머신러닝 기반 물리계층 추상화 기법을 활용한 Cascade 프로토콜 성능 모사

최정규, 김응준, 신유철, 노광석
㈜ 큐심플러스

{jk_choi, ej_kim, yc_shin, ks_noh}@qsimplus.com

Performance Emulation of the Cascade Protocol Using Machine Learning-Based Physical Layer Abstraction

Jeongkyu Choi, Eungjun Kim, Youchul Shin and Kwangseok Noh
QSIMPLUS Co., Ltd.

요 약

본 논문은 양자 키 분배 시스템의 오류 정정 단계에서 활용되는 Cascade 프로토콜의 성능을 효과적으로 모사하기 위해 머신러닝 기반의 물리계층 추상화 기법을 제안한다. 데이터는 Cascade 프로토콜 시뮬레이션을 통해 QBER 변화에 따른 FER 과 누출 정보량을 수집하였다. 수집된 데이터를 바탕으로 QBER 과 초기 블록 사이즈를 입력으로 받아 FER 과 누출 정보량을 예측하는 다항 회귀모델을 모델링하여 성능 평가 후 수식을 도출하였다.

Ⅰ. 서 론

물리계층 추상화(Physical Layer Abstraction, PLA)는 입력 변수를 기반으로 실제 물리계층의 복잡한 과정을 생략하고, 시스템 성능을 신속하게 예측할 수 있는 효과적인 기법이다 [1]. 일반적으로 PLA 는 보간(Interpolation)이나 외삽(Extrapolation) 기반의 고전적인 방법으로 구현되어 왔으며, 비교적 간단한 수학적 모델로도 성능 예측이 가능하다는 장점이 있다.

그러나 본 연구에서는 머신러닝 기반 회귀 모델을 활용하여 PLA 기법을 새롭게 구성하였다. 이를 통해 보다 유연하고 자동화된 방식으로 양자 비트 오류율(QBER)에 따른 성능 예측이 가능함을 확인하였다.

본 논문에서는 Cascade 프로토콜 시뮬레이션을 통해 QBER 변화에 따른 프레임 오류율(Frame Error Rate, FER) 및 누출 정보량(Information Leakage) 데이터를 수집하였다. 수집된 시뮬레이션 데이터를 바탕으로, 다항 회귀(Polynomial Regression) 모델을 학습하고 평가 지표를 통해 예측 정확도를 검증하였다. 검증 후에는 QBER 과 초기 블록 사이즈에 따라 FER 과 누출 정보량을 예측할 수 있는 수식을 도출하였다.

도출한 수식은 Cascade 프로토콜의 성능을 간단하고 신속하게 추정할 수 있는 방법을 제공하며, 이를 통해 머신러닝 기반 PLA 기법의 실용성과 정확성을 입증하였다.

Ⅱ. 본론

본 연구에서는 데이터 모델링 후 수식을 도출하기 위해 머신러닝 파이프라인에 관한 선행 연구[2]를 기반으로, 본 연구에 적합한 과정을 선별하여 그림 1 과 같이 파이프라인을 설계하였다.

시뮬레이션은 TTAK.KO-12.0406 표준 문서에 제시된 Cascade 프로토콜의 절차도를 참고하여 구현하였다 [3].

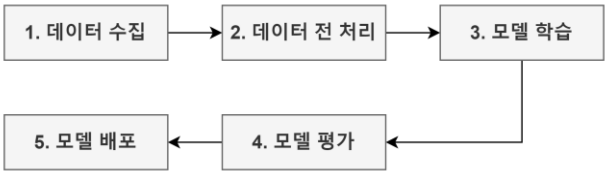

그림 1. 머신러닝 파이프라인

표 1 (a)는 Cascade 프로토콜 시뮬레이션에 사용된 주요 파라미터를 나타낸다. 초기 블록 사이즈 및 Pass 횟수는 Original Cascade 에서 제안하는 최적의 값(초기 블록 사이즈: ceil(0.73/QBER), Pass: 4 회)을 적용하였다 [4]. 시뮬레이션에서는 QBER 을 1.0%에서 11.0%까지 0.1% 간격으로 변화시키며, 이에 대응되는 FER 및 누출 정보량 데이터를 수집하였다.

전처리(Preprocessing) 단계에서는 수집된 데이터를 학습용 및 시험용 데이터셋으로 분할하고, 스케일 완화 작업을 수행하였다. 구체적으로, 학습용 데이터셋은 QBER 1.0% ~ 10.0%, 시험용 데이터셋은 10.1% ~ 11.0%의 구간으로 구성하였다. FER 은 QBER 변화에 따라 큰 폭으로 변동하는 양상을 보여, 모델 학습의 안정성을 확보하기 위해 로그 스케일로 변환하였다.

다음으로 모델 학습을 위해 QBER 과 QBER 로부터 계산되는 초기 블록 사이즈를 독립 변수(x)로 설정하였고, FER 과 누출 정보량을 각각 종속 변수(y)로 설정하였다. 이후 각 종속 변수에 대해 2 차 및 3 차 다항 회귀 모델을 구성하고 학습을 진행하였다.

회귀 모델의 성능 평가 지표로 결정 계수 (R^2) 와 평균 절대 비율 오차(MAPE)를 활용하였으며, 평가는 QBER 10.1% ~ 11.0% 구간의 FER 및 누출 정보량에 대한 실측 값과 예측 값을 기준으로 계산하였다. R^2는 1 에 가까울수록 모델의 설명력이 우수함을 의미하고, MAPE 는 0 에 가까울수록 예측 정확도가 높음을

의미한다. 표 1 (b)는 FER 과 누출 정보량에 대해 2 차 및 3 차 다항 회귀 모델의 R^2 및 MAPE 결과를 제시한 것이다. 비교 결과, FER 은 2 차 다항 회귀 모델에서, 누출 정보량은 3 차 다항 회귀 모델에서 보다 우수한 커브 피팅(Curve Fitting) 성능을 보이는 것으로 나타났다.

(a)

입력 파라미터	입력 값
반복 횟수	10,000,000 회
걸러진 키	1,000 Bit
초기 블록 사이즈	ceil(0.73 / QBER)
블록 사이즈 증가량	× 2
QBER	1.0 % ~ 11.0% (Step Size 0.1%)
Pass (반복 횟수)	4

(b)

종속변수(y)	차수	R^2	MAPE
FER	2	0.9598	4.11 %
FER	3	0.9792	2.51 %
누출 정보량	2	0.7678	0.99 %
누출 정보량	3	0.3940	1.71 %

표 1. (a) 시뮬레이션 입력 파라미터, (b) 평가 지표

그림 2 (a)와 (b)는 QBER 1.0% ~ 11.0% 구간에서 FER 및 누출 정보량의 실측 값(Actual Data)과 예측 값(Predicted Data)을 나타낸 그래프이다.

두 그래프 모두 예측 값이 실측 값의 변화 추이와 유사한 양상을 보였으며, 이를 통해 커브 피팅 성능이 양호함을 확인하였다.

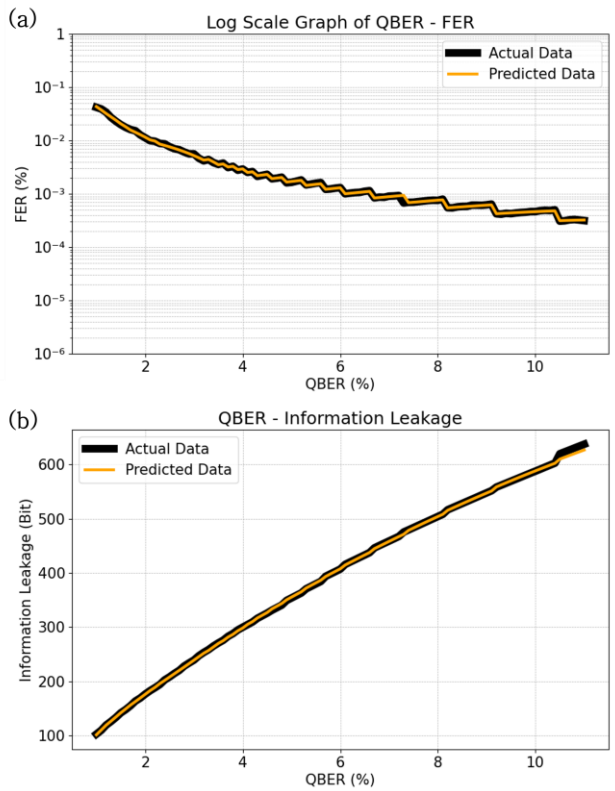

그림 2. QBER 에 따른 실측 값과 예측 값 (a) FER, (b) 누출 정보량

최종적으로, 이상의 과정을 통해 FER 은 3 차 다항 회귀 모델로, 누출 정보량은 2 차 다항 회귀 모델로 모델링하여 수식을 도출하였다.

Ⅲ. 결론

본 논문에서는 머신러닝 기반의 PLA 기법을 활용하여 FER 과 누출 정보량에 대한 다항 회귀 모델을 구축하고, 평가 지표를 통해 커브 피팅 성능을 검증하였다. 회귀 모델에서 도출된 수식만으로도 시뮬레이션 없이 FER 과 누출 정보량을 손쉽게 예측할 수 있음을 확인하였으며, 이는 성능 모사를 보다 효과적이고 효율적으로 수행할 수 있는 대안이 될 수 있음을 보여준다.

본 연구에서는 두 개의 독립 변수를 기반으로 수식을 도출하였으나, 향후에는 걸러진 키의 변화에 따른 FER 및 누출 정보량에 대한 추가 데이터를 확보하여 수식의 적용 범위를 더욱 확장할 계획이다.

수식의 적용 범위를 확장하고 머신러닝 기반의 PLA 기법을 적용함으로써, 다양한 조건에서 성능 예측이 가능해지며, 향후 보다 일반화된 모델 개발에도 기여할 수 있을 것으로 기대된다.

ACKNOWLEDGMENT

본 연구는 중소벤처기업부의 기술개발사업[RS-2023-0025843]과 정부(과학기술정보통신부)의 재원으로 한국연구재단(No. RS-2023-00242396)의 지원을 받아 수행된 연구임

참 고 문 헌

[1] Waqar Anwar, Atul Kumar, Norman Franchi, and Gerhard Fettweis, "Performance Analysis using Physical Layer Abstraction Modeling for 5G and Beyond Waveforms" *ResearchGate*, 2019.

[2] M. J. Bdair, “Enhancing Machine Learning Workflows: A Comprehensive Study of Machine Learning Pipelines,” *ResearchGate*, 2024.

[3] Telecommunications Technology Association (TTA), "Security Requirements and Test Methods for Post Processing of Quantum Key Distribution" *TTA Standard TTAK.KO-12.0406*, pp. 1-2, 18-19. Jun. 2024.

[4] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of Cryptographic Techniques, *vol. 765, Lecture Notes in Computer Science*, pp. 410- 423, Springer, Berlin, Heidelberg, 1994.