PhD Forum Abstract: Towards Robust and Low-complexity Radiometric Fingerprint

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

ABSTRACT

Authentication is challenging in the IoT because most advanced cryptographic algorithms are difficult to afford by constrained devices expected to run many months or years. Radiometric signatures have been used effectively to identify wireless devices based on imperfections in electronic circuits. This technique is also known as Radio frequency (RF) fingerprinting. Previous work proves the feasibility of this technique but mainly considered static channel conditions. In our current work, we systematically and experimentally study the impact of dynamic and complex channel conditions on the radiometric signatures. The results show a threat to identification accuracy for modulation error-based fingerprinting that was considered channel-resilient. Next step, my research aims at improving the robustness of RF fingerprint systems and make this authentication solution ready for widespread implementation.

KEYWORDS

Physical-layer security, Radio frequency (RF) fingerprint, Authentication

ACM Reference Format:

Wenqing Yan. 2020. PhD Forum Abstract: Towards Robust and Low-complexity Radiometric Fingerprint. In *Proceedings of The 18th ACM Conference on Embedded Networked Sensor Systems (SenSys '20)*. ACM, New York, NY, USA, 2 pages. <https://doi.org/10.1145/3384419.3430573>

1 INTRODUCTION

Physical-layer identification that relies on the individual hardware-level imperfection is appealing for IoT applications, as devices can achieve identification in the physical layer that avoids costly upper-layer cryptography. The RF imperfections are circuitual variations mainly from analog components such as digital-to-analog converters, filter, oscillators, mixer and power amplifiers. These minute variations among individual devices acquired at manufacture are small enough to reach the standard specification but significant enough to extract a unique fingerprint to authenticate the transmitted device. This approach is attractive but challenging for practical usage because most existing radio frequency (RF) fingerprint algorithms are sensitive to the wireless channel.

I will develop my subsequent studies in the context of reliable physical layer authentication for practical implementation. I plan

to design robust and low-complexity RF fingerprinting techniques, which can enable large-scale distributed deployment.

2 ROBUSTNESS OF RF FINGERPRINT

The wireless signal received by devices is a convolution product between the transmitted signal and the time-varying wireless channel, so it not only contains the imperfections of the transmitter but the footprint left by dynamic channels. Amani et al. confirm the communication channel's significant interference and systematically quantify the wireless channel's impact on deep learning based fingerprint accuracy RF fingerprinting [1]. Compared with systems based on costly deep learning, the modulated error based approach first proposed by Brik et al. is claimed as a resilient system against ambient noise and fluctuations of the wireless channel [2]. The modulation domain features can be easily extracted from the receiver demodulation processing chain, which is more structured than unprocessed raw I/Q samples. However, their experimental evaluation only considers a testbed environment with simple channels, and thus the broad impact of the channel characteristics is not thoroughly investigated.

3 RESEARCH CHALLENGES

The idea of achieving stable physical-layer authentication for IoT applications attracts significant interest. Due to the time-vary property of wireless channel, radio signal interacts with the surrounding environment in a complicated way, which causes a large amount of disturbance in the signal's quality. Processing the received signal and eliminating the channel disturbance is the key to designing a robust fingerprint authentication system.

Even though some research already touches on topics around the robustness of RF fingerprint [3, 4], the existing system is either explicitly designed for WiFi-only or relies on high complexity machine learning algorithms. Further research will help extend the ubiquity of RF fingerprint by making it less complicated and compatible with different communication techniques, including Zigbee, Bluetooth, and passive devices such as RFID and backscatter tags.

As the first step, the wireless channel's impact needs to be quantified for common-used transmission protocols in different complex radio environments. A comprehensive study on the sensitivity of the identification accuracy to each channel characteristics will provide insights to improve the fingerprint robustness. We have started exploring this direction by investigating the modulation error based fingerprinting system, which was considered robust. A summary of the results is shown in Section 4. As the tolerance of different physical-layer protocols towards the channel dynamics is different, the fingerprint's sensitivity in the context of different physical-layer protocols also varies. When the device can receive entirely correct packets, it does not necessarily mean the extracted fingerprint has

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

SenSys '20, November 16–19, 2020, Virtual Event, Japan

© 2020 Copyright held by the owner/author(s).

ACM ISBN 978-1-4503-7590-0/20/11.

<https://doi.org/10.1145/3384419.3430573>

good enough quality to support accurate identification. An accurate indicator that shows the fingerprint's quality would help avoid the error caused by low-quality input.

Besides, when designing the processing method to emphasize transmitter characteristics and eliminate channel impact, some by-products which indicate the dynamic channel condition might be valuable for wireless sensing research. For example, the coarse-grained frequency offset generated by the carrier recovery algorithm can indicate surrounding objects moving statuses in the radio environment. The intersection of wireless security and sensing is another interesting concept waiting for exploration.

4 CURRENT RESULTS AND NEXT STEPS

As the first step, our current work bridges the gap by providing the first evaluation of the wireless channel's impact on modulation based fingerprint system through experimental data obtained from 30 wireless devices and comprehensive wireless channel simulation with different configurations. Our work targets IoT scenarios with ultra-low-power devices, so we choose the IEEE 802.15.4 protocol and focus on the generalized radiometric features suggested for QPSK-based WiFi fingerprinting [2]: (i) frequency error, (ii) SYNC error, (iii) I/Q offset, (iv) phase error, and (v) magnitude error. We focus on three major channel characteristics (signal to noise ratio (SNR), multipath, doppler shift) and quantify the reduction in identification accuracy separately. The results show that when the receiver's packet reception ratio (PRR) remains at an acceptable level, the fingerprint accuracy is significantly reduced by disturbances from the wireless channel.

In our experiments, we evaluate the classification accuracy in terms of its error rate, put it in relation to the packet error rate, and give a detailed insight on its impact on the used features. Figure 1 shows a summary of the results. In Figure 1-(1), a lower SNR level contributes to the increased variance of all the features, which challenges the classification accuracy. A wireless environment with several transmission paths has significant negative interference to constellation related features. As shown in Figure 1-(3,4), with PRR maintaining at an acceptable level, the feature derivation can lead the identification results all wrong. Besides, transmitters and receivers' mobility tested as Figure 1-(2) also results in a doppler spread and introduces irreducible error for the fingerprint features. For a large doppler shift above 60 Hz, the receiver will synchronize with the shifted frequency, which causes noticeable deviation to synchronization related features.

Future research includes two directions. First, the current feature set is limited, and we plan to extend the fingerprint feature set and filter out the channel-resilient feature subset. Second, a classification algorithm with adjustable weights based on the dynamic channel condition can strengthen the fingerprint robustness.

5 ABOUT ME

I just started my third year as a Ph.D. student from the Computer Communication group at Uppsala University. I am passionate about exploring the interdisciplinary research area among wireless, security and machine learning. My research topic focuses on wireless network security at the physical and data-link layers.

Figure 1: Fingerprint error ratio and packet reception ratio (PRR) with different wireless channels: (1) AWGN channel with SNR from -3 dB to 10 dB; (2) Doppler channel with frequency shift from 0 Hz to 80 Hz; (3, 4) Multipath channel with second-path delay $0.1\mu\text{s}$, $0.14\mu\text{s}$.

ACKNOWLEDGMENTS

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

REFERENCES

- [1] Al-Shawabka and et al. 2020. Exposing the Fingerprint: Dissecting the Impact of the Wireless Channel on Radio Fingerprinting. In *INFOCOM IEEE Conference on Computer Communications*.
- [2] Vladimir Brik and et al. 2008. Wireless device identification with radiometric signatures. In *Proceedings of the 14th ACM international conference on Mobile computing and networking*. 116–127.
- [3] Pengfei Liu and et al. 2019. Real-time identification of rogue WiFi connections using environment-independent physical features. In *INFOCOM IEEE Conference on Computer Communications*.
- [4] Tianhang Zheng and et al. 2019. FID: Function modeling-based data-independent and channel-robust physical-layer identification. In *INFOCOM IEEE Conference on Computer Communications*.