(x=m)을 도출할 수 있다.

$$TC_o = DC_o + FC_o \cdot n + JC_o \cdot p$$

수식 2. 단일 배포 가스 비용 계산 수식

$$TC_m = DC_m \cdot n + JC_m \cdot p$$

수식 3. 다중 배포 가스 비용 계산 수식

여기서 DC_x, FC_x, JC_x에 계수를 부여해야 한다. 보통 배포 비용이 함수 실행비용보다 크다. 하지만 함수 실행을 많이 할수록 배포 비용보다 함수 실행비용이 많이 소모될 가능성이 높아진다. 다음 4.2에서 핸즈업고 테스트를 통해 계수를 찾고 수식을 완성한다.

4.2. 핸즈업고 비용 분석

핸즈업고 비용 분석을 위해 테스트의 조건을 정한다. 단일과 다중 배포 방식으로 각각 3명이 모임을 생성한다 (총 6개의 컨트랙트가 배포). 해당 모임에 참가하는 인원은 2명이다 (총 12명). 두 스마트 계약의 모집인원은 2명, 마감기한은 10분, 참가비용은 1 ether로 고정한다. 모임의 내용은 전부 다르게 설정하여 해싱 후 값을 입력한다. 조건에 따라서 실험을 진행한 결과는 다음 표 1과 같다.

표 1. 가스 효율 비교 표

항목	다중 배포(x=m)	단일 배포(x=o)
배포 비용 (DC_x)	757,531	1,071,456
참가 비용 (JC_x)	67,279 52,279 = 119,558	69,449 54,449 = 123,898
함수 실행 비용 (FC_x)	-	147,964
합계	2,631,267	1,887,042

표 1의 단위는 1,000,000,000 * wei 이다. 모든 비용은 두 가지 배포 방식에 따라 고정된 값을 가졌다. 참가비용을 보면 두 개의 값이 들어있는데 첫 번째 참가자가 실행한 비용과 두 번째 참가자가 실행한 비용이 다르게 나타난다. 이에 추가로 참가 인원 수를 늘려 비용의 추이를 보았다. 그 결과 첫 번째 참가자를 제외하고 다음 참가자들은 모두 같은 실행비용을 소모했다. 따라서, 수식에 다른 변형을 주진 않는다. 합계는 테스트 조건을 수식2와 수식3에 적용하고, 표의 값을 대입하여 계산한 결과이다. 합계는 우선 다중 배포보다 단일 배포가 효율적임을 보여준다. 하지만, 참가 인원 수와 모임의 수에 따라서 효율이 달라질 수 있다. 이는 4.3에서 그래프를 그리며 경우의 수를 따져 분석한다.

4.3으로 넘어가기 전에 표 1을 통해서 계수를 계산한다. 표 1의 값을 100,000으로 나누고 반올림한 것을 계수라고 한다. 계수를 적용한 비용 계산 수식은 다음 수식 4와 수식 5이다.

$$TC_o = 10.7 + 1.5 \cdot n + 1.2 \cdot p$$

수식 4. 계수를 적용한 단일 배포 가스 비용 계산 수식

$$TC_m = 7.6 \cdot n + 1.2 \cdot p$$

수식 5. 계수를 적용한 다중 배포 가스 비용 계산 수식

4.3. 비용 분석 결과

수식 4와 5에서 참가비용인 각 JC_o 와 JC_m는 1.2로 동일하다. 즉 두 수식에 값을 넣어 비교할 때에는 참가비용을 고려하지 않아도 된다. 모임의 수만 고려하면 된다. 따라서 n에 1부터 1씩 증가하는 정수를 넣고 값을 비교하는 그래프를 그린다. 다음 그림 3이 비교 그래프이다.

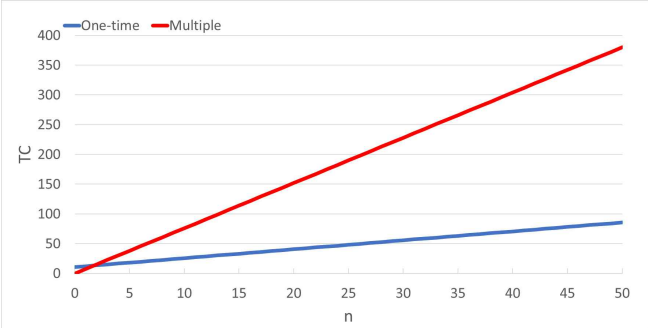


그림 3. 스마트 계약 비용 비교 그래프

그림 3을 통해, 스마트 계약에서 모임 내용이 두 개 이상일 경우부터는 단일 배포를 사용하는 것이 효율적임을 알 수 있다. 모임이 하나일 때에는 단일 배포가 12.2, 다중 배포가 7.6으로 다중 배포를 사용하는 것이 좋다.

V. 결론 및 향후 연구

본 논문은 테스트 넷을 구성하고, 인터넷 모임 내용을 증명하는 디앱인 핸즈업고의 스마트 계약을 개발 및 배포한다. 해당 스마트 계약에 내용을 담는 방법을 단일 배포 방식과 다중 배포 방식으로 분류하여 장기적이고 중복해서 계약을 사용할 때에 어떤 방식이 더 효율적인지 수식과 그래프를 통해 분석한다. 실험 결과는 스마트 계약에 하나의 모임 내용만을 담을 때에는 다중 배포 방식이, 둘 이상의 내용을 담을 때에는 단일 배포 방식이 효율적임을 보여준다. 해당 결론은 다른 스마트 계약에서도 사용할 수 있으며 배포 비용과 함수 실행비용만 구한다면, 계수 계산을 통해 효율적인 배포 방식을 선택할 수 있다.

향후 연구로는 테스트 넷이 아닌 퍼블릭 네트워크에서는 본 논문의 실험을 진행하여 비용이 어떻게 책정되는지 비교 분석해볼 필요가 있다. 또한, 함수의 개수나 계약의 구조 및 내용을 바꾸고 테스트 케이스를 세분화하여 더욱 정밀한 수식과 결과를 도출하는 실험을 진행할 수 있다.

ACKNOWLEDGMENT

이 논문은 2018년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(NRF-2018R1D1A1B07050380).

참 고 문 헌

[1] B. Vitalik,. "A next-generation smart contract and decentralized application platform.", white paper, 2014.

[2] M. Wohrer & U. Zdun. “Smart Contracts: Security Patterns in the Ethereum Ecosystem and Solidity”. 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE). IEEE. 2018.

[3] Ethereum Energy Consumption Index, https://digiconomist.net/ethereum-energy-consumption. 2022, April 14

[4] 이기영, Hartanto Kurniawan, Intan Permatasari, Yoga Andrian, 주홍택, “이더리움 기반 Hands-up & Go 분산 어플리케이션 개발”, pre-print

[5] H. Yu, and I. Song, "웹 서비스 형태 변화에 따른 소셜 네트워크 서비스의 진화", Review of Korean Society for Internet Information 11.3, 2010, p. 52-62.

[6] 김진영, 김미수, 이은석, “스마트 컨트랙트의 개발 언어별 가스에 미치는 영향 분석”, 한국정보과학회 학술발표논문집, 2021, p. 230-232.

[7] N. Grech, M. Kong, A. Jurisevic, L. Brent, B. Scholz & Y. Smaragdakis, “Madmax: Surviving out-of-gas conditions in ethereum smart contracts” Proceedings of the ACM on Programming Languages, 2(OOPSLA), 2018, p. 1-27.

[8] D. Kim, K. Choi, K. Kim & J. Kim, “A Study on Efficient Ethereum Smart Contract”. In: Proceedings of the Korea Information Processing Society Conference. Korea Information Processing Society, 2018, p. 82-84.

[9] Remix IDE, https://remix.ethereum.org, 2022, April 14



TS7:
네트워크 보안 2

2D CNN 기반 네트워크 침입 탐지 모델

이범수 [1], 김종욱 [1], 방지원 [2], 최미정 [1,2,*]
강원대학교 컴퓨터과학과 [1]
강원대학교 빅데이터메디컬융합학과 [2]

{kreasen, jw.kim, jiwonbang, mjchoi}@kangwon.ac.kr

2D CNN-Based Network Intrusion Detection Model

Beom-Su Lee[1], Jong-Wouk Kim[1], Jiwon Bang[2], Mi-Jung Choi[1,2,*]
Dept. of Computer Science, Kangwon National Univ.[1]
IGP. In Medical Bigdata Convergence Kangwon National Univ.[2]

요 약

클라우드, IoT, 5G 등 현대의 다양한 네트워크 기술은 여러 종류의 디바이스 간 연결을 가능하게 하고 빠른 속도를 지원함으로써 사람들에게 편의성을 제공한다. 하지만 네트워크 공격 형태 또한 고도화되면서 침입 사례와 새로운 공격 유형이 증가함에 따라 기존의 규칙 기반 탐지 방식으로는 새로운 공격 유형을 탐지하기 어려운 상황이다. 따라서 본 논문에서는 딥러닝과 이상 탐지 방식을 결합한 침입 탐지 모델을 제안한다. 딥러닝의 일종인 CNN을 사용하여 이상 탐지 모델을 설계하고 CICIDS 2018 데이터 셋을 샘플링 및 전처리하여 학습하고 탐지 성능을 측정하였다. 실험 결과 최고 94.27%의 정확도, 94.32%의 F1-score 등의 우수한 성능을 달성하였다. 따라서 본 논문에서 제안한 모델은 네트워크 침입을 탐지하기 위한 모델 설계에 적용될 수 있다.

Ⅰ. 서 론

클라우드, IoT, 5G 등 현대의 다양한 네트워크 기술은 여러 종류의 디바이스들 간의 연결을 가능하게 했고, 이는 많은 트래픽을 발생하고 있다. 네트워크 트래픽 양이 증가함에 따라 DDoS, Flooding 등 기존에 알려진 네트워크 공격 유형뿐만 아니라 제로 데이(Zero-day)와 같이 새로운 유형의 공격 사례 또한 빈번하게 발생하고 있어 네트워크 보안에 대한 중요성이 점점 더 커지고 있다.

위와 같은 네트워크 공격들을 방어하기 위해 사용되는 시스템은 NIDS(Network Intrusion Detection System)가 대표적이다. NIDS는 네트워크 상의 트래픽을 분석하여 침입을 탐지하는 시스템으로 규칙 기반 탐지와 이상 탐지 방식으로 구분된다. 규칙 기반 탐지는 기존에 존재하는 공격의 패턴을 분석하여 탐지하는 방식으로 패턴을 분석하여 탐지하기 때문에 정확도가 높고 오탐률이 낮지만 새로운 공격의 유형을 탐지하지 못하는 단점이 있다. 이상 탐지 방식은 정상적인 트래픽을 비교, 분석하여 공격을 탐지하는 방식으로 새로운 공격 유형을 탐지할 수 있지만 정확도가 낮고 오탐률이 높다. 따라서 이상 탐지 방식을 기계 학습 및 딥러닝과 결합하여 정확도를 높이고 오탐률을 낮추려는 연구가 활발히 이루어지고 있다 [1], [2].

본 논문에서는 딥러닝을 사용하여 높은 정확도와 낮은 오탐률을 가지는 네트워크 침입 탐지 모델을 만들기 위한 연구를 진행하였다. 설계 모델은 이미지 분류에 효과적인 CNN(Convolutional Neural Network)을 사용하였고 학습과 테스트에 사용할 데이터는 침입 탐지 모델을 위한 최신 데이터 셋인 CICIDS 2018을 사용하였다 [3]. 설계한 모델에 CICIDS 2018 데이터 셋을 적용하여 데이터가 악성(Malicious)인지 정상(Benign)인지 나타내는 이진 분류를 진행하였다. CICIDS 2018의 경우 데이터양이 많고 정상 트래픽의 비율이 높기 때문에 샘플링(Sampling)한 데이터를 사용하여 실험하였다. 실험 결과 최고 0.9427의 정확도와 0.9432의 F1-score를 달성했다.

본 논문은 다음과 같이 구성된다. 2장에서는 침입 탐지 모델에서 사용되는 데이터 셋과 딥러닝 기반의 침입 탐지 모델 연구에 대해 소개하고 3장에서는 본 논문에서 사용한 데이터 셋과 샘플링 및 전처리 방법, 설계한 CNN 모델을 소개한다. 4장에서는 실험한 환경과 실험 결과에 대해 서술하고 5장에서 결론 및 향후 연구를 다룬다.

Ⅱ. 관련 연구

1) 공개 데이터 셋

네트워크 침입 탐지를 위해 자주 사용되는 데이터 셋은 KDD Cup 99 [4], NSL-KDD [5], UNSW-NB15 [6]가 있다. 먼저 KDD Cup 99는 DARPA'98 IDS 평가 프로그램에 의해 수집된 데이터 셋으로 4가지 공격 유형(DoS, U2R, R2L, Probing)과 41개의 네트워크 관련 특징으로 구성된다. KDD Cup 99는 학습 데이터와 테스트 데이터의 중복 데이터가 많다는 문제점 때문에 중복 데이터를 제거하고 새로운 데이터를 추가한 NSL-KDD이 사용된다 [7].

UNSW-NB15은 2015년에 생성된 데이터 셋으로 IXIA PerfectStorm을 사용하여 공격 및 정상 네트워크 트래픽을 수집 및 가공하여 만든 데이터 셋이다. 9개의 공격 유형('Fuzzers', 'Analysis', 'Backdoors', 'DoS',

'Exploits', 'Generic', 'Reconnaissance', 'Shellcode', 'Worms')과 49개의 네트워크 관련 특징으로 구성된다. KDD Cup 99, NSL-KDD, UNSW-NB15의 경우 생성된 지 오래되어 현재의 공격 유형과 네트워크를 나타내기 어렵기 때문에 본 논문에서는 CICIDS 2018 데이터 셋을 사용하였다.

2) 침입 탐지 모델 연구

Kim et al.의 연구는 DoS 유형의 공격을 탐지하기 위해 CNN 모델을 제안했다 [8]. KDD Cup 99와 CICIDS 2018 데이터 셋에서 정상 트래픽과 DoS 유형의 공격을 샘플링한 데이터를 구성하여 모델을 학습하고 테스트하였다. 데이터를 전처리하여 각각 13×9 , 13×6 크기의 회색조와 RGB 이미지로 변환하였다. 이미지 유형과 컨볼루션(Convolution) 레이어의 수, 커널 크기 등을 조절하여 이진 분류 및 다중 분류에 대한 실험을 진행하여 RNN 모델보다 우수함을 보였다.

Jiang et al.의 연구는 데이터 불균형을 해결하기 위해 하이브리드 샘플링 방법을 제안했다 [9]. NSL-KDD 및 UNSW-NB15 데이터 셋에서 OSS(One-Side Selection)를 사용하여 다수 클래스의 샘플을 줄이고 SMOTE (Synthetic Minority Over-sampling Technique)로 소수 클래스의 샘플을 늘려 불균형을 해소한 데이터를 생성하였다. CNN과 BiLSTM(Bi-directional Long Shot-Term Memory)을 결합한 모델을 설계하여 생성 데이터 셋에 대한 성능을 실험하였다.

Devan et al.의 연구는 효율적인 침입 탐지를 위해 XGBoost(eXtreme Gradient Boosting)와 DNN을 결합한 모델을 제안했다 [10]. XGBoost는 특징 중요도 점수를 계산하여 분류 모델에 사용되는 특징을 고르기 위해 사용되고 DNN(Deep Neural Network)은 XGBoost를 통해 선택된 기능을 사용하여 침입 탐지 분류를 위해 사용하였다. 데이터 셋은 NSL-KDD를 사용하였으며 해당 논문에서 제안한 모델의 성능과 효율성을 검증하기 위해 로지스틱 회귀, 서포트 벡터 머신 등 기존의 기계 학습 모델과 비교하였을 때 상대적으로 우수한 성능을 보였다.

Ⅲ. 모델 설계

1) 데이터 셋

본 연구에서는 CICIDS 2018 데이터 셋을 사용한다. CICIDS 2018은 현재의 IDS 시스템을 만들기 위해 AWS 환경에서 피해 네트워크와 공격 네트워크를 구성하고 10일 동안 다양한 공격 유형을 수행하여 만든 데이터 셋이다. NSL-KDD와 UNSW-NB15와 달리 최신의 공격 유형을 포함하기 때문에 현재의 침입 탐지 모델을 설계하는데 적절하다. CICIDS 2018은 총 10개의 파일로 나누어져 있으며 약 1,600만 개의 데이터가 존재하고 14개의 공격 유형과 79개의 네트워크에 관한 특징으로 구성된다. 표 1은 데이터 셋의 공격 유형과 분포를 나타낸다.

2) 샘플링

CICIDS 2018 데이터 셋은 정상 데이터가 약 83%를 차지하는 불균형 데이터 셋이다. 불균형한 데이터를 사용하여 학습할 경우 모델 성능 저하의 원인이 되므로 데이터를 샘플링하여 학습한다. 샘플링 과정은 알고리즘 1과 같다. 10개의 파일을 하나씩 검사하여 다음 파일과 같은 공격 유형을 가지고 있는 경우 두 파일을 합치고 공격 유형별 데이터 수를 확인한다. 10만개를 기준으로 이상인 경우 10만개를 샘플링 하고 미만인 경우 해당 데이터 전체를 포함한다. 중복 데이터를 방지하기 위해 이미 샘플링된 데이터는 포함하지 않는다. 샘플링 결과 데이터 수가 약 160만개이고 정상 데이터의 비율이 약 48%인 데이터를 구성한다. 표 2는 샘플링 후 CICIDS 2018 데이터의 분포이다.

3) 데이터 전처리

본 논문에서 제안한 CNN 모델은 2차원 벡터를 입력으로 받기 때문에 전처리가 필요하다. 먼저 이상치 제거를 위해 무한대 값을 가지는 행과 null 값을 가지는 행을 제거한다. 그리고 단순히 패킷 생성 시간을 나타내는 'Timestamp'열과 항상 동일한 값을 가지는 8개의 열('Bwd PSH Flags', 'Bwd URG Flags', 'Fwd Byts/b Avg', 'Fwd Pkts/b Avg', 'Fwd Blk Rate Avg', 'Bwd Byts/b Avg', 'Bwd Pkts/b Avg', 'Bwd Blk Rate Avg')을 제거한다. 범주형 데이터는 학습 데이터로 적절치 않으므로 'Protocol'열을 원-핫(One-Hot) 인코딩을 통해 다차원 실수형 벡터로 변환한다. 모든 데이터를 [0.0, 1.0]으로 나타내기 위해 Min-Max 정규화를 사용하고 이진 분류를 위해 'Label'열을 분리하여 정상(Benign) 또는 악성(Malicious)으로 변경한다. 초기 79개의 특징은 전처리 이후 72개의 특징으로 줄어든다. $N \times N$ 크기의 2차원 벡터로 만들기 위해 9개의 제로 패딩(Zero Padding)을 추가하여 81개의 특징을 9×9 크기의 2차원 특징 벡터로 만든다.

(표 1) CICIDS 2018 데이터 분포.

Label	# of data	Label	# of data
Benign	13,390,249 (0.82978)	DDoS-HOIC	686,012 (0.04251)
FTP-Bruteforce	193,354 (0.01198)	DDoS-LOIC-UDP	1,730 (0.00011)
SSH-Bruteforce	187,589 (0.01162)	Bruteforce-Web	611 (0.00004)
DoS-GoldenEye	41,508 (0.00257)	Bruteforce-XSS	230 (0.00001)
DoS-Slowloris	10,990 (0.00068)	SQL Injection	87 (0.00001)
DoS-Hulk	461,912 (0.02862)	Infiltration	160,639 (0.00995)
DoS-SlowHTTPTest	139,890 (0.00867)	Bot	286,191 (0.01773)
DDoS-LOIC-HTTP	576,191 (0.03571)	**Total**	16,137,183 (1.00000)

(표 2) 샘플링 후 CICIDS 2018 데이터 분포.

Label	# of data	Label	# of data
Benign	800,000 (0.48334)	DDoS-HOIC	100,000 (0.06042)
FTP-Bruteforce	100,000 (0.06042)	DDoS-LOIC-UDP	1,730 (0.00105)
SSH-Bruteforce	100,000 (0.06042)	Bruteforce-Web	611 (0.00037)
DoS-GoldenEye	41,508 (0.02508)	Bruteforce-XSS	230 (0.00014)
DoS-Slowloris	10,990 (0.00664)	SQL Injection	87 (0.00005)
DoS-Hulk	100,000 (0.06042)	Infiltration	100,000 (0.06042)
DoS-SlowHTTPTest	100,000 (0.06042)	Bot	100,000 (0.06042)
DDoS-LOIC-HTTP	100,000 (0.06042)	**Total**	1,655,156 (1.00000)

4) 모델 구조

본 논문에서 제안하는 CNN 기반 탐지 모델은 그림 1 및 표 3과 같다. 입력 데이터에서 특징을 추출하기 위해 두 개의 컨볼루션 레이어를 사용하고 각 레이어에서 연산 결과를 Flatten 함수를 사용하여 각각 1차원 벡터로 만든 다음 Concatenate 함수를 통해 완전 연결(Fully Connected) 레이어를 구성한다. 마지막으로 완전 연결 레이어에서 활성화 함수로 Softmax 함수를 적용하여 정상 트래픽과 악성 트래픽을 분류한다.

각 레이어에서 사용한 세부 파라미터는 다음과 같다. 첫 번째 컨볼루션 레이어는 32개의 필터, 3×3의 필터 크기, 두 번째 컨볼루션 레이어는 16개의 필터, 2×2 필터 크기를 사용하고 활성화 함수는 ReLu 함수로 두 레이어 동일하다. 풀링(Pooling) 레이어는 모두 2×2 크기를 사용하고 최대 풀링 방식을 사용하였다. 과적합을 방지를 위해 두 컨볼루션 레이어 사이에 Dropout(0.5) 함수를 사용한다.

Ⅳ. 실험 및 실험 결과

1) 실험

먼저 샘플 데이터를 훈련 데이터와 테스트 데이터로 나누기 위해 train_test_split 함수를 사용하여 7:3 비율로 나눈다. 훈련 데이터와 학습 데이터의 분포는 표 4와 같다. 과적합을 방지하기 위해 훈련 데이터를 나누어 학습하고 평가하는 교차 검증(Cross Validation)을 8:2 비율로 사용한다.

본 논문에서 설계한 CNN 모델의 성능 평가를 위해 정확도(Accuracy), 재현율(Recall), 정밀도(Precision) 그리고 F1-score을 사용한다. 수식(1)-(4)은 평가 지표를 계산하기 위한 수식이다. TP(True Positive)는 실제 정상인 것을 모델이 정상으로 바르게 예측한 것이고 FP(False Positive)는 실제 악성인 것을 모델이 정상으로 잘못 예측한 것이다. TN(True Negative)는 실제 악성인 것을 모델이 악성으로 바르게 예측한 것이고 FN(False Negative)는 실제 정상인 것을 모델이 악성으로 잘못 예측한 것이다.

2) 실험 결과

샘플링된 CICIDS 2018 데이터를 전처리를 통해 9×9 크기의 2차원 특징 벡터로 변환하고 3.4절에서 설계한 CNN 모델을 사용하여 실험을 진행하였다. 실험은 총 10번 진행하였으며 각 실험에서 학습 데이터를 통해 30번씩 반복(Epoch)하여 모델을 학습하고 테스트 데이터를 통해 성능을 평가하였다. 성능 측정을 위한 평가 지표를 10번 실험한 결과의 최고와 평균을 계산하였고 그림 2와 같다. 실험 결과 정확도는 평균 0.9411, 최고 0.9427을 얻었다. 재현율은 평균 0.9080, 최고 0.9105를 얻었으며 정밀도의 경우 평균 0.9769, 최고 0.9843, F1-score의 경우 평균 0.9412, 최대 0.9432로 우수한 성능을 얻었다. 표 5는 10번의 실험에서 얻은 결과의 평균을 계산한 혼동 행렬이다. 본 논문에서 제안한 모델은 실제 악성일 때 모델이 양성으로 분류한 FP보다 실제 양성일 때 모델이 악성으로 분류한 FN의 발생 빈도가 높다. 따라서 재현율이 다른 평가 지표에 비해 낮고 정밀도가 상대적으로 높은 성능을 보인다.

$$Accuracy = \frac{TP+TN}{TP+FP+FN+TN} \quad (1)$$

$$Recall = \frac{TP}{TP+FN} \quad (2)$$

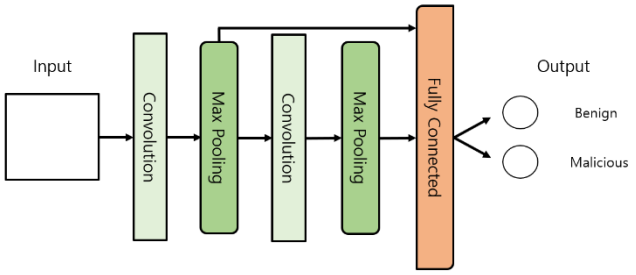
$$Precision = \frac{TP}{TP+FP} \quad (3)$$

$$F1-Score = 2 \times \frac{Precision \times Recall}{Precision+Recall} \quad (4)$$

Algorithm for Sampling CICIDS 2018

Input: files of CICIDS 2018 $\mathbb{F}$; a set of labels $\mathbb{L}$
Output: sampled data $\mathbb{D}$
begin
(1) **for** *i* **in** (# of $\mathbb{F}$-1) **do**
(2) *cur_file* ← $\mathbb{F}[i]$
(3) *next_file* ← $\mathbb{F}[i+1]$
(4) *cur_label_set* ← set of labels in $\mathbb{F}[i]$
(5) *next_label_set* ← set of labels in $\mathbb{F}[i+1]$
(6) **if** *cur_label_set* == *next_label_set* **then**
(7) $\mathbb{F}[i]$ ← merge($\mathbb{F}[i]$, $\mathbb{F}[i+1]$)
(8) **for** *label* **in** $\mathbb{L}$ **do**
(9) *data* ← data with *label* in $\mathbb{F}[i]$
(10) **if** # of *data* >= 100000 **then**
(11) concatenate Sampling(*data*, 100000) and $\mathbb{D}$
(12) **end for**
(13) **end for**
(14) **return** $\mathbb{D}$
end

(알고리즘 1) CICIDS 2018 샘플링.



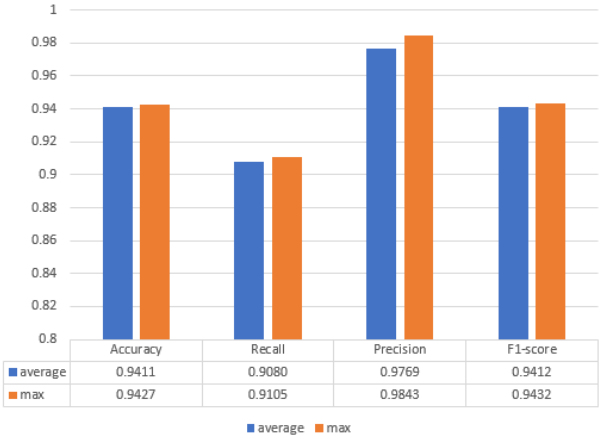
(그림 1) CNN 모델 구조.

(표 3) CNN 모델.

Layer	Out Shape	# of Parameters
Input	(-1, 9, 9, 1)	0
Conv2D-1	(-1, 7, 7, 32)	320
Max Pooing-1	(-1, 6, 6, 32)	0
Dropout	(-1, 6, 6, 32)	0
Conv2D-2	(-1, 5, 5, 16)	2064
Max Pooling-2	(-1, 4, 4, 16)	0
Flatten-1	(-1, 1152)	0
Flatten-2	(-1, 256)	0
Concatenate	(-1, 1408)	0
Dense	(-1, 2)	2818

(표 4) 학습 및 테스트 데이터 분포.

CICIDS 2018	Training set		Testing set		Total
	Benign	Malicious	Benign	Malicious	
Data	560,261 (0.3385)	598,348 (0.3615)	239,739 (0.1448)	256,808 (0.1552)	1,655,156 (1.0000)



(그림 2) 실험 결과.

(표 5) 혼동 행렬.

Confusion Matrix		Actual Class	
		Benign	Malicious
Predicted Class	Benign	234,208 (0.4717)	5,531 (0.0111)
	Malicious	23,734 (0.0478)	233,075 (0.4694)

V. 결론 및 향후 연구

네트워크 기술의 발전을 통해 다양한 디바이스들이 연결되어 네트워크 크기가 커지고, 발생하는 트래픽 양도 많아지면서 공격 사례가 증가하고 있으며 공격 유형 또한 새로워지고 있다. 특히 제로 데이 공격은 기존에 존재하는 공격의 패턴을 통해 탐지하는 규칙 기반 탐지 방식으로는 탐지할 수 없다. 따라서 딥러닝 및 기계 학습을 접목한 이상 탐지 방식 관련 연구가 활발히 진행되고 있다.

본 논문에서는 2차원 데이터를 입력으로 받는 CNN 기반의 모델을 설계하였다. 2개의 컨볼루션 레이어를 통해 연산된 값을 사용하여 완전 연결 레이어를 구성한 후 이진 분류하는 구조이다. 본 논문에서 사용한 데이터 셋인 CICIDS 2018의 경우 약 1,600만 개로 데이터양이 많고 정상 트래픽이 많은 불균형한 데이터이므로 간단한 샘플링을 통해 불균형성을 해소하여 학습과 테스트에 사용하였다. 실험 결과 최고 94.27%의 정확도, 91.05%의 재현율, 98.43%의 정밀도, 94.32%의 F1-score을 달성하는 등 우수한 성능을 보였다. 본 논문에서 제안한 모델을 활용하여 네트워크 공격을 탐지하기 위한 모델을 설계하는 데 적용될 수 있다.

본 논문에서 사용한 데이터 셋은 불균형성을 해소하기 위해 전체 데이터의 일부인 약 160만개 데이터만 사용하여 모델을 학습하고 테스트하였다. 향후 연구에서는 SMOTE, OSS 등 샘플링 기법을 사용하여 보다 많은 데이터를 사용하여 실험할 계획이다. 또한 본 논문에서 제안한 모델이 다른 데이터 셋에서도 좋은 탐지 성능을 보이는지 확인하기 위해 NSL-KDD, UNSW-NB15 등의 데이터 셋을 사용하여 모델을 학습하고 성능을 측정할 계획이다.

ACKNOWLEDGMENT

이 논문은 2020년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임.(NRF-2020R1A2C1012117)

참 고 문 헌

[1] Z. Ahmad, A. S. Khan, C. W. Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: a systematic study of machine learning and deep learning approaches," *Transactions on Emerging Telecommunications Technologies,* Vol. 32, No. 1, pp. 1-29, Jan. 2021.

[2] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network intrusion detection for IoT security based on learning techniques," *IEEE Communications Surveys & Tutorials*, Vol. 23, No.3, pp. 2671-2701, Jan. 2019.

[3] CICIDS 2018 dataset available: https://www.unb.ca/cic/datasets/ids-2018.html, Accessed on 15 Jan. 2022.

[4] KDD Cup 99 dataset available: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html, Accessed on 15 Jan. 2022.

[5] NSL-KDD dataset available: https://github.com/defcom17/NSL_KDD, Accessed on 15 Jan. 2022.

[6] UNSW-NB15 dataset available: https://research.unsw.edu.au/projects/unsw-nb15-dataset, Accessed on 15 Jan. 2022.

[7] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *Proc. of 2009 IEEE Symposium on Computational Intelligence in Security and Defense Applications (CISDA),* pp. 1-6, Ottawa, Canada, July 2009.

[8] J. Y. Kim, J. W. Kim, H. J. Kim, M. S. Shim, and E. J. Choi, "CNN-based network intrusion detection against denial-of-service attacks," *Electronics*, Vol. 9, No. 6, pp. 1-21, June 2020.

[9] K. Jiang, W. Wang, A. Wang, and H. Wu, "Network intrusion detection combined hybrid sampling with deep hierarchical network," *IEEE Access*, Vol 8, pp. 32464-32476, Jan. 2020.

[10] P. Devan, and N. Khare, "An efficient XGBoost-DNN-based classification model for network intrusion detection system," *Neural Computing and Applications*, Vol 32, No. 16, pp. 12499-12514, Jan. 2020.

가상 네트워크 관리를 위한 기계학습 기반 네트워크 공격 및 침입 탐지 시스템 설계

홍지범, 허동녕*, 남석현, 유재형, 홍원기
포항공과대학교, *한동대학교

{hosewq, obiwan96, jhyoo78, jwkhong}@postech.ac.kr, *21931011@handong.edu

A Design of Machine Learning-based Network Attack and Intrusion Detection System for Virtual Network Management

Jibum Hong, Dongnyeong Heo*, Sukhyun Nam, Jae-Hyoung Yoo, James Won-Ki Hong
POSTECH, *Handong Univ.

요 약

네트워크 기술 발전과 이에 따른 다양한 서비스가 출현하면서 트래픽 사용량이 급증하였다. 네트워크의 안정적인 관리를 위해 DoS/DDoS 와 같은 네트워크 공격이나 침입 (intrusion)과 같은 비정상 트래픽을 초기에 탐지하고 대응하는 것은 매우 중요하다. 하지만 트래픽의 증가와 함께 네트워크 공격 방법이 다양해지면서 기존의 룰 (rule) 및 통계 정보 기반의 탐지 방법은 한계를 보이고 있다. 이에 따라 최근에는 기계학습 (machine learning)을 이용한 탐지 방법이 제안되고 있다. 본 논문에서는 지도학습 기반의 딥러닝 모델을 바탕으로 네트워크 공격 및 침입 트래픽을 탐지하는 모델을 제안하고 이를 실제 환경에 적용하기 위한 시스템을 설계한다.

Ⅰ. 서 론

5G 네트워크 및 IoT 기술의 발전은 인터넷에 접근 가능한 단말의 증가와 함께 인터넷 사용에 대한 접근성을 향상시켰다. 이에 따라 네트워크 트래픽 사용량은 지속적으로 증가하게 되었으며, 정상적인 일반 트래픽과 함께 공격이나 침입 등을 목표로 하는 비정상적인 트래픽도 증가하였다.

이러한 비정상적인 트래픽은 DoS/DDoS 와 같은 서비스 거부 공격 (Denial of Service)이나 포트 스캔 (port scan) 등과 같은 다양한 원인에 의해 발생할 수 있으며, 이는 서버 및 네트워크 기능의 정상적인 동작에 심각한 영향을 초래한다. 따라서 서비스 제공업체 및 네트워크 관리자는 비정상적인 트래픽에 대한 보안 정책을 구현하기 위해 네트워크 공격 및 침입에 대한 탐지 기능을 제공해야 한다 [1].

과거에는 사용된 비정상적인 트래픽의 분류 및 탐지 기법들은 표준 포트 번호를 이용한 포트 기반의 탐지 방법이나 IP 패킷의 페이로드에 포함되어 있는 표식 (signature)를 이용하여 트래픽을 분류하였다. 하지만 이러한 기존 방법들은 암호화된 트래픽이나 네트워크 공격 방법이 다양해지면서 비정상적인 트래픽의 탐지에 한계가 있다.

이러한 문제를 해결하기 위해 네트워크 트래픽의 통계 정보를 기반으로 그 특성을 분석하여 비정상적인 트래픽을 탐지하는 방법이 제안되었다. 최근에는 인공지능 기술의 발전과 함께 기계학습 (machine learning)을 이용하여 다양한 네트워크 공격이나 침입 시 발생하는 트래픽의 특성을 학습시켜 이를 이용한 비정상적인 트래픽 탐지에 활용하는 연구가 진행되고 있다.

본 논문에서는 가상 네트워크 관리를 위해 요구되는 기능 중 보안 기능에 초점을 맞추어, 기계학습 방법 중 하나인 지도 학습을 기반으로 네트워크의 공격 및 침입 행위를 탐지하는 모델 및 시스템을 설계한다. 제안하는 지도 학습 모델은 딥러닝 알고리즘인 RNN (Recurrent Neural Network)을 기반으로 Sequential 한 구조를 지닌다. 또한 제안하는 탐지 모델을 실제 네트워크 환경에 적용하기 위한 네트워크 공격 및 침입 탐지 시스템을 설계한다.

Ⅱ. 관련 연구

네트워크 공격 및 침입 트래픽을 탐지에 대한 최근 연구는 대부분 네트워크 트래픽의 통계 정보 바탕으로 이를 분석하거나 기계학습 알고리즘을 학습시켜 도출된 모델을 기반으로 네트워크 공격 및 침입 탐지 시스템을 구현하고 있다 [2].

H. Zhang et. al. [3]은 실시간 네트워크 공격 및 침입 탐지를 위해 data mining 을 통한 flow calculation 과 딥러닝 알고리즘 중 하나인 DBN (Deep Belief Network)을 결합하여 비정상적인 트래픽을 탐지하고, 이후 SVM (Support Vector Machine) 모델을 통해 공격을 분류한다. 해당 모델은 NSL-KDD 및 CICIDS2017 과 같은 네트워크 공격 관련 공개 데이터셋을 이용하여 모델 학습 및 성능 검증을 진행하였다.

다음으로, Y. Fu et. al. [4]는 feature extraction 과 RNN 계열의 딥러닝 모델인 LSTM (Long-Short Term Memory)을 기반으로 탐지 모델을 학습시키고, 네트워크 공격 관련 공개 데이터셋 KDD Cup '99 를 기반으로 모델의 성능을 검증하였다.

이 외에도 SDN/NFV 환경에서 네트워크 공격 및 침입을 탐지하는 연구가 존재한다. L. F. Carvalho et. al. [5]는 SDN/NFV 환경에서 수집되는 네트워크 플로우의 통계 정보를 이용하여 자체적으로 제안한 deviation 계산 알고리즘을 이용하여 DoS 와 포트 스캔 등의 네트워크 공격을 탐지하고, 이를 완화하기 위한 시스템 구조를 제안하였다.

또한 T. A. Tang et. al. [6]은 SDN/NFV 환경에서 OpenFlow 스위치에서 수집되는 트래픽 통계 정보를 바탕으로 DNN (Deep Neural Network)를 활용한 딥러닝 기반의 탐지 모델을 제안하였다. 해당 DNN 모델은 NSL-KDD 데이터셋을 기반으로 학습되었으며, 학습된 모델을 SDN/NFV 환경에 적용하여 네트워크 공격 및 침입 탐지 시스템 구조를 제안하였다.

이러한 네트워크 공격 및 침입 탐지에 대한 연구들은 트래픽 정보 중 네트워크 플로우 (flow)와 관련된 통계 정보를 이용한다. 또한 모델 학습에 있어 네트워크 공격과 관련된 공개 데이터셋을 이용해 데이터를 전처리하고, 학습 및 검증한다는 공통점을 지닌다.

Ⅲ. 기계학습 기반 네트워크 공격 및 침입 탐지 모델 및 시스템 설계

1) Sequential 딥러닝 구조 기반 네트워크 공격 및 침입 탐지 모델: 기존 네트워크 공격 및 침입 탐지 모델은 대부분 data processing 과정에서 feature selection 또는 feature extraction 을 수행한 후 하나의 기계학습 알고리즘을 이용하여 탐지 모델을 학습시킨다. 이에 본 논문에서 제안하는 탐지 모델은 그림 1 과 같은 구조를 지닌다.

네트워크 공격 및 침입 탐지 모델은 Feature mapping, Encoder, Readout, Classifier 4 개 계층으로 구성된다.

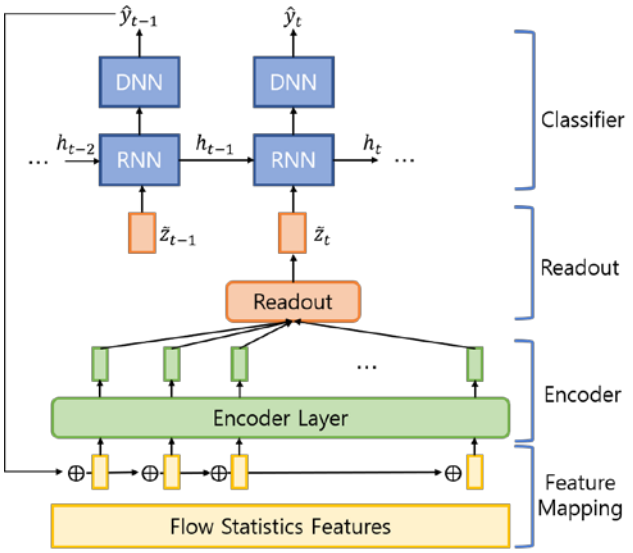


그림 1 Sequential 딥러닝 구조 기반 네트워크 공격 및 침입 탐지 모델

먼저 feature mapping 계층은 활성화 함수 (activation function)가 없는 fully connected layer 로 이루어지며, input vector 를 매핑한다. Input vector 매핑 시 사용되는 데이터는 플로우의 통계 정보를 포함하는 각 feature 로 이루어진다.

Encoder 계층은 전체 데이터를 축소시킨 벡터로 sequential 모델을 이용하여 레이어를 선형으로 구성한다. 이때 사용되는 딥러닝 알고리즘은 RNN 계열의 모델이나 encoder/decoder 구조를 지니는 Transformer [7] 모델을 사용할 수 있다.

다음으로 Readout 계층은 전체 데이터를 축약하는 역할을 수행한다. Encoder 계층에서 RNN 계열의 모델을 사용하는 경우 max, min 과 같은 함수를 통해 일반적으로 많이 사용되는 pooling 방법을 사용하거나, Encoder 계층에서 Transformer 모델을 사용하는 경우 self-attention 을 통해 가중치 합 (weighted sum)을 통해 Encoder 계층에서 들어온 벡터 집합을 축약하여 표현한다. 상기 3 개 계층은 입력값인 플로우 통계 정보를 Classifier 에서 학습할 수 있도록 변환한다.

마지막으로 Classifier 계층은 RNN 과 DNN 으로 구성된다. Classifier 계층은 시간 단계 (t)에 따른 input sequence (z)를 기반으로 hidden state (h)를 출력한다. 그 후 DNN 은 RNN 의 hidden state 를 입력으로 사용하여 탐지 결과 (y)를 출력한다. 이때, 네트워크 트래픽 데이터가 시계열 (time-series) 특징을 지니는 것을 고려하여, 출력된 특정 시점 (t)의 탐지 결과가 다음 시점 (t+1)의 탐지에 활용될 수 있도록 설계한다.

이와 같은 탐지 모델을 바탕으로, 시계열 구조를 지니는 네트워크 트래픽의 통계 정보를 플로우 단위로 수집하고, 이를 모델의 입력값으로 활용한다. 수집되는 플로우 단위 통계 정보를 나타내는 feature 는 특정 플로우의 5 tuple 정보와 함께 duration, count, 트래픽 양, 서버 로그인 횟수 등이 있다. 이후 이러한 플로우 단위 통계 정보를 입력값으로 하여 본 논문에서 제안하는 모델을 학습시키고 네트워크 공격 및 침입 행위에 대한 탐지 결과를 출력한다. 모델의 성능은 상기 설명한 네트워크 공격 및 침입 탐지와 관련된 공개 데이터셋인 KDD '99, NSL-KDD, CICIDS 2017 등을 이용하여 검증할 예정이다.

2) 네트워크 공격 및 침입 탐지 시스템 – NFV 환경 구성 및 모니터링 기능: 그림 1 에서 제안한 Sequential

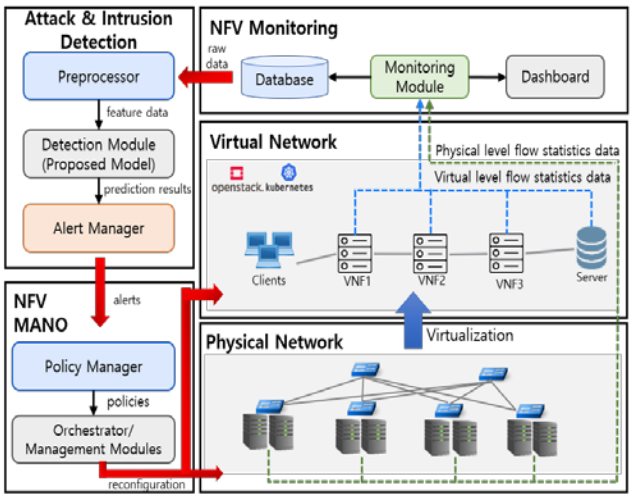


그림 2 기계학습 기반 네트워크 공격 및 침입 탐지 시스템 구조도

딥러닝 구조 기반 네트워크 공격 및 침입 탐지 모델을 기반으로, 실제 NFV 환경에 적용을 위한 네트워크 공격 및 침입 탐지 시스템의 구조는 그림 2 와 같다.

먼저 오픈 아키텍쳐와 같은 상용 하드웨어를 통해 구성된 물리 네트워크 환경에서 OpenStack/Kubernetes 와 같은 Virtual Infrastructure Manager (VIM)을 이용하여 NFV 환경을 구축한다. 이러한 NFV 환경은 인공지능 기술을 기반으로 NFV 환경을 관리하는 플랫폼 개발에 대한 연구 [8]를 기반으로 이루어지며, MEC 환경을 모사한 네트워크 토폴로지로 구성되어 있다.

이와 같은 물리 네트워크 환경을 가상화하여 가상 네트워크에서 VNF (또는 CNF)의 SFC (Service Function Chaining)를 구성하여 서비스를 운용한다. NFV 환경에서 모니터링 기능은 물리 및 가상 서버의 CPU, 메모리와 같은 자원 사용 정보와 네트워크 트래픽 정보, syslog 와 같은 로그 정보를 포함한다.

이때 네트워크 트래픽 정보는 플로우 단위로 수집한 통계 정보를 포함하며, 수집된 데이터는 모니터링 모듈로 전달되어 데이터를 대시보드를 통해 실시간 모니터링 정보를 시각화하여 제공하거나, 데이터베이스에 시계열 형태의 데이터로 저장된다.

3) 기계학습 기반 네트워크 공격 및 침입 탐지 시스템-탐지 및 관리: 구축된 가상 네트워크 환경 및 모니터링 기능을 통해 수집된 플로우 통계 정보는 데이터베이스에 저장된 데이터 (raw data) 형식으로 공격 및 침입 탐지 모듈로 전달된다.

해당 데이터는 전처리기 (preprocessor)를 통해 모듈화된 탐지 모델에 사용하기 위한 형식으로 변환된다. 다음으로, 네트워크 공격 및 침입 탐지 모듈 (Detection Module)은 전처리된 데이터를 입력값으로 하여 탐지 결과를 출력한다. 모듈이 탐지 대상이 되는 플로우를 네트워크 공격 또는 침입 행위로 분류하는 경우, 탐지 결과를 기반으로 Alert Manager 는 네트워크 관리자 혹은 자율 네트워킹 환경에서 NFV 환경의 관리 정책을 세우는 Policy Manager 에게 공격 또는 침입 행위가 발생했음을 알린다.

이후 Policy Manager 는 탐지 결과를 기반으로 공격지 주소에 대한 보안 규칙을 업데이트하거나 서비스 품질 유지를 위한 새로운 관리 정책을 생성하고, 이를 Orchestrator 에게 전달하여 정책을 실제 네트워크에 반영한다. 이 때 Orchestrator 는 필요한 경우 auto-scaling 혹은 migration 과 같은 다른 VNF Lifecycle 관리 모듈들과 연계하여 가상 네트워크를 관리한다. 이를 통해 인공지능 기반의 통합적인 closed-loop automation 을 통한 네트워크 관리의 자동화를 목표로 하는 시스템을 구현하고자 한다.

IV. 결론 및 향후 연구

본 논문에서는 가상 네트워크 관리를 위한 기계학습 기반의 네트워크 공격 및 침입 탐지 모델과 이를 실제 환경에 적용하기 위한 시스템을 설계하였다. 제안하는 탐지 모델은 RNN 을 기반으로 Sequential 한 구조를 지님으로써 기존 단일 모델을 사용한 방법보다 높은 탐지 정확도를 기대할 수 있다. 또한 이를 기반으로 설계된 탐지 시스템은 [8]과 같은 인공지능 기반의 가상 네트워크 관리 플랫폼 구조에 기반하여 설계되어 선제적인 가상 네트워크 관리에 활용이 가능하다.

향후 연구로 제안하는 탐지 모델을 구현하고, 공개 데이터셋을 활용하여 모델의 성능을 검증할 예정이다. 그 후 도출된 모델을 바탕으로 탐지 시스템을 구현하고, 실제 환경에서의 실험을 통해 제안하는 이상 탐지 시스템의 성능을 검증할 예정이다.

ACKNOWLEDGMENT

이 논문은 2022 년도 정부 (과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원 (2018-0-00749, 인공지능 기반 가상 네트워크 관리기술 개발)과 2022 년도 정부 (산업통상자원부)의 재원으로 산업기술평가관리원의 지원을 받아 수행된 연구임 (No.2009633, 초저지연 네트워크 서비스를 위한 SDN 기반 인공지능 관제 시스템 개발).

참 고 문 헌

[1] R. Boutaba et al., "A comprehensive survey on machine learning for networking: evolution applications and research opportunities", in Journal of Internet Services and Applications, vol. 9, issue 1, 2018.

[2] M. Ring, S. Wunderlich, D. Scheuring, D. Landes, A. Hotho, "A survey of network-based intrusion detection data sets", Computers & Security, vol. 86, pp. 147-167, 2019.

[3] H. Zhang, Y. Li, Z. Lv, A. K. Sangaiah and T. Huang, "A real-time and ubiquitous network attack detection based on deep belief network and support vector machine," in IEEE/CAA Journal of Automatica Sinica, vol. 7, no. 3, pp. 790-799, May 2020.

[4] Y. Fu, F. Lou, F. Meng, Z. Tian, H. Zhang and F. Jiang, "An Intelligent Network Attack Detection Method Based on RNN," 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC), pp. 483-489, 2018.

[5] L. F. Carvalho, T. Abrao, L. S. Mendes and M. L. Proenca, "An ecosystem for anomaly detection and mitigation in software-defined networking", Expert Systems with Applications, pp. 121-133, 2018.

[6] T. A. Tang, L. Mhamdi, D. McLernon, SAR Zaidi and M. Ghogho, "Deep learning approach for Network Intrusion Detection in Software Defined Networking", WINCOM, pp. 258-263, 2016.

[7] A. Vaswani, et al., "Attention is All you Need", Advances in neural information processing systems 30, 2017.

[8] S. Lange, et al., "A Network Intelligence Architecture for Efficient VNF Lifecycle Management", IEEE Transactions on Network and Service Management (TNSM), August 2020.

CNN 기반 차량용 이더넷 침입 탐지 시스템의 네트워크 패킷 표현 최적화에 관한 연구

신종훈, 홍충선
경희대학교

{michael, cshong}@khu.ac.kr

Optimizing Representation of Network Packet for Automotive Ethernet Intrusion Detection System using Convolutional Neural Network

Jong Hoon Shin, Choong Seon Hong

Kyung Hee University

요 약

기존의 자동차는 내부 네트워크는 CAN, LIN, FlexRay 와 같은 네트워크로 통신하고 외부와는 극히 제한되거나 제한된 통신 환경을 갖추고 있다. 소비자의 사용 경험과 주행 안전의 향상을 위해 향상된 차량용 네트워크 환경이 필요하다. 이로 인해 외부와 연결하는 기능이 대폭 증가한 차량이 늘고 있다. 기존의 CAN 버스와 같은 네트워크는 대역폭 및 보안이 취약하여 차량용 이더넷이 점차 채택되고 있다. 하지만 기존 이더넷의 보안 취약점으로 인해 차량에 연결된 기기가 공격당했을 때의 악영향이 매우커 보안의 중요성이 증대되고 있다. 다양한 액세스 네트워크로 차량이 연결되므로 차량에 대한 잠재 공격공간이 커지면서 차량의 제한적인 컴퓨팅 능력은 차량 보안을 어렵게 한다. 이에 본 논문은 차의 제한적인 컴퓨팅 능력과 차량의 In-Vehicle Networks 의 부하를 최소화하기 위해 최소한의 정보로 유해 트래픽 탐지가 가능하고 연산량이 작은 CNN 모델에 입력할 수 있는 네트워크 패킷의 전처리 방법과 표현을 제안한다.

Ⅰ. 개 요

최근까지 자동차는 외부와 극히 제한되거나 제한된 통신 환경을 갖추고 있었다. 극히 제안된 환경으로는 키팝, 오디오 스트리밍 또는 제조사와 긴급 통신을 위한 경우뿐이 였다. 이러한 환경에서 자동차의 보안은 상대적으로 다른 전자 부품을 포함한 기기에 비해 미약했다. 하지만 근래의 자동차의 제한된 통신 환경은 빠른 속도로 변하고 있다. Wi-Fi®, V2X 와 같은 여러 네트워크 망으로의 편입은 소비자의 사용 경험과 차량 안전을 여러 서비스를 통해 향상시키고 있다[1].

차량용 이더넷을 활용할 차량 들에서는 네트워크의 물리 계층이 in-vehicle 네트워크로써 활용이 되고, 차량용 이더넷이 기존의 Controller Area Network 나 FlexRay 를 대체한다. 이로써 향상된 네트워크 스루풋을 가지게 되는데 이로써 Advanced Driver Assistance Systems (ADAS)와 같은 기능들을 가능하게 한다[2][8].

차량의 통신 환경의 발전에는 앞서 말한 장점들이 존재하나 또한 보안적 측면에서 공격의 가능성과 공격의 효과를 크게 증가시키기도 하였다. 이러한 상황에서 자동차와 이를 지원하는 인프라의 보안은 더욱 중요해졌고 이는 자동차가 더욱 자동화, 연결될 수 록 더욱 중요해진다. 하지만 차량의 제한된 컴퓨팅 성능은 차량에서의 전통적인 유해 트래픽의 탐지 및 대응을 활용하기 어렵고 또한 이를 새로운 유형에 따라 업데이트하기에 어려움이 있다.

이에 이 논문은 네트워크 패킷을 차량에서도 탐지하고 새로운 탐지 항목을 업데이트 하기 수월하도록 기계학습, 그 중에서도 컴퓨팅 리소스를 적게 쓰는 CNN 레이어를 기반으로 하는 모델에서 사용 가능하면서 네트워크 패킷을 특성이 잘 드러나도록 전처리하는 방법을 소개한다.

이 논문의 제안 사항은 다음과 같다.

1. 네트워크 패킷의 헤더 정보만을 사용하여 네트워크 유해 트래픽 탐지
2. 연산량이 비교적 작은 CNN 모델을 조정하지 않고 이용할 수 있도록 이미지로 변환하고 효과적으로 추론할 수 있도록 하는 전처리 기법
3. 다수의 패킷을 한 번의 추론으로 탐지할 수 있도록 전처리 기법

Ⅱ. 관련 연구

네트워크 침입 탐지는 빈번히 기계 학습으로 시도되어 왔다. 1999 년도에 소개되었던 네트워크 침입 탐지

데이터 셋인 KDD-99 데이터셋만 보더라도 알 수 있다. 전통적인 기계학습, 즉 Support Vector Machine (SVM) [10], Random Forest [11], Adaptive Boosting [12]은 네트워크 침입 탐지 분류를 위하여 쓰였는데 대부분의 모델들은 데이터 분포의 차이로 인한 과적합으로 인한 높은 False Positive Rate (FPR) 점이 개선점으로 있었다.[9]

딥러닝을 이용한 시도로는, RNN, CNN, LSTM 등 여러 모델을 이용한 시도들이 있었다. 여러 시계열 패턴을 주로 보는 RNN, GRU, LSTM 을 이용한 [13]은 KDD-99 의 개선 버전인 NSL-KDD 와 UNSW-NB15 데이터 셋을 이용 하였다. 데이터의 시계열적 패턴을 주요하게 보는 특성을 이용해 탐지모델을 만들었다. 이 모델은 UNSW-NB15 데이터 셋으로 GRU 을 이용하여 64.8%, LSTM 을 이용하여 67.5%의 정확도를 보여주었다. [14]는 2 차원 즉 이미지 분류가 아닌. 1 차원 CNN 레이어를 이용하여 91.2% 의 정확도를 보여주었다.

하지만 제안되었던 논문은 각각 제안한 모델에 입력될 수 있도록 만들어졌고, 모델을 차량이나 컴퓨팅 리소스가 적은 기기에서 쓰이는 모델에 입력되도록 전처리하기에는 기술되어 있지 않거나 직관적이지 못하다. 이에 이 논문에서는 컴퓨팅 리소스가 적은 모델이나, 사용자의 컴퓨팅 리소스에 따라 널리 쓰이는 대부분의 CNN 기반 이미지 분류 모델에 입력할 수 있는 전처리 방법을 제안한다.

III. 제안 사항

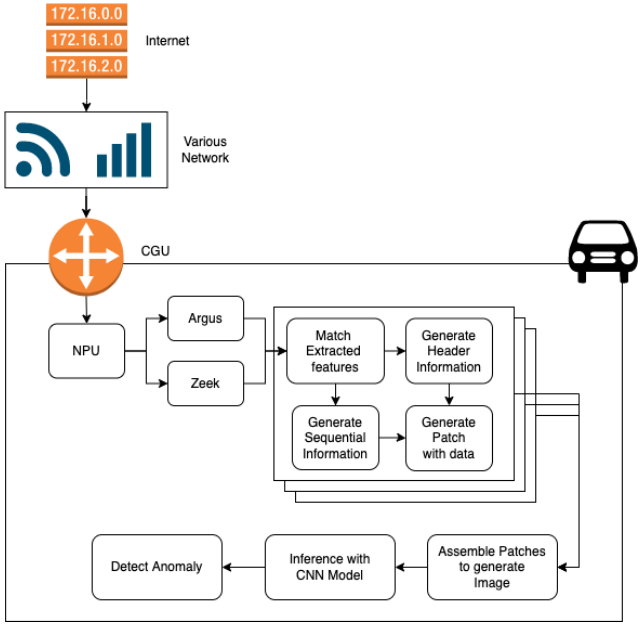


그림 1 제안된 시스템 모델

네트워크로 연결되어 있거나 차량이 바깥과 통신하는 모든 모듈과 네트워크는 공격의 통로가 될 수 있다. 해커들이 차량이 유해 트래픽으로 인한 공격을 할 때 많이 쓰이는 공격의 통로는 클라우드, UWB, 또한 모바일 앱이 있다[1]. 하지만 각각의 모듈과 네트워크 기기에서 각각 유해 트래픽 탐지를 하기보다 중앙 유닛에서 탐지하는 것이 가장 효율적일 것이다. 이에 그림 1 에서 보이듯 본 논문은 차량 네트워크의 중심이 되는 게이트웨이에서 트래픽을 NPU 로 보낸 후 유해 트래픽 탐지를 하고 최소한의 데이터, 즉 패킷만을 이용하여 탐지한다고 가정한다.

이러한 환경에서 중앙의 기계 학습 모델에서 탐지를 할 때 각 패킷의 특성을 최소한의 데이터로 최대한 풍부하게 나타내는 것이 중요하다.

패킷의 헤더에 많은 정보가 포함되어 있다고는 하나, 이에 포함되지 않은 정보들, 특히 시계열적 정보도 유해 트래픽 탐지에 있어 중요하다. TCP 패킷에서 SYN 을 포함한 패킷과 SYN_ACK 를 포함한 패킷의 시간차나, SYN_ACK 와 ACK 를 포함한 패킷의 시간차가 대표적인 예이다. 위의 정보를 이용해서 Fuzzers, DoS 공격 등의 공격 유형을 탐지할 수 있다[3].

각각의 레이어의 프로토콜의 헤더들을 종합해서 표현하고 헤더에 포함되지 않은 시계열적 정보도 포함하여 분류의 특성을 증가시켜 탐지율을 높이고 또한 DoS 와 같이 시계열 정보가 포함돼야만 탐지할 수 있는 공격들도 탐지함으로 탐지 항목의 증가도 있다.

패킷의 헤더와 시계열적 정보를 수집한 후 탐지 모델에 입력할 수 있도록 전처리를 해야 한다. 제안된 시스템 모델에서는 CNN 레이어를 이용하는 모델이 컴퓨팅 리소스도 적고 훈련 및 배포가 용이하기 때문에 CNN 모델에 입력할 수 있는 형식으로 전처리한다. CNN 레이어를 이용하는 모델은 이미지로 입력해야 한다. 이에 제안된 모델에서는 수집된 정보들을 이미지로 전처리한다.

그림 2 에서 표현되듯, 네트워크 패킷이 차량으로 들어왔을 때, 이를 게이트웨이에서 우선 각 레이어의 헤더 정보들만 수집하고 이 정보들 중 패킷을 직접적으로 나타내는 source IP, p ort 주소들과 destination IP, p ort 주소들 같은 정보는 제외하고 정해진 규격에 맞춰 이진수로 표현한다. 직접적인 주소들을 제외하는 이유는 모델 훈련 과정 중에서 과적합을 피하기 위해 직접으로 패킷의 주소를 특정할 수 있는 정보를 제외하였기 때문이다.

이진수로 표현되는 정보들이 최소한의 데이터 사용을 위해 가변적인 형태로 표현되지 않고 정해진 규격에 맞춰서 넣는데, 이는 CNN 모델 구조상 가까운 정보끼리 연관성을 높게 평가하는데(“stationarity of statistics and locality of pixel dependencies”[5]) 하나의 정보가 이미지처럼 만들어지면서 줄 바꿈이 생기면 하나의 정보가 분리되며 거리가 멀어지기에 정보의 표현이 왜곡될 수 있어 정해진 규격을 만들어 각각의 정보가 최대한 분산되지 않게 한다[4][5]. 또한 정해진 규격에 맞춰서 전처리하면서 특성을 표현할 때 사용되는 데이터의 양을 2/3 정도로 감소 하였다.

제외되는 정보, 즉 패킷을 특정할 수 있는 정보들과 일부 시계열적 패턴에 필요한 정보들, Flag 나 패킷의 도착 시간과 같은 정보를 테이블에 저장한다. 이 테이블은 정해진 시간이 지난 정보를 지운다. 이를 통해 2 초 동안의 패킷 수나 정해진 시간동안 SYN 과 같은 Flag 의 비율과 같은 특성을 표현할 수 있다.

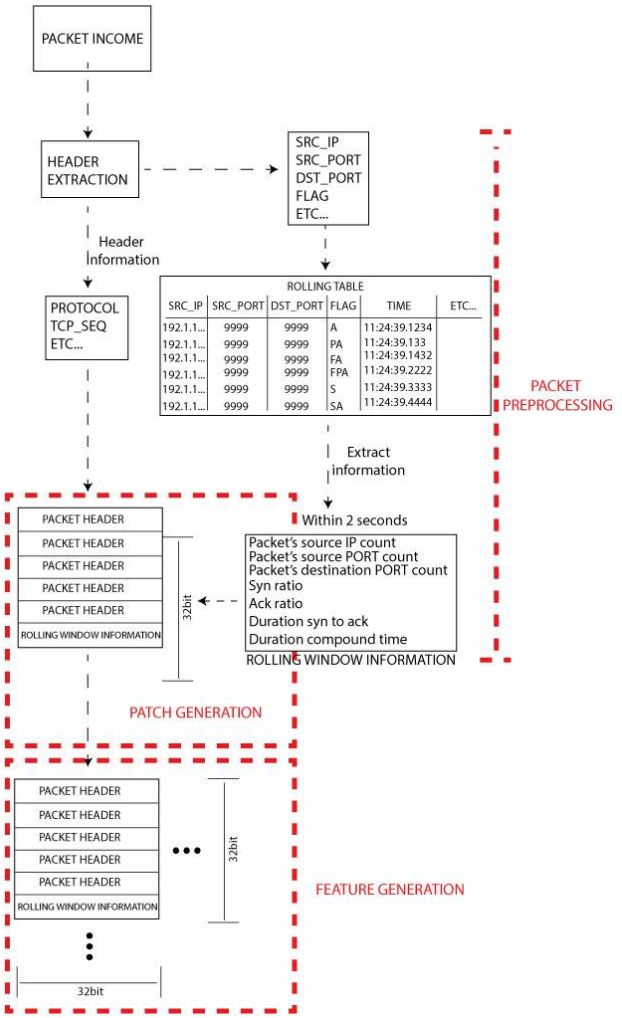


그림 2 전처리 방법의 플로우 차트

이렇게 표현된 정보들, 헤더 정보와 시계열적 패턴의 정보들은 각각의 데이터들이 정규화(식 1)된 이후에 이진수로 표현된다. 이진수로 표현된 정보들은 합쳐져서 하나의 이미지로 만들어진 후 모델에 입력이 된다. 이 두 정보들의 합은 대부분 CNN 모델에 입력되는 데이터의 표준에 가까운 정사각형의 이미지로 만든다.

$$X[i] = \frac{X[i] - X_{\min}}{X_{\max} - X_{min}} \quad (1)$$

한번의 추론에 하나의 정사각형 구조의 이미지로 표현된 한 패킷을 분류하는 것이 정확도는 높을 수 있으나, 많은 패킷이 짧은 시간에 들어올 시에 레이턴시와 일반적으로 정상 패킷이 많은 상황에서 각각의 패킷을 추론하는 것은 비효율적일 것이다. 이에 본 논문은 앞서 말한 전처리 과정을 거친 정사각형 구조의 데이터를 여러 개 쌓은 정사각형 구조의 이미지를 만든다. 이로 인해 한번의 추론에 여러 패킷을 탐지하여 많은 양의 패킷이 들어옴으로 인해 늘어날 추론으로 인한 병목 현상을 줄일 수 있다. 실험에서는 총 49 개의 패킷을 쌓아서 224 x 224 의 규격으로 학습 및 추론하였다.

III. 평가

A. 평가 지표

일반적으로 이상치 탐지의 평가 지표는 정확도,식(2)와 정밀도, 식 (3) 그리고 위양성율(FPR), 식(4)로 평가한다[9].

$$Accuracy(ACC) = \frac{TP + TN}{TP + TN + FP + FN} \quad (2)$$

$$Precision = \frac{TP}{TP + FP} \quad (3)$$

$$FalsePositiveRate = \frac{FP}{TN + FP} \quad (4)$$

B. 데이터 셋

전처리와 모델의 성능은 UNSW-NB15 데이터 셋으로 실험하였다. UNSW-NB15 데이터 셋은 현실적인 네트워크 시나리오와 풋프린트가 낮은 침입의 데이터도 포함한다. 다른 네트워크 침입탐지 데이터셋들(KDD98, KDDCUP99, NSLKDD)은 너무 오래 전에 생성되어 바뀐 네트워크 상황을 잘 반영하지 못하기에 이 데이터 셋으로 실험을 하였다. UNSW-NB15 의 공격 유형은 총 9 개의 유형으로 Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode 그리고 Worms 가 있다[3]. 또한 UNSW-NB15 는 공격 데이터의 불균형이 있는데 이를 완화시키기 위해 오버샘플링을 하였다. 오버샘플링은 데이터 양이 적은 항목의무작위의 데이터 포인트를 무작위로 복제하여 추가함으로 데이터 불균형을 완화하고 모델의 정확도를 높인다. 위의 데이터 셋에서 Worms 공격 유형은 총 173 개의 데이터 포인트가 있는데 총 257,673 개의 데이터 포인트에 비하면 미미하고 이는 0.067%에 불과하다. 오버 샘플링으로 작은 데이터 샘플에서 오는 문제점을 완화시켰다[9]. 실험 결과는 각 공격 유형을 분류하는 것이 아닌, 일반 패킷과 유해 패킷으로 나눠 이진 분류로 실험하였다[3].

각 차량의 사양에 따라 가용할 수 있는 컴퓨팅 리소스나 NPU의 유무가 다를 것이다. 이에 CNN 레이어 기반 모델은 각 차량에 따라 다르게 차용할 수 있다. 입력 형식이 이미지이기에 대부분의 이미지 분류 모델에서 작동한다.

Table 1 모델 별 성능

Model	Acc %	Precision%	FPR %
MobileNet [6]	90.24	96.27	1.96
EfficientNet [7]	90.02	96.10	2.06

컴퓨팅 리소스가 적은 CNN 모델, MobileNet[6]과 EfficientNet[7]으로 이진 이미지 분류로 실험한 결과, MobileNet 은 90.24%의 정확도, 96.27%의 정밀도, 1.96%의 위양성율를 보였다. EfficientNet 은 91.75%의 정확도, 96.10%의 정밀도, 2.06%의 위양성율를 보였다. 각 공격 항목 별 정확도는 Table 2 에 표기하였다.

Table 2 모델에 따른 항목 별 성능

Acc	MobileNet [6]	EfficientNet [7]
Normal %	96.27	96.10
Generic %	99.80	99.83
Exploits %	94.86	94.56
Fuzzers %	35.82	35.08
DoS %	95.81	95.74
Reconnaissance %	99.31	99.14
Analysis %	74.15	74.70
Backdoor %	97.71	97.71
Shellcode %	64.96	59.84
Worms %	93.85	93.85

IV. 결론 & 추후 연구

본 논문에서는 증가하는 연결된 차량의 수와 이로 인해 증가하는 위험성에 대비하기 네트워크에서 유해 트래픽을 적은 컴퓨팅 능력을 사용하여 탐지할 수 있는 CNN 레이어 기반 모델에 입력될 수 있도록 네트워크 패킷의 표현을 최적화하는 전처리 기법을 소개하였다. 제안된 방법은 네트워크 패킷의 헤더의 정보와 이를 시계열 패턴으로 분석한 정보들을 CNN 모델에서 다른 설정 없이 사용할 수 있도록 이미지 형식으로 전처리하였다. 전처리된 패킷을 활용하여 상대적으로 연산량이 적은 학습 모델들에서 다른 미세조정을 하지 않은 상태로 실험하였고 높은 탐지 확률을 보였다. 차량의 컴퓨팅 성능에 따라 차용할 수 있는 모델에 제안된 형식으로 전처리를 한다면 적은 연산량으로 효율적으로 유해 트래픽 탐지를 할 수 있다. 추후 연구에서 패킷 누적 속도의 최적화와 현재 흑백으로 표현되는 이미지를 컬러나 다른 표현 방식으로 탐지율과 정확도를 높이려고 한다.

ACKNOWLEDGMENT

이 논문은 2022 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (2020-0-00364, AI 기반 차량용 통신 기술 향상을 위한 NPU 와 응용 시스템 개발) *Dr. CS Hong is the corresponding author.

참 고 문 헌

[1] K. Matheus and Ko¨nigseder Thomas, Automotive ethernet. Cambridge, United Kingdom: Cambridge University Press, 2021.

[2] S. Jeong, B. Jeon, B. Chung, and H. K. Kim, “Convolutional neural network-based intrusion detection system for AVTP streams in Automotive Ethernet-based networks,” Vehicular Communications, vol. 29, p. 100338, 2021.

[3] N. Moustafa and J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," 2015 Military Communications and Information Systems Conference (MilCIS), 2015, pp. 1-6, doi: 10.1109/MilCIS.2015.7348942.

[4] Y. Lecun, L. Bottou, Y. Bengio, and P. Haffner, “Gradient-based learning applied to document recognition,” Proceedings of the IEEE, vol. 86, no. 11, pp. 2278-2324, 1998.

[5] A. Krizhevsky, I. Sutskever, and G. E. Hinton, “ImageNet classification with deep convolutional Neural Networks,” Communications of the ACM, vol. 60, no. 6, pp. 84-90, 2017.

[6] A. G. Howard, M. Zhu, B. Chen, D. Kalenichenko, W. Wang,T. Weyand, M. Andreetto, and H. Adam. Mobilenets: Efficient convolutional neural networks for mobile vision applications. arXiv:1704.04861, 2017.

[7] Mingxing Tan and Quoc V Le. Efficientnet: Rethinking model scaling for convolutional neural networks. arXiv preprint arXiv:1905.11946, 2019.

[8] P. Hank, S. Muller, O. Vermesan, J. Van Den Keybus,” Automotive Ethernet: In-vehicle Networking and Smart Mobility”

[9] J. Sinha and M. Manollas, “Efficient deep CNN-BILSTM model for network intrusion detection,” Proceedings of the 2020 3rd International Conference on Artificial Intelligence and Pattern Recognition, 2020.

[10] I. Ahmad, M. Basheri, M. J. Iqbal, and A. Rahim, “Performance comparison of Support Vector Machine, Random Forest, and extreme learning machine for intrusion detection,” IEEE Access, vol. 6, pp. 33789-33795, 2018.

[11] Jiong Zhang, M. Zulkernine, and A. Haque, “Random-forests-based network intrusion detection systems,” IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), vol. 38, no. 5, pp. 649-659, 2008.

[12] W. Hu, J. Gao, Y. Wang, O. Wu, and S. Maybank, "Online Adaboost-based parameterized methods for dynamic distributed network intrusion detection," IEEE Transactions on Cybernetics, vol. 44, no. 1, pp. 66-82, 2014.

[13] R. Vinayakumar, K. P. Soman, and P. Poornachandran, "Evaluation of recurrent neural network and its variants for Intrusion Detection System (IDS)," International Journal of Information System Modeling and Design, vol. 8, no. 3, pp. 43-63, 2017.

[14] R. U. Khan, X. Zhang, M. Alazab, and R. Kumar, "An improved convolutional neural network model for intrusion detection in networks," 2019 Cybersecurity and Cyberforensics Conference (CCC), 2019.

딥러닝 기반 익스플로잇 킷 탐지 모델의 입력 데이터 설계에 관한 연구

김보선, 최정우, 이민성, 백의준, 김명섭

고려대학교

{boseon12, choigoya97, min0764, pb1069, tmskim}@korea.ac.kr

A Study on the Input Data Design of DL-based Exploit Kit Detection Model

Boseon Kim, Jeong-Woo Choi, Min-Seong Lee, Ui-jun Baek, Myung-Sup Kim

Korea University

요 약

인터넷 기술이 발전하며 다방면으로 사용자들에게 여러 이점을 가져와 긍정적인 효과를 제공하지만, 인터넷 사용량이 급속도로 증가함에 따라 웹 페이지를 통한 감염 피해 사례도 늘어나고 있다. 인터넷의 보안 취약성을 악용한 사례 중 하나는 익스플로잇 킷(EK)이다. EK 탐지 방법 중 블랙리스트 기반 탐지 방법은 정보가 변경 혹은 위장된 경우와 알려지지 않은 신종 EK에 대해 취약하여 공격에 대처하지 못하거나 오탐할 확률이 매우 높다. 그래서 우리는 기존 연구에 주로 사용되는 Raw 데이터 셋과 Raw 데이터에서 블랙리스트 기반 식별 정보를 제거한 데이터 셋을 사용하여 실험하였고, Raw 데이터 셋을 사용한 실험은 높은 정확도와 작은 편차를 보였지만 Raw 데이터에서 블랙리스트 기반 식별 정보를 제거한 데이터 셋을 사용한 실험에서는 낮은 정확도와 큰 편차를 보였다. 실험 결과를 통해 블랙리스트 기반 식별 정보가 없이는 오탐률이 증가할 가능성이 있다는 것을 알 수 있다. 우리는 블랙리스트 기반 식별 정보 없이 EK를 탐지할 수 있는 방법에 대한 연구 필요성을 강조한다.

Ⅰ. 서 론

인터넷 기술이 발전하며, 다방면으로 사용자들에게 여러 이점을 가져와 긍정적인 효과를 제공하고 있다. 그러나 인터넷 사용량이 급속도로 증가함에 따라 웹 페이지를 통한 감염 피해 사례도 늘어나고 있다. 인터넷의 개방적인 네트워크 특성과 프로토콜의 보안 취약성을 악용한 사례 중 하나는 익스플로잇 킷(Exploit Kit)이다. EK는 사용자 시스템 속 프로그램의 취약점을 이용해 광고, 이메일 첨부 파일, 웹 페이지 접속 등으로 악성 코드를 유포하는 자동화된 공격 도구이다[1]. 국내 감염 피해를 입힌 주요 EK로는 블랙홀(Blackhole), 앵글러(Angler), 리그(Rig), 뉴트리노(Neutrino) 등이 있다. EK 탐지에 관한 연구가 지속되고 있고, 대표적인 방법으로는 특정 패턴이 지속적으로 사용되는 것을 감지하여 미리 정의된 시그니처를 검사하는 방법(블랙리스트 기반 탐지)이 있다. 그러나 최근 EK는 도메인 생성 알고리즘(Domain Generation Algorithm)과 고도화된 난독 기술, 백신을 우회하는 기능 등을 업데이트하여 IP나 헤더 정보를 변경하거나 호스트 위장 가능성이 존재한다. 도메인 생성 알고리즘은 수많은 도메인 주소를 동적으로 생성하는 알고리즘으로 공격 차단을 우회하는 방법이다. 사용자가 광고 배너를 눌렀을 때, 수백 개의 리다이렉션을 통해 실제 광고 페이지가 아닌 EK 랜딩 페이지로 접속하게 되고 랜딩 페이지의 URI는 계속 변경되며 패턴을 도출하기 어려워져 블랙리스트 기반 탐지로는 EK를 탐지하기에 어려움이 존재한다. 또한 블랙리스트 기반 탐지를 통해 EK를 탐지할 경우, 알려지지 않은 신종 EK에 대해 취약하여 공격에 대응하지 못하거나 탐지하지 못할 확률이 매우 높다. 따라서 블랙리스트 기반의 식별 정보를 사용하지 않는 EK 탐지 모델이 필요하다.

본 논문은 2020년도 산업통상자원부 및 한국산업기술평가관리원(KEIT) 연구비 지원에 의한 연구 (No. 20008902, IT비용 최소화를 위한 5채널 탐지기술 기반 SaaS SW Management Platform(SMP) 개발)이고, 2021년도 교육부의 재원으로 한국연구재단의 지원을 받아 수행된 지자체-대학 협력기반 지역혁신 사업의 결과 (2021RIS-004)임

우리는 정상 트래픽과 비정상 트래픽(EK)의 분류 모델이 블랙리스트 기반으로 EK 탐지를 하는지 알고자, 기존 연구에 주로 사용되는 Raw 데이터와 Raw 데이터에서 블랙리스트 기반 식별 정보를 제거한 데이터를 사용하여 실험을 진행한다. 두 실험 결과를 비교 및 분석하고자 한다.

Ⅱ. 본론

본 장에서는 정상 트래픽과 비정상 트래픽 분류 실험 과정을 설명한다.

A. 데이터 수집

실험에 사용된 데이터는 직접 수집한 응용 트래픽(정상 트래픽)과 멀웨어 감염과 관련된 EK 트래픽(비정상 트래픽)이며, 자세한 내용은 표 1과 같다[2].

표 1 데이터 셋 정보

프로토콜	분류 대상	이름	플로우	
			개수	%
HTTP	Normal (0)	E-mail	1876	49
		Kakaotalk		
		Chrome		
	Abnormal (1)	Styx-EK	1961	51
		Neutrino-EK		
		Gondad-EK		
		Sibhost-EK		
		Sweet-Orange-EK		
		Blackhole-EK		
		DotkaChef-EK		
		Fiesta-EK		
		Nuclear-EK		
		Angler-EK		
		Rig-EK		
		FlashPack-EK		
		Null-Hole-EK		
		Zemot-EK		

표 2 입력 데이터 정보 및 실험 결과

번호	제거 식별 정보		학습		테스트		차이 (학습-테스트 정확도)
	계층	필드	정확도	편차	정확도	편차	
#1	-	-	99.98	0.04	99.42	0.16	0.56
#2	IP	ip	99.92	0.04	99.10	0.15	0.82
#3	TCP	port	99.95	0.07	99.01	0.23	0.94
#4	Ethernet	ethernet	99.75	0.11	97.76	0.27	1.99
#5	HTTP	host	99.99	0.03	99.22	0.22	0.77
#6	HTTP	location	99.97	0.05	99.12	0.26	0.85
#7	HTTP	server	99.97	0.05	99.12	0.23	0.85
#8	HTTP	user-agent	99.91	0.04	98.87	0.20	1.04
#9	HTTP	referer	99.96	0.05	99.02	0.25	0.94
#10	HTTP	get/post	99.98	0.04	99.07	0.23	0.91
#11	HTTP	date	99.97	0.05	99.02	0.20	0.95
#12	HTTP	accept	99.98	0.04	99.07	0.20	0.91
#13	HTTP	accept_language	99.96	0.05	99.07	0.35	0.89
#14	HTTP	#5~13	99.88	0.07	98.82	0.26	1.06
#15	IP, TCP, Ethernet, HTTP	#2~13	99.74	0.11	97.73	0.29	2.01

B. 데이터 전처리

수집한 Pcap 파일을 JSON 파일로 변환하고 플로우 단위의 데이터로 저장한다. 플로우마다 크기가 다르기 때문에 플로우의 1~3번째 패킷을 추출하고, 부족할 경우 패딩 처리를 하여 동일한 크기의 이미지 형태로 변환한다.

C. 실험

본 연구에서는 2D CNN을 사용하여 정상 트래픽과 비정상 트래픽을 분류하였다. 정상 트래픽과 비정상 트래픽을 섞어 만든 데이터 셋 중 50%는 학습용 데이터로 사용하였고, 나머지 50%의 데이터 셋은 테스트용 데이터로 사용하였다. 과 적합을 방지하기 위해 EarlyStopping이라는 콜백 함수를 사용하여 적절한 시점에 학습을 조기 종료하도록 하였다.

실험은 총 15가지로 구성되어 있으며, 데이터 셋에 포함된 식별 정보에 따라 각각 실험을 진행하였다. 실험 결과는 표 2에 나타내었다. 각 실험은 10번 반복하였고, 학습 정확도와 테스트 정확도는 최대 정확도를 평균 낸 값이다. #1은 Raw 데이터 셋의 분류 실험 결과이고, #2부터 #13은 정상 트래픽과 비정상 트래픽을 학습할 때, 블랙리스트 기반으로 학습될 가능성이 있는 식별 정보를 Raw 데이터에서 각각 제거한 결과이다. 예시로 #2는 Raw 데이터에서 IP 계층의 ip 정보를 제거한 데이터 셋의 실험 결과이며, #3은 Raw 데이터에서 TCP 계층의 port 정보를 제거한 데이터 셋의 실험 결과이다. 비정상 트래픽의 경우, 가상 환경에서 데이터 셋이 수집되었기 때문에 #4는 Raw 데이터에서 ethernet 정보를 제거한 실험 결과이다. #5부터 #13은 Raw 데이터에서 HTTP 계층의 host, location, server, user-agent, referer, get/post, date, accept, accept_language를 각각 제외한 데이터 셋의 실험 결과이다. #14와 #15는 블랙리스트 기반 식별 정보를 조합하여 제거하여 실험하였다. #14는 Raw 데이터에서 HTTP 계층의 9가지 정보(#5~#13)를 제거한 실험 결과이고, #15는 Raw 데이터에서 블랙리스트 기반 모든 식별 정보(#2~#13)를 제외한 실험 결과이다.

실험 결과, 트래픽 분류에 주로 사용되는 Raw 데이터 셋을 사용한 실험(#1)이 높은 정확도와 작은 편차를 보이는 것을 알 수 있다. 또한 Raw 데이터 셋에서 블랙리스트 기반 식별 정보를 모두 제거한 실험(#15)은 비교적 테스트 정확도가 낮고 편차가 크며 학습 정확도와 테스트 정확도의 차이가 큰 것을 알 수 있다. #1과 #15의 실험 결과를 통해 해당 모델은 블랙리스트 기반의 분류 모델을 만들었을 가능성이 크다. Raw 데이터 셋을 사용한 #1의 경우 호스트 정보를 위장하거나 알려지지 않은 신종 공격에 대해 취약하며 우리의 가정대로 분류 모델이 해당 식별 정보를 사용하여 EK를 탐지한 경우라면 #15는 #1에 비해 오탐률이 증가할 가능성이 있다. 호스트 정보가 지속적으로 변경되거나 위장하는 상황, 신종 공격을 대비하여 위장 데이터 셋의 위험 가능성을 낮추고자 블랙리스트 기반 식별 정보를 제거한 실험(#15)은 정확도가 낮게 나옴을 알 수 있고, 기존 연구 방법인 Raw 데이터 셋을 사용한 실험(#1)은 블랙리스트 기반으로 학습을 진행하였음을 알 수 있다.

Ⅲ. 결론

우리는 EK가 지속적으로 업데이트되어 호스트 정보를 변경하거나 위장하여 블랙리스트 기반 탐지 모델이 EK를 탐지하기 어려워졌고 알려지지 않은 신종 EK에 대해 대처하지 못하고 오탐할 수 있다는 가정에 기반하여 실험을 진행하였다. 본 논문은 Raw 데이터 셋과 Raw 데이터에서 블랙리스트 기반 식별 정보를 제거한 데이터 셋을 이용하여 15가지 실험을 진행하였다. Raw 데이터 셋을 사용한 실험 결과는 99.42%의 높은 분류 정확도와 작은 편차를 보였고, Raw 데이터에서 블랙리스트 기반 식별 정보를 제거한 데이터 셋을 사용한 실험 결과는 비교적 낮은 분류 정확도와 큰 편차를 보였다. 이를 통해 블랙리스트 기반 식별 정보가 없이는 오탐률이 3.9배 증가함을 알 수 있었고, Raw 데이터 셋을 사용할 경우 해당 모델은 블랙리스트 기반의 탐지 모델을 만들 가능성이 크다는 것을 알 수 있었다. 이는 호스트 정보를 변경하거나 위장한 EK를 탐지하지 못하며 신종 EK를 탐지하지 못할 가능성이 크다.

우리는 EK를 비롯한 다양한 악성 트래픽 데이터 셋을 추가로 수집하고 블랙리스트 기반 학습에 사용될 수 있는 식별 정보를 제거한 정상 트래픽 및 비정상 트래픽을 통계 특징 기반 머신러닝 또는 CNN 기반 딥러닝을 통해 강인한 EK 탐지 모델을 구축하는 연구를 수행할 계획이다.

참 고 문 헌

[1] QIN, Yan, et al. An exploit kits detection approach based on http message graph. IEEE Transactions on Information Forensics and Security, 2021, 16: 3387-3400.

[2] Malware-Traffic-Analysis.net[Website]. (https://www.malware-traffic-analysis.net/).

Rule 기반 트래픽 분석을 통한 사용자 행위 탐지 시스템 설계

박지태, 이민성, 김보선, 신창의, 김명섭

고려대학교

{pjj5846, min0764, boseon12, realmine, tmskim}@korea.ac.kr

A Design of User Behavior Detection System through Rule-based Traffic Analysis

Jee-Tae Park, Min-Seong Lee, Boseon Kim, Chang-Yui Shin, Myung-Sup Kim

Korea Univ.

요 약

최근 다양한 응용 서비스가 발생하고 있으며, 특히 네트워크 기술의 발전에 따라 기존의 설치 형태의 응용 서비스뿐만 아니라 구독 형태의 응용 서비스(SaaS)의 사용량이 증가하고 있다. 구독 형태의 응용 서비스는 체계적으로 관리 할 수 있으며, 단체가 사용하기 편리하지만, 실제 사용자보다 더 많은 인원의 라이선스를 구독 할 경우, 불필요한 지출이 발생 할 수 있다. 따라서 SaaS 응용 서비스를 대상으로 다양한 연구가 수행되고 있으며, 그 중에서 가장 널리 알려진 분석 방법은 페이로드 시그니처를 활용한 방법이다. 하지만 페이로드 시그니처를 활용한 분석 방법은, 각 SW마다 정의되는 시그니처가 다르기 때문에 SW 별로 분석 시스템을 따로 만들어야하며, 분석 대상 SaaS SW 수가 많아 질 경우 상당히 비효율적이다. 따라서 본 논문에서는 기존 방법의 문제점을 해결하기 위하여 Rule 기반 사용자 행위 탐지 방법을 제안한다. 먼저 SaaS 서비스를 대상으로 사용자 행위에 대해 정의하고, 제안하는 방법의 시스템 구조와 정의한 Rule 구조에 대해 설명하고 논문을 마친다.

Ⅰ. 서 론

최근 네트워크 기술의 발전에 따라 설치 형태의 응용 서비스와 함께 구독 형태의 응용 서비스(SaaS)의 사용량이 증가하고 있다. SaaS 응용 서비스는 클라우드 기반 소프트웨어 제공 모델로 개인, 혹은 특정 기업 및 단체에서 사용 인원, 기간, 사용 라이선스에 따라 구매하여 사용하며, 기간이 만료 될 경우, 신문 구독처럼 기간을 연장하거나 폐지 할 수 있는 구독 형태로 서비스가 제공된다. SaaS 서비스는 점차적으로 사용이 증가하고 있으며, 기존에 설치 형태의 응용 서비스도 구독 형태의 응용 서비스로 전환되고 있는 추세이다. 가장 대표적으로 널리 알려진 SaaS 서비스는 Office 365, Adobe Creative Cloud가 있으며, 필요에 따라 사용을 조정 할 수 있기 때문에 많은 기업 및 단체에서 사용하고 있다[1-2]. 또한 기업 내에서 사용하는 비율과 필요한 서비스에 따라 적절한 금액만을 지불하여 효율적인 자산 관리도 할 수 있다. 하지만 반대로 실제로 서비스를 사용하는 비율에 대한 모니터링이 제대로 이루어지지 않는다면 불필요한 지출이 발생할 수 있다. 따라서 SaaS 응용 서비스와 사용량에 대한 정확한 모니터링이 필요하며, 특히, 기업 내 사용자의 사용 행위에 대한 탐지를 통해 실제 사용량과 구입한 라이선스를 비교하여 불필요한 지출을 확인 할 수 있다.

이러한 추세에 따라 SaaS 응용 서비스에 대해 다양한 연구가 수행되어 왔으며, 가장 널리 알려진 방법은 페이로드 시그니처를 활용하여 사용자 행위 탐지 방법이 있다[1]. SaaS 응용 서비스는 기본적으로 SSL/TLS 기반의 암호화 트래픽을 사용하기 때문에 암호화 된 페이로드 전체 내용 대신 SNI(Server Name Indication)을 사용하며, 각각의 SW 별로 공통으로 도출되는 SNI 정보를 시그니처로 정의 한다. 하지만 기본적으로 SaaS SW 별로 도출되는 SNI 정보가 다르기 때문에, 각 SW 별로 정의된 탐지 시그니처는 달라진다. 따라서 각 SW 별로 탐지 시스템과 알고리즘에 따라 매번 새로운 탐지 시스템을 구축해야하기 때문에 비효율적이다. 따라서 본 논문에서는 이러한 비효율적인 문제를 해결하기 위해 기존의 방법 대신 SaaS 서비스 대상으로 Rule 기반의 사용자 행위 탐지 방법을 제안한다.

본 논문의 구성은 본 장의 서론에 이어 2장 관련 연구에서 기존에 수행된 rule 기반의 분석 방법인 Snort Rule에 대해 설명한다. 3장 본론에서 제안하는 Rule 기반의 사용자 행위 탐지 방법에 대해 설명하며, 4장에서 결론 및 향후 연구에 대해 기술한 후 마친다.

Ⅱ. 관련 연구

Rule 기반의 분석 방법은 정의 된 특정 규칙을 활용하여 트래픽을 분석하는 방법으로, 주로 IDS(Intrusion Detection System)에서 Snort Rule이 사용된다. 정의 된 규칙을 사용하여 대응되는 패킷을 탐지하고, 탐지 된 패킷에 대하여 정의 된 규칙대로 행동(Action)을 수행한다[3-4]. 규칙은 패킷 단위로 적용되며, 패킷의 헤더 및 통계, 페이로드 정보 등을 주로 사용한다. Snort Rule의 구조에 대한 예시는 표 1에 나타나있으며, Header, Body(Option)로 구성되어 있다. Header는 대상 패킷을 판단하는 기준을 명시하며, body는 패킷을 처리하는 규칙을 나타낸다.

표 1 Snort Rule 구조 예시

Action	Prot.	SRC IP	SRC Port	->	DST IP	DST Port	Option
alert	tcp	any	any	->	any	any	...

본 논문은 2020년도 산업통상자원부 및 한국산업기술평가관리원(KEIT) 연구비 지원에 의한 연구 (No. 20008902, IT비용 최소화를 위한 5채널 탐지기술 기반 SaaS SW Management Platform(SMP) 개발) 이며, 2021년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2021S1A5C2A03097574).

Snort Rule 기반의 분석 방법은 규칙을 정의하기 위해 분석 대상 트래픽을 수집하여 해당 트래픽에서만 발견되는 공통 특징을 우선적으로 찾아야 한다. 이 때, 공통 특징을 찾으려면 많은 양의 대상 트래픽을 수집하고, 분석해야하기 때문에 많은 시간이 걸리며, 발견된 공통 특징에 따라 정확도가 달라진다.

Ⅲ. 본론

본 논문에서는 SaaS SW에 대한 사용자 행위 탐지를 목적으로 한다. 사용자 행위는 분석 대상 SW 별로 공통으로 발생하는 행위로 SW 시작, 로그인, SW 종료, 로그아웃으로 구성되며, 그림 1에 나타나있다. 사용자의 관점에서 각각의 행위는 서로 연관되어 있다. 예를 들어 SW 시작이 수행되어야 로그인, SW 종료와 같은 다른 행위가 발생 할 수 있으며, 로그인이 발생해야 로그아웃 행위가 발생 할 수 있다. 이러한 행위 간의 관계는 정확하게 사용자 행위 탐지 시 중요하기 때문에, 제안하는 방법에서는 행위 간의 관계를 Rule로 정의 하였다.



그림 1 사용자 행위 정의

제안하는 방법은 네트워크 패킷을 확인하고 정의 된 규칙에 의하여 탐지되는 패킷일 경우 정의 된 규칙대로 처리한다는 점에서 Snort Rule과 유사하다. 기존의 시그니처 기반 분석 시스템과 Rule 기반의 분석 시스템에 대한 구조는 그림 2에 나타나 있다. 시그니처 기반의 탐지 시스템은 SW 별로 시그니처와 알고리즘이 다르기 때문에 SW 별로 별개의 분석 프로그램이 필요하지만, Rule 기반의 분석 시스템의 경우 여러 개의 분석 프로그램 대신 각 SW 별로 Rule만 정의 하면 쉽고 간편하게 적용 가능하다.

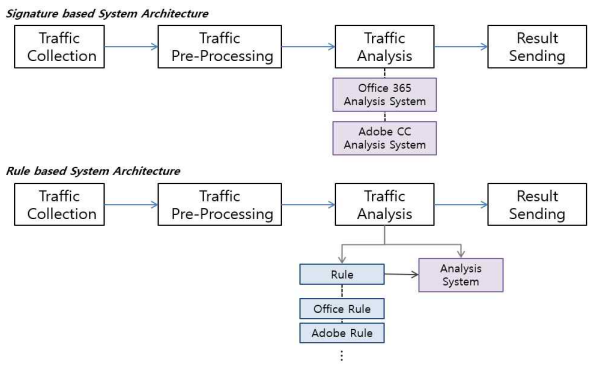


그림 2 시그니처, Rule 기반 사용자 행위 탐지 시스템 구조

본 논문에서 제안하는 방법에서 정의한 Rule은 Snort Rule의 구조와 다른 구조를 지니며, 표 2에 나타나 있다. Snort Rule은 패킷 단위로 규칙을 정의 하지만, 제안하는 방법에서는 플로우, 패킷 단위로 규칙을 정의한다. 이 때, 사용되는 Rule은 총 9가지로 구성되며, 플로우 단위에서 5가지, 패킷 단위에서 3가지, 기타 1가지로 구성된다. 플로우 단위에서의 Client IP, Port, Protocol, Server IP, Port는 플로우의 5-tuples 정보를 나타낸다.

패킷 단위에서의 방향성(Direction)은 플로우 내에서 확인 할 패킷의 방향을 나타내며, 패킷의 방향에 따라 Client to Server (C->S), Server to Client (S->C)로 구성된다. Packet Number는 확인 할 패킷이 몇 번째 패킷인지 나타내며, SNI는 확인 할 패킷에서 존재하는 String 정보를 나타낸다. Behavior는 사용 행위 간의 관계를 고려하여 대상 행동이 발생하기 위해 이전에 발생해야 하는 행동을 나타낸다. 예를 들어, 로그인 행위를 탐지 할 경우, Behavior는 SW 시작으로 정의된다.

표 2 정의 된 Rule 예시

단위	정보	Description	Example
플로우	Client IP	클라이언트 IP	any
	Client Port	클라이언트 포트	any
	Protocol	프로토콜	tcp
	Server IP	서버 IP	13.107.6.156
	Server Port	서버 포트	443
패킷	Direction	플로우 내 패킷 방향	C->S
	Packet Number	확인 할 패킷 번호	4
	SNI	SNI 정보	www.office.com
기타	Behavior	이전 발생 행위	None

Ⅳ. 결론 및 향후 연구

최근 SaaS 서비스의 사용이 증가하고 있으며, 기업에서는 불필요한 지출을 줄이기 위해 SaaS 서비스에 대한 정확한 모니터링이 필요하며, 이를 위해 실제 사용자의 정확한 행위 탐지가 필요하다. 가장 널리 알려진 SaaS 서비스 사용자 행위 탐지 방법은 페이로드 시그니처를 활용한 방법으로, 높은 정확도로 사용자 행위를 탐지 할 수 있지만, SW 별로 포함하는 SNI 정보가 다르기 때문에 SW 별로 별개의 분석 프로그램을 만들어야 한다. 점차적으로 증가하는 SaaS SW 종류를 감안하면 이는 매우 비효율적이며, 분석 프로그램이 많아질수록 과부하가 걸릴 가능성이 높아진다.

따라서 본 논문에서는 기존의 문제점을 해결하기 위해 Rule 기반의 사용자 행위 탐지 방법과 탐지에 사용되는 새로운 Rule 포맷을 제안한다. 제안하는 방법은 기존 방법과 다르게 하나의 분석 프로그램에서 각 SW 별로 정의 된 Rule을 읽고, 수집 된 패킷에 대하여 Rule에서 정의한 절차를 거친 후, 최종적으로 사용자 행위를 탐지하게 된다.

향후 연구로 Office 365의 전체 행위를 대상으로 Rule 기반 사용자 행위 탐지 시스템을 구현 할 예정이다. 또한, Adobe Creative Cloud와 같은 다른 SaaS SW를 대상으로도 Rule을 정의 할 예정이다.

참 고 문 헌

[1] 박준상, 박진완, 윤성호, 오영성, 김명섭. "응용 레벨 트래픽 분류를 위한 시그니쳐 생성 시스템 및 검증 네트워크의 개발." 한국정보처리학회 학술대회논문집 16(1) pp. 1288-1291, 2009.

[2] Dalmazo, Bruno L., J. P. Vilela, and Marilia Curado. "Performance analysis of network traffic predictors in the cloud." Journal of Network and Systems Management 25(2) pp. 290-320, 2017.

[3] 심규석, 윤성호, 이수강, 김성민, 정우석, 김명섭. "네트워크 트래픽 분석을 위한 Snort Content 규칙 자동 생성." 한국통신학회논문지 40(4) pp. 666-677, 2015

[4] A. Garg and P. Maheshwari, "Performance analysis of Snort-based Intrusion Detection System," 2016 3rd International Conference on Advanced Computing and Communication Systems (ICACCS), 2016, pp. 1-5,

BERT 기반 VM 고장 예측 기법 연구

남석현, 유재형, 홍원기
포항공과대학교 컴퓨터공학과

{obiwan96, jhyoo78, jwkhong}@postech.ac.kr

A Study on the VM Failure Prediction based on BERT

Sukhyun Nam, Jae-Hyoung Yoo, James Won-Ki Hong
Department of Computer Science and Engineering, POSTECH

요 약

5G 시대가 도래하면서 네트워크 사업자는 급변하는 요구사항에 맞춰 서비스를 제공하는 것이 요구되고 있다. 이로 인해 소프트웨어 정의 네트워킹과 네트워크 기능 가상화 기술 등이 제안되면서, 가상 머신에서 동작하는 소프트웨어 기반의 가상 네트워크 기능을 구현하는 방식으로 네트워크 요구사항에 대응하고 있다. 이러한 환경에서 가상 머신의 고장은 네트워크 단절을 일으킬 수 있기 때문에 고장이 발생하기 전에 미리 대응하도록 하는 것이 중요하다. 이를 위해 본 연구에서는 가상 머신의 로그 메시지를 이용하여 고장을 예측하는 기법을 제안한다. 제안하는 모델은 자연 언어 처리에서 문맥을 파악하여 임베딩을 생성하는 BERT 를 기반으로 각 로그 메시지를 임베딩으로 변환하여 기계학습의 입력으로 사용한다. 제안하는 모델의 성능 검증을 위하여 OpenStack 기반의 환경에서 수집한 데이터로 실험을 진행하였으며, 기존의 워드 임베딩 기반의 선행 연구에 비해 더 높은 성능을 보임을 확인하였다.

Ⅰ. 서 론

5G 시대에 본격적으로 접어들면서 네트워크 사업자는 급변하는 요구사항에 맞춰 서비스를 제공하는 것이 요구되고 있다. 하지만 소프트웨어 정의 네트워킹(Software-Defined Networking)과 네트워크 기능 가상화 (Network Function Virtualization, NFV) 등의 기술이 제안되면서 변화하는 서비스 요구에 빠르게 대응할 수 있게 되었으며, CAPEX/OPEX 를 절감시키게 되는 등 네트워크 관리의 판도가 바뀌었다. NFV 환경에서는 각 네트워크 기능을 가상 머신(Virtual Machine, VM) 상에서 동작하는 가상 네트워크 기능(Virtualized Network Function, VNF)의 형태로 제공하기 때문에 VNF 및 VM 의 관리가 매우 중요하다. 특히, VM 에 이상 상태나 고장이 발생하게 되면, 해당 VM 에서 동작하는 VNF 를 사용할 수 없게 되고 서비스 단절이 일어나므로 이를 사전에 예측하고, 대응하는 기술의 개발은 필수적이다.

전통적으로, 네트워크 장치의 고장 관리는 네트워크 장비에서 실시간으로 비정형적으로 생성되는 로그 메시지를 기반으로 이루어졌다. 로그는 장비의 상태를 가장 잘 나타내는 데이터 중 하나이지만, 시스템 개발 단계에서 로그 분석자의 편의를 고려하여 설계하는 시스템은 매우 드물며 대부분의 시스템은 체계적이지 않고 자동으로 분석하기 힘든 로그를 출력한다. 이 때문에, 컴퓨팅 장비의 로그를 자동으로 분석하고 이를 기반으로 고장이나 이상 상태를 예측, 탐지하기 위한 연구가 일부 진행되고 있지만[1-3], 여전히 매우 어려운 문제로 남아 있다.

기계 학습의 발전으로 기존에 해결하기 힘들었던 다양한 문제를 해결할 수 있게 되었으며, 이는 네트워크 관리 분야도 마찬가지이다. 기계 학습 기법 중 하나인 강화 학습 기법을 적용하여 동적인 네트워크 환경에서 최적의 서비스 응답시간을 제공하는 SFC (Service Function Chain) 구성 방법에 대한 연구[4]나, 기계 학습으로 서버의 장애를 예측 하여 VNF 를 live migration 하는 방법에 대한 연구가 존재한다[5].

로그 분석도 마찬가지로 기계 학습을 적용시킬 수 있으며, 특히 자연 언어 처리 (Natural Language Processing, NLP)에서 사용하는 기법들을 적용할 수 있다. 본 저자들의 선행연구[6]는 자연 언어 처리 분야에서 사용하는 단어를 단어의 의미를 담은 수치 벡터로 변환하는 워드 임베딩(Word Embedding)[7] 기법을 기반으로 로그 데이터를 수치 행렬로 변환시켜 기계 학습의 입력으로 사용하였다. 하지만 해당 연구는 사전에 훈련된 워드 임베딩을 기반으로 각 단어를 수치 벡터로 변환하기 때문에, 사전 학습에서 출현 빈도가 낮았던 단어에 대해서는 의미 있는 벡터로 변환하지 못하는 한계가 존재한다. 특히, 에러와 관련된 로그는 일반 상황 로그에서 사용하지 않는 단어를 포함할 확률이 높다. 최근, 자연 언어 처리 분야에서는 이러한 한계점을 해결하기 위해 문장 내에서 단어의 문맥을 파악하여 단어 별 벡터를 생성하는 기법인 언어 모델(language model)을 활용한다. 특히, 2018 년에

구글이 공개한 BERT (Bidirectional Encoder Representations from Transformers) [8]는 대량의 말뭉치로 사전 학습된 언어 모델로서, 레이블이 없는 방대한 데이터로 사전 훈련된 모델이지만, 해결하고자 하는 태스크에 맞게 추가 학습을 함으로써 기존의 모델들 보다 더 높은 성능을 보이고 있다.

본 논문에서는 SDN/NFV 환경에서 각 VNF 를 동작시키는 VM 의 고장 예측을 위한 기법을 제안한다. 제안하는 기법은 BERT 를 기반으로 VM 의 로그를 임베딩으로 변화시킨 후 합성 곱 신경망(Convolutional Neural Network, CNN)의 입력으로 사용하여 일정 시간 뒤에 VM 에 고장이 발생할지 예측한다. 제안하는 기법은 VM 의 로그를 자동으로 분석하여 고장 발생을 암시하는 비정상적인 로그 패턴이 발생하였을 때 고장을 성공적으로 예측하는 것을 목표로 한다.

Ⅱ. 관련 연구

자연 언어 처리 문제에서는 단어를 기계 학습의 입력으로 사용하기 위해서 단어의 의미를 고려한 숫자 벡터(vector)로 변환하여 사용하며, 이를 임베딩(embedding)이라 한다. 기존에는 Word2Vec [9]과 같이 대량의 말뭉치를 기반으로 사전 훈련된(pre-trained) 단어 임베딩을 사용하였다. 하지만 워드 임베딩 방법론은 사전 훈련 이후에는 임베딩을 변화시키지 못하기 때문에 사전 훈련용 말뭉치에 편향된 결과를 가진다. 이를 개선하기 위해서 사전 훈련 이후에도 훈련 단계에서 문맥을 파악하여 같은 단어일지라도 다른 임베딩을 출력하는 언어 모델이 제안되었다. 그 중, BERT [8]는 2018 년에 구글이 공개한 사전 훈련된 언어 모델이다. BERT 는 NLP 11 개 태스크에서 state-of-the-art 를 기록하여 가장 영향력 있는 언어 모델로 평가된다. BERT 는 시퀀스-투-시퀀스(sequence-to-sequence, seq2seq) 모델 중 하나인 Transformer [10]에서 인코더(Encoder)만 사용하여 설계되었으며, 해결하려는 태스크에 따라 파라미터 재조정을 위한 추가 훈련 과정인 파인 튜닝(Fine-tuning)을 진행함으로써 전혀 다른 태스크들에서 높은 성능을 달성할 수 있는 것으로 보고되고 있다.

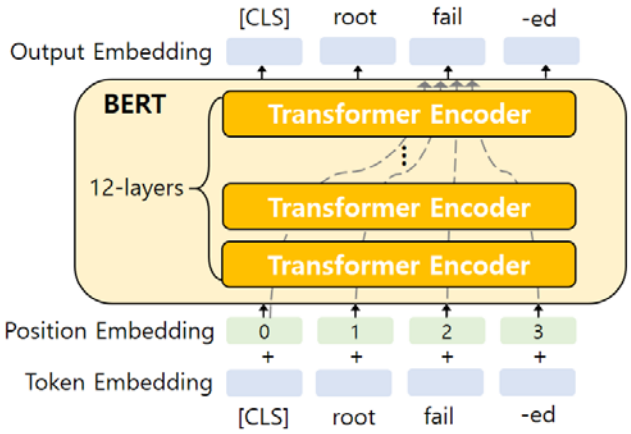


그림 1 BERT-Base 모델 동작 구조

BERT 는 단어를 더 작은 sub-word 로 쪼개어 토큰으로 사용하며, 각 토큰 별 임베딩을 생성해내는 모델이다. BERT 는 서로 다른 태스크에서 성능을 높이기 위해 두 가지 기법을 사용한다. 첫째로, BERT 는 Position embedding 을 사용하는데, 이는 문장 내에서 각 토큰의 위치를 나타내는 벡터를 생성하도록 학습된 임베딩 층이다. 입력 층에서 토큰 임베딩 층에 Position 임베딩을 합쳐 사용하여 학습과정에서 모든 토큰의 위치 정보가 함께 사용되며, 문장의 문맥을 반영한 임베딩을 생성하도록 학습할 수 있다. 둘째로, BERT 는 문장 앞에 [CLS] 라는 특별한 토큰을 추가하여서 학습시킨다. 이는 문장의 시작을 나타내는 토큰이며, 각 출력 임베딩이 문장 전체의 토큰을 기반으로 학습하는 특징으로 인해 [CLS]의 출력 임베딩이 문장의 특성을 나타내는 임베딩으로서 활용할 수 있게 한다.

구글에서 사전학습하여 공개한 BERT 모델은 BERT-Base 와 BERT-Large 가 있으며, 본 연구에서는 BERT-Base 모델을 파인 튜닝하여 활용하였다. 그림 1 은 BERT-Base 사전 학습 모델의 동작 구조를 나타낸다. 해당 모델은 12 개의 Transformer 인코더 층을 포함하며, 각 인코더는 768 차원의 은닉 층(hidden layer)을 갖고 있어 출력 임베딩 또한 768 차원의 벡터가 된다.

선행연구[2]와 [6]은 각각 시뮬레이션 환경에서 로그 메시지 기반의 네트워크 에러 메시지 예측 및 VM 고장 예측 연구이다. 두 연구 모두 로그를 벡터로 변환함에 있어서 단어 임베딩을 활용하였으며, 단어 임베딩을 CNN 의 입력으로 사용하여 일정 시간 뒤에 에러 혹은 고장이 발생할지를 예측하였다. 앞서 언급한 단어 임베딩 기반 연구의 한계로 인해 해당 연구들은 높은 성능을 보이지는 못하였다. 그 외에도 선행연구 [3]와 같이 로그를 벡터로 변환하지 않고 특정 패턴을 찾아내어 이를 토대로 정의한 로그 키(log key)의 발생 유무를 기반으로 이상 상태를 탐지하는 연구 또한 존재한다. 하지만 이러한 기법은 사용하는 시스템이 변화하면 새로 패턴을 분석하고 로그 키를 찾아내야 하는 확장성의 문제가 존재하기 때문에 단어 임베딩이나 언어 모델 기반 방법론에 비해 선호되지 않는다.

Ⅲ. 설계 및 검증

본 논문에서 제안하는 BERT 기반 VM 고장 예측 기법은 NFV 환경에서 VNF 를 동작시키는 VM 들로부터 실시간으로 로그를 수집하여 고장 예측에 활용한다. 고장 예측을 위해 BERT-Base 모델의 출력 임베딩을 입력으로 받아서 일정 시간 뒤의 고장 여부를 학습하는 CNN 을 활용한다.

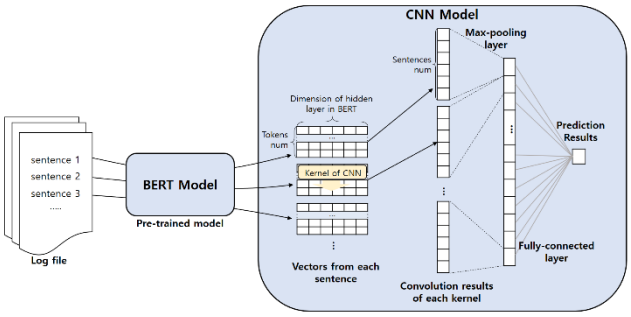


그림 2 BERT 기반 VM 고장 예측 모델 구조

그림 2 는 VM 고장 예측을 위한 BERT 및 CNN 모델의 구조를 나타낸다. BERT 모델로서 사전 훈련된 BERT-Base 모델을 사용하지만 BERT 모델 전체를 파인 튜닝하여 사용한다. VM 고장 예측 모델의 학습 과정에서 역전파(backpropagation)가 BERT 모델에까지 전달되며 전체 하이퍼 파라미터가 수정되어 해결하고자 하는 태스크에 적합한 모델로 학습된다. BERT 모델은

로그의 각 단어를 sub-word 로 tokenization 한 후, 각 토큰에 대해 임베딩 벡터를 생성한다. 해당 벡터의 차원은 BERT-Base 모델에서 사용한 인코더의 은닉층의 차원과 같으며, 768 차원이다. 일반적인 문장 분류 문제에서는 BERT 의 첫 토큰인 [CLS] 토큰 위치의 출력 임베딩을 문장 벡터로서 사용하지만, 본 연구에서는 입력 벡터에서 중요한 데이터를 추출하는데 특화된 CNN 을 활용하기 때문에 각 토큰의 출력 임베딩을 concatenate 하여 사용한다.

CNN 은 BERT 모델의 출력 임베딩을 입력으로 받아 일정 시간 뒤의 고장 발생 여부를 예측한다. 합성 곱 층에서는 커널(kernel)이 임베딩을 이동하며 합성 곱 연산을 하는데, 각 벡터는 하나의 토큰을 의미하므로 커널은 벡터의 크기(768) 와 커널 크기로 이루어진 2 차원 형태의 커널을 사용하며, 벡터 크기만큼 stride 하여 하나의 벡터에서 정보를 나누어 추출하지 않도록 한다. 커널 크기로는 3, 4, 5 를 사용하였으며, 같은 크기의 커널을 100 개씩 활용하였다. 합성 곱 층에서는 활성화 함수(Activation function)로 ReLU (Rectified Linear Unit)를 사용한다. 합성 곱 층의 결과로 커널의 개수만큼의 벡터가 생성되는데, 각 벡터는 max-pooling 층을 통해 최대값만 남도록 한다. Pooling 층을 거치면 커널의 수(3,4,5 각각 100 개씩 300)만큼의 값을 가진 벡터가 생성된다.

Pooling 층의 결과는 완전 연결 층(Fully-Connected layer)을 통해 하나의 값을 출력하도록 한다. 완전 연결 층은 하나의 값을 출력하도록 하기 위해 활성 함수로서 Sigmoid 를 이용한다. 생성된 값은 0~1 사이의 값으로, 1 에 가까울수록 고장이 발생할 확률이 높은 것을 나타내며, 임계 값인 0.5 를 넘으면 고장을 의미한다. 이를 학습시키기 위해서 학습 과정에서 고장 상태에서는 1 이, 정상 상태에서는 0 이 태깅된 로그 데이터를 사용하며, 고장 직전의 상태를 나타내는 로그도 학습시키기 위해 고장 상태보다 이전의 로그들은 고장 전 상태(pre-failure state)를 나타내는 고장 전 상태 값(pre-failure value)을 태깅하였다. 선행연구[6]에서 5 분 이후의 고장을 예측하기 위해서 고장 발생 전 3 분간 0.65 를 고장 전 태깅에 활용하는 것이 가장 성능이 높은 것을 확인하였기 때문에, 본 연구에서도 해당 값을 활용하였다. 또한, 학습에 사용하는 데이터가 0~1 사이의 값도 포함하고 있기 때문에 이를 학습하기 위해 KL-Divergence 를 기반으로 수식(1)과 같은 loss 값을 정의하였다.

$$\text{loss} = y_{\text{true}} \times \log\frac{y_{true}}{y_{pred}} \times w + (1 - y_{true}) \times \log\frac{1-y_{true}}{1-y_{pred}} \quad (1)$$

y_{true} 는 실제 값이며, y_{pred} 는 예측 값, w 는 데이터의 불균형성을 해결하기 위한 class weight 로서, 고장 데이터 대비 정상 데이터 수의 비율을 나타낸다. 제안하는 모델은 학습 과정에서 CNN 모델과 BERT 모델에 대한 파인 튜닝이 함께 진행되며, BERT 또한 각 파라미터를 수정하게 되고, 그 결과 로그데이터로부터 일정 시간 뒤의 고장 여부를 예측할 수 있다.

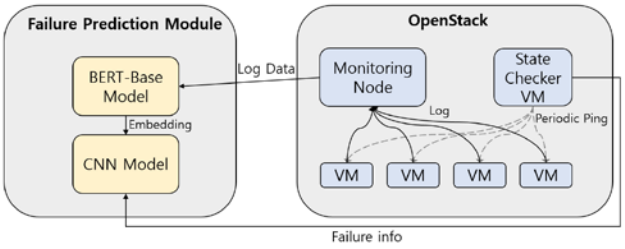


그림 3 고장 예측 성능 평가 실험 환경

제안하는 VM 고장 예측 기법의 성능 평가를 위해 그림 3 과 같이 OpenStack 기반의 실험 환경을 구축하였다. 실험 환경은 다수의 VNF 를 동작시키는 VM 들로 구성된 NFV 환경으로 이루어져있으며, 모니터링 노드(Monitoring node)가 각 VM 으로부터 로그 데이터를 수집한다. 또한 각 VM 에 고장이 발생하는지를 기록하기 위해 상태 확인 VM (State Checker VM)이 각 VM 으로 주기적으로 ping 메시지를 보내 고장 여부를 확인한다. 고장 예측 모듈(Failure prediction module)은 모니터링 노드로부터 일정 시간 동안의 로그 데이터를, 상태 확인 VM 으로부터 그로부터 일정 시간 뒤의 고장 여부를 받아서 학습시킬 수 있다. 이 때, 선행연구[6]에서 5 분간의 로그 데이터를 입력으로 하여 5 분 뒤의 고장 예측을 하였을 때 가장 성능이 높게 나왔기 때문에 본 실험에서도 해당 데이터 생성 환경을 활용하였다.

OpenStack 기반의 실험 환경에서 수집한 데이터로 제안하는 모델에 대한 검증 실험을 진행하였다. 실험 과정에서 빠른 학습을 위해 학습률(learning rate) 스케줄러(scheduler)를 활용하여 학습률을 변화시켰으며, 본 실험에서는 Cosine annealing 스케줄러를 이용하였다. 그림 4 는 실험 결과를 나타내며, 학습 epoch 에 따른 학습 손실 값(training loss, 파랑 선, 좌측 눈금)과 테스트 데이터에 대한 F1 score 값(빨강 선, 우측 눈금)을 나타낸다. 100 epoch 간의 실험 결과, 모델은 실험 데이터에 대해 0.76 의 F1 score 예측 성능을 나타내었다. 그래프에서 손실 값이 0 보다 낮아지는 형태를 보이는데, 이는 새로 정의한 손실 함수의 특성으로 인한 것으로, 고장 전 상태를 나타내는 0.65 보다 모델의 예측 값이 더 높아지면 해당 손실 함수는 음수를 반환한다. 하지만, 모델은 손실 값이 0 보다 낮아도 더 낮아지도록 학습하기 때문에 모델의 성능에는 문제가 없기는 하나, 이로 인한 과적합(over-fitting)의 가능성이 존재한다.

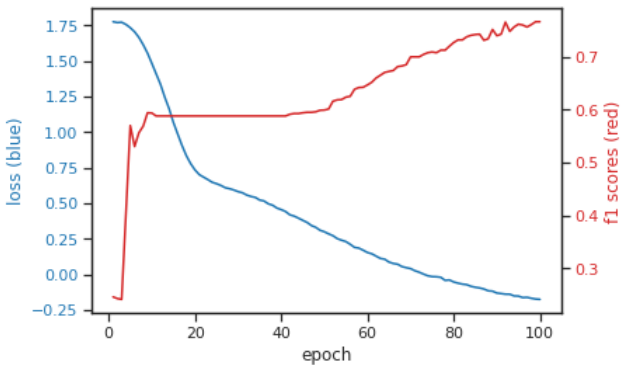


그림 4 BERT 기반 VM 고장 예측 모델 실험 결과

BERT 기반의 고장 예측 모델의 적합성 확인을 위해 본 저자들의 선행연구[6]에서 제안한 워드 임베딩 기반의 VM 고장 예측 모델과의 성능 비교 실험을 진행하였다. 해당 모델은 로그를 입력으로 받아 CNN 모델을 활용하는 것은 동일하나, 입력 임베딩으로서 Word2Vec 워드 임베딩 모델로부터 생성된 단어 임베딩을 사용하는 모델을 사용한다. 그림 5 는 실험 결과로서, 두 가지 방법으로 생성한 모델을 같은 데이터로 학습하였을 때 학습 손실 값의 변화를 나타낸다. 해당 그래프에서 알 수 있듯이 BERT 기반 모델의 손실 값이 훨씬 빠르게 감소한다. 학습 결과, 워드 임베딩을 이용한 모델은 테스트 데이터에 대해 F1 score 0.59 의 성능을 나타내어 BERT 기반 모델이 0.17 높은 성능을 나타내었다. 이를 통해 BERT 기반의 고장 예측 모델이 기존 모델보다 더 우수함을 알 수 있다.

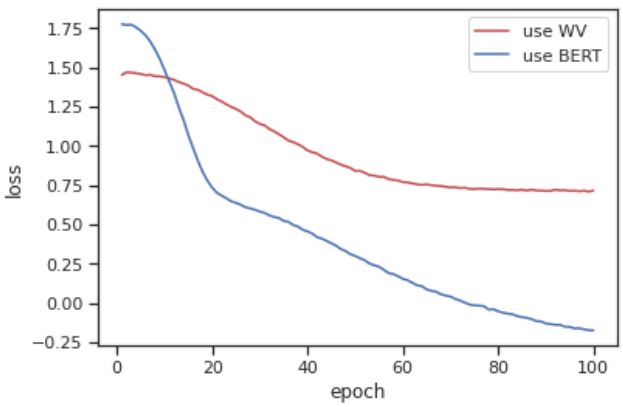


그림 5 선행연구[6]과의 성능 비교 실험 결과

IV. 결론 및 향후 연구

본 논문에서는 NFV 환경에서 VNF 를 동작시키는 VM 의 고장을 예측하기 위한 기법을 제안하였다. 제안하는 기법은 VM 들로부터 로그를 입력 받고, 이를 제안하는 BERT-CNN 모델의 입력으로 사용하여 일정 시간 뒤의 고장 여부를 예측하는 모델을 활용한다. 또한 성능 검증 실험을 통해서 기존의 워드 임베딩 기반의 모델에 비해 성능이 높은 것을 확인하였다.

본 연구는 다양한 향후 연구 방향을 가진다. 우선 제안하는 모델이 사용하는 손실 함수는 고장 전 상태를 학습하기 위해 손실 함수를 새로 설계하여 사용하였는데, 해당 손실 함수는 음수도 출력하는 문제점이 있어 수정이 필요하다. 또한, 고장 예측 연구의 가장 큰 문제점인 데이터 생성의 어려움으로 인한 성능의 한계점이 존재한다. 따라서, 데이터를 생성하기 힘든 분야에서 일부 데이터를 기반으로 가짜 데이터를 생성하며 적대적 학습을 진행하는 GAN (Generative Adversarial Networks) 을 기반으로 모델의 성능을 더 높이는 연구를 수행할 계획이다. 마지막으로, 실제 시스템에 활용할 수 있을 성능이 나온 후에 이를 통해 예측한 고장 발생 여부를 기반으로 VM migration 여부를 결정하는 시스템을 개발할 계획이다.

ACKNOWLEDGMENT

이 논문은 2022 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원(2018-0-00749, 인공지능 기반 가상 네트워크 관리기술 개발)과 2022 년도 정부(산업통상자원부)의 재원으로 산업기술평가관리원의 지원을 받아 수행된 연구임 (No.2009633, 초저지연 네트워크 서비스를 위한 SDN 기반 인공지능 관제 시스템 개발).

참 고 문 헌

[1] S. He, J. Zhu, P. He and M. R. Lyu, "Experience Report: System Log Analysis for Anomaly Detection," 2016 IEEE 27th International Symposium on Software Reliability Engineering (ISSRE), Ottawa, ON, Canada, 2016, pp. 207-218.

[2] W. Ji, S. Duan, R. Chen, S. Wang and Q. Ling, "A CNN-based network failure prediction method with logs," 2018 Chinese Control And Decision Conference (CCDC), 2018, pp. 4087-4090.

[3] M. Du, F. Li, G. Zheng, and V. Srikumar, “Deeplog: Anomaly detection and diagnosis from system logs through deep learning,” In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 1285-1298.

[4] 이도영, 유재형, 홍원기, "Deep Q-Networks 기반 Service Function Chaining 구성 연구", KNOM Conference 2021, On-line KNOM Conference Venue, Korea, April 30, 2021, pp. 13-16.

[5] 정세연, 유재형, 홍원기, "머신러닝을 이용한 서버 장애 예측 기반 VNF Live Migration", KNOM Conference 2021, On-line KNOM Conference Venue, Korea, April 30, 2021, pp. 9-12.

[6] S. Nam, J. Hong, J. Yoo, J. W. Hong, "Virtual Machine Failure Prediction using Log Analysis", The 22nd Asia-Pacific Network Operations and Management Symposium (APNOMS 2021), Tainan, Taiwan, Sep. 8-10, 2021.

[7] T. Mikolov, I. Sutskever, K. Chen, G. Corrado and J. Dean, "Distributed Representations of Words and Phrases and their Compositionality", In Advances on Neural Information Processing Systems, 2013.

[8] J. Devlin, M. Chang, K. Lee and K. Toutanova, “Bert: Pre-training of deep bidirectional transformers for language understanding,” arXiv preprint arXiv:1810.04805. (2018).

[9] Google, “word2vec,” 2013. [Online]. Available: https://code.google.com/archive/p/word2vec/ .

[10] A. Vaswani, *et al.* “Attention is all you need,” In Advances in Neural Information Processing Systems, 2017, pp. 6000-6010.