사이버 보안을 위한 양자 인공지능 연구 동향

김현지*, 김원웅*, 강예준*, 임세진*, 서화정*†

*한성대학교 (대학원생)

*† 한성대학교 (교수)

Trends in Quantum Neural Network for Cyber Security

Hyun-ji Kim*, Won-woong Kim*, Yea-jun Kang*, Se-jin Kim*, Hwa-jeong Seo*†

*Hansung University(Graduate student)

*† Hansung University(Professor)

요 약

인공지능 기술이 발달한 이후로 다양한 학습 기술, 네트워크, 가속기 그리고 실제 어플리케이션 등이 개발되고 있다. 최근에는 양자 컴퓨터가 개발됨에 따라 양자컴퓨터 상에서 동작 가능한 양자 신경망이 관심을 받고 있다. 그러나 현재의 양자 컴퓨터는 중간 규모의 양자컴퓨터이므로 오류 보정을 위한 자원이 부족하여 연산 오류가 발생하게 된다. 따라서 현재까지는 양자 신경망을 단독으로 사용하는 것이 아닌 고전 신경망과 결합하여 사용하는 하이브리드 방식의 신경망이 더 적절하다. 본 논문에서는 사이버 보안에서 양자 신경망을 사용한 연구들을 소개한다. 향후, 더 큰 규모의 양자 컴퓨터가 개발될 경우, 오류 정정이 가능한 양자 신경망을 구성할 필요가 있으며, 더 풍부한 자원을 사용하여 사이버 보안을 위한 추가적인 요소들을 학습에 반영할 수 있을 것으로 생각된다.

I. 서론

인공지능 기술이 발달하면서 그에 관련된 다양한 학습 기술, 신경망 모델, 가속기, 실제 어플리케이션 등이 개발되고 있다. 최근에는 양자 컴퓨터가 개발되면서 이를 잘 활용할 수 있는 분야인 양자 신경망이 관심을 받고 있으며, IBM, Amazon, Microsoft 등에서 양자 신경망과 관련한 다양한 라이브러리 및 개발 환경에 대한 연구가 진행되고 있다. 현재의 양자컴퓨터는 중간 규모의 양자컴퓨터이므로 오류보정을 위한 자원이 부족하기 때문에 계산 오류가 빈번히 발생할 수 있다[1]. 현재 양자 컴퓨터로 동작 가능한 양자 신경망은 양자회로만 사용할 경우, 10-qubit을 초과하기 힘들고 MNIST 데이터 셋을 사용한 이진 분류 및 다중분류가 정도가 가능한 상황이다. 그에 비해 양자 신경망과 고전 신경망을 결합한 하이브리드 신경망의 경우, 더 많은 큐비트를 사용할 수 있고, 성능 면에서 더 좋은 결과를 보이며, 다양한 어플리케이션들이 제안되었다.

II. 관련 연구

2.1 인공 신경망(Artificial Neural Networks)

인공 신경망은 생물학의 신경망을 기반으로 한 통계학적 학습 알고리즘이다. 인공 신경망은 여러 개의 레이어로 구성되어 있으며, 각 레이어는 여러 개의 뉴런으로 구성되어있다. 각 뉴런은 자신과 관련된 이전 레이어의 뉴런들의 값과 가중치에 대한 가중합을 수행한 후, 해당 값을 비선형 함수인 활성화 함수에 입력하여 최종 값을 계산한다. 이렇게 계산된 값은 다시 다음 레이어의 뉴런의 값을 결정하기 위해 사용된다. 각 레이어에서 이러한 연산을 반복적으로 수행한 후, 최종 레이어에서 출력한 값과 실제 정답 레이블을 손실함수에 입력하여 실제 값과의 차이를 표현하는 손실을 계산한다. 이후, 해당 값을 기반으로 역전파 과정을 거쳐 네트워크 내부의 가중치들을 갱신한다. 이를 통해 입력데이터에 대한 예측과 실제 답과의 손실을 최소화하도록 하여, 데이터에 대한 올바른 예측이 가능한 인공신경망으로 훈련시킨

다. 이후, 가중치가 고정된 상태인 훈련된 신경망을 사용하여 학습에 사용되지 않은 데이터들에 대한 추론을 수행한다. 또한, 데이터의 특징이나 작업에 따라 학습에 더 효과적인 신경망이 존재하며, 대표적으로 이미지 데이터 학습을 위한 convolutional nerual networks(CNN), 시계열 데이터 학습을 위한 recurrent neural networks(RNN), 데이터 생성형 신경망인 generative adversarial networks(GAN) 등이 있다.

2.2 양자 인공 신경망(Quantum Neural Networks, QNN)

양자 인공 신경망은 인공신경망의 구조 및 기능을 양자 컴퓨터 상에서 수행 가능한 양자회로로 구성한 것이다[2]. 즉, 양자 신경망은 양자역학 현상(얽힘과 중첩)을 활용한 인공지능 기술이다. 양자 신경망은 양자 컴퓨터의 큐비트와 양자 게이트로 구성된다. 따라서 고전 데이터 자체에 대한 연산이 불가능하므로, 고전 데이터를 양자 데이터로 인코딩한 후 양자 상태의 데이터(매개변수화 된 양자 회로)를 학습해야 한다. 양자 회로의 매개변수는 입력 데이터를 인코딩한 값으로 설정되며, 각 큐비트는 양자 게이트를 통과하면서 값이 변경된다. 마지막으로 큐비트의 상태를 관찰하면 중첩 상태의 큐비트가 하나의 값으로 결정된다. 결정된 값을 통해 고전 신경망과 같이 손실을 계산하고, 해당 값을 기반으로 회로 내부의 매개변수를 갱신한다. 양자 신경망은 이러한 과정을 반복하면서 학습을 수행한다. 앞서 설명하였듯이 NISQ(Noisy Intermediate Scale Quantum) 시대의 양자 프로세서는 오류정정이 어려우므로 현재의 양자 신경망은 기존의 보조 프로세서와 함께 작동해야 효과적이다. 즉, 고전 신경망과 양자 신경망을 결합한 형태인 hybrid quantum-classical neural networks[3]가 성능 면에서 더욱 안정적이다. 현재 양자 인공지능은 고전 신경망과 비슷하게 quantum support vector machine(QSVM)[4], quantum convolutional neural networks(QCNN)[5], quantum recurrent neural networks(QRNN)[6], quantum generative adversarial networks(QGAN)[7] 등 다양한 모델이 개발되었다. 또한 기존의 tensorflow, pytorch 등의 프레임워크와 양자 컴퓨팅 플랫폼인 qiskit, amazon braket, Q#, cirq 등과 결합하여 프로그래밍이 가능하다.

III. 사이버 보안을 위한 양자 인공지능 연구 동향

현재 큰 규모의 양자컴퓨터가 개발되지는 않았지만, 양자 신경망이 개발됨에 따라 사이버 보안을 위해 양자 인공지능을 활용하는 연구들이 존재한다. 표 1은 연구 동향을 정리한 표이며, 해당 표에서 볼 수 있듯이 많은 수의 큐비트를 사용할 수 없으며, 대부분 하이브리드 방식의 양자 신경망을 사용한다. 이는 현재 양자컴퓨터의 자원 제약으로 인한 것이며, 향후 더 많은 큐비트 및 양자회로가 동작 가능하다면 다양한 데이터 특징을 반영할 수 있기 때문에 현재보다 더 높은 성능의 양자 신경망을 구성할 수 있을 것으로 보인다.

표 1. 사이버 보안을 위한 양자 신경망 연구 동향(S : simulator, Q : real quantum hardware)

	Architecture	Qubit	Library	Device
[8]	Hybrid	4 or 9	Penny lane	S (penny lane)
[9]	Hybrid	5 (Max)	Penny lane	Q (IBM)
[10]	Hybrid, QNN-only	4	Tensor flow-quantum	S (Cirq)
[11]	QSVM, Hybrid	4	Qiskit	S (pennylane-cirq)

3.1 데이터 프라이버시를 위한 연합학습

[8]에서는 학습 데이터 프라이버시를 위한 Hybrid quantum-classical neural network 기반의 연합학습 기법이 제안되었다. 제안 기법은 음성 데이터에 대한 학습을 수행하여 음성을 분류하는 작업을 수행한다. 이때, 클라우드 환경에서 음성 데이터를 Mel-spectogram으로 바꾼 뒤, 이에 대한 특징 추출을 위해 QCNN을 사용한다. 이후, 추출된 특징 데이터만을 로컬 환경의 RNN

에 입력하여 최종적으로 음성을 분류해낸다. 그러나 현재의 양자컴퓨터로는 사용 가능한 큐비트의 수가 많지 않으므로, 입력 이미지를 2x2 또는 3x3으로 자른 후 학습을 수행하였다. 따라서 필요한 큐비트의 수는 4개 또는 9개이며, 실험을 통해 4개의 큐비트를 사용했을 때 더 좋은 결과를 얻었다. 이는 큐비트에 발생하는 노이즈 때문인 것으로 생각되며, 이러한 방식을 통해 양자 신경망과 고전 신경망의 하이브리드 방식을 통해 고전 방식 보다 더 높은 95.12%의 정확도를 달성하였다. 해당 기술의 구현에 사용된 양자 프레임워크는 하이브리드 신경망 구축을 위한 라이브러리인 Pennylane의 랜덤 양자 회로를 사용하였다. 또한, IBM hardward에서 수집한 노이즈가 추가된 pennylane-qiskit 시뮬레이터를 사용하였다.

3.2 어플리케이션을 위한 봇넷(Botnet) 탐지

악성 소프트웨어를 이용해 빼앗은 다수의 좀비 컴퓨터로 구성되는 네트워크인 봇넷 탐지에 대한 연구가 수행되었다[9]. 학습에 사용된 데이터는 샤넌 함수에 의해 계산되는 엔트로피 값, 도메인 이름의 확률 분포에 대한 상대 엔트로피, 도메인 이름의 문자 길이 등의 정보를 특징으로 하며, 이를 기반으로 봇넷 여부를 탐지해내도록 학습한다. 해당 기법은 QNN과 DNN의 하이브리드 방식으로 구성된다. 실험을 위해 앞서 언급한 pennylane 라이브러리의 ‘default.qubit‘ 시뮬레이터를 사용하였으며, 해당 라이브러리에서 제공하는 임베딩 레이어, 랜덤 레이어 등을 조합하여 다양한 회로에 대한 실험을 진행하였다. 또한, 양자 컴퓨터에서 발생하는 노이즈를 고려하여 IBM에서 무료로 사용 가능한 최대 5-qubit 양자 프로세서(ibmq_16_melbourne, ibmq_5_yorktown 등)를 사용하였다. 실험 결과, 양자 회로를 구성하는 레이어의 조합에 따라 성능 차이가 존재하였다. 학습에 사용된 데이터 개수가 100개인 경우, 최대 94.7%의 정확도를 달성하였으며, 데이터의 수가 1000개인 경우 최대 93.9%의 정확도를 달성하였다. 그 중, Angle Embedding과 Strongly Entangled 조합이 데이터 수가 100개인 경우에 대해 고전신경망 보다 더 높은 정확도를 달성하였다.

3.3 Control Area Network(CAN)에 대한 amplitude shift cyber attack 탐지

[10]에서는 CAN 프로토콜의 데이터 프레임을 무작위로 변경하는 amplitude shift attack에 대한 hybrid quantum-classical neural network 기반의 탐지 기법을 제안하였다. 정상적인 CAN 데이터와 공격받은 데이터를 준비한 후, 해당 데이터들을 학습하여 공격 여부를 탐지하는 방식이다. 전체적인 구성은 CAN 데이터를 이미지로 변환한 후, 고전 CNN을 통해 4x4 크기의 특징을 추출한다. 추출된 데이터는 양자 인코딩 과정을 거친 후, QNN에 입력되어 공격을 탐지해낸다. 즉, 데이터 특징 추출을 위해 고전 신경망을 사용하고, 분류를 위해 양자 신경망을 사용하는 것이다. 학습에 사용되는 데이터 셋은 총 13개의 특징을 가지지만, 양자 신경망에는 4개의 특징을 가지는 데이터만이 사용된다. 해당 논문에서는 QNN-only 모델 및 classical LSTM과 하이브리드 신경망을 비교하였다. 그 결과, 하이브리드 신경망이 더 적은 파라미터와 더 적은 epoch만을 사용하였다. 학습 및 테스트에 대한 정확도는 quantum-only의 경우 85.7% 및 62.0%, classical LSTM은 99.9% 및 87.8%를 달성하였고, 하이브리드 신경망의 경우 98.7% 및 93.9%의 정확도를 달성하였다. 즉, 양자 신경망을 사용하는 경우보다 더 안정적인 학습이 가능하고, 고전 신경망을 쓰는 경우보다 과적합 및 파라미터를 줄일 수 있었다.

3.4 Distributed Denial of Service Attack(DDoS) 침입 탐지

[11]에서는 Quantum Support Vector Machine, Hybrid quantum-classical neural network, 그리고 quantum ensemble model을 활용하여 DDoS에 대한 침입 탐지 기법을 제안하였다. 실험을 위해 DDoS 평가 데이터 셋을 사용하였으며, 해당 데이터는 source IP, destination IP, port, protocol등 총 38개의 값을 가지고 있지만, 자원 제약적인 양자 신경망에 입력되기 위해 2차원 벡터로 축소된 후, angle 임베딩을 거친다. 제안된 딥러닝 모델 구조는 3가지이다. 먼저, QSVM의 경우 qiskit에서 제공하는 라이브러리를 사용하여 양자 회로를 구성하였다. 다음으로,

hybrid 모델은 2개의 입출력 전연결 레이어와 하나의 양자 레이어를 가지며, 양자 레이어의 경우 2-qubit에 대한 회전 게이트 및 얽힘으로 구성된다. 마지막으로, ensemble quantum network는 pennylane-cirq simulator를 사용한다. 이 때, 2개의 quantum processing unit(QPU)를 사용하여 병렬적으로 연산을 수행한다. 각 양자회로를 구성하는 4-qubit 중 2-qubit만을 측정하여 값을 얻고, 해당 값들은 softmax 함수에 입력되어 출력 값을 얻는다. 마지막으로 해당 출력 값들을 모두 반영하여 최종 모델의 결과를 얻는다. 이러한 3가지 구조 중, hybrid-QNN이 99.8%의 정확도를 달성하였으며, 계산 효율성에서 가장 뛰어난 성능을 보였다.

IV. 결론

양자 컴퓨터가 개발됨에 따라 양자컴퓨터 상에서 동작 가능한 양자 인공지능 기술들이 개발되면서 사이버 보안을 위한 양자 인공신경망에 대한 다양한 연구들 또한 진행되고 있다. 양자 신경망은 양자 회로를 사용하여 고전 신경망의 구조 및 기능을 하도록 설계한 것이며, 양자 회로만을 사용한 양자 신경망과, 고전 신경망을 함께 사용하는 하이브리드 방식의 양자 신경망이 존재한다. 현재 대부분의 연구는 큐비트 등의 자원 제약, 계산 효율성 등을 위해 하이브리드 양자 신경망을 사용하고 있으며, 양자 회로만을 활용한 연구 결과도 있다. 양자 신경망은 고전 신경망보다 훨씬 적은 파라미터를 사용할 수 있으며, 큐비트를 사용하므로 데이터의 표현 범위가 넓어 더 높은 정확도를 얻을 수 있는 이점이 존재한다. 그러나 실제 양자 프로세서를 사용할 경우, 양자 컴퓨터에서 발생하는 노이즈로 인한 정확도 손실이 발생할 수 있다. 향후, 더 큰 규모의 양자 컴퓨터가 개발된다면 이러한 오류를 정정할 수 있는 양자 신경망을 구성할 필요가 있으며, 더 많은 큐비트 등의 자원을 사용하여 사이버 보안을 위한 더 많은 요소들을 학습 데이터로 사용할 수 있을 것으로 생각된다.

V.Acknowledgement

이 논문은 2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (<Q|Crypton>, No.2019-0-00033, 미래컴퓨팅 환경에 대비한 계산 복잡도 기반 암호 안전성 검증 기술개발, 100%)

[참고문헌]

[1] Bharti, Kishor, et al. "Noisy intermediate-scale quantum algorithms." Reviews of Modern Physics 94.1 (2022): 015004.

[2] Beer, Kerstin, et al. "Training deep quantum neural networks." Nature communications 11.1 (2020): 1-6.

[3] Liu, Junhua, et al. "Hybrid quantum-classical convolutional neural networks." Science China Physics, Mechanics & Astronomy 64.9 (2021): 1-8.

[4] Rebentrost, Patrick, Masoud Mohseni, and Seth Lloyd. "Quantum support vector machine for big data classification." Physical review letters 113.13 (2014): 130503.

[5] Cong, Iris, Soonwon Choi, and Mikhail D. Lukin. "Quantum convolutional neural networks." Nature Physics 15.12 (2019): 1273-1278.

[6] Bausch, Johannes. "Recurrent quantum neural networks." Advances in neural information processing systems 33 (2020): 1368-1379.

[7] Dallaire-Demers, Pierre-Luc, and Nathan Killoran. "Quantum generative adversarial networks." Physical Review A 98.1 (2018): 012324.

[8]Yang, Chao-Han Huck, et al. "Decentralizing feature extraction with quantum convolutional neural network for automatic speech recognition." ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2021

[9] Suryotrisongko, Hatma, and Yasuo Musashi. "Evaluating hybrid quantum-classical deep learning for cybersecurity botnet DGA detection." Procedia Computer Science 197 (2022): 223-229.

[10] Islam, Mhafuzul, et al. "Hybrid Quantum-Classical Neural Network for Cloud-supported In-Vehicle Cyberattack

Detection." IEEE Sensors Letters 6.4 (2022): 1-4.
[11] Payares, E. D., and J. C. Martinez-Santos. "Quantum machine learning for intrusion detection of distributed denial of service attacks: a comparative overview." Quantum Computing, Communication, and Simulation 11699 (2021): 35-43.