# RF Fingerprinting 과 DNN 을 이용한 NFC 태그 인증 시스템

이은규, 유호근, 허경무, 이재훈
고려대학교

lek7146@korea.ac.kr, hogeunyoo@korea.ac.kr, trivialdevil@korea.ac.kr, ejhoon@korea.ac.kr

# Deep Learning-based RF Fingerprinting for NFC Tag Authentication

Eunkyu Lee, Hogeun Yoo, Kyongmoo Hur, Jaehoon Lee
Korea Univ.

## 요 약

본 논문에서는 신호 수집 시스템을 통해 ISO/IEC 14443 표준을 따르는 NFC 태그의 ATQA 신호에서 하드웨어의 특성을 반영하는 RF Fingerprint 를 추출하였다. 추출된 신호 샘플을 입력으로 하는 정규화 및 완전 연결 신경망 모델을 설계·학습하여 태그를 높은 정확도로 분류함을 실험적으로 검증하였다. 추가적인 신호 재수집 실험을 통해 시간과 환경 변화에도 안정적인 NFC 태그 분류 성능을 확인하였다.

## Ⅰ. 서 론

NFC(Near Field Communication) 기술은 13.56 MHz 대역에서 작동하는 근거리 무선 통신 기술로, 다양한 분야에서 광범위하게 사용되고 있다. 그러나 NFC 기술의 광범위한 보급과 함께 다양한 보안 위험이 대두되고 있으며, 특히 카드 복제 공격과 중계 공격 등이 주요한 보안 취약점으로 지적되고 있다.

최근 연구들에서는 이러한 한계를 극복하기 위한 대안으로 RF Fingerprinting 기술이 주목받고 있다[1][2]. RF Fingerprinting 은 무선 송신기의 하드웨어 제조 과정에서 발생하는 미세한 물리적 불완전성을 이용하여 각 디바이스의 고유한 특징을 추출하는 기술이다.

본 논문에서는 RF Fingerprinting 기술에 딥러닝 모델을 적용하여, 기존 접근법의 한계를 극복하고 높은 분류 정확도를 달성하는 NFC 태그 인증 시스템을 제안한다. 정밀한 신호 수집 시스템 구축부터 ATQA(Answer To Request of Type A) 신호의 전처리 기법, 완전 연결 신경망 기반의 딥러닝 분류 모델 설계 및 최적화 과정에 이르기까지 전체적인 시스템 개발 방법론을 제시한다. 또한, 시간 경과에 따른 성능 안정성 분석을 통해 RF Fingerprinting 기술의 보안성 향상 효과를 검증한다.

## Ⅱ. 본론

NFC 태그의 고유한 RF Fingerprint 는 제조 과정에서 발생하는 회로 부품의 미세한 하드웨어 변이에서 기인한다. 이러한 물리적 불완전성은 NFC 통신 과정에서 태그가 필수적으로 송신하는 ATQA 신호에 나타나며, 이를 활용하여 태그 식별이 가능하다. ATQA 신호는 ISO/IEC 14443 표준에 따라 리더의 REQA(Request Command, Type A) 신호에 대한 응답으로 전송되는 2 바이트 신호로, 모든 태그가 동기적으로 응답하는 특성을 가진다.

본 연구에서는 정밀한 RF Fingerprint 추출을 위해 SDR(Software Defined Radio) 기반의 NFC 신호 수집 시스템을 구축하였다(그림 1). GNU Radio 를 이용하여 ISO/IEC 14443 표준을 준수하는 REQA 신호를 생성하고, 이를 USRP-2954R 에 연결된 안테나를 통해 13.56 MHz 반송파로 송신한다. 송신 안테나와 동일한 모델의 수신 안테나를 사용하여 REQA 송신과 ATQA 응답을 포함한 전체 NFC 통신 과정을 모니터링한다. 중심 주파수는 13.56 MHz, 샘플링 레이트는 10 MSamples/s 로 설정하여 신호를 수집한다.

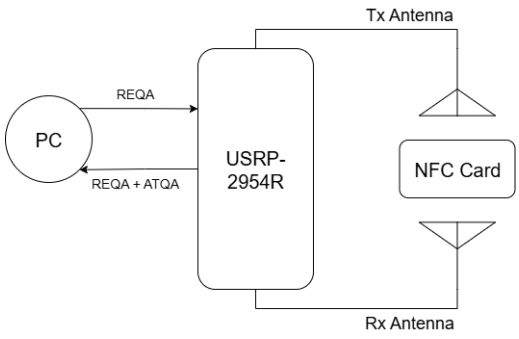


그림 1. NFC 카드 RF Fingerprinting 신호 수집 시스템 구조

수집된 원시 데이터는 REQA 와 ATQA 신호가 모두 포함되어 있으므로, RF Fingerprint 추출을 위해서는 후처리 과정이 필요하다. 수집된 연속 데이터를 REQA 신호를 기준으로 개별 세션(요청-응답 쌍)으로 분할한 뒤, ATQA 신호의 정확한 위치를 식별하기 위해 적응형 임계값 기반 검출 알고리즘을 적용한다. 각 샘플에 대해 1/2 비트 구간의 평균값을 계산하고, 이 평균값이 동적 임계값을 초과하는 지점들 중 가장 마지막에 위치한 지점을 종료 비트로 식별한다. 검출된 ATQA 종료점을 기준으로 역산하여 ATQA 신호의 시작점을 결정하고, 해당 구간의 신호를 정밀하게 추출한다. 이러한 데이터

수집 및 후처리 과정을 통해 NFC 카드 특성이 반영된 고품질 ATQA 신호를 추출할 수 있다(그림 2).

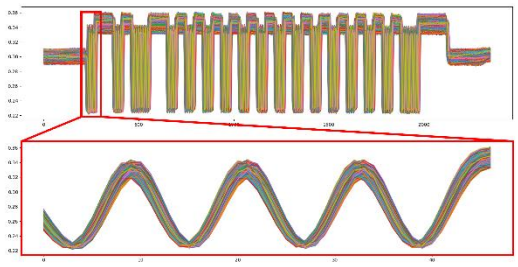

그림 2. 카드의 ATQA 신호와
딥러닝 학습에 활용되는 초기 신호 구간

RF Fingerprinting 기법을 이용한 개별 NFC 카드의 식별 가능성을 검증하기 위해 심층 신경망 기반의 분류 모델을 구축하였다. ATQA 신호에서 하드웨어 특성이 명확하게 나타나는 첫 번째 비트의 전반부 구간을 특징 추출 영역으로 선정하였다. 이 구간은 카드의 하드웨어에 기인한 고유한 신호 특성이 집중적으로 나타나는 영역으로, 해당 구간의 47 개 신호 샘플을 입력 벡터로 사용하며, Z-score 정규화를 적용하는 전처리 과정을 거친다. 이는 신호의 상대적 분포를 표준 정규분포로 변환하면서 학습 과정의 안정성을 향상시키고, 모델이 유의미한 특징을 보다 용이하게 학습하도록 돕는다.

본 연구에서는 완전연결 신경망(Fully Connected Neural Network, FCNN) 구조를 채택하였다. 네트워크는 그림 3 과 같이 구성된다.

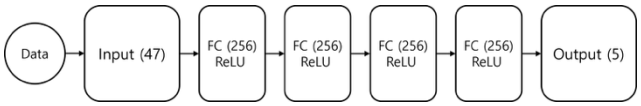


그림 3. NFC 태그 인증 시스템의 딥러닝 모델 구조

입력층과 출력층의 노드 수는 각각 47 개와 5 개이다. 은닉층은 크기가 256 인 4 개의 완전연결층으로 구성되어 있으며, 활성화 함수로 ReLU 함수를 적용하였다. 중요 특징을 보존하면서 과적합을 방지하기 위해 Dropout 기법을 적용하였다.

데이터셋은 목적에 따라 학습(train), 검증(validation), 시험(test)로 분리하였다. 학습 데이터셋을 이용해 신경망 모델 파라미터를 최적화하였으며, 전체 데이터 중 올바르게 예측한 비율을 계산하여 정확도를 측정하였다. 검증 데이터셋에서 가장 높은 정확도를 기록한 모델을 최종 모델로 선정하였고, 해당 모델에 시험 데이터셋의 정확도를 평가함으로써 모델의 성능을 측정하였다.

하이퍼파라미터는 학습률 0.001, 미니 배치 크기 128 로 설정하였고, Adam 옵티마이저를 사용하여 최적화하였다. 카드마다 약 1000 개의 데이터를 5000 Epoch 동안 반복하여 학습된 모델은 시험 데이터셋에서 98.3% 이상의 높은 정확도로 카드를 구별할 수 있음을 확인하였다(그림 4). 이는 추출된 RF Fingerprint 가 각 카드의 고유 특성을 효과적으로 반영하고 있음을 시사한다.

초기 높은 분류 성능이 데이터 수집 시점이나 환경적 요인 등에 의존할 가능성을 확인하기 위해 추가적인 검증 실험을 수행하였다. 기존에 수집한 데이터와는 상이한 시점에 수집한 데이터도 동일한 분류 성능을 갖는지 확인하기 위해, 기존 카드들에 대해 새로운 세션에서 데이터를 수집하고 기존 데이터만 학습한 동일한 모델을 통해 추론을 진행하였다(그림 5). 그 결과 99.1% 이상의 정확도로 카드를 구분할 수 있었고, 이를 통해 시간적 안정성과 학습되지 않은 데이터에 대한 모델의 강건성을 확인할 수 있었다.

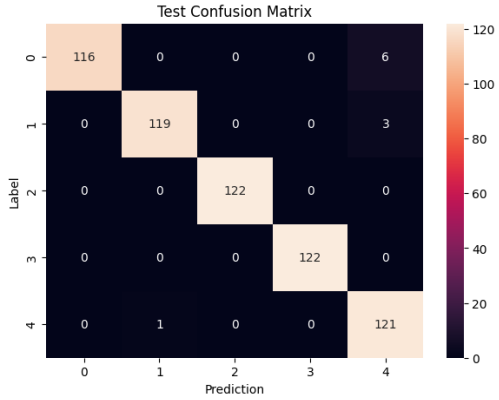


그림 4. 단일 시점 데이터에 대한 학습 및 추론 결과

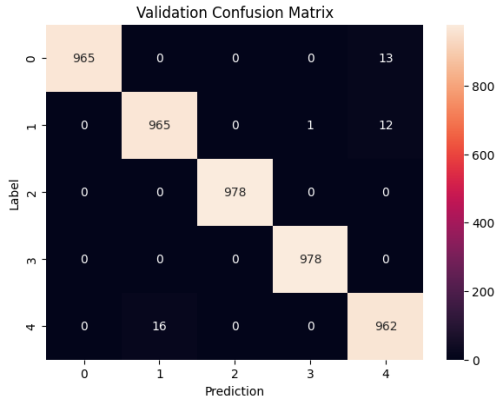


그림 5. 상이한 시점 데이터에 대한 사전 학습 모델 추론 결과

## Ⅲ. 결론

본 연구에서는 신호 수집 시스템과 완전 연결 신경망을 결합하여 NFC 태그의 ATQA 신호에서 하드웨어 불완전성을 효과적으로 추출·분류함으로써 높은 카드 인증 정확도를 확인하였다. 이를 통해 RF Fingerprinting 기법의 실용 가능성을 검증하였으며, 향후 다양한 딥러닝 아키텍처와 다중 주파수 특징 공간을 도입하여 보안성과 일반화 성능을 강화할 예정이다.

## 참 고 문 헌

[1] W. Lee, S. Y. Baek and S. H. Kim, "Deep-Learning-Aided RF Fingerprinting for NFC Security," IEEE Communications Magazine, vol. 59, no. 5, pp. 96-101, May 2021, doi: 10.1109/MCOM.001.2000912.

[2] Y. Yang et al., "Jump Out of Resonance: A Practical NFC Tag Fingerprinting Scheme," IEEE Transactions on Mobile Computing, vol. 23, no. 9, pp. 8694-8709, Sept. 2024, doi: 10.1109/TMC.2024.3354813.

[3] W. Lee, S. Y. Baek, "Deep neural network-aided radio frequency fingerprinting for identification of near field communication tags," Expert Systems with Applications, vol. 296, Part B, 2026, 129016, ISSN 0957-4174, https://doi.org/10.1016/j.eswa.2025.129016.