NFChain: A Practical Fingerprinting Scheme for NFC Tag Authentication

Yanni Yang*, Jiannong Cao†, Zhenlin An†, Yanwen Wang‡, Pengfei Hu*, Guoming Zhang*
*School of Computer Science and Technology, Shandong University, Qingdao, China.
†Department of Computing, The Hong Kong Polytechnic University, Hong Kong, China.
‡College of Electrical and Information Engineering, Hunan University, Changsha, China.

IEEE INFOCOM 2023 - IEEE Conference on Computer Communications | 979-8-3503-3414-2/23/$31.00 ©2023 IEEE | DOI: 10.1109/INFOCOM53939.2023.10229040

***Abstract*—NFC tag authentication is highly demanded to avoid tag abuse. Recent fingerprinting methods employ the physical-layer signal, which embeds the tag hardware imperfections for authentication. However, existing NFC fingerprinting methods suffer from either low scalability for a large number of tags or incompatibility with NFC protocols, impeding the practical application of NFC authentication systems. To fill this gap, we propose NFChain, a new NFC fingerprinting scheme that excavates the tag hardware uniqueness from the protocol-agnostic tag response signal. Specifically, we harness an agile and compatible frequency band of NFC to extract the tag fingerprint from a chain of tag responses over multiple frequencies, which significantly improves fingerprint scalability. However, extracting the desired fingerprint encounters two practical challenges: (1) fingerprint inconsistency under different NFC reader and tag configurations and (2) fingerprint variations across multiple measurements of the same tag due to the signal noise in generic readers. To tackle these challenges, we first design an effective nulling method to eliminate the effect of device configurations. Second, we employ contrastive learning to reduce fingerprint variations for accurate authentication. Extensive experiments show we can achieve as low as 3.7% FRR and 4.1% FAR for over 600 tags.**

***Index Terms*—NFC tag, physical-layer hardware fingerprinting, authentication.**

I. Introduction

Near-field communication (NFC) has now become a critical data exchange approach in wireless communication, which has widespread adoption in industries and people's daily lives. The COVID-19 pandemic has been further accelerating such contact-free communication in commercial scenarios in terms of packaging, tracking, and anti-counterfeiting [1]–[3]. The global NFC market size was valued at $15 billion in 2019 and is estimated to experience significant growth and reach over $54 billion by 2028 [4], [5]. Such prosperity of the NFC market facilitates its versatility for more commercial use.

A core function of NFC is anti-counterfeiting, which, however, can be easily destroyed by adversaries. This is because the data stored in the NFC tag can be easily duplicated by common NFC readers and written into empty tags to be forged. To avoid the leakage of tag information, many cryptographic algorithms, e.g., hashing and asymmetric cryptography [6]–[8], are applied to encrypt the NFC tag data. Unfortunately, the limited power supply and storage capability of the NFC tag constrain the implementation of many advanced encryption methods. Compared with software-based encryption, adding specialized hardware to the tag could bring extra computation ability [7]. However, such modification to the NFC tag incurs high deployment costs for large-scale uses [9].

*Pengfei Hu is the corresponding author.

TABLE I
Comparison with previous works

Work	Fingerprint	Scale	Device	Compat.
[11]	TSE	20	O-scope	✓
[13]	TR envelop+spectral	50	AWG+O-scope	✗
[14]	TR spectral	50	AWG+O-scope	✗
Our	**multi-frequency TRAs**	**>600**	**emulated reader**	✓

To tackle the above limitations, the tag physical-layer (PHY) signal has been investigated to extract a hardware fingerprint for tag authentication [10]–[14]. The underlying principle of PHY-based tag fingerprinting is that distinct manufacturing imperfections in tags' hardware (e.g., circuit and antenna coil) can be regarded as the tag fingerprint, which is involved in the tag's PHY signal. Such a fingerprint reflects the inherent hardware properties of the tag, which is difficult to tamper with and does not require any modification on the tag.

However, existing PHY-based NFC fingerprinting solutions are far from wide application due to unscalability and incompatibility issues, as summarized in Table I. A typical solution [11] employs the transient signal envelop (TSE) between the reader-tag communication on the resonant frequency (i.e., 13.56 MHz). However, the tiny envelop difference on a single frequency only differentiates a maximum of 20 NFC tags. Other works [13], [14] compare the spectral features of the tag reaction (TR) under the 10 V burst interrogation signal with out-of-specification frequencies for a maximum of 50 tags. Such a specialized burst signal is, however, incompatible with existing NFC protocols and hinders the normal NFC communication process. Moreover, most existing works are implemented under a fixed and strictly controlled laboratory environment using purpose-built devices (e.g., waveform generator and oscilloscope) [13]–[16]. In sum, previous solutions lack the ability to distinguish a large number of NFC tags in practical scenarios and realize real-world deployment.

To fill the above gap, we propose a new NFC fingerprinting scheme called NFChain. Our key observation is that previous works mainly stick to interrogating tags using signals with a single carrier wave (CW) frequency. These single-frequency schemes simplify the fingerprinting extraction process, which, however, is hard to differentiate a large number of NFC tags due to the extremely small hardware difference. In contrast, we find that (1) NFC tags actually can be agilely activated over

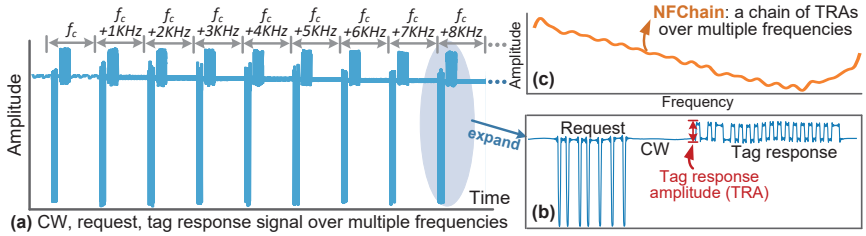

Fig. 1. (a) The PHY CW, request, tag response signal over multiple CW frequencies (ISO/IEC 14443 Type A). The frequency starts from f_c =13.56 MHz with an interval of 1KHz. (b) illustration of tag response amplitude (TRA). (c) a chain of TRAs over multiple frequencies.

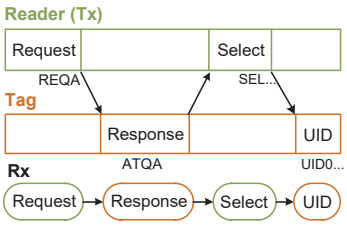

Fig. 2. The communication process between NFC reader and tag of the ISO/IEC 14443 Type A and B standard.

a wide frequency band and (2) The tag hardware manifests distinctive frequency responses, thus presenting different reactions to interrogation signals with varying frequencies. The above findings intrigue us to break the stereotype of NFC operating at a single frequency. We are the first to employ a wide frequency band in NFC for tag fingerprint extraction, which significantly enhances the fingerprint distinguishably even for an increasing number of tags. Specifically, we design a frequency hopping mechanism to automatically sweep the CW frequency within 13.56-13.76 MHz with an interval of 1 KHz to sequentially interrogate NFC tags, as shown in Fig. 1(a). Then, we employ the protocol-agnostic tag response to each interrogation signal for fingerprint extraction. We notice that NFC communication always starts with a request signal to interrogate the tag, after which the tag gives a response, as the example shown in Fig. 1(b). Then, we extract the *a chain of tag response amplitude (TRA)* over multiple CW frequencies (Fig. 1(c)), which is determined by the tag hardware components, as the unique tag fingerprint. NFChain does not rely on specialized interrogation signals and complies with FCC regulations [17] and current NFC protocols and readers. Besides, NFChain is implemented on emulated NFC readers using commodity antennas and generic software-defined radio (SDR) devices.

However, implementing NFChain for practical tag authentication encounters two major challenges. The first challenge stems from the reader diversity and tag placement. Specifically, NFC readers, even fabricated by the same manufacturer, manifest variations in their front end. Such variations result in different frequency responses, which significantly deviate the TRAs over multiple frequencies of the same tag. In addition, the tag can be arbitrarily placed on different positions relative to the reader's antenna, which affects the amount the energy harvested by the tag and the corresponding TRAs. As a result, the same tag's fingerprint measurements become inconsistent and lose effect with the change of reader and tag placement.

To address the fingerprint inconsistency, we first conduct theoretical modeling of the NFC PHY signal and investigate key factors (i.e., reader frequency responses and coil coupling coefficient) corresponding to the reader and tag placement effects. Then, we propose a simple yet effective factor nulling method. The underlying principle is to carefully design two benchmark signals from the CW and tag response signals, which inherently involve the same reader and tag displacement effects as the tag response over multiple frequencies. The designed benchmark signals are harnessed to null the corresponding factors for obtaining a consistent tag fingerprint.

Another major challenge comes from the noisy PHY signal collected from the generic radio frequency (RF) device. Previous works employ high-end but costly signal generators and acquisition devices to obtain a high-quality and precise PHY signal. In contrast, the PHY signal from cost-effective generic RF devices suffers from relatively strong noises, introducing undesired fluctuations in extracted TRAs. Concerning the tiny hardware difference among tags, such fluctuations can easily obfuscate different tags' fingerprints. Therefore, an effective method is required to narrow the differences among fingerprint measurements for the same tag under noises.

To achieve the above target, we borrow the idea of contrastive learning and develop a neural network model to learn an embedding space in which we can minimize the difference among the same tag's fingerprints. Through our delicate design of the network architecture and a contrastive loss function, fingerprint measurements of the same tag are highly similar to each other in face of PHY signal noises. Meanwhile, the difference in fingerprints from different tags is surprisingly magnified. The authentication accuracy is significantly improved using our designed model.

In sum, our work makes the following contributions:

- We design a new NFC fingerprinting scheme, NFChain, which takes advantages of an agile frequency band to extract a protocol-agnostic tag fingerprint and significantly enhance authentication scalability.
- We develop a series of effective methods to ensure the consistency of the tag fingerprint under practical settings and enhance the tag authentication performance with a novel design of the authentication model.
- We evaluate NFChain using over 600 NFC tags (10× than previous works) with 6 different models. The experimental results show that we can achieve high authentication performance with 3.7% FRR and 4.1% FAR.

II. Preliminary of NFC Communication and Design of the NFC Tag Fingerprint

In this section, we first introduce the preliminaries of the NFC communication process. Second, we demonstrate the principles of using the TRA as the NFC tag fingerprint.

A. NFC communication and the PHY signal

Current NFC protocols include ISO/IEC 14443, 15693, and 18000-3 [18]. Although these standards vary in coding and modulation, they share the same communication flow: the

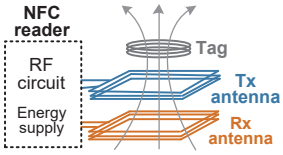

Fig. 3. Setting to capture request and response signal

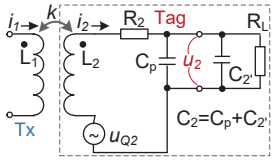

Fig. 4. Simplified circuit diagram for the reader and tag

NFC reader first sends a high-power CW signal to activate an NFC tag, followed by a request signal to initiate the NFC communication. Next, the NFC tag harvests energy from the CW signal and sends back a response. Taking an example of ISO/IEC 14443 Type A protocol in Fig. 2, the reader (i.e., transmitter Tx) first sends a request command (REQA) to the tag. After being activated, the tag sends back a response command (ATQA) to Tx. Then, the Tx sends a selection command (SEL) to the tag. Finally, the tag will report its ID.

To capture the PHY signal during NFC communication, we first connect a Tx antenna to the emulated reader using the generic SDR device, as shown in Fig. 3. Then, an NFC tag is placed above the Tx antenna. Finally, a receiver (Rx) antenna is connected to the reader beneath the Tx antenna and records the PHY signal. Fig. 1(b) illustrates the down-converted request, CW, and tag response signals of the ISO/IEC 14443 Type A protocol over a certain CW frequency.

Although different NFC protocols modulate the request signal in various ways, the tag response signal adopts the same load modulation scheme, in which a load resistor in the tag is switched on and off. The on and off states result in the low and high levels of the tag response signal, as depicted in Fig. 1(b). The distance between the high and low levels refers to the TRA, which reflects how much power the tag harvests from the Tx antenna. The amount of harvested energy is affected by tag hardware components, whose properties can vary from tag to tag due to manufacturing imperfections. As such, the TRA, which reflects the tag's hardware characteristics, has the potential to be a unique tag fingerprint.

B. Creation of NFC Tag Fingerprint from the TRA

A clear understanding of how the TRA is affected by the tag hardware is necessary for designing the tag fingerprint. We simplify the energy harvesting between reader and tag into a voltage transformer model in Fig. 4. The harvested voltage u_2 by the tag is expressed as below [19]:

$$u_2 = \frac{2\pi f \cdot k \cdot \sqrt{L_1 L_2} \cdot i_1}{\sqrt{(\frac{2\pi f L_2}{R_L} + 2\pi R_2 C_2)^2 + (1 - (2\pi f)^2 L_2 C_2 + \frac{R_2}{R_L})^2}} \quad (1)$$

where f is the CW frequency, k is the coupling coefficient between the tag and Tx antenna coils. L_1 and L_2 refer to the conduction loops of Tx antenna and tag coil, respectively. i_1 is the Tx antenna's current. C_2, R_2, and R_L denote the capacitor, coil resistance, and load resistor of the tag, respectively.

The harvested voltage u_2 measures the amount of energy harvested by the tag, which can be reflected from the amplitude of the tag response signal $y_{\text{tag}}(f,t)$ represented as:

$$y_{\text{tag}}(f,t) = A_{\text{tag}}(f) e^{-j2\pi f t}, \; A_{\text{tag}}(f) \propto u_2 \quad (2)$$

where $A_{\text{tag}}(f)$ is the tag response amplitude (TRA). Based on Eq. (1) and Eq. (2), we pinpoint two key properties that endow

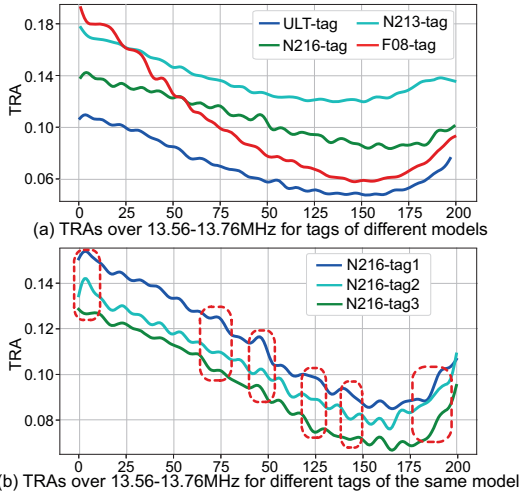

Fig. 5. TRAs over 13.56-13.76 MHz for different NFC tags

the TRA as a unique NFC tag fingerprint as follows: (1) tag hardware variations caused by manufacturing imperfections. Due to the imperfect manufacturing techniques, NFC tags, even produced by the same manufacturer, are distinct in terms of the hardware. These manufacturing imperfections cause variations of L_2, C_2, R_2 and R_L, making u_2 and A_{tag} change distinctively among different tags; (2) different TRAs under varying frequencies (f). Although NFC tag is designed to operate at the resonant frequency 13.56 MHz, in fact, it can be activated within a wider frequency band of 13.06-14.06 MHz [13], [16]. Most importantly, employing TRAs over multiple frequencies can enlarge the hardware difference among tags. In a nutshell, TRAs over a chain of frequencies $f_{\text{chain}} = [f_0, f_1, ..., f_{\text{n-2}}, f_{\text{n-1}}]$ (n is the number of frequencies), i.e., $\boldsymbol{A_{\text{tag}}(f_{\text{chain}})}$, incorporate unique tag hardware properties and can be employed as the tag fingerprint.

To show the uniqueness of the fingerprint, we conducted an exploratory experiment to collect the PHY signal and extract $\boldsymbol{A_{\text{tag}}(f_{\text{chain}})}$ from a set of NFC tags. We will introduce the details to extract the TRA in Section III-C. In this experiment, we hop the CW frequency from 13.56 MHz to 13.76 MHz with a 1 KHz interval, resulting in a chain of 201 TRAs. The extracted TRAs are depicted in Fig. 5. First, the shape of $\boldsymbol{A_{\text{tag}}(f_{\text{chain}})}$ for tags with different models (Mifare ULT, Ntag213, Ntag216, and F08) in Fig. 5(a) exhibits apparent difference. Second, for tags of the same model, we can also observe distinctive fluctuations in $\boldsymbol{A_{\text{tag}}(f_{\text{chain}})}$, as highlighted in Fig. 5(b). We further calculate the Euclidean distance among hundreds of $\boldsymbol{A_{\text{tag}}(f_{\text{chain}})}$ measurements of the 9 different tags (including tags from the same and different models) and depict the distance distribution in Fig. 6. The distance between TRAs of the same tag ('tag1-tag1') is the minimum compared with those from other tags ('tag1-tag2' to 'tag1-tag9'), showing that $\boldsymbol{A_{\text{tag}}(f_{\text{chain}})}$ can be applied to distinguish different tags.

Finally, we analyze the feature space of the designed fingerprint. Common SDR devices, e.g., HackRF, have an 8-bit ADC, which enables the normalized amplitude with a resolution of $1/2^8 \approx 3.9 \times 10^{-3}$. Our extensive experiments on various types of NFC tags show that a single-frequency

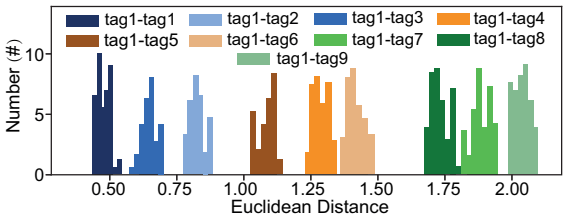

Fig. 6. Distance distribution of the tag response amplitude curve among multiple measurements for the same and different tags

TRA varies within 0.05. Thus, the TRA of a single frequency can potentially differentiate only $\frac{0.05}{3.9\times10^{-3}} \approx 13$ tags, demonstrating the limited scale of existing works that employ a single frequency for fingerprint extraction. In contrast, by hopping the frequency with an interval of 1 KHz over 13.56-13.76 MHz, the feature space is exponentially expanded to 13^{201}=7.99×10^{223}, which significantly improves the fingerprint scalability.

C. Practical Issues Affecting the Fingerprint Effectiveness

Applying $\boldsymbol{A_{\text{tag}}(f_{\text{chain}})}$ for effective NFC tag authentication encounters many practical issues. We systematically discuss these issues as follows.

1) Effect of reader diversity and tag placement: $y_{\text{tag}}(f,t)$ in Eq. (2) is the ideal tag response signal. However, the received PHY signal is a superposition of CW and tag response signals, which are affected by the frequency response $R(f)$ of the reader RF front-end (e.g., RF circuit and antenna). Meanwhile, the NFC tag is powered up based on the inductive coupling effect. Thus, the amount of harvest energy is also influenced by the coupling coefficient k between the reader antennas and the tag coil, e.g., the overlapping area and distance between the reader antenna and the tag coils [19]. Thereby, the actual received tag response signal is expressed as follows.

$$y_{\text{tag}}(f,t) = k \cdot R(f) \cdot [A_{\text{cw}}e^{j\alpha} + A_{\text{tag}}(f)e^{j\beta}] \cdot e^{-j2\pi ft}, \quad (3)$$

where A_{cw} denotes the amplitude of CW signal. α and β refer to the phases of CW and tag response signals, respectively.

In practice, NFC readers, even fabricated by the same manufacturer, manifest different frequency responses $R(f)$. In addition, the tag can be placed at different positions relative to the reader antenna in different measurements, resulting in a different k. As such, the measured fingerprint from different readers and tag placement, which is in fact $k \cdot |R(f_{\text{chain}})| \cdot \boldsymbol{A_{\text{tag}}(f_{\text{chain}})}$, become inconsistent for the same tag.

2) Effect of frequency hopping: To collect $\boldsymbol{A_{\text{tag}}(f_{\text{chain}})}$, we linearly hop the CW frequency, i.e., $f_{\text{i}} = f_0 + i \cdot \Delta f$, where f_0 is 13.56 MHz, Δf is the hopping interval, and $i \in [1, 2, ..., n]$. In our work, the received PHY signal is down-converted based on f_0. Then, the received tag response signal after down-conversion becomes:

$$y_{d_{\text{tag}}}(f_{\text{i}},t) = k \cdot R(f) \cdot [A_{\text{cw}}e^{j\alpha_{\text{i}}} + A_{\text{tag}}(f_{\text{i}})e^{j\beta_{\text{i}}}] \cdot e^{-j2\pi i\Delta ft} \quad (4)$$

We notice that the hopping range and interval need careful selection for two reasons. First, there is a trade-off between the frequency range and the effective frequency band to activate the tag. Although a wide hopping range can increase the fingerprint feature space, the reader's and tag's frequency responses dramatically decrease when the frequency is far away from f_0, rendering a too weak CW signal to activate the tag. Second, we can set a small hopping interval so that more TRAs can be collected to expand the feature space. However, a fine-grained interval could introduce more noises in TRAs, which may degrade the authentication performance.

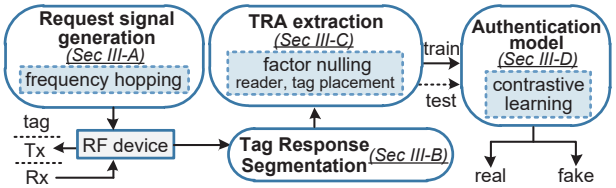

Fig. 7. Overview of NFC tag authentication system

4) Effect of noises from RF devices: The PHY signal collected by generic RF devices inevitably involves random noises (e.g., thermal and flicker noises), resulting in instantaneous variations across different measurements of $\boldsymbol{A_{\text{tag}}(f_{\text{chain}})}$ for the same tag. Such variations may narrow the distance among different tags' fingerprints due to the extremely small difference among tags' hardware components. As observed in Fig. 6, the distributions of tag7 and tag8 are close to each other, showing that their fingerprint difference is relatively small. With an increasing number of tags, the random noises from the generic RF device may incur the overlap between different tags' fingerprints and decrease the tag authentication accuracy. In NFChain, we will address the above practical issues to guarantee authentication performance.

III. NFChain Design

In this section, we introduce the detailed design of NFChain. The system overview is depicted in Fig. 7, including four modules: (1) Request signal generation: design the frequency hopping mechanism and generate the request signal to interrogate the NFC tag. (2) Tag response segmentation: locate and segment the tag response signal from the overall received signal. (3) TRA extraction: extract the $\boldsymbol{A_{\text{tag}}(f_{\text{chain}})}$ meanwhile eliminating the underlying factors that affect TRAs. (4) Tag authentication: develop an authentication model to determine whether an unknown tag is genuine or counterfeited.

A. Request Signal Generation

Although the operating frequency of NFC antennas and tags is specified at 13.56 MHz, tags can actually be activated at out-of-specification frequencies within 13.06-14.06 MHz band [13], [16]. This indicates that we can hop the CW frequency over 1 MHz to interrogate the tag. However, commodity NFC antennas' frequency responses dramatically decrease over 0.2-0.4 MHz from 13.56 MHz because a smaller bandwidth is required to increase the NFC communication range [3]. Thus, the frequency hopping range should be carefully selected to ensure the acquisition of tag response. First, we find that tags can be more easily activated for the rest of interrogations if they initially harvest higher energy. Said differently, more effective tag responses can be acquired if tags are powered up with proper CW signals at the beginning. As such, we start the frequency from 13.56 MHz, at which the tag can harvest the most energy from CW signals so that we can obtain more tag responses from the following frequencies. Second, we explore

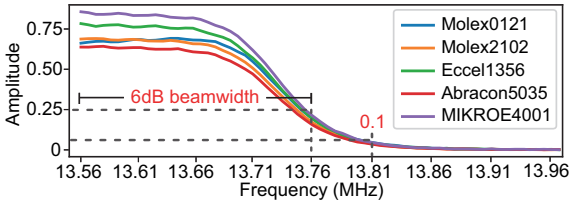

Fig. 8. Amplitude of the CW signal with frequency ranging from 13.56 MHz to 13.96 MHz using five different NFC antennas

various kinds of commodity NFC antennas and measure their CW signal amplitude over different frequencies, as shown in Fig. 8. After 13.81 MHz, the CW signal amplitude of the five antennas all drops below 0.1, which is insufficient to activate NFC tags in our extensive experiments. To ensure enough energy to power up the tag, we set the upper bound frequency to 13.76 MHz with a 6 dB-beamwidth. Finally, we investigate different hopping intervals (500 Hz - 4 KHz) between adjacent frequencies and choose 1 KHz which achieves the highest authentication accuracy as indicated by the experimental results in Section IV-C1. By doing so, we hop the frequency over 0.2 MHz band ranging from 13.56 MHz to 13.76 MHz with a 1 KHz interval, resulting in 201 frequencies.

In NFChain, the CW signal is formulated as $x^{\mathrm{i}}_{\mathrm{cw}}(t) = A_{\mathrm{cw}} \cdot e^{-j2\pi f_{\mathrm{i}} t}$, $f_{\mathrm{i}} = f_0 + (i-1)\cdot 1000$, $i \in [1, 2, ..., 200, 201]$, f_0 =13.56 MHz, $A_{\mathrm{cw}} = 1$. The request signal is designed as $x_{\mathrm{cw}}(t) \cdot x_{\mathrm{req}}(t)$, where $x_{\mathrm{req}}(t)$ is the binary coding of the request signal. Note that, compared to existing works that use specialized interrogation signals [13], [14], we make no modification to the protocol-specified request binary code while only varying its carrier frequencies. In other words, our frequency hopping scheme is fully compatible with the existing NFC protocol, especially in view of NFC tags. We set a guard time of 0.5 ms among CW signals with different frequencies to receive the tag response signal. Note that the request-response process to hop the whole 0.2 MHz frequency band only costs about 0.2 s. We note that the designed request signal can be easily integrated at the start of tag interrogation if vendors add the tag authentication function in their readers.

B. Tag Response Segmentation

With all rounds of signals between the reader and tag, we segment out the tag response signal for each frequency from the request and CW signals. As shown in Fig. 1(b), the request signal exhibits a much larger amplitude difference than the tag response signal. Meanwhile, the CW signal keeps relatively stable without much amplitude difference. Thus, we adopt the difference function and signal detection strategy in [20] to segment the tag response signal. Then, we apply a low-pass filter to eliminate the high-frequency noise caused by the subcarrier at 848 KHz [21] in the tag response signal.

C. TRA Extraction

Intuitively, we can extract the TRA by calculating the height between the high and low levels of the tag response signal. However, as discussed in Section II-C, the effects of different readers and tag placement incur inconsistent $\boldsymbol{A_{\mathrm{tag}}(f_{\mathrm{chain}})}$ for the same tag. We show the $\boldsymbol{A_{\mathrm{tag}}(f_{\mathrm{chain}})}$ measured from the same tag with different tag positions (Fig. 9(a)) and readers

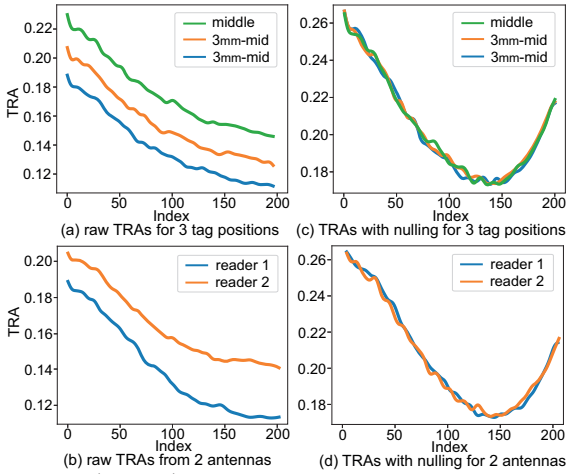

Fig. 9. $\boldsymbol{A_{tag}(f_{chain})}$ before and after *factor nulling* using different tag positions and readers

(Fig. 9(b)). The tag position is moved from the middle to the upper border of the antenna with a step of 0.3 cm. As depicted in Fig. 9, the TRAs prominently deviate from each other with only a 0.3 cm difference in the tag position. Moreover, the difference among the TRAs is further exacerbated when using two readers equipped with different antennas.

The inconsistent $\boldsymbol{A_{\mathrm{tag}}(f_{\mathrm{chain}})}$ for the same tag are caused by the coil coupling coefficient k and the reader's frequency response $R(f)$, as given in Eq. (4). Thus, we design a method, called *factor nulling*, to remove the effect of these factors and maintain fingerprint consistency. The essence of our method lies in two folds of relationships. The first fold is the relationship between the CW signal and the tag response signal. Since the tag response is modulated on the basis of CW signal, the tag response inherently contains the same reader effect $R(f)$ as the CW signal, which is expressed as follows.

$$y_{d_{\mathrm{cw}}}(f_{\mathrm{i}}, t) = R(f_{\mathrm{i}}) \cdot A_{\mathrm{cw}} e^{j\alpha_{\mathrm{i}}'} \cdot e^{-j2\pi i \Delta f t},$$

Then, if we divide $y_{d_{\mathrm{tag}}}(f_{\mathrm{i}}, t)$ by $y_{d_{\mathrm{cw}}}(f_{\mathrm{i}}, t)$, we obtain η_{i} as:

$$\eta_{\mathrm{i}} = \frac{y_{d_{\mathrm{tag}}}(f_{\mathrm{i}}, t)}{y_{d_{\mathrm{cw}}}(f_{\mathrm{i}}, t)} = \frac{k \cdot \cancel{R(f_{\mathrm{i}})} \cdot [A_{\mathrm{cw}} e^{j\alpha_{\mathrm{i}}} + A_{\mathrm{tag}}(f_{\mathrm{i}}) e^{j\beta_{\mathrm{i}}}] \cdot \cancel{e^{j2\pi i \Delta f t}}}{\cancel{R(f_{\mathrm{i}})} \cdot A_{\mathrm{cw}} e^{j\alpha_{\mathrm{i}}'} \cdot \cancel{e^{-j2\pi i \Delta f t}}}$$
$$= \frac{k[A_{\mathrm{cw}} e^{j\alpha_{\mathrm{i}}} + A_{\mathrm{tag}}(f_{\mathrm{i}}) e^{j\beta_{\mathrm{i}}}]}{A_{\mathrm{cw}} e^{j\alpha_{\mathrm{i}}'}}$$

In η_{i}, the reader effect $R(f)$ are successfully nulled. However, the factor k related to the tag placement effect still remains. Thus, we employ the second fold relationship between the tag response of the resonant frequency f_0 and that from other frequencies. Since the tag is relatively stable when placed on the reader during authentication, k keeps unchanged during frequency hopping. As such, we first divide the tag response by the CW signal on the resonant frequency as η_0:

$$\eta_0 = \frac{y_{d_{\mathrm{tag}}}(f_0, t)}{y_{d_{\mathrm{cw}}}(f_0, t)} = \frac{k[A_{\mathrm{cw}} e^{j\alpha_0} + A_{\mathrm{tag}}(f_0) e^{j\beta_0}]}{A_{\mathrm{cw}} e^{j\alpha_0'}}$$

Then, we obtain the ratio between η_i and η_0 as follows:

$$\frac{\eta_{\mathrm{i}}}{\eta_0} = \frac{\cancel{k}[e^{j\alpha_{\mathrm{i}}} + A_{\mathrm{tag}}(f_{\mathrm{i}}) e^{j\beta_{\mathrm{i}}}]}{e^{j\alpha_{\mathrm{i}}'}} \cdot \frac{e^{j\alpha_0'}}{\cancel{k}[e^{j\alpha_0} + A_{\mathrm{tag}}(f_0) e^{j\beta_0}]}$$
$$= e^{j(\alpha_0' - \alpha_{\mathrm{i}}')} \cdot \frac{e^{j\alpha_{\mathrm{i}}} + A_{\mathrm{tag}}(f_{\mathrm{i}}) e^{j\beta_{\mathrm{i}}}}{e^{j\alpha_0} + A_{\mathrm{tag}}(f_0) e^{j\beta_0}}, \quad (5)$$

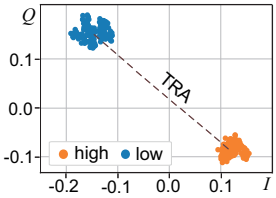

Fig. 10. Constellation of tag response signal in high and low levels

in which the factor k is successfully nulled, and $e^{j(\alpha_0^{'}-\alpha_i^{'})}$, $e^{j\alpha_i}$, $e^{j\alpha_0}$, $e^{j\beta_i}$, and $e^{j\beta_0}$ are constant phase values and do not affect the amplitude. Note that our method also eliminates the effect from frequency hopping $e^{j2\pi i\Delta ft}$, as shown in Eq. (5), which is caused by the carrier frequency offset between the signal Txx and Rx under our implementation. Then, we show the complex signal from η_i/η_0 in Fig. 10. The two concentrated clusters explicitly correspond to the logic high and low levels of tag response. As such, we can extract the factor-nulled TRA by measuring the distance between two cluster centers. The $\boldsymbol{A_{tag}(f_{chain})}$ after factor nulling in Fig. 9(c-d) exhibit a consistent pattern for different tag positions and readers.

D. Tag authentication model

Next, we develop an authentication model to detect whether the NFC tag is genuine or forged using the fingerprint. The built model should satisfy two key functions. First, the authentication model is capable of effectively distinguishing different tags' fingerprints in the face of the extremely tiny difference in TRAs, especially for tags with the same model. As shown in Fig. 5(b), the $\boldsymbol{A_{tag}(f_{chain})}$ of the tags with the same model exhibit a similar trend, which entails careful discrimination among different tags. To achieve this, we leverage two distinct characteristics of the tag fingerprint: (1) The $\boldsymbol{A_{tag}(f_{chain})}$ generally exhibits different nonlinear patterns among tags. (2) Besides the general nonlinear pattern, TRAs experience distinct fluctuations in several local frequencies, as shown in Fig. 5(b), potentially involving the unique feature of the tag. Thus, to preserve the fingerprint uniqueness, the nonlinearity and fluctuations in $\boldsymbol{A_{tag}(f_{chain})}$ should be well retained. The nonlinear activation functions (e.g., ReLU) and hidden layers in the neural network can potentially fulfill the above target.

Second, the authentication model should resist the random noises from generic RF devices. As we discussed in Section II-C, the intrinsic noises induce variations in the same tag's fingerprint measurements. Concerning the tiny hardware difference among tags, such variations can easily obfuscate different tags' fingerprints and reduce the fingerprint uniqueness. Thus, the designed model should be able to minimize the intra-distance of the same tag's fingerprint measurements. To meet this requirement, we adopt unsupervised contrastive learning, which aims to find an embedding space in which samples of the same class are 'pushed' close to each other [22], [23].

In a nutshell, we design a contrastive neural network model for tag authentication, as depicted in Fig. 11. The key feature of the model is the design of two parallel pipelines of neural networks, whose inputs come from the same tag's fingerprint measurements collected at different times. The inputs are separately embedded into two latent vectors z_m and z_n through

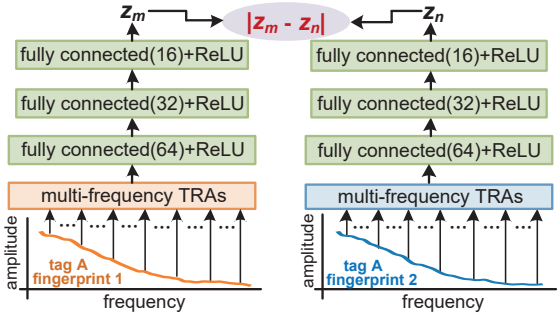

Fig. 11. Architecture of the tag authentication model

three fully connected neural network layers activated by the ReLU function to preserve nonlinearly and uniqueness. The benefit of the two inputs is that we can utilize their embedded vectors to combat random noises. Specifically, we train the model to minimize the difference between z_m and z_n because a smaller distance means a higher similarity across different fingerprint measurements of the same tag. Accordingly, we design a contrastive loss function as below:

$$\mathcal{L} = \frac{1}{J}\sum_{j=1}^{J}[z_m(j) - z_n(j)]^2, \tag{6}$$

where J is the length of the latent vector. Through our experiments, J is empirically set to 16.

Finally, we employ the loss value $\mathcal{L}$ in the model for tag authentication. When authenticating an unknown tag, one of the inputs is the genuine tag's fingerprint, while the other input is from the unknown tag. The loss value would be rather small if the unknown tag is genuine because the model is trained to minimize the difference between the same tag's fingerprint measurements. On the contrary, if the tag is forged, its embedded latent vector generates a different distribution from the genuine one. Then, the loss value will be much larger. To exemplify our idea, we train the tag authentication model for seven tags separately, test each model using fingerprints from the same tag and another 50 tags (with the same and different tag models), and obtain all loss values. As shown in Fig. 12, the loss values of the same tag are much smaller than those from different tags.

Hence, we compare the unknown tag's loss value with that of the genuine tag for authentication. Specifically, we obtain all the loss values when using the genuine tag's fingerprint measurements to train the authentication model. Then, we follow the three-sigma rule of thumb [24], which is widely used to detect anomalies (i.e., forge tags), to select a threshold for loss comparison with unknown tags. First, we calculate the mean μ_l and variance σ_l of all loss values. Then, we compare the authentication performance using the summation of μ_l and

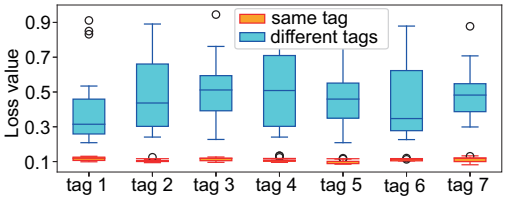

Fig. 12. Loss values of fingerprints from the same tag and different tags

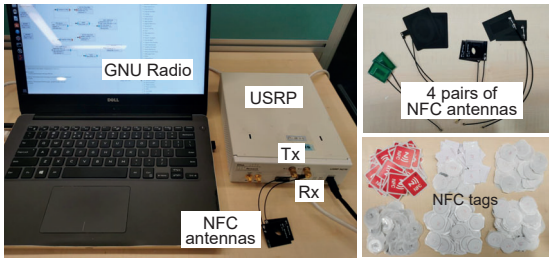

Fig. 13. Illustration of system setup, antennas, and tags

TABLE II
INFORMATION OF NFC TAGS

IC	Ant. size	#	IC	Ant. size	#
NTAG 213	ϕ: 25mm	120	Mifare ULT	ϕ: 25mm	100
NTAG 216	38*38mm	100	Mifare ULT C	ϕ: 25mm	100
NTAG 424	ϕ: 22mm	100	F08	ϕ: 25mm	120

different times of σ_1. We set the threshold as $\mu_1 + 2\sigma_1$ as it achieves the best performance. Finally, if the loss value of an unknown tag's sample is larger than the threshold, the tag is detected as a forge one, and vice versa.

IV. EVALUATION

In this section, we introduce the experimental setup, results, and security analysis of NFChain.

A. Experimental setup

1) Hardware: We build an NFChain prototype as shown in Fig. 13. In the prototype, we employ the universal software radio peripheral (USRP) N210, which is connected with commodity NFC antennas as the NFC reader. Two NFC antennas, which are synchronized and connected to the RF1 and RF2 sockets of USRP, act as the Tx and Rx antennas. We evaluate our system using four pairs of reader antennas with different RF front-end properties and over 600 NFC tags, which are selected from mainstream manufacturers that have taken over 90% market share. The authentication model is trained on a desktop with Intel CPU i7-9750H, Nvidia GeForce RTX 3060 GPU, and 32-GB memory.

2) Software: We implement the communication process between the USRP and tag using GNU Radio. The sampling rate is set to 2 MHz. The received signal is processed in Python for tag fingerprint extraction and authentication model training. The model is trained via PyTorch with the Adam optimizer. The learning rate and the number of epochs are set to 1e-3 and 500, respectively. For the genuine tag, we repeat the request-response process and collect 300 fingerprint measurements which are permutated into thousands of pairwise combinations to train the authentication model. The training data collection cost around 60 s. To save time on data collection, we can employ the multiple-flow scheduling method and network architecture proposed in [25]. For a large batch of tags, the fingerprinting process can be accelerated by employing multiple readers. The model training takes about 15 s, and each model's size is around 15 KB. In terms of model testing, we collect another 20 fingerprint measurements from each testing tag. For real-time tag authentication, it costs only 0.5 s to collect the signal and obtain the authentication result. The frequency-hopping process is relatively time-efficient since the request-reply signal is short.

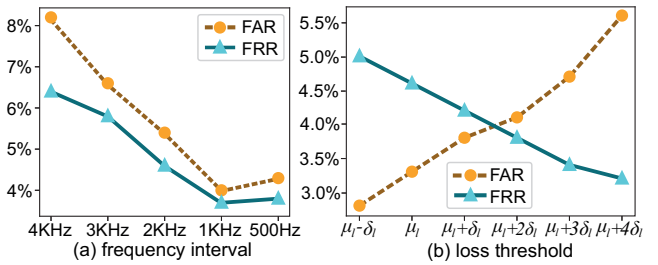

Fig. 14. FRR and FAR of different (a) frequency intervals, (b) loss thresholds

B. Evaluation metrics

In the evaluation, we employ three widely used metrics to evaluate the authentication performance, including false acceptance rate (FAR), false rejection rate (FRR), and authentication accuracy. FAR refers to the percentage of incorrectly accepted forged tags. FRR denotes the percentage of failure to accept the genuine tag. During experiments, we randomly pick out 100 tags as genuine tags in a row and use the remaining tags to attack each genuine tag's model. Meanwhile, we also check whether the model can successfully accept the genuine tag. Finally, we calculate the authentication accuracy, which is the ratio of accurate attempts over the total number of tests.

C. Experimental results

1) Selection of frequency interval: In this experiment, we investigate the effect of the frequency interval on authentication performance. We select different frequency intervals, i.e., 4 KHz, 3 KHz, 2 KHz, 1 KHz, and 500 Hz, which correspond to 51, 76, 101, 201, and 401 TRAs in the fingerprint, respectively. The FAR and FRR for different frequency intervals are shown in Fig. 14(a). FAR and FRR both drop with the decreasing interval because a smaller interval introduces more numbers of CW frequencies so that more tag features can be obtained. We achieve the lowest FAR and FRR for an interval of 1 KHz. However, the FAR and FRR increase slightly when the frequency interval further decreases to 500 Hz because more random noises are involved with a dense interval. Therefore, we set the frequency interval to 1 KHz.

2) Selection of loss threshold: In the authentication model, we compare the loss $\mathcal{L}$ with a pre-defined threshold to determine whether an unknown tag is genuine or forged. To ensure authentication accuracy, the threshold should be carefully selected as a larger threshold would make the model accept more forged tags, leading to a higher FAR. While a smaller threshold tends to reject the genuine tag. Thus, we choose different thresholds based on the mean (μ_1) and standard variation (σ_1) of the genuine tag's loss values obtained during model training. Then, we calculate the FAR and FRR based on different thresholds, as shown in Fig. 14(b). The FAR increases when the threshold grows from $\mu_1 - \sigma_1$ to $\mu_1 + 4 \times \sigma_1$. In contrast, the FRR decreases with an increasing threshold. The FAR and FRR curves intersect at near $\mu_1 + 2 \times \sigma_1$, which is set as the loss threshold in our experiment.

3) Effect of tag model: In this experiment, we investigate the authentication performance of NFC tags in different tag models. We attack the trained model using testing fingerprint measurements collected from tags with the same model as the

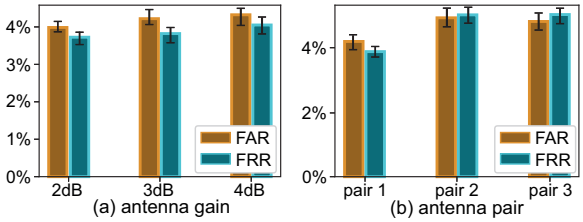

Fig. 15. FAR and FRR for different (a) antenna gains and (b) antenna pairs

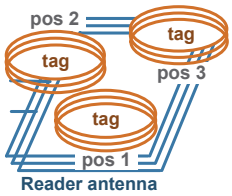

Fig. 16. Tag positions

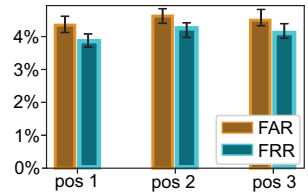

Fig. 17. FAR and FRR of 3 tag positions

genuine one, as well as tags in different models. Then, we calculate the FAR among all attacks. Meanwhile, we obtain the FRR for each model of tags. The results are given in Table III. The FAR and FRR for different tag models are all below 5%, showing the effectiveness of our authentication method for various tag models. The average FAR when the testing tag's model is the same as the genuine one is a little higher than that from different tag models. The authentication accuracy of the same tag model is also $3\% - 4\%$ lower than that of different models. This is because tags with different models have a larger difference in the hardware components. Nevertheless, our tag authentication method can still achieve around only 4% FAR for tags with the same model.

4) Effect of reader diversity: In this experiment, we evaluate our factor nulling method to tackle the reader diversity. First, we set different gains (2 dB, 3 dB, and 4 dB) for the reader's antenna. The authentication model is trained with fingerprint measurements collected with a 2 dB gain and tested using all three gains. Second, we employ three different pairs of reader antennas and use one pair of them to train the model, which is then tested using all pairs of antennas. The results are shown in Fig. 15. The FAR and FRR, when using the same and different antenna gains, are similar in Fig. 15(a). While, when using different pairs of reader antennas, the FAR and FRR experience relatively more degradation, especially for the FRR, which increases by around 1.5%. This is due to reader antennas with different sizes and circuit designs, which bring more variations in TRAs, making the model incorrectly reject more genuine measurements. Nevertheless, the FAR and FRR with different reader antennas are all below 5%.

5) Effect of tag placement: In this experiment, we evaluate our factor nulling method to deal with the tag placement effect. We place the tag at three positions on the transmitter antenna, as shown in Fig. 16. Then, we train the authentication model using samples collected from position 1 (pos 1) and test the model with samples from all three positions (pos 1, 2, and 3). The authentication results are shown in Fig. 17. The FAR and FRR are consistent for different tag positions, showing the effectiveness of our method to null the factor k and robustness to different tag placements.

TABLE III
FAR AND FRR FOR TAGS WITH THE SAME AND DIFFERENT MODELS

Same model	**Nt213**	**Nt214**	**Nt216**	**ULT**	**ULT C**	**F08**
FRR	4.3%	4.1%	3.8%	3.3%	3.5%	3.7%
FAR	4.8%	4.6%	4.3%	4.5%	4.2%	4.1%
Diff. models	**Nt213**	**Nt214**	**Nt216**	**ULT**	**ULT C**	**F08**
FAR	2.8%	2.4%	2.5%	2.6%	2.3%	2.1%

6) Comparison of authentication methods: In this experiment, we compare the performance using different authentication methods, including Euclidean distance-based, distribution-based, and our contrastive learning model. First, we calculate the Euclidean distance between every two samples of the genuine tag and take the mean (E_{m}) and standard deviation (E_{v}) of all distance values. The threshold to authenticate the tag is set to $E_{\mathrm{m}}+2\times E_{\mathrm{v}}$, which achieves the best authentication accuracy. Second, we transform TRAs into a histogram distribution. Then, we apply the earth mover's distance to measure the distance between histograms. A threshold is set to the sum of the mean and two times of standard deviation of all distribution distances for the genuine tag's fingerprint measurements. The authentication results of the three methods are given in Table IV, which shows that our method achieves the best accuracy with 22% improvement compared with another two methods. This is because the contrastive neural network model can learn a better representation of $\boldsymbol{A}_{\mathbf{tag}}(\boldsymbol{f}_{\mathbf{chain}})$, especially for the nonlinearity and fluctuations.

7) Evaluation on scalability: In this experiment, we evaluate the fingerprint scalability with an increasing number of forged tags. We randomly select 50 tags and separately train the model for each tag. Then, we choose different numbers of tags from the remaining ones to attack each model. Finally, we calculate the average FAR and present the result in Table V. We also obtain the FAR using a single TRA with 13.56 MHz frequency. When the number grows from 50 to 600, the FAR only experiences an increase of 0.6% for NFChain. Whereas the FAR largely grows by 30% for more tags when using a single-frequency TRA, showing that employing a wide frequency band effectively enhances the fingerprint scalability.

D. Security analysis

We discuss three common attacks targeting at NFChain.

1) Tag counterfeiting attack: Counterfeiters can clone the tag ID or even derive the sensitive data, e.g., password, from a genuine tag and copy them into the forged tag. Thus, using tag ID and cryptographic mechanism may fail to detect the forge

TABLE IV
AUTHENTICATION PERFORMANCE USING DIFFERENT METHODS

Method	Euclidean	Distribution	**Our model**
FAR	31.6%	25.9%	**4.1%**
FRR	23.8%	22.4%	**3.7%**
Accuracy	70.2%	76.7%	**96.2%**

TABLE V
FAR FOR AUTHENTICATING DIFFERENT NUMBERS OF TAGS

tag #	50	100	200	300	400	500	600
NFChain-FAR	3.9%	4.0%	4.15%	4.2%	4.35%	4.4%	4.5%
13.56MHz-FAR	8.5%	16.3%	25.2%	31.5%	34.4%	36.1%	39.5%

tag. However, NFChain achieves tag authentication using the intrinsic PHY feature of the tag, which is determined by the tag hardware. The PHY-based tag fingerprint is unique for each tag and extremely difficult to tamper with.

2) Feature replay attack: If counterfeiters know what kind of features are extracted as the tag fingerprint, they may iteratively emulate different combinations of features to attack the model. However, this is quite a labor-intensive process, especially for our NFChain system. Because the possible feature space of our designed tag fingerprint, which involves multi-frequency features, is extremely large. Furthermore, we can restrict the number of attempts to avoid adverse attacks.

3) Signal replay attack: Counterfeiters may overhear the communication channel between the reader and genuine tag. The eavesdropped signal may be replayed to attack the system. NFChain and existing NFC authentication approaches fail to completely defend against the replay attack if counterfeiters manage to do so. However, for NFC systems, the effective communication range is usually within 10 cm, which only leaves a quite small region for the counterfeiter to eavesdrop on the signal. Hence, the natural property of close proximity of NFC systems greatly reduces the chances of replay attack.

V. Related Work

Our work is mainly related to PHY-based tag authentication. In this section, we discuss related works in this field.

A. UHF RFID tag authentication

Ultra-high frequency (UHF) RFID mainly operates at 900-920 MHz frequency band. Existing works have investigated different features and PHY signals of UHF RFID tags for authentication [10], [12], [20], [26]–[28]. The minimum power required to energize the tag over multiple frequencies is extracted as the tag fingerprint using Voyantic Tagformance Lite [12]. The phase shift caused by the inner circuit of tags can reveal distinct hardware characteristics and act as a tag phase fingerprint [26]. A preamble signal, i.e., RN16, in the EPC-global Gen 2 protocol is used for tag authentication [10] [27]. The intuition is that temporal and spectral features of RN16 scan reflect the hardware difference among tags. However, due to the relative long-range communication distance, environmental noises become the key issue, which significantly reduces the tag fingerprint's robustness in different environments [29]. To address this issue, existing works either employ multiple tags to eliminate noises [20] or extract environment-independent features, e.g., persistent time [28].

B. HF NFC authentication

Due to the difference in communication range and protocols, most fingerprinting approaches for UHF RFID tags cannot be directly applied to NFC tags. For instance, IEC/ISO 14443 protocol does not support simultaneous multi-tag communication as the EPCglobal UHF Gen2 protocol does due to its anti-collision mechanism. Thus, NFC systems demand for alternative designs for tag authentication. The burst signal with a high voltage (10 V) have been applied to excite the NFC tag [13], [14], after which the tag response to the burst obtained using a high-end oscillator is regarded as a fingerprint. However, the burst signal is incompatible with NFC protocols. To comply with existing protocols, the envelop and spectral features of the transient signal during the frame delay time of NFC communication have been employed as the tag fingerprint [11]. Existing works also extract time-domain and spectral features from the PHY signal of tag response under the resonant frequency for tag identification [16], [30]. Although simple in PHY signal processing, these works only employ a single CW frequency to acquire the fingerprint, which greatly constrains the fingerprint scalability. Besides, their system settings are strictly controlled and limited for laboratory use. Different from previous works, the fingerprint extracted by our NFChain involves features from multiple frequencies to support high scalability and are fully compatible with existing NFC communication protocols.

C. PHY-based authentication

Apart from RFID and NFC tag authentication, PHY signals have been leveraged to authenticate diverse radio frequency (RF) devices as well, including RFID transponders, WiFi, and Zigbee nodes [31]–[34], because RF devices also bare distinctive manufacturing imperfections in their hardware components, e.g., amplifier and oscillator. Moreover, the PHY signal can effectively solve the issue of the easily forged MAC address of RF devices and enhance the device security. Existing works mainly extract device hardware differences from the channel state information (CSI), e.g., the carrier frequency offset [33] and spectrum features from the nonlinear RF front-end [34]. However, the CSI is data-dependent and susceptible to the changing wireless channel [35]. On the contrary, our NFChain is robust to the environment due to its near field communication nature.

VI. Conclusion

This paper introduces an NFC tag authentication system NFChain with a holistic design of a unique tag fingerprint and an effective authentication model. The tag fingerprint, which consists of a chain of TRAs over multiple frequencies, embeds the intrinsic hardware properties of the tag and shows distinctive patterns among different tags. Since the received tag response signal is affected by practical factors, we design a factor nulling method to remove these effects. Based on the tag fingerprint, we develop a contrastive neural network model, which not only retains the nonlinearity and tiny fluctuations in the fingerprint but also enhances the stability of the tag fingerprint among different measurements. Our experimental results show that the developed system can achieve high authentication accuracy for different configurations.

VII. Acknowledgement

This work is supported by the National Key Research and Development Program of China (No. 2021YFB3100400), the HK RGC Research Impact Fund under Grant R5034-18, the National Nature Science Foundation of China (No. 62202276, No. 62202274, and No. 62102139), the Shandong Science Fund for Excellent Young Scholars (No. 2022HWYQ-038), the Nature Science Foundation of Hunan Province of China under Grant 2022JJ30168 and the Fundamental Research Funds for the Central Universities under Grant 531118010612.

REFERENCES

[1] "Consumers embracing the convenience and security of nfc contactless technology," https://nfc-forum.org/consumers-embracing-the-convenience-and-security-of-nfc-contactless-technology/.

[2] "Covid-19 resources - nfc forum," https://nfc-forum.org/covid-19-resources/.

[3] R. Zhao, P. Wang, Y. Ma, P. Zhang, H. H. Liu, X. Lin, X. Zhang, C. Xu, and M. Zhang, "Nfc+ breaking nfc networking limits through resonance engineering," in *Proceedings of ACM Special Interest Group on Data Communication (SIGCOMM)*, 2020.

[4] "Near field communication market 2021 to 2025 growth factors, market characteristics, opportunities by type analysis and forecast," https://www.marketwatch.com/press-release/near-field-communication-nfc-market-2021-to-2025-growth-factors-market-characteristics-opportunities-by-type-analysis-and-forecast-2021-06-10.

[5] "New zealand pilots nfc tags for covid-19 tracking," https://www.healthcareitnews.com/news/anz/new-zealand-pilots-nfc-tags-covid-19-tracking.

[6] S. Shah and T. Mirza, "Security of nfc data," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 6, no. 4, pp. 341–344, 2016.

[7] T. Plos, M. Hutter, M. Feldhofer, M. Stiglic, and F. Cavaliere, "Security-enabled near-field communication tag with flexible architecture supporting asymmetric cryptography," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 21, no. 11, pp. 1965–1974, 2012.

[8] M. H. Özcanhan, G. Dalkılıç, and S. Utku, "Cryptographically supported nfc tags in medication for better inpatient safety," *Journal of medical systems*, vol. 38, no. 8, pp. 1–15, 2014.

[9] D. Saeed, R. Iqbal, H. H. R. Sherazi, and U. G. Khan, "Evaluating near-field communication tag security for identity theft prevention," *Internet Technology Letters*, vol. 2, no. 5, p. e123, 2019.

[10] 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 (TON)*, vol. 24, no. 2, pp. 846–858, 2015.

[11] H. P. Romero, K. A. Remley, D. F. Williams, and C.-M. 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, 2009.

[12] 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, 2010.

[13] B. Danev, T. S. Heydt-Benjamin, and S. Capkun, "Physical-layer identification of rfid devices." in *Proceedings of USENIX security symposium*, 2009.

[14] B. Danev, S. Capkun, R. Jayaram Masti, and T. S. Benjamin, "Towards practical identification of hf rfid devices," *ACM transactions on Information and System Security (TISSEC)*, vol. 15, no. 2, pp. 1–24, 2012.

[15] B. Danev, D. Zanetti, and S. Capkun, "On physical-layer identification of wireless devices," *ACM Computing Surveys (CSUR)*, vol. 45, no. 1, pp. 1–29, 2012.

[16] G. Zhang, L. Xia, S. Jia, and Y. Ji, "Physical-layer identification of hf rfid cards based on rf fingerprinting," in *Proceedings of International Conference on Information Security Practice and Experience*, 2016.

[17] "Fcc measurement/technical report on nfc transceiver," https://fcc.report/FCC-ID/KR5NFC30/5094021.pdf.

[18] S. A. Vowels, "Understanding rfid (radio frequency identification)," in *Ubiquitous and Pervasive Computing: Concepts, Methodologies, Tools, and Applications*. IGI Global, 2010, pp. 54–64.

[19] K. Finkenzeller, *RFID handbook: fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication*. John wiley & sons, 2010.

[20] J. Han, C. Qian, Y. Yang, G. Wang, H. Ding, X. Li, and K. Ren, "Butterfly: Environment-independent physical-layer authentication for passive rfid," in *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, 2018.

[21] V. Coskun, K. Ok, and B. Ozdenizci, *Near field communication (NFC): From theory to practice*. John Wiley & Sons, 2011.

[22] T. Chen, S. Kornblith, M. Norouzi, and G. Hinton, "A simple framework for contrastive learning of visual representations," in *Proceedings of International Conference on Machine Learning (ICML)*, 2020.

[23] T. Chen, S. Kornblith, K. Swersky, M. Norouzi, and G. E. Hinton, "Big self-supervised models are strong semi-supervised learners," *Advances in neural information processing systems*, vol. 33, pp. 22 243–22 255, 2020.

[24] F. Pukelsheim, "The three sigma rule," *The American Statistician*, vol. 48, no. 2, pp. 88–91, 1994.

[25] D. Yang, K. Gong, J. Ren, W. Zhang, W. Wu, and H. Zhang, "Tc-flow: Chain flow scheduling for advanced industrial applications in time-sensitive networks," *IEEE Network*, vol. 36, no. 2, pp. 16–24, 2022.

[26] L. Yang, P. Peng, F. Dang, C. Wang, X.-Y. Li, and Y. Liu, "Anti-counterfeiting via federated rfid tags' fingerprints and geometric relationships," in *Proceedings of IEEE International Conference on Computer Communications (Infocom)*, 2015.

[27] D. Zanetti, B. Danev, and S. Capkun, "Physical-layer identification of uhf rfid tags," in *Proceedings ACM Annual International Conference On Mobile Computing And Networking (Mobicom)*, 2010, pp. 353–364.

[28] X. Chen, J. Liu, X. Wang, H. Liu, D. Jiang, and L. Chen, "Eingerprint: Robust energy-related fingerprinting for passive rfid tags," in *Proceedings of USENIX Symposium on Networked Systems Design and Implementation*, 2020.

[29] D. Zanetti, P. Sachs, and S. Capkun, "On the practicality of uhf rfid fingerprinting: How real is the rfid tracking problem?" in *International Symposium on Privacy Enhancing Technologies Symposium*. Springer, 2011, pp. 97–116.

[30] 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, 2021.

[31] B. Danev, T. S. Heydt-Benjamin, and S. Capkun, "Physical-layer identification of rfid devices." in *USENIX security symposium*, 2009, pp. 199–214.

[32] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proceedings of the 14th ACM international conference on Mobile computing and networking*, 2008, pp. 116–127.

[33] J. Hua, H. Sun, Z. Shen, Z. Qian, and S. Zhong, "Accurate and efficient wireless device fingerprinting using channel state information," in *IEEE INFOCOM 2018-IEEE Conference on Computer Communications*. IEEE, 2018, pp. 1700–1708.

[34] W. Wang, Z. Sun, S. Piao, B. Zhu, and K. Ren, "Wireless physical-layer identification: Modeling and validation," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 2091–2106, 2016.

[35] T. Zheng, Z. Sun, and K. Ren, "Fid: Function modeling-based data-independent and channel-robust physical-layer identification," in *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*. IEEE, 2019, pp. 199–207.