



Federated Radio Frequency Fingerprinting with Model Transfer and Adaptation

Chuanting Zhang, Shuping Dang, Junqing Zhang, Haixia Zhang,
and Mark Beach

Communication Systems and Networks (CSN) Research Group



Acknowledgement

This paper is supported by **SWAN** Prosperity Partnership
(**S**ecure **W**ireless **A**gile **N**etworks)



<https://www.swan-partnership.ac.uk/>

The SWAN project is jointly funded by



TOSHIBA



ROKE



Content

- Background on Security and RF Fingerprinting
- Current Approaches and Challenges
- Our Proposed Method
- Experimental Results
- Conclusion



Wireless security threatens

- Cyber attack happens almost everywhere in many fields.

WIRI® BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY

ANY CREWBOSS SECURITY AUG 18, 2016 4:29 PM

A New Wireless Hack Can Unlock 100 Million Volkswagens

A team of researchers has found that Volkswagen stores secret keys in car components that leave almost all its vehicles since 1995 vulnerable to theft.



IOT SOLUTIONS WORLD CONGRESS
MAY 21 - 23, 2024
BARCELONA - GRAN VIA VENUE

EXHIBIT THE EVENT ACTIVITIES CONGRESS MEDIA

Back to THE INDUSTRY NEWS
Industry Articles and IoT

5 INFAMOUS IOT HACKS AND VULNERABILITIES



The Internet of Things (IoT) envisages the world where all our electronic devices can communicate with one another. Just as the internet connects people, the IoT will connect our smart gadgets together. However, as with any fledgling technology, there are teething problems that can't be ignored as connected devices become more integrated into businesses and our everyday lives. The following five IoT hacks demonstrate the current vulnerabilities in IoT.

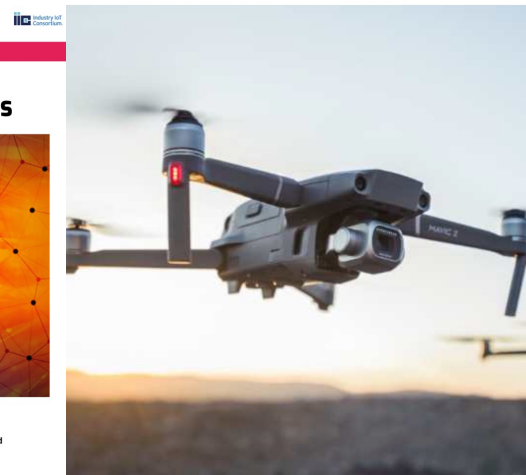
The Mirai Botnet

This hack took place in October of 2016, and it still ranks as the largest DDoS attack ever launched. The

threatpost Podcasts / Malware / Vulnerabilities / InfoSec

Human Error Blamed for Leak of 1 Billion Records of Chinese Citizens

Hack Allows Drone Takeover Via 'ExpressLRS' Protocol



kaspersky

Products Renew Downloads Support Resource Center Blog

Home Home Security Resource Center Threats

How to remove a hacker from your smartphone



Featured Article



Cracking WiFi at Scale with One Simple Trick

Ido Hoorvitch | 10/26/21

Share This! f t e in

How to

Phone had Fraudsters - harder to s; cyberattac hacks.



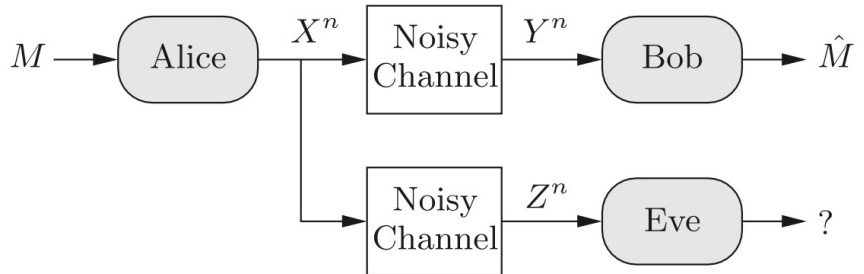
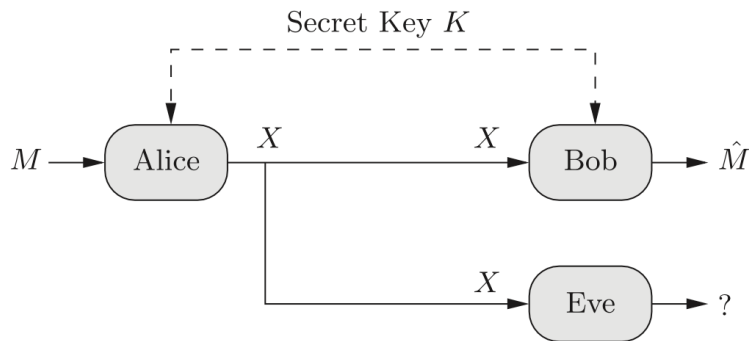
How I Cracked 70% of Tel Aviv's WiFi Networks (from a Sample of 5,000 Gathered WiFi).

In the past seven years that I've lived in Tel Aviv, I've changed apartments four times. Every time I faced the same scenario: the internet company took several days to connect the apartment, leaving me disconnected and frustrated while trying to watch laggy Netflix on the TV with my cellphone hotspot. A solution I have to this scenario is having the "Hello, I am the new neighbor" talk with the neighbors while trying to get their cell phone number in case of emergencies — and asking if I could use their WiFi until the cable company connected me. I think we all can agree that not having internet easily falls into the emergency category! Often, their cell phone number was also their WiFi password!

I hypothesized that most people living in Israel (and globally) have unsafe WiFi passwords that can be easily cracked or even guessed by curious neighbors or malicious actors.

How to achieve security

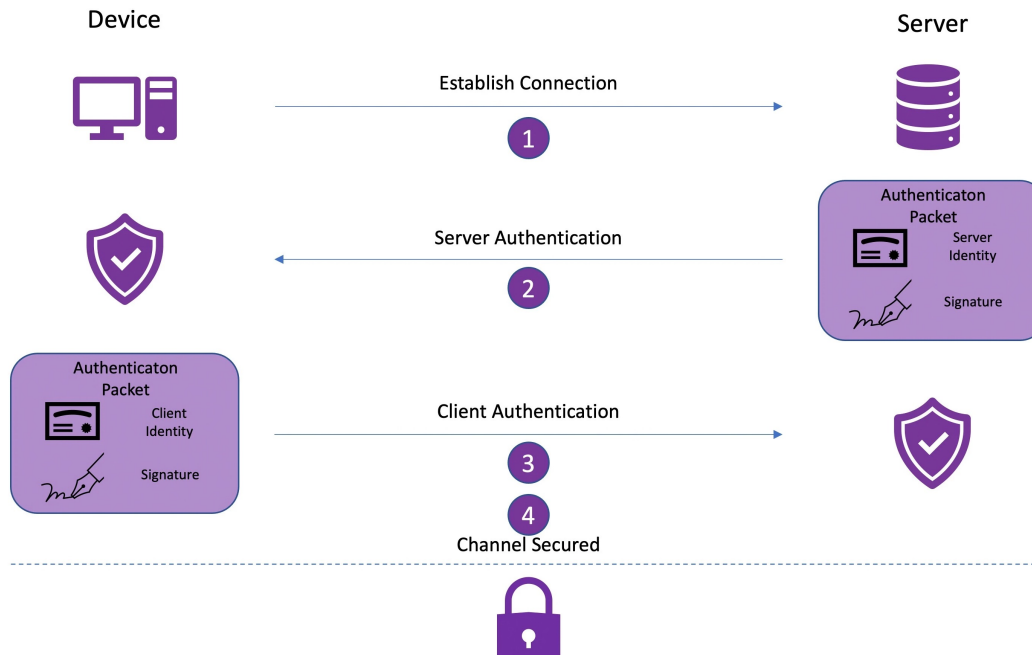
- Two fundamental primitives for any security systems.
 - **Secure transmission**



- H. V. Poor, R. F. Schaefer, "Wireless physical layer security," in Proceedings of the National Academy of Sciences, 2017, 114(1): 19-26.
- L. Lai, H. El Gamal and H. V. Poor, "Authentication Over Noisy Channels," in IEEE Transactions on Information Theory, vol. 55, no. 2, pp. 906-916, Feb. 2009.

How to achieve security

- Two fundamental primitives for any security systems.
 - **Secure transmission**
 - **Authentication/Identification**

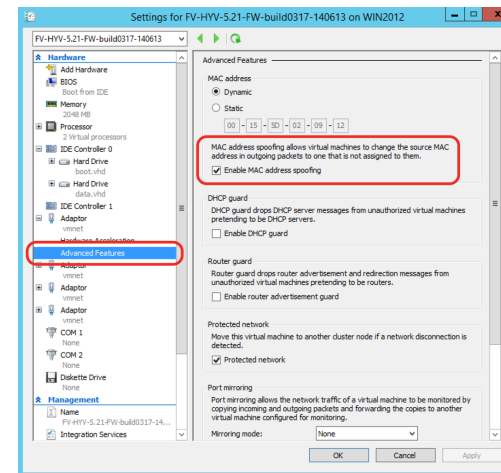


Device identification and authentication

- Traditional schemes are mainly based on techniques stemming from **cryptography** such as encryption or solely based on **MAC address**.



Security is not guaranteed if keys are compromised



MAC address can be easily manipulated

RF fingerprinting

- RFF: An emerging physical layer security technique that helps with **device identification by exploiting hardware impairments** that are hidden in the electromagnetic waves of the transmitter;
- Recent research has found that **every transmitter has its unique RF fingerprint** resulting from imperfections of analog components, which are **non-reproducible** by attackers.

RF fingerprinting

- Consider a signal $s_t = I_t + jQ_t$.

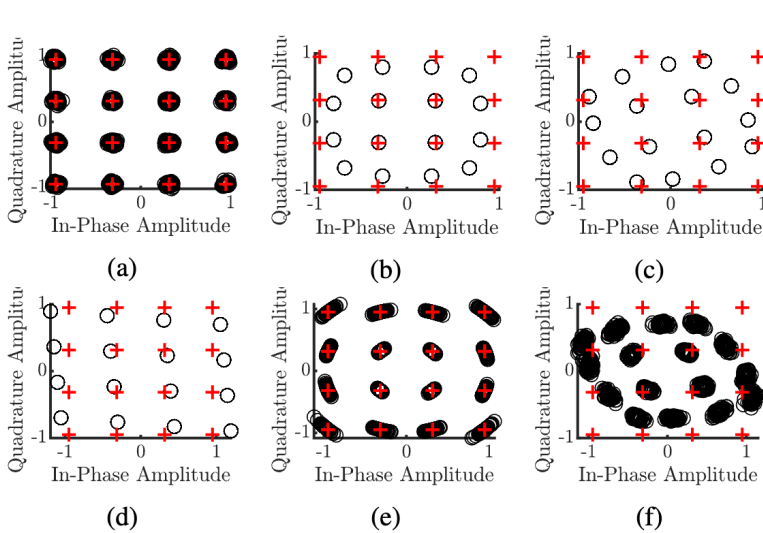
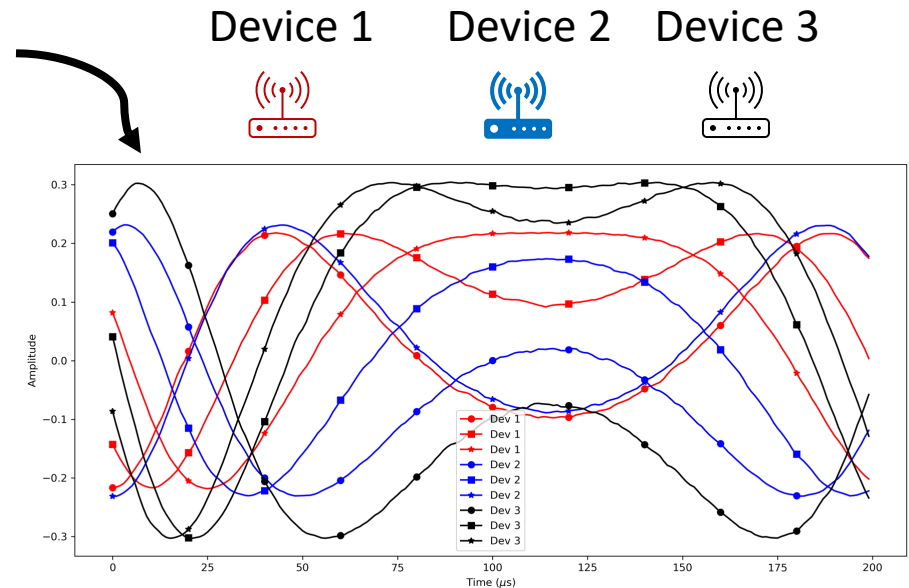


Fig. 1: RF impairments simulation. (a) Signal vs signal with AWGN noise; (b) Signal vs signal with amplifier distortion; (c) Signal vs signal with AM/PM conversion; (d) Signal vs signal with phase imbalance; (e) Signal vs signal with phase noise; (f) Signal vs signal with multiple impairments.



These hardware impairments are hidden in the signal emitted by different devices. RFF is identifying which device this signal belongs to by using a user-defined function $f(\cdot)$

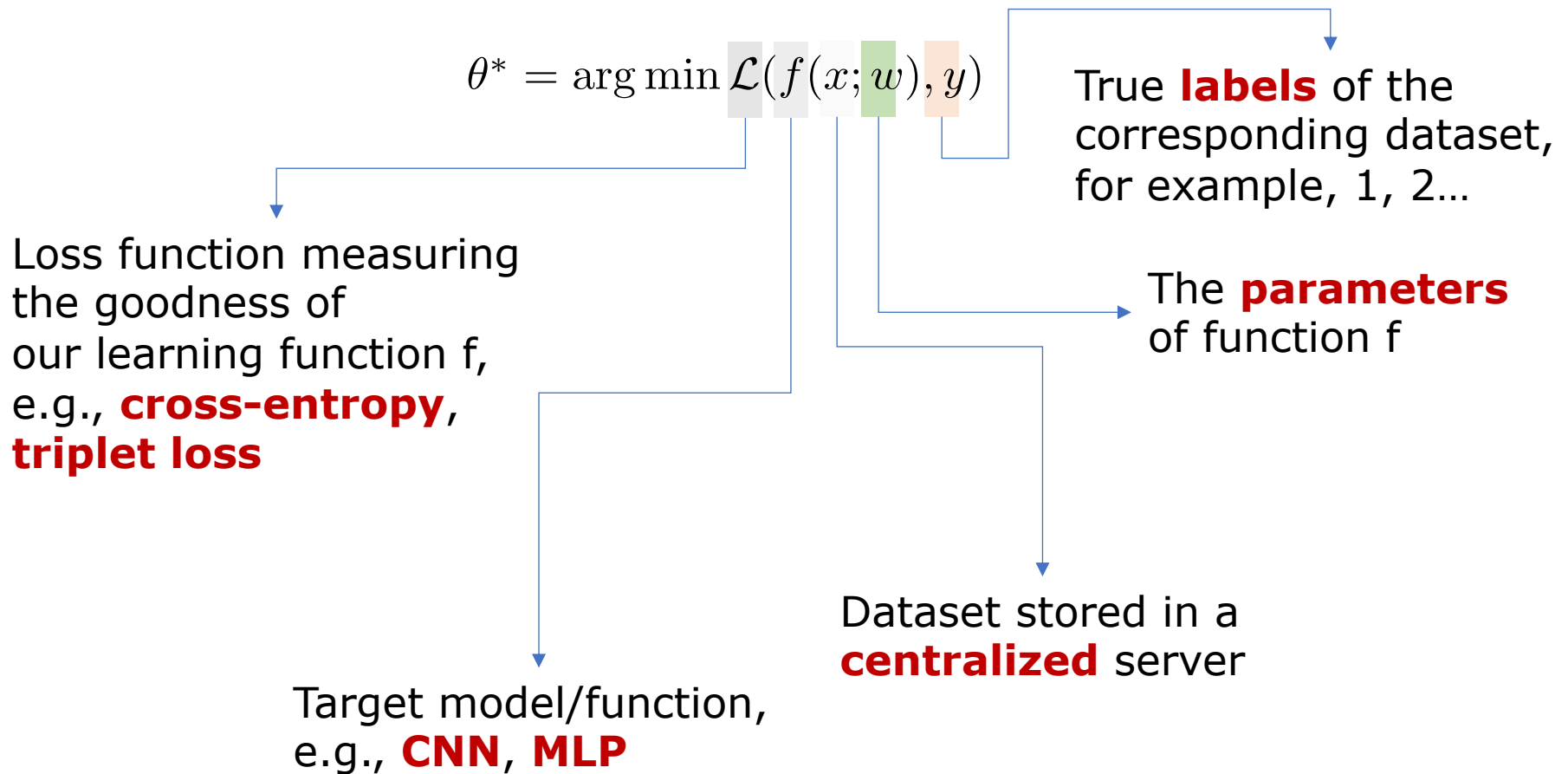
Content

- Background on Security and RF Fingerprinting
- Current Approaches and Challenges
- Our Proposed Method
- Experimental Results
- Conclusion



How to design $f(\cdot)$?

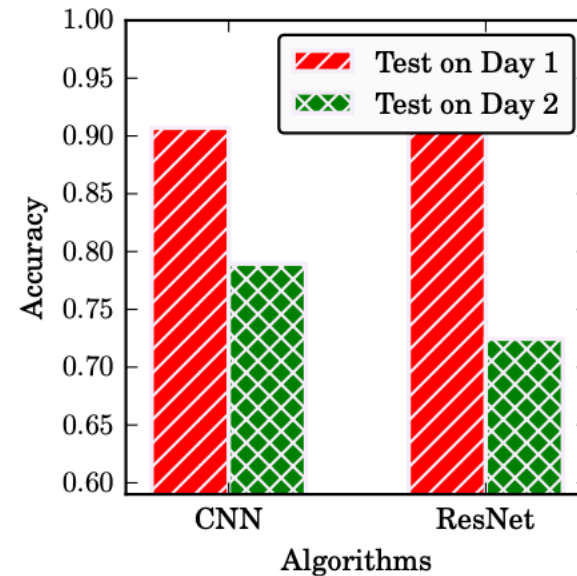
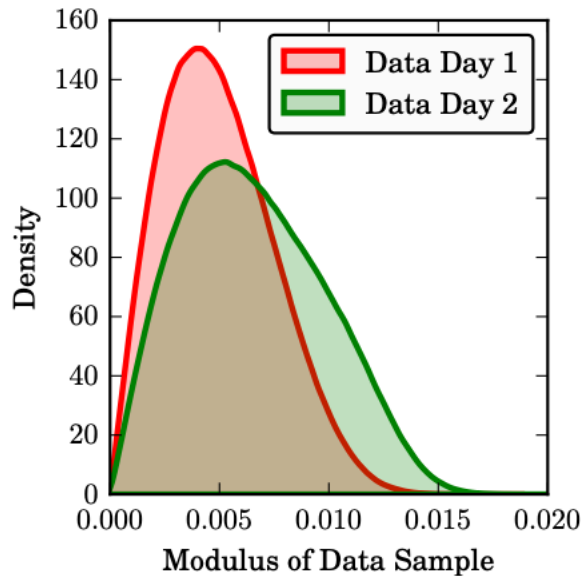
- State-of-the-art RFF learning models.



Challenges of centralized RFF

- Centralized RFF is inappropriate when **data privacy and protection** is a must; users are not incentivized to share data to a centralized entity (server) since their **data may contain private information**;
- Unrealistic to assume that a centralized dataset is always updated with signal collections as **new devices are continuously entering the market**;
- **Data distribution mismatch** between training and test if wireless environment changes.

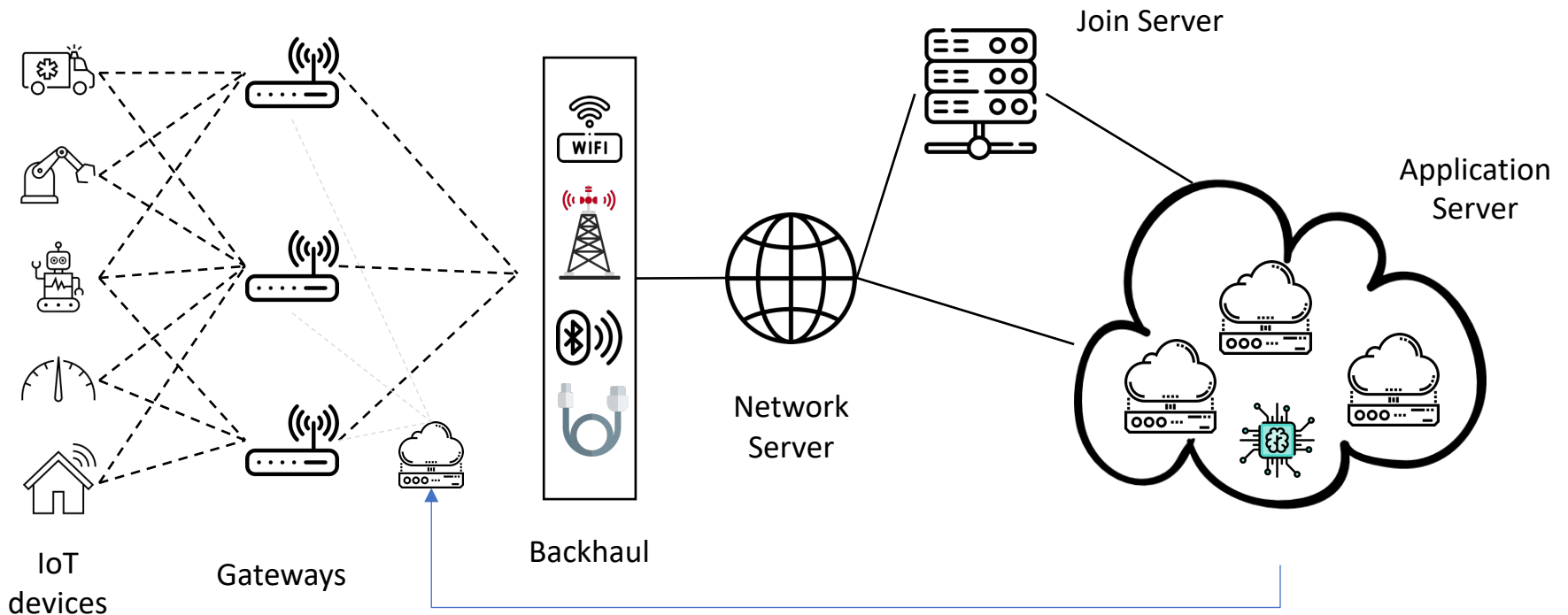
Data distribution mismatch



Train a model using data day 1 and test the model on the data of day 2, leading to a considerable performance degradation.

Solutions

- Push RF fingerprinting to the network edge and solve the data distribution mismatch using transfer learning.



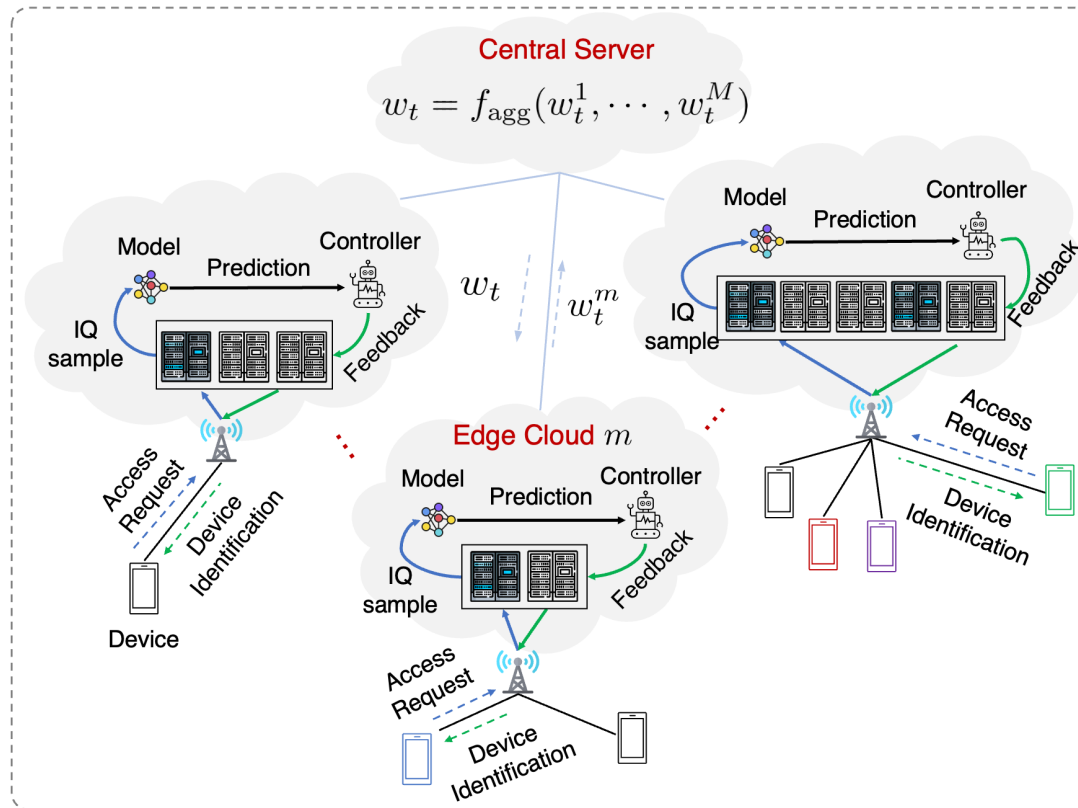
Content

- Background on Security and RF Fingerprinting
- Current Approaches and Challenges
- Our Proposed Method
- Experimental Results
- Conclusion

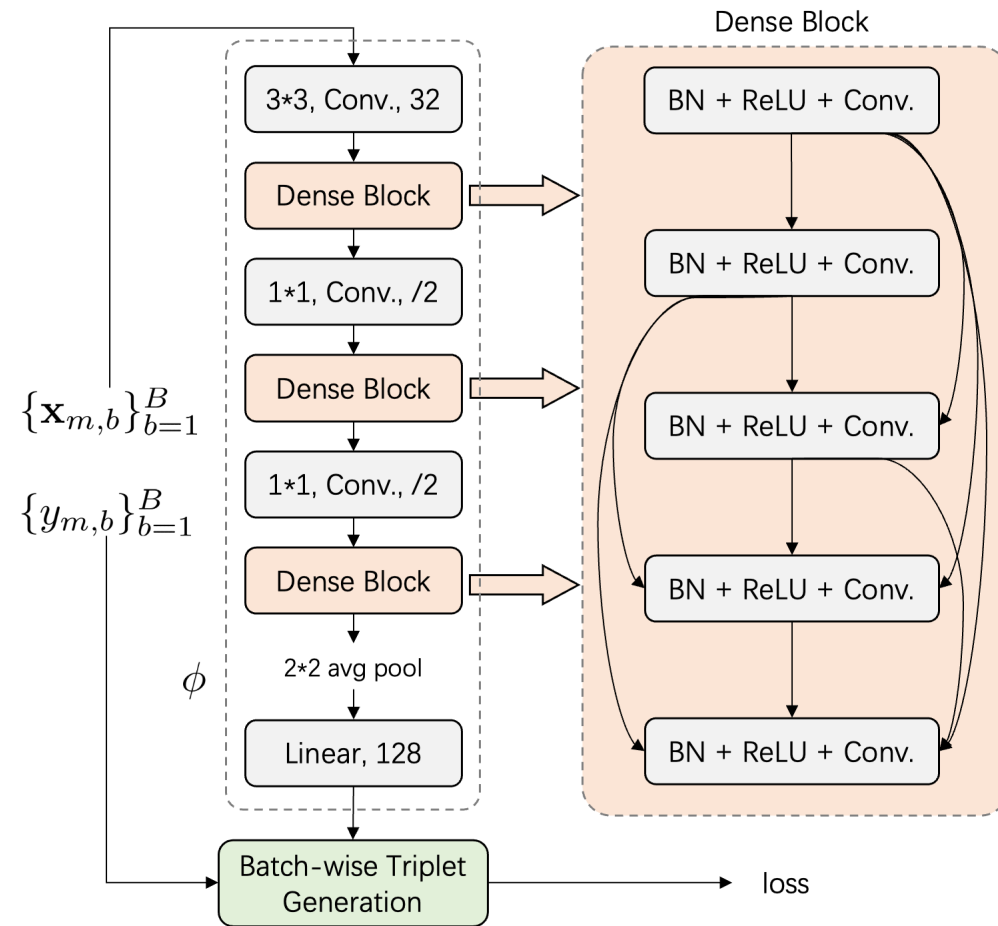


System model

- An RFF model is collaboratively trained by multiple edge nodes in a federated way.



Learning framework



- We introduce **dense connectivity** into RFF, making our framework **easy to train** (no gradient explosion or vanishing) and of **low complexity** (less parameter);
- We adopt **triplet loss** as our objective to **reinforce feature separation**

Transfer learning inspired model enhancement

- **Data distribution mismatch** between training samples and test samples will dramatically lower device identification accuracy;
- We propose **model transfer and adaption** (MTA) to solve the above challenge;
- Key idea: use the **pre-trained model** of one channel environment as the **initialization** of other environments (transfer) and **update it** using **very limited several data samples** to yield a new model (adaption).

Content

- Background on Security and RF Fingerprinting
- Current Approaches and Challenges
- Our Proposed Method
- Experimental Results
- Conclusion



Setups

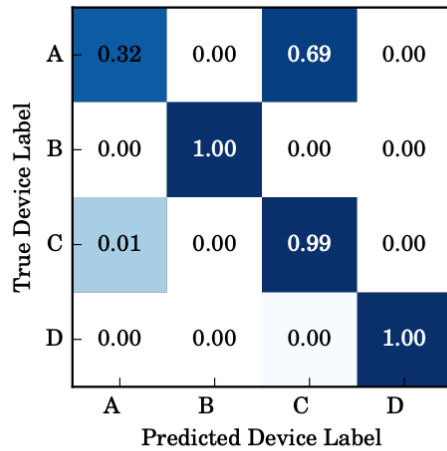
- We test our algorithm on a real world data, which is publicly available. The dataset contains **four devices' three different kinds of IQ samples**, i.e., Wi-fi, 4G LTE, 5G NR, logged in **two different days**;
- The first day's data (12000 samples) is used for training. For the second day's data (12000 samples), **ρ samples are used to perform MTA**, and others will be used to test performance;
- A federated learning scenario is mimic with **100 edge nodes**, the model is trained **50 rounds**, each round performs **10 local epochs** using **Adam** optimizer with a learning rate of 0.0001. The local batch size is 10.

Overall prediction performance

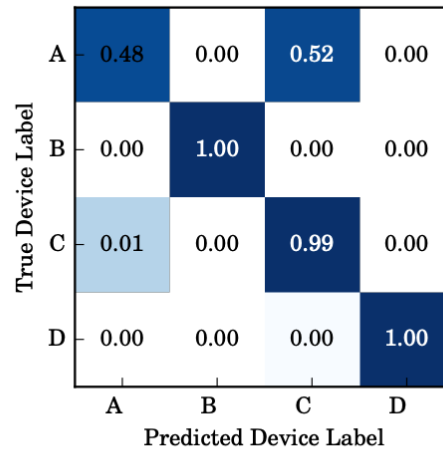
| | | Centralized ResNet | Federated MLP | Federated CNN | Federated ResNet | Proposed-Basic | Proposed-MTA |
|---------|-------------------|--------------------|---------------|---------------|------------------|----------------|---------------|
| Notes | # of Parameters | 157.54 K | 1.58 M | 1.19 M | 157.54 K | 79.95 K | |
| | Privacy-Preserved | ✗ | ✓ | ✓ | ✓ | ✓ | |
| Signals | 4G | 0.8257 | 0.7110 | 0.7895 | 0.7245 | <u>0.8683</u> | 0.9343 |
| | 5G | 0.8375 | 0.7123 | 0.7725 | 0.7448 | 0.9105 | <u>0.9100</u> |
| | WiFi | <u>0.9690</u> | 0.7205 | 0.8213 | 0.7688 | 0.7508 | 0.9800 |
| | Hybrid | 0.7268 | 0.6923 | 0.7553 | 0.7692 | <u>0.7721</u> | 0.9003 |

- We compare our algorithm with **several baselines**, i.e., centralized ResNet, federated MLP, federated CNN, federated ResNet.
- Two versions of our algorithm: **proposed-basic** and **proposed-mta**. The former means the model is trained without using MTA strategy while the latter using MTA strategy.
- Findings
 - Our algorithm achieves **much better prediction performance** than baselines, even without MTA strategy
 - Our algorithm has the **least parameter complexity**

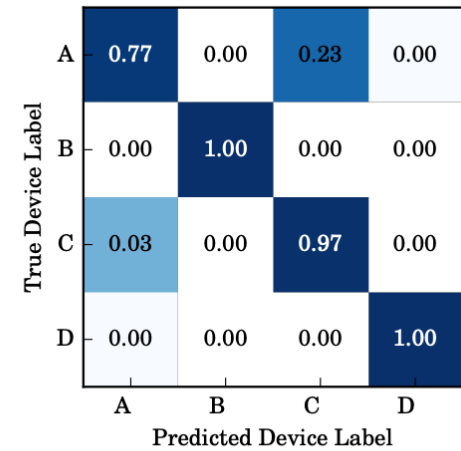
Per-device prediction performance



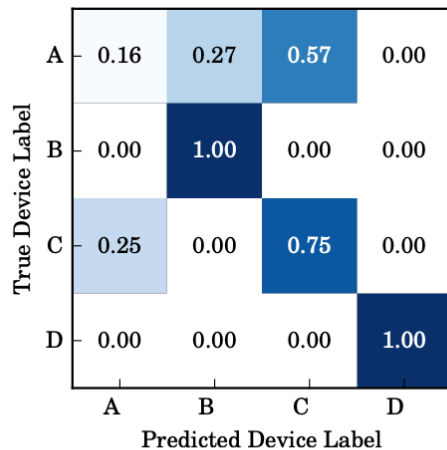
(a) Centralized ResNet (4G).



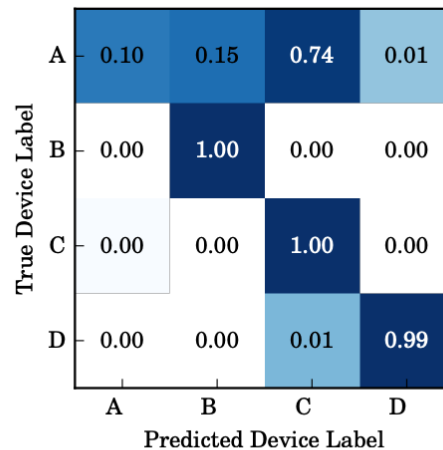
(b) Proposed-Basic (4G).



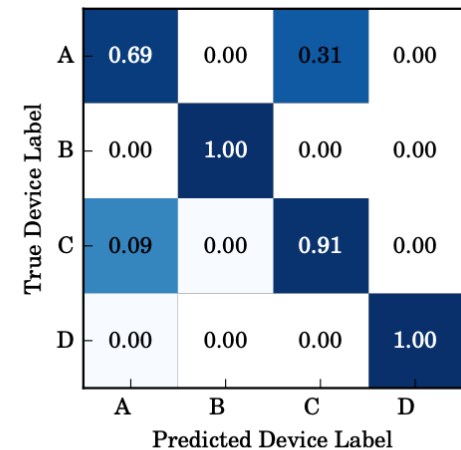
(c) Proposed-MTA (4G).



(d) Centralized ResNet (Hybrid).



(e) Proposed-Basic (Hybrid).



(f) Proposed-MTA (Hybrid).

Content

- Background on Security and RF Fingerprinting
- Current Approaches and Challenges
- Our Proposed Method
- Experimental Results
- Conclusion



Conclusion

- We considered the **RF fingerprinting problem in the scenario of federated learning** for edge networks;
- We proposed **a novel CNN framework** by introducing dense connectivity into RF fingerprinting;
- We designed **a strategy named model transfer and adaption (MTA)** to overcome the data distribution mismatch problem brought by time-varying wireless environments.

<https://www.swan-partnership.ac.uk/>



TOSHIBA



ROKE



Thanks for your time!

✉ chuanting.zhang@sdu.edu.cn

🏠 <https://chuanting.net>



IEEE International Conference on Computer Communications
17-20 May 2023 // New York area // USA

