Towards a Unified Few-Shot Learning Evaluation Framework for RF Fingerprinting

Sai Shi
Vahid Mahzoon
Xuyu Wang
Shiwen Mao
Jie Wu
Slobodan Vucetic

Table of Contents

Introduction

- **RF device fingerprints**: variations in transmitted signals due to hardware imperfections, creating unique characteristics in the physical layer, which can be used as device fingerprints
- **RF fingerprinting (RFFI)**: Classify wireless device based on the emitted signal captured by a receiver
- **Applications of RFFI**
  - Intrusion Detection: Detect unauthorized devices by recognizing unfamiliar RF signal patterns.
  - Device Authentication: Verify device identity using RF fingerprints.
  - User Tracking: Monitor user movement via consistent RF fingerprints across locations.

Introduction

- Traditional RFFI methods rely on hand-crafted physical layer features, such as transient phase, modulation, or spectral analysis.
  - Only work well with good features
  - May not capture all the complexities of real-world RF signals
- Deep learning methods can automatically capture complex feature representations from raw signals, and have been used in RF fingerprinting
- Requirement of deep learning models to work well:
  - The environmental conditions are stable
  - Large labeled data is available during training

Introduction

- **Challenge:** Distributional/domain shift **-** a change in the statistical properties of the data distributions between different environments
- RFFI is very sensitive to environmental conditions**,** which causes a model trained in one setting to perform poorly in a another

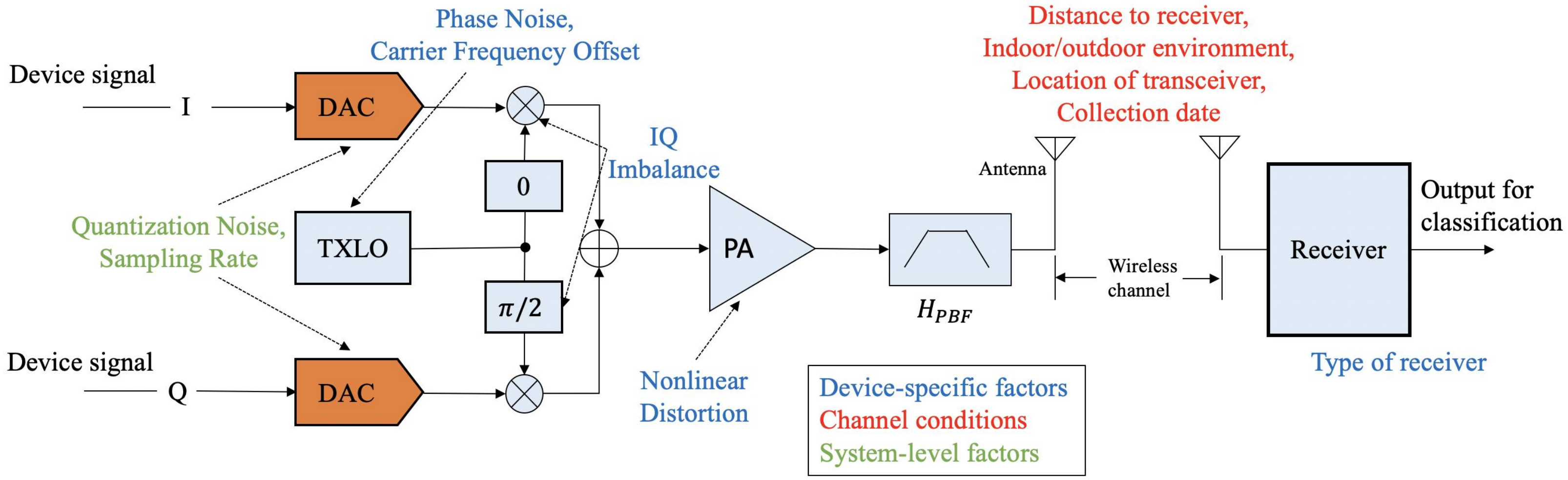


Figure - Potential domain shift in a wireless communication system (Our work focus on channel conditions - changes in the operating environment that affect signal propagation)

Related Work

- Few-shot learning (FSL): enable models to generalize to new tasks or classes using only a few labeled examples per class
  - Metric-based methods: prototypical network, matching network, etc.
  - Meta-learning methods: MAML, Reptile, Meta-SGD
  - Generation-based methods: data augmentation
- Domain adaptation (DA): adapt a model trained on one data distribution (source domain) to perform well on a different but related distribution (target domain)
  - Divergence-based methods: Maximum Mean Discrepancy (MMD), KL-divergence
  - Adversarial-based methods: Adversarial Discriminative Domain Adaptation
  - Reconstruction-based methods: Deep Reconstruction-Classification Network
- Few-shot Domain Adaptation: generalize a model trained on a source domain to a target domain with limited labeled data (typically a few examples per class) in the presence of domain shift.

Related Work: RF fingerprinting

- Model fine-tuning [1-2]
  - Freeze parameters of a pre-trained neural network and fine-tune parameters in the last few layers on target data
  - Limited performance and only compare with zero-shot baseline
- Domain adaptation
  - Adversarial-based DA [3]: focus on a single environmental change
  - KL-based alignment [4]: does not compare with other DA baselines
- Few-shot learning
  - Prototypical network with data augmentation [5]: only compare with zero-shot baseline
  - Siamese network [6]: focus on a single environmental change, does not compare with other meta-learning baselines

Related Work: research gaps

- Limitations in literature:
  - Evaluate on limited datasets or scenarios and often compare with weak or inconsistent baselines
  - Lack of analysis on a broader impact of diverse environmental factors
  - Lack of deeper analysis on how their methods mitigate domain shift
- Motivated by these research gaps, we aim to establish a standardized and reproducible FSL evaluation framework for RF fingerprinting
- Research Questions:
  - RQ1: How can RF fingerprinting models be adapted to new domains with minimal performance degradation with the help of FSL?
  - RQ2: How to fairly compare different FSL methods in RF fingerprinting and how exactly each method mitigates the domain shift problem?

Experimental Setup: Datasets

- LoRa RF dataset: time-domain IQ samples from 25 PyCom IoT devices
    - Scenario I: Different days
    - Scenario II: Different locations
    - Scenario III: Different configurations
    - Scenario IV: Different distances
- WiSig dataset: time-domain IQ samples collected over four days on 130 devices at the Orbit Testbed
- CORES dataset: signals collected over four days on 58 devices at the Orbit Testbed

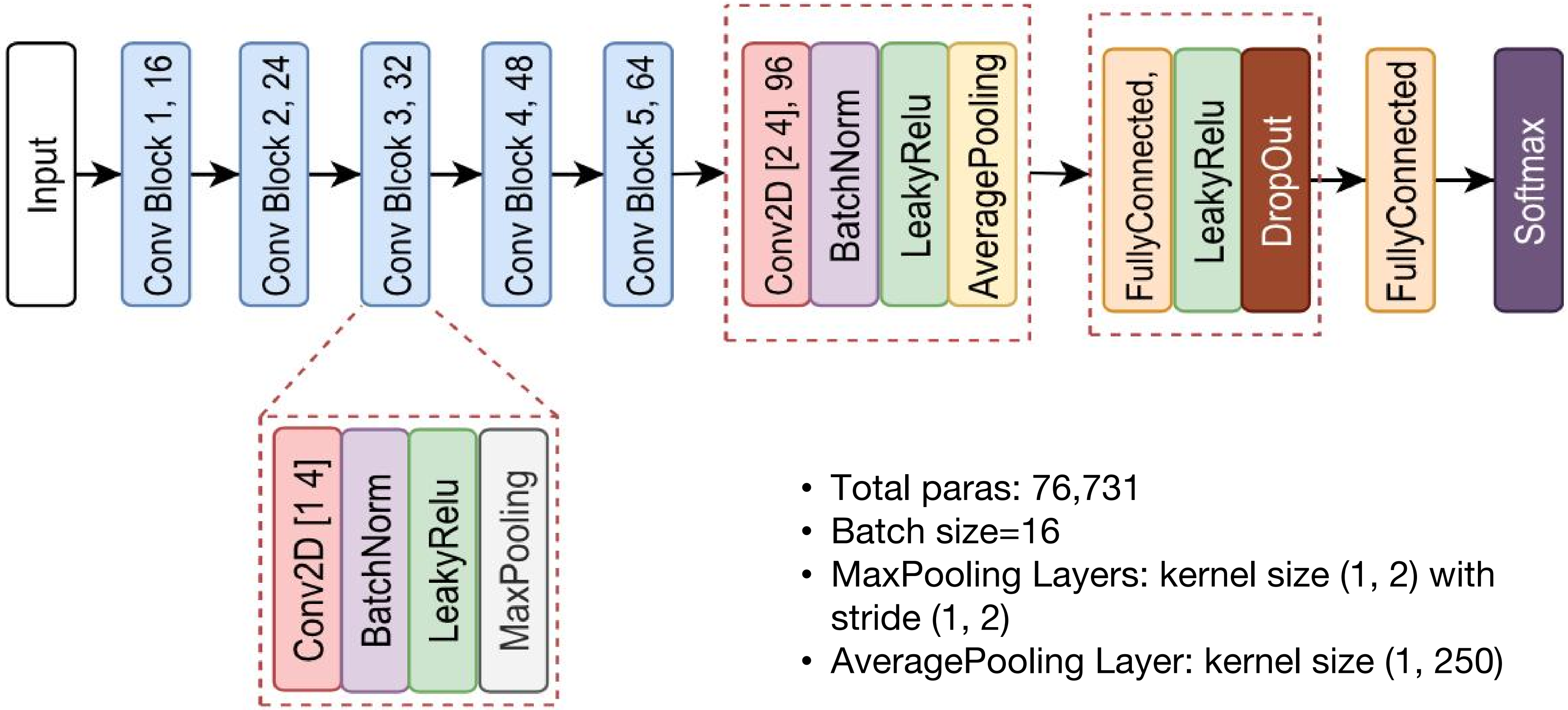
Experimental Setup: Scenarios

Setting	Domain Shift	Dataset	Source	Target
LoRa-Day	Day	LoRa	Day 1, 2	Day 3, 4
WiSig-Day	Day	WiSig	Day 1, 2	Day 3, 4
CORES-Day	Day	CORES	Day 1, 3	Day 2, 4
LoRa-Config	Configuration	LoRa	Config 1	Config 2
LoRa-Config	Location	LoRa	Office	Outdoor
LoRa-Distance	Distance	LoRa	15m	20m

Table - 6 domain-shift scenarios with diverse environmental changes

- Both source and target are split into 80% train set, 10% validation set, and 10% test set
- Model is trained using training samples from source and target (K=3), then evaluate on test samples from source and target (N=5)
- Evaluate on two baselines (weak and strong), two meta-learning and one domain adaptation methods

Approaches

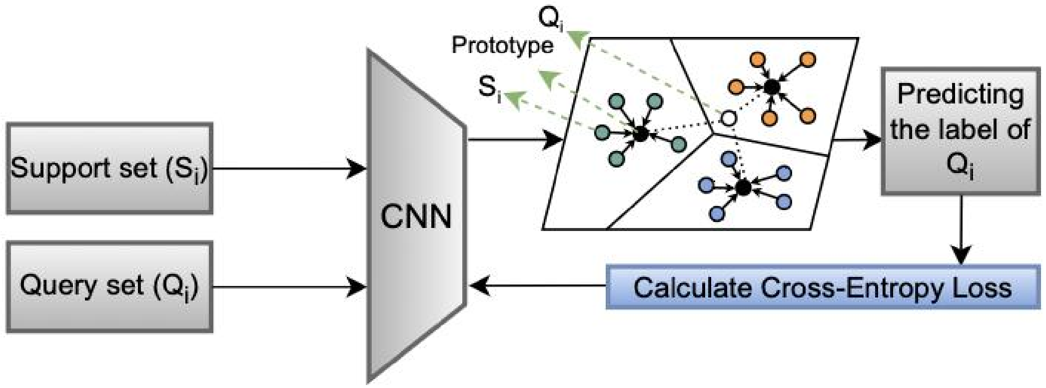


- Total paras: 76,731
- Batch size=16
- MaxPooling Layers: kernel size (1, 2) with stride (1, 2)
- AveragePooling Layer: kernel size (1, 250)

Fig - Our CNN architecture used in LoRa dataset

Approaches: few-shot learning

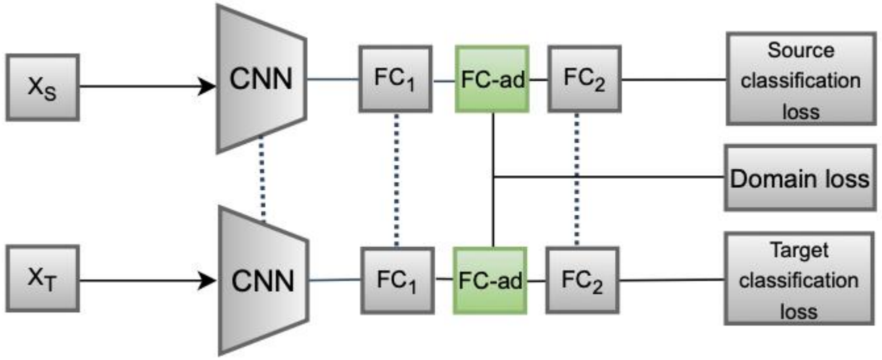
- **Metric-based FSL:** learn an embedding space and classify examples based on distance, two types of such methods are Prototypical Network (PTN) and Matching Network (MN).
- **Strength**
  - Achieve strong performance in FSL without requiring complex training procedures
  - Their distance-based classification mechanism is particularly suitable for RF fingerprinting, where signal similarity in the feature space often correlates with device identity



PTN framework

Approaches: domain adaptation

- **Divergence-based DA:** learn domain-invariant feature representations by explicitly minimizing some distance metrics between source and target distributions (e.g., Maximum Mean Discrepancy (MMD) focuses on distance between *mean embeddings* of features)
- **Strength**
  - Strong theoretical foundation on transferability across domains
  - Achieve competitive performance with lower computational requirements compared to adversarial-based DA



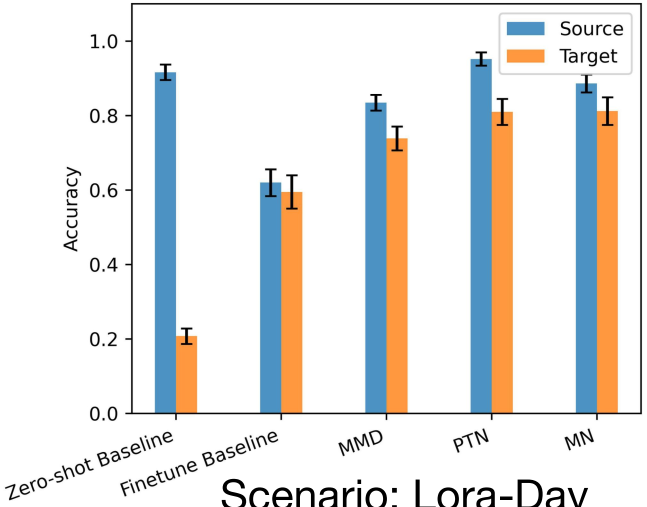
MMD-based domain alignment

Results: zero-shot baselines

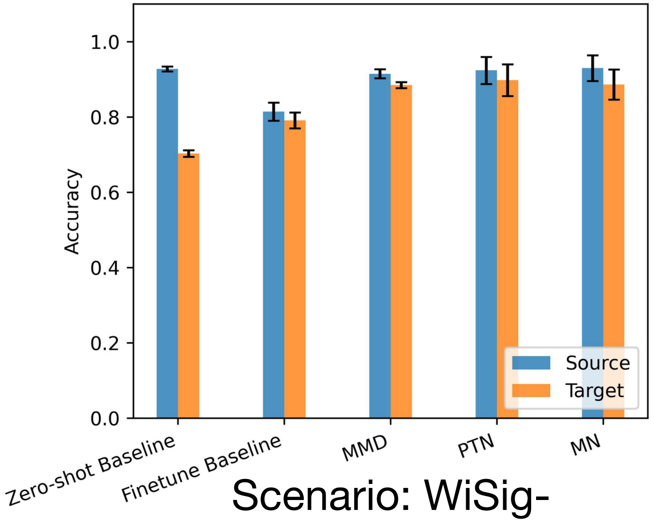
Accuracy		Target domain			
		Config 1	Config 2	Config 3	Config 4
Source domain	Config 1	65.25%	3.93%	4.13%	3.28%
	Config 2	2.52%	69.41%	3.97%	4.26%
	Config 3	3.25%	5.97%	58.69%	8.46%
	Config 4	2.10%	0.82%	4.26%	39.67%
Leave-One-Out		1.90%	3.44%	3.51%	7.15%
All-included		80.52%	73.61%	58.36%	38.56%

Accuracy under the scenario of different configurations on LoRa dataset
(* Leave-one-out uses all source tasks as train set excluding the target task, while all-included uses all source tasks as train set, including the target task)

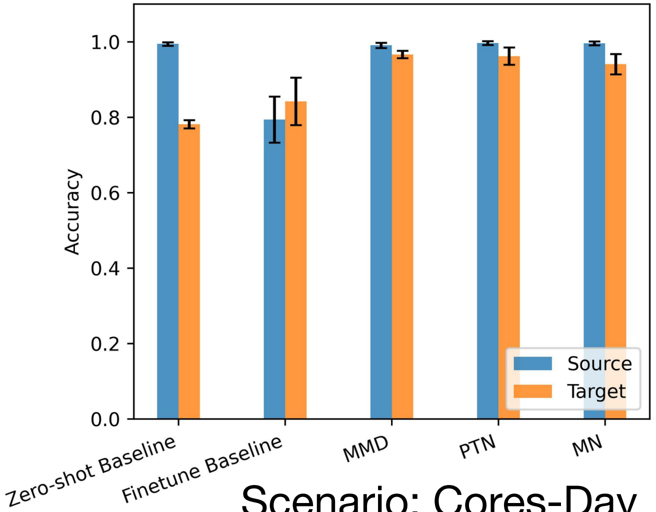
Results: FSL and DA performance



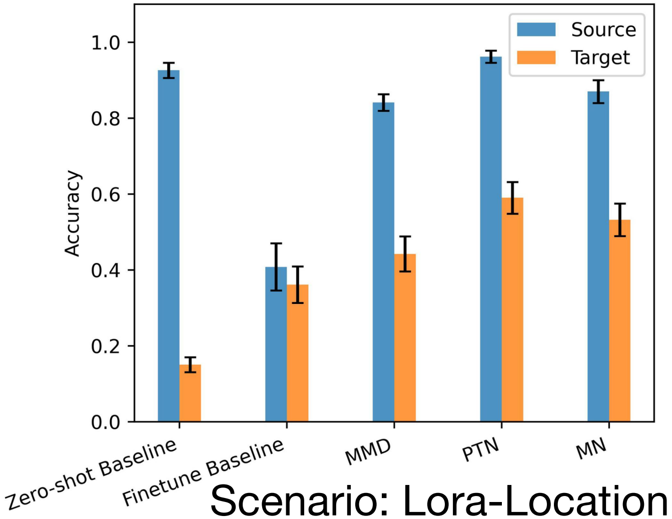
Scenario: Lora-Day



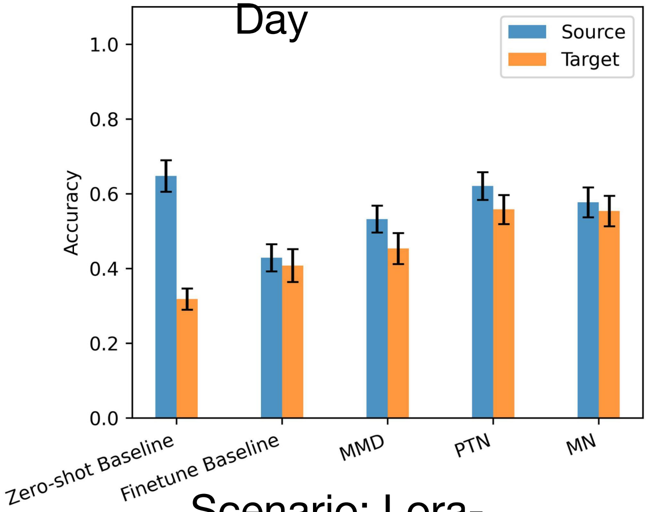
Scenario: WiSig-Day



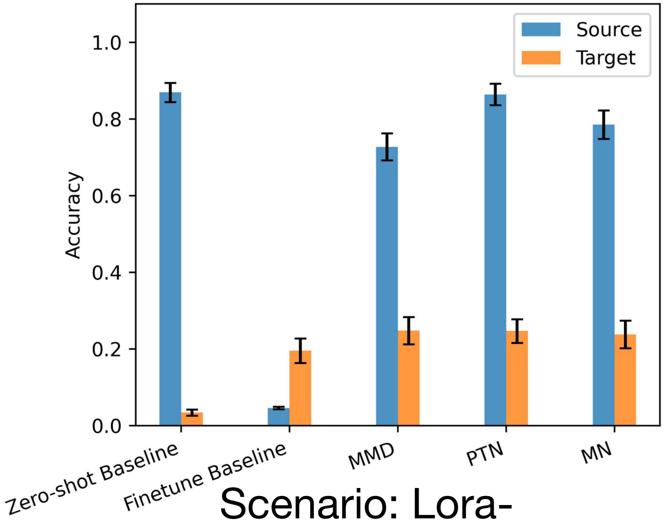
Scenario: Cores-Day



Scenario: Lora-Location

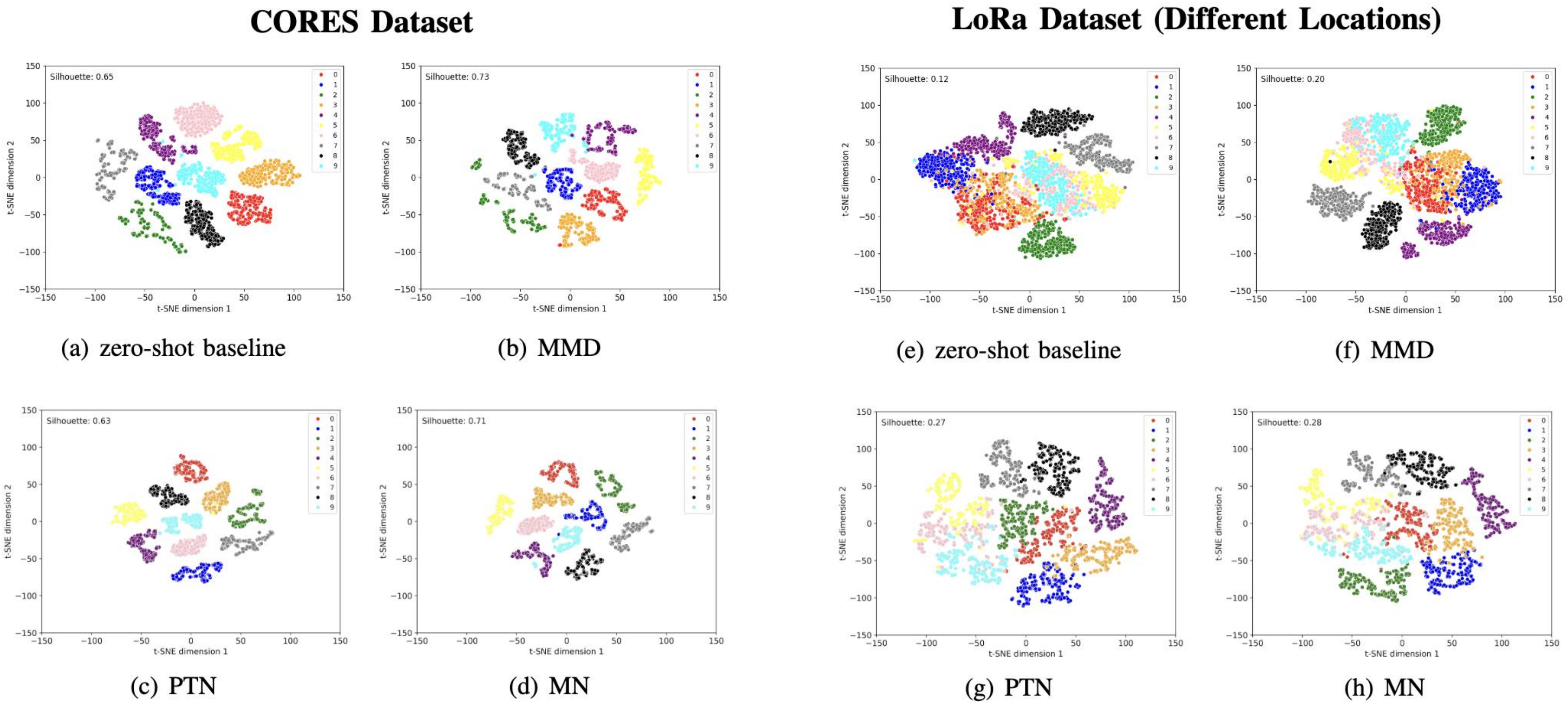


Scenario: Lora-Distance



Scenario: Lora-Config

Results: t-SNE plot



t-SNE plots comparing predictions from different methodologies across 10 classes on two datasets

Conclusion

- **Unified evaluation framework:** fixes datasets, data splits, and baselines (zero-shot and fine-tune), enabling apples-to-apples comparisons across methods.
- **Empirical benchmarking:** implement and compare three advanced methods with fine-tuning on three public RF datasets under six realistic domain shifts.
- **Representation analysis:** visualize learned embeddings and quantify clustering quality using silhouette scores to reveal how each method mitigates domain discrepancy.
- **Practical guidelines:** distill recommendations on method choice, shot-count, and evaluation design to help future RF fingerprinting FSL studies achieve fair and reproducible results.

Reference

1. T. Tian *et al.*, "Transfer Learning-Based Radio Frequency Fingerprint Identification Using ConvMixer Network," *GLOBECOM 2022 - 2022 IEEE Global Communications Conference*, Rio de Janeiro, Brazil, 2022, pp. 4722-4727, doi: 10.1109/GLOBECOM48099.2022.10000595.
2. S. Kuzdeba, J. Robinson and J. Carmack, "Transfer Learning with Radio Frequency Signals," *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, USA, 2021, pp. 1-9, doi: 10.1109/CCNC49032.2021.9369550.
3. A. Elmaghbub, B. Hamdaoui and W. -K. Wong, "ADL-ID: Adversarial Disentanglement Learning for Wireless Device Fingerprinting Temporal Domain Adaptation," *ICC 2023 - IEEE International Conference on Communications*, Rome, Italy, 2023, pp. 6199-6204, doi: 10.1109/ICC45041.2023.10279347.
4. L. Yang, Q. Li, X. Ren, Y. Fang and S. Wang, "Mitigating Receiver Impact on Radio Frequency Fingerprint Identification via Domain Adaptation," in *IEEE Internet of Things Journal*, vol. 11, no. 13, pp. 24024-24034, 1 July1, 2024, doi: 10.1109/JIOT.2024.3389491.
5. T. Zhao, X. Wang and S. Mao, "Cross-domain, Scalable, and Interpretable RF Device Fingerprinting," *IEEE INFOCOM 2024 - IEEE Conference on Computer Communications*, Vancouver, BC, Canada, 2024, pp. 2099-2108, doi: 10.1109/INFOCOM52122.2024.10621423.
6. Z. Zhang, G. Li, J. Shi, H. Li and A. Hu, "Real-World Aircraft Recognition Based on RF Fingerprinting With Few Labeled ADS-B Signals," in *IEEE Transactions on Vehicular Technology*, vol. 73, no. 2, pp. 2866-2871, Feb. 2024, doi: 10.1109/TVT.2023.3314491

Thanks for your attention!