Deep-Learning-Aided RF Fingerprinting for NFC Security

Woongsup Lee, Seon Yeob Baek, and Seong Hwan Kim

The authors discuss the feasibility of RF fingerprinting assisted by deep learning for use in identifying NFC tags. They implement a hardware testbed with an off-the-shelf NFC reader and software defined radio. An RF signal corresponding to one-bit transmission from the NFC tag is used to extract the RF characteristics, which enables rapid identification.

Abstract

Given the ever increasing use of near field communication (NFC), the security of this system is becoming increasingly important. Recently, radio frequency (RF) fingerprinting, where the physical RF characteristics of a communication device are used as a means to provide guarantees of authenticity and security, has received serious consideration due to the uniqueness of these characteristics, making cloning difficult. In this article, we discuss the feasibility of RF fingerprinting assisted by deep learning for use in identifying NFC tags. To this end, we implement a hardware testbed with an off-the-shelf NFC reader and software defined radio. An RF signal corresponding to one-bit transmission from the NFC tag is used to extract the RF characteristics, which enables rapid identification. Three different types of deep neural network are used, namely fully connected layer-based neural network,, convolutional neural network, and recurrent neural network. By experiment, we confirm that deep-learning-based algorithms can uniquely distinguish 50 NFC tags with up to 96.16 percent accuracy. We also discuss some of the key technical challenges involved in the use of deep-learning-based RF fingerprinting for NFC.

Introduction

The use of radio frequency identification (RFID) has exploded over the past few decades, leading to innovations in logistics, retail, and payment methods, and contributing to the realization of smart environments. Near field communication (NFC) is one of most widely used RFID standards when the communication range is short, that is, 10 cm for the proximity type and 1 m for the vicinity type. Its short range of communication means that NFC technology has been recognized as a safer method of protection against eavesdropping than other communication technologies such as cellular communication. However, passive RFID, including NFC tagging mode, is not a candidate for use of conventional cryptographic algorithms due to its limitations in terms of both memory capacity and computation ability. As a consequence, the crytographic algorithms of RFID are easily broken, and RFID tags can be easily cloned [1]. Moreover, NFC is also vulnerable to man-in-the-middle attack, which implies that contactless payment based on NFC may be problematic. Accordingly, it is important to devise safer security measures to tackle the security risks associated with NFC.

RF fingerprinting is an identification scheme based on unique characteristics observed in signal transmission, which are regarded as the fingerprint of the device. This technique relies on the fact that every transmitter generates device-specific distortion in its analog signal, caused by unique distortion in its analog hardware components. RF fingerprinting has been studied since the 1940s and considered for various communication systems as a means of authentication. In [2], an attempt was made to classify eight WiFi devices according to the waveforms generated by each device where a probabilistic neural network (PNN) was used. The authors of [3] exploited RF fingerprinting to suppress signaling traffic generated during the authentication process in femtocells of a cellular network using the unique RF characteristics of the Universal Mobile Telecommunications Service (UMTS) random access channel (RACH) preamble transmitted by devices. In [4], the classification of six mobile phones was investigated through the extraction of the differential constellation trace figure from radio signals.

RF fingerprinting was also applied to NFC to enhance security by providing better means of identification [5–7]. The response from the NFC tag was used to extract the RF characteristics to identify the NFC tags from the same and different manufacturers in [5, 6]. Furthermore, the authors of [7] used the reader inquiry signal to extract the RF characteristic by exploiting the inductive coupling nature of NFC. In addition, RF fingerprinting was also considered in [1, 8] as an identification method for far-field UHF RFID that operates in the 860–960 MHz frequency range, where 100 and 150 UHF RFID tags were distinguished.

In most cases, manual extraction of unique RF characteristics is difficult, and either statistical analysis or machine learning algorithms are generally used. Recently, the deep learning technique, which has seen a surge in interest in the field of communication, has begun to see application in RF fingerprinting in order to improve the accuracy of identification further [9–11]. The authors of [9] proposed convolutional neural network (CNN)-based RF fingerprinting with zero-shot learning to identify 22 LoRa devices. CNN-based RF fingerprinting was proposed, and their experiments allowed seven ZigBee devices [10] and six mobile phones [4] to be identified uniquely. Finally, more than 10,000 WiFi and ABS-S devices were iden-

Woongsup Lee is with Gyeongsang National University; Seon Yeob Baek is with the Affiliated Institute of the Electronics and Telecommunications Research Institute; Seong Hwan Kim (corresponding author) is with Korea National University of Transportation.

Digital Object Identifier: 10.1109/MCOM.001.2000912

tified using CNN-based RF fingerprinting in [11]. However, to the best of our knowledge, there are no reports in the literature of deep-learning-based RF fingerprinting used for the identification of NFC tags.

In this article, we focus on deep-learning-assisted RF fingerprinting for the identification of NFC tags. First, we provide a comprehensive explanation of NFC transmission protocols and security in NFC. We then describe our hardware testbed based on a software defined radio (SDR) and an off-the-shelf NFC reader, supported by a deep neural network (DNN) structure consisting of either a fully connected layer-based neural network (FNN), a CNN, or a recurrent neural network (RNN). The performance of deep-learning-aided RF fingerprinting is evaluated, confirming that 50 NFC tags from the same batch can be distinguished uniquely with up to 96.16 percent accuracy. In addition, some of the key future technical challenges involved in the use of RF fingerprinting in NFC are also discussed.

Background

In this section, an explanation is given of the NFC transmission protocol and other existing schemes to provide secure transmission in NFC. The existing identification methodologies for NFC based on RF fingerprinting are described, together with their limitations.

NFC Transmission Protocol

There are three modes of operation in NFC:

- NFC reader/writer mode, in which the NFC reader writes or obtains information in NFC tags such as a contactless smartcard
- NFC peer-to-peer mode in which two NFC devices communicate with each other as peers
- NFC card emulation mode in which devices with NFC capability act like smartcards for contactless payment, ticketing, and so on

In our experiments, we use the NFC reader/writer mode, given its widespread use for many tasks such as access control and transactions where the identification of tags is important; furthermore, it is possible to test many tags at low cost using this mode. Nevertheless, the proposed method could be applied to other modes as well.

In the NFC reader/writer mode, various types of NFC tags can be implemented by combining different specifications. Among the different types, Type 2 tags that follow ISO/ICE 14443A are the most widely used because they provide enough functionality to meet a wide range of needs, including low-value transactions and ticketing. Accordingly, we consider Type 2 tags in our experiments.

We now briefly describe the handshake process used between an NFC reader and a tag as defined in ISO/ICE 14443A-3. Initially, an NFC tag is in the <POWER-OFF> state. After the tag senses the reader's signal, it changes state to <IDLE>. Then the tag receives a REQuest command, Type A (REQA) message from the reader and changes its state to <READY> before sending an Answer To reQuest, Type A (ATQA) message as the response to the REQA message. Each ATQA message consists of 2 bytes of information. Given that the rate of transmission of the data is about 106 kb/s, the transmission of each bit takes 9.43 ms. For tag-to-reader transmission, the Manchester code is used to encode the data such that the signal representing logic 1 is composed of four pulses in the first half of each bit, while the signal representing logic 0 is composed of four pulses in the second half.

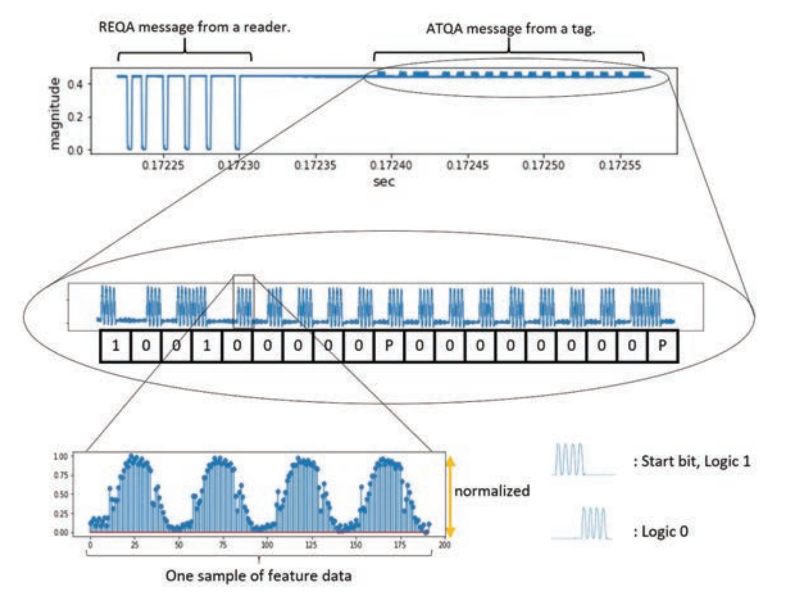

FIGURE 1. REQA and ATQA messages in ISO/IEC 14443A.

Figure 1 depicts the measured amplitude of a signal that contains REQA and ATQA messages. We note that the variation in amplitude in the REQA message is greater than that in the ATQA message because 100 percent of the amplitude shift keying (ASK) is used in reader-to-tag communications, while load modulation, which partially changes the current flowing through the coil antenna, is used in tag-to-reader communication. The ATQA message shown in the figure is composed of 19 bits. The starting bit of the ATQA message indicates the beginning of the ATQA message, and two P symbols among the logical values correspond to the parity bits for the first and last sets of 8 bits.

Security of NFC

In NFC, a tag automatically responds to an NFC reader's initiation provided that the reader and the tag are in close proximity, such that the data in the tag can easily be obtained by any NFC reader. To address this vulnerability in terms of confidentiality and authenticity, NFC security standards (NFC-SEC) stipulate public key encryption/decryption [12], and several attempts have been made to enhance the authentication mechanism of NFC [13]. However, cryptography based on a public key algorithm is not readily available for low-cost NFC tags, because the processor of the NFC tag does not usually have enough computational power to process the public key algorithm. Although NFC tags are able to process the public key algorithm, attackers can exploit weaknesses in the stream cipher to read and modify memory blocks of an NFC tag; in other words, cloning attacks are possible. Moreover, the NFC is also vulnerable to a relay attack in which the attacker mimics the NFC tag or receiver by relaying the

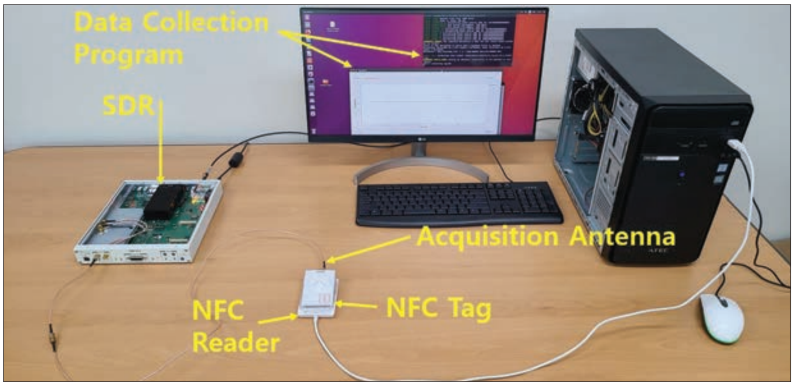

FIGURE 2. Testbed for collecting a tag's response.

data transmitted by the tag to a reader some distance away from the tag [14].

RF Fingerprinting Schemes for NFC and Their Limitations

RF fingerprinting has been considered extensively as a means of identifying NFC tags, thus enhancing the security of NFC through the prevention of cloning and counterfeiting of NFC tags [5–7]. Given that identification of the tag can be achieved at the NFC receiver using the RF signal transmitted by the tag, it is possible to overcome the low computational ability of the NFC tag. In [5], 50 NFC tags produced by the same manufacturer were tested for identification, where the tag signal was collected under a controlled environment such that the tags were placed in fixed positions with respect to the acquisition antennas, and a purpose-built NFC reader was used instead of a commercial one. The responses of the tags to arbitrarily generated high-energy bursts of a single sinusoidal carrier and a high energy linear frequency sweep were used to extract the RF fingerprint, and a matching algorithm based on inter-vector distance was used for classification. The authors of [6] used the higher order statistical features of the ATQA envelope as a fingerprint for tag identification, and a feature-matching process based on distance was developed to identify NFC tags from six different manufacturers. In [7], the RF characteristics of tags were extracted from the reader inquiry part instead of the tag response part, and the NFC tags from four different manufacturers were identified.

Although schemes based on RF fingerprinting as described above can identify NFC tags with high accuracy, they have several drawbacks that hinder their application in a practical system. More specifically, either a purpose-built NFC reader [5] or an oscilloscope capable of a high sampling rate [7] were used, which are not readily available in practice. Moreover, the classification of tags from different manufacturers were considered in [6, 7], and NFC tags from the same manufacturer were not identified correctly. Furthermore, the quantity of RF data was generally rather small in previous work; for example, just 30 REQA-ATQA signal samples were collected in [6].

With the aim of addressing the drawbacks of the previous approaches, we apply cutting-edge deep learning techniques for RF fingerprinting in NFC. To be more specific, massive amounts of RF data, corresponding to 158,620 RF signal samples per tag, were collected using an off-the-shelf NFC reader, and all NFC tags used in our experiments were obtained from the same manufacturer and the same batch, meaning that our approach is more appropriate for practical systems. Moreover, various DNN models were adopted for the extraction of diverse RF features from the data in order to achieve high accuracy of identification. Finally, only one bit length of each tag response is used to extract the RF fingerprint, which enables rapid identification of the tag.

Deep-Learning-Aided RF Fingerprinting

In this section, we demonstrate RF fingerprinting based on deep learning for NFC tag identification. To this end, we first describe the implementation of the hardware used to collect the RF data from the tag. We then describe the methodology used to collect and pre-process the RF data. Finally, we discuss the DNN structures used for the identification of the tags. The video demonstration that shows the operation of our implementation can be found in [15].

Testbed for NFC Transmission

The hardware testbed used is shown in Fig. 2. Our testbed comprises an SDR, an NFC reader, an acquisition antenna, and a desktop. An SDR is a radio communication device that can change its operation flexibly with software. In our testbed, we used a universal software radio peripheral (USRP) X300 with UBX160 daughter board by Ettus Research, and this USRP device is connected to a desktop running software to capture the tag response using the GNURADIO library. The RF input port of the USRP is connected to a coil antenna used for inductive coupling with the antenna of a reader and a tag. Moreover, ACR 122 is used as the NFC reader.

An NFC tag is placed on an NFC reader at a fixed position, and the acquisition antenna is placed between the tag and reader to join the inductive coupling with a reader and tag and sense the changes in the electromagnetic wave. We consider tags following ISO/IEC 14443 type A and use a sampling rate of 40 Msamples/s and a carrier frequency of 20.4 MHz to collect the signal containing the ATQA message from the tag. The RF signal is gathered for a duration of approximately 18 minutes for each tag where the NFC reader continuously queries the tag during this period such that the RF signals from a large number of REQA and ATQA messages are assembled. Note that the accumulated RF signal data is used for the training and test of the considered NFC tag identification scheme, and we have utilized a long data acquisition time to collect a sufficiently large amount of RF signal data. During the collection of the RF data, only the magnitude of the RF signal is recorded. It should be noted that all tags come from the same manufacturer and batch, which suggests small difference in the RF characteristics among tags.

Data Collection and Pre-Processing of Data

First, we refine and split the collected RF signal data into multiple samples, which constitute the training and test dataset for our DNN model. In this article, only the RF signal of the ATQA message is used to create these samples because this signal is transmitted from the tag, so it contains the unique RF characteristics of each tag, which are used for its identification later on. Note that one bit of the ATQA message always contains four pulses (Fig. 1), where the shape of the envelope of each of these pulses is slightly different according to the unique RF characteristics of each tag. Accordingly, we separate these four sequential pulses belonging to the same bit and use these sliced pulses for tag identification. The use of these pulse data as the feature data for our DNN model is also beneficial because these will be always transmitted by the tag regardless of the bit sequence of the ATQA message.

Given that the duration of one bit is 9.43 ms and the sampling rate is 40 Msamples/s, four pulses that occupy half of each 1 bit duration are composed of 188 points, where each point corresponds to the magnitude of the pulses at each instant. In order to allow for the possible inaccurate detection of the starting point of a pulse, we add two more points at the start and end, respectively, such that the feature data are composed of 192 points in all. In addition, we adjust the quantity of feature data used to train the DNN models to be the same for all tags in order to balance the size of the training dataset for each label and thus prevent bias in the prediction. As a result, 158,620 samples are used for each NFC tag, and 7,931,000 samples are used in total. It is worth mentioning that our proposed method of identification can determine each tag by observing the signal that corresponds to one bit of the message, allowing instant execution.

Having obtained the feature data through slicing, we normalize the scale of the data such that the maximum and minimum of the data points in the feature data are 1 and 0, respectively. Normalization of the feature data is vital because the scale of the RF signal that corresponds to the ATQA message is very small (Fig. 1), which can deteriorate the training performance of the DNN models. Moreover, if we do not normalize the feature data properly, the absolute value of the RF signal itself could be used by the DNN models, which could hinder the discovery of the true RF characteristics of the tags (i.e., the unique pattern of the pulse shape).

In Fig. 3, we show samples of the collected RF signal data from three NFC tags, whose indices are 1, 18, and 20, respectively, where top, middle, and bottom figures correspond to randomly selected RF signal data from each tag. The samples of the RF signal data for a complete set of tags can be found in [15]. From the figure, we confirm that each set of RF signal data is composed of four pulses, as expected. Moreover, we observe that pulses from different tags have a similar shape, so it is hard to find the unique pattern from the shape, whereas the shapes of the pulses collected from the same tag are slightly different for each sample. Accordingly, we confirm that finding the unique characteristics (i.e., the fingerprint) of the RF signal manually is somewhat challenging.

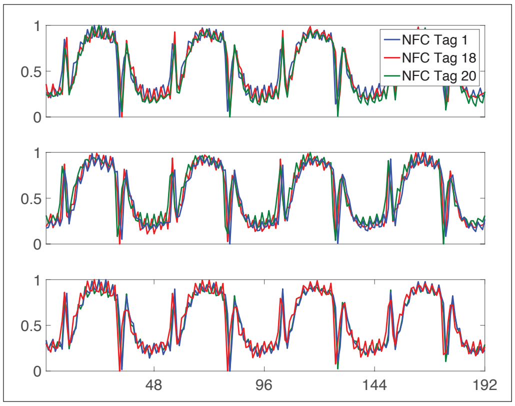

FIGURE 3. Samples of RF signal data collected from NFC tags 1, 18, and 20.

Note that the accumulated RF signal data is used for the training and test of the considered NFC tag identification scheme, and we have utilized long data acquisition time to collect a sufficiently large number of RF signal data. During the collection of the RF data, only the magnitude of the RF signal is recorded.

DNN Models for RF Fingerprinting on NFC

We consider three different types of DNN models for RF fingerprinting for NFC tags, namely FNN, CNN, and RNN. First, FNN, which is one of the most basic DNN structures, is composed of sequentially connected layers of hidden nodes, where the output of each hidden node is forwarded to all hidden nodes in the subsequent layer. The input of the considered FNN is the RF signal data, pre-processed according to the methodology described in the previous section, and the output of the FNN is the probability distribution that each tag is detected. Consequently, the number of inputs and outputs are 192 and 50, respectively. In this article, we consider FNN with 6 fully connected layers, where the number of hidden nodes for each layer is set to 256. Moreover, the rectified linear unit (ReLU) is employed as an activation function such that the negative inputs to the layers are blocked by the ReLU. The last layer of the FNN is fed into the softmax function whose number of outputs is the same as the total number of NFC tags (i.e., 50). Given that the output of the softmax function is non-negative and the sum of all outputs is always 1, this output can be regarded as the probability of the presence of each tag.

Second, CNN is widely used to extract spatial features from input data, and is taken into account here. For the CNN considered, the input and output are the RF signal data and the probability distribution for each NFC, as for FNN. In the CNN, the input data are first fed into 6 convolutional layers, that execute one-dimensional convolution in which the size of the kernel and the number of filters are set to 6 and 128, respectively. Then the output of these convolution layers is fed into one fully connected layer with 256 hidden nodes. As for FNN, the last layer of the CNN is fed into the softmax function in order to determine the probability that each tag is detected.

Third, RNN is mainly used to deal with sequential data, and is also considered here. We use a gated recurrent unit (GRU)-based RNN, which is a simpler variant of long short-term memory (LSTM), with 100 memory cells. Unlike FNN and CNN in which 192 data points of feature data are fed in simultaneously, the RNN takes these data points one by one, and the internal state of the RNN is updated according to each sequence of input data. The last of the data, the internal state of the memory, is forwarded to the softmax function, as for FNN and CNN.

During training, cross entropy is used as a loss function, and the dropout and batch normalization are employed to prevent overfitting and improve the training performance. Moreover, an Adaptive Moment Estimation (Adam) gradient descent algorithm is used to update the weights and biases of the DNNs. Subsequent to the train-

Algorithm	Precision	Recall	Accuracy	F1-score
FNN	0.9616	0.9616	0.9616	0.9614
CNN	0.9498	0.9499	0.9499	0.9498
RNN	0.9611	0.9609	0.9609	0.9608
LR	0.3898	0.3547	0.3547	0.3487
RAF	0.2955	0.3004	0.3004	0.2753
SVM	0.3876	0.3938	0.3938	0.3842

TABLE 1. Performance comparison of considered algorithms.

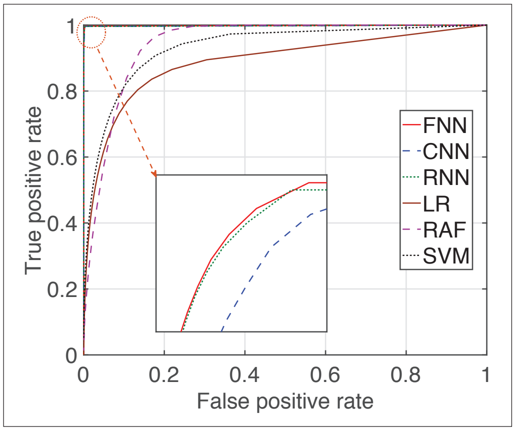

FIGURE 4. ROC curve of the considered algorithms.

ing, the NFC tag can be identified by feeding in RF signal data containing four pulses from the ATQA message, where the output of the DNN with the highest value is chosen as the index of the tag.

Experimental Results

In this section, we discuss the performance of deep-learning-based RF fingerprinting for NFC tag identification. In the performance evaluation, the RF signal data is collected using the testbed through the procedure described earlier. A and B, where 90 percent of the collected RF signal data is used for training, and the rest of the data is used for evaluation; that is, the training and test sets comprise 7,137,900 and 793,100 samples, respectively. Note that in the practical implementation, the output of the testbed, which is the RF signal of a tag, is pre-processed and then becomes the input of the DNN structure, which determines the index of the tested tag.

For comparison, we consider three popular machine-learning-based algorithms: logistic regression (LR), random forest (RAF) with 200 decision trees with the maximum depth of 6, and support vector machine (SVM) with a linear kernel.

In Table 1, we show the classification performance of the considered algorithms, where the precision, recall, accuracy, and F1-score are used as performance metrics. Since the identification of NFC tags is a multi-class problem, we have averaged the performance metrics obtained for each tag to obtain the performances given in Table I. Note that the accuracy of the baseline performance using the ZeroR classifier that selects the most popular class is only 0.02.

As can be seen from the results, all the considered algorithms provide performance far better than that of the baseline scheme, and the performance of the deep-learning-based algorithms also surpasses that of conventional machine-learning-based algorithms. In particular, FNN achieves 96.16 percent accuracy, which is sufficiently high compared to previous work on RF fingerprinting. The accuracy of CNN is the lowest among all the deep-learning-based algorithms considered, but it is still greater than 94.9 percent, which is also high. It is worth noting that although we use only a small portion of the signal, corresponding to one bit of an ATQA message, the NFC tag can still be identified with high accuracy.

In Fig. 4, we show the receiver operating characteristic (ROC) curve for the considered algorithms. The area under the curve (AUC) is measured as 0.9983, 0.9978, 0.9980, 0.89, 0.9405, and 0.9331 for the FNN, CNN, RNN, LR, RAF, and SVM, respectively, where a higher AUC indicates better classification performance. As expected from the performance comparison in Table 1, the deep-learning-based algorithms FNN, CNN, and RNN show better ROC curves and higher AUC than the conventional machine-learning-based algorithms LR, RAF, and SVM. Furthermore, we find that FNN and CNN provide the best and worst performance among all the deep-learning based algorithms considered, which also coincides with the results in Table 1.

Finally, in Fig. 5 we show the confusion matrix for 13 randomly selected NFC tags with FNN, where each row and column correspond to the true and predicted tag index. The confusion matrices for a complete set of tags and the other algorithms can be found in [15]. In the confusion matrix, we note that all the diagonal elements are close to 1, and all off-diagonal elements are close to 0, which reveals that NFC tags are identified with high accuracy. It is interesting to note that the confusion matrix is near-symmetric, such that when tag A is misidentified to tag B with a high probability, tag B is also likely to be misidentified to tag A with a high probability. For example, in Fig. 5, we note that the probability that tag 18 is misclassified to tag 20 is high, while the probability of the reverse case is also high.

Research Challenges

In the following, we discuss some of the research challenges connected with the future use of RF fingerprinting to improve security in tag identification.

Collection of Training Data: In order to achieve high accuracy in RF fingerprinting using deep learning, a large number of training samples need to be collected. For example, in our implementation, the RF signal data were measured for 18 minutes on each NFC tag. In practice, it can be hard to obtain a sufficient number of training samples for each tag. A deep learning algorithm based on a generative model, for example, a generative adversarial network (GAN), capable of generating realistic synthetic training data can be used to solve problems encountered in the collection of training samples.

Lack of Interpretability: Given that the physical RF characteristics of an NFC tag are found through DNN, it is difficult to be clear on the key differences in RF characteristics that discriminate between tags. This lack of interpretability can limit the application of RF fingerprinting because its operation can be unpredictable, and also hinder meaningful insights regarding RF characteristics of tags. Explainable artificial intelligence (XAI) can be used to solve this problem.

Varying Channel Dynamics: The wireless channel condition between NFC tag and reader can change significantly according to the configuration, for example, the distance between tag and reader and the orientation of the NFC tag on the reader. As a consequence, the shape of the RF signal can change according to variations in wireless channel conditions, which could possibly affect the tag identification. To solve this problem, RF signal data must be collected under various channel conditions such that DNN models can cope with varying channel conditions.

Optimal DNN Structure: In our implementation, three different off-the-shelf DNN structures are considered. However, in order to further improve the accuracy of NFC tag identification, an optimized DNN structure that takes into account the characteristics of RF signal from NFC tag has to be designed.

Conclusions

We have considered deep-learning-based identification of NFC tags using RF fingerprinting as a means of enhancing the security of NFC by preventing the cloning attack. The performance of the considered identification scheme has been verified using real RF signals obtained by a hardware testbed composed of an off-the-shelf NFC reader and an SDR device, where 50 NFC tags from the same batch have been classified. Through evaluation, we have confirmed that among all considered DNN structures, which are FNN, CNN, and RNN, the FNN achieves the highest accuracy for tag identification with 96.16 percent accuracy, while all DNN structures achieve comparably higher accuracy than conventional machine-learning-based algorithms. We have also confirmed that the proposed scheme can extract the unique pattern from RF signal corresponding to one-bit transmission, which enables rapid identification of tags.

Acknowledgment

This research was supported in part by the Affiliated Institute of the Electronics and Telecommunications Research Institute (ETRI), in part by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2018R1D1A1B07040796), and in part by Korea National University of Transportation in 2020.

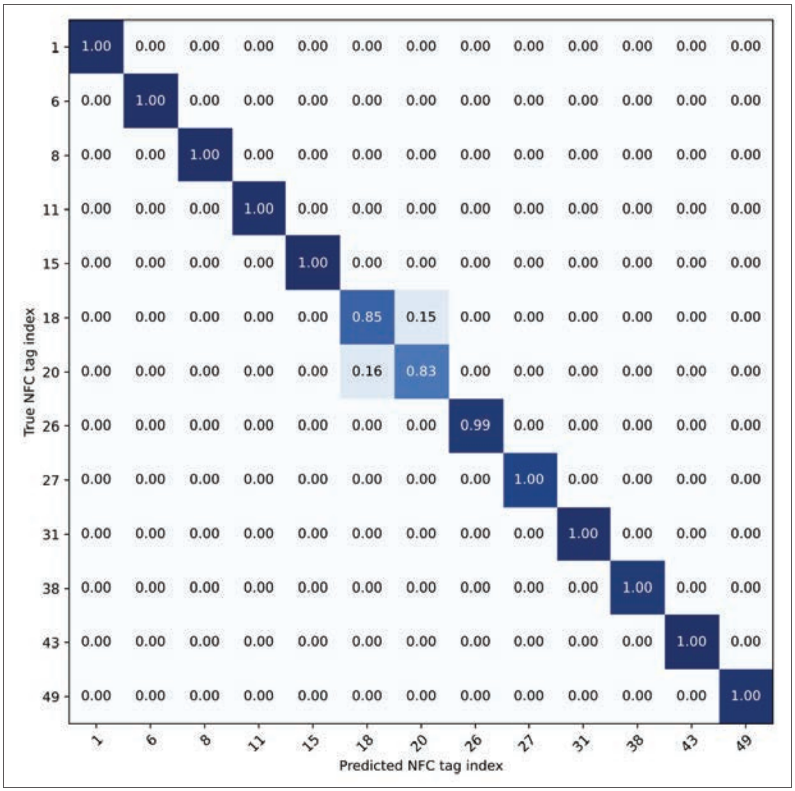

FIGURE 5. Confusion matrix for selected NFC tags with FNN.

References

[1] S. C. G. Periaswamy, D. R. Thompson, and J. Di, "Fingerprinting RFID Tags," *IEEE Trans. Depend. Sec. Comp.*, vol. 8, no. 6, Nov. 2011, pp. 938–43.

[2] O. Ureten and N. Serinken, "Wireless Security Through RF Fingerprinting," *Canadian J. Elect. Comp. Eng.*, vol. 32, no. 1, May 2007, pp. 27–33.

[3] I. O. Kennedy *et al.*, "Radio Transmitter Fingerprinting: A Steady State Frequency Domain Approach," *Proc. VTC-Fall*, Calgary, Canada, Sept. 2008.

[4] S. Wang *et al.*, "A Convolutional Neural Network-Based RF Fingerprinting Identification Scheme for Mobile Phones," *Proc. IEEE INFOCOM*, Toronto, Ontario, Canada, July 2020.

[5] B. Danev, T. S. Heydt-Benjamin, and S. Capkun, "Physical-Layer Identification of RFID Devices," *Proc. USENIX Security Symp.*, Montreal, Canada, Aug. 2009.

[6] G. Zhang *et al.*, "Physical-Layer Identification of HF RFID Cards Based on RF Fingerprinting," *Proc. ISPEC*, Zhangjiajie, China, Nov. 2016.

[7] H. P. Romero *et al.*, "Electromagnetic Measurements for Counterfeit Detection of Radio Frequency Identification Cards," *IEEE Trans. Microwave Theory Tech.*, vol. 57, no. 5, May 2009, pp. 1383–87.

[8] J. Han *et al.*, "GenePrint: Generic and Accurate Physical-Layer Identification for UHF RFID Tags," *IEEE/ACM Trans. Net.*, vol. 24, no. 2, Apr. 2016, pp. 846–58.

[9] P. Robyns *et al.*, "Physical-Layer Fingerprinting of LoRa Devices Using Supervised and Zero-Shot Learning," *Proc. WiSec*, Boston, MA, July 2017.

[10] K. Merchant *et al.*, "Deep Learning for RF Device Fingerprinting in Cognitive Communication Networks," *IEEE JSAC*, vol. 12, no. 1, Feb. 2018, pp. 160–67.

[11] T. Jian *et al.*, "Deep Learning for RF Fingerprinting: A Massive Experimental Study," *IEEE Internet of Things Mag.*, vol. 3, no. 1, Mar. 2020, pp. 50–57.

[12] ISO/IEC Std. ISO/IEC 13157-2:2016, "Information Technology Telecommunications and Information Exchange Between Systems — NFC Security — Part 2: NFC-SEC Cryptography Standard Using ECDH and AES," 2016.

[13] M. Q. Saeed and C. D. Walter, "Off-Line NFC Tag Authentication," *Proc. ICITST*, London, U.K., Dec. 2012.

[14] Y.-J. Tu and S. Piramuthu, "On Addressing RFID/NFC-Based Relay Attacks: An Overview," *Decision Support Sys.*, vol. 129, art. no. 113194, Feb. 2020.

[15] "Additional Results"; https://github.com/seotaijiya/NFC_DATA, accessed Dec. 29, 2020.

Biographies

Woongsup Lee [S'07, M'13] (wslee@gnu.ac.kr) received his B.S. and Ph.D. in electrical engineering from the Korea Advanced Institute of Science and Technology (KAIST) in 2006 and 2012, respectively. Since 2014, he has been with the Department of Information and Communication Engineering at Gyeongsang National University, South Korea, where he is now an associate professor.

Seon Yeob Baek [S'04, M'11] (sybaek@nsr.re.kr) received his B.S. and Ph.D. degrees in electrical engineering from KAIST in 2003 and 2010, respectively. Since 2010, he has been with the Affiliated Institute of the Electronics and Telecommunications Research Institute, South Korea, where he is a principal researcher.

Seong Hwan Kim [S'07, M'14] (seonghwan.kim@ut.ac.kr) received his B.S. degree in electrical engineering from Korea University in 2006, and his M.S. and Ph.D. degrees in electrical engineering and computer science from KAIST in 2008 and 2013, respectively. Since 2020, he has been an associate professor with the Major of Data Science, Korea National University of Transportation.