NFChain: A Practical Fingerprinting Scheme for NFC Tag Authentication

YANG Yanni[^], CAO Jiannong[*], **AN Zhenlin**[*], WANG Yanwen[#], HU Pengfei[^], ZHANG Guoming[^]

[^]Shandong University, China

[*]The Hong Kong Polytechnic University, China

[#]Hunan University, China

Content

- **Background of NFC Tag Fingerprinting**
  - Existing approaches
  - Preliminaries of NFC
- **NFChain Design**
  - System overview
  - Practical challenges
  - Our solutions
- **Experiments and Evaluation Results**
- **Discussion**

NFC Tag & Its Authentication

- The global NFC market size is estimated to experience significant growth and reach over $54 billion by 2028.

NFC Tag & Its Authentication

- The global NFC market size is estimated to experience significant growth and reach over $54 billion by 2028.
- Then core function of NFC, **anti-counterfeiting**, can be easily destroyed by adversaries.
- NFC tag authentication is IMPORTANT!

Existing NFC Tag Authentication Methods

- **Cryptography-based methods**
  - Apply cryptographic algorithms for encryption
  - Pros: convenient to use and apply
  - **Cons: easy to forge**

Existing NFC Tag Authentication Methods

- **Cryptography-based methods**
  - Apply cryptographic algorithms for encryption
  - Pros: convenient to use and apply
  - **Cons: easy to forge**
- **Physical-layer (PHY) methods**
  - Physical-layer signal reflects distinct manufacturing imperfection in tags’ hardware – **tag fingerprint**
  - **Pros:** reflects **inherent** hardware properties of the tag, difficult to tamper

PHY-based NFC Fingerprinting Methods

Fingerprint	Scale	Device	Compatibility
Transient signal envelop [1]	20	Oscilloscope	✓
Tag response envelop [2]	50	AWG* + Oscilloscope	✘
Tag response spectrum [3]	50	AWG* + Oscilloscope	✘

AWG: arbitrary waveform generator

[1] 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.

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

[3] 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.

PHY-based NFC Fingerprinting Methods

Fingerprint	Scale	Device	Compatibility
Transient signal envelop [1]	20	Oscilloscope	✓
Tag response envelop [2]	50	AWG* + Oscilloscope	✘
Tag response spectrum [3]	50	AWG* + Oscilloscope	✘

AWG: arbitrary waveform generator

Existing PHY-based NFC fingerprinting solutions are far from wide application due to unscalability and incompatibility issues

Our NFChain

- A new NFC fingerprinting scheme: NFChain

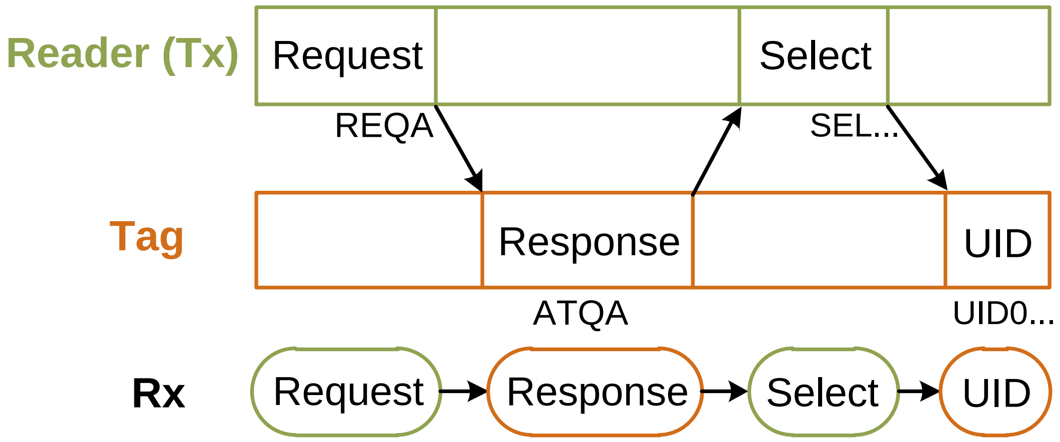
Single carrier wave (13.56MHz) → Wider frequency band (13.56-13.73MHz)

  - **Benefits:** Enhance the fingerprint distinguishably for the increasing number of tags

- Meanwhile, we employ the **protocol-agnostic tag response** signal to extract an unique tag fingerprint

Preliminaries of NFC

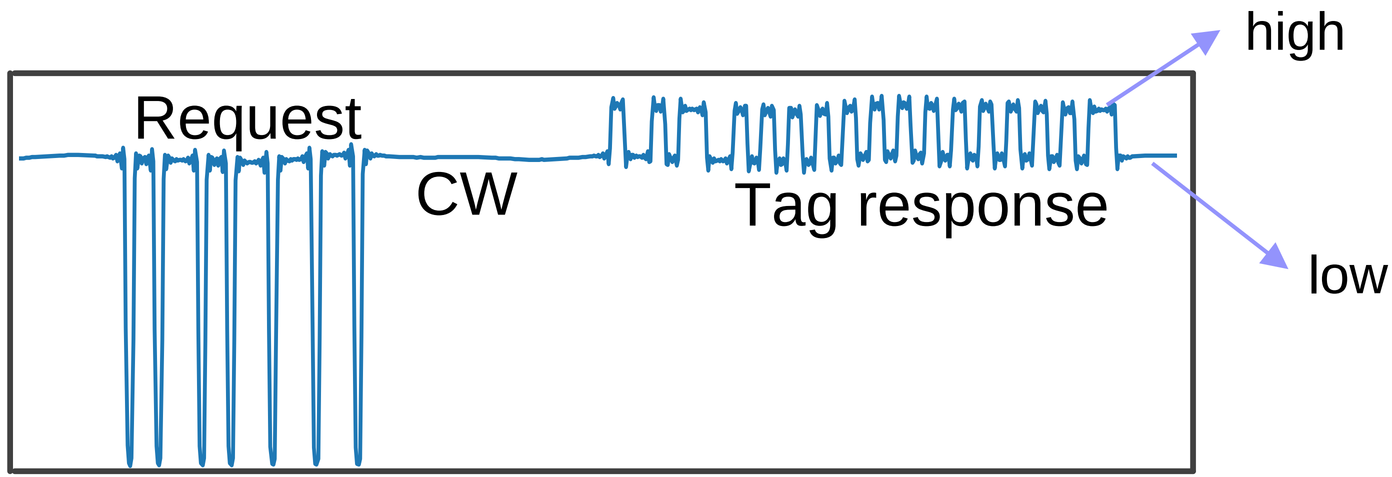
- NFC communication
  - NFC reader sends the carrier wave (**CW**) and **request** signal to activate the tag;
  - Tag **harvests energy** and sends back a **response**;



Communication between NFC reader and tag (ISO/IEC 14443)

Preliminaries of NFC

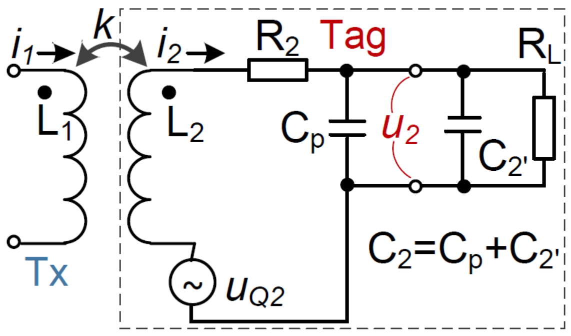
- NFC communication
  - Tag response across various NFC protocols adopts the same load modulation scheme – **protocol-agnostic**
  - A load resistor in the tag is switched on and off, resulting in the low and high levels of the tag response signal



PHY signal of the CW and request signal from reader, the tag response signal from the tag

Preliminaries of NFC

- Characterize the harvest voltage u_2 by the NFC tag



Simplified circuit for reader and tag

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

Signal frequency **Tag hardware**

(1) Tag manufacturing imperfections (L_2, C_2, R_2, R_L) cause distinctive variations of u_2 among different tags.

(2) Signal frequency (f) also determines u_2. A wider frequency band can enlarge the tag distinctiveness.

From Energy to Tag Response Amplitude

- The harvested voltage u_2 can be reflected from the tag response amplitude (**TRA**)
- Tag response signal $y_{tag}(f,t)$ under frequency f :

$$y_{tag}(f,t) = A_{tag}(f) e^{-j2\pi f t}$$

↓

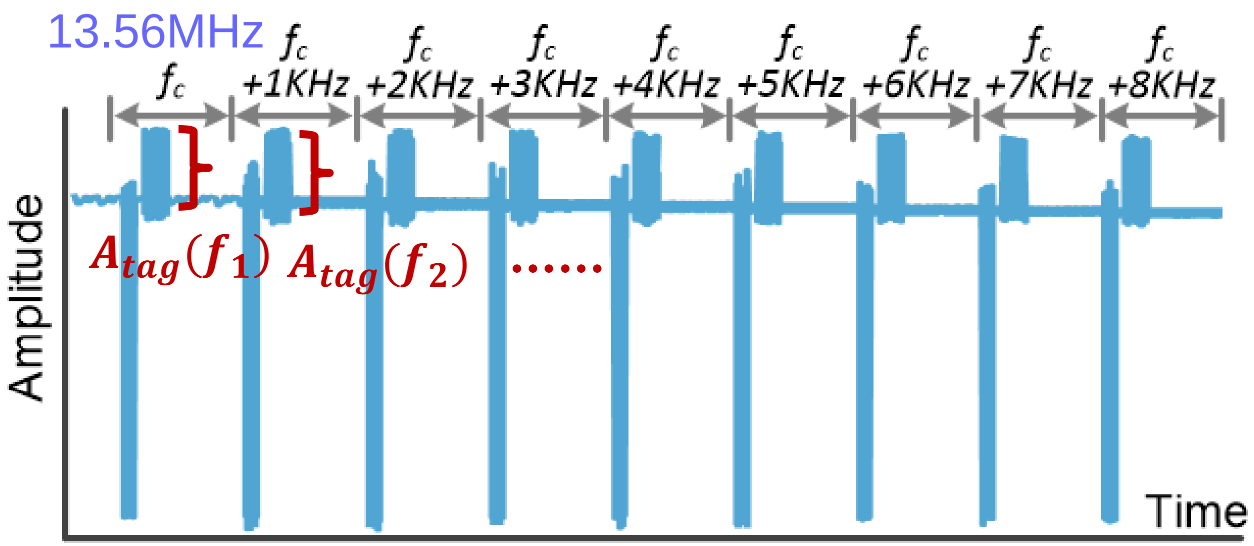
TRA $A_{tag}(f) \propto u_2$

From Energy to Tag Response Amplitude

- The harvested voltage u_2 can be reflected from the tag response amplitude (**TRA**)
- Tag response signal $y_{tag}(f,t)$ under frequency f:

$$y_{tag}(f,t)=A_{tag}(f)e^{-j2\pi ft}$$

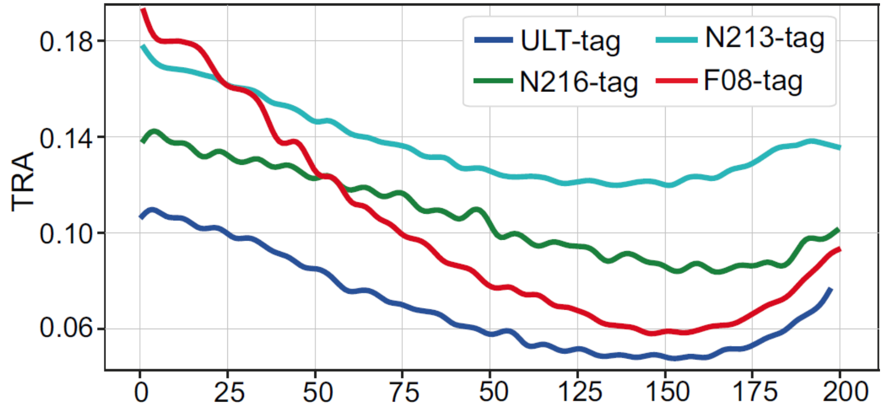
- Multi-frequency $[f_0, f_1, f_2, \ldots, f_n]$ TRA: $A_{tag}(f_{chain})$



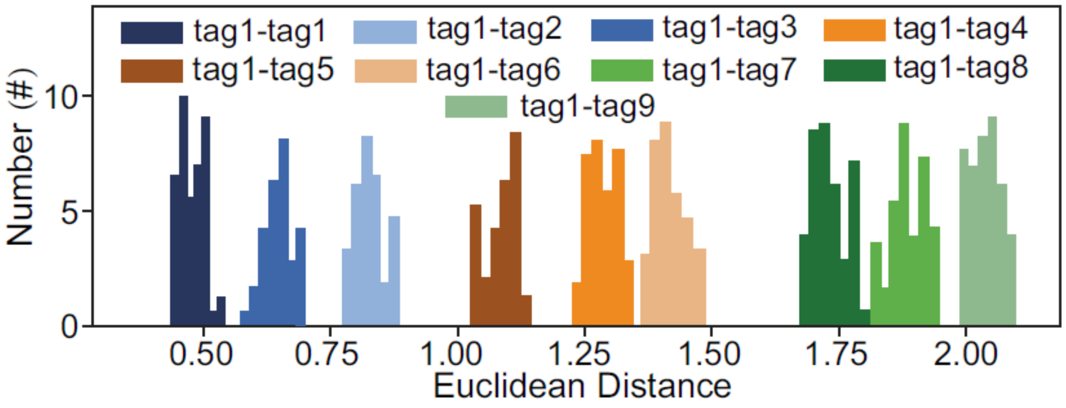
The PHY CW, request, tag response signal of multiple frequencies

Preliminary Experiment

- Extract TRAs from 9 tags (Mifare ULT, Ntag213, Ntag216, and F08) within 13.56 - 13.76MHz (frequency hopping: 1KHz).



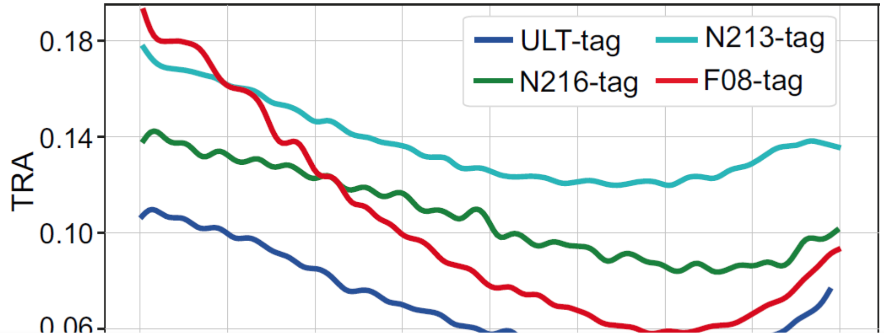
TRAs of tags in different models



Euclidean distance between tag1 and tagn

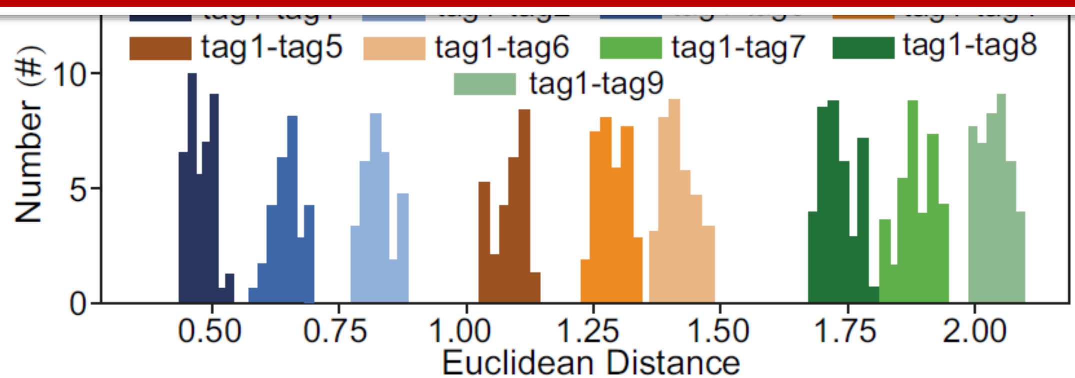
Preliminary Experiment

- Extract TRAs from 9 tags (Mifare ULT, Ntag213, Ntag216, and F08) within 13.56 - 13.76MHz (frequency hopping: 1KHz).



TRAs of tags in different models

Multi-frequency TRAs have the potential for NFC tag authentication



Euclidean distance between tag1 and tagn

Practical Issues

- **Effect of reader diversity and tag placements**
  - Received signal is a superposition of CW and tag response, meanwhile affected by the frequency response of reader $\boldsymbol{R}(\boldsymbol{f})$ and the coupling coefficient between reader and tag coils $\boldsymbol{k}$

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

Tag placement affects k

Practical Issues

- **Effect of reader diversity and tag placements**
  - Received signal is a superposition of CW and tag response, meanwhile affected by the frequency response of reader $\boldsymbol{R(f)}$ and the coupling coefficient between reader and tag coils $\boldsymbol{k}$

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

Tag placement affects k

Reader diversity varies $R(f)$

Practical Issues

- **Effect of reader diversity and tag placements**
  - Received signal is a superposition of CW and tag response, meanwhile affected by the frequency response of reader $\boldsymbol{R}(\boldsymbol{f})$, coupling coefficient between reader and tag coils $\boldsymbol{k}$,

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

The measured fingerprint from different readers and tag placement, i.e., $k \cdot |R(f)| \cdot A_{tag}(f_{chain})$ become inconsistent for the same tag.

Practical Issues

- **Effect of frequency hopping**
  - We linearly hop the CW frequency, i.e., $f_i = f_0 + i \cdot \Delta f$

$$y_{tag}(\boldsymbol{f_i}, t) = k \cdot R(f_i) \cdot [A_{cw} e^{j\alpha_1} + A_{tag}(\boldsymbol{f_i}) e^{j\beta_1}] \cdot e^{-j2\pi \boldsymbol{i \Delta f} t}$$

  - Trade-off between the frequency range and the effective frequency band to activate the tag

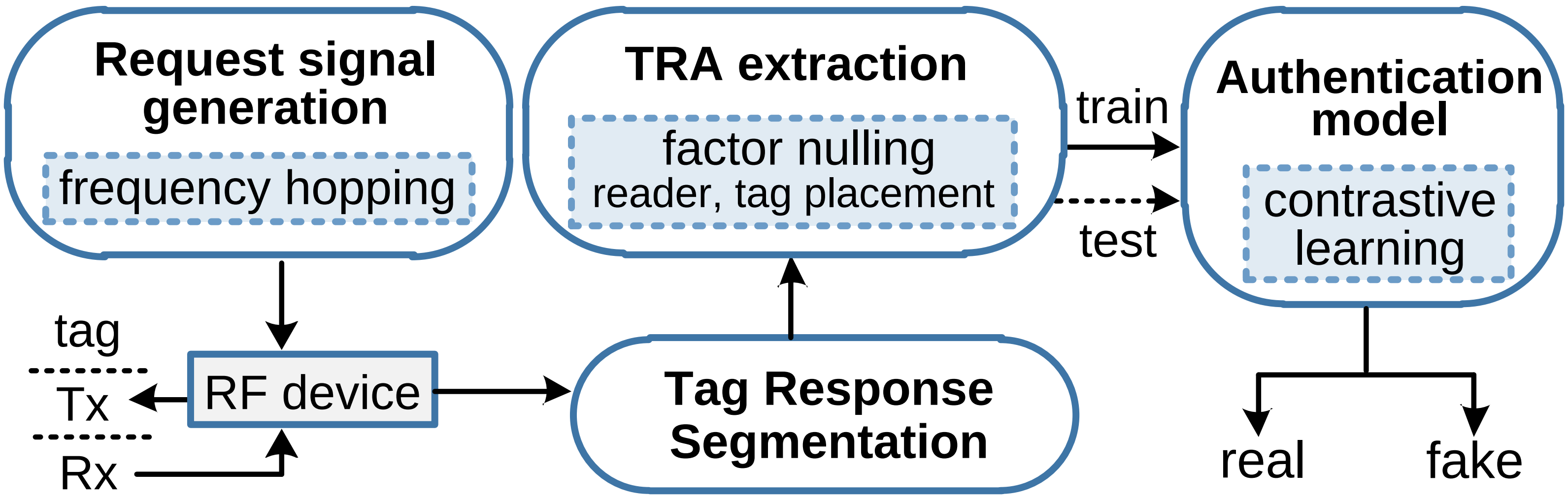
Wider frequency band
Fine-grained frequency

Fewer energy to activate tags and more noises in TRAs

Larger tag fingerprint feature space

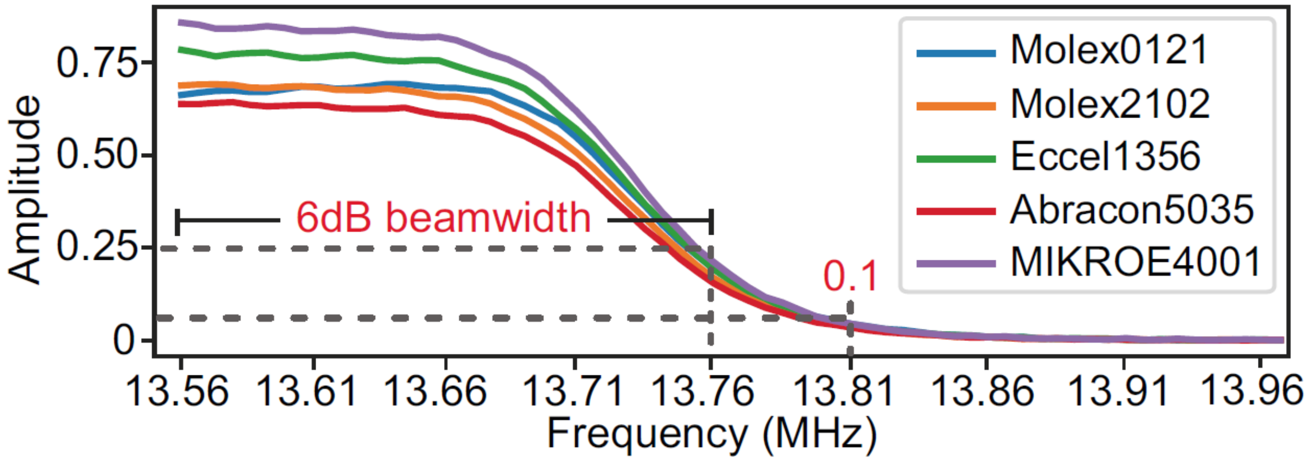
NFChain Design

- **System Overview**



NFChain Design

- **Request signal generation**
  - To ensure enough energy to power up the tag, we set the upper bound frequency to 13.76 MHz with a 6 dB-beamwidth



  - 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.

NFChain Design

- **TRA extraction**
  - **Factor nulling method**: tackle the inconsistency issue of tag fingerprint due to reader diversity and tag placement

1 **Employ CW signal to null R(f)**

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

$$\eta_i = \frac{y_{d_{tag}}(f_i, t)}{y_{d_{cw}}(f_i, t)} = \frac{k \cdot R(f_i) \cdot [A_{cw} e^{j\alpha_i} + A_{tag}(f_i) e^{j\beta_i}] \cdot e^{j2\pi i \Delta f t}}{R(f_i) \cdot A_{cw} e^{j\alpha_i'} \cdot e^{-j2\pi i \Delta f t}}$$

$$= \frac{k[A_{cw} e^{j\alpha_i} + A_{tag}(f_i) e^{j\beta_i}]}{A_{cw} e^{j\alpha_i'}}$$

NFChain Design

- **TRA extraction**
  - **Factor nulling method**: tackle the inconsistency issue of tag fingerprint due to reader diversity and tag placement

2 **Employ the resonant frequency (f_0) signal to null k**

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

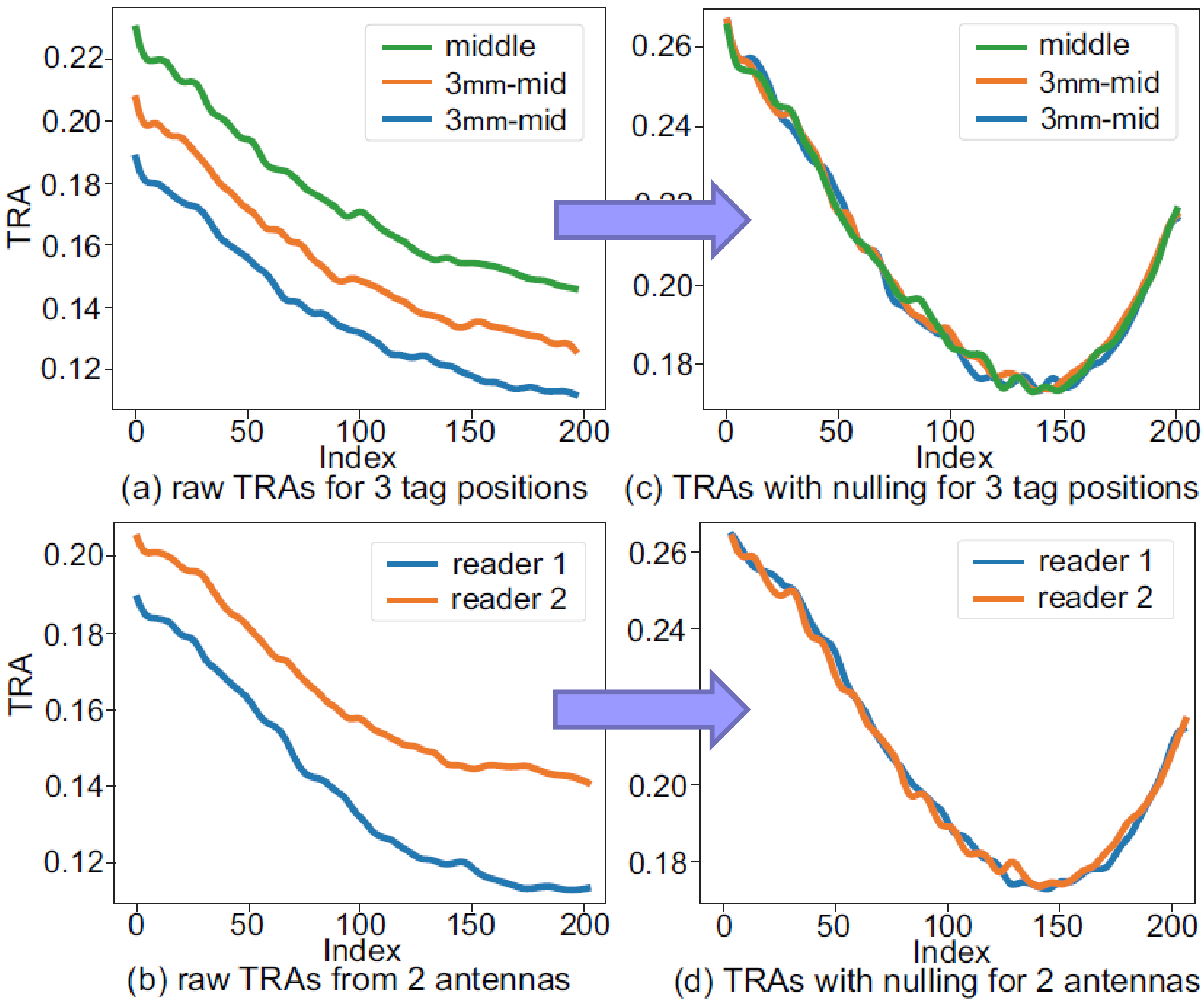
$$\frac{\eta_i}{\eta_0} = \frac{\cancel{k}[A_{cw}e^{j\alpha_i} + A_{tag}(f_i)e^{j\beta_i}]}{A_{cw}e^{j\alpha_i'}} \cdot \frac{A_{cw}e^{j\alpha_0'}}{\cancel{k}[A_{cw}e^{j\alpha_0} + A_{tag}(f_0)e^{j\beta_0}]}$$

$$= e^{j(\alpha_0' - \alpha_i')} \cdot \frac{A_{cw}e^{j\alpha_i} + A_{tag}(f_i)e^{j\beta_i}}{A_{cw}e^{j\alpha_0} + A_{tag}(f_0)e^{j\beta_0}}$$

NFChain Design

- **TRA**
  - **Fa** ... e of tag fin

2



(a) raw TRAs for 3 tag positions

(c) TRAs with nulling for 3 tag positions

(b) raw TRAs from 2 antennas

(d) TRAs with nulling for 2 antennas

NFChain Design

- **Tag authentication model**
  - **Model requirement (1):** Distinguish different tags' fingerprints facing the extremely tiny difference in TRAs

1. **Observation:** $A_{tag}(f_{chain})$ **generally exhibits nonlinear pattern**
2. **Observation:** $A_{tag}(f_{chain})$ **experience distinct fluctuations in several local frequencies**

↓

Apply nonlinear activation functions and hidden layers in the neural network

NFChain Design

- **Tag authentication model**
  - **Model requirement (1):** Distinguish different tags' fingerprints facing the extremely tiny difference in TRAs

1. **Observation: $A_{tag}(f_{chain})$ generally exhibits nonlinear pattern**
2. **Observation: $A_{tag}(f_{chain})$ experience distinct fluctuations in several local frequencies**

Apply nonlinear activation functions and hidden layers in the neural network

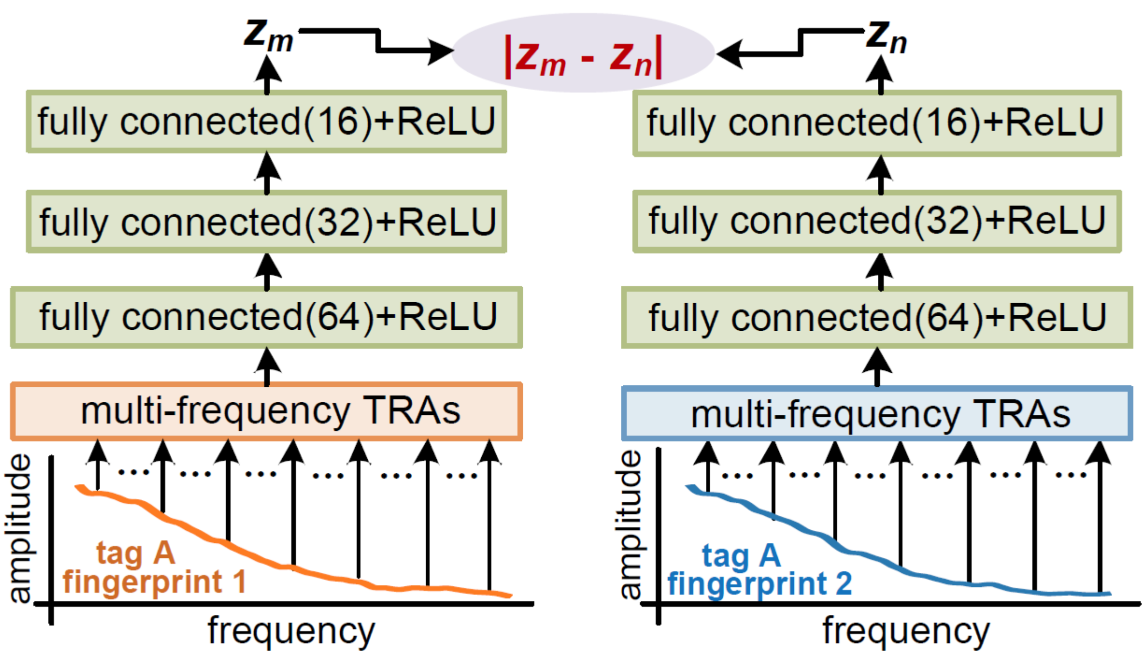
  - **Model requirement** (2): resist the random noises from generic RF devices

Apply unsupervised contrastive learning: samples of the same tag are 'pushed' close to each other

NFChain Design

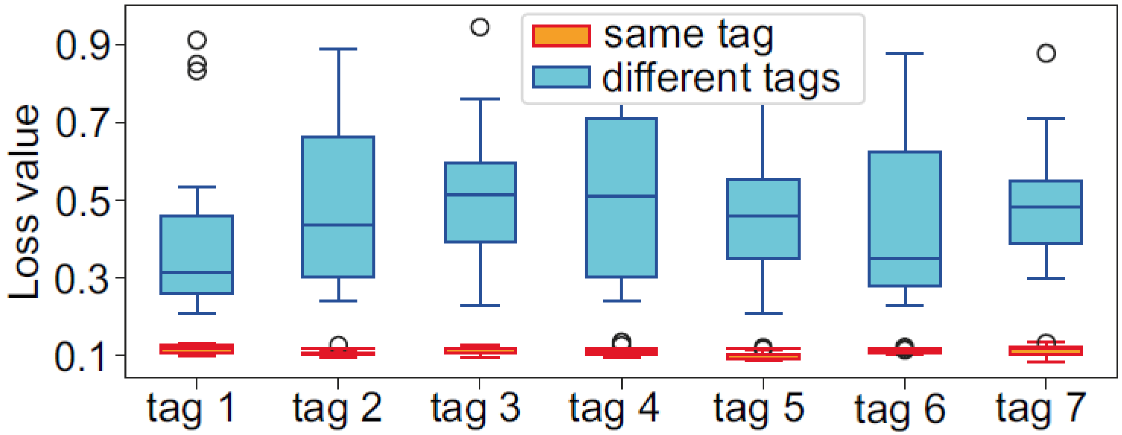
- **Tag authentication model – contrastive learning**
  - Apply fully connected neural network and ReLU function to preserve nonlinearly and uniqueness
  - Apply the following loss function to maintain a higher similarity across different fingerprint measurements of the same tag

$$Loss = \frac{1}{J}\sum_{j=1}^{J}[z_m(j) - z_n(j)]^2$$



NFChain Design

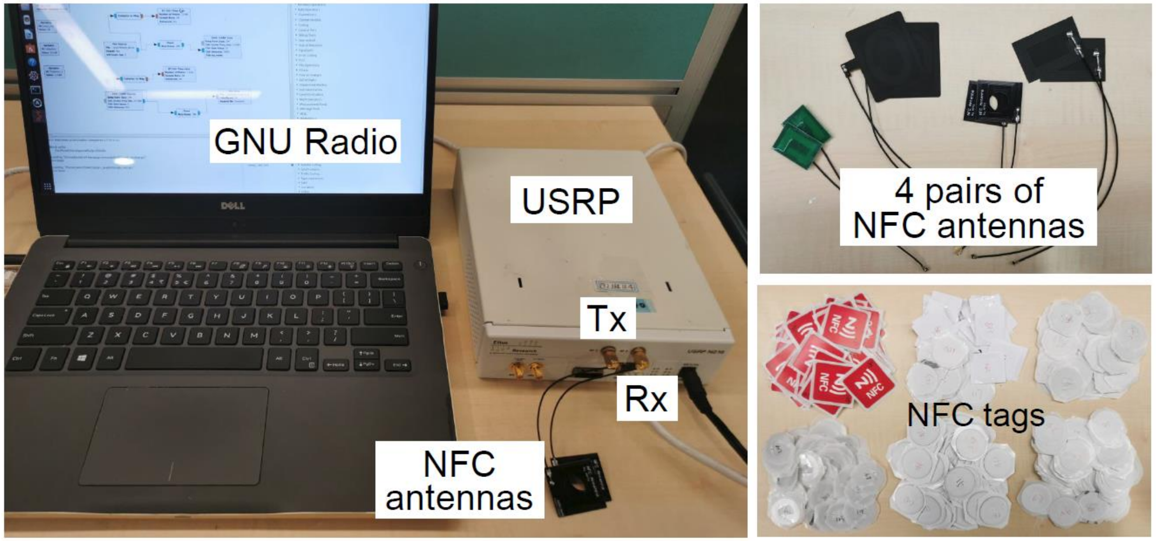
- **Tag authentication**
  - Compare the unknown tag's loss value with that of the genuine tag for authentication
  - Obtain the mean (μ) and standard deviation (σ) of genuine tag's loss values as the authentication threshold ($\mu + 2\sigma$)



Loss values of fingerprints from the same tag and different tags

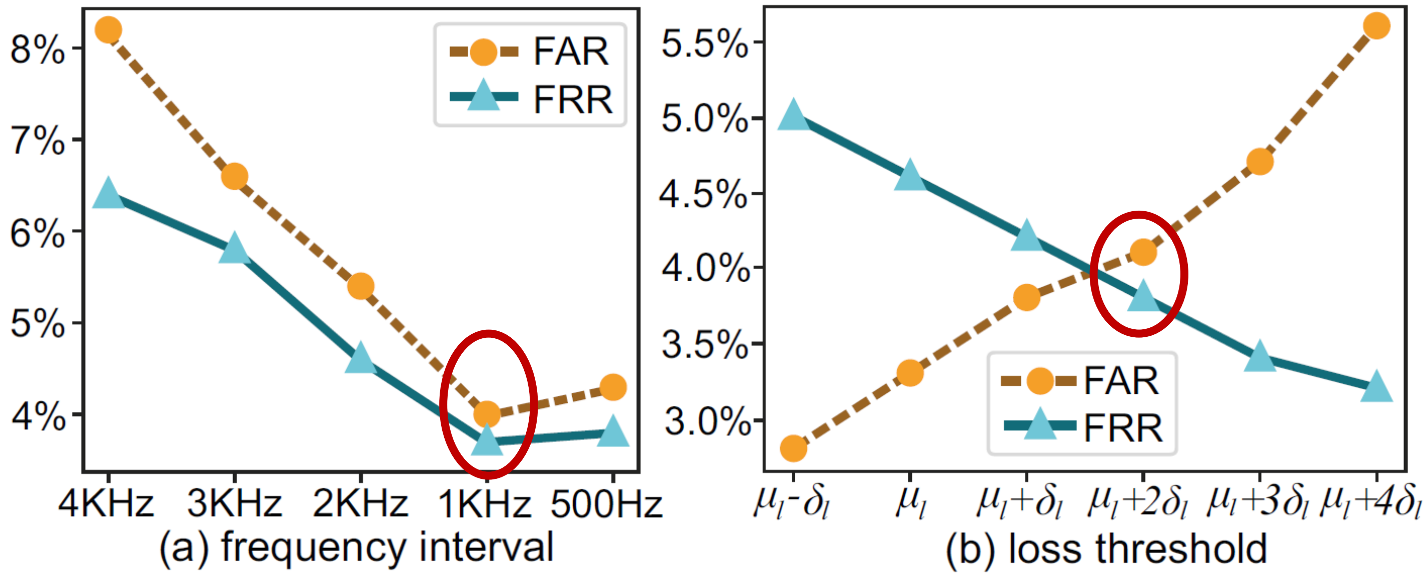
Experiments

- **Experimental setup**
  - **Hardware:** USRP N210, 4 pairs of NFC antennas (different types), 6 models of NFC tags (total 600 tags)
  - **Software:** GNU Radio (sampling rate 2MHz), Pytorch
  - **Evaluation metrics**: false acceptance rate (FAR), false rejection rate (FRR), and authentication, accuracy



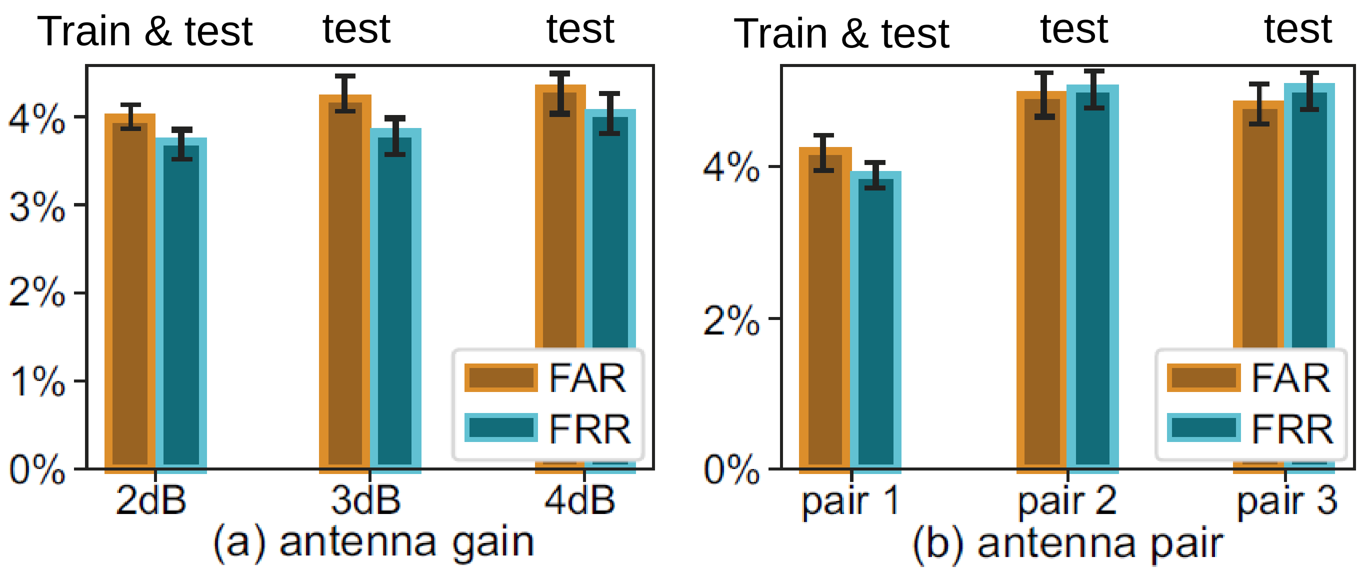
Experimental Results

- **Selection of frequency interval and loss threshold**
  - Frequency interval: 1KHz
  - Loss threshold: $\mu + 2\sigma$



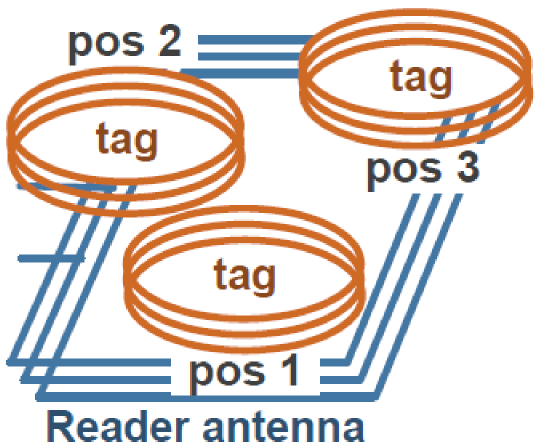
Experimental Results

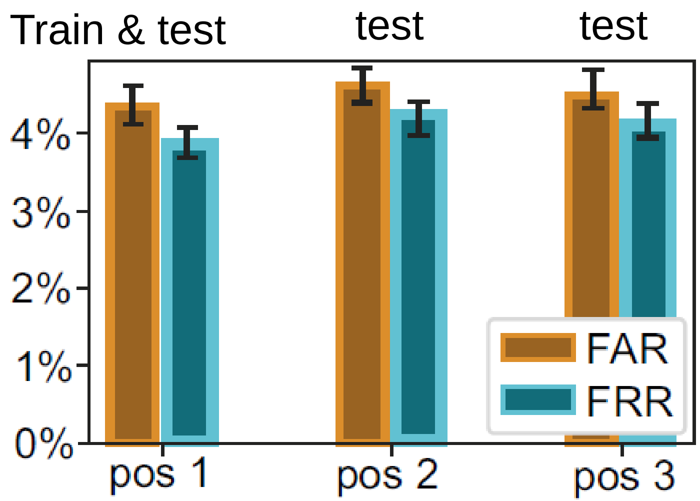
- **Effect of reader diversity and tag placement**
  - Different reader antenna gains and pairs: the FAR and FRR increase by ~1.5%



Experimental Results

- **Effect of reader diversity and tag placement**
  - Different tag placements: the FAR and FRR increase by ~1.0%





Experimental Results

- **Effect of tag model**
  - The FAR and FRR for different tag models are all below 5%
  - The authentication accuracy of the same tag model is 3% − 4% lower than that of different models

Same model	Ntag213	Ntag216	ULT	ULT C	F08
FRR	4.3%	3.8%	3.3%	3.5%	3.7%
FAR	4.8%	4.3%	4.5%	4.2%	4.1%

Diff. models	Ntag213	Ntag216	ULT	ULT C	F08
FAR	2.8%	2.5%	2.6%	2.3%	2.1%

Discussion & Limitation

- Current data collection for genuine tags is time consuming, we will consider saving the time cost by reducing the manual collection of TARs many times.

- Conduct more experiments under environment changes (temperature and humidity).

thank you!