南京郵電大學 Nanjing University of Posts and Telecommunications

FID:基于函数建模的数据独立和信道鲁棒的物理层识别

T. Zheng, Z. Sun and K. Ren, "FID: Function Modeling-based Data-Independent and Channel-Robust Physical-Layer Identification," IEEE INFOCOM 2019 - IEEE Conference on Computer Communications, Paris, France, 2019, pp. 199-207, doi: 10.1109/INFOCOM.2019.8737597

王润青

目 录

CONTENTS

研究背景

BACKGROUND

PART ONE

研究背景

基于密码技术

局限

- 需要额外计算资源

基于硬件指纹

优点

- 安全性
- 可靠性
- 高效性

优点

- 强安全性
- 防御物理攻击

射频指纹身份认证

优点

- 成本低
- 不需要额外的计算资源和硬件

现有射频指纹识别方法

射频指纹识别方案

01 基于位置的射频指纹识别

基于目标设备位置信息的无线电信号强度（RSS）、信道状态信息（CSI）、信道频率响应(CFR）等特征，用设备独特位置进行设备识别

02 基于瞬态和基于前导的射频指纹识别

基于过渡信号和前导信号中提取特征进行构建，利用经过身份验证的设备传输的所有RF信号数据包中某个固定段的唯一性来进行设备识别

03 基于调制误差的射频指纹识别

基于调制误差的系统，将调制误差的统计数据分配为设备指纹[1]

04 基于射频功率放大器建模的识别

射频功率放大器无线系统系统中一个重要的硬件部件，现有技术可以识别不同功率的放大器

05 基于深度学习的射频指纹识别

利用卷积神经网络（CNN）和递归神经网络(RNN）对无线信号进行分类，识别物联网设备

[1] Vladimir Brik, Suman Banerjee, Marco Gruteser, and Sangho Oh. Wireless device identification with radiometric signatures. In Proceedings of the 14th ACM international conference on Mobile computing and networking, pages 116127. ACM, 2008.

目前研究局限

- **数据依赖性：只使用相同的信号段进行识别，容易受到信号重放攻击**
- **低鲁棒性：大多现有指纹识别系统对空间变化和信道效应不具有鲁棒性**[2]
- **受限的特征空间：大多现有指纹识别系统完全依赖某些特征，性能受到相关低维空间限制**

现有的大多数射频指纹识别系统具有数据依赖性，对空间变化和无线信道效应不具有鲁棒性

基于位置的认证 对空间变化敏感

基于瞬态的认证 具有数据依赖性

基于前导的认证 具有数据依赖性

基于调制误差的认证 受低维特征空间限制

[2] Boris Danev and Srdjan Capkun. Transient-based identification of wireless sensor nodes. In Proceedings of the 2009 International Conference on Information Processing in Sensor Networks, pages 2536. IEEE Computer Society, 2009.

南京郵電大學
Nanjing University of Posts and Telecommunications

本文工作

Our work

PART TWO

研究目标与所作贡献

研究目标：

- 通过从设备随机收集的射频数据包识别物联网设备，避免重放攻击
- 对空间变化和多径信道具有鲁棒性
- 识别在低维特征空间中无法区分的物联网设备

贡献：

- 将物理层过程抽象为数学表达式F
- 考虑F直接推出的困难性，借助F建立函数模型并将其作为射频指纹，进行硬件识别
- 基于该函数模型设计指纹识别系统FID
- 将方案应用到实验中，验证其性能

南京郵電大學
Nanjing University of Posts and Telecommunications

射频指纹识别系统函数建模

FID FUNCTION MODELING FOR FINGERPRING

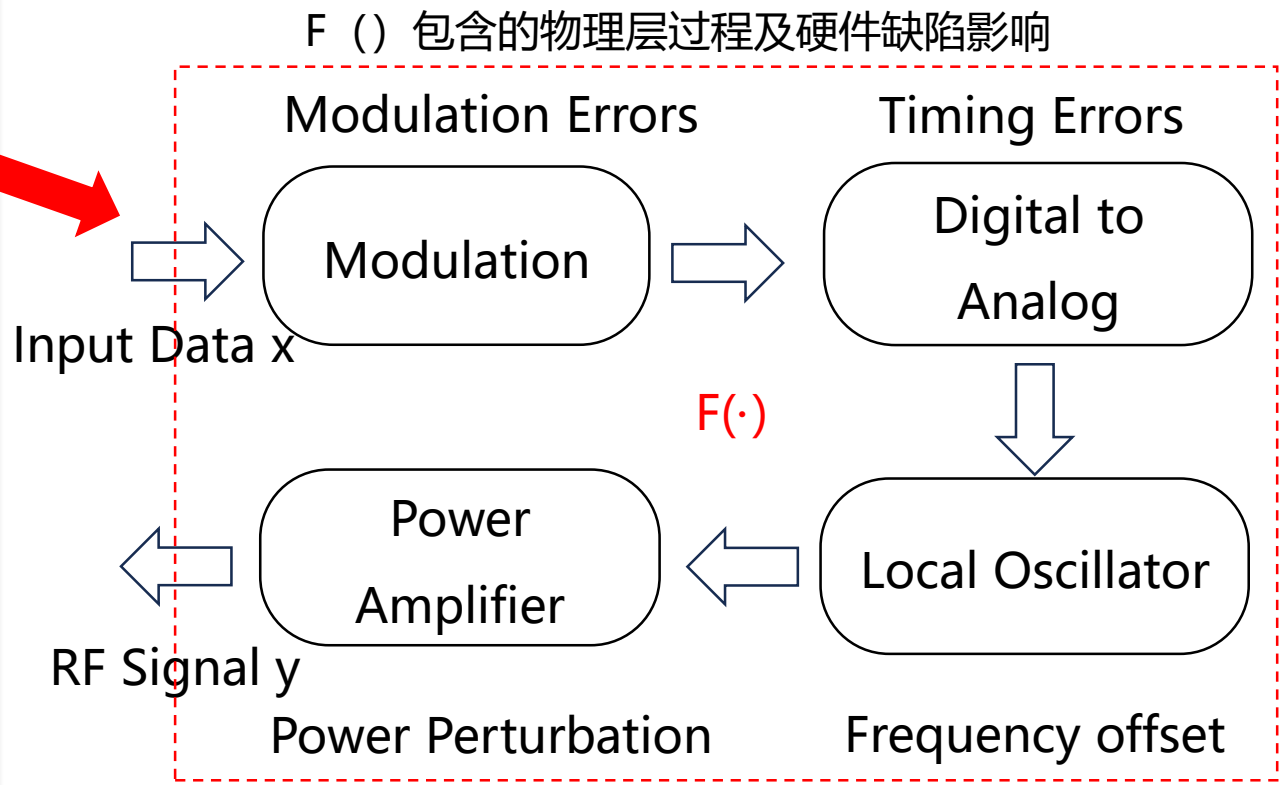
PART THREE

FID函数模型建模

数学函数F()：

- F()为物理层从调制到功率放大过程的数学表达式，可以代表无线设备物理层过程中硬件缺陷的所有影响
- F()的输入为传输数据x，输出射频信号y，即y=F(x)
- F()与传输的数据和外部无线信道无关

F()直接推出具有困难性，提出一个模型学习F()，并利用该函数模型作为射频指纹识别系统FID的指纹



硬件缺陷的函数模型

01 建模函数选取

简化：选择一个更简单的中间函数f()建模

$$y = F(x)$$

$$y = f(T(x))$$

$$y = f(ideal)$$

建模函数可以进行简化的原因

由传输数据x到理想信号ideal的转换由通信协议定义

T(x)=ideal

其中T()为通信协议，是已知的

F()函数输入：传输数据x

F()函数输出：无线设备发出的射频信号

F()函数的输入：理想信号

F()函数的输出：无线设备发出的射频信号

硬件缺陷的函数模型

02 定义和符号

符号：

理想信号ideal：x(t)
射频信号y：y(t)

$y(t) = f(x(t))$

信号采样:

在$kT_s + \tau(k = 0,1,2 \ldots)$处采样

1.采样间隔Ts

2.采样相位τ

第n个采样值为x[n]、y[n]

硬件缺陷的函数模型

03 f（•）的离散形式

y[n]：

· y[n]受到x[n]及其两侧信号的影响，是关于理想信号一段的函数

· y[n]是关于采样相位τ的函数

信号采样

理想信号的一段，即x[n]两侧信号：

$$x_n(t) = \{x(t) \mid (n-k)T_s < t < (n+m)T_s\}$$

f()的离散形式可以表示为：

$$y[n] = f(x_n(t), \tau)$$

硬件缺陷的函数模型

04 f（•）的推演

$$f(x_n(t),\tau) = A^t(x_n(t),\tau)e^{iw_c^t t + i\theta^t(x_n(t),\tau)}$$

本地振荡器存在缺
波频偏

$$f(x_n(t),\tau) = A^r(d)\left(1+\mathrm{pow}^r(x_n(t),\tau)\right)$$
$$e^{i\theta_0 + i(\Delta w^t - \Delta w^r)(nT_s+\tau)+i\theta(nT_s+\tau)+i\Theta^r(x_n(t),\tau)}$$

分解为
性部分

f

载波频
偏，输出转化为能
获取到的接收信号

$$f(x_n(t),\tau) = A_0^r(1+\mathrm{pow}^r(x_n(t),\tau))$$
$$e^{i\theta_0 + i(\Delta w^t - \Delta w^r)(nT_s+\tau)+i\theta(nT_s+\tau)+i\Theta^r(x_n(t),\tau)}$$

硬件缺陷的函数模型

05 多径信道建模

多径信道是由信道反射和折射引起的，如果无线通信中存在多条路径，接收到的信号可以看作射频信号的总和

$$Z[n] \approx \sum_{i=1}^{N} h[i] \cdot f(x_{n-i}(t), \tau)$$

$f(x_n(t), \tau)$从$Z[n]$中反卷积出来，用于设备识别

射频指纹识别系统设计

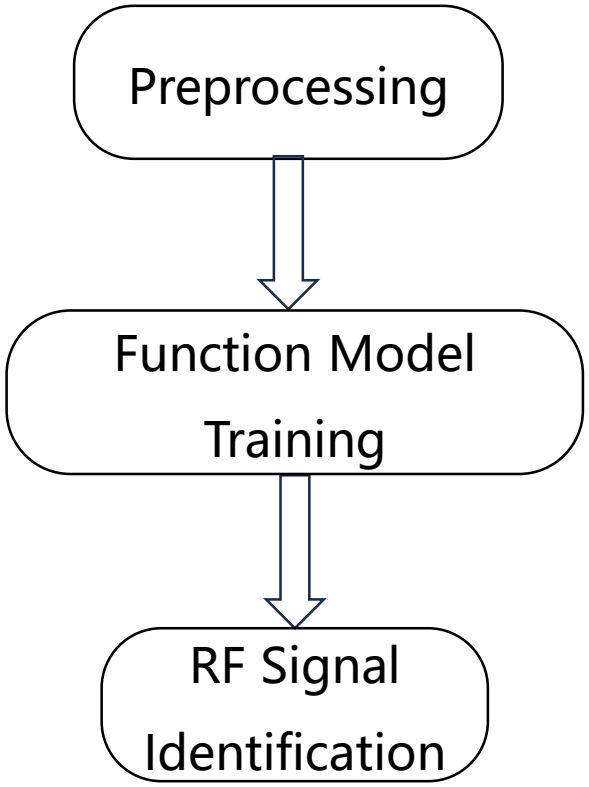
FID SYSTEM DESIGN

PART FOUR

FID系统

FID系统模块：

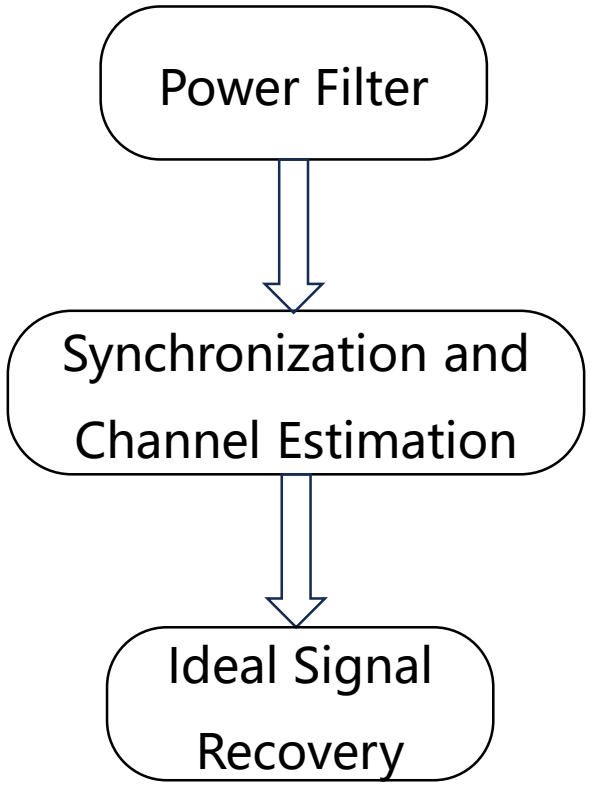
- **预处理模块：从接收信号中提取线性项和参数**
- **函数模型训练模块：训练函数模型**
- **射频信号识别模块：利用来自预处理模块和函数模型训练模块的输出结果识别接收到的射频信号**



系统模块

FID系统模块

01 预处理模块



功能滤波器找到每个信号包的起点和终点,定位信号包

同步和信道估计同步接收到的包，计算载波频偏

$$\Delta w^t - \Delta w^r = \left[E\left(\angle(z^*[n]z[n+1]) - \angle(x^*[n]x[n+1])\right)\right]/T_s$$

理想信号恢复计算出理想的数字样本

$$e^{i\left(\sum_{i=p+1}^{i=n}\theta(iT_s)-\theta((i-1)T_s)+\theta(p)\right)}$$

计算得到接收信号中所有线性部分，作为下面两个模块的输入

FID系统模块

01 预处理模块•计算载波频偏

将接收样本的反卷积结果视为$z[n]$，相邻接收数字样本之间的相位差$\Delta\theta_z[n]$

$$\Delta\theta_z[n] = \angle(z^*[n]z[n+1])$$

载波频偏计算：

$$\Delta w^t - \Delta w^r = \left[E\left(\angle(z^*[n]z[n+1]) - \angle(x^*[n]x[n+1])\right)\right]/T_s$$

FID系统模块

01 预处理模块•计算理想数字样本

根据建模结果：

$$\Delta\theta_z[n] = (\Delta w^t - \Delta w^r)T_s + \theta((n+1)T_s + \tau) - \theta(nT_s + \tau) \\ +\Theta^r(x_{n+1}(t), \tau) - \Theta^r(x_n(t), \tau)$$

两个相邻理想信号的相位差$\theta((n+1)T_s) - \theta(nT_s)$可由其近似表示：

$$\angle(z^*[n]z[n+1]) - (\Delta w^t - \Delta w^r)T_s$$

理想数字样本恢复：

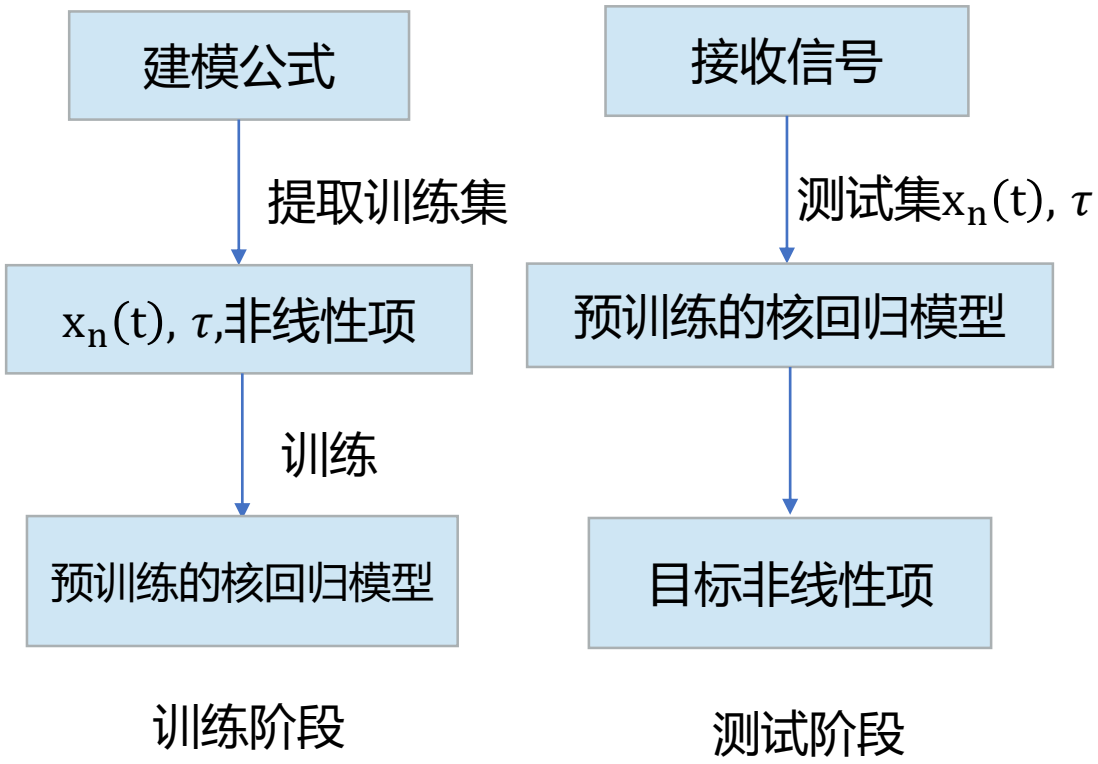
$$e^{i\left(\sum_{i=p+1}^{i=n}\theta(iT_s) - \theta((i-1)T_s) + \theta(p)\right)}$$

硬件缺陷的函数模型

02 函数模型训练模块·核回归模型

为了实现核回归，在信号段$x_n(t)$中选择有代表性的数字样本代替$x_n(t)$作为输入向量：

$$[x'[n-k], x'[n-k+1], \ldots, x'[n+m-1], x'[n$$



FID系统模块

03 射频信号识别模块

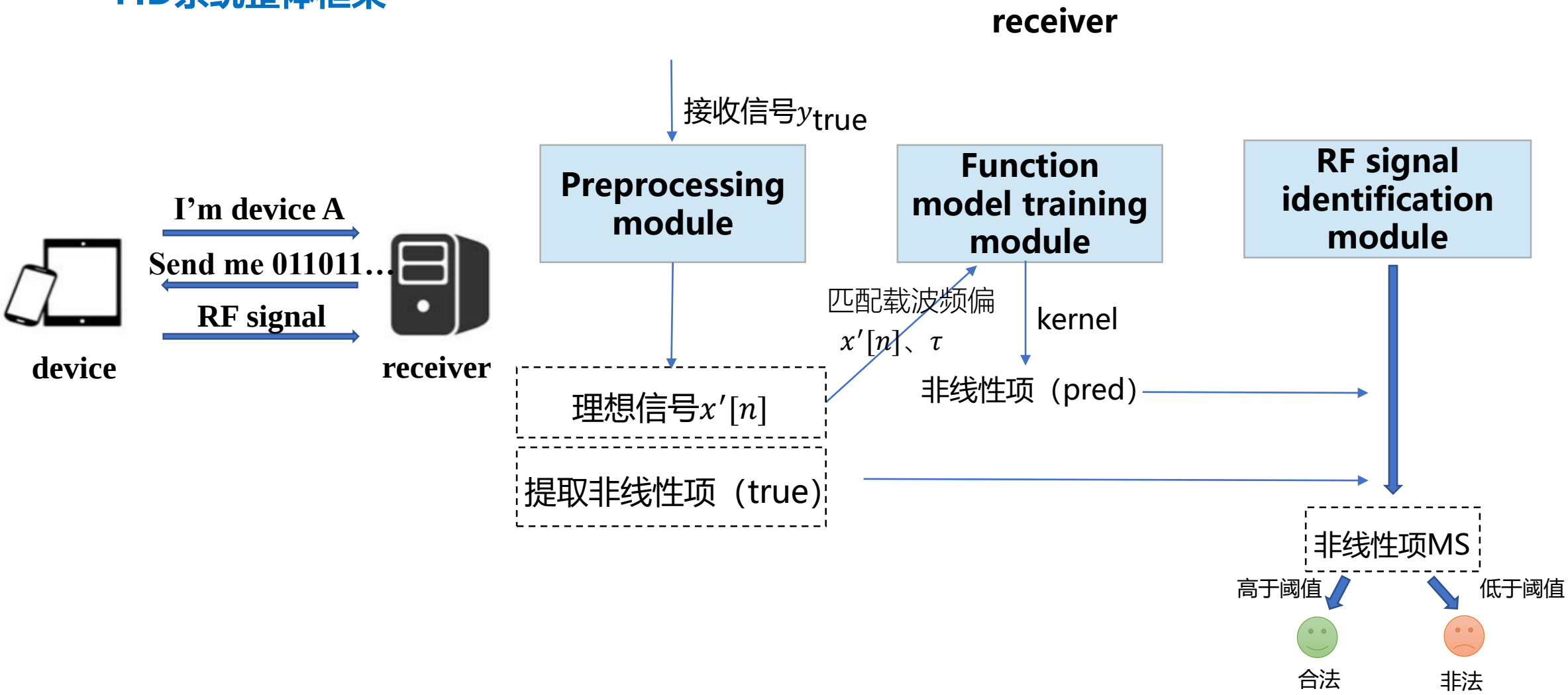
利用前两个模块识别接收到的射频信号，将接收到的射频信号与函数模型计算/预测的信号进行匹配

$$MS = 1 - \sum_{i=1}^{N} \left(y_{i,pred} - y_{i,\,\text{true}}\right)^2 / \sum_{i=1}^{N} \left(y_{i,\,\text{true}} - y_{\text{true}}\right)^2$$

通过打分结果，对设备进行识别

FID系统模块

FID系统整体框架



南京郵電大學
Nanjing University of Posts and Telecommunications

实验与分析

EXPEROMENTS AND ANALYSIS

PART FIVE

验证与评估

01 实验

性能指标：

- GAR：真实接受率
- GRR：真实拒绝率
- FAR：错误接受率
- FRR：错误拒绝率

GAR/GRR是指FID系统使用其函数模型成功/失败识别合法设备的比率

FAR/FRR是指FID系统使用其函数模型成功/失败识别非法设备的比率

平均识别精度（BIA）：

$$BIA = \frac{GAR + FRR}{GAR + FAR + GRR + FRR}$$

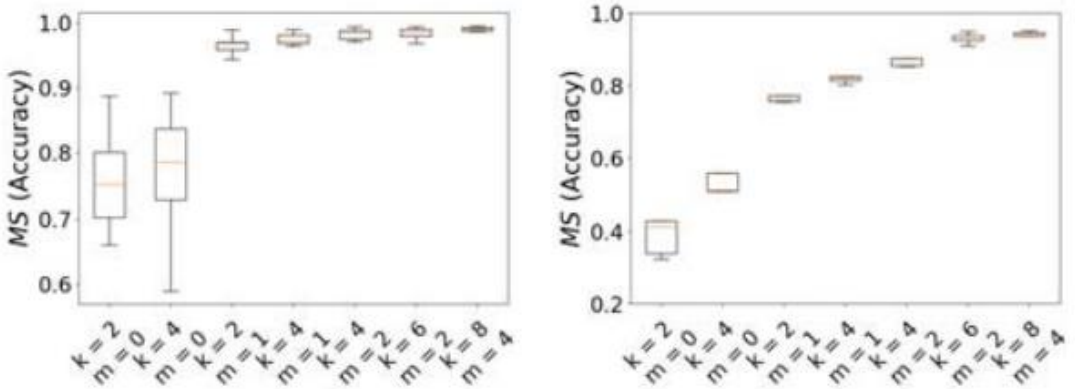
用于评估FID系统的整体性能

验证与评估

02 函数模型精度

任务：

- 验证两个核回归模型$pow^r(x_n(t),\tau)$、$\Theta^r(x_n(t),\tau)$的准确性
- 输入向量$[x'[n-k],x'[n-k+1],\ldots,x'[n+$



(a) $pow^r(x_n(t),\tau)$ (b) $\Theta^r(x_n(t),\tau)$

Fig. 8: Modeling accuracy of those two KR models

设置k=8和m=4训练模型

验证与评估

03 函数模型效率

- 函数模型的训练时间高度依赖训练数字样本的数量
- 当训练数据量大于40000时，建模精度可以进行设备识别
- 相比于RNN，本文函数模型更加省时

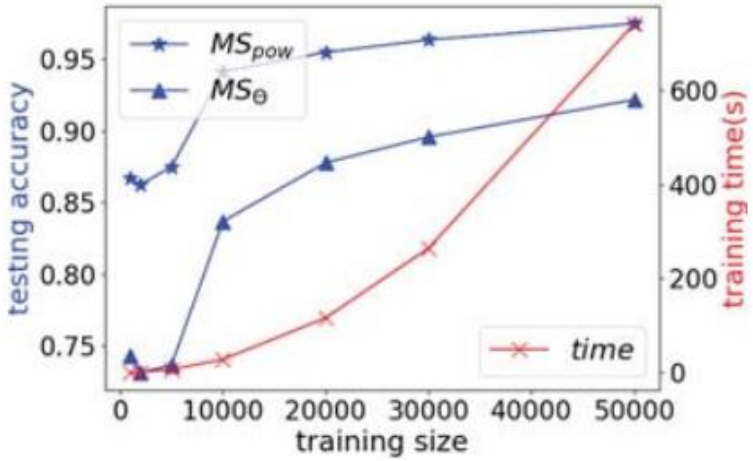


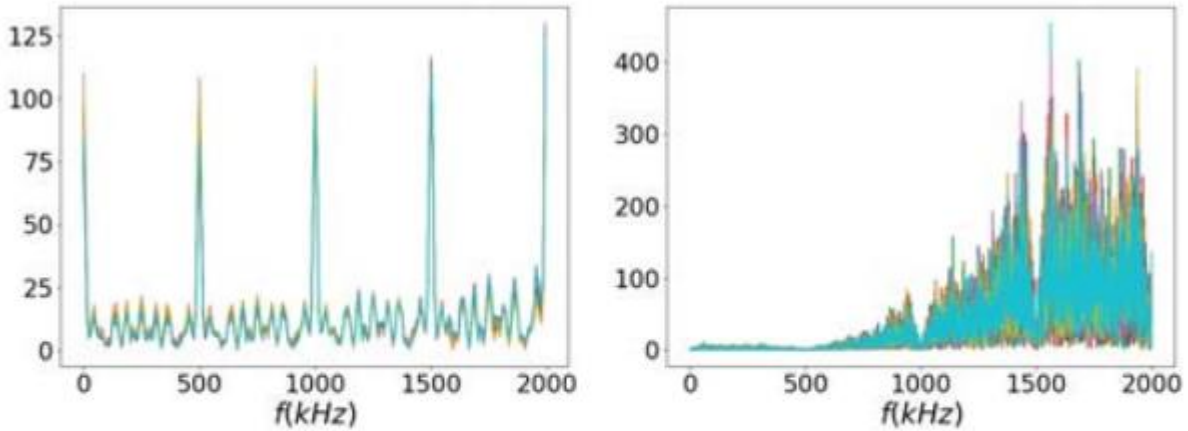
Fig. 9: Testing accuracy and training time

训练数字样本数量的增加，训练时间随之增加
训练数据量大于40000时，模型精度较高

验证与评估

04 数据独立性验证

- 所有输入数据由随机数生成器生成，所有用于训练、测试和识别的射频信号包都是随机信号包
- 计算收集到的信号包的相关性，相关系数均值为0.18~0.19，方差约为0.03，前导信号间的相关系数均值为0.98~0.99
- 绘制随机采集信号包的FFT频谱，前导信号FFT频谱相似，随机信号数据包FFT频谱不同



(a) preambles (b) random packets

Fig. 10: FFT Spectrums of the 10 preambles and 10 random packets collected from one device

验证与评估

05 识别性能评估

性能评估：

- 可以准确识别调制误差系统无法区别的相似度高的两对传感器

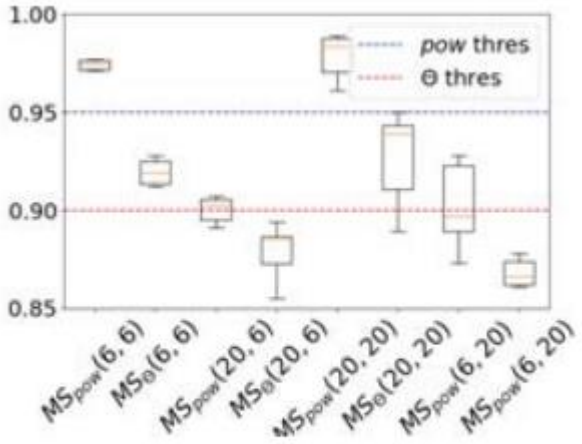


Fig. 11: MSs of two most similar sensors

TABLE I: Comparison between $\mathcal{F}$ID and modulation error-based system (in line-of-sight environments)

	$\mathcal{F}$ID				Modulation error-based System	
	overall performance		two most similar devices		overall performance	two most similar devices
GAR, GFR	0.97, 0.03	1.0, 0.0	0.94, 0.06	1.0, 0.0	0.91, 0.09	0.58, 0.42
FAR, FFR	0.0, 1.0	0.0, 1.0	0.0, 1.0	0.0, 1.0	0.12, 0.88	0.44, 0.56
BIA	0.99	1.0	0.97	1.0	0.90	0.57

总结

CONCLUSION

PART SIX

总结与展望

总结

1.针对大多现有射频指纹识方法具有数据依赖性等局限，提出一种射频指纹识别系统

2.将物理层过程抽象为数学表达式F，借助F进行函数建模，并将该模型作为硬件识别的射频指纹

3.基于该函数模型设计射频指纹识别系统FID，进行实验，验证其性能

未来展望

1.通过射频指纹识别系统FID，攻击者使用高端射频收发器能够复制与真实信号非常相似的信号

2.函数建模方法可以用于攻击大多数现有的射频指纹系统，防御这种攻击具有挑战性

南京郵電大學
Nanjing University of Posts and Telecommunications

感谢聆听！