

NFC에서 무선 핑거프린팅 기술 적용을 위한
GAN 기반 채널데이터 증강방안

I. 서 론

GAN based Data Augmentation of
Channel Data for the Application of RF
Finger-printing in NFC

Woongsup Lee*

*Associate Professor, Department of Information and
Communication Engineering, Institute of Marine Industry,
Gyeongsang National University, 53064 Korea

ABSTRACT

RF fingerprinting based on deep learning (DL) has gained interests as a means to improve the security of near field communication (NFC) by allowing identification of NFC tags based on unique physical characteristics. To achieve high accuracy in the identification of NFC tags, it is crucial to utilize a large number of training data, however it is hard to collect such dataset in practice. In this study, we have provided new methodology to generate RF waveform from NFC tags, i.e., data augmentation, based on a conditional generative adversarial network (CGAN). By using the RF waveform of NFC tags which is collected from the testbed with software defined radio (SDR), we have confirmed that the realistic RF waveform can be generated through our proposed scheme.

Keywords : Generative adversarial network (GAN), RF finger printing, NFC communication, Deep learning, Data augmentation.

근거리 무선통신(near field communication, NFC) 기술은 13.56MHz의 주파수 대역을 이용하여 10cm 이내의 근거리에서 통신을 수행하는 기술이다. NFC 기술은 모바일 결제 및 출입을 위한 개인 인증 등의 용도로 활발하게 사용되고 있다. NFC 태그들은 기존의 무선장비들과 달리 처리 능력에 한계로 인해 낮은 수준의 보안 기술만 사용가능하므로 다양한 보안위협에 취약하다. 특히 NFC 태그의 경우 복제(cloning) 및 릴레이 어택(relay attack)에 매우 취약하므로 [1] 이를 해결하기 위한 다양한 기술들이 개발되고 있다.

무선 핑거프린팅(RF fingerprinting) 기술은 NFC 태그의 물리적 특성을 이용하여 무선장비를 식별하는 기술로서, NFC 태그의 식별방안으로 활발하게 연구되고 있다 [2-4]. 특히 최근에 딥러닝(deep learning) 기술을 활용하여 장비식별을 위한 무선신호특성(무선지문)을 쉽게 추출하는 방식들이 개발되면서, 무선 핑거프린팅 기술의 적용이 더욱 용이해지고 있다 [5-8]. [8]의 연구에서는 다양한 심층신경망(deep neural network, DNN) 구조를 활용하여 50개의 NFC 태그로부터 각 태그들의 무선 신호 특성을 추출하고 이를 기반으로 96.16%의 확률로 NFC 태그를 정확하게 분류할 수 있음을 보였다.

딥러닝에 기반을 둔 무선 핑거프린팅 기술에서는 DNN의 학습을 위해 각 태그들로부터 많은 양의 무선 신호를 실측하고, 이를 DNN 구조에 맞게 가공(preprocess) 하는 것이 필요하다. 하지만 높은 수준의 분류 정확도 지닌 DNN 구조를 학습하기 위해서 매우 많은 실측채널 데이터가 필요하므로 이를 준비하는데 오랜 측정시간을 비롯한 다양한 어려움을 겪을 수 있다.

최근 DNN 기술 중 하나인 생산적 적대 신경망(generative adversarial network, GAN)을 이용하여 인공적으로 데이터를 생성하여 학습에 활용하는 데이터 증강기법(data augmentation)이 개발되었다 [9-10]. 이러한 데이터 증강기법을 이용하여 적은 수의 원본 데이터

Received 12 August 2021, Revised 18 August 2021, Accepted 19 August 2021

* Corresponding Author Woongsup Lee (E-mail:wslee@gnu.ac.kr, Tel:+82-55-772-9171)

Associate Professor, Department of Information and Communication Engineering, Institute of Marine Industry, Gyeongsang National University, 53064 Korea

Open Access <http://doi.org/10.6109/jkiice.2021.25.9.1271>

print ISSN: 2234-4772 online ISSN: 2288-4165

만을 사용하여도 많은 수의 데이터를 생성할 수 있으므로 DNN의 학습 및 성능검증에 큰 도움을 줄 수 있다.

본 연구에서는 NFC 태그 무선 핑거프린팅을 위한 GAN에 기반을 둔 무선채널 데이터 증강방안을 제안한다. 또한 소프트웨어 정의 라디오 (software defined radio, SDR) 기반 테스트베드를 통해서 수집된 실측 채널 데이터를 이용하여 NFC 태그의 무선채널 데이터 증강이 가능함을 확인하였다. 본 개발 방안은 딥러닝에 기반을 둔 다양한 무선통신기술에서 채널데이터 증강기술로 활용될 수 있다.

II. 시스템 환경 및 테스트베드

본 연구에서는 ISO/IEC 14443 type 2 기반의 NFC 태그를 분류하는 무선 핑거프린팅 기법을 고려하였다. 본 연구에서 고려한 무선 핑거프린팅에서는 NFC 태그로부터 NFC 리더로 전송되는 신호인 ATQA (Answer To reQuest, Type A) 메시지에 해당하는 RF 파형을 사용하였고, 하나의 메시지에 포함되는 19 bit 중 1bit에 해당하는 RF 파형을 슬라이싱(slicing) 하여 무선지문을 검출하였다 [8]. 특히 NFC 전송에서는 맨체스터 코드를 사용하여 데이터가 전송되므로 0 혹은 1이 전송됨에 따라 신호의 앞쪽 혹은 뒤쪽에 4개의 펄스를 포함하게 되는데, 각 bit별로 전송되는 4개의 펄스를 무선지문 (RF feature)으로 사용하였다. 또한 실제 수집되는 RF 신호의 크기가 매우 작기 때문에 펄스데이터의 최소/최대 값이 0과 1이 되도록 데이터 정규화를 적용하였다.

NFC 태그를 분류하기 위한 DNN 훈련데이터를 수집하기 위해서 SDR과 상용 NFC 리더 (ACR 122) 및 수집 안테나로 이루어진 하드웨어 테스트베드를 구축하였다. 테스트 베드에서는 universal software radio peripheral (USRP) X300를 SDR 장비로 사용하였고 USRP 장비와 연결된 컴퓨터의 GNURADIO 기반 프로그램을 이용하여 태그에서 나오는 RF 신호를 수집하였다. 데이터 수집을 위해서 40 Msps의 샘플링레이트를 사용하였다. 이를 통해서 무선지문 데이터로 사용한 각 펄스마다 192개의 샘플링 포인트를 얻을 수 있었다 [8]. 본 연구에서 구현한 하드웨어 테스트베드가 그림 1에 나와 있다.

NFC 태그를 분류하기 위한 DNN 구조로 200개의 히든노드(hidden node)를 가지는 완전연결신경망(fully-

connected neural network, FNN) 구조를 고려하였고, 전체 레이어수는 4로 설정하였다. 각 레이어에서는 활성화 함수(activation function)로 ReLU(Rectified Linear Unit)를 고려하였다. 또한 학습에서의 과적합(over-fitting)을 막고 정확도를 높이기 위해서 드롭아웃(dropout)과 배치 정규화(batch normalization)를 적용하였다. 본 테스트베드에서는 4개의 NFC 태그를 분류하기 때문에 마지막 레이어에는 4개의 출력을 지닌 softmax 함수를 사용하였다.



Fig. 1 Implemented hardware testbed for RF fingerprinting.

III. CGAN 기반 무선채널데이터 증강방안

본 연구에서 GAN을 이용하여 실제 NFC RF 파형과 유사한 파형을 생성하였다. GAN은 생성자(generator)와 감별자(discriminator)의 서로 경쟁하는 두 신경망으로 이루어져 있다 [9-10]. 학습을 통해 생성자가 새로운 데이터를 생성하고 감별자가 이를 실제 훈련 데이터셋에서 나온 데이터인지 합성 데이터인지 구별하게 훈련함으로써 생성자가 실제 훈련 데이터셋의 데이터와 유사한 데이터를 생성할 수 있게 한다.

특히 본 연구에서는 CGAN (conditional GAN) 기술을 사용하여 태그별로 다른 파형을 생성할 수 있게 구현하였다. CGAN에서는 데이터의 라벨 값을 생성자의 입력으로 주어서 라벨에 따라서 다른 데이터가 생성될 수 있게 한다. 본 연구에서는 CGAN 사용을 통해서 테스트베드에서 사용한 4개의 NFC 태그에 대한 RF 파형을 각각 생성할 수 있게 구현하였다.

NFC 태그 분류를 위한 DNN과 마찬가지로 감별자와 생성자를 위한 DNN 구조로 FNN을 사용하였다. 감별자는 512개의 히든노드를 가진 4 레이어 구조를 고려하였고 활성화함수로는 leaky ReLU를 사용하였으며 정규화를 위해서 드롭아웃을 사용하였다. 감별자의 경우 생

성데이터와 학습데이터만을 구별하면 되므로 마지막 레이어에는 1개의 sigmoid 함수를 사용하였다. 생성자를 위한 DNN 구조에서는 256, 512, 1024, 192개의 히든 노드를 지닌 4 레이어 구조를 사용하였고, 감별자 네트워크와 마찬가지로 leaky ReLU를 활성화함수로 사용하였으며 정규화를 위해서 드롭아웃을 사용하였다. 생성자는 192개의 데이터 포인트를 지닌 RF 파형이므로 생성자 네트워크의 최종 레이어는 192개의 출력을 가지도록 구성하였다.

IV. 결과분석

본 장에서는 개발된 GAN 기반 무선채널데이터 증강방안의 성능을 분석하였다. 우선 그림 2에서는 그림 1의 하드웨어 테스트베드를 이용하여 실제 수집된 NFC 태그의 RF 파형을 보여준다. 각 부분 그래프는 본 연구에서 고려된 4개의 태그에 해당되는 파형을 보여준다. RF 파형에서 확인할 수 있듯이 RF 파형이 4개의 펄스로 이루어져 있는 것을 확인할 수 있다. 또한 4개 NFC 태그의 RF 파형이 거의 비슷한 것을 확인할 수 있는데, 이를 통해 실제 분석적인 방법으로 무선지문을 추출하는 것이 어렵고 딥러닝 기반 무선지문 추출이 필요함을 확인할 수 있다.

그림 3과 4에서는 제안된 GAN기반 무선채널데이터 증강방식을 통해서 생성된 RF 파형을 보여준다. 그림 3에서는 GAN 네트워크 학습 전에 생성된 파형을 보여주고, 그림 4에서는 GAN 네트워크 학습 이후에 생성된 파형을 보여준다. 결과에서 확인할 수 있듯이 학습 전에는 랜덤한 노이즈와 같은 파형이 생성되지만 충분한 학습 이후에는 그림 2의 파형과 유사한 RF 파형을 생성하는 것을 확인할 수 있다. 본 결과를 통해 제안된 GAN 기반 기술을 이용하여 실제 RF 파형과 유사한 RF 파형을 생성할 수 있음을 확인할 수 있다.

Table. 1 Performance of GAN based augmentation.

Performance metric	GAN augmentation	Real channel
Precision	0.9910	0.9998
Recall	0.9911	0.9998
F1-score	0.9910	0.9998

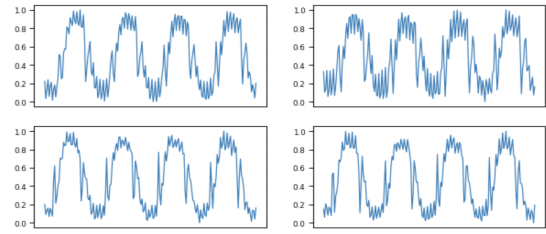


Fig. 2 RF waveform of collected data.

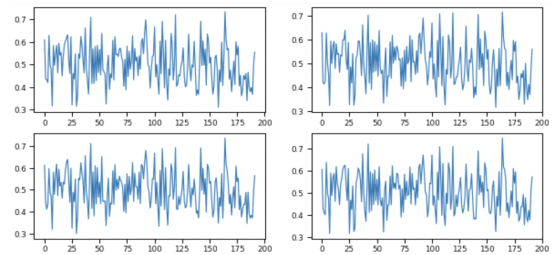


Fig. 3 RF waveform of GAN augmentation (w/o training).

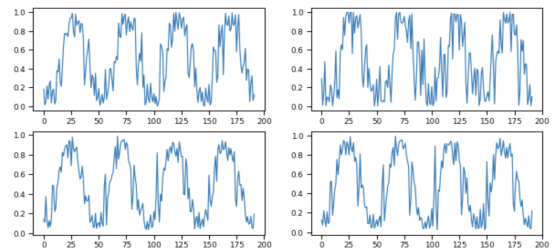


Fig. 4 RF waveform of GAN augmentation (w. training).

데이터 증강방식의 정량적 성능검증을 위해 학습된 DNN 기반 무선 핑거프린팅 분류기를 이용하여 1) 실제 수집된 RF 파형(Real channel)과 2) GAN을 이용하여 생성된 RF 파형(GAN augmentation)에 대한 분류 정확도를 측정하여 표1에 정리하였다. 성능분석지표로는 정밀도 (precision), 재현률 (recall), F1-score를 고려하였다 [11]. 표1의 결과는 실제 수집된 RF 파형을 기반으로 학습된 분류기에, 학습에 사용되지 않은 수집 RF파형과 GAN으로 생성된 RF 파형을 입력으로 사용하여 얻어졌다. 결과에서 확인할 수 있듯이 DNN 기반 무선 핑거프린팅 분류기가 실제 수집된 RF 파형과 GAN을 통해서 생성된 RF 파형 모두 높은 정확도로 분류할 수 있는 것을 확인할 수 있다. 또한 [8]의 기존 연구에 비해서 더 적은 수의 NFC태그를 사용하였기 때문에 [8]에서 얻어진 96.16%보다 높은 정확도로 NFC 태그들을 분류할 수 있

음을 확인 할 수 있다.

그림 5에는 GAN을 이용하여 생성된 데이터의 분류 정확도를 혼동행렬(confusion matrix)로 표현하였다. 결과에서 확인할 수 있듯이 모든 NFC 태그에 대해서 GAN으로 생성된 데이터가 정확하게 분류되는 것을 볼 수 있다. 이를 통해서 제안 데이터 증강방식을 통해 실제 RF 파형에 근접한 파형을 생성할 수 있음을 확인할 수 있다.

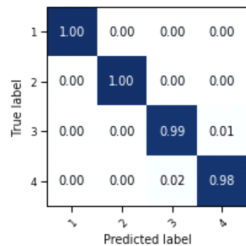


Fig. 5 Confusion matrix with GAN augmentation.

V. 결론

본 연구에서는 GAN을 이용하여 특정 NFC 태그의 RF 파형을 인공적으로 생성하는 방안을 개발하였다. 데이터 수집 및 성능분석을 위해서 딥러닝 기반 무선 핑거프린팅을 수행하는 하드웨어 테스트베드를 구축하였고, 실제 GAN을 통해서 생성한 RF 파형이 높은 정확도로 해당 태그로 분류되는 것을 확인할 수 있었다.

ACKNOWLEDGEMENT

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2021R1F1A1046932).

REFERENCES

- [1] S. C. G. Periaswamy, D. R. Thompson, and J. Di, "Fingerprinting RFID Tags," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 6, pp. 938-943, Nov. 2011.
- [2] G. Zhang, L. Xia, S. Jia, and Y. Ji, "Physical-layer Identification of HF-RFID Cards Based on RF Fingerprinting," in *Proc. of ISPEC*, Zhangjiajie, China, Nov. 2016.
- [3] H. P. Romero, K. A. Remley, D. F. Williams, and C. Wang, "Electromagnetic Measurements for Counterfeit Detection of Radio Frequency Identification Cards," *IEEE Transactions on Microwave Theory and Techniques*, vol. 57, no. 5, pp. 1383-1387, May. 2009.
- [4] J. Han, C. Qian, P. Yang, D. Ma, Z. Jiang, W. Xi, and J. Zhao, "GenePrint: Generic and Accurate Physical-layer Identification for UHF RFID Tags," *IEEE/ACM Transactions on Networking*, vol. 24, no. 2, pp. 846-858, Apr. 2016.
- [5] P. Robyns, E. Marin, W. Lamotte, P. Quax, D. Singelée, and B. Preneel, "Physical-layer Fingerprinting of LoRa Devices Using Supervised and Zero-shot Learning," in *Proc. of WiSec*, Boston, MA, USA, Jul. 2017.
- [6] K. Merchant, S. Revay, G. Stantchev, and B. Nousain, "Deep Learning for RF Device Fingerprinting in Cognitive Communication Networks," *IEEE Journal on Selected Areas in Communications*, vol. 12, no. 1, pp. 160-167, Feb. 2018.
- [7] T. Jian, B. C. Rendon, E. Ojuba, N. Soltani, Z. Wang, K. Sankhe, A. Gritsenko, J. Dy, K. Chowdhury, and S. Ioannidis, "Deep Learning for RF Fingerprinting: A massive Experimental Study," *IEEE Internet of Things Magazine*, vol. 3, no. 1, pp. 50-57, Mar. 2020.
- [8] 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.
- [9] Y. Yang, Y. Li, W. Zhang, F. Qin, P. Zhu, and C. Wang, "Generative-Adversarial-Network-Based Wireless Channel Modeling: Challenges and Opportunities," *IEEE Communications Magazine*, vol. 57, no. 3, pp. 22-27, Mar. 2019.
- [10] M. Patel, X. Wang, and S. Mao, "Data Augmentation with Conditional GAN for Automatic Modulation Classification," in *Proc. of WiSec*, Linz, Austria, Jul. 2020.
- [11] W. Lee, S. Kim, J. Ryu, and T. Ban, "Fast Detection of Disease in Livestock based on Deep Learning," *Journal of the Korea Institute of Information and Communication Engineering*, vol. 21, no. 5, pp. 1009-1015, May. 2017.