LoFin: LoRa-based UAV Fingerprinting Framework

Maryna Veksler[1], David Langus Rodríguez[2], Ahmet Aris[2], Kemal Akkaya[1], A. Selcuk Uluagac[2]
1Advanced Wireless and Security Lab., [2]Cyber-Physical Systems Security Lab.
Florida International University
{mveks001, dlang029, aaris, suluagac, kakkaya} @fiu.edu

Overview

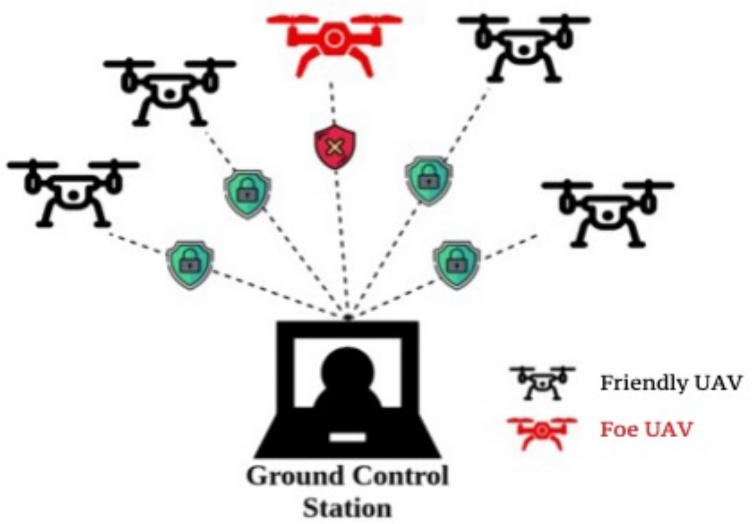
- Introduction
- Related Work
- Background
- LoFin Architecture
- Performance Evaluation
- Conclusions & Future Work

Introduction

- Unmanned Aerial Vehicles (UAVs) have become a world phenomenon:
  - Used for surveillance, reconnaissance, search & rescue missions
    - Intelligent decision making, mobility, and sensing capabilities
- UAV applications often involve long distance communications with the controller (GCS):
  - Reliable network channel for security and large transmission radius
- Long Range (LoRa) communication protocol:
  - Long-range and low-power technology
  - Consistent coverage across urban and rural areas

Motivation

- UAV applications require strong security:
  - Impersonation attacks
  - Attack may steal sensitive information
  - Mission infiltration
  - Communication disruption
- Intrusion Detection system is required:
  - No sniffing tools developed for UAV communicating via LoRa
  - Radio frequency (RF) analysis not effective due to channel interference and reconfiguration of LoRa channel



Related Work

- **Device Fingerprinting is an effective technique to detect the device impersonation attack**
  - LoRa fingerprinting:
    - Analysis of physical (PHY) layer radio frequency (RF) using deep learning (DL) [1, 2]
    - Challenges: varying configurations of LoRa protocol
  - UAV fingerprinting:
    - RF statistical analysis [3,4]
    - Challenges: affected by signal-to-noise (SNR) ratio
- **Our Contribution → LoFin:**
  - Do not require analysis of physical layer communications:
    - Resistant to changes in (1) RF signals due to external factors, (2) LoRa parameters
  - Passive fingerprinting:
    - No processing overhead
  - Encryption immunity with preserved data security

Background

❑ LoRa Stack

- ❖ LoRa physical layer – chirp spread spectrum (CSS) radio frequency modulation system
- ❖ LoRaWAN communication protocol and network architecture of upper layers
- ❖ LoRa provides flexibility to configure multiple transmission parameters for improved data rate:
  - Spreading factor (SF), bandwidth (BW), coding rate (CR) and carrier frequency (CF)
  - Adjusted based on the payload size and transmission range
- ❖ LoRaWAN provides two methods for device activation:
  - Over-the-air-activation (OTAA) provides dynamic assignment of device addresses and session keys.
  - Activation-by-Personalization (ABP) requires hardcoding of device addresses and session keys

❑ LoRa-based UAV Communications:

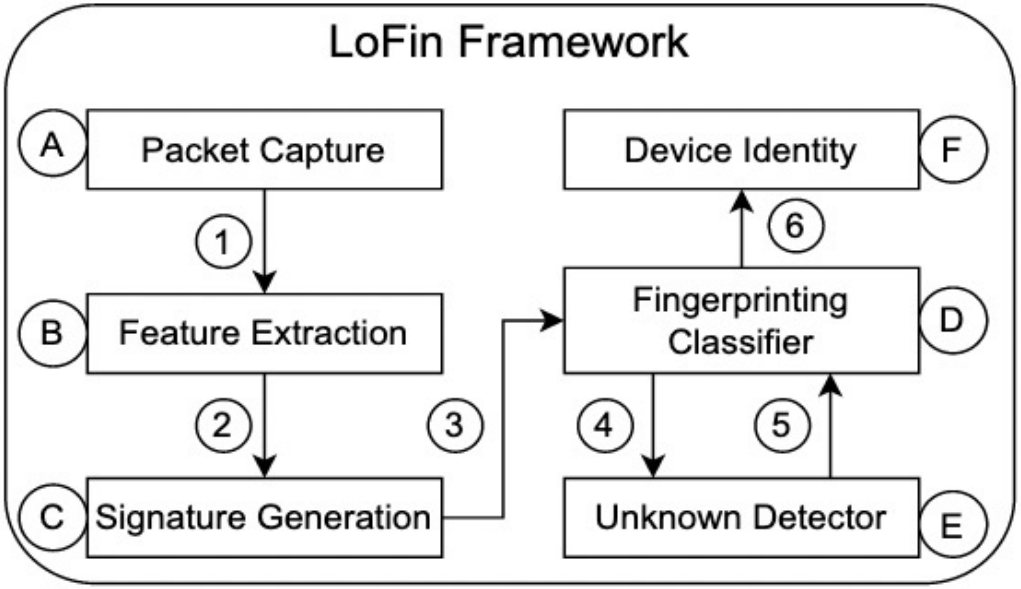
- ❖ Real-time quality monitoring system [5]
- ❖ Marine coastal environment monitoring [6]
- ❖ UAVs as end-node and gateway devices in LoRa network [7]

Threat Model & Assumptions

- Assumptions:
  - Network consists of multiple LoRa-based UAVs and sensors
  - LoFIN set up on the centralized server to passively capture network traffic
- Attacks & scenarios considered:
  - Passive Impersonation:
    - Network infiltration to mimic the behavior of legitimate UAV
  - Active attack
    - Disrupt functionality of the device identification tool and network communications
  - LoRa Configurations:
    - Periodic changes of the protocol configuration may impact accuracy of proposed detection mechanism

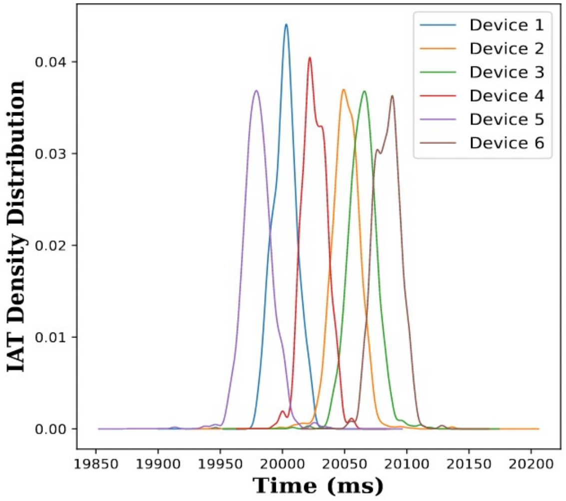
LoFin Architecture - Overview

- Overview:
  - Passively collects network traffic
  - Extract device-specific features
  - Generate device signature
  - Classification process & detection of unknown device signatures
  - Devices identify – a foe or a friend



LoFin Architecture - Components

- **4 major components:**
  - *feature extraction, signature generation, classifier, and unknown detector*
- **Feature Extraction:**
  - Considered features:
    - Payload length, device address, SNR, and combination of LoRa configuration parameters
  - Selected inter-arrival time (IAT) for device signature generation
    - Manufacturing defects introduce unique noises to the data transmission process, resulting in fixed time overhead
  - IAT for LoRa is affected by Time on Air (ToA):
    - Represent the time it takes a signal to travel from sender to receiver
    - ToA is directly affected by spreading factor (SF) and bandwidth (BW) L:oRa parameters
  - $\boldsymbol{IAT = (t_i - t_{i-1}) - ToA_i}$



LoFIN Architecture – Components contd.

Signature Generation

- Time-series extraction
  - Extract time-series of length *l* for each set of IAT values
  - Extracted features split into N shorter series

$$time\_series = [IAT_1, IAT_1, IAT_2, ...IAT_n].$$

- Statistical Analysis
  - Using tsfresh obtained 816 distinctive features
  - Selected 367 significant features based on p-score and relevance table

Fingerprinting Classifier

- Machine Learning classifiers: KNN, RF, GaussianNB, and SVM)
- Produces probability vector, V_p indicating similarity value for known device
- V_p is passed to ***unknown detector,*** to filter out unknown devices:
  - Then classification results for known devices are interpreted to determine device identity

LoFIN Architecture – Components contd.

Unknown Detector

- Responsible for identifying potentially adversarial devices within LoRa network
- Intermediate stage of ***fingerprinting classifier***
  - Applies probability measures to filter out suspicious devices
  - Threshold approach to spot samples yielding low closeness in regard to known devices

Effectiveness Metrics

- Accuracy (ACC) to measure overall system performance

$$ACC = \frac{TP + TN}{TP + FP + TN + FN}$$

- Precision & Recall
  - Accuracy for specific device class and indication of the number of mishits for a given class

$$Precision = \frac{TP}{TP + FP} \qquad Recall = \frac{TP}{TP + FN}$$

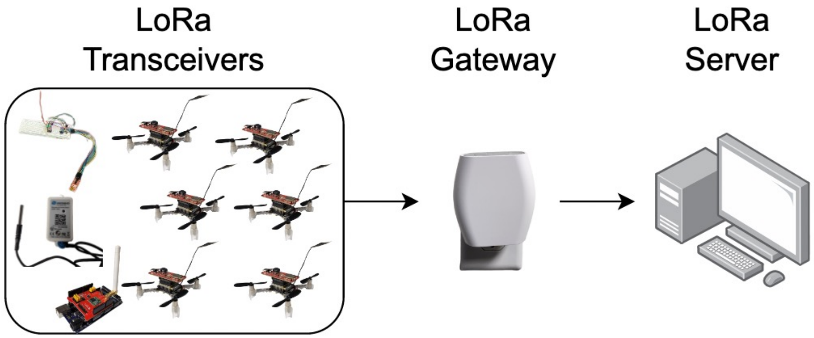
Performance Evaluation - Testbed

❑ Devices Summary

Device	Device Type	Quantity
CrazyFlee with Arduino expLoRaBLE	Drone Telemetry	6
Arduino Mega	LoRa Transceiver 1	1
Arduino Mini	LoRa Transceiver 2	1
Dragino LHT65	Temperature Sensor	1

❑ Testbed Setup:

- ❖ CrazyFlie drones programmed using Bitcraze library [8]
- ❖ Arduino expLoRaBLE as telemetry
- ❖ MAVLink protocol



❑ Data Collected:

- ❖ Total of ≅ 24,000 network packets
- ❖ 1,200 packets for each device
- ❖ Additional data collected to implement adversarial random delay scenario
- ❖ 70% of data used to train LoFin classifier

Performance Evaluation - Experiments

- **Devices setup:**
  - Drone Telemetry devices configured for a synchronized mission of data collection
  - Rest of the devices transmit independently
- **LoFin Configurations:**
  - Extracted 40 time series vectors consisting of 30 consecutive IAT values for each device
  - Selected optimal ML algorithm for fingerprinting classifier
    - RF with 10 trees, *entropy function* as quality measure of a split, and random split of 42
    - KNN with "ball_tree" algorithm for nearest neighbors computation
  - 5 K-Fold cross validations
    - Optimal model fitting

Performance Evaluation - Experiments

- Experiment 1 – Isolated Environment
  - All devices are known and isolated from the adversary
  - Accuracy: **100%** for RF classifier and **99.2%** for KNN
- Experiment 2 – Different Configuration Scenarios (Table 1)
  - LoFin is trained for devices transmitting using **SF7**
  - Set LoRa SF configuration to **SF10** for 4 devices and apply LoFin framework

Device	RF		KNN	
	Precision	Recall	Precision	Recall
Drone Telemetry 1*	1.0	1.0	1.0	1.0
Drone Telemetry 2*	1.0	1.0	1.0	1.0
Drone Telemetry 3	1.0	1.0	0.89	1.0
Drone Telemetry 4	1.0	1.0	0.88	1.0
Drone Telemetry 5	1.0	1.0	1.0	1.0
Drone Telemetry 6*	1.0	1.0	1.0	1.0
LoRa Transceiver 1*	1.0	1.0	1.0	0.67
LoRa Transceiver 2	1.0	1.0	1.0	1.0
Temperature Sensor	1.0	1.0	1.0	1.0
Average Accuracy	1.0		0.972	

Table 1. Results for experiment 2

Performance Evaluation - Experiments

Experiment 3 – Impersonation Attack (Table 2)

- 6 identical drone telemetry devices;
  - 1 is selected to represent an **adversary**
- Evaluated unknown detector ability to detect foe's traffic
- ***Unknown detector*** cannot be used with KNN:
  - Requires probability vector
- **100%** classification and true negative rate;
  - False negative rate **below 10%**

Devices	Precision	Recall
Drone Telemetry 1	1.0	1.0
Drone Telemetry 2	1.0	1.0
Drone Telemetry 3	1.0	1.0
Drone Telemetry 4	1.0	1.0
Drone Telemetry 5	1.0	1.0
Drone Telemetry 6*	N/A	N/A
Average Accuracy	1.0	
True Negative Rate	1.0	
False Negative Rate	0.082	

Table 2. Results for experiment 3

Performance Evaluation - Experiments

❑ Experiment 4 – Random Delay Attack (Table 3)

- ❖ Implemented artificial delay to 1 drone telemetry device
  - Used built-in probabilistic random() library to design random delay algorithm
- ❖ Overall accuracy is **95%** for RF-based fingerprinting classifier
- ❖ Unknown detector trade-off
  - Benign traffic may be marked as potentially adversarial

```
p=0; d=0, counter=0;
while(True):
   select p from [30,70] and d from [1,5]
   if  counter == p:
      wait d and transmit
      p=0; d=0, counter=0;
   else:
      transmit
          counter += 1
```

Device	RF		KNN	
	Precision	Recall	Precision	Recall
Drone Telemetry 1*	1.0	0.86	1.0	0.57
Drone Telemetry 2	1.0	1.0	1.0	1.0
Drone Telemetry 3	1.0	1.0	1.0	1.0
Drone Telemetry 4	1.0	1.0	0.86	1.0
Drone Telemetry 5	1.0	1.0	1.0	1.0
Drone Telemetry 6	0.92	1.0	0.91	0.91
LoRa Transceiver 1	1.0	1.0	1.0	0.67
LoRa Transceiver 2	1.0	1.0	1.0	1.0
Temperature Sensor	1.0	1.0	1.0	1.0
Average Accuracy	0.991		0.964	

Table 3. Results for experiment 4

Conclusion & Future Work

- **LoFin:**
  - 1st framework to passively fingerprint LoRa devices using MAC layer information
  - 100% precision and recall for majority of the scenarios
  - Resistant to changes in LoRa configurations
  - 100% detection of unknown devices with false-negative rate below 10%
  - Not influenced by changes in PHY layer
- Future Work:
  - Increase number of devices and its diversity
  - Improve LoFin robustness against random delay attack

Acknowledgements

This work is partially supported by the US National Science Foundation Awards: NSF-CAREER-CNS-1453647, NSF-1718116, NSF-1663051, Microsoft, and US Army Research Office (Grant Number W911NF-21-1-0264). The views expressed are those of the authors only, not of the funding agencies.

References

1. G. Shen, J. Zhang, A. Marshall, L. Peng, and X. Wang, “Radio frequency fingerprint identification for lora using spectrogram and cnn,” in IEEE INFOCOM 2021 - IEEE Conference on Computer Communications.
2. A. Elmaghbub and B. Hamdaoui, “Lora device fingerprinting in the wild: Disclosing rf data-driven fingerprint sensitivity to deployment variability,” IEEE Access, vol. 9, pp. 142 893–142 909, 2021.
3. N. Soltani, G. Reus-Muns, B. Salehi, J. Dy, S. Ioannidis, and K. Chowdhury, “Rf fingerprinting unmanned aerial vehicles with non-standard transmitter waveforms,” IEEE Transactions on Vehicular Technology, vol. 69, no. 12, pp. 15 518–15 531, 2020.
4. M. Ezuma, F. Erden, C. K. Anjinappa, O. Ozdemir, and I. Guvenc, “Micro-uav detection and classification from rf fingerprints using machine learning techniques,” in 2019 IEEE Aerospace Conference.
5. A. Rahmadhani, Richard, R. Isswandhana, A. Giovani, and R. A. Syah, “Lorawan as secondary telemetry communication system for drone delivery,” in 2018 IEEE International Conference on Internet of Things and Intelligence System (IOTAIS), pp. 116–122.
6. C. A. Trasvĩ na-Moreno, R. Blasco, Marco, R. Casas, and A. Trasvĩ naCastro, “Unmanned aerial vehicle based wireless sensor network for marine-coastal environment monitoring,” Sensors, vol. 17, no. 3, 2017.
7. M. H. M. Ghazali, K. Teoh, and W. Rahiman, “A systematic review of real-time deployments of uav-based lora communication network,” IEEE Access, vol. 9, pp. 124 817–124 830, 2021.
8. “Bitcraze: Documentation,” https://www.bitcraze.io/documentation/start/.

Thank you! Q&A


THANK
YOU
GRACIAS
ARIGATO
SHUKURIA
GOZAIMASHITA
EFCHARISTO
JUSPAXAR
DANKSCHEEN
TASHAKKUR ATU
YAQHANYELAY
SUKSAMA
EKHMET
GRAZIE
MEHRBANI
PALDIES
KOMAPSUMNIDA
MAAKE
BOLZÏN
MERCI
BÏYAN
SHUKRIA
TINGKI