

*Digital Comprehensive Summaries of Uppsala Dissertations
from the Faculty of Science and Technology 2341*

Design and Identification of Wireless Transmitters for a Low-power and Secure Internet of Things

WENQING YAN



ACTA UNIVERSITATIS
UPSALIENSIS
2023

ISSN 1651-6214
ISBN 978-91-513-1973-5
urn:nbn:se:uu:diva-515943



UPPSALA
UNIVERSITET

Dissertation presented at Uppsala University to be publicly examined in 101121, Sonja Lyttkens, Ångström, Regementsvägen 1, Uppsala, Tuesday, 16 January 2024 at 09:00 for the degree of Doctor of Philosophy. The examination will be conducted in English. Faculty examiner: Associate Professor Haitham Hassanieh (École Polytechnique Fédérale de Lausanne (EPFL)).

Abstract

Yan, W. 2023. Design and Identification of Wireless Transmitters for a Low-power and Secure Internet of Things. *Digital Comprehensive Summaries of Uppsala Dissertations from the Faculty of Science and Technology* 2341. 75 pp. Uppsala: Acta Universitatis Upsaliensis. ISBN 978-91-513-1973-5.

Wireless communication is a key enabler for connecting billions of Internet of Things devices. For networked embedded devices operating on limited energy resources, wireless communication dominates the power consumption. Moreover, as networked devices increasingly handle sensitive data, security concerns in wireless communication are continuously expanding. This dissertation develops novel solutions for low-power and secure wireless communication.

Wireless transmitters consist of a series of steps, involving both analog and digital components, each playing a distinct role in the transmit chain. Conventional transmitters employ power-hungry analog components, leading to power consumption on the order of milliwatt. Backscatter transmitters significantly reduce communication power consumption to levels well below one milliwatt. This remarkable power efficiency is achieved by offloading power-hungry components to an external carrier emitter. However, backscatter transmitters encounter challenges in applications that demand medium to long communication range, because they rely heavily on powerful emitters in their proximity for an effective communication range. Instead of removing power-hungry components, our solution integrates the functions of these components into a low-power design. While still requiring an emitter, our transmitter does not reflect the carrier signal. Instead, we utilize a weak carrier signal to stabilize the transmitter, allowing a communication range of over one hundred meters even when the emitter is far away. This contribution takes a step forward in moving low-power communication beyond backscatter.

Passive radiometric fingerprinting leverages imperfections of hardware components to identify and authenticate transmitters. Its passive nature fits well to secure low-power transmitters operating within constrained resources. To enhance the viability of radiometric fingerprinting, we make three contributions in this dissertation to facilitate its widespread deployment. First, compared to conventional radios, low-power backscatter communication has a fundamentally different composition of hardware components in its transmit chain. In our work, we decompose fingerprints in a backscatter system for dual identification of tags and emitters. Beyond security purposes, recognizing the emitter embeds a notion of locality, enabling fingerprinting usage in backscatter network management tasks such as emitter coordination. Second, the dynamic nature of real-world wireless channels significantly impacts the robustness of fingerprinting. We decompose channel impacts and develop a hybrid system. This system employs pertinent strategies for different channel factors, ensuring reliable performance across complex wireless conditions. Lastly, based on the understanding of components' contributions to the transmit chain, we design a lightweight fingerprinting system. We demonstrate a complete implementation seamlessly integrated within the constraints of a single low-cost off-the-shelf chip. This contribution simplifies the conventionally bulky setup using sophisticated signal acquisition equipment and dedicated computer processing resources, which facilitates the practical deployment of fingerprinting on low-cost embedded devices.

Keywords: Wireless transmitters, Wireless embedded systems, Physical-layer security, Radiometric fingerprinting, Radio frequency fingerprinting, Identification, Authentication, Backscatter communication, Internet of Things

Wenqing Yan, Department of Information Technology, Computer Architecture and Computer Communication, Box 337, Uppsala University, SE-75105 Uppsala, Sweden. Department of Information Technology, Division of Computer Systems, Box 337, Uppsala University, SE-75105 Uppsala, Sweden.

© Wenqing Yan 2023

ISSN 1651-6214

ISBN 978-91-513-1973-5

URN urn:nbn:se:uu:diva-515943 (<http://urn.kb.se/resolve?urn=urn:nbn:se:uu:diva-515943>)

Dedicated to my parents and dear Ning

List of Papers

This thesis is based on the following papers, which are referred to in the text by their Roman numerals.

- I Ambuj Varshney*, **Wenqing Yan***, and Prabal Dutta. 2022. Judo: Addressing the Energy Asymmetry of Wireless Embedded Systems through Tunnel Diode based Wireless Transmitters. In *Proceedings of the 20th Annual International Conference on Mobile Systems, Applications and Services (MobiSys'22)*. DOI: 10.1145/3498361.3538923
- II Muhammad Sarmad Mir*, **Wenqing Yan***, Prabal Dutta, Domenico Giustiniano, and Ambuj Varshney. 2023. TunnelLiFi: Bringing LiFi to Commodity Internet of Things Devices. In *Proceedings of the 24th International Workshop on Mobile Computing Systems and Applications (HotMobile'23)*. DOI: 10.1145/3572864.3580327
- III **Wenqing Yan**, Sam Hylamia, Thiemo Voigt, and Christian Rohner. 2020. PHY-IDS: A Physical-layer Spoofing Attack Detection System for Wearable Devices. In *Proceedings of the 6th ACM Workshop on Wearable Systems and Applications - in conjunction with MobiSys'20*. DOI: 10.1145/3396870.3400010
- IV **Wenqing Yan**, Thiemo Voigt, and Christian Rohner. 2022. RRF: A Robust Radiometric Fingerprint System that Embraces Wireless Channel Diversity. In *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'22)*. DOI: 10.1145/3507657.3528542
- V **Wenqing Yan**, Madhushanka Padmal, Dilushi Piumwardane, Thiemo Voigt, and Christian Rohner. 2023. Decomposing Radiometric Fingerprints in Backscatter Systems. *under submission*.
- VI **Wenqing Yan***, Mikolai-Alexander Gütschow*, Thiemo Voigt, and Christian Rohner. 2023. ORF: Towards On-board Radiometric Fingerprinting Fully Integrated on an Embedded System. *under submission*.

Reprints were made with permission from the publishers.

* Co-primary authors contributed equally to the work.

List of Papers not Included in the Dissertation

- Saptarshi Hazra, Thiemo Voigt and Wenqing Yan. 2021. PLIO: Physical Layer Identification using One-shot Learning. In *IEEE 18th International Conference on Mobile Ad Hoc and Smart Systems (MASS'21)*.
DOI: 10.1109/MASS52906.2021.00050
- Sam Hylamia, Wenqing Yan, André Teixeira, Noor Badariah Asan, Mauricio Perez, Robin Augustine, and Thiemo Voigt. 2020. Privacy-preserving Continuous Tumour Relapse Monitoring using In-body Radio Signals. In *IEEE Security and Privacy Workshops*.
DOI: 10.1109/SPW50608.2020.00030
- Christofer Flinta, Wenqing Yan, and Andreas Johnsson. 2020. Predicting Round-trip Time Distributions in IoT Systems using Histogram Estimators. In *IEEE/IFIP Network Operations and Management Symposium (NOM'20)*.
DOI: 10.1109/NOMS47738.2020.9110315
- Sam Hylamia, Wenqing Yan, Christian Rohner, and Thiemo Voigt. 2019. Tiek: Two-tier Authentication and Key Distribution for Wearable Devices. In *International Conference on Wireless and Mobile Computing, Networking and Communications (WiMOB'19)*.
DOI: 10.1109/WiMOB.2019.8923555
- Wenqing Yan, Christofer Flinta, and Andreas Johnsson. 2019. Machine-Learning Based Active Measurement Proxy for IoT Systems. In *IFIP/IEEE Symposium on Integrated Network and Service Management (IM'19)*.

List of Posters and Demos

- Moteen Amin Shah, Adithya Bijoy, Manoj Gulati, Wenqing Yan, and Ambuj Varshney. 2023. Going Beyond Backscatter: Rethinking Low-Power Wireless Transmitters using Tunnel Diodes. In *Proceedings of the 29th Annual International Conference on Mobile Computing and Networking (MobiCom'23)*.
DOI: 10.1145/3570361.3615744
- Tobias Mages, Wenqing Yan, Ambuj Varshney, and Christian Rohner. 2023. An Educational Platform to Learn Radio Frequency Wireless Communication. In *Proceedings of the 21st Annual International Conference on Mobile Systems, Applications and Services (MobiSys'23)*. **Best Demo Award**
DOI: 10.1145/3581791.3597292
- Wenqing Yan, and Ambuj Varshney. 2022. Enabling L3: Low Cost, Low Complexity and Low Power Radio Frequency Sensing using Tunnel Diodes. In *Proceedings of the 28th Annual International Conference on Mobile Computing And Networking (MobiCom'22)*.
DOI: 10.1145/3495243.3558281
- Daniel Nilsson, and Wenqing Yan. 2021. Identifying Bluetooth Low Energy Devices. In *Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems (SenSys'21)*.
Best Poster Award
DOI: 10.1145/3485730.3492880
- Wenqing Yan. 2020. PhD Forum Abstract: Towards Robust and Low-complexity Radiometric Fingerprint. In *Proceedings of the 18th Conference on Embedded Networked Sensor Systems (SenSys'20)*.
Best Ph.D. Forum Presentation
DOI: 10.1145/3384419.3430573
- Wenqing Yan, and Christian Rohner. 2020. Sensitivity of Radiometric Fingerprint against Wireless Channel. In *Proceedings of the 18th Conference on Embedded Networked Sensor Systems (SenSys'20)*.
Best Poster Award
DOI: 10.1145/3384419.3430455

Contents

Part I: Dissertation Summary	17
1 Introduction	19
1.1 Research Questions	21
1.2 Contributions	23
1.3 Methods	24
1.4 Roadmap	25
2 Background	27
2.1 Resource-constrained Embedded Systems	27
2.2 Conventional Radio Frequency Transmitters	28
2.3 Backscatter Transmitters	30
2.4 Tunnel Diode	31
2.5 Imperfections in Wireless Transmitters	32
2.6 Radiometric Fingerprinting Systems	33
2.7 Machine Learning Classifiers	34
2.8 Wireless Channels	35
3 Summary of Papers	39
4 From Commodity IoT Radios to Backscatter to Beyond Backscatter ...	47
4.1 Commodity IoT Radios	47
4.2 Backscatter Radios	48
4.3 Radio Technologies Beyond Backscatter	51
5 Transmitter Identification with Fingerprints in Wireless Signals	53
5.1 Channel-specific Fingerprints	53
5.2 Hardware-specific Fingerprints	53
5.3 Channel-robust Fingerprinting Systems	55
6 Conclusions and Future Work	57
6.1 Conclusions	57
6.2 Future Work	59
Appendix A: Radio Datasets	63
References	67
Part II: Papers	77

Acknowledgements

As I culminate this incredible journey towards my PhD, I am filled with immense gratitude towards those who have supported, guided, and inspired me along this path. Their encouragement, wisdom, and insights have been invaluable to my growth as a researcher and my personal development.

First and foremost, this journey would not have been possible without the efforts made by my supervisor, Prof. Christian Rohner, whose expertise, understanding, and patience added considerably to my growth. Over the past five years, his guidance has allowed me ample freedom to explore research directions that resonate with my interests. Our numerous discussions have been enlightening, consistently encouraging me to consider new perspectives and aiding in my discovery of innovative solutions. Furthermore, he has been a thoughtful mentor, closely attentive to my progress, and always providing genuine concern for my feelings.

Next, I would like to extend sincere gratitude to my co-supervisor, Prof. Thiemo Voigt. His guidance and consistent encouragement have been important throughout my journey. He has been an essential source of support, always ready to provide timely assistance, insightful feedback, and valuable advice. I am truly grateful for the dedicated time and effort he has invested in my development.

My heartfelt appreciation goes to my co-supervisor, Prof. Ambuj Varshney, for being an invaluable mentor and my closest collaborator. His unwavering passion, hard work, and steadfast dedication to excellence have been a source of inspiration. The depth and insight of our discussions, whether during experiments, bike rides, or tea breaks, have significantly influenced my growth as a researcher. I am thankful for his role in broadening my horizons and enlightening my PhD journey.

I wish to extend my sincere thanks to all my collaborators. In particular, Prof. Prabal Dutta, Dilushi Piumwardane, Madhushanka Padmal, Muhammad Sarmad Mir, Sam Hylamia, and Mikolai-Alexander Gütschow. I am deeply grateful for their contributions and the spirit of teamwork. I would like to thank all past and present group members in UNO and CoRe for engaging discussions, and all the fun we have had in the last few years. I would like to thank Prof. Per Gunningberg for his guidance in helping me reflect critically on my work. I am also grateful to Dr. Andreas Johnsson, who encouraged me to pursue PhD studies, setting me off on the path to becoming a researcher. I want to thank Carlos Pérez-Penichet, from whom I learned much valuable knowledge and experience during my initial few years as a PhD student. A special thanks

to Laura Marie Feeney for her enormous patience and instructive feedback. I also appreciate my current office mates, Tobias and Mehmatali, and previous office mates, Dilushi and Ahmed, for countless enriching conversations about life and research, contributing to a rewarding experience.

Throughout this journey, I have been fortunate to have the companionship of many friends. I extend my heartfelt thanks to Andreas Soleiman, Amin Kaveh, Feiyang Liu, Han Wang, Jin Hu, Keren Zhai, Lorenzo Corneo, Saba Akbari, Weining Song, Yusen Liu, and Yuning Jiang. I am truly grateful for their friendship and for being there for me, both in times of stress and celebration.

Lastly, and most importantly, I must express my profound gratitude to my parents and to my beloved husband, Ning. I am truly thankful for their endless support and encouragement, not only during my PhD journey but throughout my life. They are my greatest source of inspiration and strength.

Wenqing Yan
December 2023

This work has been funded by the Swedish Foundation for Strategic Research (SSF) and Vetenskapsrådet (Swedish Research Council).

List of Acronyms

AWGN	Additive White Gaussian Noise
COTS	Commercially Off The Shelf
DC	Direct Current
DFE	Direction Finding Extension
DSP	Digital Signal Processing
FPGA	Field Programmable Gate Array
IC	Integrated Circuit
IDS	Intrusion Detection System
IF	Intermediate Frequency
IoT	Internet of Things
kNN	K Nearest Neighbor
LiFi	Light Fidelity
LO	Local Oscillator
LOS	Line of Sight
MCU	Microcontroller Unit
ML	Machine Learning
NLOS	Non Line of Sight
NN	Neural Network
OvO	One vs One
OvR	One vs Rest
RF	Radio Frequency
RFC	Random Forest
RFID	Radio Frequency Identification
RNR	Region of Negative Resistance
RSSI	Received Signal Strength Indicator
SDR	Software Defined Radio
SNR	Signal to Noise Ratio
SoC	System on Chip
SoM	Self-oscillating Mixer
SVM	Support Vector Machine
TDO	Tunnel Diode Oscillator

Part I:
Dissertation Summary

1. Introduction

The rapid evolution of the Internet of Things (IoT) has enriched our daily lives, offering expansive applications in healthcare, remote collaboration, and interactive entertainment. The foundational building block of the IoT vision is networked embedded systems, forming an interconnected and intelligent ecosystem. Considering deployment requirements, these embedded devices are typically constrained and operate within limited energy resources, relying on small batteries or energy harvested from the environment. Examples expand from lightweight sensing platforms dispersible by the wind [1] to micro-sensors implanted in the human body [2].

The cornerstone of networked embedded systems is wireless communication. The rising ubiquity of small embedded devices poses a pressing need for developing low-power wireless communication solutions designed for limited power budgets. Moreover, as devices increasingly handle sensitive data, such as health information and biometric data, the importance of secure wireless communication systems is steadily growing. A fundamental challenge arises *How to provide low-power and secure wireless communication?*

The primary objective of wireless communication is to convey information between points that are not physically connected. As illustrated in Figure 1.1, a wireless communication system consists of a data source, a transmitter encoding the data into a wireless signal, a communication channel through which the signal propagates, a receiver decoding the signal, and a data sink. In the context of this dissertation, radio frequency (RF) wireless communication using electromagnetic waves is considered.

A wireless transmitter consists of three essential blocks to generate electromagnetic waves, as illustrated in Figure 1.2. The protocol stack is essential for formatting data and handling communication tasks such as encoding, error correction, and encryption. It ensures efficient, reliable, and secure transmission of data across networks. The modulator is where the data is modulated onto a low-frequency electrical signal by altering its amplitude, phase, or frequency. Following the modulation, the information-bearing signal passes the RF stage, where it is first mixed with a high-frequency carrier and up-converted to the desired RF frequency band. Then, the electrical signal is amplified and converted to an electromagnetic wave via an antenna. In conventional digital communication systems, the protocol stack and modulator are implemented using digital processing components, while the RF stage predominantly employs analog components such as oscillators, RF mixers, filters, and amplifiers.



Figure 1.1. Elements of a wireless communication system [3].

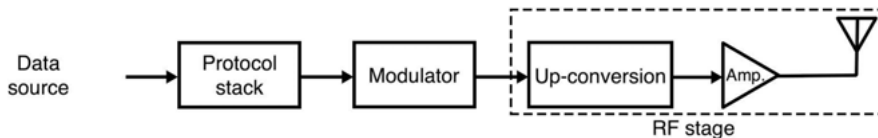


Figure 1.2. Basic blocks of a wireless transmitter [4].

Backscatter offers a promising approach to designing low-power transmitters, significantly reducing the power consumption of the communication from milliwatts to microwatts [5]. Backscatter systems decompose tasks in the RF stage and deploy them on two devices: The emitter handles the power-hungry task of high-frequency carrier generation. The passive tag, serving as the data source, exclusively performs low-power modulation operations by reflecting the external carrier signal.

Despite rapid advancements in backscatter technology, there has been no large-scale adoption due to several reasons. One primary concern is the limited communication range in comparison to active radios. In industrial monitoring and agricultural management scenarios, a communication range of tens to hundreds of meters is essential for effective wireless connectivity. To achieve a long communication range between the tag and the receiver, existing backscatter tags heavily depend on the emitter, requiring proximity (a few meters) to a strong emitter. This requirement significantly restricts their deployments in practical scenarios. Additionally, backscatter tags modulate external carrier signals by toggling the antenna terminal using an RF switch in accordance with a digital signal. Due to the usage of digital signals, the spectral efficiency of the reflected signal is inherently poor [6], which complicates the network formation and prevents tags from coexisting with other devices.

The first part of my dissertation introduces a novel low-power transmitter architecture to alleviate challenges inherent in backscatter. Instead of the decomposition strategy used in backscatter, the transmitter integrates the power-hungry tasks of high-frequency carrier generation and the mixing in a single power-efficient step. Our design trades stability for low power consumption. To improve the communication quality, we deploy a weak emitter to stabilize the transmitter. We rethink the asymmetric roles of the emitter and transmitter and weaken the dependence between them. Operating within the same low-power budget as a backscatter tag, our transmitter attains a long communica-

tion range (more than one hundred meters), even when the emitter is located far away (exceeds one hundred meters).

The increasing trend towards low-power and miniaturized networked embedded devices motivates a reconsideration of how to secure wireless communication systems. Identification and authentication are essential, ensuring that only authenticated devices can connect and exchange data over the wireless network. Traditional methods often apply resource-intensive cryptographic algorithms. Although advancements in lightweight cryptographic solutions and hardware acceleration are promising, adopting such methods puts additional demands on the limited resources available on embedded devices.

Radiometric fingerprinting identifies wireless devices utilizing unique characteristics inherent in the radiated electromagnetic waves. Electronic components in the transmit chain exhibit inconsistent performance due to manufacturing variances [7]. As a result, the signal emitted from the transmitter does not just carry the primary data but also the intrinsic fingerprint of the transmitter hardware. By examining such hardware-specific fingerprints, the receiver can identify the transmitting device. The passive nature of such mechanisms entirely relieves the overhead of identification and authentication functionalities from the transmitter side. The second part of the dissertation focuses on radiometric fingerprinting, covering both active commodity radios and backscatter radios.

The propagation of electromagnetic waves from a transmitter to a receiver is influenced by their distance and environmental factors. Consequently, the received signal is affected not only by the hardware-specific fingerprint but also by the characteristics of the wireless channel. These channel characteristics can influence device identification in both positive and negative ways. From one perspective, channel characteristics can serve as spatial fingerprints to locate and potentially identify the transmitter. Wireless channel properties often vary in real-world situations due to user movements and environment dynamics. From another perspective, the transient effects of the wireless channel can degrade the quality of hardware-specific fingerprints, making it difficult to distinguish individual transmitters. To address this, this dissertation introduces methods to enhance the robustness of radiometric fingerprinting, ensuring reliable transmitter identification.

1.1 Research Questions

My work centers around advancing low-power and secure wireless communication, branching into two directions. The first direction explores how to design low-power transmitters, extending beyond backscatter techniques. The second direction investigates how to apply radiometric fingerprinting techniques for robust and efficient transmitter identification in practical deployments.

1.1.1 Low-power Wireless Transmitters

The vision of IoT is built on embedded systems interconnected through wireless communication. Backscatter technology emerges as a promising solution to enable low-power ubiquitous connectivity, consuming power at least two orders of magnitude lower than commodity active transmitters (see the comparison in Chapter 3).

However, backscatter has not yet achieved widespread adoption among IoT application scenarios. A critical challenge lies in its limited communication range [5], which can be attributed to two main factors. First, the signal undergoes dual path loss, initially during its propagation from the carrier emitter to the tag, and subsequently from the tag to the receiver. As the distance between the carrier emitter and the tag increases, the tag communication range drops significantly [8, 9, 10]. Second, during the backscatter reflection operation, the signal experiences return loss at the tag. Consequently, to compensate for the losses, emitters radiate strong signals [11, 12, 13]. Despite this, a strong bond exists between the tag and the external carrier emitter. For a long communication range of tens to hundreds of meters, the tags need to be located in close proximity to an emitter [9, 10, 14, 15].

Furthermore, backscatter tags modulate information by toggling RF switches among antenna terminals with a digital baseband signal, producing unwanted harmonics and out-of-band interference. While solutions like adjusting antenna impedance to approximate analog baseband signal operations exist, they add complexity to the backscatter design [6, 12, 14, 16, 17]. These challenges lead to the following question: *Instead of the reflection-based backscatter mechanism, can we design a transmitter with a power budget similar to a backscatter transmitter while offering enhanced communication range and spectral efficiency?*

1.1.2 Wireless Transmitter Identification with Radiometric Fingerprints

Hardware-specific fingerprints embedded in wireless signals are used to identify transmitters. Passive radiometric fingerprinting methods are suitable for identifying resource-constrained transmitters, adding a valuable layer of security to wireless communication systems. Such methods can also be integrated with cryptographic techniques to enhance existing security mechanisms. Although radiometric fingerprinting has proven effective, it has not yet achieved widespread deployment.

In real-world scenarios, complex wireless channels challenge the robustness of fingerprinting [18, 19, 20, 21]. In practice, the received signals are compounds of the hardware-specific fingerprints and the transient impact of the wireless channel. It is challenging to perfectly separate them, particularly when the impact of the wireless channel dominates and hides the transmitter's

fingerprints [20]. Therefore, we ask: *How can we improve the robustness of a radiometric fingerprinting system under diverse wireless channels?*

There is also an emergence of new low-power transmitter designs, i.e., backscatter technology, with fundamentally different compositions of the electronic components in the transmit chain. We need to understand *How do the components contribute to fingerprints in backscatter systems? Is it possible to identify both the carrier emitter and the backscatter tag?*

Finally, an important aspect of widespread deployment is enabling fingerprinting on embedded devices with limited resources. Most existing system implementations demand expensive equipment to conduct high-resolution signal acquisition [22, 23, 24], dedicated processing operations [25] and substantial computational tasks [19, 21, 26]. With this in mind, we ask the question: *Is it feasible to implement a complete radiometric fingerprinting system on a low-cost and low-power system on chip (SoC)?*

1.2 Contributions

In general, my dissertation delves into low-power and secure wireless communication, and contributes to the state of the art in three notable ways. The questions formulated in Section 1.1 are addressed in six papers.

Design Low-power Wireless Transmitter beyond Backscatter

We propose a low-power tunnel diode-based self-oscillating mixer (SoM) transmitter architecture (Paper I). The transmitter tag locally generates a weak and unstable high-frequency carrier signal and mixes it with an analog baseband signal in a single power-efficient SoM step. The mixing is accomplished efficiently using the nonlinearity of the tunnel diode, which enables the use of analog baseband signals and prevents the generation of unwanted harmonics. Our transmitter trades stability for low power consumption, which is sidestepped by using an external carrier via the injection-locking phenomenon. Although the system requires an emitter, it fundamentally differs from backscatter by not reflecting the carrier signal. Given that a weak carrier can stabilize the transmitter, the emitter can be located significantly away from the transmitter without compromising the communication range. Expanding on this design, we demonstrate an application of a low-power bridge to replicate visible light communication signals onto radio waves, which allows widespread IoT devices to receive light signals with their existing radio transceivers (Paper II).

Relation between Transmitter Components and Fingerprint Features

We attribute fingerprints back to imperfect hardware components and establish a systematic understanding of how imperfections influence fingerprinting features. In the context of backscatter systems, we define fingerprinting features based on the role and characteristics of critical hardware components

within the backscatter architecture. We emphasize the separation of the carrier and emitter and achieve accurate identification of both tags and carrier emitters, even in complex scenarios with multiple tags sharing several carrier emitters (Paper V). Based on the understanding of the transmit chain, we engineer fingerprint features and integrate their extraction in a coherent receiver architecture, enabling an efficient implementation on embedded devices. We demonstrate a complete radiometric fingerprinting chain seamlessly integrated within a single low-cost SoC (Paper VI).

Robust Fingerprinting in Challenging Wireless Environments

We study the severe impact of the wireless channel on radiometric fingerprinting and present mitigation strategies to make the fingerprinting system more robust even in challenging environments. Based on the fundamental insight of how multipath propagation parameters impact the features in a particular and non-random way, we employ a data augmentation method based on structured channel simulation to optimize the fingerprint classifier strategically. On top of that, noise compensation and a feature denoising filter are used to enhance the system stability in noisy conditions with weak signals. We demonstrate the system performance with significantly improved robustness across various real-world environments (Paper IV). In another work, we concentrate on channel characteristics. We use the received signal strength as an indicator to monitor the channel behavior between transmitters and receivers. Based on the pattern of channel dynamics, we propose a spoofing detection system to augment wearable device security under body motions (Paper III).

A major portion of this dissertation tackles the challenges associated with low-power and secure wireless communication in practical deployment. Backscatter transmitters strongly depend on external emitter infrastructures. Our first contribution offers a low-power design, enabling a long communication range with reduced dependence on emitters. Radiometric fingerprinting encounters challenges in practical scenarios due to diverse wireless channels and costly system deployment. Our second and third contributions address these challenges, enabling low-cost deployment while providing a robust fingerprinting service.

1.3 Methods

This dissertation follows system research methodology to understand how systems function and interact. System research is crucial for deepening our understanding of complex systems and integrating technologies to tackle challenges in a dynamic, interconnected world. All my work involves the use of real hardware to study phenomena and evaluate solutions. We use quantitative research methods to analyze and assess system performance. In addition, Monte Carlo

and numerical simulations are used to decompose complex systems, model their components, and study their interactions in a controlled environment.

While the objectives of our experiments vary slightly, they can primarily be categorized into two types. First, experiments are used to quantify and characterize specific phenomena. For instance, in Paper I, we quantify the tunnel diode oscillator stability by conducting controlled experiments. More commonly, experiments are deployed to demonstrate and evaluate the system performance. For example, in Paper IV, we conduct experiments in different wireless environments to demonstrate the robustness of the designed system.

My dissertation centers around wireless communication. The inherent complexities and dynamics of wireless environments make experimental setups, measurements, and analysis necessary but difficult. We tackle this challenge in different steps to approach realistic scenarios. When the wireless environment is not the primary research focus, we perform experiments under ideal conditions. Small-scale experiments are carried out in offices with cables, completely avoiding the effects of multipath and interference. If the setup with cables is not feasible, we place devices at close yet sufficient distances, mitigating major impacts from surrounding wireless environments. Most large-scale experiments take place in an anechoic chamber isolated from complex wireless conditions. These experiments help us to set up a benchmark, such as the benchmark dataset in fingerprinting work. When the wireless environment is a critical impact factor, we perform experiments in a variety of everyday settings inside office buildings. Moreover, we also conduct outdoor experiments for long-range communication setups.

Due to the complexities of wireless systems and their interactions with the environment, developing, testing, and optimizing a system design solely through real-world experimentation is often challenging or impractical. Wireless systems can be complex with numerous variables at play. Simulations allow us to break down these complexities, model different components, and observe their interactions in a controlled setting. Monte Carlo simulation based on the statistical wireless channel is used in Paper IV to provide a systematic overview of the wireless channel's impact. Paper V employs numerical simulations to model the variation of backscatter fingerprints under varying voltages, assessing the robustness of the fingerprinting technique. In this dissertation, all simulations are conducted in Matlab in a hybrid manner, with part of the input from actual measurements.

1.4 Roadmap

This dissertation is structured into two parts. Part I provides a comprehensive summary including six chapters, while Part II is a compilation of the research papers included in this dissertation. The remainder of Part I is organized as follows. Chapter 2 introduces background information to facilitate

understanding this dissertation. Chapter 3 describes a summary of the six papers that constitute the core of my dissertation. Chapter 4 discusses the development of low-power communication systems from commodity IoT radios, to state-of-art backscatter technologies, to beyond backscatter designs. Chapter 5 reviews existing research on radiometric fingerprinting that aligns with or complements my work. Chapter 6 expands the vision towards future directions and concludes the dissertation.

2. Background

This chapter establishes the essential background knowledge. My dissertation centers around wireless communication systems. This chapter begins with an introduction to the architecture of transmitters. Then we discuss the imperfections inherent in transmitter hardware. Lastly, we present the characteristics and dynamics of wireless communication channels.

2.1 Resource-constrained Embedded Systems

The fundamental building block of IoT is the integration of a wireless communication interface with an embedded system. Such a system commonly combines sensing, computing, and wireless communication capabilities to monitor, gather, and process data from the environment and transmit it to other devices.

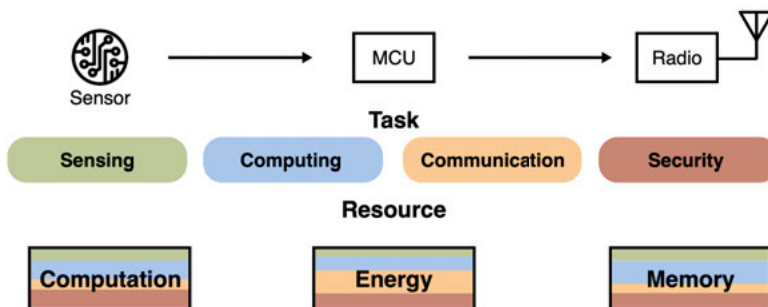


Figure 2.1. In embedded systems, the sensing, computing, communication and security tasks are handled by hardware components sharing limited computation, memory and energy resources.

The tasks of sensing, computing and communication are handled by specific hardware components. Sensors are responsible for converting the physical phenomena of interest into digital signal formats suitable for processing. The computing tasks are usually handled by an microcontroller unit (MCU) which performs local processing and orchestrates coordination among the hardware components. Within the scope of this dissertation, communication is managed by a radio frequency (RF) transceiver, which encompasses both digital and analog components.

In an era of rapidly expanding device interconnectivity, the emphasis on security to ensure confidentiality, integrity, and availability has become essential. In some cases, specialized security components, such as cryptographic co-processors and accelerators, or specialized designs, such as trusted execution environments, are employed to provide enhanced protection against potential threats.

All these hardware components share available computation, memory and typically energy resources. Advances in semiconductor and packaging technologies have now enabled diverse low-cost and low-power sensors operating on merely tens of microwatts power. Additionally, computing tasks, facilitated by constrained and low-power microcontrollers, require only hundreds of microwatts power [27, 28]. In contrast, the communication task implemented using commercial radio technologies, including BLE, ZigBee, WiFi, LoRa and Sigfox, still demands a few to tens of milliwatts power (see from the comparison in Chapter 3) [5, 28].

Embedded systems often face resource-related constraints, due to requirements concerning size, cost and battery lifetime. Depending on the specific application, various tasks may occupy varying proportions of the available resources. Addressing these constraints while maintaining the system's functionality stands as a fundamental challenge in the design of embedded systems.

2.2 Conventional Radio Frequency Transmitters

In this section, we review the conventional RF transmitter architecture commonly employed in wireless communication. As illustrated in Figure 1.2, a transmitter, at an abstract level, comprises three primary components: the protocol stack, modulator, and RF stage. Different architectures are adopted for the implementation of the digital wireless transmitter. We start with the straightforward direct-conversion transmitter architecture. As shown in Figure 2.2, a digital computation unit follows the protocol stack performing encoding, data packaging and modulation tasks. Consequently, it generates an information-bearing baseband signal at a low frequency. After that, the baseband signal is mixed with a high-frequency carrier signal generated by a local oscillator (LO), and is directly up-converted to the desired RF transmission band. After up-conversion, the signal passes through an RF amplifier, increasing its power to the desired transmission level. Typically, a band-pass filter is added after the amplifier to eliminate any unwanted harmonics and spurious emissions. The resulting signal is then transformed into an electromagnetic wave and radiated out through an antenna. The electromagnetic wave propagates at the speed of light and can be received by a receiver in its communication range.

As shown in Figure 2.3, the heterodyne architecture introduces an additional frequency conversion stage, where the baseband signal is first converted

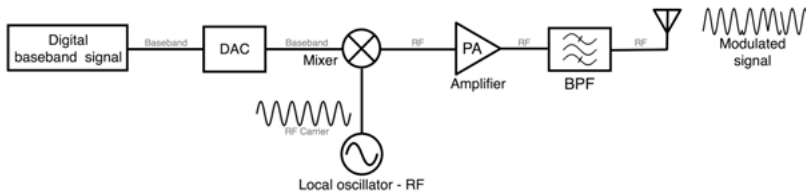


Figure 2.2. The architecture of direct-conversion transmitters.

to intermediate frequency (IF) band for processing, then mixed with a high-frequency LO converting to desired RF frequency. The superheterodyne transmitter is an advanced version of the heterodyne transmitter, typically involving multiple conversion and amplification stages to produce high-quality RF signal for transmission. Unlike in the direct-conversion transmitter, the filtering and amplification take place at low frequencies during IF stages. Low-frequency filters and amplifiers are more stable, with higher gain and reduced power draw. By selecting the well-tuned IF and filters, the transmitter can attenuate image frequency signals, minimize phase noise, and counteract direct current (DC) offset.

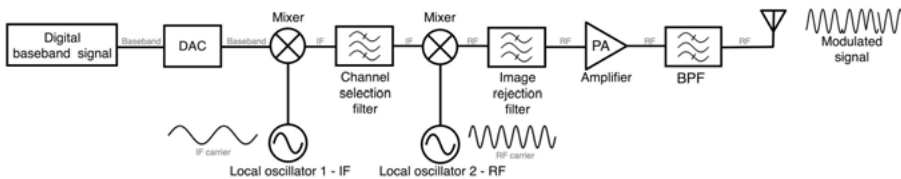


Figure 2.3. An example of heterodyne transmitters.

The direct-conversion transmitter stands out for its simplicity and compactness due to the elimination of IF stages. This architecture inherently leans towards a low power draw. With the advancements in integrated circuit (IC) design and digital signal processing (DSP), direct-conversion designs have become more common, especially in modern digital communication systems where integration and miniaturization are priorities. On the other hand, while heterodyne or superheterodyne architectures are more complex, they provide enhanced selectivity and flexibility. These architectures are widely used in commercially off the shelf (COTS) transceiver chips that demand high performance. Furthermore, their inherent flexibility makes them adept at supporting a wide variety of wireless standards and modulation schemes. This versatility renders them ideal for multimode, multiband signaling schemes [29].

2.3 Backscatter Transmitters

Backscatter tags operate by reflecting and absorbing an external RF signal to convey information. The incident RF signal can be a modulated ambient signal, such as a TV, WiFi or Bluetooth signal, or an unmodulated carrier. We consider an unmodulated carrier in this dissertation, noted as $S_{in}(t) = Ae^{j(2\pi f_c t + \varphi)}$ where A is the amplitude, f_c is the carrier frequency and φ is the phase of the incoming signal. This unmodulated carrier signal is generated by an external emitter device. The fundamental principle behind reflecting the RF signal is the impedance mismatching between the antenna complex impedance Z_A and the load complex impedance Z_L . The resulting complex reflection coefficient is given as:

$$\Gamma = \frac{Z_L - Z_A}{Z_L + Z_A} \quad (2.1)$$

This coefficient describes the ratio of the incoming signal $S_{in}(t)$ and the reflected signal $S_{out}(t)$ as below:

$$S_{out}(t) = \Gamma S_{in}(t) = |\Gamma| A e^{j(2\pi f_c t + \varphi + \angle \Gamma)} \quad (2.2)$$

The process of modulating data onto the carrier involves changing the load impedance Z_L , typically achieved by switching between different impedance configurations using an RF switch. For example, consider the three special cases: $Z_L = Z_A$, $Z_L = \infty$, and $Z_L = 0$. In these cases, Γ equals 0, 1, and -1 , respectively, and the incident signal is reflected with corresponding amplitude and phase shifts. In the simplest case, γ is either 0 or 1, representing either fully absorbing or reflecting the incident signal. The fundamental idea of backscatter is switching between more than two load impedances to obtain the reflection and absorption states.

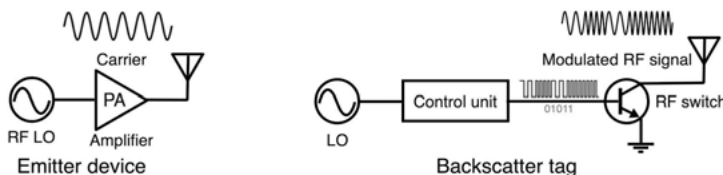


Figure 2.4. The architecture of backscatter communication systems.

A digital backscatter tag consists of two major modules, i.e., the control unit and the RF frontend. We show a 2-FSK backscatter system in Figure 2.4. The two impedances $Z_L = 0, Z_L = \infty$ are selected. A low-power MCU or field programmable gate array (FPGA) serves as the control unit, generating a control signal embedding information on two frequency tones. This control signal toggles the RF switch at different speeds, inducing impedance changes to reflect and thereby modulate the incident RF carrier. By selecting specific

impedances and switching between them, the circuit can play different roles in the transmission process, such as shifting the phase or/and amplitude in modulation schemes [12, 30, 31, 32, 33, 34] or suppressing the mirror image in single sideband backscatter [8, 14].

Backscatter Harmonics. Backscatter tags achieve modulation by toggling RF switches controlled by information-bearing signals. As a result, the signals are mixed with the incident carrier. Given the RF switches are digital components, the control signal is inherently limited to a square waveform. During the mixing process, the square signal introduces undesired harmonics. A square wave can be written as a Fourier series, which is the summation of sinusoidal components located at the harmonics of its fundamental frequencies:

$$square(t) = \frac{4}{\pi} \sum_{n=1}^{\infty} \frac{1}{n} \sin(n \cdot 2\pi ft), \text{ where } n = 1, 3, 5 \dots \quad (2.3)$$

Backscatter System Communication Range. In backscatter systems, the received signal strength is determined by multiple parameters, including the carrier emitter transmission power P_t , the distance between the emitter and the tag d_1 , the distance between the tag and the receiver d_2 , the wavelength of the RF signal λ , the reflection coefficient of the tag Γ , the loss in energy due to modulation α , and antenna gain G_t, G_{tag}, G_r . The signal strength at the receiver can be modeled with Friis path loss model [9]:

$$P_r = \left(\frac{P_t G_t \lambda^2}{(4\pi d_1)^2} \right) \left(G_{tag}^2 \alpha \frac{\Gamma^2}{4} \right) \left(\frac{G_r \lambda^2}{(4\pi d_2)^2} \right) \propto \frac{1}{(d_1 d_2)^2} \quad (2.4)$$

There are three key terms. The first term models the signal generated by the emitter and then propagates to the tag. Similarly, the third term models the signal propagation from the tag to the receiver. The middle term models the backscatter reflection operation. Given a backscatter system with fixed configuration ($P_t, \lambda, \alpha, \Gamma, G_t, G_{tag}, G_r$) and receiver sensitivity (the minimum P_r that a receiver can detect), the maximum product of d_1 and d_2 is determined. The communication range d_2 is large when the emitter is located close to the tag (small d_1). Conversely, as the distance d_1 to the emitter increases, the communication range of the tag d_2 diminishes.

2.4 Tunnel Diode

Tunnel diodes, a type of semiconductor diode, are notable for their ability to operate at very high frequencies. They were discovered more than half a century ago [35] and were the first semiconductor devices to demonstrate quantum tunneling. Quantum tunneling is a physics phenomenon that allows electrons to move through a barrier (P-N junction in the diode) even when they lack the energy that would normally be needed to do so.

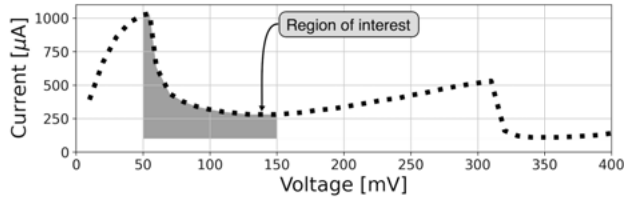


Figure 2.5. The I - V characteristics of a tunnel diode GE 1N 3712.

Tunnel diodes have several remarkable properties. The most distinctive feature is its region of negative resistance (RNR) [36]. Consider biasing a tunnel diode with a DC voltage and varying the bias voltage (V). This relationship between the current (I) passing through a tunnel diode and the bias voltage (V) is nonlinear. When plotted on a current-voltage (I - V) graph, the curve of the tunnel diode first rises and then dips down, indicating negative differential resistance. Moreover, tunnel diodes operate at low voltages. In Figure 2.5, we display the RNR for the GE 1N3712 tunnel diode [37] used in Paper I and Paper II. It only consumes tens of microwatts of power to bias the tunnel diode to the RNR. Additionally, tunnel diodes can switch on and off very rapidly, making them useful in high-frequency applications. Tunnel diodes can be used in the design of logic elements, switching circuits, and RF components, such as amplifiers [36] and oscillators demonstrated in our work.

2.5 Imperfections in Wireless Transmitters

In the production of electronic components, inherent variabilities invariably introduce non-ideal characteristics, often termed as imperfections. This is due to limitations in manufacturing techniques. As a result of a compromise between cost and performance, such imperfections are considered acceptable. In a wireless transmit chain, the imperfections present in both analog and digital components [38, 39]. Hardware imperfections manifest themselves in the radiated signal through deviation from the standardized ideal signal. Such deviation stems from the individual components but is also affected by the adopted transmitter architecture.

For analog components such as amplifiers, mixers and filters, non-linear behavior and phase noise lead to distortion and unwanted harmonics. Oscillators bring along a unique set of challenges, including frequency offset, instability, spurious oscillation, phase noise, harmonic distortion, and amplitude instability. Passive components, such as capacitors, resistors, and inductors, are manufactured with particular tolerance levels, meaning that their actual values might differ from the stated ones by a certain margin. For quadrature transmitters, any imbalance between the in-phase and quadrature signals can lead to distortion in the modulated symbols. The digital-to-analog con-

verter (DAC) components, which bridge the digital and analog segments of signal processing, possess a fixed resolution, limiting the accuracy of signal depiction. Moreover, their non-linearity can further induce further harmonic distortion in the output signal. While digital components are manufactured to a more consistent standard, they often rely on clock signals produced by oscillators. The impairments of oscillators can introduce imperfections such as jitter and skew in the time domain. Furthermore, both analog and digital components emit thermal noise, which can degrade the quality of the transmitted signal.

2.6 Radiometric Fingerprinting Systems

Radiometric fingerprint systems are designed to identify wireless transmitters based on the unique characteristics of their transmitted signals. This concept was initially investigated in the radar community for military applications, including spectrum management, traffic analysis, or targeted transmitter tracking [40]. A radiometric fingerprinting system consists of multiple wireless transmitters and a fingerprint identifier or authenticator on the receiver side.

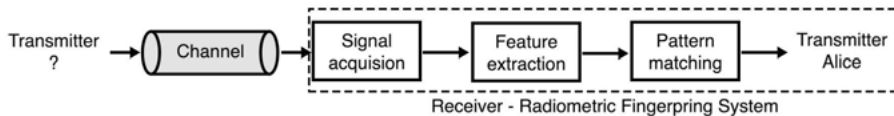


Figure 2.6. The overview of a radiometric fingerprinting system for identification.

Radiometric fingerprinting systems operate in three stages: signal acquisition, fingerprint feature extraction, and device identification or authentication through classification. Transmitters generate RF signals for communication following a specific physical-layer standard. As shown in Figure 2.6, once signals are acquired, their characteristics are extracted as distinct features, forming fingerprints. Subsequently, a matching algorithm determines the identity of the extracted fingerprint, drawing on knowledge from previously enrolled profiles. For an authentication service, the receiver executes the demodulation and obtains the transmitter’s self-claimed identity decoded in the data frame, such as the media access control address (MAC) or Internet protocol (IP) address. By checking the alignment between self-claimed identity and fingerprint identity, the system makes a decision whether to accept or reject the authentication request.

The fingerprinting system fundamentally tackles a classic pattern-matching challenge, spanning both enrollment and testing phases. When a device initially joins the network, its fingerprint is recorded at the receiver and registered as a device profile associated with its identity. Profiles for all enrolled devices are stored in a library, which aids decision-making in the testing

phase. To implement pattern matching, there are mainly two types of algorithms. Traditional methods measure the difference between captured fingerprints and enrolled profiles using distance metrics in the feature space, such as the Euclidean distance or Mahalanobis distance. The state-of-art methods utilize machine learning (ML) algorithms, such as support vector machine (SVM) [22, 41, 42, 43], k nearest neighbor (kNN) [22, 43, 44], or neural network (NN) [45]. These ML algorithms are trained with enrolled profiles. During the testing stage, the well-trained model judges the identity linked to the corresponding fingerprint. ML algorithms exhibit advantages in exploring nonlinear properties and handling outliers and obviate the need for the tedious distance threshold presetting process of the traditional methods.

2.7 Machine Learning Classifiers

This dissertation employs multiple supervised ML algorithms in different system designs. The basic supervised learning problem can be summarized as finding an accurate approximation, f^* , of a function, f , that expresses the relationship between the target variable Y and the input variable X :

$$f : X \rightarrow Y \quad (2.5)$$

Supervised learning uses a finite labeled training set to approximate the function f . As the training set is fed into the algorithm, the algorithm f^* adjusts its parameters until it has been fitted appropriately and outputs a well-trained model. In the classification problem, Y is discrete class C_k where $k = 1, \dots, K$. Classification aims at taking an input vector X and assigning it to one of the C_k classes [46]. In this dissertation, four supervised learning classification algorithms were used in the fingerprinting system evaluation, including SVM, kNN, random forest (RFC) and NN.

SVM operates by finding optimum hyperplanes that separate the data points into classes. These hyperplanes are determined by support vectors, which are data points near the hyperplane. The optimum hyperplane maximizes the margin from these points. To prevent overfitting, a soft margin is used to allow some misclassifications for better generalization. For non-linear data, SVM uses kernel tricks to project data into higher dimensions. Commonly used kernels are polynomial, radial basis function (rbf) and sigmoid. While primarily for binary classification, SVM can extend to handle multi-class classification problems using one vs rest (OvR) or one vs one (OvO) strategies. In testing, the class with the highest confidence from all SVMs is selected as output.

kNN is a machine learning algorithm that uses all training data points directly. For classification, it identifies k closest training samples to a new instance based on distance metrics like Euclidean or Manhattan distance. The class is then predicted using a majority vote from these neighbors. The choice of k

is crucial. A small k can lead to an overfitting problem and the result only captures noise with high variance. However, a large k can oversimplify the model, causing high bias and reduced accuracy.

RFC is an ensemble learning method that combines multiple decision trees to produce a more accurate and stable prediction. By using random subsets of data and features for each tree, it mitigates overfitting and offers robust performance. A decision tree is a supervised ML algorithm used for both classification and regression tasks. It works by splitting the data into subsets based on feature values, making decisions at each node until it reaches a leaf node with a predicted outcome. The tree structure consists of root nodes, internal nodes, and leaf nodes, representing decisions, conditions, and outcomes, respectively. **NN** consists of interconnected neurons arranged into layers: an input layer, one or more hidden layers and an output layer. Each neuron applies a linear transformation by computing a weighted sum of its input, adds a bias, and then applies an activation function that introduces non-linearity. A loss function is used to measure the error between the predicted output of the network and the true target values in the training data. Training involves forward propagation of data and backward adjustment of weights using optimization techniques like gradient descent, based on the error from a loss function. For classification, the number of output layer nodes matches the number of classes.

2.8 Wireless Channels

Wireless communication channels are dynamic due to noise, interference, and unpredictable changes because of user movement and environmental shifts. Even minor environmental changes can significantly distort the received signal magnitude, phase, and frequency. In indoor settings, small-scale fading dominates, resulting from *multipath* propagation and *Doppler* shift. Additionally, the transmitted power dissipates and interference alters the signal strength and background noise, that is *signal to noise ratio (SNR)*.

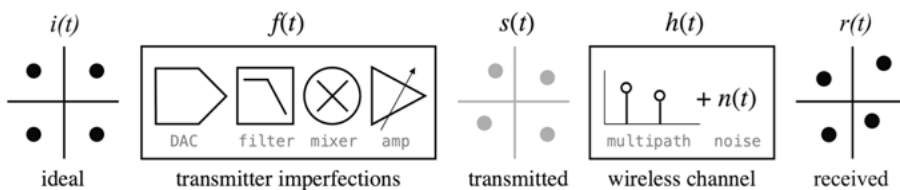


Figure 2.7. The model of a wireless communication system.

The wireless signal, radiated out from the transmitter antenna, passes through the wireless channel in the air and reaches the receiver antenna. As shown in Figure 2.7, considering transmitter imperfections $f(t)$, the signal radiated out

from the transmitter $s(t)$ can be modeled as:

$$s(t) = i(t) * f(t) \quad (2.6)$$

where $*$ is the convolution operation and $i(t)$ is an ideal information-bearing signal. Hardware-specific fingerprints deviate the transmitted signal from the ideal signal. When considering wireless channels $h(t)$, the signal observable to the receiver $r(t)$ can be modeled as:

$$r(t) = s(t) * h(t) = i(t) * f(t) * h(t) \quad (2.7)$$

The received signal involves both the transmitter fingerprint and the transient impact from the channel.

The *multipath* phenomenon occurs when a signal takes multiple paths from the transmitter to the receiver due to reflection, refraction, scattering, and diffraction off various obstacles and surfaces such as furniture, walls, glass and even the ground. This results in multiple signal versions at the receiver, differing in time, phase, and amplitude. In practice, a multipath channel has an inherent time-varying nature, which leads to fading. To model this, ray-tracing techniques are used, representing waveforms as particles and tracing their paths. Due to the radio channel's variability, statistical models are often preferred, modeling each path with a random time-varying impulse response, statistically characterizing signal attenuation [47]. The channel equivalent time-varying impulse response of a single path can be written as below:

$$h(\tau, t) = \alpha(t) e^{-j\varphi(t)} \sigma(t - \tau(t)) + n(t) \quad (2.8)$$

where the path delay $\tau(t)$ is determined by the path length $d(t)$ with Equation $\tau(t) = r(t)/c$. $\varphi(t) = 2\pi f_c \tau(t) - \varphi_D(t)$, where *Doppler* phase shift is captured by $\varphi_D(t)$, and Doppler frequency shift is $f_D = \frac{1}{2\pi} \frac{d\varphi_D(t)}{dt}$. *Noise* $n(t)$ follows the normal distribution. $\alpha(t)$ is a function of path loss. For a channel with N paths, the channel response $h(t)$ is the sum of every path:

$$h(t) = \sum_{i=0}^N \alpha_i(t) e^{-j\varphi_i(t)} \sigma(t - \tau_i(t)) + n(t) \quad (2.9)$$

Each path in the above *multipath* model can be modeled as a random process. The received signal in-phase $r_I(t)$ and quadrature $r_Q(t)$ components can be expressed with two Gaussian random variables with mean zero and equal variance σ^2 . The amplitude $z(t) = |r(t)| = \sqrt{r_I(t)^2 + r_Q(t)^2}$ can be characterized by a Rayleigh distribution when there is no line of sight (LOS) path:

$$p_Z(z) = \frac{z}{\sigma^2} \exp\left(-\frac{z^2}{2\sigma^2}\right), \quad z \geq 0 \quad (2.10)$$

If the channel has a fixed LOS component, the received signal equals the superposition of a complex Gaussian component and a LOS component. The

signal amplitude can be shown to have a Rician distribution given by:

$$p_z(z) = \frac{z}{\sigma^2} \exp\left[-\frac{(z^2 + s^2)}{2\sigma^2}\right] I_0\left(\frac{zs}{\sigma^2}\right), \quad z \geq 0 \quad (2.11)$$

where $2\sigma^2$ is the average power in the non line of sight (NLOS) *multipath* components and $s^2 = \alpha_0^2$ is the power in the LOS component. I_0 is the modified Bessel function of zeroth order.

The time variation of the channel due to the relative significant motions of either transmitter, receiver, or surrounding environment causes a *Doppler* shift in the received signal. The *Doppler* frequency shift is given by:

$$f_D = \frac{v \cos(\theta)}{c} f_c \quad (2.12)$$

where c is the velocity of signal propagation and the object is moving at a spatial angle θ with velocity v . The *Doppler* power spectrum $S(f)$ represents how the power of the received signal is distributed across various frequency shifts due to the *Doppler* effect. Different propagation environments and mobility patterns result in various shapes for $S(f)$. With uniformly distributed scatterers around a consistently moving receiver, $S(f)$ is bell-shaped and zero beyond $\max(f_D)$.

The *noise* term $n(t)$ in Equation 2.8 and 2.9, can be represented using additive white gaussian noise (AWGN). The *noise* exhibits a flat spectrum across frequencies and follows a Gaussian distribution in time. The AWGN model simulates the random noise that remains independent of and can be added to the signal of interest.

3. Summary of Papers

Paper I

Ambuj Varshney*, Wenqing Yan*, and Prabal Dutta. 2022. Judo: Addressing the Energy Asymmetry of Wireless Embedded Systems through Tunnel Diode based Wireless Transmitters. In *Proceedings of the 20th Annual International Conference on Mobile Systems, Applications and Services (MobiSys'22)*. DOI: 10.1145/3498361.3538923

Summary

In this paper, we introduce Judo, a low-power transmitter architecture based on a tunnel diode self-oscillating mixer (SoM). We refer to the conventional transmitter architecture and simplify the RF stage using a tunnel diode SoM circuit. Our design achieves low-power radio transmissions by integrating the stages of a radio transmitter into a single power-efficient step. In this step, a high-frequency carrier signal is generated locally and mixed with the analog baseband signal with a peak power draw around $48 \mu\text{W}$. Judo transmitters make trade-offs to achieve significant power efficiency, which is countered by a number of design choices. First of all, Judo transmitters radiate weak signals. We employ a highly sensitive receiver to maintain a long communication range. Secondly, Judo transmitters trade stability for power efficiency. While Judo transmitters can operate independently, the communication quality is degraded in dynamic environments. To address this issue, we stabilize the transmitter using the injection-locking phenomenon. An emitter device generates a carrier signal to stabilize the transmitter. As Judo transmitters can latch onto even weak signals, it allows the emitter device to be located significantly far away from the transmitter, and still support a long communication range. Based on this architecture, we designed a transmitter with a frequency-shift keying modulation scheme. Our evaluation demonstrates that Judo transmitters can achieve a communication range exceeding 100 m, even when the transmitter is located at 100 m away from a carrier emitter generating a signal of 25 dBm strength.

Reflections

This paper was my initial attempt at exploring low-power transmitter design using tunnel diodes. This was also my first collaboration with Prof. Ambuj Varshney, who had done work enhancing backscatter communication through tunnel diodes. Initially, our focus was characterizing the instability of tunnel diode oscillator (TDO). In our experiments, we discovered a design that can feed baseband signals into the TDO, enabling the circuit to serve dual roles as a SoM. This discovery formed the basis of Judo. The main contribution of this work is a novel low-power transmitter architecture, using a design principle fundamentally distinct from long-existing backscatter. Judo architecture closely resembles a conventional transmitter but operates on a low power budget similar to a backscatter transmitter, without inheriting its limitations. We demonstrate a new way to achieve wireless communication with power consumption at the microwatt level. This research not only prepared me with solid knowledge about low-power transmitter design but also laid the groundwork for subsequent research on backscatter fingerprinting (Paper V).

My Contributions

In this paper, Prof. Ambuj Varshney and I share the co-primary authorship. This work builds on Ambuj's earlier TDO research [48, 49]. Together, we discovered the SoM property. Based on this discovery, we designed the Judo transmitter architecture. We conducted experiments collaboratively. I took the lead in analyzing the experimental data, interpreting results, and processing graphs. I contributed to writing and structuring the manuscript.

Paper II

Muhammad Sarmad Mir*, Wenqing Yan*, Prabal Dutta, Domenico Giustini-ano, and Ambuj Varshney. 2023. TunnelLiFi: Bringing LiFi to Commodity Internet of Things Devices. In *Proceedings of the 24th International Workshop on Mobile Computing Systems and Applications (HotMobile'23)*. DOI: 10.1145/3572864.3580327

Summary

In this paper, we introduce a light receiver architecture allowing commodity IoT devices to receive light fidelity (LiFi) transmissions using their existing radio transceivers. We named this system TunnelLiFi. The key component is a TunnelLiFi tag acting as a LiFi-RF bridge that replicates information contained in LiFi transmissions onto radio waves. TunnelLiFi tag evolves from Judo transmitter architecture by coupling a photodiode with the tunnel diode

SoM. The SoM property allows the mixing of a weak photodiode signal with a locally generated RF carrier signal, drawing less than 100 μ W of power. The system consists of a LiFi transmitter, the TunnelLiFi tag, and an RF receiver. An external LiFi transmitter, built on open VLC project [50], is used to modulate the light and transmit baseband information. The TunnelLiFi tag's photodiode receives this signal and the tunnel SoM mixes it with an RF carrier signal. As a result, radio transmissions from the TunnelLiFi tag can be received by commodity radio transceivers. Similar to Judo, an external weak carrier signal stabilizes the emitted RF signal via injection locking, enhancing the link quality. Our prototype demonstrates TunnelLiFi as a low-power bridge that can operate with low bitrates (2.93 kbps) even in low-light conditions (300 lux).

Reflections

This paper is a follow-up work of Judo, and considers a novel application of tunnel diode SoM, acting as a LiFi-RF bridge. LiFi simultaneously provides energy, illumination, and information, making it a good candidate for IoT connectivity. However, adopting LiFi technology requires changes to both the transmission and reception infrastructure. This work focuses on the receiver design challenge and rethinks the LiFi receiver architecture. TunnelLiFi design provides a low-power solution enabling pervasive radio transceivers to receive LiFi signals. The contribution of this work lies in its potential to facilitate widespread deployment of the LiFi technology.

My Contributions

Muhammad Sarmad Mir and I share the co-primary authorship for this work. Prof. Ambuj Varshney proposed the idea of leveraging a Judo transmitter architecture to design a LiFi-RF bridge. Together, we performed the proof-of-concept experiments. Sarmad then conducted subsequent experiments during his visit to NUS (University of Singapore). I analyzed the experimental data and also contributed to writing the manuscript.

Paper III

Wenqing Yan, Sam Hylamia, Thiemo Voigt, and Christian Rohner. 2020. PHY-IDS: A Physical-layer Spoofing Attack Detection System for Wearable Devices. In *Proceedings of the 6th ACM Workshop on Wearable Systems and Applications - in conjunction with MobiSys'20*. DOI: 10.1145/3396870.3400010

Summary

In this paper, we introduce a spoofing intrusion detection system (IDS) for wearable devices leveraging body motion and lightweight statistical algorithms. This system utilizes the received signal strength indicator (RSSI) time series to monitor channel behavior between the transmitter and receiver. With body movement, the RSSI time series pattern of off-body devices differs from the on-body devices, and the on-body devices at different positions also differ from each other. This diversity in channel dynamics is used to identify frames that violate the regular pattern of the wireless signal from legitimate wearables. The system is evaluated using bodyworn devices positioned differently in real-world attack scenarios, including both on-body and off-body attackers. The results show that the system can detect naive attackers accurately, and maintains good accuracy even for sophisticated attackers.

Reflections

This short paper is the first project at the beginning of my Ph.D. journey, marking the start of my exploration in the wireless mobile computing research field. I am funded by a project focusing on securing wearables and implants. The initial idea is to leverage the wireless channel dynamics due to human body movement to secure the system. RSSI, a common link metric easily collected via transceiver chip APIs, offers low-resolution information about the transmitter's location. While RSSI has been used in stationary setups to detect spoofing devices, our work investigates its dynamics in wearable contexts. We find that RSSI time series exhibit distinct patterns during body movements, which are leveraged to identify the transmitter in this project.

My Contributions

I am the lead author of this paper. I identified and formulated the research question with feedback from Prof. Christian Rohner. I designed the framework and developed the algorithms. Sam Hylamia set up the wearable testbed. I implemented the system and conducted all experiments. I wrote the manuscript with inputs from all co-authors.

Paper IV

Wenqing Yan, Thiemo Voigt, and Christian Rohner. 2022. RRF: A Robust Radiometric Fingerprint System that Embraces Wireless Channel Diversity. In *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'22)*.

DOI: 10.1145/3507657.3528542

Summary

In this paper, we present RRF, a robust radiometric fingerprinting system designed to offer reliable identification/authentication under channel fading disturbances. Complex wireless channels significantly impact the accuracy of identifying transmitter devices using radiometric fingerprints. Through practical experiments and systematic simulations, we decompose the channel impact factors into three components, multipath, noise, and Doppler. We analyze the impact of each factor. The results indicate that multipath and noise dominate the distortions, and affect fingerprint features in a specific way. Leveraging these insights, we design pertinent strategies to deal with different channel impacts. Our system deploys a hybrid pipeline that combines wireless channel simulation, signal processing, and machine learning. In this pipeline, RRF first utilizes structured channel simulations to adjust the decision boundaries of the fingerprint classifier, which improves its tolerance towards multipath channel interference. Then, in the identification phase, RRF relies on noise compensation and a feature denoising filter to augment the system's stability for weak reception signals. Our experimental results show that RRF achieves an average accuracy consistently above 99% in empirical scenarios with complex channels.

Reflections

In the prior PHY-IDS project, I learned about the limitations of channel characteristics for transmitter identification, such as the ease of spoofing and sensitivity to device movement. In pursuit of a more effective alternative, I turned to radiometric fingerprinting and followed the work of Brik et al. [22]. Although not a new concept, my experimental results reveal the significant impact of wireless channel interference on radiometric fingerprinting. Most existing research emphasizes the ability to differentiate devices and often omits necessary designs to enhance the robustness under diverse wireless channel conditions. To bridge this research gap, I started the RRF project. This work contributes to understanding the impacts of wireless channels on radiometric fingerprints. We suggest using pertinent strategies to deal with different channel impacts. We demonstrate that already a simple ML model, combined with an established feature representation and modest signal processing, is sufficient to take the robustness of the radiometric fingerprinting system to a new level.

My Contributions

I am the primary author of this work and the sole student contributor. I identified and formulated the research question. I proposed the solution employing simulation-based data augmentation to enhance the system's robustness.

Then, the idea is further completed together with Prof. Christian Rohner. I designed the system framework and implemented it. I conducted all the experiments. I also wrote the majority of the manuscript.

Paper V

Wenqing Yan, Madhushanka Padmal, Dilushi Piumwardane, Thiemo Voigt, Christian Rohner. 2023. Decomposing Radiometric Fingerprints in Backscatter Systems. *under submission*.

Summary

In this paper, we present a backscatter radiometric fingerprinting system designed to identify tags and carrier emitters. The passive radiometric fingerprinting approach fits well with backscatter systems, which prioritize low power and simplicity. Backscatter systems delegate the power-intensive generation of high-frequency carriers to an external emitter device, while the low-power tag modulates data by reflecting these carrier signals. In this paper, we systematically analyze the backscatter architecture and decompose the fingerprint. This allows us to accurately distinguish and classify both tags and carrier emitters with a true accept ratio of over 98.4% and below 1.6% false accept ratio. Fingerprinting backscatter systems are inherently more challenging than conventional radio transmitters due to the emitter-tag separation with a simple architecture. To offer a comprehensive perspective, we assess the importance of features in conjunction with three sets of conventional transmitters. In addition, we seek insights into fingerprint stability. Our finding suggests that tag fingerprints are susceptible to voltage variations.

Reflections

In this paper, I combined the backscatter knowledge and experience collected in the fingerprinting project. Existing backscatter fingerprinting works predominantly focus on radio frequency identification (RFID) systems. In RFID system, the carrier emitter is integrated with the receiver, which overlooks the diversity of carrier emitter devices. The major contribution of this paper is demonstrating the feasibility of fingerprinting both the tag and the emitter device. Unlike fingerprinting commercial off-the-shelf (COTS) transmitters, collecting a large number of backscatter tags is challenging due to the lag in commercialization. In the evaluation, we used ten tags based on Carlos Pérez-Penichet's design.

My Contributions

I am the lead author of this paper. I identified and formulated the research question. I designed the framework and implemented the system. The data collection was a collaborative effort with co-authors. I conducted all evaluation experiments. I wrote the manuscript with feedback from all co-authors.

Paper VI

Wenqing Yan*, Mikolai-Alexander Gütschow*, Thiemo Voigt, Christian Rohner. 2023. ORF: Towards On-board Radiometric Fingerprinting Fully Integrated on an Embedded System. *under submission*.

Summary

In this paper, we demonstrate the first fully integrated on-board radiometric fingerprinting system, designed for low-cost and low-power COTS receivers. While radiometric fingerprinting systems have proven effective, existing systems require specialized hardware and non-trivial computational capability to extract fingerprint features, hindering their widespread adoption. To advance towards practical deployment, we transfer the entire fingerprinting pipeline, including signal acquisition, feature extraction and classification, to an nRF52833 embedded SoC that costs under 6 dollars. We achieve raw signal acquisition at a high sampling rate by re-purposing the Bluetooth direction finding extension (DFE) functionality. Our fingerprint feature extraction builds on a lightweight coherent-receiver pipeline, and we deploy a simple classification model for identity determination. The final prototype can identify a single frame within one second, consuming energy equivalent to half a second of active channel monitoring. Based on the experiments with 32 transmitter devices, our system consistently delivers over 92% identification accuracy.

Reflections

In this paper, we address another practical challenge in radiometric fingerprinting. In our earlier endeavors in fingerprinting, we were disappointed by the reliance on cumbersome and expensive setups requiring costly software defined radio (SDR) and dedicated computer processing resources. This project began with a critical question thrown out by Prof. Christian Rohner about the feasibility of a cost-effective implementation. The bottleneck to achieving it is the acquisition of signals at appropriate sampling rates using low-cost receivers. Typically, embedded transceiver chips offer only limited statistical link quality metrics rather than providing access to raw signal data. However,

the emerging support for the Bluetooth DFE in COTS devices changes this situation, paving the way for this project. For the first time, ORF showcases a radiometric fingerprinting system fully integrated on a cheap and low-power SoC.

My Contributions

I am one of the lead authors sharing co-primary authorship with Mikolai-Alexander Gütschow, a Master's thesis student under my supervision. Prof. Christian Rohner and I formulated the research question. I suggested using the nRF52833 SoC and investigated the viability of implementing our system on it. Mikolai adapted the system architecture from the RRF project for embedded implementation by translating it effectively into C code. We conducted the evaluation experiments together. I wrote the manuscript with feedback from all co-authors.

4. From Commodity IoT Radios to Backscatter to Beyond Backscatter

This chapter presents an overview of IoT communication radios that are commercially available and backscatter radios described in related research. By offering a horizontal comparison across different radios, this chapter contextualizes the results presented in Paper I within a broader context.

4.1 Commodity IoT Radios

In the realm of IoT, a variety of commercial radios, i.e. WiFi, Bluetooth, Zigbee/Thread, Sigfox, and long-range radio (LoRa) are employed to meet the varying demands of data rate, communication range, and power consumption, thereby ensuring optimal performance across diverse applications and deployment scenarios. Each radio technology has carved out its own niche in the marketplace. WiFi, with its high data rates reaching up to 9.6 Gbps in WiFi 6, is preferred in scenarios demanding transmission of large data volumes with low latency. However, it is characterized by relatively high power consumption. In contrast, Zigbee/Thread and BLE (Bluetooth Low Energy) are optimized for low power consumption. BLE is suitable for short-range point-to-point communications with up to 2 Mbps data rate [51]. Zigbee/Thread, with IEEE 802.15.4 as the underlying physical and network layer protocol, is optimized for reliable and low-power mesh networks with lower data rates of 250 kbps [52]. For long-range, low-power IoT applications, LoRa and Sigfox are the preferred protocols. LoRa, utilizing chirp spread spectrum (CSS) modulation, can achieve a communication range of several kilometers, with low data rates ranging from 0.3-50 kbps [53]. Sigfox, while operating at even lower data rates of up to 100 kbps, maintains a comparable range and is similarly efficient in terms of power usage [54].

In general, commercial radios have relatively high power consumption, typically consuming a few to hundreds of milliwatts. Appendix A lists parameters determining the energy efficiency of the aforementioned technologies, collected from the datasheet of COTS transceiver chips or SoCs widely used in IoT applications. In the following section, Figure 4.1 compares Judo with commodity and backscatter radios to provide a holistic view of the dissertation contribution in a broader context.

4.2 Backscatter Radios

RFID and Modified RFID for Sensing. RFID remains the dominant backscatter application in the market. It is known for its battery-free design with extremely low power consumption and is primarily used for short-range identification and tracking. As the IoT landscape expands, RFID sensing integration has gained traction, with manufacturers like NXP [55], Smartrac [56], RadioForce [57] offering RFID sensors for environmental monitoring. Open-source platforms like WISP [58] and Moo [59] enable advanced low-power applications, such as battery-free camera [60] and microphones [61]. However, these systems rely on complex, costly, and power-hungry RFID readers which can only interact with RFID tags.

Backscatter Beyond RFID. Extensive studies enhance the backscatter system communication performance and compatibility with existing commodity radios, which unlock the potential of backscatter beyond RFID. Some works deploy unmodulated excitation signals like RFID and enable the interoperation with commodity radios, such as WiFi [14], Bluetooth [17, 62], IEEE 802.15.4 [8]. Passive WiFi demonstrates tens of meters communication range with up to a few Mbps data rate [9]. LoRa backscatter presents a CSS backscatter design, enabling long-range communication at a few kilometers [12]. LoRea focuses on narrow-band communication, demonstrating a comparable communication up to kilometers [11].

Ambient Backscatter Ambient backscatter modulates information onto RF signals already present in existing systems. These ambient signals often carry their own data. Early attempts, using TV signals [63] and WiFi transmissions [64] for tag communication, face range (below a few tens of centimeters), and data rate (a few kbps) limitations. BackFi [65] improves the data rate to Mbps levels but is still constrained to a short communication range of a few meters. FS-Backscatter mitigates the carrier signal interference by shifting the excitation signal to an adjacent spectrum [66]. HitchHike increases the communication range to tens of meters with codeword translation [15]. Syncscatter further extends the communication range of ambient backscatter by symbol-level synchronization [10]. PLoRa utilizes ambient LoRa transmission, enabling long-range backscatter communication [13].

Energy per Bit Comparison. To assess how efficiently different communication technologies utilize the energy, the data rate is a key factor. Higher data rates may consume more power but can be more energy-efficient over time, making energy per bit a valuable metric. Figure 4.1 shows the active power draw in relation to data rates. The dotted diagonal lines represent energy per bit, indicating the amount of energy consumed to transmit a single bit of information. As illustrated, backscatter systems are typically around 100 times more efficient than conventional radios, which is advantageous for battery-constrained or energy-harvesting applications. When comparing backscatter systems described in related research, the power consumption largely depends

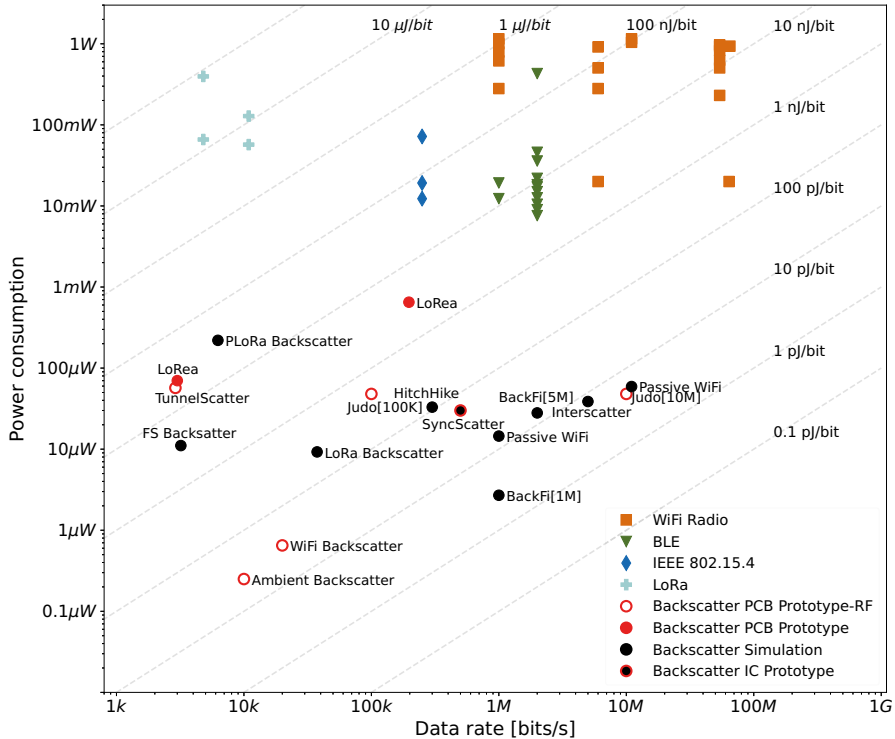


Figure 4.1. The energy per bit of Judo and wireless radio technologies, including commercial radios and backscatter systems introduced in research papers. The full dataset can be found in Appendix A Table 1 and 2.

on the implementation. An implementation using off-the-shelf discrete components can consume a magnitude higher power than the implementation in a sub-micron ASIC design. Most backscatter systems report below sub-hundred microwatts power consumption based on simulations. SyncScatter, being an exception, shows a $30 \mu\text{W}$ consumption in an IC prototype. Due to the absence of an accurate tunnel diode model, in Judo (Paper I), we estimate the power draw by measurement using a prototype with discrete components. While Judo is not a backscatter design, its energy per bit metric based on the prototype is comparable with existing backscatter works. In our work, we also demonstrate the potential to support higher data rates with even better efficiency.

Communication Range Comparison. In backscatter systems, where tags serve as the data source, the communication range of these tags is crucial. However, it is misleading to consider only the tag-to-receiver communication range. The maximum effective communication range in backscatter systems is determined by the product of emitter-to-tag (d_1) and tag-to-receiver (d_2), as described in Equation 2.4. Configurations with a very short emitter-to-tag

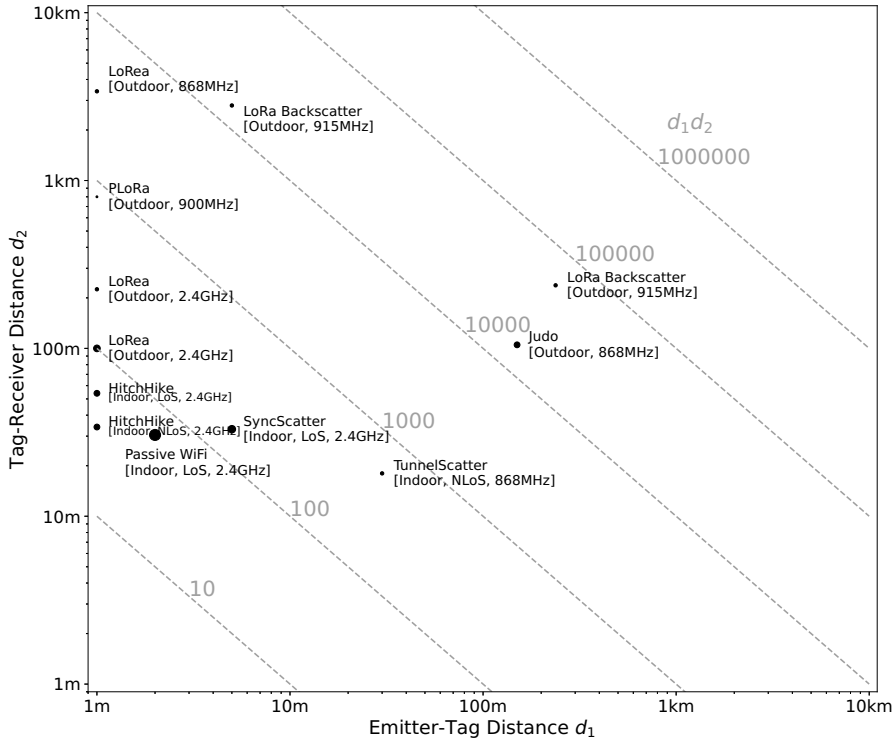


Figure 4.2. The communication range of backscatter systems. The marker size represents the bitrate. The backscatter communication range is determined by the product of emitter-tag distance d_1 and tag-receiver distance d_2 . The full dataset can be found in Appendix A Table 3.

distance (d_1) are impractical for real-world deployments and fail to highlight the advantages of backscatter technology over conventional active radios. To effectively compare different backscatter systems, we use the range metric d_1d_2 , considering both emitter-to-tag and tag-to-receiver distances. This metric is also applied to the Judo system, due to its similar bistatic configuration, ensuring a consistent comparison across systems. Figure 4.2 shows the communication range comparison of existing backscatter systems. The dotted diagonal lines show the d_1d_2 metric. The marker size represents the data rate. Among the listed systems, Judo outperforms most systems in range, except the LoRa backscatter system [12]. The remarkable communication range of LoRa backscatter is mainly attributed to the high link budget provided by CSS modulation and the uses of the sub-GHz frequency band. Judo operates at the same frequency band but deploys narrowband FSK modulation. Moreover, Judo uses 100 kbps data rate, which is at least three times higher than the data rate demonstrated in the LoRa backscatter. Notably, the design of Judo is modulation-agnostic and can also support CSS, offering the potential for further communication range enhancement.

4.3 Radio Technologies Beyond Backscatter

Backscatter systems divide tasks in the conventional radio RF stage into two devices. The emitter infrastructure manages the power-hungry task of generating high-frequency carriers. This allows tags to only perform low-power modulation operations by reflecting the incident carrier signal. While the power consumption of the backscatter tag is orders of magnitude less than conventional transmitters, the total energy required for every transmission across emitter, tag, and receiver devices is unchanged at best. Two approaches have emerged targeting an improvement in overall system energy efficiency, shifting beyond traditional backscatter.

Reflection Amplifier. One approach replaces the standard RF switch in a backscatter tag with a low-power reflection amplifier, allowing the carrier signal to be backscattered with a gain. Negative-resistance elements such as transistors or tunnel diodes are used in reflection amplifiers. Amato et al. create a tunnel diode-based reflection amplifier that operates in the 5.8 GHz band with a gain of 34 dB while consuming 45 μW [67, 68, 69, 70]. Adeyeye et al. design a repeater in the 5.8 GHz frequency band using a tunnel diode reflection amplifier with a gain as high as 50 dB while consuming 40 μW [71]. Varshney et al. design a tunnel diode reflection amplifier operating in the 868 MHz band with a reflection gain of 35 dB and a peak biasing power of 57 μW [48]. Kimionis design a transistor-based reflector in the 900 MHz frequency band with a reflection gain of 10.2 dB and a peak power consumption of 325 μW [72]. Dong et al. leverage tunnel diode reflection amplifier with 22 dB gain to strengthen weak GPS signals [73]. However, the reflection gain amplifies unwanted harmonics inherent in backscatter mixing operations as well, covering a significant part of the unlicensed spectrum. In Paper I and II, Judo transmitters are not reflection-based and leverage the SoM property to overcome this challenge.

Modulated Noise Communication. Another innovative approach is Modulated Noise Communication (MNC). This method moves one step further and directly eliminates the generation of high-frequency carriers, leveraging Johnson noise left by the transmitter resistors to modulate baseband data. Kapetanovic et al. demonstrate a prototype with a low data rate up to 26 bps and a limited range up to 7.3 m [74]. From the system view, MNC operates independently like a traditional transmitter, eliminating the complexity associated with the emitter in backscatter systems. Circuit-wise, MNC mirrors backscatter modulation by altering antenna loads, sharing the advantages of minimal power consumption and simplicity.

5. Transmitter Identification with Fingerprints in Wireless Signals

In wireless communication systems, fingerprints embedded in signals can be leveraged to identify transmitters. This chapter overviews existing fingerprinting works and puts the results presented in Paper III, IV, V and VI into a broad research field.

5.1 Channel-specific Fingerprints

Channel-specific fingerprints capture properties of the communication channel, which have gained popularity in indoor localization due to their simplicity and minimal hardware requirements. They leverage features such as received signal strength [75, 76, 77], channel state information (CSI) [78], and channel frequency response [79, 80]. Unlike conventional geometric localization approaches, fingerprinting methods employ pattern matching to determine device positions, which excels in cluttered indoor environments with stable configuration [76, 77, 78]. These systems commonly involve multiple measurements at different points in space to improve the precision and robustness of localization. Channel-specific fingerprints fit better in localization rather than device identification due to their low uniqueness. Using channel-specific fingerprints for device identification relies heavily on the assumption of stationary users and environments, making them hard to apply in practical scenarios where moving objects are pervasive in the environment. Paper III investigates wearable scenarios. Based on the pattern of body movement, channel-specific time series are utilized to identify transmitters.

5.2 Hardware-specific Fingerprints

Hardware-specific fingerprints highlight unique imperfections of electronics on the transmitter. We also term them radiometric fingerprints in this dissertation. Radiometric fingerprints were first investigated in the radar community as specific emitter identification (SEI) for military usage to track enemy radars during World War II [81]. Research emerged in the mid- and late-90s to detect illegal radio VHF FM transmitters [82, 83, 84]. With the proliferation of commodity wireless communication devices, radiometric fingerprints have been

explored to identify WiFi, ZigBee, Bluetooth, LoRa and RFID transmitters in diverse scenarios, including device cloning, defective device detection, and access control. In this section, I structure existing systems shown in related research into five categories.

Transient-based Fingerprints. Early works focus on the transient phase at the beginning of each radio transmission before frequency synthesizers settle on the pre-set frequency. Unique features of the transient signal, such as the amplitude profile [85], phase characteristics [86], adjacent Fourier transform spectra [23], and energy envelope [42] are leveraged for device identification. However, systems relying on the transient phase are sensitive to device locations and antenna polarization [23]. Moreover, the duration of the transient phase is usually at a sub-microsecond level, requiring high-speed signal acquisition equipment, which increases the implementation cost.

Modeling-based Fingerprints. A few works have focused on mathematically expressing hardware imperfections by modeling the signal transmission process in the transmit chain. These models primarily address nonlinear distortions from transmitter hardware, such as DACs and amplifiers [18, 25, 87]. The model parameters, obtained either from statistical modeling [87] or captured signals using data-driven regression [25], serve as device fingerprints. Modeling-based fingerprints commonly do not cover [18] or only partially cover the complex disturbance from wireless channels [18, 25].

High-dimensional Raw Signal Fingerprints. Neural network (NN) algorithms have been increasingly exploited to automate feature extraction in radiometric fingerprinting systems. The capability of NN allows the usage of high-dimensional signals in the time or frequency domain as raw fingerprints. Various formats of raw fingerprints are used, including I/Q signal time series [26], time series of error between ideal and synchronized signals [19], and constellation trace plots in image format [88, 89]. However, NN-based fingerprinting is significantly impacted by wireless channels. Al-Shawabka et al. quantify the impact with experimental data [20]. While raw signals contain all hardware-specific information, they are often very noisy. Leveraging NN to process raw signals demands extensive computation resources, making it less suitable for efficient fingerprinting. Additionally, NN are often criticized for their black-box nature, lacking in flexibility and interpretability. In our work, we adopt a white-box approach, focusing on analyzing and eliminating different channel disturbances.

Low-dimensional Modulation Domain Fingerprints. Modulation-based fingerprints assign statistics of the modulation errors as device fingerprints, which are extracted via well-defined signal processing procedures. Modulation-related features are first proposed by Brik et al. [22] for WiFi systems. The initial features include frequency error, SYNC correlation, I/Q offset, magnitude error, and phase error. Then this technique is explored in several ISM band technologies, including ZigBee [90], BLE [91] and LoRa [88, 92]. And features

are expanded to I/Q imbalance [41], modulation shapes [93], and constellation error [94]. The fingerprints in this category are interpreted depending on the underlying modulation scheme. However, with the guidance of wireless communication knowledge, the crafted features refine structured fingerprints containing more intense information. Modulation domain fingerprinting typically requires fewer resources than methods that process large volumes of raw signals, making it efficient for embedded systems deployment with limited computation, memory and energy resources. This dissertation (Paper IV, V, VI) focus on modulation domain fingerprints. We utilize the side information from the demodulation pipeline, allowing for seamless integration into the receiver chain with minimal additional resource demands.

Fingerprints in Backscatter Systems. Existing backscatter fingerprinting works are mainly conducted in the RFID context. Features in time and frequency domains are used to fingerprint RFID tags [95, 96]. Some works focus on fingerprints unique in backscatter designs. RCID leverages the reflection coefficient of RFID tag circuit as the fingerprint [97]. Hu-Fu uses the coupling features between two tags to identify tags, eliminating the wireless channel disturbance but requiring two tags to operate simultaneously [98]. Eingerprint leverages distinct energy storage capability of passive RFID tags to authenticate them [99]. HarvestPrint uses frequency variations during the capacitor discharge in low-power tag oscillators to fingerprint tags [100]. All these systems only identify backscatter tags. In contrast, our work (Paper V) fingerprints both tags and emitters for the first time. We move the scope to general backscatter fingerprinting systems beyond RFID.

5.3 Channel-robust Fingerprinting Systems

Effective fingerprinting systems should maintain robustness against positional changes, environmental variations, and device mobility. The wireless channel is a major contributor to accuracy degradation in radiometric fingerprinting [18, 19, 20, 21]. To enhance the robustness of the radiometric fingerprinting system towards complex channel disturbances, multiple methods are proposed.

Several works investigate frequency domain features robust to locations to fingerprint WiFi devices [101, 102]. These features leverage the relative relation between subcarriers, which are limited to wideband radios. One approach alleviates channel effects by restoring a less distorted version of the transmitted signal with the channel estimation support [25, 103]. However, this approach requires either a known reference signal or sophisticated algorithms for channel estimation. Another approach deploys a transfer learning method and retrains the model during deployment [104]. Training models is often resource-intensive and time-consuming, which is not always practical in actual deployments. Several works focus on the low signal strength condi-

tion and devise a hybrid classifier by adjusting feature weights based on the received signal SNR level [90, 105, 106]. However, these systems overlook other impact factors, such as multipath.

To make fingerprinting systems robust to unseen complex channels, Soltani et al. leverage CNN together with data augmentation, which expands the training set with various channel-distorted fingerprints considering both multipath and noise impacts [21]. Similarly, our work (paper IV) adopts data augmentation methods with the support of wireless channel models. Differently, our method decomposes different channel impact factors. With detailed guidance that benefits from the structured feature space, we deploy distinct strategies towards multipath and noise, resulting in a more explainable and efficient system design.

6. Conclusions and Future Work

6.1 Conclusions

Wireless communication is a key enabler for the IoT, connecting billions of devices. The increasing prevalence of constrained embedded devices, operating on limited energy resources, requires developing low-power and secure wireless communication solutions. This dissertation addresses this need by designing low-power wireless transmitters and developing passive radiometric fingerprinting systems for robust and efficient transmitter identification.

Our work contributes to understanding the role of transmitter components and channel factors in wireless communication systems. We present a novel strategy for designing low-power transmitters by rearranging the functions of components. By analyzing the impacts of wireless channel factors, we improve the robustness of the fingerprinting system under complex channel distortions. And by understanding how components contribute to signal generation, we engineer the fingerprint features enabling the resource-efficient implementation on embedded devices.

Backscatter has long been considered a promising candidate for low-power wireless communication. It facilitates the deployment of embedded systems using small batteries, such as thin film or printed types, or battery-free options that harvest energy from environmental sources. However, in real-world deployments, the communication range of backscatter transmitters strongly depends on an external emitter infrastructure. For an extended communication range, backscatter requires the proximity of the transmitter tags to an emitter device that generates strong signals.

In this dissertation, we propose a transmitter design that rethinks the principle of backscatter design. Instead of offloading power-hungry tasks to an external emitter, as backscatter does, we integrate these tasks into the RF stage in a single low-power manner. While resembling conventional transmitters, this design distinguishes itself through its remarkable power efficiency, consuming only tens of microwatts power. This efficiency comes at the cost of stability, which we address by using an external carrier emitter to stabilize the signal. We rearrange the functions of transmitter components and redefine the role of the emitter device. Our transmitter can latch onto a weak carrier signal, significantly reducing its dependence on emitters. This allows the transmitter to communicate over a hundred meters, even when the emitter is more than a hundred meters away. This contribution provides a viable solution to the range limitations inherent in backscatter systems, potentially expanding their application in various real-world scenarios.

Radiometric fingerprinting identifies wireless transmitters based on their hardware components' unique and inherent imperfections. Its passive nature adds a valuable security layer, enabling the identification of transmitters without requiring active cooperation from the devices being identified. This method protects wireless communication systems from various security threats, including device cloning, spoofing, and replay attacks. This dissertation adapts radiometric fingerprinting for real-world deployments, applying it to both conventional active radios and backscatter radios.

The dynamic nature of real-world wireless channels significantly challenges the robustness of radiometric fingerprinting. The key idea is to decompose the complex channel interference into individual impact factors and systematically assess each factor's impact on radiometric fingerprints. These understandings enable us to develop tailored strategies that effectively mitigate wireless channel disturbances. The proposed system substantially enhances fingerprinting robustness, achieving consistent identification accuracy across complex wireless environments. This work makes radiometric fingerprinting effective in real-world deployments under diverse scenarios.

Most prior radiometric fingerprinting works rely on sophisticated signal acquisition equipment and dedicated computer processing resources. Our work demonstrates a resource-efficient radiometric fingerprinting chain. From signal acquisition to feature extraction and classification, all are seamlessly integrated within the confines of a single SoC (Paper VI). This contribution simplifies the traditionally complex setup, facilitating the large-scale deployment of fingerprinting systems on low-cost COTS embedded devices.

Backscatter transmitters fundamentally differ from conventional active transmitters regarding the electronic component composition within the transmit chain. In backscatter systems, the radio transmission is a joint effort between the backscatter transmitter and the carrier emitter. Our work demonstrates the dual identification of backscatter transmitters and carrier emitters in different scenarios. Beyond security applications, recognizing the emitter embeds a notion of locality, exposing fingerprinting usage in backscatter network management tasks such as coordinating emitters.

In general, this dissertation is anchored in the rapidly evolving landscape of enhancing connectivity among IoT devices. Our works contribute to understanding the roles of components in wireless communication systems and demonstrate the practical implications of these insights in real-world applications.

6.2 Future Work

As we look toward the future, it is intriguing to speculate on how the ideas and results from this dissertation can be leveraged and expanded upon in new and innovative ways. In this section, I will discuss several directions as potential areas for future development and exploration.

Stand-alone Tunnel Diode SoM Transmitters The tunnel diode SoM transmitter, proposed in Paper I, employs a design principle of trading stability for low-power consumption. Experimental results demonstrate the transmitter’s capability of communicating across several floors indoors without requiring a carrier emitter. However, the radiated signal is noisy, unstable, and can be affected by changes in the environment. In our work, the injection-locking phenomenon is used to improve the tunnel diode SoM stability, which requires an external emitter. Like a backscatter system, employing an additional emitter device increases the complexity of system deployment. An open challenge is alternative methods to stabilize the tunnel diode SoM without increasing system complexity. The possible direction is leveraging another communication channel to feed the injection-locking signal, e.g., flexible conductive substrates [107].

Fingerprinting Tunnel Diode SoM Transmitters The hardware-specific fingerprints of transmitters are closely related to its architecture as well as components in the transmit chain. The tunnel diode SoM transmitter employ a novel architecture that incorporates unique hardware blocks, thereby unveiling opportunities for effective fingerprinting. Our experimental observations have revealed that the I-V curve of the tunnel diode exhibits distinct variations from one component to another. These variations, stemming from inherent imperfections in the components, potentially leave unique and identifiable fingerprints in the emitted signals.

Unknown Device Detection in Radiometric Fingerprinting In radiometric fingerprinting system implementations, data-driven ML classifiers trained with fingerprints from enrolled devices, are used for identification. One realistic attack model involves adversaries using unenrolled devices. Detecting such devices requires the classifier to identify data points that differ from its training data. This is particularly challenging due to the lack of prior knowledge of unknown fingerprints. The solution to address this issue depends on the choice of classifier. In Paper IV, we briefly discuss solutions for the SVM classifier, and another collaborative work proposes a solution for the neural network classifier [108]. Still, designing a comprehensive system that effectively manages unenrolled devices is an open challenge.

Obfuscating Fingerprints to Defense Privacy Threats Radiometric fingerprinting can be used implicitly by overhearing the wireless communication signals. This implies that fingerprinting is a double-edged sword. On the one hand, it can enhance security for legitimate entities by adding an additional identification layer without the typical overhead associated with such operations. On the other hand, this technology could potentially be exploited by illegitimate entities to track users, raising significant privacy and security concerns [109]. To mitigate this privacy threat, finding a practical and effective method to obfuscate hardware-specific fingerprints remains an unresolved research area.

Leveraging Fingerprinting to Improve Communication Quality

Hardware imperfections typically exist due to the limitation of manufacturing processing as well as the compromise between cost and performance. For example, while manufacturers could employ high-quality components with high precision in their radios, this approach would raise the cost per device. The tolerance of acceptable hardware imperfections depends on the radio technology parameters, such as data rates, operating frequencies, and modulation schemes. 5G cellular technology, operating at millimeter-wave frequencies with GHz bandwidths, is particularly sensitive to such imperfections. Hardware imperfections can significantly degrade the quality of the communication. By analyzing transmitter fingerprints, the receiver can adapt its signal processing algorithms specifically to that transmitter. This tailored approach can lead to clear signal reception and reduced error rates.

Summary in Swedish

Trådlös kommunikation är en viktig förutsättning för IoT. Utvecklingen går mot allt mindre IoT-enheter och därmed även ett minskande utrymme för batterier och andra energikällor. De relativt begränsade energiresurserna tvingar fram nya strömsnåla och robusta kommunikationslösningar. Denna avhandling adresserar detta behov och presenterar nya radiosändare med extremt låg effekt. Vidare utvecklar vi i avhandlingen passiva och robusta radiometrisk fingeravtryckssystem för identifiering av olika sändare med lågt effektbehov.

Backscatter-tekniken anses vara en lovande kandidat för trådlös kommunikation med låg effekt. Tekniken är attraktiv för inbyggda system som använder extremt små batterier, t.ex. tunnfilmsbaserade eller tryckta batterier. Tekniken passar även för de alternativ som skördar små mängder energi från omgivningen. I verkligheten begränsas dock användandet av den korta räckvidden. Backscatter-sändarnas kommunikationsräckvidd är starkt beroende av en infrastruktur av externa redan existerande radiosändare som genererar tillräckligt starka signaler för scattering på en frekvens som harmoniserar med backscatter-systemet. För att få en praktisk räckvidd kräver backscatter-tekniken att dess sändare befinner sig i närheten av någon av dessa externa sändare.

I den här avhandlingen föreslår vi en ny sändare som omprövar den rådande närhetsprincipen. Istället för att flytta energiintensiva uppgifter till en extern sändare, som nuvarande backscatter gör, integrerar vi dessa på ett strömsnålt sätt i sändaren. Även om konstruktion i grunden liknar nuvarande sändare utmärker den sig genom sin anmärkningsvärda energieffektivitet. Den förbrukar endast tiotals mikrowatt. Denna effektivitet kommer dock på bekostnad av stabiliteten i radiosignalen. Vi hanterar detta problem genom att använda en extern bärvågsemitter för stabilisering. Genom att omorganisera funktionerna hos hårdvarukomponenterna komponenter i signalgenereringskedjan kan vår unika design av sändaren utnyttja en svagare bärvåg, vilket avsevärt minskar dess beroende av en extern infrastruktur. Detta gör att vår sändare kan kommunicera över hundra meter istället för ett antal meter och är ett signifikant vetenskapligt bidrag jämfört med tidigare räckvidder. Potentiellt kan det utöka antalet tillämpningar för backscatter för verkliga scenarier.

Radiometrisk fingeravtryck som identifierar trådlösa sändare är baserade på fabriktypiska radioenheter och inneboende små men normala ofullkomligheter i hårdvaran. Fingeravtrycket tillför därför ett värdefullt säkerhetslager genom en identifiering av sändaren utan att kräva en kostsam aktiv kommunikation mellan enheter. Metoden skyddar trådlösa system från säkerhetsshot inklusive kloning av enheter, förfalskningsattacker och replay-attacker.

I avhandlingen undersöks tillämpningen av fingeravtryck både på konventionella radiosändare och backscatter-sändare. Fokus är anpassning av fingeravtrycksmetoden för verkliga driftsättningar.

Den dynamiska karaktären hos radiokanalen och interferensen från andra källor utmanar avsevärt robustheten hos radiometrisk fingeravtryck. För att förstå och kompensera för påverkan på radiosignalen delar vi upp den i enskilda påverkansfaktorer och bedömer systematiskt varje faktors inverkan på fingeravtrycket. Denna förståelse har vi erhållit genom kontrollerad kanalsimulering och verkliga experiment. Det har gjort det möjligt för oss att utveckla skraddarsydda strategier som effektivt reducerar störningarna. Vi menar att våra resultat gör att radiometrisk fingeravtryck blir användbara i verkliga komplexa signalmiljöer.

Tidigare fingeravtrycksmetoder kräver sofistikerad signalbearbetning som behöver avsevärda datorresurser. Vårt arbete demonstrerar att det är möjligt att designa en resurseffektiv fingeravtryckskedja. Allt från signalinhämtning till extraktion och klassificering av radiofaktorerna har integrerats sömlöst inom ramen för en enda SoC. Detta förenklar storskalig användning av fingeravtryckssystem på billiga standardiserade IoT-enheter.

I backscatter-system baseras transmissionen på en koordinering mellan backscatter- och bärvågssändarnas signaler. Notera att hårdvaran i dessa två enheter båda lämnar ett överlappande fingeravtryck på back-scattersignalen. Vi har forskat hur man kan dela upp fingeravtrycket dem emellan. I praktiken innebär att det blir möjligt att göra en samtidig identifiering av bägge sändarna. Vi har visat på effektiviteten hos vår metod genom praktiska experiment i uppsättningar av radioparametrar olika scenarier. Utöver säkerhetstillämpningar ger en igenkänning av sändaren en uppfattning om lokalitet, vilket gör att fingeravtryck även kan användas till att koordinera sändare.

Avhandlingen är positionerad i området strömsnåla IoT-enheter som är ett snabbt växande. Vårt vetenskapliga bidrag är framförallt förståelsen för hårdvarukomponenter och kanalfaktorer roll i kommunikationssystemet. Vi visar också de praktiska konsekvenserna av dessa insikter i verkliga tillämpningar.

Appendix A.

Radio Datasets

The following datasets are used to compare the energy per bit and communication range between commodity radios, backscatter radios, and the Judo system introduced in this dissertation.

Chip	Radio Standard	Year	Bitrate (bps)	Tx Power (dBm)	Power Draw (mW)	EPB (nJ/bit)
UBI206 [110]	WiFi	2022	6M	-	20	3.3
UBI206	WiFi	2022	72.2M	-	20	0.3
DA16200 [111]	WiFi	2019	1M	9.5	280.5	280.5
DA16200	WiFi	2019	6M	8	280.5	46.8
DA16200	WiFi	2019	54M	2	231	4.3
ESP32 [112]	WiFi	2016	1M	19.5	792	792
ESP32	WiFi	2016	54M	16	627	11.6
CC3200 [113]	WiFi	2014	1M	18	1000.8	1000.8
CC3200	WiFi	2014	1M	13	615.6	615.6
CC3200	WiFi	2014	6M	18	914.4	152.4
CC3200	WiFi	2014	6M	4	504	84
CC3200	WiFi	2014	54M	14.8	824.4	15.3
CC3200	WiFi	2014	54M	4	504	9.3
CYW43362 [114]	WiFi	2010	11M	18.5	1152	104.7
CYW43362	WiFi	2010	54M	15.5	972	18
CYW43362	WiFi	2010	65M	14.5	936	14.4
CYW43438 [115]	WiFi	2010	1M	20	1152	1152
CYW43438	WiFi	2010	11M	18	1044	94.9
CYW43438	WiFi	2010	54M	15	936	17.3
EFR32FG28	BLE	2023	2M	0	35.82	17.9
Apollo4 [116]	BLE	2020	2M	0	17.16	8.6
BlueNRG-2N [117]	BLE	2020	2M	-2	45.9	23
nRF5340 [118]	BLE	2019	1M	0	12.3	12.3
nRF5340	BLE	2019	2M	0	12.6	6.3
DA14531 [119]	BLE	2019	2M	0	7.59	3.8
DA1469 [120]	BLE	2019	2M	0	9	4.5
CC2652R [121]	BLE	2018	2M	0	21.9	11
QN908x [122]	BLE	2017	2M	0	10.5	5.3
nRF52840 [123]	BLE	2016	1M	0	19.2	19.2
ESP32 [112]	BLE	2016	2M	0	429	214.5
CSR102x [124]	BLE	2016	2M	0	15	7.5
CC2640 [125]	BLE	2015	2M	0	18.3	9.2
nRF52840 [123]	ZigBee	2016	250K	0	19.2	76.8
nRF5340 [126]	ZigBee	2019	250K	0	12.3	49.2
CC2538 [127]	ZigBee	2012	250K	0	72	288
SX1276 [128]	LoRa	2016	4.8K	20	396	82500
SX1276	LoRa	2016	4.8K	7	66	13750
RN2483 [129]	LoRa	2015	10.9K	14	128.37	11777.1
RN2483	LoRa	2015	10.9K	-4	57.09	5237.6
ATA8520E [130]	SigFox	2016	100	14	95.4	954000

Table 1. Power consumption, data rate and energy per bit of commercial radios.

Estimating the power consumption of radios can be challenging when measurements cannot be directly performed on the hardware. Power consumption measurements highly depend on the scenarios, including parameter configurations (data rate, transmission power, and duty cycling) and hardware setups (CPU, memory, peripherals, clock, and power management unit status). The measurement scenarios vary between different chips. Most datasheets report the power consumption when the power management unit is enabled. Some datasheets only list the power consumption with the maximum transmission power. When multiple transmission power levels or data rates are available, several combinations are listed for a comprehensive range of power efficiency calculations.

Backscatter System	Year	Bitrate (bps)	Implementation	Power Draw (μW)	EPB (nJ/bit)
Judo*	2022	100K	PCB prototype- RF analog components	48.00	0.48
SyncScatter [10]	2021	500K	IC prototype 65nm	30.00	0.06
TunnelScatter [48]	2019	2.9K	PCB prototype- RF analog components	57.00	19.66
PLoRa [13]	2018	6.25K	Simulation FPGA	220.00	35.20
LoRa Backscatter [12]	2017	37.5K	Simulation IC 65nm	9.25	0.25
LoRea [11]	2017	3K	PCB prototype	70.00	23.33
LoRea [11]	2017	197K	PCB prototype	650.00	3.30
FS Backscatter [66]	2016	0.63K	Simulation HSPICE	45.00	71.43
HitchHike [15]	2016	300K	Simulation IC 45nm	33.00	0.11
Passive Wi-Fi [9]	2016	11M	Simulation IC 65nm	59.20	0.0054
Passive Wi-Fi [9]	2016	1M	Simulation IC 65nm	14.50	0.0145
Interscatter [14]	2016	1M	Simulation IC 65nm	28.00	0.0025
BackFi [65]	2015	5M	Simulation - modeling	38.70	0.0077
BackFi [65]	2015	1M	Simulation - modeling	2.70	0.0027
Wi-Fi Backscatter [64]	2014	20K	PCB prototype- RF analog components	0.65	0.0325
Ambient Backscatter [63]	2013	10K	PCB prototype- RF analog components	0.25	0.0250

Table 2. Power consumption, data rate and energy per bit of backscatter radios. When multiple data rates are available and the power estimation setup is not clearly stated, the maximum data rate is considered for energy per bit calculation. The power consumption reported in different works depends on the implementation. * represents the work covered in this dissertation.

Backscatter System	Environment	d_1 (m)	E power (dBm)	d_2 (m)	Bitrate (bps)	Frequency band
Judo*	Indoor (LoS)	60	3	60	3K	868MHz
Judo*	Indoor (LoS)	30	3	30	100K	868MHz
Judo*	Outdoor	150	25	105	100K	868MHz
SyncScatter [10]	Indoor (LoS)	5	30	33	500K	2.4GHz
TunnelScatter [48]	Indoor (NLoS)	30	16	18	3K	868MHz
PLoRa [13]	Outdoor	1	21	800	97	900MHz
LoRa Backscatter [12]	Outdoor	5	30	2800	10K	915MHz
LoRa Backscatter	Outdoor	238	30	238	10K	915MHz
LoRea [11]	Outdoor	1	28	3400	3K	868MHz
LoRea	Outdoor	1	26	225	3K	2.4GHz
LoRea	Outdoor	1	26	100	197K	2.4GHz
HitchHike [15]	Indoor (LoS)	1	30	54	300K	2.4GHz
HitchHike	Indoor (NLoS)	1	30	34	300K	2.4GHz
Passive Wi-Fi [9]	Indoor (LoS)	2	30	31	11M	2.4GHz

Table 3. Communication range of backscatter radios. The communication range of a backscatter tag is determined by the product of emitter-tag distance d_1 and tag-receiver distance d_2 . * represents the work covered in this dissertation.

References

- [1] Vikram Iyer, Hans Gaensbauer, Thomas L Daniel, and Shyamnath Gollakota. Wind dispersal of battery-free wireless devices. *Nature*, pages 427–433, 2022.
- [2] Mohamed R Abdelhamid, Ruicong Chen, Joonhyuk Cho, Anantha P Chandrakasan, and Fadel Adib. Self-reconfigurable micro-implants for cross-tissue wireless and batteryless connectivity. In *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking (MobiCom'20)*, pages 1–14, 2020.
- [3] Simon Haykin. *Communication systems*. John Wiley & Sons, 2008.
- [4] John G Proakis and Masoud Salehi. *Fundamentals of communication systems*. Pearson Education India, 2007.
- [5] Vamsi Talla, Joshua R Smith, and Shyamnath Gollakota. Advances and open problems in backscatter networking. *GetMobile: Mobile Computing and Communications*, pages 32–38, 2021.
- [6] Yuan Ding, Romwald Lihakanga, Ricardo Correia, George Goussetis, and Nuno Borges Carvalho. Harmonic suppression in frequency shifted backscatter communications. *IEEE Open Journal of the Communications Society*, pages 990–999, 2020.
- [7] Anu Jagannath, Jithin Jagannath, and Prem Sagar Pattanshetty Vasanth Kumar. A comprehensive survey on radio frequency (RF) fingerprinting: traditional approaches, deep learning, and open challenges. *Computer Networks*, page 109455, 2022.
- [8] Carlos Pérez-Penichet, Frederik Hermans, Ambuj Varshney, and Thiemo Voigt. Augmenting IoT networks with backscatter-enabled passive sensor tags. In *Proceedings of the 3rd Workshop on Hot Topics in Wireless (HotWireless'16)*, HotWireless '16, NY, USA, 2016. ACM.
- [9] Bryce Kellogg, Vamsi Talla, Shyamnath Gollakota, and Joshua R Smith. Passive Wi-Fi: Bringing low power to Wi-Fi transmissions. In *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI'16)*, pages 151–164, 2016.
- [10] Manideep Dunna, Miao Meng, Po-Han Wang, Chi Zhang, Patrick Mercier, and Dinesh Bharadia. SyncScatter: Enabling WiFi like synchronization and range for WiFi backscatter communication. In *18th USENIX Symposium on Networked Systems Design and Implementation (NSDI'21)*, pages 923–937, 2021.
- [11] Ambuj Varshney, Oliver Harms, Carlos Pérez-Penichet, Christian Rohner, Frederik Hermans, and Thiemo Voigt. LoRea: A backscatter architecture that achieves a long communication range. In *Proceedings of the 15th ACM Conference on Embedded Network Sensor Systems (SenSys'17)*, pages 1–14, 2017.

- [12] Vamsi Talla, Mehrdad Hessar, Bryce Kellogg, Ali Najafi, Joshua R. Smith, and Shyamnath Gollakota. LoRa Backscatter: Enabling the vision of ubiquitous connectivity. *Proceedings of the ACM on interactive, mobile, wearable and ubiquitous technologies (IMWUT'17)*, pages 105:1–105:24, 2017.
- [13] Yao Peng, Longfei Shangguan, Yue Hu, Yujie Qian, Xianshang Lin, Xiaojiang Chen, Dingyi Fang, and Kyle Jamieson. PLoRa: A passive long-range data network from ambient lora transmissions. In *Proceedings of the 2018 Conference of the ACM Special Interest Group on Data Communication (SIGCOMM'18)*, pages 147–160, 2018.
- [14] Vikram Iyer, Vamsi Talla, Bryce Kellogg, Shyamnath Gollakota, and Joshua Smith. Inter-Technology Backscatter: Towards internet connectivity for implanted devices. In *Proceedings of the 2016 ACM annual conference of the Special Interest Group on Data Communication (SIGCOMM'16)*, pages 356–369, 2016.
- [15] Pengyu Zhang, Dinesh Bharadia, Kiran Joshi, and Sachin Katti. Hitchhike: Practical backscatter using commodity wifi. In *Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems (SenSys'16)*, pages 259–271, 2016.
- [16] John Kimionis and Manos M Tentzeris. Pulse Shaping: The missing piece of backscatter radio and RFID. *IEEE Transactions on Microwave Theory and Techniques*, pages 4774–4788, 2016.
- [17] Maolin Zhang, Si Chen, Jia Zhao, and Wei Gong. Commodity-level BLE backscatter. In *Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys'21)*, pages 402–414.
- [18] Wenhao Wang, Zhi Sun, Sixu Piao, Bocheng Zhu, and Kui Ren. Wireless physical-layer identification: Modeling and validation. *IEEE Transactions on Information Forensics and Security*, pages 2091–2106, 2016.
- [19] Kevin Merchant, Shauna Revay, George Stantchev, and Bryan Nossain. Deep learning for RF device fingerprinting in cognitive communication networks. *IEEE Journal of Selected Topics in Signal Processing*, pages 160–167, 2018.
- [20] Amani Al-Shawabka, Francesco Restuccia, Salvatore D'Oro, Tong Jian, Bruno Costa Rendon, Nasim Soltani, Jennifer Dy, Stratis Ioannidis, Kaushik Chowdhury, and Tommaso Melodia. Exposing the Fingerprint: Dissecting the impact of the wireless channel on radio fingerprinting. In *IEEE Conference on Computer Communications (INFOCOM'20)*, pages 646–655, 2020.
- [21] Nasim Soltani, Kunal Sankhe, Jennifer Dy, Stratis Ioannidis, and Kaushik Chowdhury. More is Better: Data augmentation for channel-resilient RF fingerprinting. *IEEE Communications Magazine*, pages 66–72, 2020.
- [22] Vladimir Brik, Suman Banerjee, Marco Gruteser, and Sangho Oh. Wireless device identification with radiometric signatures. In *Proceedings of the 14th ACM international conference on Mobile computing and networking (MobiCom'08)*, pages 116–127, 2008.
- [23] Boris Danev and Srdjan Capkun. Transient-based identification of wireless sensor nodes. In *International Conference on Information Processing in Sensor Networks (IPSN'09)*, pages 25–36, 2009.
- [24] Qingrui Pan, Zhenlin An, Xueyuan Yang, Xiaopeng Zhao, and Lei Yang. RF-DNA: Large-scale physical-layer identifications of RFIDs via dual natural

- attributes. In *Proceedings of the 28th Annual International Conference on Mobile Computing And Networking (MobiCom'22)*, pages 419–431, 2022.
- [25] Tianhang Zheng, Zhi Sun, and Kui Ren. FID: Function modeling-based data-independent and channel-robust physical-layer identification. In *IEEE Conference on Computer Communications (INFOCOM'19)*, pages 199–207, 2019.
- [26] Kunal Sankhe, Mauro Belgiovine, Fan Zhou, Shamnaz Riyaz, Stratis Ioannidis, and Kaushik Chowdhury. ORACLE: Optimized radio classification through convolutional neural networks. In *IEEE Conference on Computer Communications (INFOCOM'19)*, pages 370–378, 2019.
- [27] Action Nechibvute, Albert Chawanda, and Pearson Luhanga. Piezoelectric energy harvesting devices: An alternative energy source for wireless sensors. *Smart Materials Research*, 2012.
- [28] Joshua Adkins. *Resource-Constrained Sensing as a Shared Utility*. PhD thesis, University of California, Berkeley, 2023.
- [29] Tony J Roupheal. *Wireless Receiver Architectures and Design: Antennas, RF, synthesizers, mixed signal, and digital signal processing*. Academic Press, 2014.
- [30] Stewart J Thomas, Eric Wheeler, Jochen Teizer, and Matthew S Reynolds. Quadrature amplitude modulated backscatter in passive and semipassive UHF RFID systems. *IEEE Transactions on Microwave Theory and Techniques*, 2012.
- [31] Jordan Besnoff, Morteza Abbasi, and David S Ricketts. High data-rate communication in near-field RFID and wireless power using higher order modulation. *IEEE Transactions on Microwave Theory and Techniques*, 2016.
- [32] Ricardo Correia, Alirio Boaventura, and Nuno Borges Carvalho. Quadrature amplitude backscatter modulator for passive wireless sensors in IoT applications. *IEEE Transactions on Microwave Theory and Techniques*, 2017.
- [33] Chenren Xu, Lei Yang, and Pengyu Zhang. Practical backscatter communication systems for battery-free internet of things: A tutorial and survey of recent research. *IEEE Signal Processing Magazine*, 2018.
- [34] Gang Yang, Ying-Chang Liang, Rui Zhang, and Yiyang Pei. Modulation in the air: Backscatter communication over ambient OFDM carrier. *IEEE Transactions on Communications*, 2017.
- [35] Leo Esaki, Yasuhiko Arakawa, and Masatoshi Kitamura. Esaki diode is still a radio star, half a century on. *Nature*, pages 31–31, 2010.
- [36] RCA Corporation. Semiconductor and Materials Division. *RCA Tunnel Diode Manual*. RCA technical manual. RCA, 1963.
- [37] General Electric. Tunnel Diode 1N3712.
- [38] Lydi Smaini. *RF analog impairments modeling for communication systems simulation: application to OFDM-based transceivers*. John Wiley & Sons, 2012.
- [39] Kevin McClaning. *Wireless receiver design for digital communications*. IET, 2012.
- [40] Kenneth I Talbot, Paul R Duley, and Martin H Hyatt. Specific emitter identification and verification. *Technology Review*, 113, 2003.
- [41] Zhuo Fei, Yuanling Huang, and Chen Jian. Radio frequency fingerprint

- extraction of radio emitter based on I/Q imbalance. *Procedia computer science*, pages 472–477, 2017.
- [42] Yingjun Yuan, Zhitao Huang, Hao Wu, and Xiang Wang. Specific emitter identification based on hilbert–huang transform-based time–frequency–energy distribution features. *IET communications*, pages 2404–2412, 2014.
- [43] Crystal Bertocini, Kevin Rudd, Bryan Nousain, and Mark Hinders. Wavelet fingerprinting of radio-frequency identification (RFID) tags. *IEEE Transactions on Industrial Electronics*, 2011.
- [44] Guangquan Huang, Yingjun Yuan, Xiang Wang, and Zhitao Huang. Specific emitter identification based on nonlinear dynamical characteristics. *Canadian Journal of Electrical and Computer Engineering*, pages 34–41, 2016.
- [45] Francesco Restuccia, Salvatore D’Oro, Amani Al-Shawabka, Mauro Belgiovine, Luca Angioloni, Stratis Ioannidis, Kaushik Chowdhury, and Tommaso Melodia. DeepRadioID: Real-time channel-resilient optimization of deep learning-based radio fingerprinting algorithms. In *Proceedings of the Twentieth ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc’19)*, pages 51–60, 2019.
- [46] Christopher M Bishop and Nasser M Nasrabadi. *Pattern recognition and machine learning*. Springer, 2006.
- [47] Andrea Goldsmith. *Wireless communications*. Cambridge university press.
- [48] Ambuj Varshney, Andreas Soleiman, and Thiemo Voigt. Tunnelscatter: Low power communication for sensor tags using tunnel diodes. In *The 25th Annual International Conference on Mobile Computing and Networking (MobiCom ’19)*, pages 1–17. ACM, 2019.
- [49] Ambuj Varshney and Lorenzo Corneo. Tunnel emitter: Tunnel diode based low-power carrier emitters for backscatter tags. In *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking (MobiCom ’20)*. ACM, 2020.
- [50] Ander Galisteo, Diego Juara, and Domenico Giustiniano. Research in visible light communication systems with OpenVLC1.3. In *Proceedings of the 2019 IEEE 5th World Forum on Internet of Things, WF-IoT*, 2019.
- [51] Bluetooth Core Specification 5.4. <https://www.bluetooth.com/specifications/specs/core-specification-5-4/>.
- [52] IEEE. IEEE standard for information technology– local and metropolitan area networks– specific requirements– part 15.4: Wireless medium access control (MAC) and physical layer (PHY) specifications for low rate wireless personal area networks (WPANs). *IEEE Std 802.15.4-2006 (Revision of IEEE Std 802.15.4-2003)*, pages 1–320, 2006.
- [53] TS001-1.0.4 LoRaWAN L2 1.0.4 Specification. <https://resources.lora-alliance.org/technical-specifications/ts001-1-0-4-lorawan-12-1-0-4-specification>.
- [54] Sigfox Device Radio Specifications. <https://build.sigfox.com/sigfox-device-radio-specifications#the-full-specification>.
- [55] NXP NTAG SmartSensor. <https://www.nxp.com/products/wireless-connectivity/nfc-hf/ntag-smartsensor:NTAG-SMART-SENSOR>, 2023.
- [56] Smartrac RFID Sensor Tags. <https://rfid.averydennison.com/en/>

- home/products-solutions/rfid-sensor-tags.html, 2023.
- [57] RadioForce Active M2M / IoT / RFID Sensors. <https://www.radioforce.net/en/products/technologies/sensoring-active/sensors>, 2023.
- [58] Wireless Identification and Sensing Platform (WISP). <https://sites.google.com/uw.edu/wisp-wiki/home>, 2023.
- [59] Hong Zhang, Jeremy Gummesson, Benjamin Ransford, and Kevin Fu. Moo: A batteryless computational RFID and sensing platform. *University of Massachusetts Computer Science Technical Report UM-CS-2011-020*, 2011.
- [60] Saman Naderiparizi, Aaron N Parks, Zerina Kapetanovic, Benjamin Ransford, and Joshua R Smith. WISPCam: A battery-free RFID camera. In *2015 IEEE International Conference on RFID (RFID'15)*, pages 166–173, 2015.
- [61] Vamsi Talla and Joshua R Smith. Hybrid analog-digital backscatter: A new approach for battery-free sensing. In *2013 IEEE International Conference on RFID (RFID'13)*, pages 74–81, 2013.
- [62] Joshua F Ensworth and Matthew S Reynolds. Every smart phone is a backscatter reader: Modulated backscatter compatibility with bluetooth 4.0 low energy (BLE) devices. In *2015 IEEE international conference on RFID (RFID'15)*, pages 78–85, 2015.
- [63] Vincent Liu, Aaron Parks, Vamsi Talla, Shyamnath Gollakota, David Wetherall, and Joshua R Smith. Ambient backscatter: Wireless communication out of thin air. *Proceedings of the 2012 Conference of the ACM Special Interest Group on Data Communication (SIGCOMM'13)*, pages 39–50, 2013.
- [64] Bryce Kellogg, Aaron Parks, Shyamnath Gollakota, Joshua R Smith, and David Wetherall. Wi-fi Backscatter: Internet connectivity for rf-powered devices. In *Proceedings of the 2014 Conference of the ACM Special Interest Group on Data Communication (SIGCOMM'14)*, pages 607–618, 2014.
- [65] Dinesh Bharadia, Kiran Raj Joshi, Manikanta Kotaru, and Sachin Katti. BackFi: High throughput wifi backscatter. *Proceedings of the 2018 Conference of the ACM Special Interest Group on Data Communication (SIGCOMM'15)*, pages 283–296, 2015.
- [66] Pengyu Zhang, Mohammad Rostami, Pan Hu, and Deepak Ganesan. Enabling practical backscatter communication for on-body sensors. In *Proceedings of the 2016 Conference of the ACM Special Interest Group on Data Communication (SIGCOMM'16)*, pages 370–383, 2016.
- [67] Francesco Amato, Christopher W Peterson, Muhammad B Akbar, and Gregory D Durgin. Long range and low powered RFID tags with tunnel diode. In *2015 IEEE International Conference on RFID Technology and Applications*, pages 182–187. IEEE, 2015.
- [68] Francesco Amato. *Achieving hundreds-meter ranges in low powered RFID systems with quantum tunneling tags*. PhD thesis, Georgia Institute of Technology, 2017.
- [69] Francesco Amato and Gregory D Durgin. Tunnel diodes for backscattering communications. In *2018 2nd URSI Atlantic Radio Science Meeting*, pages 1–3. IEEE, 2018.
- [70] Francesco Amato, Christopher W Peterson, Brian P Degnan, and Gregory D Durgin. Tunneling RFID tags for long-range and low-power microwave applications. *IEEE Journal of Radio Frequency Identification*, pages 93–103,

- 2018.
- [71] Ajibayo O Adeyeye, Charles Lynch, Aline Eid, Jimmy GD Hester, and Manos M Tentzeris. Energy autonomous two-way repeater system for non-line-of-sight interrogation in next generation wireless sensor networks. *IEEE Transactions on Microwave Theory and Techniques*, pages 1779–1788, 2022.
 - [72] John Kimionis, Apostolos Georgiadis, Ana Collado, and Manos M Tentzeris. Enhancement of RF tag backscatter efficiency with low-power reflection amplifiers. *IEEE Transactions on Microwave Theory and Techniques*, pages 3562–3571, 2014.
 - [73] Huixin Dong, Yirong Xie, Xianan Zhang, Wei Wang, Xinyu Zhang, and Jianhua He. GPSMirror: Expanding accurate GPS positioning to shadowed and indoor regions with backscatter. In *Proceedings of the 29th Annual International Conference on Mobile Computing and Networking (MobiCom’23)*, 2023.
 - [74] Zerina Kapetanovic, Miguel Morales, and Joshua R Smith. Communication by means of modulated johnson noise. *Proceedings of the National Academy of Sciences*, 119(49):e2201337119, 2022.
 - [75] Yong Sheng, Keren Tan, Guanling Chen, David Kotz, and Andrew Campbell. Detecting 802.11 MAC layer spoofing using received signal strength. In *Proceedings of the 27th Conference on Computer Communications (INFOCOM’08)*, 2008.
 - [76] Rongrong Wang, Haiyong Luo, Qu Wang, Zhaohui Li, Fang Zhao, and Jingyu Huang. A spatial–temporal positioning algorithm using residual network and LSTM. *IEEE Transactions on Instrumentation and Measurement*, pages 9251–9261, 2020.
 - [77] Navneet Singh, Sangho Choe, and Rajiv Punmiya. Machine learning based indoor localization using Wi-Fi RSSI fingerprints: An overview. *IEEE Access*, pages 127150–127174, 2021.
 - [78] Xiangyu Wang, Xuyu Wang, and Shiwen Mao. Indoor fingerprinting with bimodal CSI tensors: A deep residual sharing learning approach. *IEEE Internet of Things Journal*, pages 4498–4513, 2020.
 - [79] Liang Xiao, Larry J Greenstein, Narayan B Mandayam, and Wade Trappe. Using the physical layer for wireless authentication in time-variant channels. *IEEE Transactions on Wireless Communications*, 2008.
 - [80] Neal Patwari and Sneha K Kasera. Robust location distinction using temporal link signatures. In *Proceedings of the 13th annual ACM international conference on Mobile computing and networking (MobiCom’07)*, 2007.
 - [81] DL Margerum. Pinpointing location of hostile radars (amplitude scanning, multiple beam and dual baseline phase comparison direction finding receivers for installation in aircraft to locate and analyze radar signatures). *Microwaves*, 8:60–64, 1969.
 - [82] Howard C Choe, Clark E Poole, M Yu Andrea, and Harold H Szu. Novel identification of intercepted signals from unknown radio transmitters. In *Wavelet Applications II*, volume 2491, pages 504–517. SPIE, 1995.
 - [83] J Toonstra and Wintold Kinsner. Transient analysis and genetic algorithms for classification. In *IEEE WESCANEX 95. Communications, Power, and*

- Computing. Conference Proceedings*, volume 2, pages 432–437. IEEE, 1995.
- [84] J Toonstra and W Kinsner. A radio transmitter fingerprinting system odo-1. In *Proceedings of 1996 Canadian Conference on Electrical and Computer Engineering*, volume 1, pages 60–63. IEEE, 1996.
- [85] Oktay Ureten and Nur Serinken. Wireless security through RF fingerprinting. *Canadian Journal of Electrical and Computer Engineering*, 32(1):27–33, 2007.
- [86] Jeyanthi Hall, Michel Barbeau, Evangelos Kranakis, et al. Detection of transient in radio frequency fingerprinting using signal phase. *Wireless and optical communications*, 9:13, 2003.
- [87] Adam C Polak, Sepideh Dolatshahi, and Dennis L Goeckel. Identifying wireless users via transmitter imperfections. *IEEE Journal on selected areas in communications*, pages 1469–1479, 2011.
- [88] Yu Jiang, Linning Peng, Aiqun Hu, Sheng Wang, Yi Huang, and Lu Zhang. Physical layer identification of LoRa devices using constellation trace figure. *EURASIP Journal on Wireless Communications and Networking*, 2019:1–11, 2019.
- [89] Linning Peng et al. Deep learning based RF fingerprint identification using differential constellation trace figure. *IEEE Transactions on Vehicular Technology*, pages 1091–1095, 2019.
- [90] Xinyu Zhou et al. A robust radio-frequency fingerprint extraction scheme for practical device recognition. *IEEE Internet of Things Journal*, pages 11276–11289, 2021.
- [91] Hadi Givehchian, Nishant Bhaskar, Eliana Rodriguez Herrera, Héctor Rodrigo López Soto, Christian Dameff, Dinesh Bharadia, and Aaron Schulman. Evaluating physical-layer BLE location tracking attacks on mobile devices. In *2022 IEEE Symposium on Security and Privacy (SP'22)*, pages 1690–1704. IEEE, 2022.
- [92] Ning Chen, Aiqun Hu, and Hua Fu. LoRa radio frequency fingerprint identification based on frequency offset characteristics and optimized LoRaWAN access technology. In *IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, 2021.
- [93] Boris Danev, Thomas S Heydt-Benjamin, and Srdjan Capkun. Physical-layer identification of RFID devices. In *USENIX security symposium*, pages 199–214, 2009.
- [94] Yuanling Huang and Hui Zheng. Radio frequency fingerprinting based on the constellation errors. In *2012 18th Asia-Pacific Conference on Communications (APCC)*, pages 900–905. IEEE, 2012.
- [95] Davide Zanetti, Boris Danev, and Srdjan Capkun. Physical-layer identification of UHF RFID tags. In *Proceedings of the 16th annual international conference on Mobile computing and networking (MobiCom'10)*, 2010.
- [96] Jinsong Han, Chen Qian, Panlong Yang, Dan Ma, Zhiping Jiang, Wei Xi, and Jizhong Zhao. GenePrint: Generic and accurate physical-layer identification for UHF RFID tags. *IEEE/ACM Transactions on Networking*, 2015.
- [97] Jiawei Li, Ang Li, Dianqi Han, Yan Zhang, Tao Li, and Yanchao Zhang. RCID: Fingerprinting passive RFID tags via wideband backscatter. In *Proceedings of IEEE Conference on Computer Communications*

- (INFOCOM'22), 2022.
- [98] Ge Wang, Haofan Cai, Chen Qian, Jinsong Han, Shouqian Shi, Xin Li, Han Ding, Wei Xi, and Jizhong Zhao. Hu-fu: Replay-resilient RFID authentication. *IEEE/ACM Transactions on Networking*, 2020.
- [99] Xingyu Chen, Jia Liu, Xia Wang, Haisong Liu, Dong Jiang, and Lijun Chen. Fingerprint: Robust energy-related fingerprinting for passive RFID tags. In *Proceedings of the 17th USENIX Symposium on Networked Systems Design and Implementation (NSDI'20)*, 2020.
- [100] Revathy Narayanan, Ambuj Varshney, and Panos Papadimitratos. Harvestprint: Securing battery-free backscatter tags through fingerprinting. In *Proceedings of the 20th ACM Workshop on Hot Topics in Networks (HotNets'21)*, 2021.
- [101] Guyue Li, Jiabao Yu, Yuexiu Xing, and Aiqun Hu. Location-invariant physical layer identification approach for WiFi devices. *IEEE Access*, pages 106974–106986, 2019.
- [102] Pengfei Liu, Panlong Yang, Wen-Zhan Song, Yubo Yan, and Xiang-Yang Li. Real-time identification of rogue WiFi connections using environment-independent physical features. In *IEEE Conference on Computer Communications (INFOCOM'19)*, pages 190–198. IEEE, 2019.
- [103] Nora Basha, Bechir Hamdaoui, Kathiravetpillai Sivanesan, and Mohsen Guizani. Channel-resilient deep-learning-driven device fingerprinting through multiple data streams. *IEEE Open Journal of the Communications Society*, pages 118–133, 2023.
- [104] Seth Andrews, Ryan M Gerdes, and Ming Li. Towards physical layer identification of cognitive radio devices. In *2017 IEEE Conference on Communications and Network Security (CNS)*, pages 1–9, 2017.
- [105] Linning Peng, Aiqun Hu, Junqing Zhang, Yu Jiang, Jiabao Yu, and Yan Yan. Design of a hybrid RF fingerprint extraction and device classification scheme. *IEEE internet of things journal*, pages 349–360, 2018.
- [106] Jiabao Yu, Aiqun Hu, Guyue Li, and Linning Peng. A robust RF fingerprinting approach using multisampling convolutional neural network. *IEEE Internet of Things Journal*, pages 6786–6799, 2019.
- [107] Xingda Chen, Deepak Ganesan, Jeremy Gummeson, and Mohammad Rostami. COCOON: A conductive substrate-based coupled oscillator network for wireless communication. In *Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems (SenSys '21)*, pages 84–96, 2021.
- [108] Saptarshi Hazra, Thiemo Voigt, and Wenqing Yan. PLIO: Physical layer identification using one-shot learning. In *2021 IEEE 18th International Conference on Mobile Ad Hoc and Smart Systems*, 2021.
- [109] Hadi Givehchian, Nishant Bhaskar, Alexander Redding, Han Zhao, Aaron Schulman, and Dinesh Bharadia. Practical obfuscation of BLE physical-layer fingerprints on mobile devices. In *2024 IEEE Symposium on Security and Privacy (SP'24)*, pages 73–73. IEEE Computer Society, 2023.
- [110] UBI206 Specifications. <https://www.ubilite.com/product/>.
- [111] DA16200 Ultra-Low Power Wi-Fi SoC for Battery-Powered IoT Devices. <https://www.renesas.com/us/en/products/wireless-connectivity/wi-fi/low-power-wi-fi/da16200-ultra-low-power-wi-fi-soc-battery-powered-iot-devices>.

- [112] ESP32 Series Datasheet. https://www.espressif.com/sites/default/files/documentation/esp32_datasheet_en.pdf.
- [113] CC3200 SimpleLink 32-bit Arm Cortex-M4 Wi-Fi wireless MCU with 2 TLS/SSL and 256kB RAM. <https://www.ti.com/product/CC3200>.
- [114] CYW44362 Single-Chip IEEE 802.11 b/g/n MAC/Baseband/Radio + SDIO. <https://www.digikey.sg/htmldatasheets/production/1955350/0/0/1/cyw43362.html>.
- [115] CYW43438 Single-Chip IEEE 802.11 b/g/n MAC/Baseband/Radio + SDIO. <https://www.digikey.se/en/htmldatasheets/production/1955353/0/0/1/cyw43438>.
- [116] Apollo4. <https://ambiq.com/apollo4/>.
- [117] BlueNRG-2N, Bluetooth LE 5.2 Wireless Network Coprocessor. <https://www.st.com/en/wireless-connectivity/bluenrg-2n.html>.
- [118] Nordic Semiconduct. nrf52833 product specification. https://infocenter.nordicsemi.com/pdf/nRF52833_PS_v1.5.pdf, 2023. [Online; accessed 25-May-2023].
- [119] DA14531, Ultra Low Power Bluetooth 5.1 SoC. <https://www.renesas.com/us/en/document/dst/da14531-datasheet>.
- [120] DA1469x, Multi-Core Bluetooth 5.2 SoC Family with System PMU. <https://www.renesas.com/us/en/document/dst/da1469x-datasheet>.
- [121] CC2652R, SimpleLink 32-bit Arm Cortex-M4F multiprotocol 2.4 GHz wireless MCU with 352kB Flash. <https://www.ti.com/product/CC2652R>.
- [122] QN908x, Ultra low power Bluetooth 5 system-on-chip solution. <https://www.nxp.com/docs/en/nxp/data-sheets/QN908x.pdf>.
- [123] nRF52840, Multiprotocol Bluetooth 5.4 SoC supporting Bluetooth Low Energy, Bluetooth mesh, NFC, Thread and Zigbee. <https://www.nordicsemi.com/products/nrf52840>.
- [124] CSR102x, Qualcomm CSR102x Bluetooth Low Energy Product Family. <https://www.qualcomm.com/products/technology/bluetooth/csr102x#Documentation>.
- [125] CC2640, SimpleLink 32-bit Arm Cortex-M3 Bluetooth® Low Energy wireless MCU with 128kB Flash. <https://www.ti.com/product/CC2640>.
- [126] nRF5340, Dual-core Bluetooth 5.4 SoC supporting Bluetooth LE, Bluetooth mesh, NFC, Thread and Zigbee. <https://www.nordicsemi.com/products/nrf5340>.
- [127] CC2538, 32-bit Arm Cortex-M3 Zigbee, 6LoWPAN, and IEEE 802.15.4 wireless MCU with 512kB Flash and 32kB RAM. <https://www.ti.com/product/CC2538>.
- [128] SX1276/77/78/79, 137 MHz to 1020 MHz Low Power Long Range Transceiver. <https://www.mouser.com/datasheet/2/761/sx1276-1278113.pdf>.
- [129] RN2483, Low-Power LoRa Technology Transceiver Module. <https://www.microchip.com/en-us/product/rn2483#document-table>.
- [130] ATA8520E, Single-Chip SIGFOX RF Transceiver. <https://www.microchip.com/en-us/product/ata8520e>.

Acta Universitatis Upsaliensis

Digital Comprehensive Summaries of Uppsala Dissertations from the Faculty of Science and Technology 2341

Editor: The Dean of the Faculty of Science and Technology

A doctoral dissertation from the Faculty of Science and Technology, Uppsala University, is usually a summary of a number of papers. A few copies of the complete dissertation are kept at major Swedish research libraries, while the summary alone is distributed internationally through the series Digital Comprehensive Summaries of Uppsala Dissertations from the Faculty of Science and Technology. (Prior to January, 2005, the series was published under the title “Comprehensive Summaries of Uppsala Dissertations from the Faculty of Science and Technology”.)

Distribution: publications.uu.se
urn:nbn:se:uu:diva-515943



ACTA UNIVERSITATIS
UPSALIENSIS
2023