Poster: Radiometric Signatures for Wireless Device Identification over Dynamic Channels

Wenqing Yan
Uppsala University
wenqing.yan@it.uu.se

Thiemo Voigt
Uppsala University, RISE SICS
thiemo@sics.se

Christian Rohner
Uppsala University
christian.rohner@it.uu.se

***Abstract*—Radiometric signatures have been shown effective in identifying wireless devices based on imperfections in their electronics, also known as fingerprinting. Previous work mainly considered static channel conditions. In this work, we experimentally study the impact of movement and dynamic channel conditions on the radiometric signatures. We demonstrate the feasibility of fingerprinting when channels are dynamic.**

I. INTRODUCTION

Device identification and authentication are two of the most fundamental challenges in network security. In this work, we focus on fingerprinting, leveraging on hardware imperfections of transmitters. Unique characteristics in the emitted wireless signals are used as signatures to differentiate their source [1]. Existing work distinguishes between transient-based [2] and modulation-based [3] approaches to extract characteristic features of the devices. Both approaches, by default, regard the significant difference coming from transmitter hardware but ignore the influence of the transmission channel. In many practical applications such as public transportation, industrial networks or body area networks, sensors are placed on moving parts, resulting in dynamic channel characteristics. We experimentally explore to what extent dynamic channels affect the radiometric signature. More specifically, we study the impact of distance and movement on the features of modulation-based IEEE 802.15.4 fingerprinting.

II. EXPERIMENT SETUP

We set up our experiments in an anechoic chamber to isolate the impact of distance $(0.5m, 1m, 2m)$ and movement speed $(0.2m/s, 1m/s)$ from multi-path effects and human interference. This project targets wearable applications, so our experiment focuses on linear moving speed slower than $1m/s$, which is approximate to human body daily motions. To control the movement accurately, we use a motor-controlled linear rail.

The IEEE 802.15.4 standard is designed for ultra-low-power use cases. It employs a combination of Direct Sequence Spread Spectrum along with O-QPSK to achieve robust transmissions. QPSK modulation encodes two data bits into four carrier phase offsets using two independent carrier components (in-phase (I), quadrature (Q)). During the demodulation process, errors are measured by comparing phasors corresponding to the I/Q values of a signal. In our experiments, we focus on the radiometric features suggested for QPSK-based WiFi fingerprinting [3]: (i) frequency error, (ii) SYNC error, (iii) I/Q offset, (iv) phase error, and (v) magnitude error. The fingerprinting targets are three identical Zolertia Firefly nodes.

III. OBSERVATIONS

Table I summarizes the Kullback–Leibler divergence to quantify the difference in feature distributions between the different experimental setups relative to the static experiment at 0.5m. We compare the experiments for the same fingerprinted target fixed at different distances with the same transmission power. Increasing the distance makes the feature distribution diverge more. Fingerprinting is noise sensitive. As the signal to noise ratio (SNR) gets low, the noise distorts the characteristics coming from transmitter hardware imperfections, making fingerprinting difficult.

There are no significant wireless distortions that appear within the amount of speed slower than $1m/s$, as shown by the experiments marked in bold. Compared to experiments with static transmitter positions, distance has a more significant impact on the modulation error than the speed. For protocols with a low symbol rate like 802.15.4, less inter-sample interference makes the fingerprint work robustly against channel dynamics.

The results indicate that when the SNR stays above a certain threshold, channel dynamics might not impact modulation-based fingerprint accuracy for IEEE 802.15.4 devices, which means that a modulation-based device identification scheme is feasible for moving devices such as wearable equipment.

TABLE I
KL DIVERGENCE COMPARISON BETWEEN DIFFERENT EXPERIMENT WITH REFERENCE NODE NO.1 PLACED 0.5M FROM THE RECEIVER

Features	Node2 static	Node3 static	**1m** static	2m static	**0.5-1m** 0.2m/s	**0.5-1m** 1m/s
Frequency	5.0525	5.0552	0.0001	0.0054	0.0032	0.0066
SYNC	0.7624	0.2933	0.2786	1.2992	0.2623	0.3183
I Offset	0.4232	0.0677	0.3054	0.7665	0.0823	0.1614
Q Offset	0.0826	0.1535	0.2237	0.4007	0.2420	0.0707
Phase	0.3410	0.0520	0.0795	0.1023	0.0764	0.0796
Emax	1.3696	0.5347	1.1875	2.0390	0.6504	0.3578

REFERENCES

[1] Y. Sheng and et al., "Detecting 802.11 mac layer spoofing using received signal strength," in *INFOCOM '08*.

[2] B. Danev and S. Capkun, "Transient-based identification of wireless sensor nodes," in *IPSN '09*.

[3] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *MobiCom '08*.

This project is financially supported by the Swedish Foundation for Strategic Research

DOI 10.1109/SPW50608.2020.00037