ADVANCING MOBILE INTEROPERABILITY AND SECURITY THROUGH CONTROLLED MAGNETIC FIELDS

DONGHUI DAI

PhD

The Hong Kong Polytechnic University

2025

The Hong Kong Polytechnic University

Department of Computing

Advancing Mobile Interoperability and Security Through Controlled Magnetic Fields

Donghui Dai

A thesis submitted in partial fulfillment of the requirements for
the degree of Doctor of Philosophy
January 2025

CERTIFICATE OF ORIGINALITY

I hereby declare that this thesis is my own work and that, to the best of my knowledge and belief, it reproduces no material previously published or written, nor material that has been accepted for the award of any other degree or diploma, except where due acknowledgment has been made in the text.

Signature: ____________________

Name of Student: Donghui Dai

Abstract

As integrated circuit technology continues to advance, the capabilities of mobile devices expand correspondingly, bringing increased security challenges and a greater need for innovative applications. Magnetic inductive coupling, which enables energy transfer between circuits via a controlled magnetic field, has emerged as a key technology, enhancing the versatility and functionality of mobile systems. However, current research primarily focuses on optimizing applications such as wireless charging and near-field communication, as exemplified by protocols like Qi and NFC respectively. There is limited investigation into the security threats posed by magnetic inductive coupling. Additionally, the application of magnetic inductive coupling is constrained, with few efforts made to extend its use to new scenarios or higher frequency bands. Consequently, the potential of magnetic inductive coupling in mobile computing has not been fully tapped, which has restricted its widespread adoption and practical deployment across various mobile platforms. To bridge these gaps, our work includes assessing security threats and unveiling a range of interoperable applications through controllable magnetic inductive coupling fields, extending from low frequency to ultra-high frequency range.

First, we analyze a physical side-channel attack strategy enabled by controlled magnetic inductive coupling in the Low Frequency (LF) band. Specifically, a novel type of inaudible voice command attack initiated through controllable magnetic interference from a wireless charger is investigated. We demonstrate that smart device

microphones experience significant magnetic interference during wireless charging, primarily due to inadequate protection against electromagnetic interference at frequencies around 100kHz or below. Exploiting this vulnerability, we developed two types of inaudible voice attacks designed to inject malicious voice commands into devices while they are being wirelessly charged. These attacks use either compromised wireless chargers or attached accessory devices to manipulate the magnetic leakage and deliver the commands. Extensive experiments were conducted across various devices and voice assistants. The evaluations confirm the effectiveness of these attacks in typical commercial charging settings, and appropriate countermeasures have been suggested to mitigate the threats.

Second, we introduce a novel physical side-channel communication scheme enabled by controlled magnetic inductive coupling in the High Frequency (HF) band. This system, called MagCode, enhances mobile payment security by utilizing controllable benign magnetic interference from an NFC reader. This interference produces barcode-like stripes on images captured by a smartphone's CMOS sensor positioned near the NFC reader. This method enables simplex communication between an NFC reader and smartphones that either lack NFC capabilities or have them disabled, by precisely modulating the magnetic-induced stripes with information bits. We design and implement a stack of protocols from the physical to the transport layer and test the proof-of-concept prototype across multiple smart devices to guarantee robust performance. The evaluation results indicate that data throughput is satisfactory, achieving speeds up to 2.58 kbps, with transactions typically completed within 1.8 seconds.

Third, we investigate an effective RFID inventory mechanism enabled by controlled magnetic inductive coupling at the Ultra-High Frequency (UHF) band. The system, named RFID+, employs spatially controllable magnetic inductive coupling to enhance the distance and precision of near-field RFID inventory within logistical networks. RFID+ optimizes energy harvesting from tailored magnetic fields through the matching loops of standard UHF RFID tags, achieving spatial accuracy akin to HF

NFC systems and significantly lowering miss-reading and cross-reading rates. Key innovations include a specialized multi-turn, capacitor-segmented coil antenna and a rapid inventory algorithm that combines traditional radiative coupling with magnetic coupling to enhance the overall performance and efficiency of RFID inventory systems. Pilot studies in real-world warehouse and logistics settings demonstrate that RFID+ substantially reduces the misreading rate from 22.9% to a remarkable 1.06%, while effectively eliminating cross-reading issues.

In conclusion, this thesis explores the dual aspects of controlled magnetic fields in mobile intelligence, addressing both its potential threats and opportunities. Specifically, it delves into and mitigates vulnerabilities to inaudible voice injection attacks resulting from controlled magnetic interference in the LF band. Concurrently, it explores two innovative mobile applications, including a novel contactless payment system powered by controlled HF band magnetic coupling interference and a highly accurate RFID near-field inventory system utilizing spatially controllable magnetic fields in the UHF band.

Publications Arising from the Thesis

Regular Articles

1. Donghui Dai, Zhenlin An, Zheng Gong, Qingrui Pan, Lei Yang, “RFID+: Spatially Controllable Identification of UHF RFIDs via Controlled Magnetic Fields,” in *Proc. of USENIX NSDI*, 2024.

2. Donghui Dai, Zhenlin An, Qingrui Pan, Lei Yang, “MagCode: NFC-Enabled Barcodes for NFC-Disabled Smartphones,” in *Proc. of ACM MobiCom*, 2023.

3. Donghui Dai, Zhenlin An, Lei Yang, “Inducing Wireless Chargers to Voice Out for Inaudible Command Attacks,” in *Proc. of IEEE S&P*, 2023.

4. Donghui Dai, Zhenlin An, Qingrui Pan, Lei Yang, “Harnessing NFC to Generate Standard Optical Barcodes for NFC-Missing Smartphones,” *IEEE Transactions on Mobile Computing*, 2024.

5. Zhimin Mei, Donghui Dai, Jingyu Tong, Zheng Gong, Lei Yang, “Repurposing Optical Mice for Acoustic Eavesdropping,” in *Proc. of IEEE INFOCOM*, 2025.

6. Yuanhao Feng, Donghui Dai, Xiaopeng Zhao, Jingyu Tong, Zheng Gong, Lei Yang, “Deciphering Micro-Scale, Sub-Hertz Mechanical Vibrations in Industry 4.0: A Battery-Free Sensing Approach,” in *Proc. of IEEE PerCom*, 2025.

7. Zheng Gong, Zhenlin An, Donghui Dai, Jingyu Tong, Shuijie Long, Lei Yang,

"Enabling Cross-Medium Wireless Networks with Miniature Mechanical Antennas," in *Proc. of ACM MobiCom*, 2024.

8. Shen Wang, Xiaopeng Zhao, Donghui Dai, Lei Yang, "Mirror Never Lies: Unveiling Reflective Privacy Risks in Glass-laden Short Videos," in *Proc. of ACM MobiCom*, 2024.

Demo Articles

1. Donghui Dai, Zhenlin An, Lei Yang, "Inducing Wireless Chargers to Voice Out," in *Proc. of ACM MobiCom Demo*, 2022. (**Best Demo Award Runner-up**)

2. Zheng Gong, Zhenlin An, Jingyu Tong, Donghui Dai, Lei Yang, "Constructing Smart Buildings with In-concrete Backscatter Networks," in *Proc. of ACM MobiCom Demo*, 2022. (**Best Demo Award Runner-up**)

3. Donghui Dai, Zhenlin An, Qingrui Pan, Lei Yang, "MagCode: Bringing NFC Feature to All Smartphones," in *Proc. of ACM MobiCom Demo*, 2023.

Acknowledgments

It is with immense gratitude and heartfelt appreciation that I acknowledge the invaluable contributions of those who have played a pivotal role in the successful completion of my Ph.D. dissertation. I am deeply thankful to the many individuals whose support, guidance, and diverse contributions have been instrumental in making this journey both possible and meaningful.

First and foremost, I would like to express my heartfelt gratitude to my supervisor, Dr. Lei Yang. His invaluable guidance has been instrumental in shaping my academic knowledge and research capabilities, allowing me to conduct original, systematic, and comprehensive research. His innovative and thought-provoking ideas have offered me profound insights into what it truly means to be a scholar. Under his mentorship, I have cultivated an appreciation for research depth and quality, developed the ability to identify novel research ideas, and refined my skills in academic writing and presentations. His unwavering support and mentorship have not only enabled me to engage in exciting and meaningful research but have also been pivotal in the successful completion of this thesis.

Secondly, I wish to express my profound appreciation to my collaborators and friends who have consistently supported me throughout my Ph.D. journey. I am especially thankful to my co-authors, Dr. Zhenlin An, Dr. Qingrui Pan, Dr. Yuanhao Feng, Mr. Jingyu Tong, Mr. Zheng Gong, Mr. Xiaopeng Zhao, Mr. Zhimin Mei, and Mr. Shen Wang, for their invaluable expertise in various research fields and system design. Their insightful discussions and collaborative efforts have greatly enriched my academic perspective and played a crucial role in the success of my work. Additionally, I am deeply grateful to other members of the research group, including Mr. Sicong Liao, Ms. Xuanzhi Wang, Mr. Lubing Han, Mr. Fengrui Zhang, Mr. Zhicheng Wang, Ms. Zhuhang Li, Mr. Guosheng Wang, and all other friends. Their shared experiences, unwavering support, and lasting friendship have been a constant source of inspiration and motivation. Their contributions and camaraderie have not only made this journey academically fruitful but also immensely fulfilling personally.

Finally, I would like to express my heartfelt gratitude to my beloved parents and siblings for their unwavering support, encouragement, and love throughout my graduate school journey. Their steadfast presence has been the foundation of my success, providing me with the resilience and confidence to overcome challenges and excel in my research endeavors. Most importantly, I am deeply grateful to my girlfriend, Ms. Hongyan Pei, for her extraordinary love and support, which has been a constant source of strength and inspiration. My Ph.D. journey has been marked by significant academic achievements, notably achieving a perfect success rate with 4 acceptances out of 4 submissions. This smooth academic progression would not have been achievable without their unwavering belief in my abilities and their invaluable emotional and moral support. Their encouragement has been the driving force behind my relentless pursuit of excellence, and I will always hold their instrumental role in this pivotal chapter of my life close to my heart.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background

The past decade has witnessed a rapid growth of mobile systems across numerous sectors, including audio intelligence, contactless payments, smart retail, and industrial automation. Notably, global smartphone shipments surged to approximately 316.1 million units in the third quarter of 2024 alone [1]. Moreover, portable systems such as handheld RFID readers [2] are increasingly used in manufacturing settings, propelling Industry 4.0 advancements. This extensive proliferation is bolstered by a range of wireless technologies, each engineered to cater to the specific needs of different applications. Among these technologies, magnetic inductive coupling, commonly simplified to magnetic coupling or inductive coupling, plays a crucial role in enhancing both the functionality and efficiency of mobile systems. Rooted in the principles of electromagnetic induction, where a magnetic field generated by an alternating current in one coil induces a voltage in another, this technology has a rich history dating back to Michael Faraday's discovery in 1831. Since then, it has evolved from fundamental scientific concepts to sophisticated applications in modern mobile systems, becoming indispensable for enabling technologies like wireless charging and short-distance wireless data transmission.

Magnetic inductive coupling has become prevalent in modern mobile systems, thanks to its operational principles rooted in near-field interactions that confer several advantages. First, this type of controlled magnetic coupling takes place within the antenna's near-field region, devoid of far-field radiation, which eliminates multipath effects. Consequently, signals coupled in this manner are not prone to multipath interference, greatly improving the system's resistance to external disruptions. Second, the operational range of magnetic inductive coupling is generally confined to short distances, ensuring limited transmission reach (i.e., within the Rayleigh distance). This constraint enhances security by safeguarding data against potential man-in-the-middle eavesdropping [3]. Finally, unlike far-field beamforming, which directs energy in a specific direction, near-field magnetic beamforming expands spatial flexibility in the range domain by utilizing spherical waves to achieve spotlight-like beam focusing. This sophisticated technique precisely concentrates energy at targeted locations [4] instead of directions. Altogether, these attributes significantly boost the physical reliability, security, and capability of mobile systems that incorporate controllable magnetic coupling techniques.

Magnetic inductive coupling has enabled two important applications in modern mobile systems. In the LF band, wireless charging has become a popular feature, utilizing controllable magnetic inductive coupling to transmit power across an air gap to electronic devices for energy replenishment. This technology improves user convenience, reduces overheating risks, and eliminates the reliance on diverse connector standards. In the HF band, near-field communication (NFC) has become increasingly prevalent in smart devices such as smartphones and smartwatches, enhancing transmission security through secure short-range coupling and streamlining user interactions with its convenient "tap-and-go" functionality. Additionally, there have been efforts to combine NFC with wireless charging to enhance user experience [5–7]. These established applications highlight the critical role of controllable magnetic inductive coupling in today's mobile systems.

1.2 Motivation

Although controllable magnetic inductive coupling has seen commercial success in applications like wireless charging and NFC protocols, its comprehensive potential within mobile systems remains largely untapped. Current research has predominantly concentrated on these specific uses, resulting in a narrow scope that overlooks the broader possibilities and capabilities of this technology. Specifically, the limitations of current research can be summarized in the following three key aspects:

Firstly, the application scenario of magnetic inductive coupling in mobile systems remains limited. Most existing work focuses primarily on two limited scenarios: wireless charging and NFC. These efforts largely aim at optimizing charging efficiency [8–12], reducing power consumption [13, 14], or exploring combined functionality for both wireless charging and NFC [7,15,16]. However, these studies have yet to transcend the boundaries of these two specific use cases. More recently, researchers have started to investigate innovative applications such as magnetic sensing [17–19] to detect human activities, and in-body magnetic backscatter [20, 21] for powering and communicating with implanted medical devices. Unfortunately, these emerging technologies are still in the early stages of development and require specialized hardware, making them challenging to directly integrate into existing mobile systems.

Secondly, the operating frequency for magnetic inductive coupling in mobile systems is limited to low ranges. Typically, existing systems function within the LF/HF bands, where the exploration of higher frequency applications is insufficient. This limitation stems from the characteristics of electrically small coil antennas at these lower frequencies, which primarily exhibit a *reactive* near-field region. The *radiative* near-field region in these scenarios is minimal and can often be disregarded. The *reactive* near-field is capable of maintaining a high coupling coefficient and generating a uniform magnetic field essential for effective inductive coupling. However, as the frequency increases to the UHF band or beyond, the antennas become electrically large (i.e., their perimeter approaches or exceeds the operating wavelength in free space), resulting in a near-field zone predominantly characterized by the *radiative* region rather than the *reactive* region. Research [22] shows that electrically large coil antennas struggle to produce a uniform magnetic field across their near-field region due to phase inversion along the loop, which can render the magnetic inductive coupling mechanism ineffective. Although recent studies [4, 23–25] have begun exploring magnetic inductive coupling for communication and sensing solutions at higher frequencies (e.g., UHF and even super high-frequency ranges) using advanced techniques like phase compensation [26] and beam focusing, these efforts are still in their early stages, with a primary focus on theoretical and simulation-based research.

Thirdly, the security analysis of magnetic inductive coupling in mobile systems is still limited. Most efforts in mobile systems security aim to eliminate electromagnetic interference from frequencies outside the inductive coupling operating band to enhance physical security. For example, smartphones employ Faraday cages and electromagnetic interference (EMI) filters designed to block or mitigate radio electromagnetic radiation that might disrupt electronic device functionality. These protective measures are primarily focused on interferences from external sources at frequencies above 100 MHz, well beyond the frequencies used for wireless charging and NFC. Some advanced studies [27, 28] have focused on suppressing magnetic interference, but their applications are limited to high-power scenarios, such as electric vehicle charging, which involves transferring energy at kilowatt levels. Despite these efforts, the security risks associated with magnetic leakage during the wireless charging of common mobile devices are still largely unaddressed. Recently, there have been instances of surfing-based attacks [29,30] that exploit magnetic leakage during charging to monitor app activities and user interactions on smartphones. However, these attacks primarily involve passively observing voltage dynamics during the charging process, rather than actively assessing the direct threats to device functionality caused by magnetic leakage.

In conclusion, the current limitations have significantly restricted the widespread and practical deployment of magnetic coupling technologies. Driven by these challenges, our research sets out to achieve three key objectives: (1) to develop more interoperable applications of controllable magnetic inductive coupling, broadening its use beyond traditional contexts; (2) to expand the operating frequency range into higher bands, thereby enhancing the technology's capability; and (3) to conduct an exhaustive analysis of the security risks and develop effective countermeasures for maliciously controlled magnetic coupling attacks in mobile systems. These objectives seek to unlock the full potential of magnetic inductive coupling across a broader spectrum of security and application domains.

1.3 Research Scope and Contribution

In this dissertation, we explore the extensive capabilities of controllable magnetic inductive coupling, aiming to enhance its application across more secure, interoperable, and widespread scenarios along an expanded frequency spectrum. As depicted in Fig. 1.1, the structure of this dissertation is carefully organized into three distinct sections, each focused on different frequency bands. These sections encompass: an analysis of voice assistant security vulnerabilities in the LF band caused by wireless charging; explorations in the HF band utilizing NFC-enabled magnetic leakage for novel contactless payment communication methods; and investigations in the UHF band employing magnetic antennas for spatially controllable inductive coupling, enabling precise near-field identification of RFID tags. These three sections collectively address critical aspects of system security, reliable communication, and magnetic powering, spanning from low-frequency to ultra-high frequency ranges. This

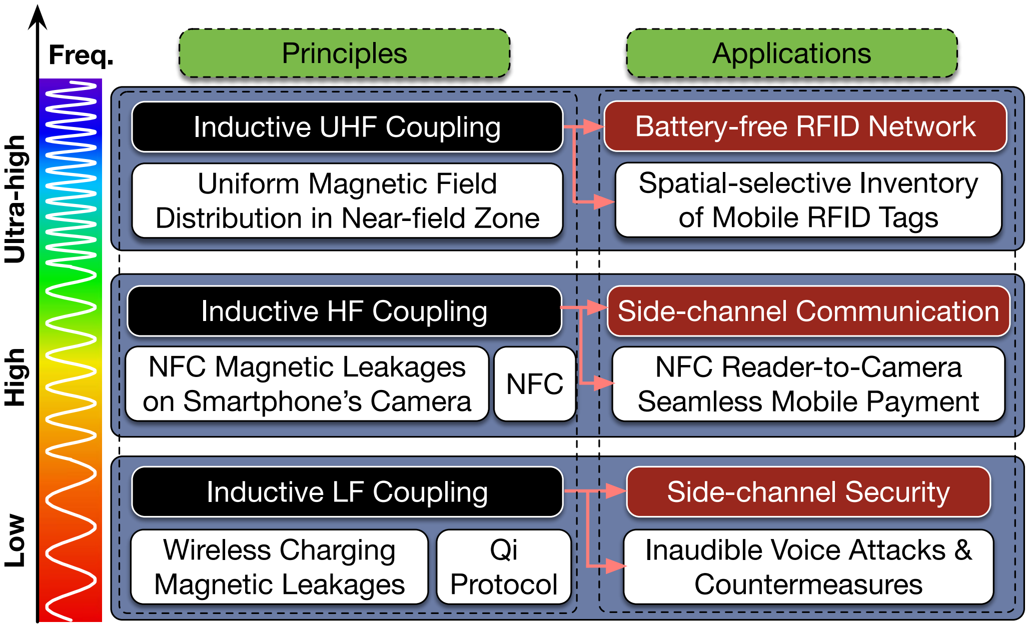

Freq.
Ultra-high
High
Low
Principles
Applications
Inductive UHF Coupling
Uniform Magnetic Field Distribution in Near-field Zone
Battery-free RFID Network
Spatial-selective Inventory of Mobile RFID Tags
Inductive HF Coupling
NFC Magnetic Leakages on Smartphone's Camera
NFC
Side-channel Communication
NFC Reader-to-Camera Seamless Mobile Payment
Inductive LF Coupling
Wireless Charging Magnetic Leakages
Qi Protocol
Side-channel Security
Inaudible Voice Attacks & Countermeasures

Fig. 1.1: Research framework of the dissertation.

comprehensive coverage ensures that the dissertation encapsulates the full scope of mainstream mobile systems and provides a holistic view of how magnetic inductive coupling can be optimized across a wide spectrum of mobile applications. Specifically, the contributions of the dissertation are summarized as follows:

■ Magnetic LF Coupling: Inaudible Voice Attacks and Countermeasures

Recent works demonstrated that speech recognition systems or voice assistants can be manipulated by malicious voice commands, which are injected through various inaudible media, such as ultrasound, laser, and electromagnetic interference (EMI). In this work, we explore a new kind of inaudible voice attack through the magnetic interference induced by a wireless charger operating in the low-frequency range (according to the Qi protocol, ranging from 100 to 205 kHz). Essentially, we show that the microphone components of smart devices suffer from severe magnetic interference when they are enjoying wireless charging, due to the absence of effective protection against the EMI at such low frequencies. By taking advantage of this vulnerability, we design two inaudible voice attacks, HeartwormAttack and ParasiteAttack, both of which aim to inject malicious voice commands into smart devices being wirelessly charged. They make use of a compromised wireless charger or accessory equipment (called parasite) to inject the voice, respectively. We conduct extensive experiments with 17 victim devices (iPhone, Huawei, Samsung, etc.) and 6 types of voice assistants (Siri, Google STT, Bixby, etc.). Evaluation results demonstrate the feasibility of two proposed attacks with commercial charging settings. In summary, our contribution is that we present the first discovery of vulnerabilities in voice systems caused by LF magnetic coupling leakage during wireless charging. Standard industry practices predominantly concentrate on shielding against magnetic interference for frequencies above 100 MHz or focus solely on protecting the motherboard area directly behind the wireless charging receiver coil. Our research reveals that these conventional protective measures are insufficient. Furthermore, we have devised a range of countermeasures, incorporating both software and hardware approaches, to shield against this type of low-frequency magnetic interference. This research seeks to raise awareness of the significant security risks posed to smart device voice systems by maliciously controlled magnetic couplings originating from wireless chargers.

■ **Magnetic HF Coupling: NFC-to-Camera Mobile Payment System**

Mobile payment has achieved explosive growth in recent years due to its contactless feature, which lowers the infection risk of COVID-19. In the market, near-field communication (NFC) and barcodes have become the de facto standard technologies for mobile payment. The NFC-based payment outperforms barcode-based payment in terms of security, usability, and convenience. It is especially more user-friendly for the amblyopia group. Unfortunately, NFC functionality is unavailable in nearly half of smartphones in the market nowadays due to the shortage of NFC modules or being disabled for security reasons. In this work, we present MagCode [31], a cross-technology communication between an NFC reader and a camera, which allows customers to enjoy the high security and convenience of NFC-based payment and the pervasiveness of cameras. At the heart of MagCode is the harmless magnetic interference on the CMOS image sensor of a smartphone placed near the NFC reader, which operates at a high frequency of 13.56 MHz, resulting in a group of barcode-like stripes appearing on the captured images. We take advantage of these stripes to encode the data and achieve simplex communication from an NFC reader to an NFC-denied or NFC-disabled smartphone. In particular, we design and implement a stack of protocols from the physical to the transport layer and test the proof-of-concept prototype across 11 smart devices. Extensive evaluations demonstrate a maximum throughput of 2.58 kbps, which outperforms the magnetometer-based solution [32] by 58×. It takes 1.8 seconds on average to accomplish the data exchange between an NFC reader to a smartphone in relation to mobile payments. In summary, our contribution is that we first reveal that magnetic coupling leakage from NFC readers can induce the appearance of barcode-like stripes on images captured by smartphones. This phenomenon serves as an intriguing physical side-channel between the reader and the camera, introducing an NFC-like mobile payment feature to all smartphones, regardless of their inherent NFC capabilities. Our study aims to pioneer a novel application by harnessing the existing magnetic inductive coupling signals in NFC readers. This work not only expands the functionality of mobile devices but also demonstrates the potential of magnetic couplings in facilitating secure side-channel communication connections.

■ Magnetic UHF Coupling: Spatially Controllable RFIDs Inventory

In the fast-paced landscape of UHF RFID technology, achieving precise spatial-selective identification is of critical importance in the logistics and retail domain. This work introduces RFID+, a magnetically-driven UHF RFID system that leverages the matching loops of commercial-off-the-shelf UHF RFID tags for efficient energy harvesting from tailored magnetic fields. The RFID+ delivers a level of spatial precision comparable to that of HF NFC systems, effectively mitigating issues of miss-reading and cross-reading. Our primary contributions reside in the development of a specialized multi-turn, capacitor-segmented coil antenna and an innovative fast inventory algorithm. The RFID+ seamlessly integrates traditional radiative coupling with the innovative magnetic inductive coupling in UHF RFID systems, bolstering their overall performance and efficiency. Real-world pilot studies in warehouses and logistics settings reveal that RFID+ significantly diminishes the miss-reading rate from 22.9% down to a remarkable 1.06%, while entirely eliminating cross-reading challenges. Moreover, our RFID+ variant demonstrates better resilience against materials traditionally challenging for UHF RFID, such as water bottles and containers. These advancements make RFID+ exceedingly relevant for practical applications in logistical networks. In summary, our contribution is that we extend the operating frequency of magnetic inductive coupling to the UHF band, enabling the development of spatially controllable UHF near-field RFID identification applications. This study aims to leverage the inherent advantages of near-field technology in UHF RFID systems to address the prevalent issues of miss-readings and cross-readings found in traditional far-field inventory mechanisms. Our approach involves designing an electrically large coil antenna for the UHF band to emulate the near-field properties of electrically small coil antennas used in LF/HF bands, achieved through a novel multi-turn segmented antenna prototype. This advancement not only broadens the frequency range of magnetic inductive coupling into higher bands but also opens up new application scenarios that were traditionally overlooked.

In conclusion, the contributions of this dissertation have significantly enriched our understanding of controllable magnetic inductive coupling, uncovering its extensive potential beyond conventional applications. By identifying LF band side-channel security vulnerabilities within mobile voice systems, uncovering novel physical side-channels in HF bands for mobile payment, and extending the operating frequency to the UHF band for battery-free RFID network applications, this research not only broadens the scope of magnetic inductive coupling but also enhances its practical applicability across various technological fields. Each discovery paves the way for further exploration and innovation, underscoring the potential of magnetic inductive coupling as a pivotal element in advancing mobile interoperability and security of next-generation wireless systems. However, it is important to acknowledge that these advancements represent just the beginning of what can be achieved, and much work remains to fully exploit and refine the magnetic coupling for broader application and deeper impact.

1.4 Organization of the Dissertation

The rest of the dissertation is organized as follows:

- **In Chapter 2**, we conduct an extensive literature review on current methodologies within the realm of magnetic inductive coupling in mobile systems, focusing on security analyses and innovative applications. Firstly, the review explores studies related to inaudible voice attacks induced by LF wireless charging. It begins by analyzing prior works for injecting inaudible voice commands into smart assistants and then introduces conventional electromagnetic compatibility strategies implemented in smart devices. Next, we explore magnetic interference in the HF band and evaluate the performance of prior physical side-channel-enabled short-range communication systems. Finally, we discuss various UHF magnetic antenna designs optimized for near-field RFID inventory management and compare their characteristics with previously proposed radiative RFID systems.
- **In Chapter 3**, we introduce a novel type of inaudible voice attack triggered by LF magnetic interference from a wireless charger. Through a feasibility study, we first demonstrate that smart device microphones can inadvertently record magnetic-inductive sounds during wireless charging, highlighting the lack of effective protection against low-frequency magnetic coupling. Next, we explain how to clone a victim's voiceprint via zero-shot learning to bypass biometric authentication safeguards. Building on these findings, we then elaborate on the design principles of

two inaudible voice attacks, HeartwormAttack and ParasiteAttack, aimed at injecting malicious voice commands into devices during wireless charging. These attacks exploit either a compromised wireless charger or an accessory device to deliver malicious commands. Experimental results validate the practicality of these attacks under typical commercial charging conditions. Finally, we address the limitations of these attack strategies and propose countermeasures from both hardware and software perspectives to mitigate the security vulnerability.

- **In Chapter 4**, we introduce a novel cross-technology communication system between an NFC reader and a camera which allows customers to enjoy the high security and convenience of NFC-based payment and the pervasiveness of cameras. To establish feasibility, we first demonstrate that benign HF magnetic interference on a smartphone's CMOS image sensor, when positioned near an NFC reader, produces barcode-like stripes in captured images. These visual patterns are used to encode data, enabling simplex communication from the NFC reader to the smartphone. Building on this foundation, we then designed and implemented a comprehensive protocol stack, spanning from the physical layer to the transport layer, to enable the seamless operation of the proposed system. A proof-of-concept prototype was rigorously tested across various smart devices. Finally, the evaluation results demonstrate adequate data throughput and low latency, highlighting the system's practicality and efficiency for mobile payment applications.
- **In Chapter 5**, we introduce a magnetically-driven UHF RFID system named RFID+, which utilizes the matching loops of off-the-shelf UHF RFID tags to efficiently harvest energy from magnetic fields for inventory purposes. Firstly, we conduct a feasibility study to confirm that magnetic inductive coupling can effectively activate and communicate with COTS RFID tags. Building on this foundation, we then outline the design criteria for a magnetic antenna aimed at achieving a uniform magnetic field distribution within the near-field region. Key innovations include the development of a specialized multi-turn, capacitor-segmented coil antenna array. Next, we introduce a prefetching-enabled rapid inventory algorithm

that seamlessly integrates traditional radiative coupling with near-field magnetic coupling. Real-world pilot studies in warehouse and logistics environments reveal that RFID+ dramatically reduces the miss-reading rate from 22.9% to a remarkable 1.06% while virtually eliminating cross-reading issues. Finally, evaluations demonstrate that RFID+ exhibits improved resilience against challenging materials, such as water bottles and containers.

- **In Chapter 6**, we summarize the research problems and key contributions of this dissertation, which include the development of inaudible attacks enabled by LF magnetic couplings, side-channel communication for mobile payments facilitated by HF magnetic interference, and a spatially controllable RFID reading system powered by UHF magnetic field. Then, this chapter outlines potential future directions, emphasizing the prospects for extending magnetic inductive coupling into new wireless security and mobile application scenarios. It highlights two promising magnetic coupling-driven research topics: attacks and countermeasures on acoustic sensing systems and acceleration optimization for RFID near-field communication systems. Such expansion could further exploit the versatility and effectiveness of magnetic inductive coupling, thereby enhancing the capabilities of modern mobile systems.

Chapter 2

Literature Review

2.1 Security Flaws in Wireless Charging Systems

Voice assistants have become an integral feature of mobile devices such as smartphones and smartwatches, making them a target for various inaudible voice injection attacks using external tools. However, existing approaches have overlooked the potential of wireless chargers as attack vectors. Wireless charging systems typically consist of two primary components: a charger, which acts as the transmitter emitting energy via strong LF magnetic coupling, and a receiver device that captures this energy to convert it into electrical power. Due to the inherent inefficiency of energy transfer, magnetic leakage inevitably affects other components, such as microphones. This represents a critical oversight, as wireless chargers can exploit the insufficient defenses of smart devices against LF magnetic interference, introducing a novel and previously untapped avenue for compromising device security.

In this section, we will first provide a comprehensive review of existing inaudible voice command injection attacks. Subsequently, we will thoroughly investigate current smart device protections against electromagnetic interference (e.g., wireless charging magnetic leakages) to expose prevailing vulnerabilities.

2.1.1 Recent Surge in Inaudible Voice Attacks

A number of recent studies have demonstrated the feasibility and the negative consequences of inaudible voice command injection attacks. **(1) Vibration-based Attacks**. The first group attempts to trigger the mechanical vibrations of a microphone's membrane and inject the voice commands [33–39]. Backdoor [33] shows that a microphone that is originally designed to record human voice only can receive ultrasonic signals because the membranes can be vibrated by ultrasound as well. DolphinAttack [35] uses this physical characteristic to demonstrate inaudible voice attacks toward many popular voice controllable systems by injecting ultrasound signals over the air. The follow-up work named LipRead [34] further extends the attack range from 5 to 25 ft by using an array of ultrasonic transducers. Unlike these existing studies, our attacks never trigger any mechanical vibrations but directly induce the voice signals on the circuits of a microphone, thereby successfully bypassing the defense method of detecting abnormal vibrations [40]. **(2) Coupling-based Attacks.** The second group leverages the electromagnetic interference (EMI) to launch the inaudible voice attack [41–44]. EMI is an intervention generated by external excitations that affect peripheral sensitive electrical circuits and sensors by electromagnetic induction, energy coupling, or conduction. GhostTalk [41] firstly finds that microphones suffer from the bogus audio signals caused by the EMI from the wireless communication at the ultra-high frequency (i.e., 800-900MHz). The follow-up work [42] utilizes the front-door coupling on headphone cables to capture the forged AM-modulated signals at high frequency (i.e., 80-108 MHz) from the air. These previous EMI-based attack methods at high or ultra-high frequency are now completely disabled by Faraday cages equipped for microphones [45]. Another line of work uses light to induce the coupling current at microphones and initiate the inaudible voice attack [43]. However, keeping in line with the sight of the victim device is required despite the long range. By contrast, our attacks utilize the ubiquitous wireless chargers to attack smart devices when not in use, which is more unnoticeable to users. Recently, the authors in [44] even proposed that the audio signals can be injected directly into the power line through a modified charging cable wire. We move forward and show that wireless chargers can also be manipulated to perform inaudible attacks. To the best of our knowledge, we are the first to use the wireless chargers' magnetic leakage as an EMI to induce the coupling current in microphones for injecting inaudible commands [46].

2.1.2 Electromagnetic Compatibility on Charging Systems

Electromagnetic Compatibility (EMC) is the ability of electrical systems to function acceptably in their electromagnetic environment. Here, we mainly review the studies on EMC in microphones and chargers. **(1) EMC for Microphones.** A white book [45, 47] from Infineon Technologies (a worldwide semiconductor manufacturer) shows that the EMC for current MEMS microphones is achieved through three main measures (Sec. 3, pp.16), namely, using capacitors to filter low and high-frequency interference, adding a series resistor or ferrite, and connecting microphone grounds to the circuit board ground plane with vias. After a complete analysis of the EMI of current microphone MEMS, Ko et al. [48] point out that the EMI suppression on MEMS microphone can be further improved by 14 dB by increasing the number of micro bumps, adding the ground via in the substrate, and applying metal coating around the acoustic port. Reitsema et al. [49] emphasized suppressing the down-conversion of high-frequency disturbances to audio frequency and compensating for the remaining disturbance signals. **(2) EMC for Wireless Chargers.** Wireless charging utilizes electromagnetic induction to transfer power and inevitably causes EMI in peripheral circuits of devices to be charged, such as smartphones, watches, and electric vehicles. However, current state-of-the-art studies [27, 28, 50–53] are primarily focused on EMI suppression in scenarios involving electric vehicle charging, where the transfer of extremely high power (kilowatts) is required to meet energy demands. At present, EMC solutions for wireless charging in other contexts, such as portable devices, remain largely unexplored.

2.2 Physical Side-Channel Communication Systems

Short-range communication systems have achieved significant success, driven by the widespread adoption of NFC technology. Recently, numerous NFC-like physical side-channel communication systems have been proposed to support a variety of mobile applications. These systems utilize unintended physical phenomena, such as electromagnetic, acoustic, optical, or thermal emissions, to establish covert or secondary communication channels over short distances. By leveraging specific physical interactions within the environment, they enable either mutual data exchange or one-way data transfer. However, the potential of HF NFC magnetic leakage as a viable side channel remains largely underexplored, as the magnetic interference generated by NFC on various components of mobile systems (e.g., camera) is frequently disregarded.

In this section, we first analyze the magnetic compatibility strategies of image sensors in mobile devices to identify opportunities for converting negative magnetic interference into a functional side channel. Subsequently, we present a detailed review of existing short-range side-channel communication systems and evaluate their performance in comparison to our proposed NFC-to-camera MagCode system [31, 54].

2.2.1 Electromagnetic Interference on Image Sensors

EMI is a persistent challenge in wireless systems, occurring in a wide variety of contexts. Previous studies on camera EMI have primarily focused on analyzing its effects [55–57], reducing internal EMI [58], or mitigating external EMI [59–62]. A white paper from AMS OSRAM, a leading semiconductor manufacturer, highlights that most image sensors lack advanced shielding due to the low energy dissipation at the interface [58, 60]. Only a few specialized cameras [61, 62] incorporate EMC shielding housings. Previous research [55] has shown that the images captured by charge-coupled device (CCD) or complementary metal-oxide-semiconductor (CMOS) sensors can be disrupted by intentionally controlled external EMI, while [59] demonstrated that CMOS cameras may experience operational faults at specific frequencies. The objective of the proposed MagCode system is fundamentally different from these prior efforts. Rather than mitigating interference, it is the first work to transform traditionally "negative" magnetic interference into a "positive" carrier signal, creating a novel communication bridge between cameras and NFC readers.

2.2.2 Short-Range Communication Systems

Recently, a large number of works have been proposed to achieve short-range communication, such as NFC with different technologies. Dhwani [63] is an acoustics-based NFC system that uses microphones and speakers on mobile phones. Ripple [64] employs physical vibrations as the communication carrier. DeafAid [65] utilizes the speaker-to-gyroscope channel to build robust protocol-independent communication. Pulse [32] achieves a low bitrate communication between a TX coil and the magnetometer, which is limited to 50-100 Hz low sampling of the magnetometer. MagneComm [66] uses the CPU EM leakage to set up the side channel between the CPU and a magnetometer. Met [67] develops a magnetic-based toothbrush sensing system by using a specific coil antenna array. We compare these related works with MagCode in Table. 2.1. First, MagCode is the first to achieve the CTC between an NFC reader and a camera. No previous works have been proposed on this topic to bridge the gap to the best knowledge. Second, the bitrate of MagCode is much higher than the existing solutions. Limited to the low sampling of built-in sensors, the bitrates of Ripple, DeafAid, Pulse, and MagneComm are far less than one kbps. We highlight the outperformance in red as shown in Table. 2.1. Third, the most similar work is the Pulse, which also employs the magnetic field as the carrier but uses a magnetometer as the receiver. However, the bitrate of Pulse is about 44 bps due to the 50-100 Hz sampling rate of a magnetometer. In contrast, MagCode outperforms Pulse by 58×. Fourth,

Table 2.1: Comparison with Related Systems.

Solution	**Tech.**	**Bitrate (bps)**
NFC [68]	Induction	106 k
Dhwani [63]	Speaker to Microphone	2.4 k (1.075×)
Ripple [64]	Vibra-motor to Accelerator	200 (12.9×)
DeafAid [65]	Speaker to Gyroscope	47 (55×)
Pulse [32]	Magnetic to Magnetometer	44 (58×)
MagneComm [66]	CPU to Magnetometer	110 (23×)
MagCode	**NFC to Camera**	**2.58 k**

although the bitrate remains less than that of NFC, it is sufficient for short-message communication like transaction ID in mobile payment systems. In short, MagCode is the most promising solution alternative to NFC for NFC-disabled smartphones.

2.3 Magnetic Antenna for UHF RFID Systems

UHF RFID systems typically consist of a reader and a group of passive tags. The reader usually employs electrical antennas, such as patch antennas, to transmit UHF carrier signals that wirelessly power and activate the passive tags. These tags harvest the transmitted energy through a radiative coupling mechanism and backscatter their data, such as the Electronic Product Code (EPC), to the reader using the reflected signal. Recently, magnetic antennas have emerged as a promising solution to challenges like miss-reading and cross-reading in traditional RFID communication, offering a uniform magnetic field distribution within the near-field region. Consequently, it is essential to thoroughly review prior advancements in magnetic antenna technology to assess its potential applicability in the UHF band.

In this section, we first review traditional UHF RFID systems that utilize techniques like beamforming and phase estimation to enhance their inventory performance in RF-unfriendly environments. Subsequently, we explore prior efforts in antenna designs aimed at generating uniform magnetic fields within the UHF near-field region.

2.3.1 UHF RFID Communication Systems

Over time, UHF RFID systems have been thoroughly tested and understood [69–75]. Their vulnerabilities, including missed readings, are heightened in RF-unfriendly environments [76] or due to multipath issues [69]. Historical attempts at remedying these inaccuracies have explored beamforming [77], nonlinear backscattering [78], wideband signal [72] and wave optimization [79, 80]. Besides missed readings, cross-reading errors are a challenge [81]. Localizing UHF RFID tags has been a primary method to sieve out unwanted tags from the ROI [71, 72]. Still, most localization solutions are antenna-intensive, with RFGo [82] using eleven antennas, proving costly and intricate for industrial settings. The NFC+ solution [70] proposes enhanced NFC technology as a UHF RFID substitute. Although NFC is highly secure [31], its low throughput is its Achilles' heel. The industry has explored merging HF NFC and UHF RFID technologies by developing dual-frequency tags [83]. However, this approach compromises the low-cost benefit of standard tags due to the need for custom-designed alternatives. In contrast, RFID+ innovatively combines the best features of both technologies, enabling accurate UHF RFID tag detection with spatially controllable magnetic fields while also ensuring full compatibility with legacy RFID tags.

2.3.2 Magnetic Antenna Design and Application

(1) Magnetic Antenna Design: Recent studies have focused on developing magnetic antennas for near-field UHF RFID applications [84, 85], highlighting this technology's potential to substitute LF/HF RFID in tagging individual items [86]. Traditional solid-line loop antennas primarily be utilized as RFID reader antennas in low frequency [87] and high frequency [88, 89] RFID systems. However, these antennas struggle to maintain a uniform magnetic distribution within the ROI at the UHF band, mainly due to their inability to be electrically small [90]. Addressing this, Dobkin et al. introduced the use of lumped series capacitors in loop antennas to counteract current nulls and enhance magnetic strength in the UHF range [26]. Later studies [91, 92] examined the properties of segmented line capacitors, eliminating the need for discrete circuit components. This led to investigations into various distributed capacitor designs [93–96]. While our work is inspired by existing research, RFID+ is the first to harmoniously integrate disparate elements (e.g., capacitor-segmented loops, multi-turn UHF coils, HISs, coil arrays, etc) into a unified practical system. **(2) Magnetic Power Transfer:** Additionally, research on magnetic antenna-enabled power transfer [70, 97–100] has gained significant attention in the networking academic community. While traditional NFC operating at 13.56 MHz [70] and magnetic charging at 1 MHz [99] remain dominant in the HF band, advancements such as magnetic resonance [97] and beamforming techniques [98, 99] are driving innovation and expanding the scope of this technology.

Chapter 3

Magnetic LF Coupling: Inaudible Voice Attacks & Countermeasures

3.1 Introduction

Voice assistants have become an increasingly popular human-computer interaction approach in smart devices (e.g., smartphones or wearables) with the recent incredible advances achieved in the field of speech recognition. For example, Apple Siri [101] and Google Now [102] allow users to initiate phone calls and launch apps through their voices; Alexa [103] even allows users to instruct an Amazon Echo to control their entire smart home. With the spread of voice assistants, a built-in microphone (as a compulsory component for a smart device) has become a new vulnerability under sneaky and malicious *inaudible voice attacks*. In these attacks, inaudible voice commands, which are unintelligible and unnoticeable to human listeners, can take control of the victim devices [35].

The known voice command attacks can be initiated via different types of inaudible media, such as the ultrasound [33–38], laser [43], and EMI [41, 42, 44]. Particularly, a large number of works attacked computer systems through the EMI [104–106] in

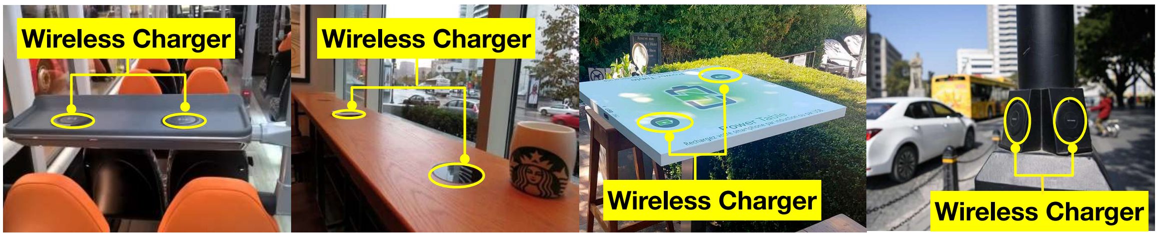
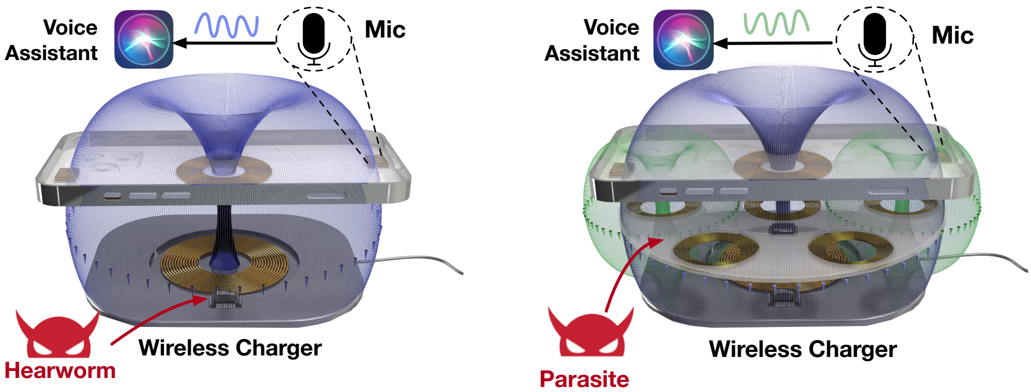


Fig. 3.1: Illustration of wireless chargers in public. With the fast spread of wireless charging technology, wireless chargers are becoming public facilities everywhere.

the last decades. Recently, these potential EMI were reused to initiate inaudible voice attacks on smartphones through the external wireless circuitry [41], headphone cables [42] and power lines [44]. As an important countermeasure against the potential EMI [45], the industry equips today's microphones with Faraday cages (a kind of EM shield) and EMI filters, especially against the 3G/4G signals operating at 800-900 MHz [41–43]. Unfortunately, a recent study shows that magnetic fields can still penetrate Faraday cases due to the immunity of magnetic fields to electromagnetic shields [107], which is also confirmed by our preliminary tests.

By taking advantage of the above vulnerability, we explore a new type of inaudible voice attack through the wireless chargers, which produce the well-modulated magnetic interference to inject the voice commands into the microphones as if they were recorded from a physical sound. Wireless charging delivers power from an energy supply to smart devices without contact. Wireless charging also encourages the production of completely sealed or even waterproof device casing, which substantially improves convenience, usability, and reliability. Thus, wireless charging is becoming a de facto power supply solution for a vast number of smart devices, especially for wearables (such as Apple Watch or AirPod). Fig. 3.1 shows some typical public wireless charging stations, where numerous free wireless chargers are deployed in public everywhere and hundreds of millions of people benefit from them every day. Nevertheless, these public wireless chargers are becoming potential security breaches.

Achieving magnetic-inductive sound (MIS) at microphones is very challenging because



(a) HeartwormAttack

(b) ParasiteAttack

Fig. 3.2: Attack scenarios. The blue curves represent the magnetic field generated by the TX coil of the wireless charger, while the green curves represent the fields generated by the TX coils of the parasite.

of a fundamental communication issue, that is, there exists an about 80 kHz frequency gap between microphones and chargers. Specifically, a microphone can only record the voice below 22 kHz, where higher frequencies will be completely filtered out, whereas a wireless charger produces magnetic fields at 100 kHz to 200 kHz. To address this issue, we propose two attacking approaches, HeartwormAttack and the ParasiteAttack, as shown in Fig. 3.2.

- **HeartwormAttack**: We envision that an adversary can install the malware called *heartworm* into a wireless charger during the manufacturing phase. The compromised charger can opportunistically trigger a victim device to execute an expected command through the MIS, as shown in Fig. 3.2(a). Such an attack uses the non-linearity of the amplifier in a microphone to downconvert the MIS from charging frequency into an audible spectrum.
- **ParasiteAttack**: We envision that an adversary attaches small and thin accessory equipment called *parasite* onto a public wireless charger, as shown in Fig. 3.2(b). As a Near-field Communication(NFC) card, the parasite uses a receiving (RX) coil to "steal" power from the host charger and drives one of the transmitting (TX) coils to directly generate the magnetic-filed at the voice frequency, which further

produces MIS at microphones.

Both attacking approaches have pros and cons. First, the HeartwormAttack must intrusively hack the wireless chargers in advance, whereas the ParasiteAttack can be launched anytime after parasites are deployed. Second, commercial wireless chargers are usually not equipped with wireless communication modules (e.g., Wi-Fi and Bluetooth). Thus, the HeartwormAttack can only work offline using pre-stored voice commands. In contrast, the ParasiteAttack allows the adversary to inject an on-demand voice in real-time through the 4G/5G functionality of the parasite equipment.

We have tested the two attacks on 17 device models including smartphones, smartwatches, tablets, and add-on microphones, which involve 6 voice controllable systems or speech recognition systems. Each attack is successful on at least one SR system. The attacking demos can be found at [108]. We believe this list is by far not comprehensive. Nevertheless, this study serves as a wake-up call to consider the security breach caused by the magnetic interference and reconsider what functionality shall be introduced in voice assistant systems.

Totally, we made the contributions as follows. First, we discover the potential security threat of magnetic interference to most audio-capable devices and demonstrate such a security threat by using wireless chargers. Second, we show that adversaries can inject a sequence of inaudible voice commands into microphones through two approaches that are, HeartwormAttack and ParasiteAttack. Both two attacks are validated on 17 popular smart devices and 6 common speech recognition systems. Third, we suggest both hardware-based and software-based countermeasures to alleviate the attacks. We also raise a practical concern on the negative consequence resulting from the excessive demand for faster wireless charging.

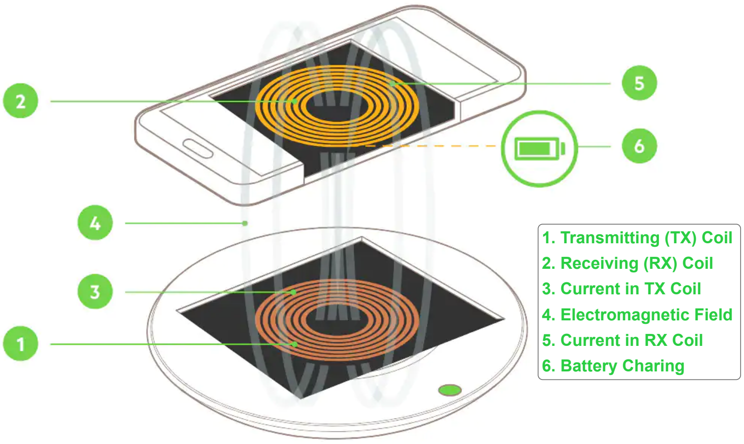


Fig. 3.3: Illustration of wireless power transfer.

3.2 Background of Wireless Power Transfer

3.2.1 Principles of Wireless Power Transfer

Wireless power transfer (WPT, aka wireless charging) works on the principle of electromagnetic induction. Both the transmitter (i.e., a wireless charger) and the receiver (i.e., a smart device) are equipped with coils. Coils of wire in the transmitter create a magnetic field as the current passes through. Alternating magnetic fields can then induce an electrical current in any close-loop conductor nearby. If the conductor is the coil of a device's charging circuit, then the transmitter and the receiver are inductively coupled with each other via the magnetic fields. Thus, they effectively form a transformer with a specific coupling coefficient. The transmitter delivers power to the receiver through the transformer.

As shown in Fig. 3.3, the transmitter (a charging station) and the receiver (a smart device) are inductively coupled with each other by the two coils to form a transformer with a specific coupling coefficient. The transmitter is composed of a TX coil and an inverter that is used to convert a DC low voltage (5 to 20V) power source to an AC high voltage of 50 to 100V. This AC voltage is used to energize the TX resonance tank circuit to create a tuned magnetic field frequency in the range of 100 kHz to 200

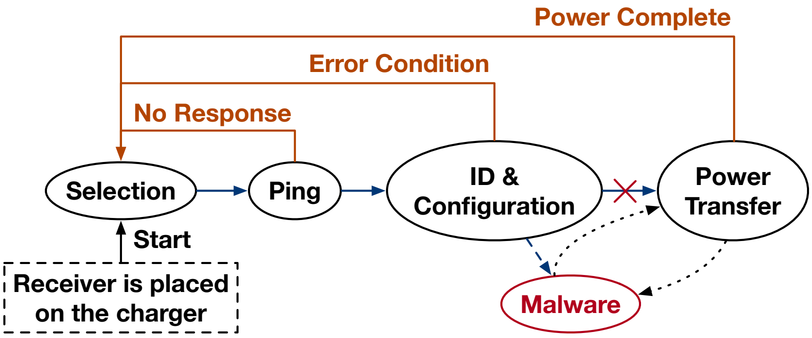


Fig. 3.4: The charging procedure specified in Qi standard

kHz. The receiver (RX) is also composed of an RX coil and a rectifier that converts the power harvested from the magnetic field back to DC power that can then be used to charge a battery. The receiver creates a resonant LC tank circuit to improve the power transfer efficiency by matching the TX response frequency. Accordingly, the maximum efficiency is given by

$$\eta_{\max} = \frac{k^2 Q_1 Q_2}{1 + \sqrt{1 + k^2 Q_1 Q_2}} \tag{3.1}$$

where Q_1 and Q_2 represent the quality factor of TX and RX coils, respectively, k is the coupling coefficient between the RX and RX coils. Clearly, the efficiency can be improved by raising the quality factor. However, a higher Q will reduce the bandwidth.

3.2.2 Charging Workflow in Qi Standard

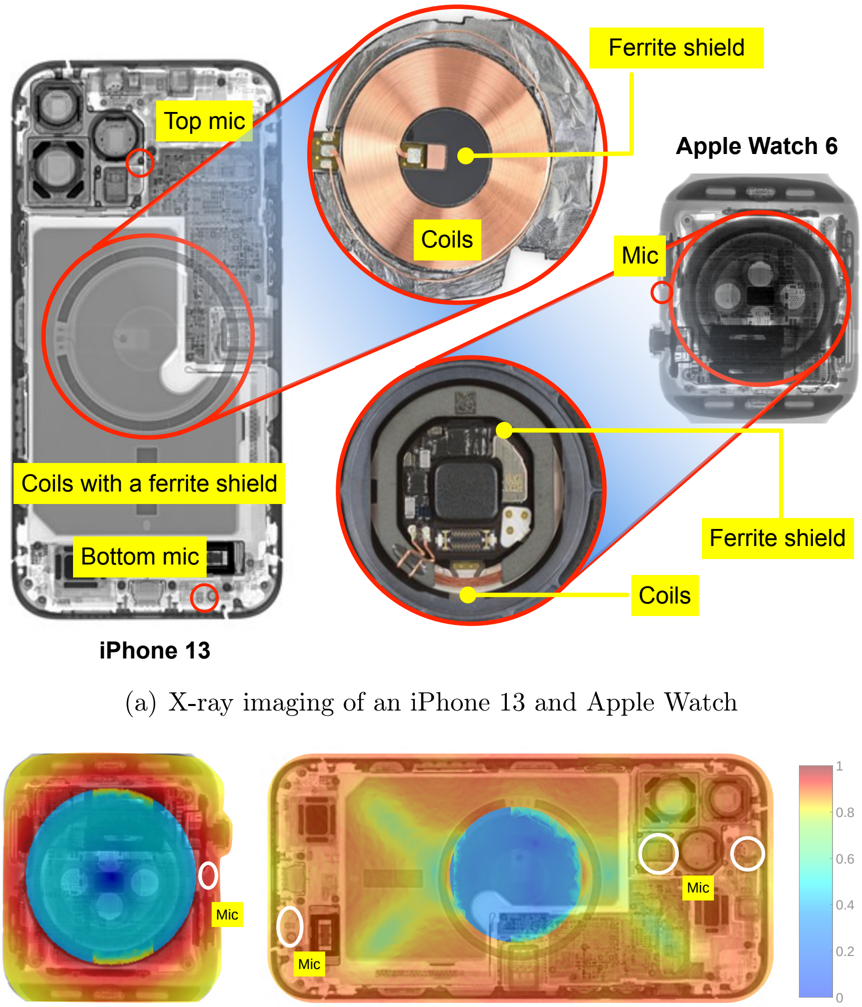
We must integrate the voice injection into a victim device in accordance with the Qi standard seamlessly so that the charging process is uninterrupted by the voice injection, which is key to keeping a dying victim device alive and preventing a smart device from detecting abnormalities. The Qi standard specifies a complicated charging workflow. For clarity, we show a simplified workflow in Fig. 3.4. Initially, the wireless charger starts with extremely low power for safe charging. By default, it is in a selection state, during which it checks the placement of a receiver. Once a smart device is placed, the charger turns into the ping state, where it sends out a digital ping pulse and listens for a response from a receiver. This step aims to detect the presence of a receiver rather than non-rechargeable matter. The charger then transits to the identification and configuration state, during which the two sides exchange the configuration information, such as the manufacturing model, battery capacity, acceptable maximum power, etc. Finally, the charger creates a power transfer contract (PTC), including the parameters of the power transfer. Afterward, the charger raises the power based on the PTC and starts to transfer power to the receiver. During the transfer state, the receiver can also adjust the PTC parameters to meet the battery requirement. From the figure, we could find that the best attack timing should be after the PTC has been established.

3.3 Feasibility on Magnetic-Inductive Sound

Our core idea is to skip the microphone diaphragm, but *directly induce* an acoustic signal at the onboard circuits of a microphone by using a manipulated magnetic field. In this section, we conduct the feasibility analysis and verification experiments to answer three key questions: (1) Can the microphone receive magnetic interference when the device is being wirelessly charged? (2) Can the leaked magnetic field violate the current EMI protections? (3) Which part of a microphone is interfered?

3.3.1 Magnetic Interference in Smart Devices

In the field of electronic engineering, EMI is a phenomenon that may occur when an electronic device is exposed to an electromagnetic field. The magnetic field generated by a wireless charger will induce an eddy current in the circuits of a nearby device and cause magnetic interference (i.e., a type of EMI). To address such potential hazards,



(a) X-ray imaging of an iPhone 13 and Apple Watch

(b) Distributions of magnetic field over two devices

Fig. 3.5: Magnetic interference over two smart devices

existing smart devices usually use a ferrite shield to protect the motherboard from the EMI. Fig. 3.5(a) shows the X-ray imaging of an iPhone 13 and Apple Watch 6 from the backside. The RX coils are arranged in the back center of device bodies. A circular ferrite shield is inserted between the RX coil and the motherboard to protect the internal circuits. However, the ferrite shield only covers the area right behind the RX coil, where the magnetic field is at the strongest. The remaining areas beyond the coverage of the shield still receive magnetic interference from the TX coil of the wireless charger.

To quantify the magnetic interference, we compute the distributions of the magnetic field over the whole motherboards of the two devices by using Ansys Maxwell [109]. In the simulation, we use the shell models from [110, 111] and manually model the internal circuity and main components including the RX coil with a ferrite sheet. The exciting source is the Ansys built-in standard A2 coil model [112]. On the basis of the Biot-Savart Law, the magnetic field strength $\mathbf{B}(r)$ at the distance r from the center of the transmitting coils, is computed as follows:

$$\mathbf{B}(\mathbf{r}) = \frac{\mu_0}{4\pi} I \int_C \frac{d\ell \times r}{|r|^3} \tag{3.2}$$

where μ_0 is the vacuum permeability, I is the charging current, C is the current's flow path in the coil, and $d\ell$ is a vector along the path. We adopt the recommended charging settings specified in the Qi standard [112], which is the most widely adopted wireless power transfer (WPT) protocol on the market. Specifically, the charging frequency and the power are set to 100 kHz and 15 W, respectively. The A2 TX coil [112] with 20 mm inner diameter and 40 mm outer diameter is utilized for the charger. The Qi Example 4 RX coil with 28 mm diameter and 47 mm outer diameter is used for the receiver. The magnetic shield made of Mn-Zn ferrite is 1 mm thick. The TX and RX coils are spaced by 1 cm.

Fig. 3.5(b) shows the distribution results. The magnetic strength behind the ferrite shield is mostly reduced to zero. However, the remaining areas, especially the marginal areas where microphones are located, are fully exposed to the strong magnetic field. This phenomenon is caused by the functional principle of ferrite shield, i.e., ferrite materials cannot weaken magnetic fields but distract the field lines from them to the nearby areas [113] as observed in the figure. As a result, the magnetic strength is actually enhanced in the areas beyond the shield. Therefore, the ferrite shield cannot protect the microphone from magnetic interference. Worse, the industry is quite "aggressive" in raising the charging power to pursue faster charging. To date, 50 W and even 80 W chargers are found on the market [114], which further intensify the magnetic interference to other components like microphones.

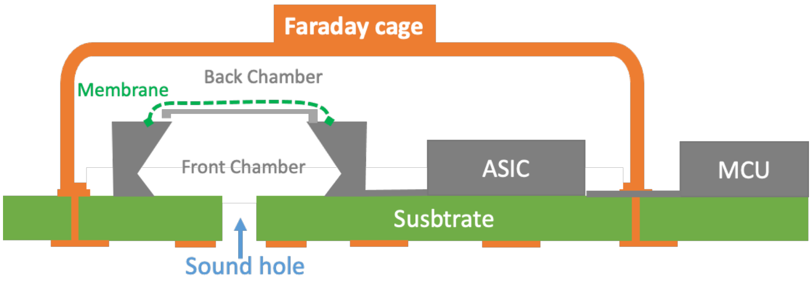


Fig. 3.6: On-board structure of a digital MEMS microphone

3.3.2 Magnetic Interference to Microphones

A microphone is a component that can convert sound waves into electrical signals. There are two types of microphones, electret condenser microphone (ECMs) and Micro electro mechanical system (MEMS), available on the market. Due to the miniature package size and lower power consumption, MEMS microphones dominate smart devices. Thus, this paper focuses mainly on MEMS microphones. Nevertheless, MEMS and ECMs work similarly. The MEMS microphones can be further divided into two types, analog MEMS and digital MEMS microphones. If the output of the microphone is an analog signal, it is called an analogy MEMS microphone (like ADMP 401 and TDK 4086 [115]); otherwise, it is called a digital MEMS microphone (like Infineon IM69D130 [116]). The main difference is that the analog MEMS microphone contains all components (i.e., transducer, filter, and amplifier) except ADC [117], while the digital MEMS microphone further integrates the ADC. For example, all Apple iPhones use analog MEMS microphones, and most Samsung phones use digital MEMS microphones. Either way, the workflows of the two types of microphones are similar.

Fig. 3.6 illustrates the packaging and interconnection structure of a typical digital MEMS microphone, which consists of a diaphragm and a complementary perforated backplate. When a sound wave is present, air pressure passing through the holes induces mechanical vibrations in the diaphragm—a thin, flexible membrane that bends

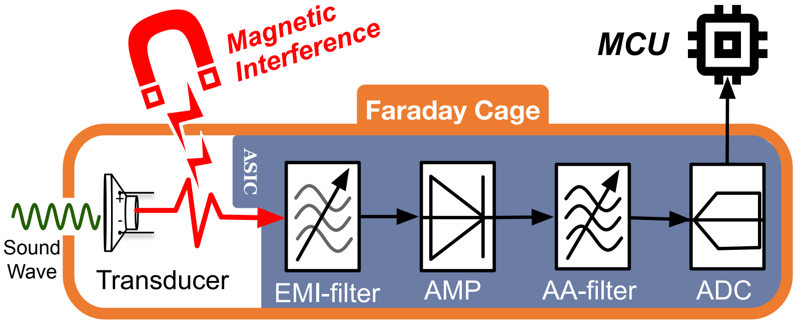


Fig. 3.7: Architecture of a MEMS microphone

in response to pressure changes. These mechanical vibrations cause a change in the capacitance of a capacitor, producing an AC signal. This process effectively converts air pressure into an analog acoustic signal, which is subsequently amplified, filtered, and digitized by the accompanying ASIC chip. The digitized acoustic signal is then transmitted to an external acoustic microchip for further processing.

Similarly, Fig. 3.7 displays the internal structure of a digital MEMS microphone, which is comprised of two primary components: an acoustic transducer and an ASIC chip. When a sound wave presents, the air pressure triggers the mechanical vibrations of the diaphragm and further causes a capacitive change of a connected capacitor. In this way, air pressure is converted into an analog acoustic signal for further processing. The acoustic signal is then amplified, filtered, and digitalized by the following ASIC chip. Finally, the acoustic signals are transmitted to other components like MCU. The industry has made efforts to protect the microphone from the previously reported EMI [41–43] as follows:

(1) Faraday Cage: The whole microphone component is protected by a Faraday cage from disturbance of EM signals, except a small hole reserved to capture the sound wave from the air. A Faraday cage is formed by a continuous covering of conductive material, such as copper [48]. EM signals outside are prevented from going into the cage due to the skin effect [118], and their energy is mostly dissipated in the form of heat. A Faraday cage can only attenuate EM signals with wavelengths shorter than

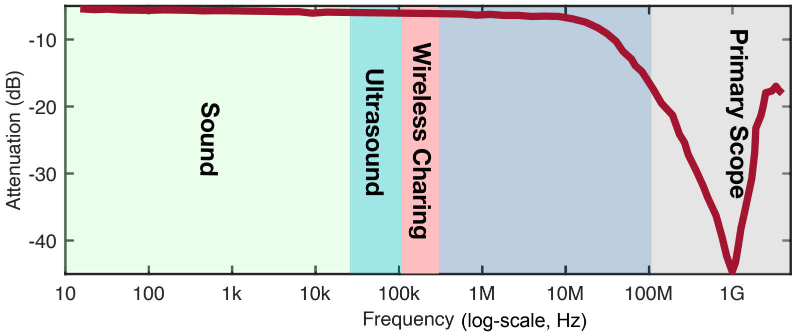


Fig. 3.8: Working spectrum of a commercial EMI filter

the skin depth. Mathematically, a Faraday cage acts as a low-pass filter to move out EM signal above frequency f:

$$f \geqslant \frac{\rho}{\pi\mu\delta^2} \tag{3.3}$$

where δ denotes the skin depth, ρ denotes the resistivity of the conductor, and μ denotes the permeability of the conductor. In accordance with the datasheet [45], the Faraday cages of MEMS microphones are made of copper (i.e., $\mu = 1.256 \times 10^{-7}$ H/m and $\rho = 1.68 \times 10^{-8}\ \Omega \cdot m$) and their depths are approximately 2.06 μm. Substituting these settings into Eqn 3.3, we find out $f \geqslant 1$ GHz. Therefore, the current Faraday cages can only shield 1 GHz or above EMI caused by common wireless communications, such as FM Radio, Bluetooth, WiFi, Cellular, and GPS. They fail to defend against the magnetic interference at 100 kHz caused by wireless chargers unless 100× thicker Faraday cages than the current are adopted.

(2) EMI Filter: As shown in Fig. 3.7, the analog sound signal is pre-processed by an EMI filter before being amplified. The filter aims to eliminate the potential EMI. We show the working spectrum of an EMIF02-MIC03F2 filter in Fig. 3.8. This filer is fabricated by STMicroelectronics [119] and dominates the market of MEMS microphones. It can be seen that these EMI filters focus on shielding 100 M or above EMI. As stated in [45] (Sec. 4, pp.15), the filters mainly aim to suppress the EMI from GSM communications (e.g., TDMA noise) at 800 to 900 MHz and 1800 to 1900 MHz, which is far higher than the operating frequency of wireless charging.

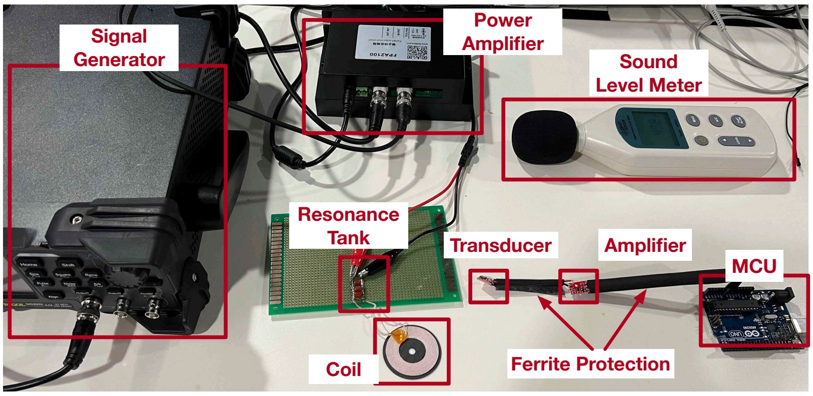


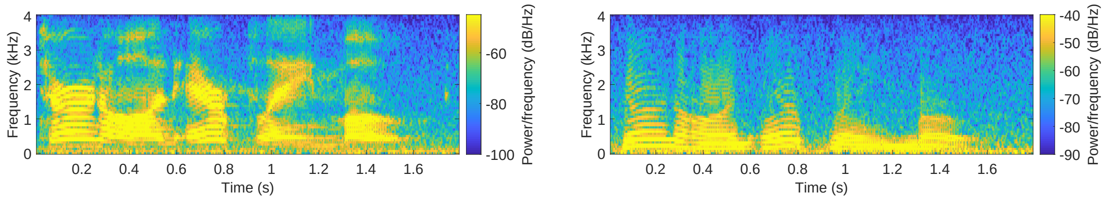
Fig. 3.9: Experimental setup for feasibility verification

In summary, the two existing industrial countermeasures against the EMI reported previously well protect microphones from interference at 100 MHz or above. They fail to eliminate the magnetic interference at a low frequency.

3.3.3 Real-life Verification

Given the above theoretical analysis, we verify the feasibility of generating a clear magnetic-inductive sound (MIS) on real microphones by using charging coils. The experimental setup is shown in Fig. 3.9. We use a vector signal generator to produce a voice signal below 20 kHz. The voice signal is then amplified by a power amplifier to 15 W. The amplified voice signal is then passed through a resonant tank circuit and broadcasted by a standard A2 TX coil into the air. The distance between the microphone and the coil is about 3 cm.

First, we use the signal generator plus the TX coil to transmit a voice clip of "turn on airplane mode". Meanwhile, we used an iPhone 8 to record the clip. We also play the signal by a loudspeaker directly and use the recorded version as the baseline. As shown in Fig. 3.10, the spectrograms of two recordings exhibit similar patterns as that of the original voice. We also notice that the components at higher frequencies (e.g., > 5 kHz) are more attenuated than those at lower frequencies in the MIS. Actually, the energy at frequencies above 5 kHz is ignored in speech perception systems because



(a) Speaker-played voice

(b) Magnetic-inductive sound

Fig. 3.10: Spectrograms of the voice signals. (a) shows the original voice signal; (b) and (c) show the voice recorded by iPhone 8 but injected by a speaker and a TX coil, respectively.

human speech mainly concentrates on the lower frequencies [120].

This experiment fully demonstrates the feasibility of MIS at the microphone. Second, we use an external MEMS microphone (i.e., TDA1308 from Knowles [121]) to record chirp signals with or without the transducer, as shown in Fig. 3.11. In each case, we play the chirp signal sweeping from 100 Hz to 22 kHz by the loudspeaker and TX coil, respectively. Fig. 3.11(a) and (b) show the results of speaker-played sound (SPS) and MIS with the transducer. Both methods can generate the chirp signals in the spectrograms. Then, we forcedly remove the transducer from the microphone. In the figure, (c) and (d) show the results without the transducer. Consequently, none SPS is observed in the spectrogram but the MIS still presents. This experiment fully demonstrates that MIS is completely not produced by the acoustic vibrations, which should be captured by the transducer only. Finally, we assemble an external microphone using several separated components to mimic a MEMS microphone. As shown in Fig. 3.9, the microphone is composed of a Knowles SPV1840LR5H-B [122] transducer (C1), a MAX9812 [123] amplifier integrating an internal low-pass filter (C2), and an onboard ADC (C3). These three components are connected through two wires (W1 and W2) as follows:

$$\mathrm{C1} \xrightarrow{\mathrm{W1}} \mathrm{C2} \xrightarrow{\mathbf{W2}} \mathrm{C3} \tag{3.4}$$

Now, we repeat to play the chirp signals using the TX coil. At each time, one of the C1, C2, W1, and W2 is exposed to the magnetic interference, and others

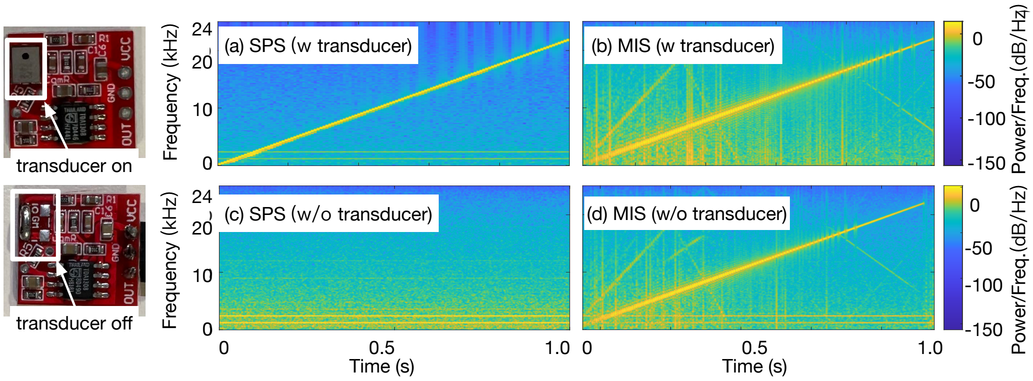


Fig. 3.11: Spectrograms of chirp signals recorded by a MEMS microphone with and without the transducer component.

remain wrapped with ferrite sheets. Fig. 3.12(a) shows the baseline when everything is wrapped with ferrite sheets, and no signal is recorded. Fig. 3.12(b)-(e) shows that MISs are always detected when C1, W1, C2, or W2 is exposed to the interference in turn. This demonstrates that magnetic interference affects all circuity instead of a specific component or a wire. Even a small fragment of wire can still capture the MIS. However, we ensure that the interference only works before the ADC because the injected voice is an analog signal that cannot be recognized by the follow-up digital components. Thus, we should consider the microphone as a whole to defend against magnetic interference.

3.4 Overview

The preliminary experiments fully verify the presence of MIS caused by a charging TX coil. These positive results encourage us to conduct further studies on leveraging MIS to inject inaudible voice attacks. In this section, we introduce a general attack model and then present two attack approaches from a high level.

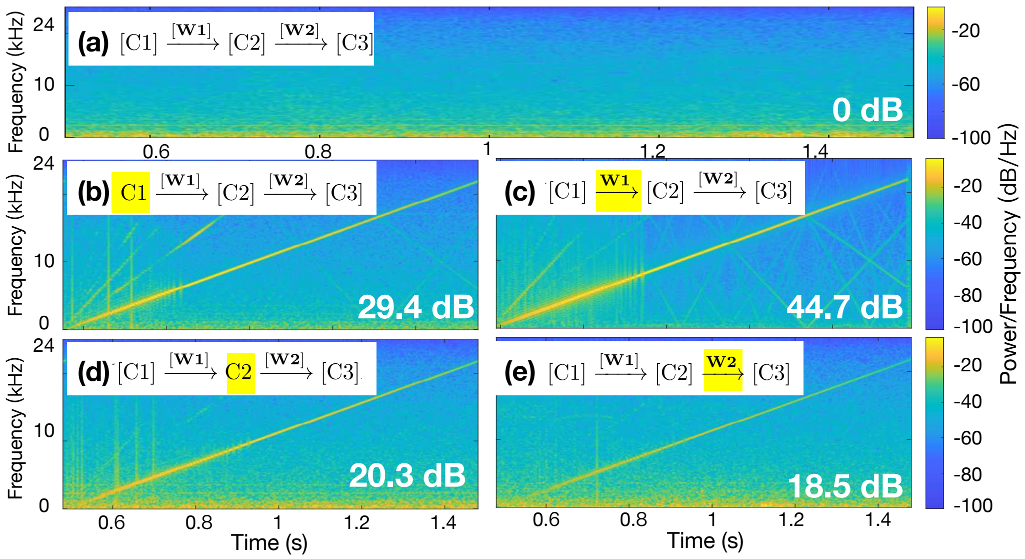


Fig. 3.12: Spectrograms of chirp signals recorded by an assembled microphone. The microphone consists of three separated components (C1, C2, and C3) and two wires (W1 and W2). (a) shows the absence of the signal when all components are wrapped by ferrite sheets. (b)-(e) show the presence of chirp signals when C1, W1, C2, and W2 are exposed to the interference in turn.

3.4.1 Threat and Attack Model

We adopt the similar threat model used in previous inaudible voice attacks, like Dolphinattack [35] and so on [34, 36–39]. The goal of the adversary is to inject malicious voice commands into voice assistants equipped on mobile devices, such as Apple Siri [101], Google Assistant [124] and Samsung Bixby [125]. The smart soundboxes like Alex are not considered since they are usually powered by cables. Through these commands, the adversary can execute unauthenticated actions, such as visiting a malicious website to launch a subsequent drive-by-download attack, making fraud calls to the victim's friends and family, injecting fake information such as fake instant messages, emails, online posts, and even calendar events, or turning on airplane mode to deny all incoming connections [35].

- **Adversarial Abilities**. We assume that the adversary lacks any direct access privileges to the victim's devices nor the capability to implant malware within them.

Modifications to the device settings are also outside the adversary's control. However, the adversary possesses comprehensive knowledge regarding the characteristics of the targeted smart devices. They are capable of discerning the specific model and manufacturer of the victim's device, information that could potentially be gleaned during the handshake phase of WPT data exchanges. It is conceivable that activation phrases such as "Hey, Siri" might be uniquely identified through voice fingerprinting. We further hypothesize that the adversary has the means to covertly monitor the victim via a concealed microphone positioned near the wireless charger or through other analogous side channels. Any speech intercepted in this manner may include the activation command, which could then be used directly for activation. In instances where the direct use of the intercepted command is not viable, the adversary might resort to employing AI-driven voice synthesis technologies to replicate the voice-fingerprinted activation commands [126–128], leveraging the overheard speech. We assume that the adversary possesses a foundational capacity for inference using small-scale AI models, or alternatively, has the capability to offload computational tasks to an external server through wireless connectivity options such as Bluetooth or Wi-Fi.

- **Attack Conditions**. We assume that adversaries can modify the firmware of a wireless charger or attach accessory equipment nearby to a wireless charger. Our attack is initiated when the victim's devices are being wirelessly charged using a public or private wireless charger. The chargers might be deployed in a cafe, street, park, or mounted in a car [129]. One goal of the adversary is to attack victim devices without being noticed. The voice commands generated through the magnetic field are apparently inaudible to humans. Correspondingly, the first command is initiated to turn down the volume to the extent that users cannot hear feedback clearly from the voice assistant. Without loss of generality, we assume that the victim devices are placed a few centimeters away from a wireless charger. The majority of voice assistants are allowed to be waked up and conduct many security-sensitive tasks (e.g., making phone calls, reading messages, or turning on Bluetooth [130]) even

Table 3.1: Available tasks for different VAs when the screen is locked.

VA models Commands	Apple Siri	Google Assistant	Samsung Bixby	Xiaomi Xiaoai
Make phone calls	√	√	√	√
Read messages or emails	√	√	√	×
Send messages	√	×	√	√
Send emails	√	×	√	×
Search the websites	√	√	√	√
Turn on/off WiFi	√	√	√	√
Turn on/off Bluetooth	√	√	√	√
Turn on airplane mode	√	√	√	√
Mute/Unmute the phone	√	√	√	√
Set/Delete alarms	√	√	√	√
Set/cancel appointments	√	√	√	√
Get location	√	×	×	×
Open payment apps	×	×	×	×
Open social apps[1]	×	×	×	×
Access photos	×	×	×	×

[1] Social apps including Facebook, WhatsApp, and WeChat.

when their screens are locked. This makes sense because the ultimate goal of the voice assistant systems is to free users' hands and accomplish major tasks through the voice when smartphones are placed far away and locked by default. We list all security-sensitive and privacy-sensitive tasks that can be accomplished by voice assistants in Table. 3.1. The voice injection introduces some Gaussian noises unavoidably. The voice assistants are assumed to equip with de-noising algorithms, which can well deal with the Gaussian noise introduced by the background, internal circuity or our voice injection.

3.4.2 Attacking Approaches

The feasibility of generating MIS on microphones has been fully verified in benchmark experiments. However, launching inaudible voice attacks via wireless chargers still remains challenging due to the working frequency gap between the charger and the microphone. The sensitivity spectrum of microphones targets between 20 Hz to 22 kHz and ideal signals beyond this spectrum should be filtered. Thus, an antialiasing filter (AA-filter) is adopted after the amplifier, as shown in Fig. 3.7. The MIS between 100∼200 kHz will be removed. To resolve this problem, we propose two attacking approaches on account of the intrusiveness, that is, HeartwormAttack and ParasiteAttack. Specifically, HeartwormAttack utilizes the nonlinearity of the amplifier inside a microphone to downconvert the MIS. On the contrary, ParasiteAttack utilizes the parasite device to harvest energy at a high frequency but generates MIS at the voice band. Detailed information about the proposed attacks will be discussed in Section 3.6 and 3.7.

3.5 Voice Command Generation

Smart voice assistants (e.g., Siri) operate through a dual-phase process comprising both activation and recognition. It requires activation before accepting general voice commands. Only the initial activation command is subject to voice fingerprinting, while the general control commands are not. This means that any voice, even one synthesized by text-to-speech (TTS) models, can trigger the general commands. Hence, to manipulate a voice assistant, we must first generate activation commands before inserting the general control instructions.

One straightforward method to create the activation command involves capturing the activation phrase from the target and executing a replay attack. Nonetheless, the chances of directly recording the activation command are typically slim. More often than not, the microphone picks up regular conversations, such as discussions among friends or questions posed to waitstaff. So, how can we replicate the target's activation phrase (e.g., "Hey, Siri") without access to an actual recording of it? Real-time voice cloning [131, 132] emerges as a contemporary solution, adeptly tackling this challenge through zero-shot learning. It allows for the creation of new speech in the target speaker's voice using just a few seconds of their audio, all without altering any of the pre-trained model's parameters. Therefore, such techniques facilitate the

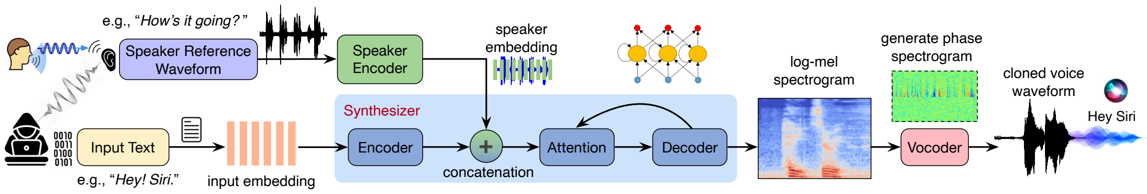


Fig. 3.13: Operational flow of the real-time voice cloning mechanism. The system consists of three components: the speaker encoder, synthesizer, and neural vocoder. Each of the components is trained independently.

unauthorized impersonation of a victim's voice, making them ideal for activating smart assistants in a data efficient manner.

3.5.1 Voice Cloning via Zero-shot Learning

The architecture of a real-time voice cloning system typically encompasses three distinct, pre-trained elements [133]: (1) a speaker *encoder network* is tasked with generating a fixed-size embedding vector from merely a few seconds of a reference audio clip from the intended speaker; (2) a sequence-to-sequence *synthesis network* is responsible for producing a mel spectrogram [134] from a series of grapheme inputs, conditioned on the target speaker's embedding vector; (3) a *vocoder network* is employed to transform the mel spectrogram back into time-domain waveform samples. Fig. 3.13 illustrates the operational flow of the voice cloning mechanism. Subsequently, each of these components will be discussed in further detail:

(1) Speaker Encoder. The speaker encoder conditions the synthesis network using a reference speech signal from the target speaker. Effective generalization relies on a representation that captures the unique characteristics of various speakers and the capability to pinpoint these traits using only a brief adaptation signal, regardless of its phonetic content and background noise. A speaker-discriminative network, GE2E [135], trained on a text-independent speaker verification task, meets these requirements exceptionally well. Thus, we employ it as the speaker encoder network to extract the voice features of the victim speaker. This network transforms a series of log-mel spectrogram frames, derived from speech of any length, into a fixed-sized embedding vector (i.e., d-vector). It is originally trained using a generalized end-to-end speaker verification loss to ensure that embeddings from the same speaker exhibit a high degree of cosine similarity, whereas embeddings from different speakers are distinctly separated in the embedding space. This property makes the embedding suitable for conditioning the synthesis network on speaker identity. Specifically, the network, comprising a stack of three LSTM layers with 768 cells each, processes input 40-channel log-mel spectrograms. Each layer is followed by a projection to 256 dimensions. The ultimate embedding is generated by applying L_2-normalization to the final frame's output from the top layer. The training data is composed of 1.6-second-long labeled speech audio segments. During inference, utterances of any length are segmented into 800ms windows with a 50% overlap. The network processes each window independently, and the resulting outputs are averaged and normalized to produce the expected utterance embedding.

(2) Synthesizer. We utilize the Tacotron 2 [127] sequence-to-sequence feature prediction network with attention to convert input character sequences into sequences of mel spectrogram frames. This network comprises an encoder and an attention-equipped decoder. The encoder transforms a text character sequence into a hidden feature representation, which is then used by the decoder to generate a spectrogram. Specifically, input characters are encoded into a 512-dimensional embedding and passed through three convolutional layers. The output from the last convolutional layer feeds into a single bi-directional LSTM [136] layer to produce the encoded features. At each timestep, this output is concatenated with the target speaker's embedding vector and fed directly into the attention layer of the decoder, as illustrated in Fig. 3.13. The decoder, an autoregressive recurrent neural network, generates a mel spectrogram frame by frame from the encoded sequence. During training, the text is first transformed into a phoneme sequence to speed up convergence and improve the pronunciation of rare words and names. The training employs a transfer learning strategy, using the pretrained speaker encoder (with fixed parameters) to extract a speaker embedding from target audio. The target's spectrogram features are generated from 50ms frames with a 12.5ms stride, processed through an 80-channel mel-scale filterbank and logarithmic dynamic range compression.

(3) Neural Vocoder. We employ the well-known autoregressive WaveNet model [137] as a vocoder, transforming the mel spectrograms produced by the synthesis network back into time-domain waveforms on a sample-by-sample basis. This network includes 30 dilated convolution layers. The mel spectrogram produced by the synthesis network encapsulates all the essential details required to generate high-quality voices from a variety of speakers. The primary function of the vocoder is to produce the phase spectrogram and then integrate it to generate the waveform. This allows the creation of a vocoder simply by training it with data from multiple speakers.

3.5.2 Naturalness Analysis of Cloned Voices

So far, we have explored the theoretical aspects of using zero-shot voice cloning to generate activation commands for the target. However, it is essential to assess the naturalness of the synthesized voice and its ability to bypass common voice fingerprinting security measures on smartphones. To evaluate this, we conducted an experiment with 10 volunteers, including six males (M1-M6) and four females (F1-F4). All volunteers are bilingual, fluent in both English and Mandarin Chinese. Each volunteer recorded two 5-second audio clips as reference waveforms, one in English and one in Mandarin. We then synthesized cloned voices replicating the same content and asked all volunteers to rate the naturalness of the cloned audio using the popular Mean Opinion Score (MOS) [138] metric. The MOS is expressed as a single rational number, typically ranging from 1 to 5, where 1 indicates the lowest naturalness quality and 5 indicates the highest. The results, presented in Table 3.2, show that the cloned voices achieved an average MOS of 3.87 for English and 3.86 for Mandarin, indicating a satisfactory level of naturalness and demonstrating that the cloned voices can accurately replicate the speaker's voice fingerprint.

Next, we synthesized the activation commands and used them to activate an iPhone 8. In each test, Siri was authenticated using the voice fingerprints of the respective volunteers in advance, and then the synthesized activation command was played back 20 times per individual. We used the Successful Activation Rate (SAR)—defined as the proportion of successful activations out of total attempts for each participant—to assess the authenticity of the cloned voices. The results, shown in Table 3.2, reveal that all 10 cloned voices successfully triggered Siri, with an average SAR of 93.0% for English and 90.5% for Mandarin. Even in the least successful case (M3), the SAR was approximately 55%-65%. The lower recognition rate for volunteer M4 was attributed to his strong dialect accent not present in the training data. Nevertheless, these findings confirm that the final line of defense, voice fingerprinting on smartphones, can be easily compromised through voice cloning. This opens up the potential for creating magnetic-inductive inaudible voice command intrusions in voice-assisted devices.

3.5.3 Voice Cloning in Low-Resource Attack Devices

There are concerns about whether neural network-based voice cloning techniques can be integrated and operate on low-resource attack devices. In reality, the resource-intensive training phase of the voice cloning models can be conducted offline. Once trained, two practical methods can support the inference process within the parasite

Table 3.2: Naturalness evaluation results of the cloned voices.

Lang.	Metrics		M1	M2	M3	M4	M5	M6	F1	F2	F3	F4
en-US	MOS ↑	μ	3.93	3.74	3.58	3.74	3.89	3.93	4.09	4.25	3.74	3.81
		σ	0.07	0.36	0.09	0.17	0.10	0.14	0.20	0.11	0.15	0.20
	SAR (%) ↑		**100%**	**85%**	**65%**	**90%**	**95%**	**100%**	**100%**	**100%**	**95%**	**100%**
zh-CN	MOS ↑	μ	3.79	3.58	3.44	4.13	3.90	3.80	4.11	4.29	3.71	3.86
		σ	0.14	0.07	0.08	0.24	0.15	0.11	0.16	0.13	0.25	0.43
	SAR (%) ↑		**100%**	**65%**	**55%**	**100%**	**100%**	**95%**	**100%**	**100%**	**90%**	**100%**

label. The first approach involves using wireless connections such as Wi-Fi or Bluetooth to facilitate interaction between the embedded circuit and the attacker. The recorded reference voice from the speaker can be offloaded to a server for inference. Once the synthesis is complete, the generated activation voice can be transmitted back to the parasite label to initiate the attack. Alternatively, the inference process can also be fully executed at the edge node using model compression techniques like Knowledge Distillation [139] and Model Pruning [140].

3.6 Design of HeartwormAttack

In this section, we introduce the HeartwormAttack where malware called *heartworm* is implanted into a public wireless charger in advance. The heartworm takes control of the MCU to inject the voice commands by using the existing hardware components in accordance with the Qi standard, i.e., the de facto standard for wireless charging on the market.

3.6.1 Architecture of a Wireless Charger

Fig. 3.14 shows the schematic diagram of a wireless charger, which contains five main components: a power supply, an inverter, a resonance tank, a TX coil, and an MCU. The charger accepts a 12 voltage direct current (DC) as input. The inverter can convert the DC into an alternating current (AC) signal at some frequencies. Internally, the inverter contains four power field-effect transistor (FET) switches, denoted by S1∼S4, which can be turned on or off by the MCU. The inverter is controlled by the MCU to toggle between two states:

- *Positive.* When the switches of S1 and S4 are on, but S2 and S3 are off, the current flow (highlighted in red) passes through the coil from the bottom to the top, leading to an upward magnetic field around the TX coil.

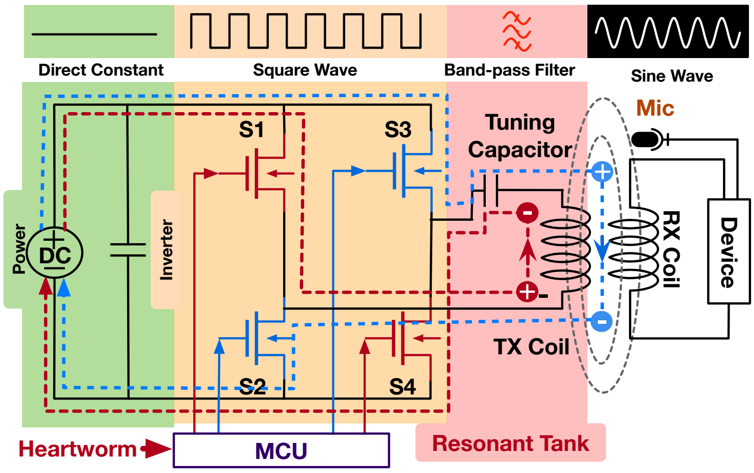


Fig. 3.14: Schematic diagram of a wireless charger

- *Negative.* When the switches of S2 and S3 are on, but S1 and S4 are on, the current flow (highlighted in blue) passes through the coils from top to bottom, leading to a downward magnetic field around the TX coil.

A square wave is created when the MCU controls the inverter to toggle periodically between the two states at a fundamental frequency f, as shown in the figure. The resonant tank acts as a frequency-selective network that only allows the wave at or around the fundamental frequency to pass. It is well known that a square wave can be decomposed into an infinite set of harmonic sinusoidal waves, that is, $\sin(2\pi \cdot ft)$, $\sin(2\pi \cdot 2ft)$, $\sin(2\pi \cdot 3ft), \cdots$. As a result, only the sinusoidal wave at frequency f, i.e., $\sin(2\pi ft)$, can successfully pass through the resonant tank and arrive at the TX coil and trigger an alternative magnetic field at frequency f.

3.6.2 Generating Analog Signals using a Digital MCU

A voice is an analog signal full of fine-grained amplitudes, but the MCU can only turn on or off the four switches to produce a digital signal with two amplitude levels (i.e., a positive level or a negative level). To address this challenge, we adopt pulse-width modulation (PWM), which can emulate any analog signal with digital means.

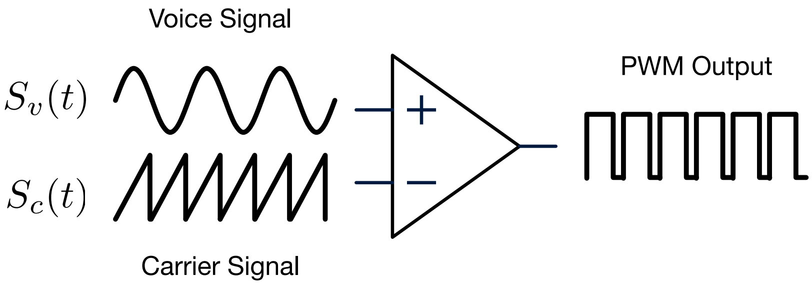


Fig. 3.15: The implementation of PWM modulation.

Acting as an amplitude-based modulation scheme, PWM generates variable-width pulses to represent the amplitude of an analog signal. PWM is a powerful technique for controlling analog circuits. It has been used in many applications, ranging from communications to power control and conversion. For example, the wireless charger MCU of SWBTC [141, 142] which holds the highest market shares, allows adjusting the duty cycle by 10% to 50%. The analog voice signal is emulated by using a series of pulses with different widths. The pluses are created by toggling the inverter at a fast rate. Let $S_v(t)$, and $S'_v(t)$ denote the real voice signal and the emulated voice signal. In addition, PWM also requires a carrier signal denoted by $S_c(t)$. Their relationship can be formulated as follows:

$$S'_v(t) = \mathrm{PWM}(S_v(t), S_c(t)) \approx S_v(t)S_c(t) \tag{3.5}$$

where PWM represents the modulation scheme. The PWM scheme can be modeled as a function, which accepts two inputs. One input is the analog signal to be emulated, denoted by $S_v(t)$, and the other one is the carrier denoted by $S_c(t)$. Fundamentally, the PWM function is implemented using a comparator as shown in Fig. 3.15. The output of PWM is a digital signal with high and low amplitudes. Formally, the function is defined as follows:

$$\mathrm{PWM}(S_v(t), S_c(t)) = \begin{cases} 1 & S_v(t) \geqslant S_c(t) \\ 0 & S_v(t) < S_c(t) \end{cases} \tag{3.6}$$

The most common PWM carrier is a sawtooth carrier, which ramps upward and then sharply drops periodically at a frequency f_c. The sawtooth carrier can be formally defined as follows:

$$S_c(t) = 2\pi f_c t - \lfloor 2\pi f_c t \rfloor$$

For clarity, we assume to emulate a single-tone sinusoid signal, i.e., $S_v(t) = \cos(2\pi f_v t)$. According to the derivation in [143], the output signal is:

$$\begin{aligned}
&\mathrm{PWM}(S_v(t), S_c(t)) = A_0 + A_1 \cos(2\pi f_v t) \\
&+ \sum_{m=1}^{+\infty} \frac{1}{m\pi} \left\{ \sin\left[m\left(2\pi f_c t\right)\right] - B_m \sin\left[m\left(2\pi f_c t\right) - m\phi_d\right] \right\} \\
&+ \sum_{m=1}^{+\infty} \sum_{n=\pm 1}^{\pm\infty} \frac{C_m}{m\pi} \sin\left[\frac{n\pi}{2} - m\left(2\pi f_c t\right) - n\left(2\pi f_v t +\right) + m\phi_d\right]
\end{aligned}$$

where A_0, A_1, B_m, C_m are the constant amplitude gain and ϕ_d is the phase shift. To verify the effectiveness of the PWM-emulated voice, we use the signal generator to transmit a single-tone signal through a TX coil. Fig. 3.16 compares the original signal, the PMW-emulated signal, and the signal recorded by the MEMS microphone. The amplitude of all signals is normalized because we focus on if the voice signal can be successfully recovered here. It can be seen that the signal is almost recovered without any loss. For simplification, we can consider the hacked charger as a wireless transmitter, which can modulate the signal generated via the MCU onto a carrier. Actually, the chargers can use this way to exchange the data with the devices being charged.

3.6.3 Using Nonlinearly Effect as a Downconverter

Suppose the microphone receives a combination of two sinusoidal signals at the frequencies of f_1 and f_2, which is formalized as follows:

$$S_{\text{in}}(t) = \cos(2\pi f_1 t) + \cos(2\pi f_2 t) \tag{3.7}$$

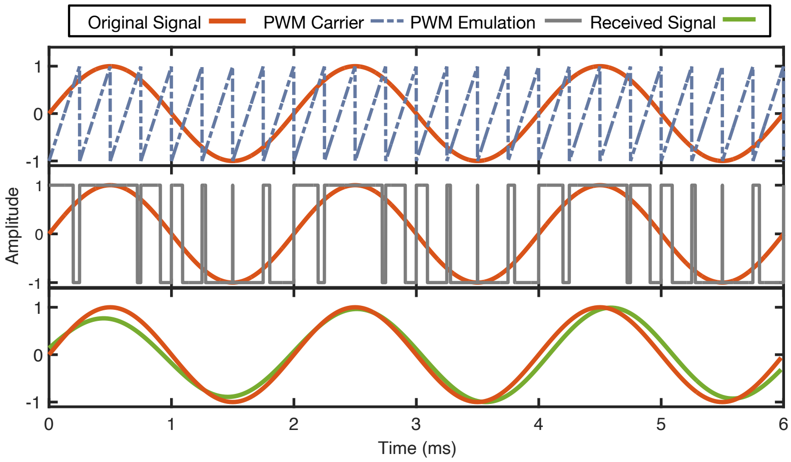


Fig. 3.16: Pulse-width Modulation (PWM)

Amplifiers inside microphones are expected to be linearly proportional to the input S_{in}, but known to exhibit the nonlinearity [33, 35]:

$$
\begin{aligned}
S_{\text{out}}(t) =& \overbrace{As_{\text{in}}(t)}^{\text{Linear}} + \overbrace{Bs_{\text{in}}^2(t)}^{\text{Nonlinear}} \\
=& A\left(\cos(2\pi f_1 t) + \cos(2\pi f_2 t)\right) + B\left(\cos(2\pi f_1 t) + \cos(2\pi f_2 t)\right)^2 \\
=& A\cos(2\pi f_1 t) + A\cos(2\pi f_2 t) \\
& + B + 0.5B\cos(2\pi 2 f_1 t) + 0.5B\cos(2\pi 2 f_2 t) \\
& + B\cos(2\pi(f_1 + f_2)t) + B\cos(2\pi(f_1 - f_2)t)
\end{aligned}
\tag{3.8}
$$

where $S_{\text{out}}(t)$ is the output signal from the amplifier, A is the gain for the input signal, and B is the gain for the quadratic term. It can be seen that the above signal has frequency components at f_1, f_2, $2f_1$, $2f_2$, $f_1 + f_2$ and $f_1 - f_2$. Before digitizing and recording, the microphone applies a low pass filter (LPF) to remove frequency components above its cutoff frequency 24 kHz. To put this into perspective, when $f_1 = 110$ kHz and $f_2 = 100$ kHz, f_1, f_2, $2f_1$, f_2, $f_1 + f_2$ are all greater than 24 kHz and thereby removed totally except $f_1 - f_2 = 10$ kHz. Consequently, what remains becomes:

$$S_{\text{out}}(t) = B + B\cos(2\pi(f_1 - f_2)t) \tag{3.9}$$

Therefore, we can view the amplifier plus the LPF as a frequency downconverter, which downconverts a combination of two signals at higher frequencies of f_1 and f_2

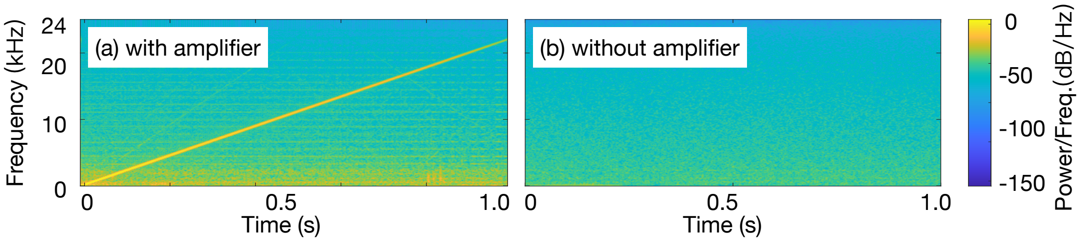


Fig. 3.17: Nonlinearity effect.

into a lower frequency at $f_1 - f_2$. Next, we will use this downconverter to pull down the high charging frequencies to the voice band.

On the charger side, we use the PWM to transmit the following signal:

$$\begin{aligned}\mathrm{PWM}(S_v(t)+1, S_c(t)) &= (S_v(t)+1)S_c(t) = S_c(t) + S_v(t)S_c(t) \\ &= \cos(2\pi f_c t) + S_v(t)\cos(2\pi f_c t)\end{aligned} \tag{3.10}$$

where 1 represents the DC component. On the microphone side, after the above signal passes through the "downconverter" (i.e., substituting Eqn. 3.10 into Eqn. 3.9), we obtain the finally recorded signal as follows:

$$S_{\text{out}}(t) = B + BS_v(t)\cos(2\pi(f_c - f_c)t) = B + BS_v(t) \tag{3.11}$$

where B is a constant and only affects the voice volume. In this way, we successfully close the frequency gap between the charger and the microphone.

To verify the nonlinearity effect, we transmit the chirp signal sweeping from 100 $\sim$ 122 kHz using the PWM and the TX coil. Meanwhile, we use the previously assembled microphone to capture the MIS. Fig. 3.17(a) shows that the microphone can successfully capture the downconverted chirp signal even if it is modulated onto a carrier at 100 kHz. Then, we use a flying wire to short-circuit the amplifier and repeat the experiment. As a result, no signal is detected anymore as shown in Fig. 3.17(b). This fully demonstrates the presence of the nonlinearity effect of the amplifier.

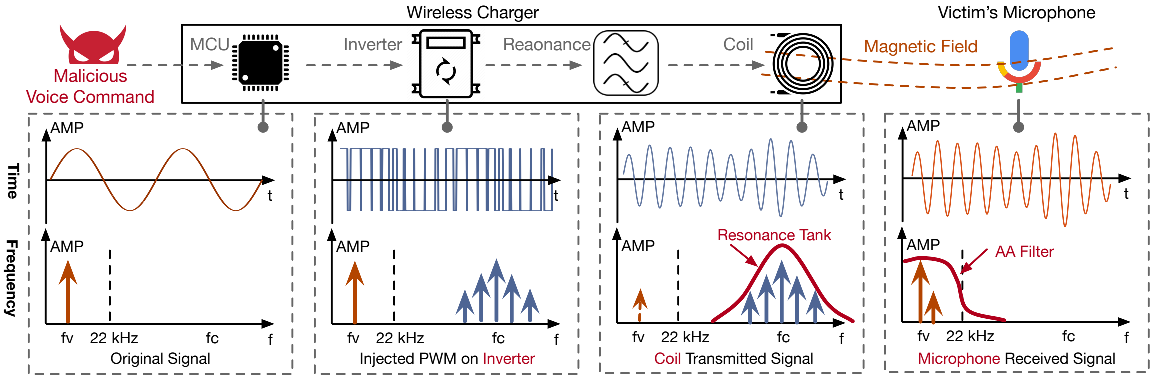


Fig. 3.18: Workflow of HeartwormAttack. The heartworm manipulates the MCU to generate the predefined PWM-emulated voice commands at the charging frequency (∼ 100 KHz) using the inverter, which is further propagated into the air. Finally, the MIS can be received and downconverted at the microphone (< 24kHz). Finally, the voice commands are executed by the voice assistants. The figure plots the time and frequency domain at different states.

3.6.4 Summary

We summarize the workflow of heartworm attack in Fig. 3.18. To inject a voice command, the heartworm takes control of the MCU to generate a PWM-emulated voice command and then manipulates the GPIO pins by using high-level programming instructions to generate the digital signals, which drive the TX coil to produce an amplitude-varying magnetic field. Consequently, an MIS that piggybacks the voice commands is captured by a nearby microphone. Then, the MIS is automatically downconverted to audible voice commands by the downconverter (i.e., amplifier plus LPF) due to the nonlinearity effect. Finally, the command is executed by the voice controllable systems. The voice commands modulated onto the magnetic field are injected into the microphone without triggering any mechanical vibration, so no in-air voice can be detected or heard.

3.7 Design of ParasiteAttack

In this section, we introduce a non-intrusive attacking approach called ParasiteAttack, which launches the attack through accessory equipment called parasite. The battery-free parasite is as thin and small as an NFC tag. The adversary adheres to the parasite on the top of a charger and disguises it as a sticker by printing some signs, such as "Free Charging" or "Quick Charging," which mislead users into viewing a parasite label as a part of the real wireless charger. Additional examples of deployment in library and subway station settings are depicted in Fig. 3.19 and Fig. 3.20, respectively.

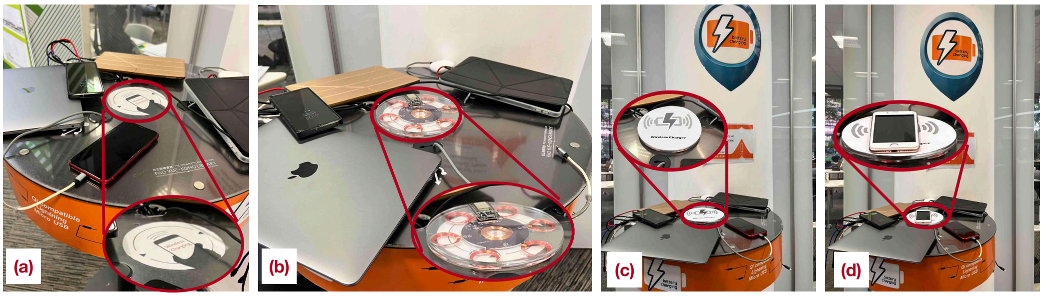


Fig. 3.19: ParasiteAttack in our library. (a) the public wireless charger; (b) the parasite label sticked onto the wireless charger; (c) the parasite label with a cover-up is disguised as a signboard; (d) a victim is using our parasite label to charge his smartphone.

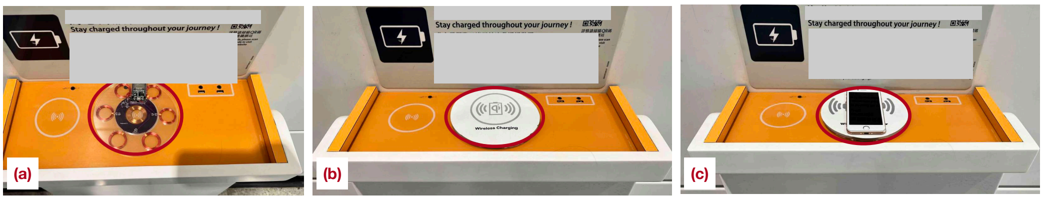
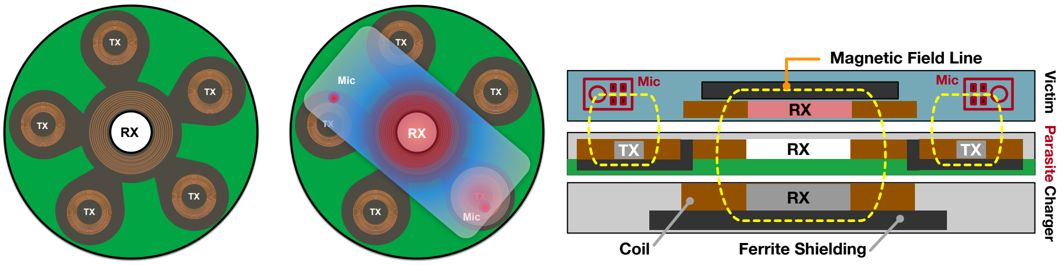


Fig. 3.20: ParasiteAttack in a subway station. (a) the public wireless charger sticked with a parasite label; (b) the wireless and the parasite label with a signboard cover-up; (c) a victim is using the parasite label to charge his smartphone.

3.7.1 Parasite in a Nutshell

The parasite is deployed between the host wireless charger and the smart device. We design the parasite as a battery-free device to be small, compact, and not eye-catching. Fig. 3.21 shows the architecture of a parasite. Specifically, a parasite label



(a) Top view (b) Top view (c) Side view

Fig. 3.21: Architecture of a parasite label. (a) and (b) show the top view of a parasite label without and with a phone respectively. (c) shows the side view of the attack scenario where the parasite presents between a phone and a charger. They are stacked in a pile.

is composed of an inner RX coil and several outer TX coils. After the power transfer contract is established, the parasite uses the inner RX coil to steal power from the underneath charger and boosts the attack using outer TX coils. The center of the RX coil is empty without a ferrite shield such that the magnetic field created by the host charger can reach the RX coil of the victim device with minimal attenuation. Multiple TX coils are deployed on a ring to ensure at least one TX coil is located nearby the victim's microphone even if the device's posture is uncertain. The TX coils are shielded from the RX coil and the host charger's TX coil by using ferrite sheets to avoid potential mutual interference.

3.7.2 Parasite Architecture

Fig. 3.22 shows the schematic diagram of a parasite's circuits. The RX coil and its corresponding resonant tank are designed to work at 100 kHz in accordance with the physical-layer guideline of the Qi standard. The harvested power is stored in the module of power management (PM), which boosts an MCU and a wireless communication module such as a Wi-Fi or Bluetooth transceiver, allowing the adversary to initiate the controllable voice attack in real-time fashion. The key module is the power converter, that is, AC-DC-AC converter. It has two purposes: first, it can

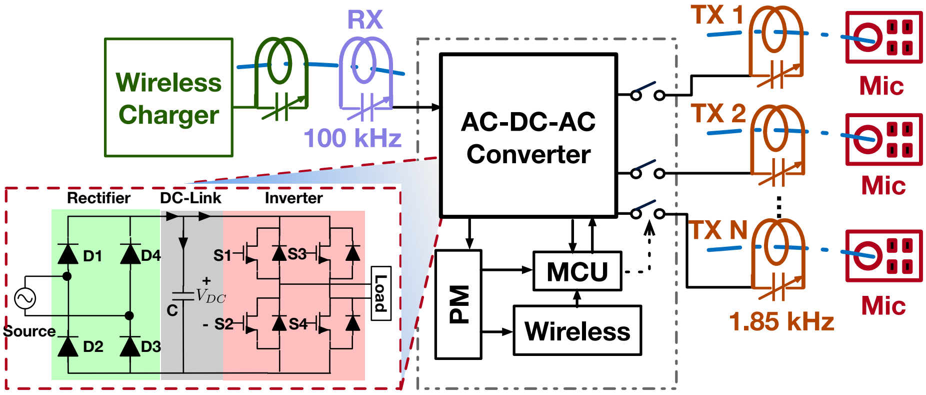


Fig. 3.22: Schematic diagram of a parasite

rectify AC to DC for boosting the MCU and the communication; second, it also converts the high-frequency current at 100 kHz harvested from the RX coil down to a low-frequency current at 1.85 kHz for TX coils. Therefore, the additional downconversion on microphones is needless because the parasite exactly transmits the voice in the operating range of a microphone directly. In the following, we will elaborate on the design of a parasite.

3.7.3 Stealing Power from a Host Wireless Charger

We adopt a Qi Example 4 coil as the RX coil, which consists of 66 strands of 0.88 mm diameter Litz wires. The inner and outer diameters of the coil are 47 and 28 mm, respectively. Thus, a 615 mm^2 hole is found in the center of the RX coil, which allows the above victim device to absorb energy as usual. In the view of the victim, the parasite is totally transparent. Inspired by the electric power transmission system [144] and motor control [145], we use an AC-DC-AC power converter to convert the AC inducted by the RX coil to DC. The power converter has three main components: a rectifier, a DC-link, and an inverter. Specifically, the rectifier consists of four diodes to provide full-wave rectification, that is the whole of the input waveform to one of constant polarity at its output. The DC-link consists of a capacitor, which can remove ripples caused by the rectifier and absorb the power surges between the

RX coil and the TX coils. The power surges are inevitable because the voice signal modulated on the TX coils might cause varying strength of the output power. The inverter inside the converter is used to generate a new AC at 1.85 kHz as a carrier to modulate the voice signal. A reverse diode should be added in parallel to each FET switch to protect it from reverse surges in case no-load disperses the redundant energy at TX coils.

3.7.4 Voicing Out through TX Coils

Similar to the HeartwormAttack, the MCU manipulates the inverter inside the power converter to create a PMW-emulated voice signal, which is further propagated into the air through the TX coils. Here, we skip the modulation procedure (which is as same as the heartworm attack) and focus on the key question: *how could we design the TX coils to maximize the magnetic strength at a victim's microphone?*

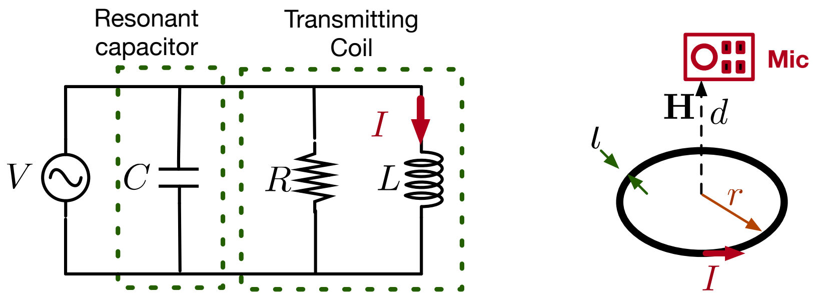
The input current is evenly distributed on the coil because the size of the coil is relatively small compared to the carrier wavelength. Hence, the coil itself can be regarded as a combination of an inductor and a resistor. An additional capacitor is added across the coil to form a resonator. In this way, the transmitter is usually modeled as the equivalent RLC parallel circuitry, as shown in Fig. 3.23(a). Correspondingly, the natural oscillation frequency of the circuity is determined by

$$f = \frac{1}{2\pi\sqrt{LC}} \tag{3.12}$$

We can tune the resonant frequency to any wanted frequency by changing the value of the capacitor. The efficiency of a magnetic transmitter is measured by using a physical parameter called *quality factor* denoted by Q, which is defined as follows:

$$Q = \frac{2\pi f L}{R} \tag{3.13}$$

When a current flows into a resonator, the resonant current passing through the coil will be amplified by $Q\times$ of the input current. Correspondingly, the magnetic field



(a) The equivalent circuit model

(b) Loop model

Fig. 3.23: The equivalent circuit model of a TX coil

strength can be enhanced by $Q\times$ compared with a resistive load although the input power stays the same [70]. However, a trade-off is found between the fundamental frequency f, half-power bandwidth B, and quality Q in an inductive system. Their relationship is represented as follows:

$$B = \frac{f}{Q} \tag{3.14}$$

The above equation suggests that the quality factor of a resonator is inversely proportional to the communication bandwidth. Considering that the narrowest band of the recognizable human voice is between 300 Hz and 3.4 kHz [120], then $f = 1.85$ kHz (i.e., the center frequency) and $B = 2.46$ kHz. Thus, the maximum Q that we can achieve is 0.75; otherwise, the voice might be incompletely propagated out.

Given an input power P, the magnetic field H generated by the TX coil at a victim's microphone to the coil can be modeled as follows [70]:

$$H \propto \sqrt{\frac{PQ}{r\left[\ln\left(\frac{8r}{l}\right) - 2\right]}} \frac{r^2}{(d^2 + r^2)^{\frac{3}{2}}} \tag{3.15}$$

where r is the radius of the coil, l is the wire radius, and d is the distance between the victim microphone and the coil. Clearly, we may increase P, r, l, Q, or decrease d to achieve a stronger magnetic field at the microphone. All the parameters are illustrated in Fig. 3.23. Our purpose is to enhance H by choosing appropriate parameters. Q cannot be increased because of the bandwidth constraint. l logarithmically contributes to H. Thus, even a significant raise in l only leads to minimal improvement at H. Moreover, l determines the thickness of the label, which should be as small as possible for better concealment. r is also constrained by the area of the top surface of the host charger. Thus, the only method of enhancing H is to shorten distance d. In other words, we should put the TX coil of a parasite tightly close to the victim's microphone as much as possible. However, the horizontal orientation of the victim device is unclear although knowing its RX coil must be overlapped with the RX of the parasite label for best-efficient charging. To address this issue, we deploy a number of TX coils on a ring around the RX coil, as shown in Fig. 3.21(a). As a result, we always find a close TX coil that is placed right below the microphone regardless of which horizontal angle the device is toward. The practical implementation might adopt a denser arrangement.

Transmitting voice commands at multiple TX coils concurrently might disperse the magnetic power. Thus, only a single TX coil is chosen to connect to the power converter each time using switches, as shown in Fig. 3.22. However, how can we know which TX coil should be chosen? When any metallic object is close to a TX coil, it will absorb some energy due to the vortex effect, resulting in the current or voltage change in the TX coil. In this way, we can determine which TX coil is under the victim device. The parasite polls all TX coils to choose the one that can cause vortex effect as the best TX coil for the voice attack.

3.7.5 Avoiding Foreign Object Detection

In the Qi standard, the wireless charger is required to detect foreign objects for safety charging [112], which prevents deformation or damage from occurring due to excessive heat generation in the event a metallic object is placed between the TX and RX coils. Such detection might consider our parasite label as a foreign object and stop the charging. Two methods are used for foreign object detection (FoD) in the

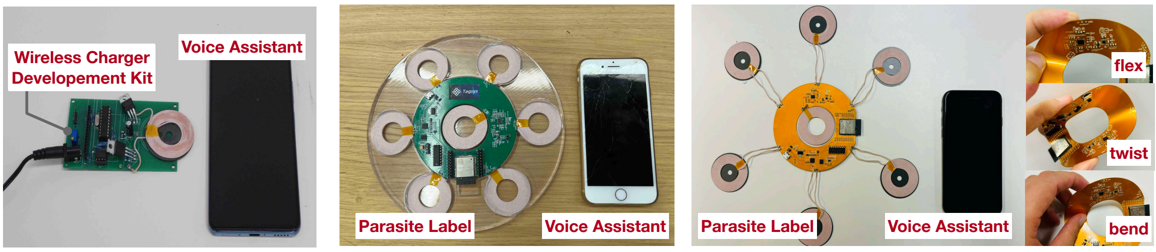
Qi standard [146]. (1) *Checking quality factor.* Similar to our previous approach for detecting the microphone location, the wireless charger can examine the frequency or quality factor of its resonant tank to determine the presence of the foreign object. The RX coil of the parasite label is well-tuned to align with the TX coil of the wireless charger already. Thus, the parasite will not trigger the report of a foreign object. (2) *Checking power loss.* The smart device approximates the received power and sends it to the wireless charger, which computes the power loss between the transmitted and the received power. If the loss exceeds a threshold (i.e., 500 mW), a foreign object is reported. The parasite label can forge a false power report or interfere with the report from the smart device to avoid detection. As demonstrated in the evaluation, we find that it is easy to avoid the FoD since the commercial chargers usually adopt a relatively higher threshold.

3.8 Implementation and Evaluation

3.8.1 Implementation

We developed the heartworm malware using a development kit for wireless charging and prototypes the parasite label:

HeartwormAttack. Fig. 3.24(a) shows the development kit for wireless charging. This kit comprises of a STC12C2052AD MCU [147] with 72 MHz clock frequency (i.e., f_{CLK}), an inverter with JRF540N FET switches [148], and a standard A11 coil from TKD [149]. The maximum output power is 30 W. We also developed a heartworm malware using the PWM timer API in MCU. The carrier frequency of PWM (i.e., f_{PWM}) is 1 MHz, while the duty cycle can be varied from 0% to 100%. Therefore, we use $\log_2(f_{\mathrm{CLK}}/f_{\mathrm{PWM}}) = 6$ bits to control the inverter. The analog voice commands are firstly sampled with a 16 kHz rate and then PWM-emulated. The commands are finally generated by the MCU.



(a) HeartwormAttack (b) ParasiteAttack PCB (c) ParasiteAttack FPC

Fig. 3.24: Prototypes. (a) a wireless charger development kit is employed for the HeartwormAttack; (b) The rigid PCB prototype for ParasiteAttack; (b) The flexible FPC prototype for ParasiteAttack.

ParasiteAttack. As shown in Fig. 3.24(b), we prototype the parasite label using a 4-layer annular PCB, which holds the main circuits (e.g., MCU, rectifier, and inverter). The inner hole accommodates a Qi Example 4 RX coil from TDK [150] to harvest power from the real charger, while six TX coils are arranged along the outer margin of the PCB to launch voice attacks at microphones. All coils comprise 2 mm thin Litz wires. The full-wave rectifier comprises 1N400x diodes [151] and TS61005 power FET switches [152]. The power converter (i.e., AC-DC-AC converter) is a reconfigurable platform controlled by an external low-power ESP32-C3 microcontroller [153], which is integrated with a Wi-Fi module internally. Therefore, we can control the parasite label remotely through Wi-Fi. An LM7805 voltage regulator [154] is adopted for power management, which can stabilize the rectified current and power up the ESP32. Similarly, the analog voice commands are sampled with a 16 kHz rate. The carrier frequency of PWM is 100 kHz, and 10 bits are used to control the inverter. The thickness of the PCB parasite label is approximately 2 mm. Although relatively compact, there remains a risk of detection via visual inspection and impedance variation checks. Therefore, we have also implemented the parasite on a Flexible Printed Circuit (FPC), as illustrated in Fig. 3.24(c). Utilizing FPC technology enables us to reduce the thickness of the parasite label to that of an A4 sheet of paper, significantly enhancing its stealthiness. Moreover, FPCs offer the advantage of being able to flex, bend, and twist without damaging the circuitry. This flexibility allows for their application in diverse public environments, including foldable wireless charger docks and chargers with irregular shapes.

3.8.2 Experiment Setup

We test our attacks across eight types of smartphones and three types of smartwatches, which were all released after 2018 when the functionality of wireless charging was ready to be generally adopted among smart devices. The three types of tablets are from the series of Apple iPad series. Unfortunately, iPads have not offered the wireless charging function to date. Nevertheless, we still test the attacks on these tablets considering a generalized scenario, where they are accidentally placed near a wireless charger. We finally test three types of add-on microphones, which are the most popular components for developing smart wearables. We connect these microphones to an Arduino for voice recording. We test the following three power levels: 15, 30, and 50 W. The Qi standard specifies the 15 W default power and the 30 W maximum power, while the enhanced quick chargers on the market adopt 50 W power [114]. Unless specified, the distance between the charger and the victim devices is less than 5 cm, the transmitting power is set to 15 W, and iPhone 8 is employed by default. We use an AR824 sound level meter [155] to measure the environmental noise strength in the unit of dBA, which represents the relative loudness of sounds in air as perceived by the human ear on average. All experiments are conducted in a quiet lab room with a background noise level of 45 dBA.

3.8.3 Feasibility Results

Table 3.3 summarizes the experiment results. The attack is viewed as a “success” (ticked with $\surd$) once the speech recognition (SP) system can successfully recognize the short wake-up voice commands (e.g., “Hey Siri”, “Hey Google” and “Hi Xiaoai”) recorded by the microphones under attacks. The table reveals the following findings:

Table 3.3: Experimental devices, speech recognition and results. The Qi column indicates if the smart device is compatible with wireless charging.

Type	Manuf.	Model	Rel.Date	OS	SR	Qi	ParasiteAttack			HeartwormAttack		
							Recog.	Power	Dist.	Recog.	Power	Dist.
Smartphone	Xiaomi	V9 Pro	2019/09	MIUI 12.0	Xiaoai	Yes	$\surd$	$\geqslant 15$W	< 1cm	$\surd$	$\geqslant 15$W	3cm
Smartphone	Xiaomi	V11	2021/01	MIUI 12.5	Xiaoai	Yes	$\surd$	$\geqslant 15$W	< 1cm	$\surd$	$\geqslant 30$W	4cm
Smartphone	Huawei	Mate 20 Pro	2018/10	Harmony OS 2.0	Xiaoyi	Yes	$\surd$	$\geqslant 15$W	< 1cm	$\surd$	$\geqslant 15$W	3cm
Smartphone	Huawei	Honor V30 Pro	2019/11	Magic UI 3.0	YOYO	Yes	$\surd$	$\geqslant 15$W	< 1cm	$\surd$	$\geqslant 15$W	5cm
Smartphone	Apple	iPhone 8	2017/09	iOS 15.1	Siri	Yes	$\surd$	$\geqslant 15$W	< 1cm	$\surd$	$\geqslant 15$W	2cm
Smartphone	Apple	iPhone 11	2019/09	iOS 15.0	Siri	Yes	$\surd$	$\geqslant 50$W	< 1cm	$\times$	N.A	3cm
Smartphone	Apple	iPhone 12	2020/10	iOS 15.1	Siri	Yes	$\surd$	$\geqslant 50$W	< 1cm	$\times$	N.A	3cm
Smartphone	Samsung	Galaxy 21	2021/01	One UI 3.1	Bixby	Yes	$\surd$	$\geqslant 50$W	< 1cm	$\times$	N.A	3cm
Smartwatch	Samsung	Galaxy Watch 4	2021/08	One UI 3.0	Bixby	Yes	$\surd$	$\geqslant 15$W	< 1cm	$\surd$	$\geqslant 15$W	< 1cm
Smartwatch	Huawei	GT2 Pro	2020/12	Harmony OS 2.0	Xiaoyi	Yes	$\surd$	$\geqslant 15$W	< 1cm	$\surd$	$\geqslant 15$W	< 1cm
Smartwatch	Apple	Watch 7	2021/10	WatchOS 8.0.1	Siri	Yes	$\surd$	$\geqslant 15$W	< 1cm	$\surd$	$\geqslant 30$W	< 1cm
Tablet	Apple	iPad(6th)	2018/03	iPadOS 15.0.1	Siri	No	$\surd$	$\geqslant 15$W	< 1cm	$\surd$	$\geqslant 15$W	3cm
Tablet	Apple	iPad Air 4	2020/10	iPadOS 15.0.1	Siri	No	$\surd$	$\geqslant 50$W	< 1cm	$\surd$	$\geqslant 50$W	3cm
Tablet	Apple	iPad mini 6	2021/09	iPadOS 15.1.0	Siri	No	$\surd$	$\geqslant 15$W	< 1cm	$\surd$	$\geqslant 50$W	3cm
Add-on Mic	SparkFun	ADMP401	2010/04	Windows 10	Google STT	No	$\surd$	$\geqslant 15$W	< 1cm	$\surd$	$\geqslant 15$W	3cm
Add-on Mic	Knowles	SPH0690LM4H-1	2019/06	Windows 10	Google STT	No	$\surd$	$\geqslant 15$W	< 1cm	$\surd$	$\geqslant 15$W	3cm
Add-on Mic	Joy-IT	KY-037	2017/06	Windows 10	Google STT	No	$\surd$	$\geqslant 15$W	< 1cm	$\surd$	$\geqslant 15$W	3cm

• First, the attacks are successfully conducted in 91% cases (31 out of 34), where each device can be successfully attacked in at least one case. We believe this list is by far not comprehensive. Nevertheless, the results serve as a warning to consider the security breach caused by wireless charging.

• Second, the ParasiteAttack performs better than the HeartwormAttack. The average minimum power that the HeartwormAttack and ParasiteAttack require are about 28.2 W and 23.2 W, respectively. Namely, the HeartwormAttack needs additional 5 W power for the voice injection. This is because magnetic interference generated by the HeartwormAttack experiences two extra attenuations, which are caused by the non-linearity of a microphone's amplifier and the $2\times \sim 3\times$ further distance compared with ParasiteAttack.

• Third, high-end smartphones adopt substantially effective packaging techniques and EMI shield materials, which is reflected in HeartwormAttack failures on iPhone 11, 12, and Galaxy 21. They are well protected against the HeartwormAttack even when using 50 W transmitting power. Unfortunately, these devices still suffer from ParasiteAttack when the TX coil of the parasite is placed close (< 1 cm) to the microphone.

Overall, regardless of the types of models, manufacturers, and speech recognition

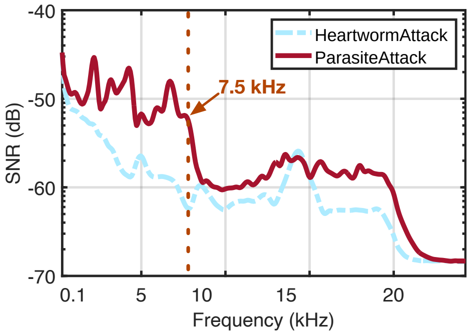


Fig. 3.25: Frequency response

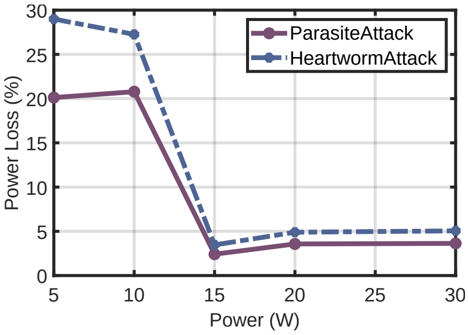


Fig. 3.26: Charging efficiency

systems, the commercial off-the-shelf devices all fail to defend against the proposed attacks when given sufficient power. Particularly, the transmitting power plays a key role in attacking. In the industry, the current aggressive pursuit of faster charging via raising the transmitting power will intensify the potential magnetic interference and thus considerably increase the rate of attacking success. This reminds us of the potential negative consequence of faster or quick charging. In addition, whether victim devices support wireless charging is not a prerequisite for our attacks. On the contrary, those devices without WPT functionality become more vulnerable when getting close to a wireless charger because they have very little protection against magnetic interference.

3.8.4 Frequency Response Analysis

Next, we quantify the quality of the injected voice by analyzing the frequency response, that is, the quantitative measure of the output spectrum of a system or device in response to a stimulus. In the experiment, we transmit a chirp sound sweeping from 100 Hz to 22 kHz with the two attacking approaches. Fig.3.25 compares the two frequency responses. We find that: (1) ParasiteAttack achieves a higher SNR in the range of 100 Hz to 7.5 kHz, which exactly covers the human speech spectrum. This demonstrates that the parasite label is rationally designed and meets the attacking requirements. (2) By contrast, the response of a HeartwormAttack is relatively

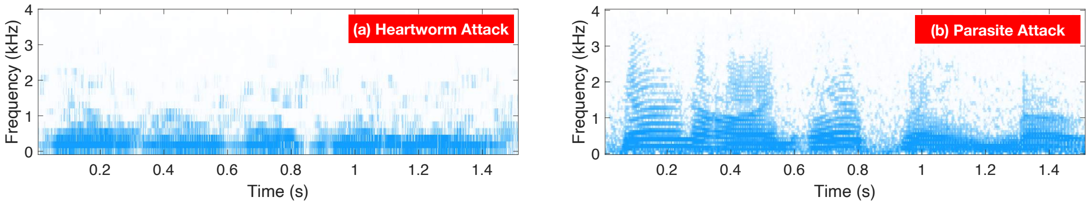


Fig. 3.27: Spectrograms of the voice signals. (a) and (b) show the voice injected HeartwormAttack and ParasiteAttack

unsatisfactory. Notably, a wireless charger's TX coil is not designed for our attack but to provide more power. Thus, the quality factor of its coil is over 77, and the operating frequency is 100 kHz. Based on Eqn. 3.14, its half-power bandwidth is as small as $100/77 \approx 1.2$ kHz [156]. Theoretically, the power of frequency components above 2.4 kHz is nearly zero.

Fig. 3.27 shows the spectrograms of two recorded voices, which are injected by HeartwormAttack and ParasiteAttack, respectively. As analyzed above, we clearly observe a cutoff at 2.4 kHz in Fig. 3.27(a). This suggests that the optimal voice that the HeartwormAttack injects into microphones should be less than 2.4 kHz. Nevertheless, the current voice recognition systems usually ignore high-frequency components and exhibit strong fault tolerance. Thus, HeartwormAttack still works well in practice for keyword-based commands.

3.8.5 Stealthiness Analysis

We would like to evaluate the stealthiness of our attacks, that is, if being cautious of the attacks is easy. First of all, we invited 20 subjects including 10 males and 10 females, who are aged between 15 and 40. These subjects were requested to stay nearby the wireless charger (< 1 m) and report if any voice or noise was heard during the attack. As a result, none of them heard any sound and realized the attacks had occurred. Thus, the attacks or the voice commands are completely inaudible.

However, the attacks might still be discovered through the two implicit side channels.

(1) Power Efficiency. Both attacks consume a certain amount of power from the wireless charger and thereby affect the charging efficiency, making the user feel that it takes a longer time to charge than usual. In the experiment, we charge a victim smartphone *with* or *without* attacks. In each trial, the initial percentage of the remaining battery power is fixed at 50%. We then observe how much power percentage can be recharged after half an hour. Let $P_{\mathrm{w/o}}$ and P_{w} respectively denote the increased power percentage without and with a sustained attack, i.e., playing wake-up commands continuously. Apparently, $P_{\mathrm{w/o}} > P_{\mathrm{w}}$ because the attack consumes additional power. Choosing $P_{\mathrm{w/o}}$ as the baseline, we compute power loss as the ratio of $1 - P_{\mathrm{w}}/P_{\mathrm{w/o}}$. Fig. 3.26 shows the power loss of the two attacking approaches. As a result, the power loss is below 5%, which is substantially small to be noticed by users when the charging power is larger than 15 W. Interestingly, the HeartwormAttack consumes more power than the ParasiteAttack because the PMW-emulated signals do not fit the follow-up resonate tank effectively and additional energy is dissipated into the air in the form of heat. **(2) Magnetic Leakage**. The RX and TX coils of the parasite label might introduce a stronger magnetic field around the victim device, which might alert users of abnormal magnetic flux. To this end, we use an HT201 Gaussmeter [157] to measure the magnetic flux density (denoted by B) as a function of the distance to the charger. The measurements are repeated 20 times, and the median is reported for each distance. Fig. 3.28 shows the median density with a varying distance from 0 to 10 cm. Consequently, the magnetic density caused by ParasiteAttack is almost similar to that of the HeartwormAttack when the distance is less than 4.9 cm because the TX coil of the charger is far larger than that of TX coil of the parasite label, thereby dominating the magnetic field. In short, the abnormal magnetic fields caused by the two attacks are drowned in the charger's field when the distance is less than 4.9 cm. Beyond this distance, the density caused by a parasite label attenuates to an extremely small value (i.e., 65 μT) close to the geomagnetic field [158]. Overall, being cautious of the attacks is difficult for users regardless of the power loss or magnetic leakage.

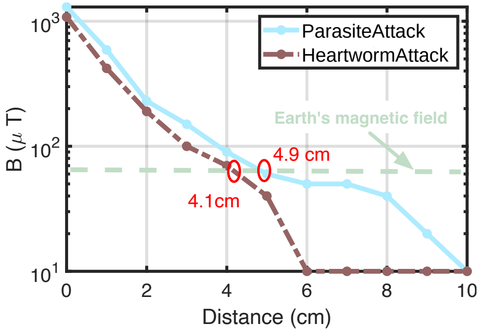


Fig. 3.28: Magnetic leakage

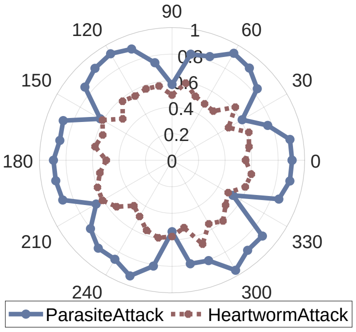


Fig. 3.29: Orientation

3.8.6 Avoiding Foreign Object Detection

The current wireless charging techniques require the chargers to detect foreign objects for safety charging, which considers the parasite label as the foreign object by "mistake". Therefore, we test if the detection across five commercial wireless chargers: Fast Charge 2.0 (C1) [159] from Samsung, Charging Stand (C2) [160] from Baseus, Charging Pad (C3) [161] from UGREEN, MagSafe (C4) [162] and MagSafe Duo (C5) [162] from Apple. In the experiment, we place the parasite label on the top of a charger and use a wireless charging power test module [163] to check whether FoD is triggered and measure the charging power loss. Specifically, we utilize the wireless charging power meter to measure the power transferred from the wireless charger to the smartphone, both with and without parasite attacks. The measurement log is presented in the table 3.4. It is evident that the overall power loss caused by the parasite attack remains below 500 mW. Therefore, detecting the presence of the parasite label as a foreign object solely based on power loss is challenging.

The FoD results are further shown in Table 3.5 where × denotes the detection failure. Consequently, the average power loss caused by ParasiteAttack is only around 1.08% of the overall power consumption and all these charges failed to detect the presence of our parasite label. This result shows that the current FoD mechanism is remarkably easy to dodge.

3.9 Impact Analysis

The performance is further measured using the recognition success rate, which is defined as the percent of words successfully recognized by the Google Speech-to-Text toolkit [164].

3.9.1 Impact of Horizontal Orientation

In wireless charging, the horizontal orientation of smart devices is uncertain in practice, which may affect the attack performance. In this experiment, we launched the two attacks in this experiment by placing the phone at different angles under a 30 W charging power. Fig. 3.29 shows the recognition rate in different angles. The rate under the HeartwormAttack remains highly similar at all angles because the distance between the TX coil and the microphone is irrelevant to the orientation in this attack. By contrast, the rate under the ParasiteAttack fluctuates remarkably in angles, resulting from the petal-shaped TX design. (see Fig. 3.24(b-c)). Consequently, even the minimum rate measured in the ParasiteAttack when the microphone is located in the space between two adjacent TX coils is slightly greater than that of HeartwormAttack.

Table 3.4: Wireless charging power test log.

Without parasite attack					
Time	Mode	U (V)	I (A)	Power (W)	Freq (kHz)
14:48:05	EPP	8.54	1.66	14.1	139.6
14:48:10	EPP	8.54	1.66	14.1	139.4
14:48:15	EPP	8.54	1.6	13.6	140
14:48:20	EPP	8.44	1.66	14.0	139.8
With parasite attack					
Time	Mode	U (V)	I (A)	Power (W)	Freq (kHz)
14:50:05	EPP	8.54	1.59	13.6	137.5
14:50:10	EPP	8.19	1.63	13.4	138.0
14:50:15	EPP	8.19	1.72	14.1	137.9
14:50:20	EPP	8.54	1.59	13.6	138.0

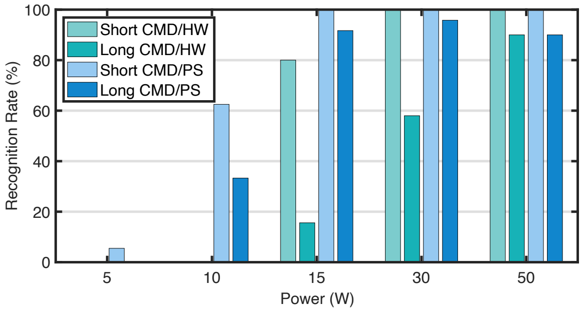


Fig. 3.30: Impact of charging power

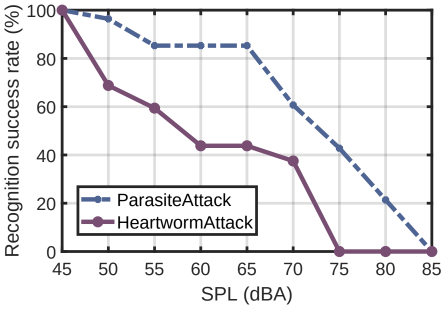


Fig. 3.31: Environmental noise

3.9.2 Impact of Charging Power

The previous validation experiment summarizes the minimum charging power required to recognize the wake-up commands successfully. Here, we further evaluate the impact of charging power by testing short and long voice commands, "Open the Door" (3 words, Short CMD) and "Call 1234567890" (11 words, Long CMD). The commands are repeated ten times, and the mean rate is reported. Fig. 3.30 shows the recognition rate in the five power settings where HW and PS are short for HeartwormAttack and ParasiteAttack, respectively. The results confirm that the charger power is the most important parameter for the two attacks. Specifically, the recognition rate increases as the charging power is raised; second, the minimum power to recognize the short and the long commands are 5 W and 10 W in the ParasiteAttack, while that is 15 W and 15 W in the HeartwormAttack. Namely, the HeartwormAttack requires more power due to the attenuations caused by the downconversion and the longer distance.

Table 3.5: FoD Results.

Model	Loss(mW)	Loss(%)	FoD
C1	337.0 mW	1.12%	×
C2	331.8 mW	1.10%	×
C3	320.5 mW	1.06%	×
C4	155.6 mW	1.03%	×
C5	163.3 mW	1.08%	×

Table 3.6: Noise Results.

Scene	SPL(dBA)	HW.	PR.
Library	35-45	100%	100%
Park	45-55	68.8%	96.4%
Cafe	55-65	43.8%	85.3%
Subway	60-75	37.5%	60.7%
Bus	70-85	0	21.4%

3.9.3 Impact of Environmental Noise

Speech recognition is known to be sensitive to background noises and is recommended to be used in a quiet environment. Thus, we examine the inaudible voice command injection with the two attacks regarding the controllable and the uncontrollable Environment noises. **(1) Controllable Environment**: In this experiment, we used a speaker to play recorded traffic noise and controlled the noise strength by adjusting the speaker volume. Fig. 3.31 shows the recognition results of the two attacks under different environmental sound pressure levels (SPL). As desired, the rate linearly decreases as the noise strength increases. Certainly, the results also depend on how strong the speech recognition system is resilient to noise. Considering the injection, the recognition rates under the HeartwormAttack and ParasiteAttack are over 60% when the noise is lower than 55 and 70 dBA, respectively. **(2) Uncontrollable Environment.** We then conducted the experiment in five real-life environments: library, park, cafe, subway station, and bus. The recognition results are listed in Table. 3.6. Specifically, ParasiteAttack performs well in the various scenarios except for the bus, whereas HeartwormAttack is more adapted to a relatively quiet environment like the library or park. The noise reaches a maximum level of 70-85 SPA on a bus where both two attacks underperform. Overall, noise is a long-standing challenge that voice recognition systems are facing. Both attacks more or less introduce extra noise into the injected voice, leading to a lower recognition rate.

3.9.4 Impact of Carrier Frequency

(1) Charging Carrier. Qi standard allows a charger to choose a frequency between 100 - 200 kHz to transfer power [112], which might affect the performance of the HeartwormAttack because the voice command is piggybacked by the charging carrier. In this experiment, the heartworm transmits a 1 kHz signal tone but at different-frequency charging carriers. Fig. 3.32 shows the signal-to-noise (SNR) of

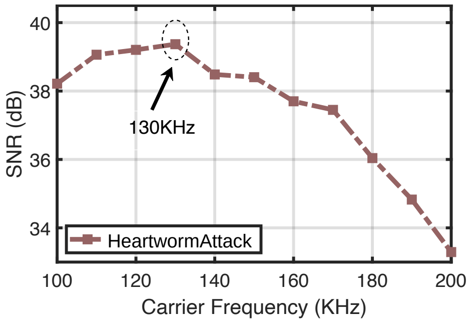


Fig. 3.32: Charging carrier

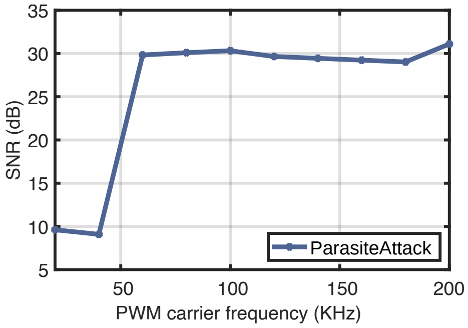


Fig. 3.33: PWM carrier

the recorded MIS as a function of the carrier frequency. We observe that the 130 ± 30 kHz carriers best fit the attack. This result confirms our previous assumption that a charger improves the charging efficiency at the cost of bandwidth. Therefore, the HeartwormAttack should be launched during 100 ∼ 130 kHz around. **(2) PWM Carrier**. The frequency of PWM carrier is a key parameter to emulate the voice command in the ParasiteAttack. There is a trade-off in choosing the carrier frequency, namely, a higher frequency better emulates the voice signal but consumes much power. Fig. 3.33 shows the SNR of the recorded MIS as a function of PWM frequency. It can be seen that the SNR is maintained at the maximum (i.e., ∼ 30 dB) when the carrier frequency is above 60 kHz, which is triple higher than the maximum frequency of the voice (i.e., 24 kHz). However, the clock frequency of the MCU is 1 MHz, and the carrier frequency must be an integral division of the clock frequency. Thus, the optimal frequency is 100 kHz.

3.10 Limitations & Countermeasure

3.10.1 Limitations of Proposed Attacks

We successfully inject magnetic-inductive inaudible commands into smart devices via their microphones. However, the two proposed attack approaches are still limited in many aspects as follows. These limitations will help us to find the corresponding countermeasures. **(1) Short attack range.** The intensity of the magnetic field degrades rapidly at $\mathcal{O}(1/d^6)$ with the distance d [70]. Thus, the attacks are launched successfully only when the smartphone is placed exactly on the wireless charger where the distance is less than 5 cm as reported. **(2) Voice fingerprinted activation.** Nowadays, iPhone or other models have started to use the fingerprinted voice to activate the assistant, which is an effective way to defend against all inaudible voice attacks including ours. Thus, the adversary must obtain the voice fingerprint and imitate the wake-up commands in practice. Voice cloning [126] can mitigate this constraint but require short voice clips from the victim through a side channel. **(3) Higher charging power.** As mentioned early, the charging power plays a key role in the attack. To achieve a higher success rate, both attacks require a minimum charging power of 10 W, 15 W, or even 50 W. **(4) Aimless attack.** All inaudible voice attacks are unidirectional, that is, the attack device (e.g., charger) cannot obtain any feedback from the victim devices. As a result, the attacks are initiated aimlessly. For example, "turn speaker off", "download a software" and "transfer money". The three consecutive voice commands are less logically connected. **(5) Need for extra equipment.** The ParasiteAttack must be initiated by the parasite label, which is stuck onto the wireless charger. Even if installed snugly, the parasite label is still likely to be found by careful users because the depth of charging is increased by $2 \sim 3$ cm. **(6) Additional protection for high-risk tasks.** Some high-risk tasks, especially for financial issues (such as payment, bank transfer, photo access, etc.) require the double-check with the password or the face-based authentication although they can be initiated by the VA. **(7) Background noise.** The noises introduced by our attack may impact the quality of the injected voice. While, in most cases, the adversarial commands are still clean enough to pass the voice biometrics.

3.10.2 Countermeasure Recommendations

Inspired by the limitations, we design the following countermeasures to defend against the potential magnetic interference. **(1) Upgrading hardware design.** The magnetic interference has not attracted enough attention at present because wireless charging has been quickly spread in recent years. As mentioned early, the outdated EMI countermeasures (including the Faraday cage and the EMI filter) can only protect the microphones from interference at 1 MHz above. Thus, the most effective countermeasure is to upgrade the hardware design for newly developed smart devices. For example, mounting the MEMS chip and the ASIC chip inside a ceramic substrate; sealing a microphone with a polymer foil [165]; adopting the material (e.g., mu-metal for oscilloscope protection) with higher magnetic permeability for the device's casing. **(2) Throughout fingerprinted.** To date, the verification of voice fingerprints is limited to the wake-up commands such as "Hi, Siri!". Once the voice assistant is activated successfully, the follow-up voice interactions will skip the verification for a quick response. We should take fingerprint verification all the time. **(3) Abnormal voice detection**. Both HeartwormAttack and ParasiteAttack introduce some particular acoustic characteristics, which can be utilized to detect the presence of the attacks. For example, the voice injected by HeartwormAttack and ParasiteAttack is cut off at 2.4 kHz and 4 kHz, respectively, where the absence of higher frequencies can be used as a typical feature of the abnormal voice command. Actually, a similar countermeasure has been studied in some previous work [40, 166, 167] to defend against other attacks. **(4) Abnormal commands**. As mentioned, the attacks cannot obtain feedback from smart devices. They have to attempt the pre-defined commands successively. These commands are not logically connected. We can detect malicious commands via analyzing the purposes of these commands and their connections. **(5) Sophisticated FoD**. The current FoD algorithms fail to detect the presence of a parasite label. We could develop a more sophisticated algorithm through various parameters, including power consumption, magnetic density, and so on. We could also encrypt the data exchanged between the charger and the device. **(6) Disabling microphone**. The microphones or the voice assistants shall be automatically disabled when the devices are being charged. **(7) Limitation on charging power**. Finally, the industry is advised to properly limit the charging power to avoid the negative consequence of quick charging.

3.11 Conclusion

In this work, we first demonstrated that low-frequency magnetic inductive coupling (i.e., magnetic interference) from wireless chargers is a practical threat to the microphone system and can be manipulated to inject malicious voice commands into smart devices. This work will raise awareness of such great potential safety hazards on smart devices.

Chapter 4

Magnetic HF Coupling: NFC-to-Camera Mobile Payment System

4.1 Introduction

As the COVID-19 pandemic swept the world, consumers grew increasingly concerned with traditional methods of in-person payment, including cash and dipping or swiping their card at the point of sale. Instead, they have looked toward contactless *mobile payments* via smartphones as safer alternatives. A February 2020 report from Juniper Research forecasted global contactless transaction values would triple from $2 trillion in 2020 to $6 trillion by 2024 [168].

Nowadays, two major technological players, namely, NFC and barcode, are on the market as contactless communication technologies for mobile payment.

- **NFC**. The NFC uses short-range high-frequency wireless communication to exchange data between NFC readers and smart devices, e.g., Apple Pay and Google

Fig. 4.1: Barcode-based Mobile Payment

Pay e-wallets. NFC has been adopted widely since the introduction of contactless credit cards. Over the past decades, NFC readers have become the most common payment terminals everywhere, e.g., retail stores, restaurants, etc.

- **Barcode**. The 1D or 2D barcodes visually encode bits of information in the form of stripes or blocks, which can be identified by the built-in cameras of smartphones. In particular, the QR code (a type of 2D barcode) has been rapidly adopted for mobile payment in the recent decade because of the rapid development of microelectronic techniques. Fig. 4.1 shows some examples of payment barcodes.

NFC-based vs. Barcode-based Payment. (1) The barcode-based mobile payment is known for its high usability across different types of smartphones because cameras have become compulsory components of smartphones. However, this type of payment is susceptible to many security risks, such as replay attacks [169–171], synchronized token lifting and spending attacks [172], and so on. Because of these potential risks, China's central bank has tightened rules on mobile payments made by scanning a barcode and limiting the use of static QR codes in mobile payments [173]. All these concerns are derived from the visibility of optical codes at long distances, allowing an attacker to capture codes sneakingly from a place far away. In contrast, the NFC-based payment has been adopted for decades and has been demonstrated to be a secure payment solution due to the nature of the near field (i.e., a few centimeters). (2) Barcode-based payments also require additional efforts to focus the camera on the barcodes, which is difficult for the amblyopia group (e.g., the elderly) who are suffering from cataracts, presbyopia, and other visual disturbances. By contrast, tapping

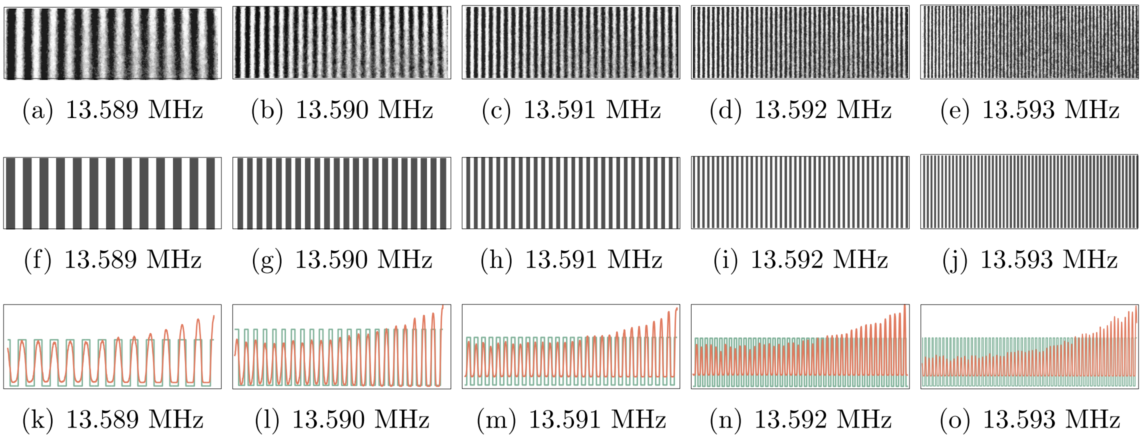


Fig. 4.2: Grayscale images, binarized images, and pixel signals under the magnetic interference. The pictures are taken using an iPhone X with an interfered frequency varying from 13.589 MHz to 13.593 MHz. The first row of (a)-(e) shows the top 1000 rows of the original images in grayscale, on which there appear several alternating stripes caused by the magnetic interference; the second row of (f)-(j) shows the barcode images after binarization processing; and the third row of (k)-(o) shows the mean pixel signals extracted from the gray-scale images (in red) and that extracted from the barcode images (in green).

smartphones on an NFC reader is more user-friendly. In short, NFC-based payment outperforms barcode-based payment in terms of security, usability, and convenience. Unfortunately, today only 2 billion out of the total 3.4 billion active smartphones are equipped with NFC modules, as described in a public report [174]. Namely, nearly (3.4-2)/3.4=41% of smartphones do not support the NFC functionality. In fact, this percentage is much higher in developing or undeveloped countries where most people still use legacy or low-end smartphones. Another report [175] from NFC forum stated that only 20% of the world's population are enjoying the NFC with their smartphones. In addition, iPhone series usually disables the NFC functionality from the third-party payment solutions for security reasons. These NFC-denied or NFC-disabled smartphones cannot support NFC-based mobile payment, thereby preventing the further growth of the NFC market.

Is there an approach to enjoying the pervasiveness of built-in cameras but also holding the high security and convenience of NFC in mobile payment? The answer is affirmative because of our newly discovered insight that the magnetic field generated by an

NFC reader causes a harmless magnetic interference (MI) on CMOS image sensors equipped in smart devices. Specifically, when the camera is tapped on an NFC reader, the MI results in barcode-like stripes alternating in white and black on the grayscale images captured by the camera. Fig. 4.2 shows some examples. This harmless MI offers us an opportunity to achieve cross-technology communication (CTC) between NFC readers and NFC-disable smartphones. The rationale behind MI is in the sequential per-column readout approach, in which the values of a pixel array are read out column by column (see § 4.2).

Inspired by the insight, this work presents MagCode, a cross-technology communication system between an NFC reader and a camera, allowing customers to enjoy the high security and convenience of NFC-based payment and the pervasiveness of cameras. Technically, MagCode takes advantage of the MI to encode data into the barcode-like images, which can be further recognized by the interfered cameras. Commercially, the MagCode can be integrated seamlessly into the current barcode-based payment systems, except that the transmitting module becomes an NFC reader. Functionally, MagCode is used as simply as NFC, i.e., tapping on the NFC reader with a camera. MagCode could provide an economical, transitional, and trade-off solution before the wider spreading of NFC. It allows enjoying the dividend of mobile payment even if the users' smartphones are absent NFC modules. A preliminary demo video can be found at [176].

Translating MagCode into a practical system is non-trivial because of the following technical challenges:

- First, whether magnetic interference is pervasive and safe for smartphones in the current market is unclear. To address this concern, we conduct a feasibility study in §4.2. Particularly, we present the rationale behind the interference and modelled it mathematically. We also validate the model across 11 different models of smartphones from eight manufacturers. The results demonstrate that MI is indeed a general phenomenon across different smartphones. A long-term safety experiment, including up to 10 k interference tests, shows the MI does not introduce any temporary or permanent damage to smartphones.

- Second, engineering MagCode needs to address many practical issues. For example, which frequency should be used? How are bits encoded into the barcodes on images? How does the smartphone know the data is received perfectly? When and how the communication is terminated? To answer these questions, we design and implement a stack of protocols from the physical to the transport layer. The details are elaborated in §4.3.

Contributions. We implement a prototype of MagCode reader on USRP X310 software-defined radios and develop a smartphone app for decoding. We evaluate MagCode across 11 types of smartphones and five payment codes generated from five mainstream mobile payment APPs. In summary, we make the following contributions. First, to the best of our knowledge, we are the first to present a CTC scheme between a camera and an NFC reader, which could promote the further development of mobile payment. Second, we establish the operational feasibility and security of this one-way communication paradigm across commercial smartphone models. Finally, we design and implement a stack of protocols to achieve such a reliable simplex communication scheme. Extensive experiments have also been conducted to verify the outperformance.

4.2 Feasibility Study

In this section, we introduce the background of image sensors and model the magnetic interference of the NFC reader.

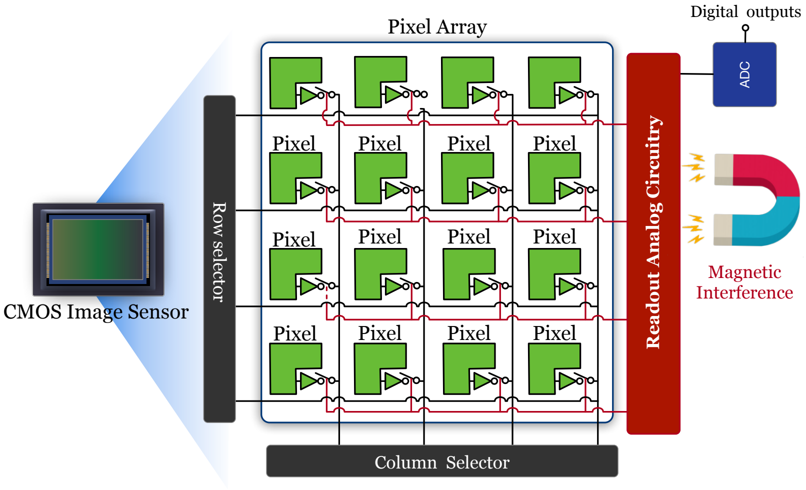


Fig. 4.3: Block diagram of the commercial CMOS image sensor

4.2.1 Background of Image Sensor

The demand for cameras (i.e., image sensors) has continued to grow rapidly because of the increasing popularity of digital video cameras in surveillance, smartphones, wearables, and so on. Nowadays, there are two dominant imaging technologies, namely, CCD and CMOS sensors, on the market. The CCD is known for its general reputation for superior image quality (i.e., high quality and low noise) but at the cost of size and high energy consumption. In contrast, the CMOS image sensors offer high levels of integration, which reduces the complexity of the circuitry, small size, and lower power consumption. Standard CMOS mixed-signal technology allows the manufacturer to implement all functions, such as timing, exposure control, analog-to-digital conversion (ADC), and digital image processing block on one piece of chip, also called "camera-on-a-chip." Because of these attractive merits, the mass production of CMOS image sensors for full-scale digital cameras was started as early as 1997, and they have developed to become the standard components for smartphones. Next, we focus on CMOS image sensors.

Fig. 4.3 shows the simplified block diagram of a commercial CMOS image sensor. The core of the sensor is a two-dimensional array of photo-detector components called *pixels*, which can sense the incident light intensity. The charge created by a pixel is converted to a voltage signal and passed on to the readout analogy circuity. Today's CMOS image sensor usually contains millions of pixels (e.g., 1920 × 1080), which requires extremely complicated circuitry to read out simultaneously. To address this issue, the pixel values are read out line-by-line in practice. That is, the image sensor uses an array of "row selector" and "column selector" switches to transfer one and only one column of pixel values to a set of storage capacitors each time. The transferred pixel values are then read out sequentially to the ADC for digitalization. The digital pixel values are eventually fed into the digital signal processing (DSP) unit. Given a CMOS image sensor with a resolution of 1920 × 1080, it would transfer the pixel values by 1080 times from the array to the final DSP. That is why sometimes the term "1080P" is short for this resolution to emphasize the "bottleneck" of the transmission.

4.2.2 Magnetic Interference on Image Sensor

In the field of electronic engineering, electromagnetic interference (EMI) indicates a phenomenon wherein analog circuitry is interfered with to generate undesired noise when it is exposed to an electromagnetic field. As a kind of EMI, magnetic interference (MI) occurs when the circuitry is exposed to the alternating magnetic field, leading to an eddy current in the corresponding circuits. Recently, *we found that when the camera module of a smartphone is close to a magnetic field operating at 13 MHz around, the captured images after graying exhibit many undesired stripes alternating in white and black.* This phenomenon was reported by the previous work [55] at the earliest, where this work explored the potential negative effect of this EMI on the quality of photos when a digital camera locates near a magnetic source. Our purpose is to explore the positive effect of this MI, i.e., using it as a side channel to achieve cross-technology communication.

We set up a preliminary experiment, as shown in Fig. 4.4, to validate the magnetic

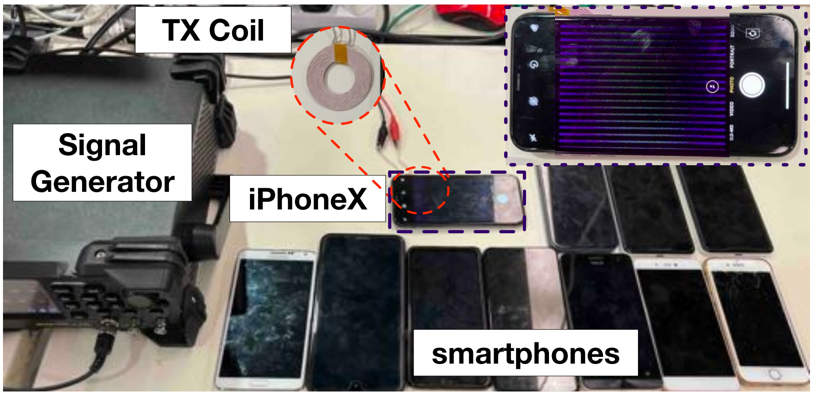


Fig. 4.4: Experimental setup for the real-life feasibility verification.

interference. Specifically, we utilize a RIGOL DG2052 [177] arbitrary waveform generator (AWG) to produce a regular sinusoidal signal at 13.56 MHz around (i.e., the operating frequency of NFC). The maximum output power of the AWG is 200 mW, which is fully compatible with the NFC standard [178]. The generated signal will be broadcasted by a standard NFC Class 4 coil [179] into the air with a 100 mW default output power. A higher TX power (e.g., 100-200 mW) is not required since the default power is enough. In the experiment, we place smartphones (e.g., iPhone X) onto the coil where the distance between the camera and the coil is about 3 cm. The results are shown in Fig. 4.2. The figures from (a) to (e) in the first row show the grayscale images taken by the smartphone's camera, which is interfered with by the NFC equipment when the frequency varies from 13.589 MHz to 13.593 MHz. The image resolution is 4032 × 3024 pixels, but only the top 1000 rows are shown in the figures because of space limitations. The camera is very close to the coil and thereby loses focus. The captured image is supposed to be in black and full of Gaussian noises. Nevertheless, we can clearly observe many alternating stripes, which appear in a certain pattern from left to right. The number of stripes increases with an increasing carrier frequency.

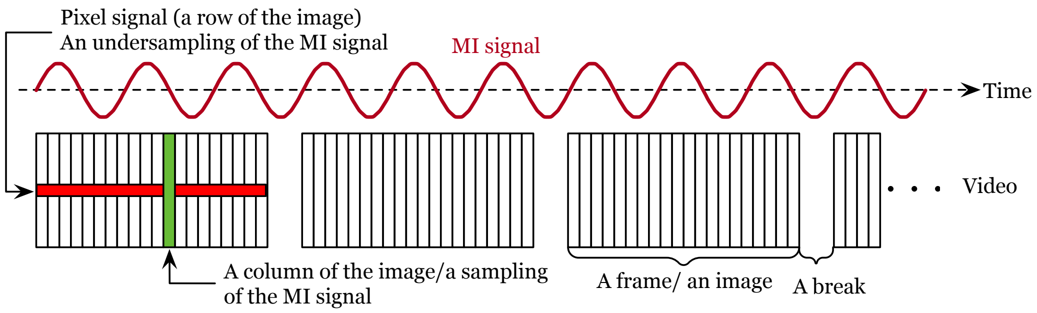

Pixel signal (a row of the image)
An undersampling of the MI signal
MI signal
Time
Video
A column of the image/a sampling of the MI signal
A frame/ an image
A break

Fig. 4.5: Pixel signal modeling. Readout of a column pixel each time is a sampling of the magnetic interference signal. Each row is a pixel signal, which is an instance of the undersampling of the MI signal. A video is a discontinuous sampling process in which there exists a break exists between two adjacent frames.

4.2.3 Modeling Magnetic Interference

Although the magnetic field is imposed on all pixels of the CMOS image sensor instantaneously and simultaneously, only a single column of pixels will be read out and recorded by the DSP each time. Therefore, columns of the image receive different interference from the alternating magnetic field (i.e., MI signal). As shown in Fig. 4.5, we can consider each readout of a column as a sampling of the MI signal, while pixels in each column represent the repetitive samples at the same sampling time. Consequently, the pixel values in each row reflect a discrete sampling of the MI signal. We call this sampling signal *pixel signal*, as shown in Fig. 4.5. Suppose the MI signal is a regular sinusoidal signal at a carrier frequency f_c as follows:

$$s(t) = \sin(2\pi f_c t) \tag{4.1}$$

Let f_{readout} denote the readout frequency (i.e., the sampling frequency). The frequency f_c is about 13.56 MHz but the f_{readout} is around $300 - 700$ kHz. The sampling frequency is hundreds of times lower than the carrier frequency, leading to an aliasing effect based on the Nyquist–Shannon sampling theorem. As a result, the sampled signal (i.e., the pixel signal) fails to maintain the original spectrum characteristics. The pixel signal can be written as follows:

$$P[k] = \sin(2\pi f_{\text{pixel}} \times \frac{k}{f_{\text{readout}}} + \phi) \tag{4.2}$$

where ϕ is the initial phase. The frequency f_{pixel} is determined by f_c and f_{readout} as follows:

$$f_{\text{pixel}} = f_c - N \times f_{\text{readout}} \tag{4.3}$$

where $-f_{\text{readout}}/2 < f_{\text{pixel}} \leqslant f_{\text{readout}}/2$ and $N \in \mathbb{N}$. If the image contains C columns, it takes C/f_{readout} seconds to read out all pixel values. Thus, there will be $n = C \times f_{\text{pixel}}/f_{\text{readout}}$ alternating stripes emerging in the image from left to right as expected. The f_{readout} is a constant term for a particular smartphone. Thus, the strip number n increases with the increasing f_{c} until $f_{\text{pixel}} \to f_{\text{readout}}/2$ and $n \to C/2$. Afterward, both f_{pixel} and n start decreasing until equal to zero.

Fig. 4.5 shows that we can transmit endless data with MI by using the real-time video recording function. In this case, each image becomes a carrier to capture a portion of the signal, and the frame breaks result in a binary erasure channel, which will be further discussed in §4.3.

4.2.4 Real-Life Verification

To visually understand the model, we show the red pixel signals in the third row of Fig. 4.2, which are extracted from the grayscale images. As mentioned above, each row is an instance of the pixel signal. We calculate the mean values of the pixels in the same column and plot the mean pixel signals in the figures. The image background is uneven, leading to slight fluctuations in the red pixel signal. To remove such uneven noise, we further convert the captured images to binary images by replacing all pixels with luminance greater than the mean with the value 1 (white) and replacing all other pixels with the value 0 (black). Interestingly, we obtain barcode images in the second row of Fig. 4.2. The white bars correspond exactly to the first half periods of the pixel signals (i.e., above mean), while the black bars correspond to the second half periods (i.e., below mean). From this perspective, we could say that the result of the magnetic interference is a barcode, which can be used to convey the data.

Table 4.1: The configurations of the smartphones and their built-in cameras.

Phone				Camera Configuration						Video Resolution	Frame Rate	Optimal Frequency[1]	Erasure Ratio[2]	Throughput[3]
No.	Manu.	Model	Real.Date	Manu.	Model	Type	Chroma	Pixel Size	Sensor Size	(Max)	(fps)	(MHz)	(@30 fps)	(bps)
P1	Apple	iPhone 7	2016/09	Sony	IMX315	CMOS	RGB	1.22 μm	1/2.93″	3840 × 2160	30, 60, 120, 240	13.543, 13.585, 13.590	68.6%	1043 @60 fps
P2	Apple	iPhone 8	2017/09	Sony	IMX315	CMOS	RGB	1.22 μm	1/2.93″	3840 × 2160	30, 60, 120, 240	13.431, 13.432, 13.433	68.6%	1043 @60 fps
P3	Apple	iPhone X	2017/11	Sony	IMX315	CMOS	RGB	1.22 μm	1/2.93″	3840 × 2160	30, 60, 120, 240	13.541, 13.542, 13.590	68.6%	1043 @60 fps
P4	Apple	iPhone 12	2020/10	Sony	IMX503	CMOS	RGB	1.40 μm	1/3.40″	3840 × 2160	30, 60, 120, 240	13.508, 13.509, 13.659	79.9%	861 @60 fps
P5	Google	Pixel 3 XL	2018/10	Sony	IMX363	CMOS	RGB	1.40 μm	1/2.55″	3840 × 2160	30, 120, 240	13.564, 13.565, 13.566	23.8%	919 @30 fps
P6	Huawei	Honor 8X Max	2018/09	Sony	IMX471	CMOS	RGB	1.00 μm	1/3.13″	1920 × 1080	30, 120	13.538, 13.592, 13.593	21.0%	906 @30 fps
P7	Redmi	Note 9	2020/11	Samsung	S5KGM1	CMOS	RGB	0.80 μm	1/2.00″	1920 × 1080	30, 120	13.480, 13.528, 13.575	60.0%	808 @30 fps
P8	OnePlus	OnePlus 6	2018/05	Sony	IMX519	CMOS	RGB	1.22 μm	1/2.6″	3840 × 2160	30	13.665, 13.666, 13.667	46.0%	780 @30 fps
P9	ASUS	Zenfone 5 LTE	2014/07	Sony	IMX214	CMOS	RGB	1.12 μm	1/3.06″	1920 × 1080	30	13.545, 13.546, 13.547	47.3%	802 @30 fps
P10	Samsung	Galaxy Note 3	2013/09	Sony	IMX135	CMOS	RGB	1.12 μm	1/3.06″	3840 × 2160	30	13.563, 13.564, 13.565	19.0%	1036 @30 fps
P11	Xiaomi	Mi 5s	2016/09	Sony	IMX387	CMOS	RGB	1.55 μm	3/4.00″	3840 × 2160	30	13.510, 13.511, 13.512	48.0%	791 @30 fps

[1] The optimal frequencies that MagCode works at for communication. There might exist more than three frequencies, but only three frequencies are listed in the table;
[2] The erasure ratio is defined as the ratio of the break duration between two adjacent frames to the whole duration of a frame including the break. It indicates how much percent of the time is unavailable for communication. [3] The maximal throughput at an optimal setting.

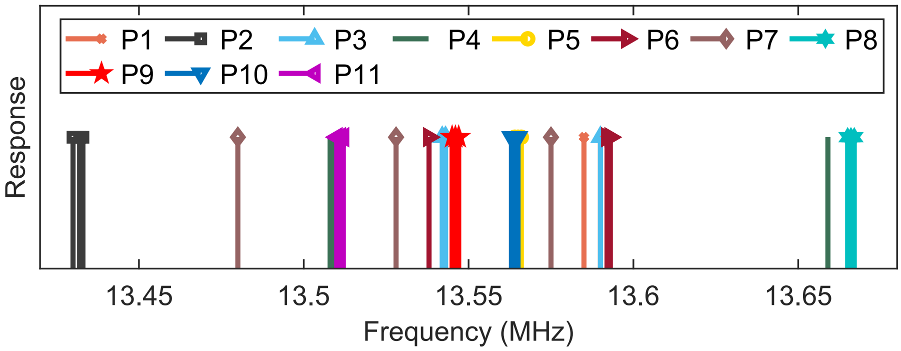
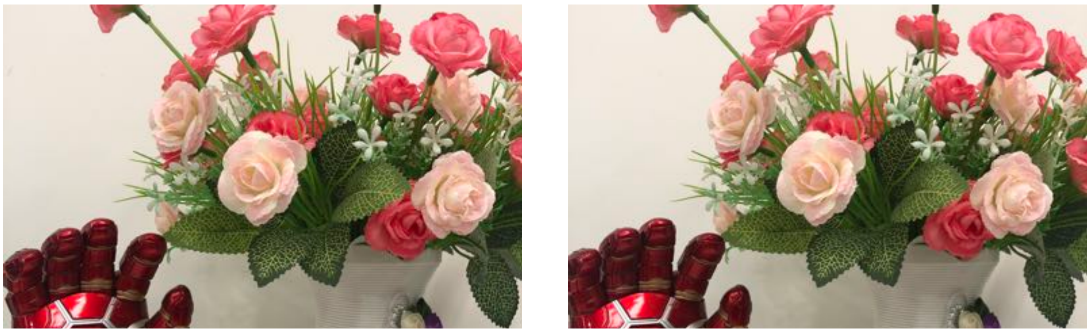


Fig. 4.6: Frequency responses of 11 smartphones in the spectrum of 13.4-13.7 MHz.

In the experiments, the interference frequency f_c is set to 13.589, 13.590, 13.591, 13.592, and 13.593 MHz respectively. After a large number of testing and measurement, we find that the f_{readout} of iPhone X in imaging mode is about 301.95 kHz. Thus, based on Eqn. 4.3, the $f_{\text{pixel}} = f_c - N \times f_{\text{readout}} = 1.25, 2.25, 3.25, 4.25, 5.25$ kHz. There are $C = 3024$ columns in the images. Consequently, we should observe $n = C \times f_{\text{pixel}}/f_{\text{readout}} = 13, 22, 33, 44$ and 53 periodic stripes in the images, which remains almost consistent with the experimental results (see Fig. 4.2). There exist $1-2$ period errors because the clocks of the reader and the smartphones are not well-synchronized, both of which have their own clock drifts [180].

In addition, we also verify the magnetic interference across the other 10 models of smartphones, which are produced by the top eight popular manufacturers. The detailed configurations of these smartphones and the verification results are summarized in Table 4.1. In short, we have the following findings: first, magnetic interference is



(a) Before test

(b) After 10 K tests

Fig. 4.7: Safety check: visual comparison

a general phenomenon that affects all kinds of smartphones. No matter whether a smartphone has installed NFC modules, magnetic interference always exists and it is mainly influenced by built-in imager models. Thus, it can be used as a general side channel to achieve communication between an NFC reader and smartphones. Second, the frequency response indicates the optimal interference frequency causing the detectable pixel signal. Fig. 4.6 shows the results of the frequency response across the 11 types of smartphones in the spectrum of 13.4 and 13.7 MHz. We can see that the same smartphone might respond at multiple interference frequencies, and different smartphones might respond at different frequencies. This finding suggests that the NFC reader should first recognize the smartphone model and then chooses an appropriate frequency as the carrier.

4.2.5 Safety Check

One might be wondering if the image sensor is damaged by the frequent and long-term magnetic interference. Technically, the 100 mW transmitting power is totally in accord with the NFC standard, which guarantees electromagnetic compatibility even if other electronic components are placed near the NFC coil. To further validate the safety, we compare two photos in Fig. 4.7, which were captured by an iPhone X before and after 10,000 interference tests, respectively. In each test, the camera is closely exposed to the magnetic field for over 10 seconds. Suppose MagCode is used ten times each day. There are about 365 × 3 × 10 = 10,950 uses in total within three years (i.e., the average lifespan of a smartphone). From the figures, we do not notice any evident difference in the quality of the two photos visually. In addition, we adopt five typical full reference image quality assessment algorithms [181–184] to evaluate the image similarity quantitatively. The results are shown in Table 4.2. The average similarity score between two images across different metrics is 97.2%. The remaining 2.8% difference may be caused by environment light variants or pixel mismatch during imaging. Both the visual and quantitative results demonstrate that MagCode does not damage the camera sensor.

4.3 System Design

Although we present MagCode in the context of mobile payment, the technique can be widely applied to a variety of NFC applications, e.g., access control, transport cards, ticketing, smart home, parking access, healthcare, etc. In this section, we elaborate on MagCode in detail.

4.3.1 Overview

We first look into MagCode from a high level with respect to the system scope and the workflow.

System Scope. Our mobile payment system has three parties. The first party is

Table 4.2: Safety check: quantitative measure.

Metrics	aHash [181]	dHash [181]	pHash [182]	SSIM [183]	MS-SSIM [184]
Similarity(%)	98.93	98.23	98.47	95.69	94.54

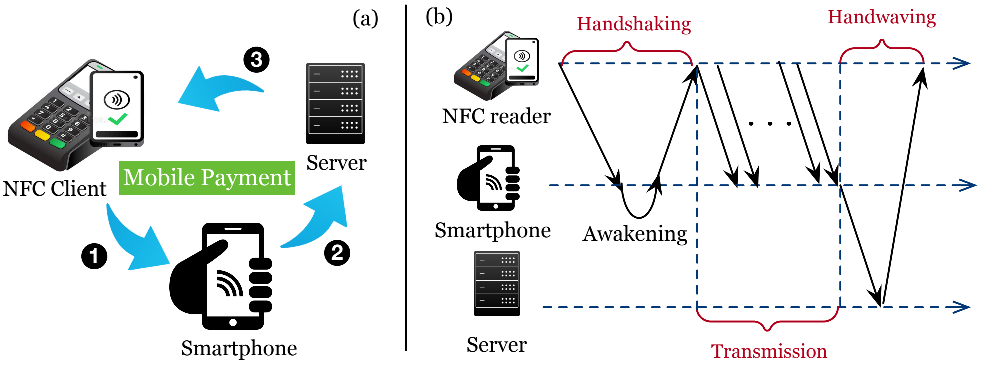


Fig. 4.8: The general workflow for mobile payment

.

the NFC reader. Sometimes, it is also called a point of sale (POS) machine or NFC terminal. After decades of development, POS machines have been widely adopted as the main payment devices deployed at the checkpoints of supermarkets, stores, and restaurants. We aim to update the firmware of the NFC reader to support MagCode. The second party is an NFC-disabled smartphone that the customer wishes to use for the payment. Similar to the barcode-based payment, the smartphone is required to keep a connection with the Internet via WiFi or cellular networks. On the smartphone, we run a payment APP that can access the camera module for video recording. The third party is the backend server (such as Alipay, PayPal, WeChat Pay, etc.), which performs the transaction tasks (such as identifying authentication, money transfer, termination, etc.).

MagCode in a Nutshell. Fig. 4.8 shows the detailed workflow of the MagCode-based mobile payment system. The communication is initiated by the NFC reader with a handshake phase, during which the NFC recognizes the smartphone model and awakens the payment APP. After the handshaking, the NFC reader continuously broadcasts packets, in which the data are encoded by the Fountain codes. On the receiver side, the smartphone launches the camera to record video, in which each frame is binarized into barcodes and then further decoded into packets. Once the smartphone decodes sufficient packets from the video, it sends the decoded data to

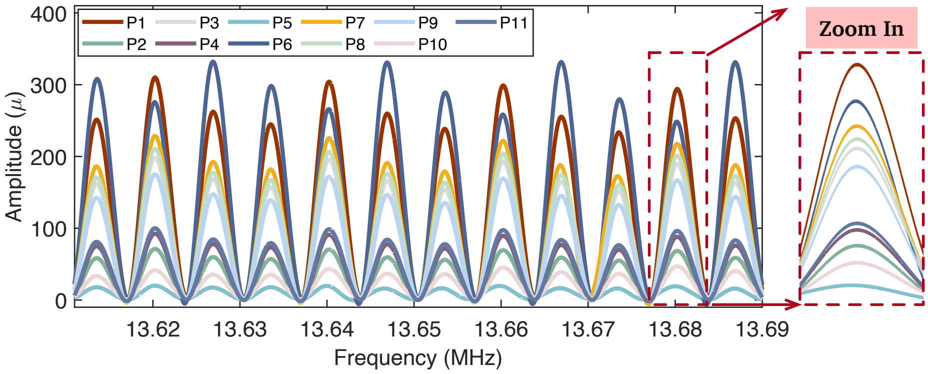


Fig. 4.9: Frequency response to a stepped frequency sweeping signal challenge across 11 types of smartphones. The responses exhibit different trends and thus can be used 5o recognize the smartphone model.

the server for the next move. Finally, the server sends an acknowledgment to the NFC reader for the communication termination. In sum, a customer just needs to use the smartphone's camera to record a video (which incorporates the transaction ID and the NFC reader information) first and then initiate the transactions via the back server, i.e., NFC Reader ⇒ Smartphone ⇒ Server ⇒ NFC Reader.

4.3.2 Handshaking

A handshake is the process of negotiation between two participants (e.g., NFC reader and smartphone) through the exchange of information that establishes the protocols of a communication link in the beginning. In MagCode, we also require a handshaking phase as follows.

• **Smartphone → NFC reader**. As mentioned above, different models of smartphones might respond at different carrier frequencies. To achieve optimal communication performance, we first identify the type of smartphone and choose its appropriate response frequency to set up the link. The challenge is that the communication of MagCode is unidirectional. That is, the smartphone cannot transmit messages to the NFC client directly (similar to the barcode-based payment). Inspired by wireless charging, we can use the algorithm for foreign object detection (FoD) to determine whether a receiver exists and the type of receiver placed close to the TX coil. The basic idea is that the load impedance of the TX coil will be changed when any conductor (e.g., a smartphone) gets into its magnetic field. Specifically, the voltage at the TX coil is given by:

$$V(t_2) = V(t_1)\exp\left(-\frac{\omega(t_2 - t_1)}{2Q}\right) \tag{4.4}$$

where $V(t_2)$ and $V(t_1)$ are the voltage of the TX coil at time t_2 and t_1. The $\omega = 2\pi f$ is the angular frequency. The Q is called *Q-factor*, which is a general purpose and dimensionless parameter that describes how underdamped an oscillator or resonator is. After a simple transform, the Q can be calculated as follows:

$$Q(f) = \frac{-f\pi(t_2 - t_1)}{\ln(\frac{V(t_2)}{V(t_1)})} \tag{4.5}$$

When a resonated RX coil is fed into the TX coil, the $Q = f_c/\Delta f$ (i.e., bandwidth Δf) and the two participants match with each other. The Q-factor is highly related to the physical characteristics of the RX. When feeding different types of foreign objects, the Q value measured by Eqn. 4.5 will vary considerably. Thus, we can use a group of Q values, which are measured across the NFC bandwidth, as an entire fingerprint to identify the receiver. However, the Q value is not easy to obtain in time domain directly, and thus, we could use the frequency response as unclonable physical fingerprints to distinguish different phone models in practice [185]. Specifically, the NFC reader broadcasts an OFDM signal at 13.56 MHz with 25 subcarriers across the 250 kHz bandwidth in total. Thus, each OFDM subcarrier is 10 kHz. Fig. 4.9 shows the frequency response range from 13.6 to 13.7 MHz measured from the 11 smartphones when they get close to the reader's TX coil. These curves exhibit their unique trends. A naive but effective K-nearest neighbors (KNN) algorithm is utilized to classify these 11 models, and the average accuracy that it could achieve is about 95.6%. Even if the model is misclassified and results in transmission failure, the operator could choose the correct model of the target smartphone on the NFC reader's user interface after recognizing it manually.

• **NFC reader → Smartphone**. We develop a mobile app for the smartphone to recognize the NFC-enabled barcodes. It has a backend service that runs without a UI. When the backend service detects the NFC connection request, it will wake up our app and pop up the front UI automatically. To this end, the backend service uses the magnetometer inside the smartphone to detect a series of changes in the magnetic field. The successful detection will trigger the subsequent communication phase. Why then should we not continue to use the magnetometer to receive the data from the NFC reader? The sampling rate of magnetometers is limited to 50-100 Hz. The low efficiency of the magnetometer will take several minutes to receive sufficient packets from the NFC reader, making customer lose their patience. Thus, the magnetometer is only used to awaken the payment APP by detecting the presence of a pre-designed magnetic envelope signal. Certainly, the mobile app can also be woken up manually in case the automatic wake-up fails, or the smartphone is not equipped with a magnetometer.

Summary. The handshaking occurs simultaneously on both sides. On the one hand, the NFC reader repeats to broadcast the stepped frequency sweeping signal and meanwhile calculates the Q value. Once a type of smartphone is identified, it starts to send the transaction data with known optimal parameters. When facing an unknown or new smartphone model, the NFC reader can simply broadcast a pre-defined probe message, via which the receiver app can instantly estimate all parameters (like C and $f_{readout}$) that the reader requires. Eventually, this new configuration is quickly uploaded to the central database for other NFC readers through such a crowdsourcing approach. On the other hand, after detecting the pre-designed magnetic signal, the smartphone wakes up our payment app to capture a few seconds of video for the following data decoding.

Compatibility Discussion. Referring to our experiment, MagCode only requires broadcasting the signals with a bandwidth of 250 kHz and a transmitting power of 8 mW. According to NFC standard ISO1443B, the bandwidth of an NFC reader is about

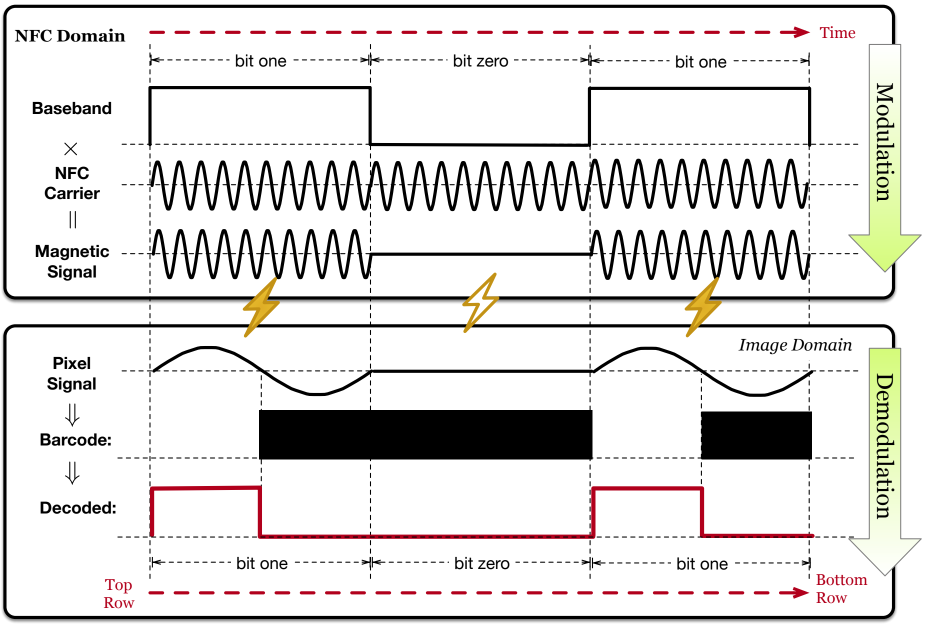


Fig. 4.10: Modulation and demodulation of MagCode.

1.7 MHz, and the default power is 100 mW. Thus, the current hardware requirements of MagCode are compatible with the corresponding NFC standards. For readers with OFDM function, the frequency response can be obtained through firmware upgrades. If the RF frontend of the reader does not support OFDM, we can still detect the frequency responses by traversing each sub-carrier sequentially, at the cost of time. Thus, MagCode can be implemented purely through the firmware upgrade at the NFC readers and without any modification in hardware.

4.3.3 PHY: Modulation and Demodulation

In the physical layer, NFC supports two modulation schemes, on/off keying (OOK) and binary phase shift keying (BPSK), with a Manchester or a Miller coding format. To maintain the maximal compatibility with existing NFC readers, we choose the OOK (i.e., 100% ASK) for the modulation, i.e., imposing or not-imposing MI represents bit one or bit zero. We show the modulation and demodulation procedures in Fig. 4.10. The two procedures occur at the NFC reader and the smartphone.

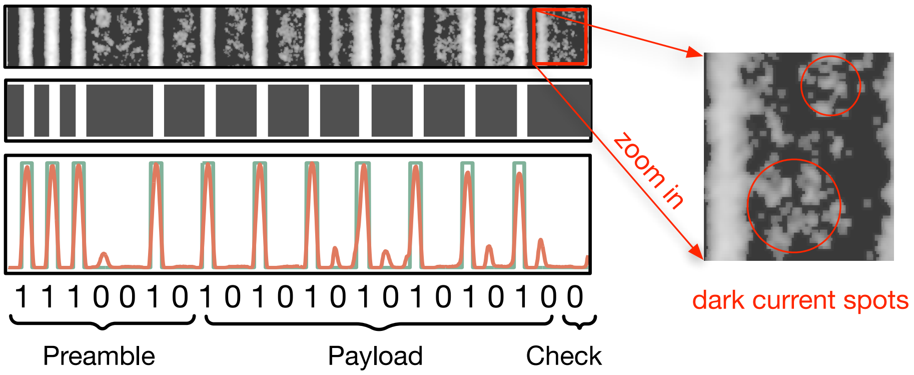


Fig. 4.11: An example of an interfered image that carries a short packet. Specifically, the first row is the captured grayscale image; the second row is the barcode image after the binarization; the third row is the mean pixel signals extracted from the grayscale images (in red), and that extracted from the barcode images (in green); the last row shows the decoded packet.

Modulation. On the NFC side, the bits are represented in non-return-to-zero (NRZ) format in the baseband, i.e., a high (or a low) voltage edge represents bit one (or bit zero), as shown in Fig. 4.10. The baseband signal operates at f_{pixel} or less. The NFC carrier is a regular sinusoidal signal operating at f_c. The modulation also multiplies the baseband signal by the carrier. As a result, the MI is present during the bit one period and is absent during the bit zero period. The modulated signal is eventually propagated into the air via the NFC coil.

Demodulation. On the smartphone side, the camera captures the signal by recording a video. Each frame (i.e., an image) of the video captures the pixel signal, which is automatically downconverted from f_c to f_{pixel} due to the aliasing effect. To decode the pixel signal, the frame is first binarized into a barcode, as shown in Fig. 4.10. By default, the background of each image is black; otherwise, it requires removing the background by differencing. In a barcode, the white bar corresponds to the first half period of bit one, while the black bar corresponds either the second half period of bit one or the whole period of bit zero. From the barcodes, we can further decode a regular square signal. Bit one contains a transition from a high-voltage edge (i.e., white bar) to a low-voltage edge (i.e., black bar), but bit zero only contains two low-voltage edges (i.e., two black bars). Thus, the output of the physical layer on the smartphone is the square signal.

Physical-layer Capacity. Suppose the image resolution is $R \times C$ and the frame rate is F fps. As analyzed in §4.2, there exist $C \times f_{\text{pixel}}/f_{\text{readout}}$ bits at most that can be modulated in each image. Thus, the theoretical maximal data rate of MagCode in the physical layer approximates $C \times F$ when $f_{\text{pixel}} = f_{\text{readout}}$. To put it into perspective, given 4032×3024 pixels @ 60 fps setting, the maximal physical-layer capacity is up to $3024 \times 60 = 181.44$ kbps, which is about 3,628× than the data rate of a magnetometer-based communication system.

4.3.4 DLL: Reliable Transmission

In the data link layer, we need to address an important issue called *asynchronous transmission* as follows.

Intra-frame asynchronization. In MagCode, there is no way to synchronize the NFC reader and the smartphone in time. Thus, the smartphone does not know when the transmission is started. The packet transmitted from the NFC reader might arrive at any column of a frame. To address this issue, each packet is started with a pre-defined preamble. The receiver conducts the autocorrelation with the incoming signal, and the result will peak exactly at the beginning of the packet. Similarly, we adopt a seven-bit Barker code (i.e., $[1, 1, 1, 0, 0, 1, 0]$) and one bit for the parity check. The packet structure is shown as follows:

$$\underbrace{[1,1,1,0,0,1,0]}_{\text{Preamble}}\ \underbrace{[\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots]}_{\text{Payload}}\ \underbrace{[1]}_{\text{Check}}$$

Specifically, the beginning of the packet is identified by sliding the preamble template along the square signal until a peak is found. Then, we use a simple integrator to identify the following bits. Finally, if the parity check passes, the payload is correctly

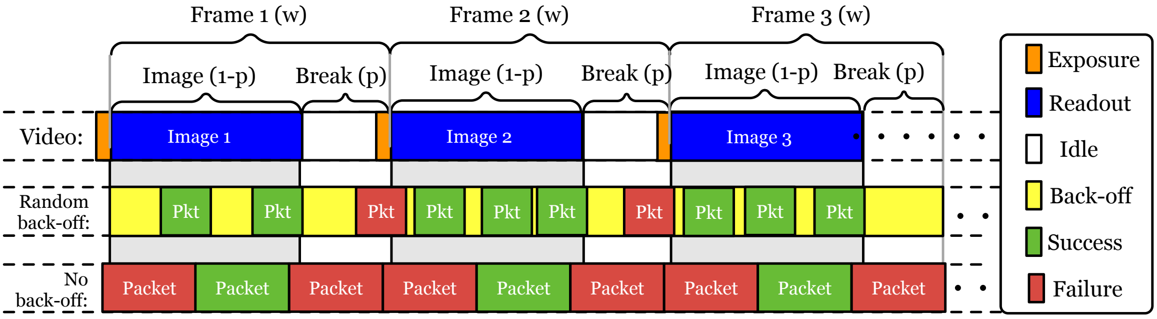


Fig. 4.12: The packet transmission in the data link layer

received; otherwise, the packet is dropped. Fig. 4.11 shows an example of an interfered image that carries a short packet with the preamble and the parity check bit.

Inter-frame asynchronization. The size of each packet is fixed in MagCode. There is a trade-off in choosing an appropriate packet size. On the one hand, we desire a larger packet such that the percent of bits for preamble and parity check is reduced and the cost minimized. On the other hand, the smartphone cannot receive the packets continuously, as shown in Fig. 4.5. Considering a resolution of 1920 × 1080 pixels and $f_{\text{readout}} = 310$ kHz in the recording mode, it takes 1080/310 kHz ≈ 3.5 ms to read out the whole image during a frame. The image resolution is usually reduced in the recording mode. Even if using 240 fps (i.e., the highest frame rate in the iPhone series), each frame lasts $1/240 \approx 4.2$ ms. As a result, about a 0.7 ms break (mainly for exposure) still exists between two adjacent frames, during which the channel is erased (see Fig. 4.5). Actually, the majority of low-end smartphones can only support the highest frame rate of 120 or 240 fps, resulting in up to 35% and 18% erasure ratios, respectively. The packets must be dropped if any part of them is erased because of the breaks. Thus, we desire a shorter packet to reduce the total number of erased packets.

Fig. 4.12 illustrates the transmission case where the smartphone receives the packets in discontinuous windows with a regular pattern. Let w denote the total number of bits that can be received during the whole frame window, including a break, in which total $w \times (1-p)$ bits can be received successfully during the image window, and $w \times p$ bits are erased due to the break. The p is the percent of erased bits (i.e., erasure ratio in bits). Now, the problem is formalized as follows: given the fixed receiving pattern, how can the NFC reader transmit packets to achieve the maximal goodput? The packet is L bits in size, where C bits are used for the preamble and the parity check. Whenever a packet is transmitted, we insert a random back-off denoted by B bits where $0 \leqslant B \leqslant L + wp$. The back-off strategy is to avoid the worst case, where a relatively large delay is caused by the worst arrival time of the first packet. Suppose N packets are transmitted, then the arrival time in bits of the n^{th} packet is computed as follows:

$$S_n = \left(\sum_{i=1}^{n} B_i\right) + (n-1)L \tag{4.6}$$

where $n = 1, 2, \ldots, N$ and B_i is the back-off time for the i^{th} packet. The total time consumed to transmit the N packets equals $S_N + L$. Then, the number of packets that can be successfully received is given by the following:

$$N_s = \Big| S \in \{S_1, S_2, \ldots, S_N\} | 0 \leqslant (S \bmod w) < w(1-p) - L \Big| \tag{4.7}$$

where $|\cdot|$ is the cardinality of a set. The above condition means the successfully received packet must arrive and end during an image window. Our goal is to find the appropriate packet length L to maximize the following goodput, which is defined as a number of good bits (bits excluding preamble and parity check) per second:

$$\underset{L}{\operatorname{argmax}} = \frac{E(N_s)(L-C)}{S_N + L} \tag{4.8}$$

where $E(\cdot)$ is the expected value.

We conduct a large number of simulations to find out the appropriate parameter L. The results are shown in Fig. 4.13. The goodput and L are illustrated with the times of w and the percentage of the frame length, respectively. We consider two frame rates, 240 and 120 fps, where the break period takes up 18% and 35% respectively. Random variables B that follow two different kinds of probability distributions, namely,

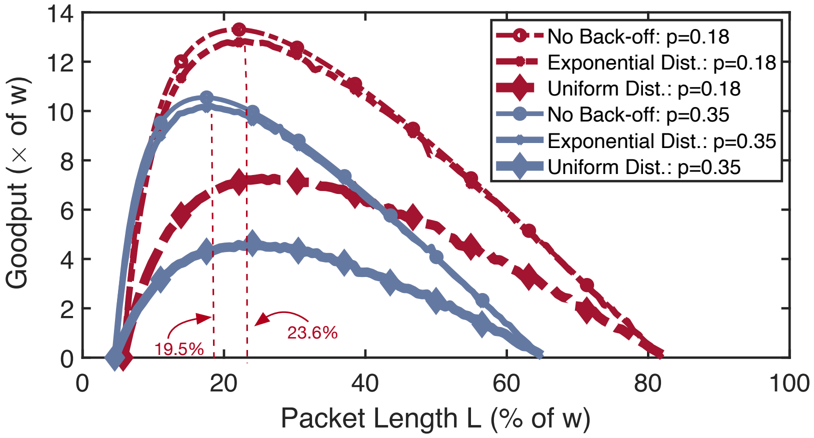


Fig. 4.13: Goodput vs. Packet length

uniform and exponential distributions, are considered for the back-off mechanism. Surprisingly, the optimal length $L \approx 20\%w$ regardless of which back-off strategy or frame rate is adopted. It is about a quarter of the readout time. The maximal goodput is achieved when the packets are transmitted continuously without back-off. It is reasonable because the no-back-off strategy ensures that at least two packets can be received successfully in each image. However, we still advise adopting exponential randomness for the back-off to avoid the worst case, although the occurrence probability is small. Meanwhile, the goodput of this exponential-back-off strategy is quite close to that of the no-back-off strategy.

4.3.5 TCL: Transmission Integrity

The goal of the transport control layer (TCL) is to guarantee the integrity of the data which are transmitted through multiple packets, even if some packets are lost or out of order. In MagCode, about 15%-50% of packets are lost in the link layer because of frame breaks between two adjacent frames. No reception acknowledgment could be sent back to the NFC reader. Thus, the re-transmission mechanism employed in conventional wireless communication does not work for us.

To resolve the above issue, we adopt Fountain codes [186] (i.e., erasure codes) to

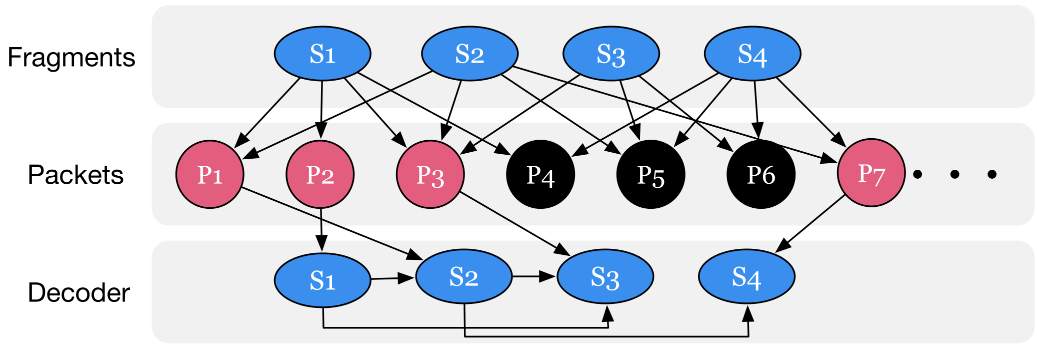


Fig. 4.14: Illustration of LT code

encode and recover the data in the transport layer. Fountain code is well known for its strong recovery capability of encoded data as long as a sufficient number of packets are received. In the past decade, a large number of schemes were proposed to generate the fountain codes (e.g., Tornado codes [187], LT codes [188], Raptor codes [189], etc.), among which the LT code is the first realization of Fountain code. In MagCode, we adopt LT code for the data encoding in the transport layer.

Fig. 4.14 illustrates the basic idea of LT code. First, the data are divided into data into K equal length fragments, e.g., S_1, S_2, S_3, S_4. Instead of transmitting the data itself, the transmitter (e.g., NFC reader) randomly selects d fragments and executes the XOR operation on these d fragments. For example, the first seven packets are transmitted as follows:

$$\begin{array}{lll} P_1 = S_1 \otimes S_2 & P_2 = S_1 & P_3 = S_1 \otimes S_2 \otimes S_3 \\ \cancel{P_4 = S_1 \otimes S_4} & \cancel{P_6 = S_3 \otimes S_4} & \cancel{P_5 = S_2 \otimes S_3 \otimes S_4} \\ P_7 = S_2 \otimes S_4 & & \end{array}$$

These packets are transmitted continuously. Unfortunately, only P_1, P_2, P_3, and P_7 are successfully received, and the other three packets are lost for some reason (e.g., frame breaks), as shown in Fig. 4.14. Even so, the receiver can still recover the data as follows:

$$S_1 = P_2, S_2 = P_1 \otimes S_1 = P_1 \otimes P_2, S_3 = P_3 \otimes S_1 \otimes S_2$$
$$S_4 = P_7 \otimes S_2 = P_7 \otimes P_1 \otimes P_2$$

The above decoding process is described as follows: after many packets have been received, we first determine and release the one-degree packets (e.g., P_2), in which only one fragment is involved. If there is no such packet received (e.g., P_1), decoding is paused temporarily until the coming of expected packets. Next, the edges connecting the released fragments to their neighbor (i.e., the fragments take participate in identical packets) are deleted. This process repeats until all packets are gradually decoded.

The number of chosen fragments, called *degree*, must follow the robust soliton distribution $\mu(d)$ [190]. On average, the K fragments can be recovered from any $K + \mathcal{O}(\sqrt{K}\ln^2(k/\delta))$ of the packets with probability $1 - \delta$, where δ is a user-defined parameter. During the transmission, no feedback is required. The receiver determines the integrity of each fragment by using the parity check bit. The transmission can be terminated until the entire data are recovered. This feature is especially desired for MagCode because the communication is unidirectional due to hardware limitations. We refer to [190] for the detailed encoding algorithm.

4.3.6 Hand-waving

The smartphone requests the transaction with the received data after receiving the entire data successfully from the NFC reader. The server conducts the transactions and eventually sends an acknowledgment to the NFC reader for termination. The NFC reader can also cancel the transaction automatically after time out.

4.4 Implementation

NFC Reader. We prototype the customized NFC reader on a USRP X310 software-defined radio with a UBX daughterboard. The center carrier frequency is 13.56 MHz. The USRP is further connected to a standard NFC Class 4 coil antenna [179].

The default output power is 100 mW, which complies with the FCC regulation part 15 [178]. At the backend, the USRP is connected via Ethernet cables to a 64-bit machine running Ubuntu 20.04. We use Matlab to generate the baseband signal of MagCode data packets. We implement the LTcode encoder and decoder based on [191]. The sampling rate is 2 MS/s.

Smartphone Receiver. 11 smartphones are tested as shown in Table. 4.1. We develop a mobile app for the smartphone to receive the NFC-enable barcodes. The app first invokes the built-in magnetometer sensor to detect the NFC reader request. The sampling rate of the magnetometer is 50 Hz by default. Once detected the request, it uses the built-in API to capture a video. By default, the frame rate is 30 Hz, and the resolution is 1920×1080 pixels. We use Matlab to develop a physical layer decoder to extract bits out of the recorded video. The decoder first uses a matching filter to improve the SNR, then uses a Gardener symbol synchronizer [192] to correct the symbol timing shifting and finally demodulate with a hard decision.

4.5 Evaluation

4.5.1 Performance in Handshaking

First, we evaluate the performance of MagCode in the handshaking phase, during which the NFC reader intends to detect the smartphone model while the mobile APP is triggered by the proximity event.

■ **Smartphone → NFC Reader**. The NFC reader uses frequency response as a signature to identify smartphone models. Specifically, the reader broadcasts a stepped sweeping signal. Meanwhile, it slides a 1-second window on the receiving baseband signal for the frequency response analysis until an evident response change is detected, indicating the occurrence of a proximity event. Then, the reader uses the response

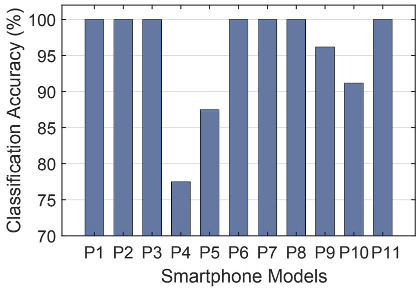


Fig. 4.15: Smartphone classification

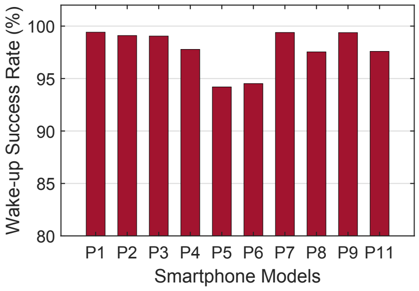


Fig. 4.16: Wake-up Success Rate

spectrum as a signature to sort the smartphone model from the database. In the experiment, we placed a smartphone camera onto the coil at a random angle. A total of 11 smartphones were tested. For each smartphone, we collect 400 frequency responses, wherein 80% samples are used for training the KNN classifier [193] and 20% samples for testing. The results are shown in Fig. 4.15. Specifically, we achieve 100% accuracy in classifying seven models, including P1, P2, P3, P6, P7, P8, and P11. The classification accuracy for P4, P5, P9, and P10 are 77.5%, 87.5%, 96.2%, and 91.2%, respectively. Overall, the average identification accuracy is above 95%. The frequency response depends highly on the size, appearance, materials, and shell structure of smartphones. In the worst case, 22.5% of P4 (i.e., iPhone 12) smartphones are wrongly classified as P2 (i.e., iPhone 8). This error is mainly because both models are from the iPhone series and adopt extremely similar shells and materials. Table 4.1 suggests that the hardware configurations (e.g., the frame rate, resolution, etc.) of P2 and P4 are also similar, as thus, one setting fits all iPhones even if the classification sometimes fails.

■ **NFC reader → Smartphone**. We employ the built-in magnetometer to detect the proximity events for awakening our mobile APP. The wake-up success rate is computed as the percentage of proximity events that are successfully detected over a total of 150 attempts. In each trial, the backend service running on the smartphone uses the magnetometer to detect the presence of the chirp envelope signal. Fig. 4.16 shows the rate as a function of the 10 smartphone models except for the P10, which

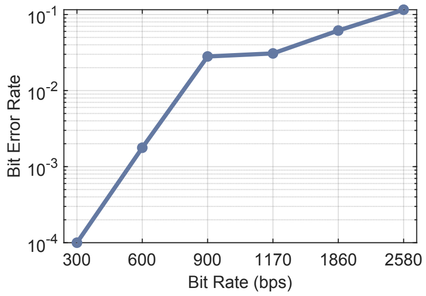


Fig. 4.17: BER vs. Bit Rate

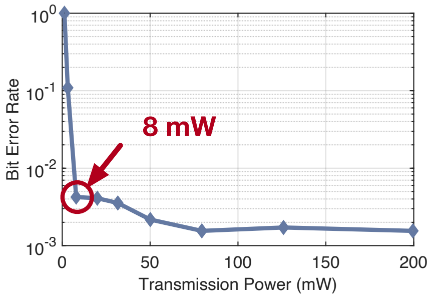


Fig. 4.18: Impact of Power

doesn't equip with a built-in magnetometer. The figure shows that above 94% of proximity events can be successfully detected. Particularly, Google Pixel 3XL relatively underperforms with a 94% accuracy because the magnetometer of the Google Pixel is arranged away from the camera module, unlike other smartphones, which usually arrange them close on the board. As claimed before, the APP can be manually launched in case of a shortage of magnetometers or wake-up failure.

4.5.2 Performance in the Physical Layer

First, we evaluate the performance of MagCode in terms of its transmission capacity in the physical layer, which can be reflected in the bit error rate (BER). The BER is defined as the percent of bits that are successfully decoded over the total number of transmitted bits. By default, we use an iPhone 12 to record the video with 1080P@30 fps and about 301 kHz readout frequency.

■ **BER vs. Bit Rate**. To understand how the bitrate affects the BER in the physical layer, we adjust the frequency of the baseband to make the reader transmit the data with varying bitrates, i.e., 300 bps, 600 bps, 900 bps, 1170 bps, 1860 bps, and 2580 bps. In each setting, we transmit 10 k bits to calculate the BER. Fig. 4.17 plots the BER in the log scale as a function of the bitrate. A higher bitrate leads to a larger bandwidth and a smaller symbol window, which cause decoding difficulty. In particular, the BER is increased to 0.01 when the bitrate is over one kbps. Usually, 10% BER is the tolerable upper limit in practice. From this perspective, MagCode can achieve a practical bitrate of up to 2.58 kbps in the physical layer. This value is far less than the theoretical upper band of 181.44 kbps analyzed previously for two main reasons. First, CMOS image sensors are not designed to sense MagCode, which is a trade-off solution between the NFC and barcode. The thermal noise intensified by the magnetic interference is not well suppressed in the hardware layer. Second, it is well known that the CMOS image sensors suffer from the dark-current degradation problem that a large dark current generated from the photodiode will cause many white spot defects on an image when no light is captured (i.e., the image becomes dark) [194]. Because the camera is placed close to the reader TX coil and little light is captured, the dark current dominates the pixel value, thereby resulting in many noisy white spots (see Fig. 4.11). Even so, MagCode still outperforms the magnetometer-based solution (i.e., Pulse [32]) by 58×. We hope that the manufacturers of CMOS sensors can optimize the hardware design to embrace MagCode in the near future.

■ **BER vs. Transmission Power**. We evaluate the effects of transmission power on the BER. Fig. 4.18 shows the BER as a function of the power. The BER decreases as power increases from 1 mW to 200 mW. The default transmission power of major commercially available NFC readers is limited to 100-200 mW as required by FCC part 15 [178]. The BER remains at an acceptable level ($< 4\%$) even if the transmission power is as low as 8 mW. No evident difference is observed as long as the power is above 50 mW, i.e., half of the current minimal default power. From this perspective, MagCode is more energy-efficient than the conventional NFC because no energy is required to power up the passive NFC chips.

■ **BER vs. Distance**. Fig. 4.19 shows the BER as a function of the distance between the smartphone and NFC reader. Clearly, the BER rapidly increases as the increase of distance. The BER goes up to 14% when the distance is over 4 cm. This is because the energy of a magnetic field degrades at $O(1/d^6)$ with distance d. This feature exactly meets the high-security demand for short-range communication.

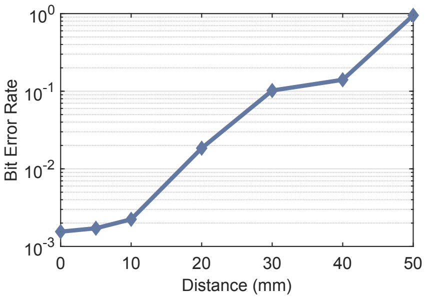


Fig. 4.19: Impact of Distance

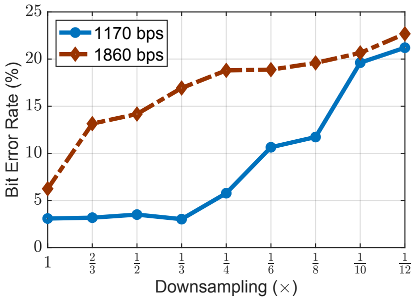


Fig. 4.20: Impact of Resolution

Thus, the security of MagCode is as good as the conventional NFC, whose working range is also about 4-10 cm.

■ **BER vs. Resolution**. We are also interested in how the image resolution affects the BER. To this end, we use the smartphone to receive images with a default resolution of 1080P. The transmitted bitrate is set at 1860 and 1170 bps, respectively. We then downsample the received images uniformly. Fig. 4.20 shows the BER as a function of downsampling rate, which is defined as the percent of remaining columns after downsampling. For 1170 bps bitrate, the BER remains nearly unchanged when the downsampling rate is $\leqslant 1/3$ (or resolution $\geqslant$ 360P). For the 1860 bps bitrate, the BER increases significantly with the increase in downsampling. As aforementioned, each column is a result of a sampling of the MI signal. The downsampling deletes the samples, leading to higher BERs.

■ **BER vs. Ambient Light**. Finally, we evaluate the effects of ambient light. In a dark environment, the pixel value of the white bar caused by the MI only is about 40 out of 255 in grayscale. The white pixel value is 255 and the black is 0. We simulate the lighting by adding an intensity offset from 0 to 240 to all pixels. Fig. 4.21 shows the BER as a function of the intensity offset. MagCode is rather resilient to the background lightness when its lightness is from 0 to 200. When the offset is over 200, the pixel values of white bars (i.e., 240) are saturated, thereby becoming 255 (i.e., information lost), and those of black bars become 200 (very close to 255). In this

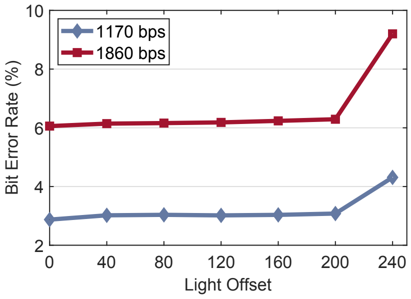


Fig. 4.21: Impact of Ambient Light

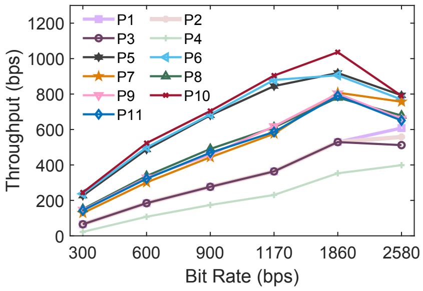


Fig. 4.22: Throughput vs. Bit Rate

case, both are difficult to be distinguished. However, such over-saturated cases are nearly impossible to happen in real-world mobile payment scenarios.

4.5.3 Performance in Data Link Layer

Then, we evaluate the performance of MagCode in the data link layer. In this layer, the whole packet is discarded once its parity check fails (including the packets truncated by frame breaks). The packet success rate (PSR) and the throughput and are employed as the main criteria. The PSR is the ratio of the number of packets successfully received to the total number of packets transmitted. The throughput in the unit of bps is defined as the number of bits that are successfully decoded. The packet length is set to about 20% of the frame (see §4.3). By default, a 30-fps frame rate is set.

■ **Throughput vs. Bit Rate**. First, we evaluate the throughput under various bitrates in the link layer. The reader transmits 1000 packets with a random payload. The throughputs of the 11 models of smartphones at 30 fps are shown in Fig. 4.22. All the throughputs exhibit a similar trend that the throughput increases as the increasing bitrate first, and the maximal through is achieved at 1860 bps bitrate. A higher bitrate takes less time to transmit a single packet, and thus, more packets can be transmitted. However, as mentioned previously, the BER is also increased at an increasing bitrate, and thus, the penalty (i.e., the number of failed packets) is also

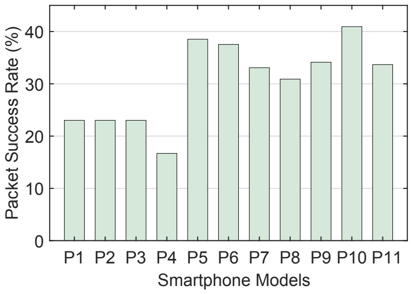


Fig. 4.23: PSR vs. Phones

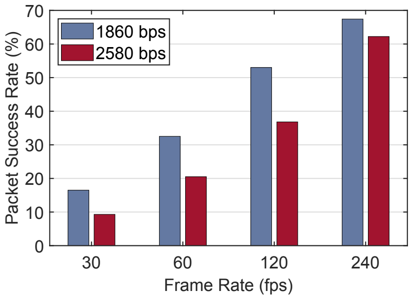


Fig. 4.24: PSR vs. Frame Rate

increased. Thus, the optimal bitrate is 1860 bps from the perspective of the link layer. Even in a worse case P4, the communication throughput is 400 bps, which is sufficient to transmit an entire QR code V2 [195] in less than one second. This rate can meet the general demand for mobile payment.

■ **PSR vs. Smartphones**. We further measure the PSR across different smartphones. In the experiment, we adopt the optimal 1860 bps bitrate and 30 fps frame rate. The results are shown in Fig. 4.23. The PSR varies considerably among different smartphones, resulting from different hardware performances. First, P1-P4 underperforms others. These four smartphones are from the iPhone series. Their underperformance is caused by the higher ensure ratio of up to 70%-80%. In other words, the iPhone series adopt a far higher readout frequency (e.g., about 301 kHz) than others, which allows taking only 30% of frame time to read out an image. As a result, 70% of the time during a frame is unavailable to receive the packets. Second, as shown in Table 4.1, other smartphones (particularly low-end smartphones) only support 30 fps. Their erasure ratio varies from 19% to 48%, which is far less than iPhones. Thus, more packets can be received, and their PSRs are relatively higher.

■ **PSR vs. Frame Rate**. From Table 4.1, the iPhone series can support four kinds of frame rates. Thus, we test the effects of the frame rate on the PSR concerning the iPhone series. In the experiment, the iPhone 12 is adopted, and two bitrates are tested. Fig. 4.24 shows the results. As desired, the throughput is greatly improved

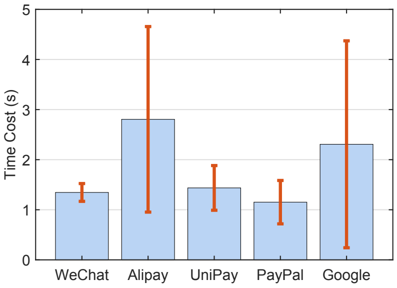


Fig. 4.25: Time Cost vs. QR Codes

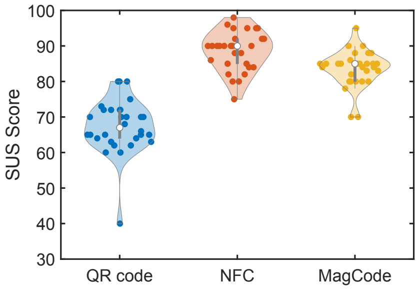


Fig. 4.26: User Experience

as the frame rate increases because the erasure ratio is greatly compressed from 80% at 30 fps to 30% at 240 fps, which increases the available time of reception. In particular, the maximal PSR of 68% is achieved at 240 fps with 1860 bps bitrate. Thus, we strongly advise using a higher frame rate rather than 30 fps for MagCode when the receivers are iPhone series.

4.5.4 Performance in Transport Layer

Finally, we evaluate the performance of MagCode in the transport layer. In this layer, the Fountain codes are used to resist channel erasure and out-of-order transmission at the price of time. Thus, we care more about the total time cost in terms of mobile payment applications.

■ **Time Cost**. We find the payment barcodes (i.e., QR codes) on Internet from five main mobile payment APPs: WeChat, AliPay, UniPay, PayPal, and Google Pay. We retrieve the raw data from these QR codes using Inlite [196] to determine what transaction information is delivered. Fig. 4.1 shows some examples. Their average lengths of the data are 570, 1190, 607,484, and 978 bits. Then, we transmit these transaction data using MagCode to an iPhone 12. In this experiment, we collect 10 different barcodes from each APP and barcode data are repeated to transmit 10 times. Fig. 4.25 compares the time cost taken on receiving the data. The fountain codes are probabilistic algorithms, and thus, the time cost does not remain constant in each trial. As a result, we take 1.23 ± 0.17, 2.80 ± 1.86, 1.43 ± 0.44, 1.15 ± 0.43 and 2.31 ± 2.06 s on transmitting the transaction data of the five APPs. The time on Alipay and Google pay varies considerably since their transaction length varies significantly. We guess that they might introduce more random bits to resist the guessing attack. On average, the iPhone takes 1.8 s on code recognition, which is a completely minimal cost that a human can accept. After all, focusing the camera on barcodes usually takes $3 - 10$ s in the barcode-based payment.

■ **User Experience**: We then delved into evaluating user experience associated with MagCode. A balanced group of 30 participants, consisting of 15 males and 15 females aged between 20 and 70, was recruited to participate in a comparative analysis of the usability of NFC, QR code, and MagCode payment services. This was accomplished through their responses to the standard System Usability Scale (SUS) questionnaires [197]. Such a simple, ten-item attitude Likert scale provides a comprehensive view of subjective usability evaluations. It is worth noting that the eldest participant experienced slight visual impairment. SUS scores range from 0 to 100, with higher scores indicating a more satisfactory user experience. The distribution of results is visually presented in Fig. 4.26, with the average SUS scores being 89 for NFC, 68 for QR code, and 84 for MagCode. Overall, user feedback was predominantly positive. Our results reveal that 96.7% of participants consider the MagCode to be simpler to use than traditional QR codes, as evidenced by their responses to the question: "I thought the system was easy to use." Many users expressed frustration with the precise alignment required for QR codes and appreciated that MagCode eliminates this issue. They praised MagCode for its ease of use and improved security, especially its capability to wirelessly retrieve information. Nearly all participants agreed that people would quickly learn to use this system. Despite these advantages, NFC was rated slightly higher than MagCode, mainly due to its faster data transfer rate. Some volunteers are concerned that MagCode might not integrate well with various NFC functions.

4.6 Conclusion

In this work, we propose, MagCode, a novel cross-technology communication system between an NFC reader and the camera. We revisit the EMI of the NFC reader and explore a side channel from an NFC reader to a camera for mobile payment to close the gap for NFC-denied or -disabled smartphones.

Chapter 5

Magnetic UHF Coupling: Spatially Controllable RFIDs Inventory

5.1 Introduction

Ultra-high frequency (UHF) Radio-Frequency IDentification (RFID) has arisen as a transformative non-contact identification paradigm in the logistics and retail domains [198–200]. By harnessing wireless radio frequency (RF) communication, RFID infrastructures can effortlessly access unique Electronic Product Codes (EPC) from passive RFID tags affixed to various items. A key criterion is the pinpoint identification of tagged objects within a predetermined Region of Interest (ROI). For instance, in automated shopping arenas, RFID systems discern customer selections within a specified vicinity near the departure point, commonly termed the checkout zone; in environments such as airports or manufacturing units, RFID systems adeptly oversee an array of items transitioning on conveyors; within warehouse contexts, RFID systems diligently oversee item dynamics at ingress and egress junctures. The efficacy of the RFID paradigm hinges on its prowess to execute these operations expeditiously and with unparalleled accuracy, even amidst challenging operational conditions.

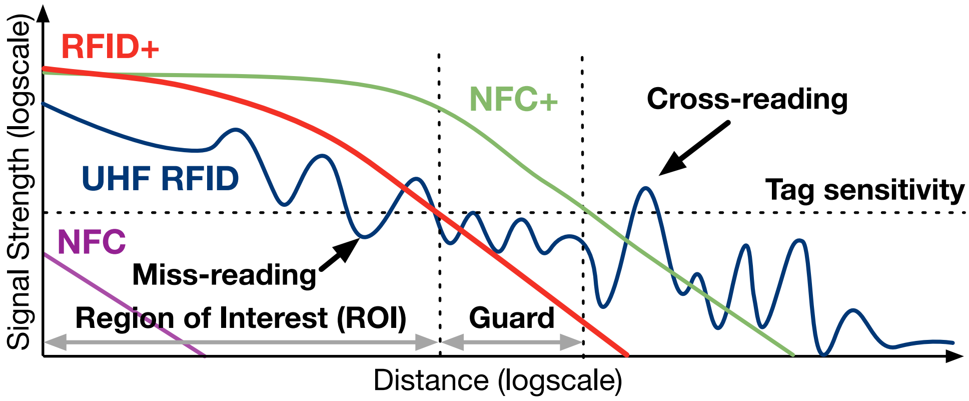


Fig. 5.1: The unpredictable propagation behavior of RF signals has traditionally rendered UHF RFID susceptible to anomalies of miss-reading and cross-reading. RFID+ defies this norm by introducing a controlled magnetic field, effectively addressing both miss-reading and cross-reading challenges similar to the HF NFC+.

Nevertheless, without fully realizing the extensive capabilities of RFID, present-day RFID systems remain under the shadow of two significant challenges: *miss-reading anomaly* and *cross-reading anomaly*. Conventionally, UHF RFID tags operate in far-field domains, where the RF signal propagates as planar electromagnetic (EM) waves, decaying at a pace of $\mathcal{O}(1/r^2)$ in relation to distance r. As depicted in Fig. 5.1, governing the far-field RF signals is intricate due to their multifaceted interplay with RF-inimical materials such as metals or liquids. These signals are prone to reflection or absorption. Particularly, within the ROI, there is the potential for multipath signals to nullify each other, culminating in "blind zones" where the RF intensity is not sufficient to trigger relevant RFID tags (i.e., the miss-reading anomaly). In contrast, outside the designated ROI, multipath signals may combine constructively, inadvertently leading to the recognition of undesired tags (i.e., the cross-reading anomaly). For instance, as illustrated in Fig. 5.2(a-b), the confined and crowded nature of the checkout lane in an automated store inherently leads to unavoidable tag miss-reading and cross-reading anomalies.

Modern RFID systems face challenges in addressing cross-reading and miss-reading anomalies [69,201] simultaneously. While increasing transmission power and sensitiv-

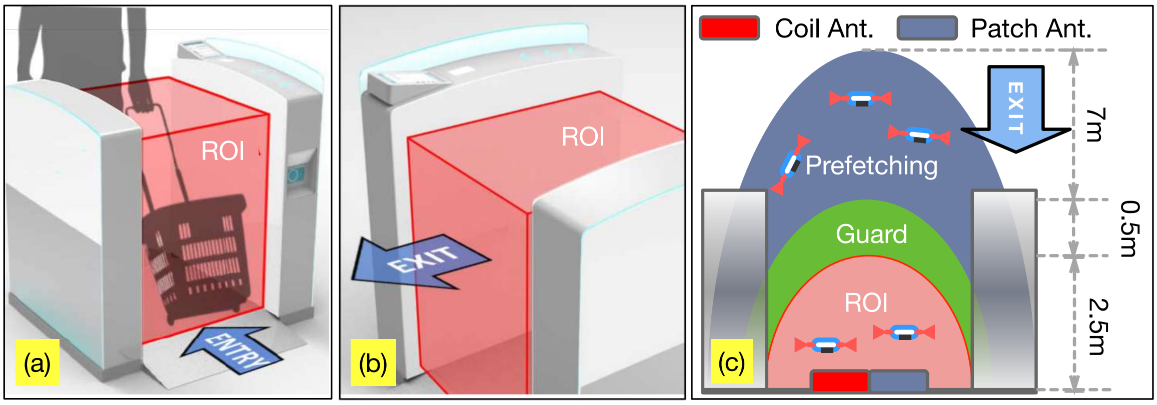


Fig. 5.2: Checkout lane. (a) and (b) show the entrance and the exit of the lane. These two figures are reproduced from [82]. (c) shows our prefetching augmented ROI coverage.

ity can improve detection, it often leads to unintended cross-readings. On the other hand, mitigating cross-reading can cause missed detections. Although recent debates favor a localization-based approach over the traditional binary reading, its effectiveness is questioned due to challenges like the "garbage in, garbage out" [70, 202]. While RFGo [82] leverages machine learning for enhanced detection, it falls short in dynamic scenarios. NFC+ [70] previously explored the potential of long-range, magnetical-coupling HF NFC at 13.56MHz as an alternative to UHF RFID for improved ROI management. Magnetic signals inherently minimize cross-reading owing to their rapid decay, and diminish the likelihood of miss-reading because of their pronounced penetration through challenging materials such as liquids and metals. However, NFC+ still faces three challenges: (1) HF tags are substantially more expensive than UHF tags, posing deployment barriers; (2) existing infrastructures, heavily reliant on UHF RFIDs [203], face challenges in adopting NFC due to compatibility issues; (3) NFC's reading rate of 50 tags/s is dwarfed by RFID's 200 tags/s, making NFC less suitable for high-speed inventory tasks such as those involving moving tags on conveyors or checkout zones.

Contrary to HF NFC tags that use *coil antennas* for inductive or magnetic coupling, UHF RFID tags commonly utilize *dipole antennas* to capture and emit electromagnetic waves. The absence of coils may give the *misleading impression that UHF RFID* *tags are ill-suited for energy harvesting from magnetic fields.* However, as illustrated in Fig. 5.5, the architecture of a standard UHF RFID tag includes a small loop (highlighted in blue) situated near the chip. Commonly referred to as the “matching” or “tuning” loop, this component is critical in optimizing energy harvesting and offering protection against over-voltage issues. Our findings indicate that this inherent loop structure can, in fact, enable UHF RFID tags to harvest energy from magnetic fields, thereby mimicking the inductive coupling characteristics as seen in HF NFC.

In this work, we introduce RFID+, a magnetically-driven UHF RFID system that innovatively repurposes the matching loop of a UHF RFID tag as an RF frontend for both energy harvesting and communication. The system’s objective is the spatially selective identification of UHF RFIDs through precision-controlled magnetic fields. As depicted in Fig. 5.1, RFID+ not only emulates the propagation features of NFC+ but also overcomes its limitations. Specifically, RFID+ effectively interfaces with widely-used, economical UHF RFIDs while maintaining a high reading rate.

However, translating RFID+ into practice poses three significant engineering hurdles:

- Initially, the feasibility of harnessing energy from magnetic fields through the matching loops of commercial UHF RFIDs has not been thoroughly investigated. To fill this research void, we conduct an exhaustive feasibility study that shines light on the underlying principles of magnetically-driven UHF RFID systems. Through empirical evaluations conducted in real-world scenarios, we not only establish the viability of this technique but also substantiate its effectiveness and broad applicability.
- Secondly, the necessity arises for the integration of a coil antenna into a UHF RFID reader, enabling the creation of a controllable magnetic field. Traditional wavelength-matched loop antennas (single-coil) commonly seen in HF NFC (i.e., 13.54 MHz) become problematic when shifted to the UHF band (i.e., 860 – 960 MHz). This difficulty stems from the notably shorter wavelength at UHF relative to

the loop's circumference, potentially leading to certain regions experiencing mutual magnetic field nullification. To address this concern, we put forward a tailored multi-turn, capacitor-segmented coil antenna complemented by a high-impedance reflector, striving for an even and directional magnetic field distribution.

- Thirdly, RFID systems driven by magnetic fields have a range that caps at about 3m, substantially less than the potential 10m span of those powered by radiative methods, largely attributed to the swift dissipation of magnetic fields. This confined ROI intensifies the need for prompt tag reading. To mitigate potential delays, especially with fast-moving tags, we initially engage a conventional far-field, radiatively-coupled reader to prefetch potential tags moving toward the ROI. Subsequently, we incorporate Bloom filters alongside the near-field, magnetically-coupled reader to streamline the inventory procedure.

Contributions. This study re-examines the intricate ROI management in UHF RFID through the lens of inductive coupling. We present three major contributions: 1) We validate the potential of magnetically-driven UHF RFID; 2) We introduce innovative coil antenna designs and a tailored inventory algorithm for RFID+; 3) Through rigorous tests and real-world pilots, we demonstrate RFID+'s efficacy. We hope that this research revitalizes academic discourse surrounding magnetically-driven UHF RFID systems in typical scenarios.

5.2 Magnetically-Driven UHF RFID

In this section, we start by exploring the basics of UHF RFID, introduce inductive coupling via tags' matching loops, and finally assess the feasibility across COTS UHF tags.

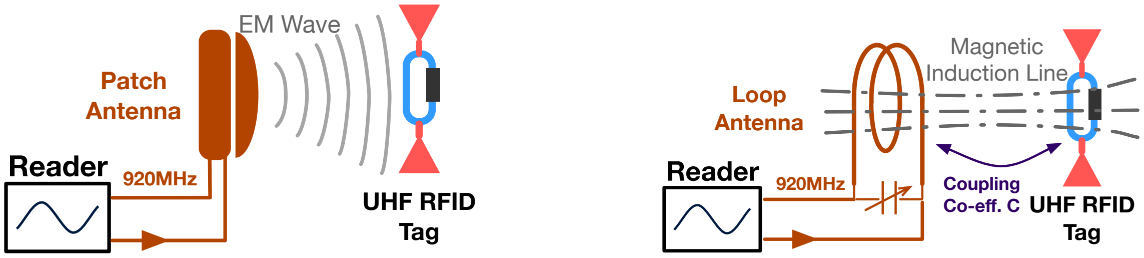
5.2.1 Background

The coupling mechanism describes the means by which systems engage in the interchange of energy or information. The mechanisms adopted by HF NFC and UHF RFID vary significantly, largely owing to the different frequency ranges in which these systems operate.

• **Inductively-Coupled HF NFC**: Operating at 13.56MHz, HF NFC employs inductive coupling facilitated by coil antennas. In this arrangement, an oscillating electrical current flows through the reader's coil, generating a variable magnetic field in the surrounding area. When an NFC tag comes within this field's sphere of influence, the magnetic flux induces a current in the tag's coil antenna, thereby activating the NFC chip and initiating communication with the reader. Given the reactive nature of these fields, the effective communication range is generally limited to a short span of several centimeters.

• **Radiatively-Coupled UHF RFID**: Typically operating within the 860-960 MHz frequency range, UHF RFID utilizes radiative coupling, commonly executed through dipole antennas. In this scenario, the reader emits a UHF radio wave that, upon reaching an RFID tag, induces an electric current in the tag's antenna. Utilizing backscatter technology, the tag then modifies and reflects the wave back to the reader. This method allows for a substantially extended operational range, often reaching up to several meters.

In essence, while HF NFC primarily employs inductive coupling for close-proximity interactions, UHF RFID leverages radiative coupling to enable longer-distance engagements.



(a) Radiatively-Coupled RFID

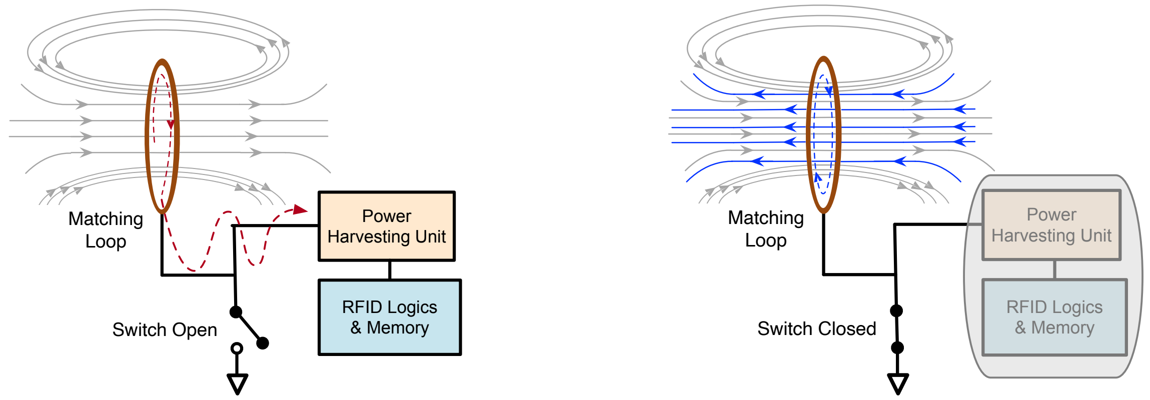
(b) Inductively-Coupled RFID

Fig. 5.3: Rationale behind Magnetically-driven UHF RFID

5.2.2 Inductive Coupling via Matching Loops

Inductive coupling usually requires coil-configured antennas that the UHF RFID tags are short of. Thus, it seems that UHF RFID tags are not reactive to magnetic fields at first glance. Actually, as illustrated in Fig. 5.6, every RFID tag inherently incorporates a single-turn coil, referred to as the matching loop. This essential component bridges the gap between dipole-style antennas and the tag's integrated chips (ICs), serving three primary functions: Firstly, it facilitates impedance matching between the antenna and the chip, ensuring optimal power conveyance. Secondly, this loop aids in adjusting the voltage levels to align with the chip's requisites. Lastly, by safeguarding the correct impedance and voltage calibrations, it inadvertently fortifies the RFID chip against potential over-voltage detriments.

These loops can essentially act as standalone coil antennas. When exposed to a magnetic field, these loops capture an induced electrical current that then flows to energize the chip, successfully accomplishing inductive coupling. Therefore, it becomes feasible to power and interface with UHF RFID tags through magnetic fields, akin to the operation seen in NFC systems. To elucidate further, let us juxtapose the operational mechanics of conventional radiatively-coupled RFID systems with those of our innovative magnetically-coupled ones. Fig.5.3(a) portrays the conventional system where the reader is equipped with a patch antenna – a specific variation of a dipole antenna. A tag derives its power from the transmitted electromagnetic waves



(a) Non-reflective

(b) Reflective

Fig. 5.4: Magnetic backscatter communication. (a) With the switch is open, the induced current is directed towards the harvesting unit; (b) With the switch is closed, the coil experiences a short-circuit. The current generated within the coil fosters an opposing magnetic field, which subsequently resonates with the reader's coil, acting as a reflection.

fully using its own dipole antenna. On the other hand, Fig.5.3(b) illustrates our approach: the reader comes outfitted with a coil antenna, purposed for the generation of concentrated magnetic fields. This magnetic flux subsequently traverses the tag's matching loop, thereby inducing an electric current. The distinction between the two approaches lies solely in their signal propagation mechanisms – via either a patch or a coil antenna. All other system parameters, including the operating frequency and transmission power, remain unaltered, making this a financially judicious solution.

5.2.3 Communication Immutability

A concern may arise regarding the necessity of altering communication protocols when passive tags obtain power through magnetic fields. This concern can be addressed by examining the two communication links of UHF RFID: the downlink and the uplink.

- **Downlink (Reader ⇒Tag)**: In the downlink, where the reader communicates to the tag, the goal is to query tags or send specific commands. The reader employs an Amplitude Shift Keying (ASK) method, encoding different bit values with varying

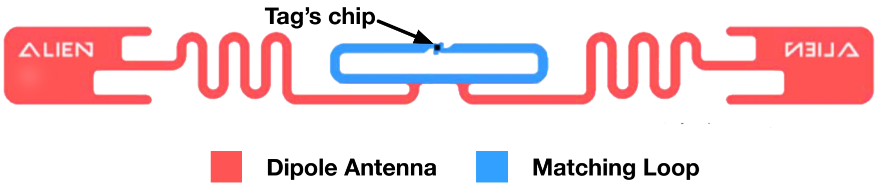


Fig. 5.5: Structure of a Typical UHF RFID Tag. It consists of an integrated chip, matching loop and a dipole antenna.

amplitude levels. This ASK causes magnetic strength changes, inducing a current with amplitude variation in the tag's matching loop. Thus, even with magnetic power derivation, the tag's chip can decode ASK commands.

- **Uplink (Tag ⇒ Reader)**: In the uplink, where tags communicate to the reader, the primary goal is to send the stored EPC. When energized by the reader's signal, passive tags use "backscatter modulation" to transmit data. This process involves a switch that connects the tag's peripherals to its IC, as depicted in Fig. 5.4. When the switch is on, the tag directs the induced current from the loop to the chip, making it absorbent and non-reflective. However, when off, the tag grounds the chip, and the loop-initiated current, following Lenz's law, creates an opposing magnetic field. This renders the RFID tag reflective, sending the loop-induced power back to the reader. The tag thus communicates bits by toggling between its reflective and non-reflective states or backscattering.

Thus, the modulation techniques employed for both downlink and uplink communication remain unmodified.

5.2.4 Inventory Process Using Inductive Coupling

Without loss of generality, Fig. 5.5 displays a standard UHF RFID tag design, showcasing a small loop (highlighted in blue) adjacent to its chip. Consistently, as Fig. 5.6 further demonstrates, it is a fundamental trait for nearly every RFID tag to embody a single-turn coil, known as the matching loop. This loop is instrumental in the mag-

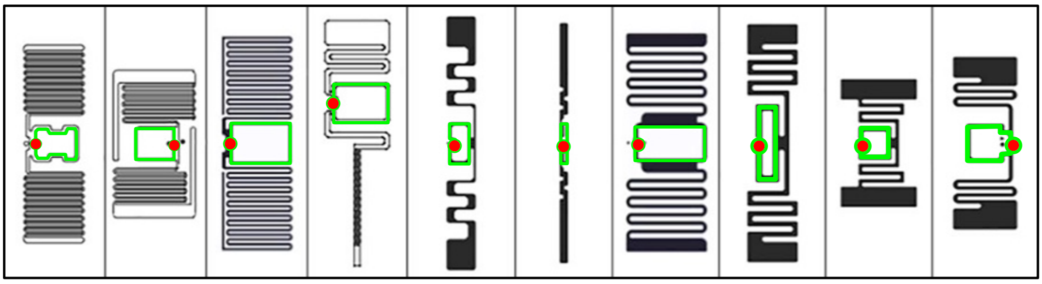


Fig. 5.6: The Popular UHF RFIDs. Each type of tag contains a matching loop (green) that bridges the dipole antenna with the chip.

netic energy harvesting process within our system. To inventory such tags via UHF inductive couplings, the reader must adhere to the UHF RFID Gen2 air interface protocol, which involves several steps: (1) The process begins with the reader initiating an inventory session by sending out a `Select` command to select a group of tags for participation. (2) This is followed by a `Query` command to initiate a new frame, during which each tag that has not yet been identified chooses a random time slot to respond. (3) In its allocated slot, a tag first sends out a 22-bit short response (i.e., `RN16`) to aid in detecting signal collisions. (4) If the `RN16` is successfully decoded by the reader, it indicates a collision-free transmission from a single tag (known as a singleton slot). (5) Subsequently, the reader requests a longer, 128-bit response (i.e., `PC+EPC+CRC`) by issuing an `ACK` command. Therefore, according to the protocol, a tag must initially transmit an `RN16` response before it can send its complete EPC response.

5.2.5 Experimental Verification

We verify the feasibility of the magnetically-driven approach using standard COTS RFID hardware. Fig. 5.7 provides a visual representation of the experimental configuration, showcasing the tags evaluated. We utilized a widely-used commercial RFID reader (Impinj R420 [204]) set to a frequency of 920MHz. Alongside this, we deployed the USRP X310 [205] device as a dedicated sniffer to capture the communication be-

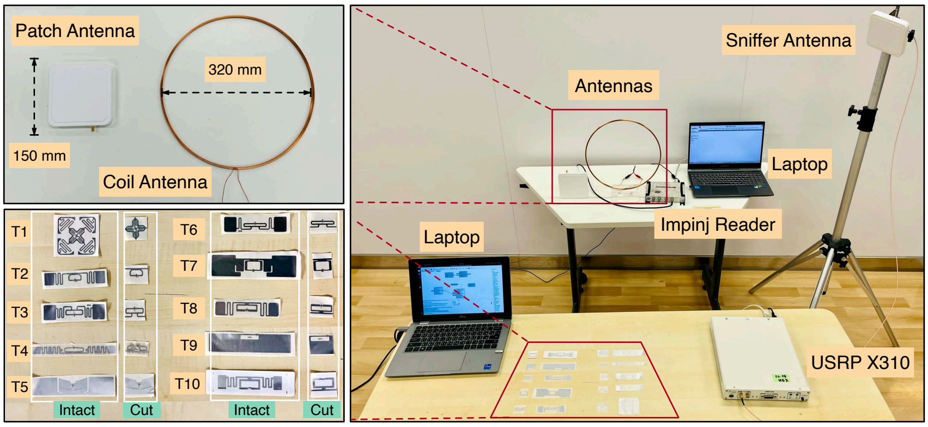


Fig. 5.7: Experiment Validation. A commercial Impinj reader is equipped with a patch antenna and a coil antenna, respectively. Ten types of commercial tags are tested.

tween the reader and the tag. Our tests incorporated two distinct reader antennas: a 15 × 15 cm^2 patch antenna and a coil antenna with a 32cm diameter. The reader is alternately connected to each of these antennas, with the transmission power maintained at 30dBm. The sniffer was strategically placed close to the reader antenna, roughly 30cm away. For each trial, we arranged each tag in an approximately parallel orientation to the loop to maximize the capture of magnetic flux.

Inventory with the Coil Antenna. To test the viability of a magnetically-driven UHF RFID system, we initiated a preliminary experiment using the configuration depicted in Fig.5.7. An Impinj M4 tag [206] was placed 10cm away as part of the experimental setup. *The Impinj reader is equipped with the coil antenna for tag activation and querying.* Concurrently, the sniffer discreetly recorded the leaked RF transmissions. As depicted in Fig. 5.8, the normalized amplitude of the intercepted signal is showcased. The figure clearly delineates the reader's command signals and the tag's backscattered responses. The inventory process kicks off with a `Select` command, promptly followed by a `Query`. Responding to the query, the tag emits a `RN16` reply that includes a fixed 6-bit preamble for signal identification, succeeded by 16 random bits to facilitate channel contention, as illustrated in Fig. 5.9. This is subsequently acknowledged by the `ACK` command, indicating the slot's availability.

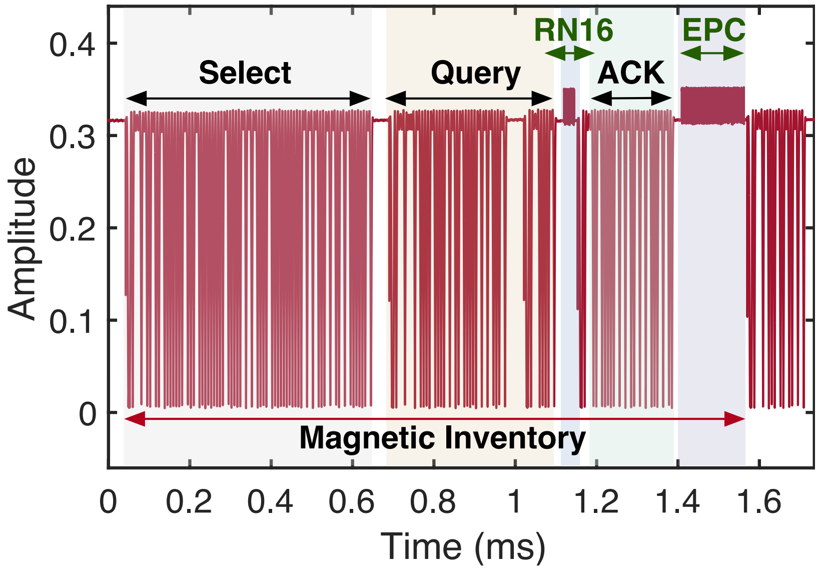


Fig. 5.8: RF signal acquired by the sniffer when the tag was queried by a magnetically-driven UHF RFID reader.

Conclusively, the tag broadcasts its `EPC`. This process closely parallels the inventory sequence observed in radiatively-coupled RFID Gen2 systems. It validates that COTS RFID tags can be activated and queried using magnetic fields while the communication protocol remains consistent.

Comparative Tests on Loop Role. Fig. 5.8 has validated that COTS RFID tags can be activated and queried using magnetic fields while the communication protocol remains consistent. To test if tags can continue to harness energy from magnetic fields using only matching loops, we conducted two comparative inventory tests with an M4 tag (i.e., T1) positioned 50cm away. We alternated between using a patch and coil antenna for the reader. The first test assessed the `RN16` responses of the unaltered tag. The signals from both antennas were largely consistent, as seen in Fig. 5.9(a) and (b). In the second test, after cutting off the tag's dipole antenna and leaving only the matching loop (see Fig. 5.7), the tag was unresponsive to EM-waves but still functions effectively when exposed to magnetic fields, as shown in Fig. 5.9(c) and (d). The comparative results emphasize the crucial role of the matching loop in energy harvesting. The comparative analyses were also conducted for the other nine

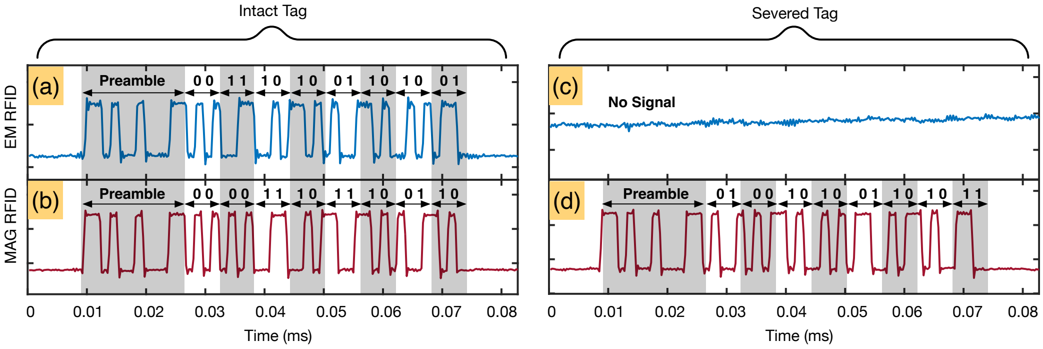


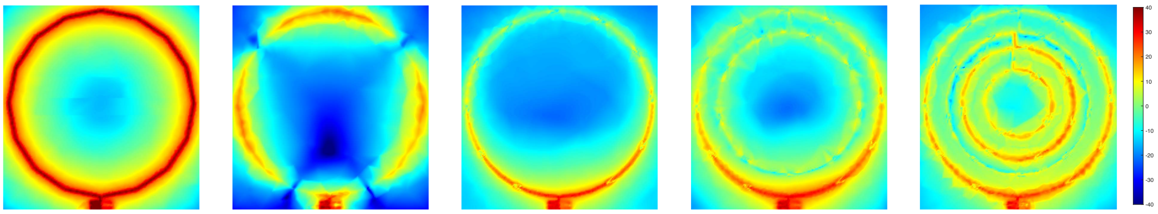
Fig. 5.9: Captured RN16 signals from a tag across four distinct conditions. (a) and (b) display signals procured from the unaltered tag, powered by EM waves and magnetic fields, correspondingly. (c) and (d) illustrate signals from the modified tag whose dipole antenna is cut off. As a result, it is unresponsive to EM-wave query anymore but still functions effectively when exposed to magnetic fields.

tag types (T2-T10, as depicted in Fig. 5.7). The outcomes were consistent across all tests.

5.3 Overview

At a high level, RFID+ is elegantly simple: We strategically replace the conventional electric patch antennas of UHF RFID readers with tailored coil antennas, in the pursuit of precisely controlled magnetic field emission aimed at UHF RFID tags within a specified ROI. Benefiting from rapid attenuation and strong penetration capabilities, magnetically-driven RFID+ minimizes miss-reading and cross-reading anomalies. To this end, we introduce a unique multi-turn, capacitor-segmented coil design for our UHF RFID system in §5.4 and devise a prefetching-based algorithm to speed up readings in §5.5. The subsequent sections elaborate on the technical details.

Scope. The matching loops inherent in existing UHF RFID tags are clearly not optimized for energy extraction from magnetic fields, resulting in low radiation efficiency and a relatively limited range. Our approach balances compatibility with controllability, designed to integrate seamlessly with existing UHF RFID tags while offering



(a) Loop@13.56 MHz (b) Loop@920MHz (c) One coil@920MHz (d) Two coils@920MHz (e) Four coils@920MHz

Fig. 5.10: Simulated magnetic intensity in the vicinity of five distinct antenna structures. (a) denotes an unsegmented loop actuated by a 13.56 MHz HF excitation signal; (b) illustrates an unsegmented loop energized by a 920 MHz UHF signal; (c) offers a depiction of a segmented loop equipped with lumped capacitors, resonating to a 920 MHz UHF signal; (d) presents a two-turn segmented loop integrated with fork capacitors, subjected to a 920 MHz UHF excitation; and (e) displays a multi-turn segmented spiral loop with fork capacitors, stimulated by a 920 MHz UHF signal.

precise ROI management in near-field settings like conveyor belts or checkout zones. In such environments, the desired operational range is approximately 100-200cm, consistent with prior findings [70, 72, 82]. Thus, our intent is not to supplant existing radiatively-coupled UHF RFID systems or to extend the long-range reading capability, but rather to complement them by offering improved spatial controllability within confined ROIs.

5.4 Spreading Magnetic Fields

In this section, we delve into the novel coil antenna design tailored for our magnetically-driven UHF RFID system.

5.4.1 Necessity of a Novel Coil Antenna

Why are traditional coil antennas inadequate for the specific requirements of magnetically-driven UHF RFID systems? To answer this question, we use ANSYS HFSS [207] software to simulate the distributions of magnetic fields generated by a 7.5cm radius single-turn coil at both 13.56MHz (HF NFC norm) and 920MHz (UHF RFID

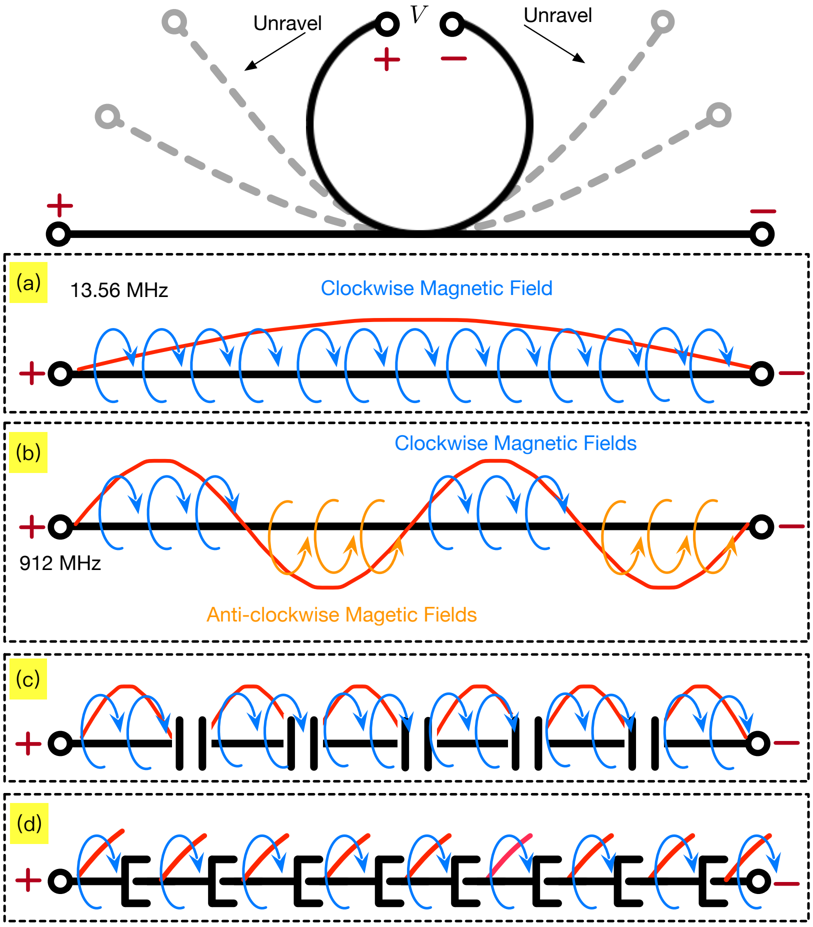


Fig. 5.11: Analysis on a loop antenna. (a) Magnetic fields remain in consistent directions at 13.5MHz; (b) The magnetic fields change their directions alternatively along the coil. (c) The capacitor-segmented coil eliminates the disparities in the initial phase. (d) The microstrip lumped caption-segmented coil.

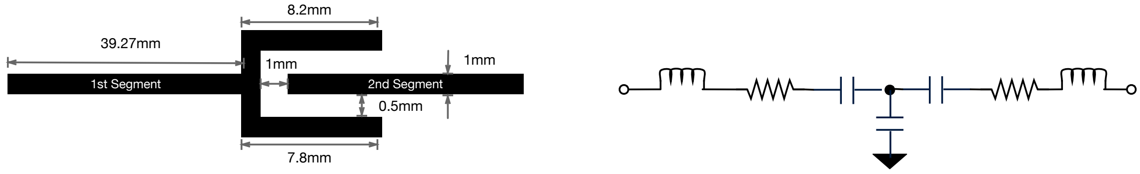
standard). The findings, illustrated in Fig. 5.10(a), reveal a uniform magnetic field distribution at the 13.56MHz frequency. However, at 920MHz, the field distribution shown in Fig. 5.10(b) exhibits irregularities, including four intensified regions surrounding the loop and five weaker areas, or “blind zones,” both centrally and at the corners. Such uneven distribution highlights the limitations of conventional coil antennas for UHF RFID applications, specifically in terms of potential activation failures in these blind zones.

The observed unevenness can be explained as follows: the coil is considered as a com-position of countless tiny elements, each generating its unique magnetic field with an initial phase. The overall field is the sum of these individual fields. Phase alignment results in constructive field addition, while misalignment can cause mutual nullification. To better visualize the phase variations as the signal traverses the coil, we represent the loop linearly, depicted in Fig.5.11. With HF signals, characterized by a 22-meter wavelength, phase discrepancies across coil elements are negligible due to the significant disparity between the wavelength and the coil's 50 cm circumference. A maximum phase difference is just 0.14 radians, ensuring a predominantly in-phase superposition, as displayed in Fig.5.11(a). Conversely, the UHF signal has a wavelength of 32 cm, comparable to the coil's circumference. As the signal traverses the coil, it completes about two cycles, as depicted in Fig. 5.11(b). This causes each element's initial phase to fluctuate between 0 and 2π repeatedly. The clockwise magnetic fields stem from positive currents, while negative currents yield anti-clockwise ones. When refashioned into a loop, these opposing magnetic fields combine out-of-phase, resulting in the observed uneven distribution. Thus, there arises a pressing demand to pioneer a novel coil antenna design tailored for the proposed magnetically-driven UHF RFID systems.

5.4.2 Capacitor-Segmented Coil Antenna

The loop antenna's limitation stems from the incoherent amalgamation of different elements because of phase discrepancies. A straightforward remedy might be to shrink the loop's size to 1/4 wavelength, ensuring better phase alignment. Yet, antenna theory fundamentals suggest that a loop antenna resonates (evident as a purely real impedance) only when its circumference is roughly equal to a wavelength [90]. More accurate dimensions need to be ascertained through specialized 3D electromagnetic simulation.

Capacitor-Segmented Loop. To counteract the loop antenna's limitations, we



(a) Microstrip Lumped Capacitor

(b) Equivalent circuit

Fig. 5.12: Fork-shaped Lumped Capacitor. (a) shows the structure and the size of the lumped capacitor. (b) shows the equivalent circuit.

propose segmenting the loop physically and inserting capacitors between adjacent segments, as shown in Fig. 5.11(c). Each segment can then be modeled as an equivalent RLC circuit. Let R, L and C represent the intrinsic resistance and inductance of a segment, and the capacitance respectively. Capacitors are known to resist sudden voltage changes. Under AC conditions, the current behind a capacitor obtains a phase shift ϕ, which is given by:

$$\phi = \arctan\left(\frac{2\pi f L - \frac{1}{2\pi f C}}{R}\right) \tag{5.1}$$

where f symbolizes the frequency of the signal. This equation indicates that by fine-tuning the capacitor's value, one can methodically counterbalance a desired phase shift. As shown in Fig. 5.11(c), segmentation at intervals of half a wavelength along the line results in a 180° phase change each time. By strategically selecting the capacitance values, a corrective phase shift of $-180°$ is introduced by each capacitor. This ensures the RF signal flowing between consecutive capacitors retains a uniform initial phase shift. Such alignment gives rise to uniform clockwise magnetic fields across segments. When the linear arrangement is formed into a loop, this coherence is maintained, yielding a consistent magnetic field distribution. This technique can uphold the loop's size while guaranteeing a balanced field distribution.

Fork-Shaped Lumped Capacitor. Utilizing a single discrete capacitor is straightforward, but integrating several capacitors onto a PCB might result in unexpected power consumption and enlarged dimensions. Contemporary antenna systems lean towards microstrip lumped antennas that smartly embed lumped components within the antenna's design. Inspired by prior designs in microstrip antennas [91,92,208], we adopt the fork-shaped lumped capacitors. As shown in Fig. 5.12(a), the capacitor is implemented by the microstrip line. In the figure, two segments are positioned 1mm apart. The former segment ends with a three-sided forked shape that interfaces with the beginning of the subsequent segment. Specifically, the dimensions of the top, left, and bottom sides are 8.2mm, 4mm, and 7.8mm, respectively. The bottom side is slightly shortened compared to the top to fit the arc design. Fig.5.12(b) presents the equivalent circuit where the three sides are modeled as individual capacitors.

The capacitance of the lumped capacitor is approximated by $8\varepsilon\sqrt{A/\pi}$, where A represents the area of the forked configuration and ε is the permittivity coefficient. This equation suggests that a considerable area is needed to achieve a substantial capacitance and the corresponding large phase shift. Thus, to avoid bulky capacitors, we trim the segment length, thereby adjusting the required phase. Each segment, featuring the aforementioned fork-shaped capacitor, was iteratively determined in HFSS by tuning the phase shifts according to segment length. Specifically, our design sets the segment length at 3.927cm, roughly 11.9% of the 32.872cm wavelength, deviating from the standard half-wavelength model. It is crucial to note the compromise: this design necessitates four times as many lumped capacitors than its half-wavelength counterpart. Fig. 5.11(d) showcases this coil design. As the signal traverses a 3.927cm segment, its phase shifts by 42.84°. The lumped capacitor then counters this shift by -42.84°, ensuring consistent signal alignment across segments.

5.4.3 Spiral Coil Antenna

As illustrated in Fig.5.10(c), the capacitor-segmented loop offers a markedly even distribution of magnetic field intensity compared to the conventional loop design. The updated design spreads this energy more uniformly. However, a region of diminished intensity remains near the center. This drawback can be remedied by using

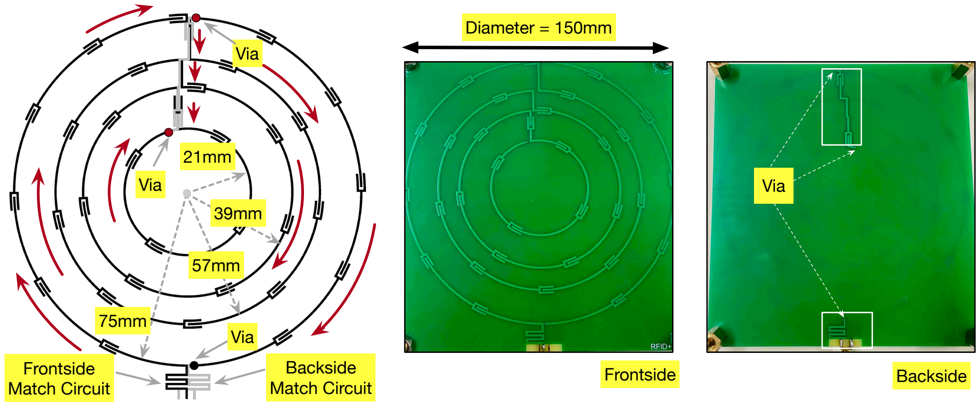
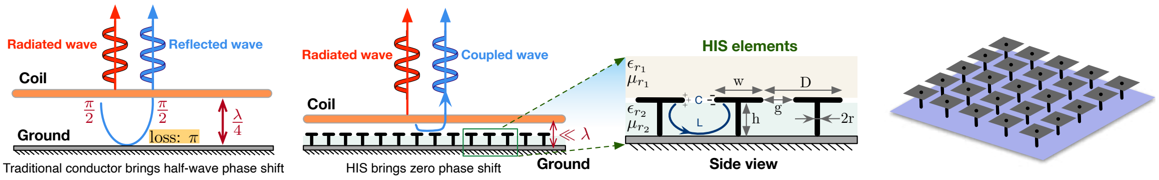


Fig. 5.13: Spiral Coil Antenna. Multi-turns of coils are arranged in a spiral fashion.

multi-turn coils. Accordingly, we introduce a spiral coil antenna, whose design and implementations are shown in Fig.5.13. This design features four distinct coil turns, artfully arranged in a spiral layout, with both the start and end points of the coil connected using via-holes. A greater coil density might seem beneficial but poses a challenge: the potential coupling between neighboring coils. To alleviate this potential interference, we reserve an 18mm spacing between them (i.e., half of the segment length) after iterative optimization. The simulated magnetic intensity distribution of two-turn and four-turn coil antenna are shown in Fig. 5.10(d) and (e), respectively. The simulation results reinforce our hypothesis that a spiral configuration not only enhances the effective electrical length of the loop antenna but also accentuates its intensity with the addition of more turns.

5.4.4 Directional Coil Antenna

Many applications, like inventory management, require directional coverage to meet user expectations. It is also notable that today's EM-driven UHF RFID systems use directional patch antennas. Thus, aligning with industry norms, our next steps will focus on crafting a directional coil antenna. A conventional solution is to place a metal reflector behind the coil antenna to direct magnetic fields forward. However, this approach faces the issue of half-wave loss. When RF signals transition from



(a) Traditional Metal Reflector

(b) Sideview of HIS

(c) Bird's-eye View of HIS

Fig. 5.14: Reflection-Induced Phase Shift. (a) When magnetic signals encounter a metallic ground, they experience a 180° phase shift due to half-wave loss. To counterbalance this phase shift, the separation between the coil and the ground must be set to $\lambda/4$. If the gap is less than $\lambda/4$, reflected signals will destructively interfere with the upward-propagating magnetic waves. (b) Illustrates a side view of the mushroom-structured HIS, designed to minimize the phase shift from reflections, effectively bringing it close to zero. (c) Depicts a top-down or bird's-eye view of the HIS.

low to high impedance boundaries, the reflected wave undergoes a 180° phase shift. As depicted in Fig. 5.14(a), if the coil-reflector gap is $< \lambda/4$, these shifted magnetic fields destructively interfere with those from the opposite side. The constructive superpositions occur only when the gap is set to $\lambda/4$. For our 32cm wavelength, a separation of about 8cm is required, increasing antenna thickness.

Mushroom-like HIS. Inspired by the artificial magnetic conductors [209], we introduce a high-impedance surface (HIS) approach to intrinsically mitigate the half-wave loss. The core principle behind HIS is illustrated in Fig.5.14(b) and (c). Resting atop a metallic base, a series of compact square patches are arranged in a grid pattern. These mushroom-like patches (called HIS elements) connect to the base via central via-holes, with a deliberate spacing between them. As a result, adjacent elements essentially function as capacitors, connected through the via-hole to the base metal below. Given the inherent parasitic resistance, two proximate HIS elements together resemble a standard parallel resonant RL circuit. The impedance related to an HIS can be expressed as:

$$Z_{\text{HIS}} = \frac{j\omega L}{1 - \omega^2 LC} = \frac{j\omega L}{1 - (\omega/\widehat{\omega})^2} \tag{5.2}$$

where ω signifies the angular frequency of the prevailing magnetic field, while $\widehat{\omega} = 1/\sqrt{LC}$ represents the resonant angular frequency. The L and C refer to the parasitic resistance and lumped capacitance, respectively. Their values are calculated as outlined in [210]:

$$L = \frac{\eta_s}{\omega}\tan(\beta h) \text{ and } C = \frac{1}{\pi} w\varepsilon_0(\varepsilon_{r_1} + \varepsilon_{r_2})\cosh^{-1}\Big(\frac{D}{g}\Big) \tag{5.3}$$

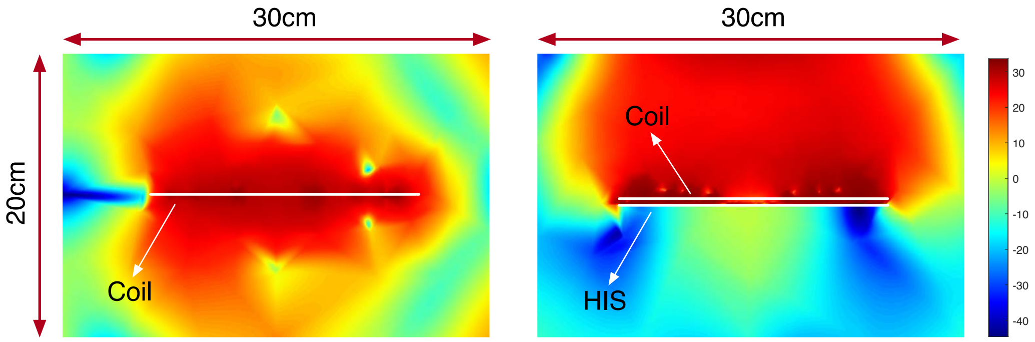
Here, $\eta_s = \sqrt{\mu_0\mu_{r_2}/\varepsilon_0\varepsilon_{r_2}}$ and $\beta = \omega\sqrt{\mu_0\mu_{r_2}\varepsilon_0\varepsilon_{r_2}}$ stand for the intrinsic wave impedance and propagation constant, respectively. The constants ε_0 and μ_0 are the permittivity and permeability of a vacuum, with relevant parameters defined in Fig. 5.14(b). By varying the size and spacing of these elements, one can fine-tune the resonant frequency and achieve the desired impedance characteristics for specific applications.

Zero-Phase Shift. When the HIS's resonant frequency $\widehat{\omega}$ aligns with the frequency ω of the impinging magnetic field, the HIS manifests as an "infinite" impedance surface, as evident from Eqn. 5.2. This phenomenon arises because the equation's denominator approaches zero. In this scenario, the magnetic field's reflected phase by the HIS is articulated by

$$\theta = \text{Im}\left(\ln\left(\frac{Z_{\text{HIS}} - \eta_0}{Z_{\text{HIS}} + \eta_0}\right)\right) \approx 0 \tag{5.4}$$

because $Z_{\text{HIS}} \gg \eta_0$. This implies that an HIS can proficiently eliminate the 180° phase shift induced by the half-wave loss, facilitating constructive coupling of the reflected waves via the HIS. By leveraging the properties of the HIS, it becomes possible to significantly reduce the required separation between the HIS and the coil antenna to well below $\lambda/4$. Simultaneously, nearly all of the magnetic energy is constructively redirected to the opposing side of the antenna.

Fig. 5.15 showcases the simulated results of the HIS reflector, utilizing Ansys HFSS [207] as the simulation platform. Throughout the simulation process, the spiral antenna was strategically positioned a mere 10 mm ($\ll \lambda/4$) above the HIS substrate. In the absence of the reflector, as visualized in Fig. 5.15(a), the magnetic field displays a balanced distribution across both the superior and inferior facets of the antenna. Yet, when the reflector is introduced beneath the UHF magnetic antenna, as illustrated in Fig. 5.15(b), there is a pronounced intensification of the field on the antenna's top surface, accompanied by a significant attenuation on its lower side. These results



(a) Without HIS

(b) With HIS

Fig. 5.15: Simulated magnetic intensity without and without an HIS reflector attached to the spiral coil antenna. (a) shows the magnetic field distribution on the antenna's tangent radiation plane without HIS; (b) illustrates the magnetic field distribution with the HIS in place.

vividly demonstrate the prowess of the HIS-based reflector in steering the magnetic field, accentuating the radiation efficiency and gain in the desired direction while simultaneously attenuating undesired emissions. The incorporation of this reflector could lead to power conservation for the antenna due to its innate ability to enhance signal superposition constructively.

5.4.5 Coil Antenna Array

In near-field communications, interactions are primarily driven by magnetic fields, which are divided into reactive and radiative near-field domains. The reactive near-field resides close to the antenna, typically within $0.62\sqrt{D^3/\lambda}$, while the radiative near-field or Fresnel Region extends to about $2D^2/\lambda$, with D representing the antenna's maximum linear dimension(i.e., aperture). For optimal performance, our single coil's outermost circumference is set to λ, making its diameter $D = \lambda/\pi$. Theoretically, the near-field range of a single-turn coil antenna becomes approximately 12cm, which falls short for many practical applications. Despite incremental advancements from components such as capacitor-segmented, multi-turn coils, and the zero-phase reflection of HISs, the range expansion is still insufficient, extending to

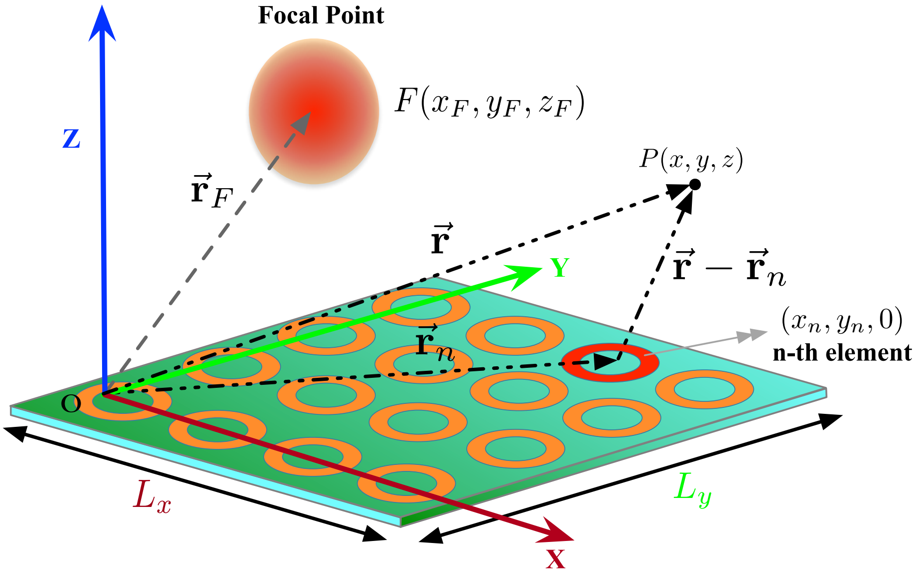


Fig. 5.16: Magnetic Antenna Array forms a near-field focal point at inventory region.

merely 50cm. To ensure comprehensive coverage, we utilize an array of coil antennas to shape the detection zone as needed. As previously discussed, the near-field range R is influenced by the square of the antenna aperture D, following the relationship $2D^2/\lambda$. Consequently, augmenting the aperture by a factor of three through an array setup could lead to a ninefold enhancement in the near-field range.

For an antenna array with N coils, as shown in Fig. 5.16, adjacent coils are spaced by $\lambda/2$. The n^{th} coil's position is represented by $\vec{r}_n$ or coordinates $(x_n, y_n, 0)$ with n spanning from 1 to N. Each coil follows a uniform radiation pattern, denoted as $\widehat{B}(\vec{r})$, indicating the magnetic field vector. This pattern is adjusted based on the decay factor $\frac{1}{R}e^{-\mathbf{J}2\pi R/\lambda}$, where R denotes the maximum operational range. The total magnetic field generated by the array at an observation point $P(x, y, z)$ or $\vec{r}$ is given by:

$$B(\vec{r}) = \sum_{n=1}^{N} C_n B_n(\vec{r}) = \sum_{n=1}^{N} A_n e^{\mathbf{J}\varphi_n} \cdot \widehat{B}(\vec{r} - \vec{r}_n) \cdot \frac{e^{-\mathbf{J}2\pi||\vec{r}-\vec{r}_n||/\lambda}}{||\vec{r} - \vec{r}_n||} \tag{5.5}$$

where $C_n = A_n e^{\mathbf{J}\varphi_n}$ is the n^{th} coil's complex excitation coefficient. Each coil is activated with an amplitude A_n and a modifiable phase φ_n.

To direct the magnetic field towards the ROI, the phase shifts of the N coils' excitation coefficients in the array must be tuned. For a desired concentration of the magnetic field at point $\vec{r}_F$, the distance to the origin is $R_F = ||\vec{r}_F||$ and the unit vector pointing to this spot is $\vec{\hat{r}}_F = \vec{r}/||\vec{r}||$. The conjugate phase method, as referenced in [211, 212], suggests setting each antenna's phase φ_n as:

$$\varphi_n = \frac{2\pi}{\lambda} \|\vec{r}_F - \vec{r}_n\| = \frac{2\pi}{\lambda}\sqrt{R_F^2 + \|\vec{r}_n\|^2 - 2R_F\vec{\hat{r}}_F \cdot \vec{r}_n} \tag{5.6}$$

When R_F is much larger than coil size L, the phase adjustments needed to focus on point F are linear and quadratic. The Fresnel approximation, cited in [213], captures this:

$$\varphi_n \approx -\frac{2\pi}{\lambda}\left(\vec{\hat{r}}_F \cdot \vec{r}_n\right) + \frac{2\pi}{\lambda}\frac{\|\vec{r}_n\|^2}{2R_F} \tag{5.7}$$

A constant phase term, $-2\pi R_F/\lambda$, is omitted as it's relatively insignificant. This approximation is valid with an error under $\pi/8$ if $R_F > \sqrt[3]{L^4/8\lambda}$. However, for closer focal points, necessitating $F \gg L$ to be invalid, Eqn. 5.6 should be used for accurate phase fine-tuning. To achieve complete coverage of a ROI, the array simply needs to adjust its focal point for meticulous traversal of the area. The small size of the area renders the scanning process effortlessly manageable in practical applications. Furthermore, inventory advancements [203, 214, 215] that prioritize tag localization before communication can be swiftly integrated into RFID+, given its primary focus on enhancing the RF frontend, which permits extensive customization for the signal processing backend.

5.5 Fast Inventory

In this section, we incorporate the far-field UHF RFID system with the proposed near-field UHF RFID system to expedite inventory processing for tags within the ROI.

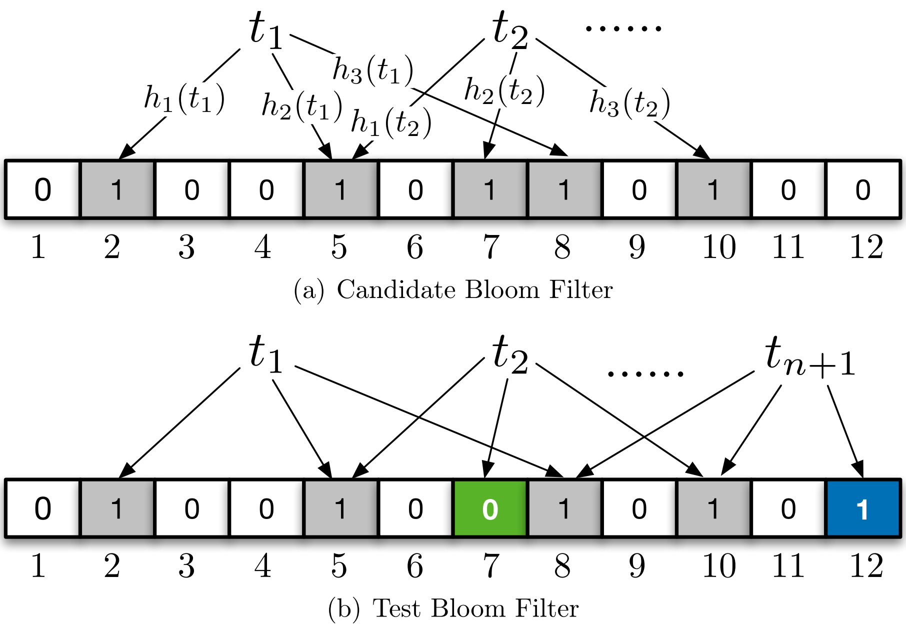
5.5.1 Dual-Coupling Systems

Magnetically-driven RFID systems, despite recent advancements, can only reach a maximum range of about 2.5m, significantly less than the 12m of radiatively-driven RFIDs due to magnetic properties. This constrains their use to smaller ROIs like gates or checkout lanes. Within these narrow confines, a high reading rate, the number of tags recognized per second, becomes essential. Slow readings might miss rapidly moving tags. Fig. 5.2 shows a self-service checkout scenario, where the system must quickly detect all tagged items in a brief timeframe to ensure a smooth customer experience. Currently, prevalent RFID systems use the Q-adaptive anti-collision protocol, a time-division-based ALOHA derivative. As described in [216], the peak efficiency of such protocols is approximately 36.8%. This means nearly 74% of the time is lost to channel contention, posing a significant efficiency challenge.

To mitigate the low efficiency in the channel competition, we present a prefetching mechanism that harmoniously combines both radiatively-driven RFID and magnetically-driven RFID systems to enhance the reading speed within the ROI. In this configuration, one reader interfaces with a patch antenna, while another is connected to our innovatively designed coil antenna. For clarity, the two readers are called *far-field reader* and *near-field reader*, respectively. Both antennas are strategically positioned toward the direction from which the tags approach. As depicted in Fig. 5.2(c), a conceivable setup would have the two antennas suspended above the checkout lane, angled antero-inferiorly. This arrangement ensures that the coil antenna encompasses the entirety of the near-field ROI (approximately the 3m-long lane), while the patch antenna extends its coverage to a broader 10m-long far-field region, inclusive of the ROI and its surrounding area. Leveraging the extended reach of the far-field RFID reader, it becomes feasible to preemptively identify a set of candidate tags expected to traverse through the ROI. While this set might occasionally register cross-readings or omit certain tags, it still offers a substantial advantage by expediting the operations of the near-field reading. In summary, the far-field antenna initially pre-fetch a set of potential tags, enabling the near-field reader to swiftly verify their presence in the ROI based on the far-field's prior knowledge. This time-divided dual-stage approach guarantees that operations in the far-field and near-field do not interfere with each other.

5.5.2 Acceleration via Prefetched Bloom Filter

Utilizing a set of prefetched tags (i.e., candidate tags), there is no longer a need for exhaustive inventory processing in the near-field. Therefore, we employ Bloom filters (BF) to swiftly ascertain the presence or absence of these candidate tags in the region of interest [217–220]. BF is a time-efficient probabilistic data structure that accurately represents the existing set of tags. It can be used to fast test whether an element is a member of the set. As depicted in Fig. 5.17, a Bloom filter succinctly characterizes a set $T = \{t_1, t_2, \ldots, t_n\}$ comprising n tags through an array of M bits, which are initialized to 0. By leveraging K distinct hash functions, denoted as $\{h_1, h_2, \ldots, h_K\}$, each tag is mapped to an integer within the span of $\{1, \ldots, M\}$. For every tag t in T, the bits corresponding to $H = \{h_1(t), \ldots, h_K(t)\}$ are assigned the value 1. Even though a bit might encounter collisions, its value remains 1. To determine if a tag t resides in T, it suffices to verify whether all bits associated with $\{h_1(t), \ldots, h_K(t)\}$ are indeed 1. If even one isn't, then t is not a member of the set. As a case in point, tag t_2 is not part of T as, in the test BF, its seventh bit does not hold the value of 1. If all related bits are 1, we postulate that t is within T, albeit with a caveat: there is a minuscule chance (e.g., < 0.001) of misclassification, leading to a false positive. Moreover, if a particular bit is 0 in the candidate BF but transitions to 1 in the test BF, this alteration indicates the presence of a previously unaccounted-for tag in the ROI. For example, the last bit '1' in the test BF is caused by the uncollected tag t_{n+1} (i.e., $t_{n+1} \notin T$). In less complex situations (e.g., $n < 100$), using a dictionary search method suffices to meet the goals, specifically enabling the system to expedite the inventory process through straightforward dictionary queries. However, with the



(a) Candidate Bloom Filter

(b) Test Bloom Filter

Fig. 5.17: Fast Inventory with Bloom Filters. (a) shows a candidate Bloom filter, which is a concise bitmap representing the collected candidate tags, acquired by the far-field reader. (b) shows the test Bloom filter acquired from the near-field reader on site. By comparing these two bitmaps, we can swiftly discern the tags residing within the ROI. For example, the tag t_2 is a cross-reading, i.e., absent from the ROI, while tag t_{n+1} represents a tag undetected by the far-field reader.

increase in the number of tags, the search time complexity of a dictionary scales linearly as $\mathcal{O}(n)$. On the other hand, BFs offer efficient lookups for tag presence, maintaining fast query times regardless of the dataset's size n, with a complexity of $\mathcal{O}(\log_2(n))$. Therefore, BF is ideally suited for rapid inventory applications in warehouses.

To leverage the prefetched Bloom Filter for accelerating RFID+'s inventory process, the far-field reader first gathers a set of candidate tags, denoted as T, using the time-intensive Q-adaptive algorithm. The EPCs of these collected tags are then used to construct a Candidate Bloom Filter. Notably, the construction does not necessitate any back-and-forth communication between the reader and the tags, but it is generated by the algorithm. Both the EPCs and the BF are passed to the near-field reader via Ethernet cables.

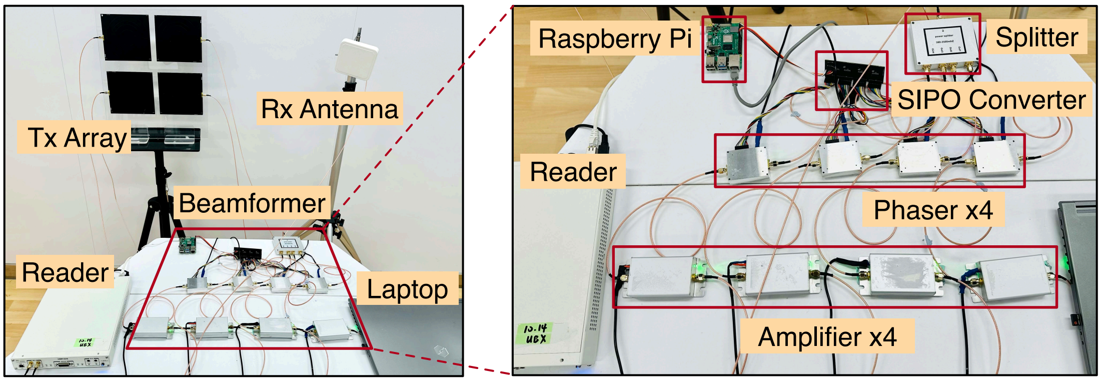


Fig. 5.18: Experiment setup.

In the next phase, the near-field reader uses the previously obtained BF to check for the presence of tags within the ROI quickly. Rather than transmitting their full 96-bit `EPC`s, the tags merely send 16-bit `RN16` packets to indicate their presence, thus speeding up the inventory process significantly. We adopt the method outlined in previous work [217, 221] to test the BF on-site directly, which has theoretically demonstrated that the acquisition overhead is reduced by approximately 60%. The algorithm subsequently performs a comparative analysis to identify which candidate tags are genuinely in the ROI, i.e., checking the slots during which a desired tag responds based on the hashing results. This can be seen as a streamlined polling algorithm that verifies tags against a predefined list of names without the need for channel competition. Finally, for missing tags that are not indicated by the BF, the near-field reader uses the `Select` command to explore them.

5.6 Implementation

In this section, we introduce the system implementation of RFID+ and conduct the microbenchmark on coil arrays.

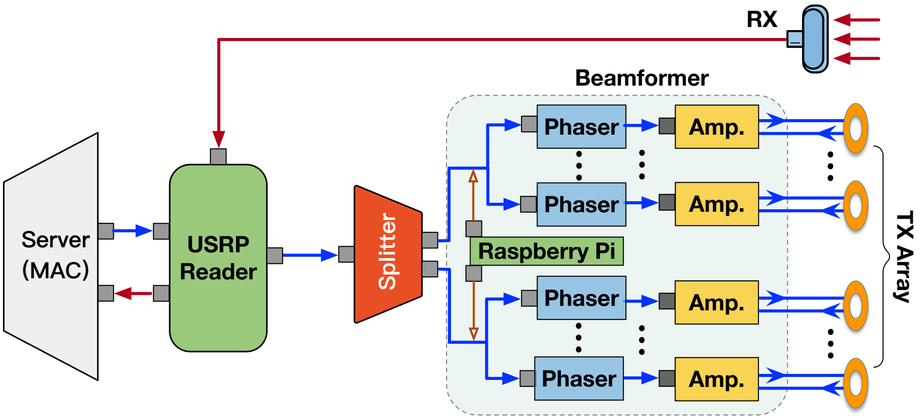


Fig. 5.19: Illustration of Near-Field Reader.

5.6.1 Fabrication

Given that RFID+ utilizes dual-coupling to blend far-field and near-field characteristics, it necessitates two distinct sets of reader hardware for implementation in actual deployments. Specifically, a commercial Impinj R420 reader [204], accompanied by its patch antenna, serves as the far-field reader in our prototype. In contrast, the near-field reader is custom-constructed around the foundation of the USRP X310 [205].

- **Near-Field Reader**. Our near-field reader prototype is anchored in the capabilities of the USRP X310, which boasts two independent RF frontend configurations. One interface is dedicated to an array of coil antennas for transmission (TX). The secondary interface liaises with a compact patch antenna designed for reception (RX). It should be noted that integrating the TX and RX into a monostatic mode is technically feasible and would further reduce the system's size, benefiting dynamic scenarios. The detailed architecture of the near-field reader is illustrated in Fig. 5.19. After undergoing upconversion in the USRP, the emergent signal is bifurcated, creating four separate paths. These distinct routes are meticulously controlled by analog phasers, specifically the PHSA-152+ model from Mini-Circuits [222]. These state-of-the-art phasers grant a high level of precision in phase adjustments, offering an impressive eight-bit granularity. Following this, the signals are subjected to an amplification process, ensuring they achieve a robust transmission power of 30 dBm. Subsequently, these fortified signals are disseminated by an ensemble of four coil antennas. To streamline and synchronize the operations of the phaser units, a Raspberry Pi 4 Model B [223] is strategically deployed, acting as the central coordination hub with the aid of a customized Serial-In to Parallel-Out (SIPO) Converter.

• **Coil Array**. At the heart of the system lies a 2×2 coil antenna array, encompassing four distinct coil antennas, each of which has a 75mm radius and about 1.4λ circumference. (see Fig. 5.13). The exact size and shape of the antenna are determined through iterative optimization to enhance the near-field magnetic intensity. As depicted in Fig. 5.18, these antennas are integrated onto a two-layer 1.6mm FR-4 printed circuit board (PCB), with HIS reflectors secured to the rear via plastic standoffs. They operate primarily around the 920MHz. Performance enhancement is achieved with an impedance-matching circuit, aligning the antenna to the 50Ω RFID reader standards. Each antenna unit, measuring 17cm by 16cm, incurs an approximate manufacturing expense of $65.53, as detailed in Table. 5.3.

5.6.2 Microbenchmark

Before embarking on a detailed performance evaluation, we initially provide a quantitative analysis of the performance improvements attributable to each antenna design component.

• **Component Gain**. We used a magnetic field probe to measure the H-field strength induced by each component of the designed antenna, assessing their respective gains. Different coils, such as conventional single-turn, segmented-line single-turn, multi-turn, along with HIS reflectors, were constructed for evaluation. The data in Tab. 5.1 show that the gains from the capacitor-segmented, multi-turn, and directional components were 3.01 dB, 1.96 dB, and 1.68 dB, respectively, contributing to a total increase of 6.65 dB in the H-field's peak strength.

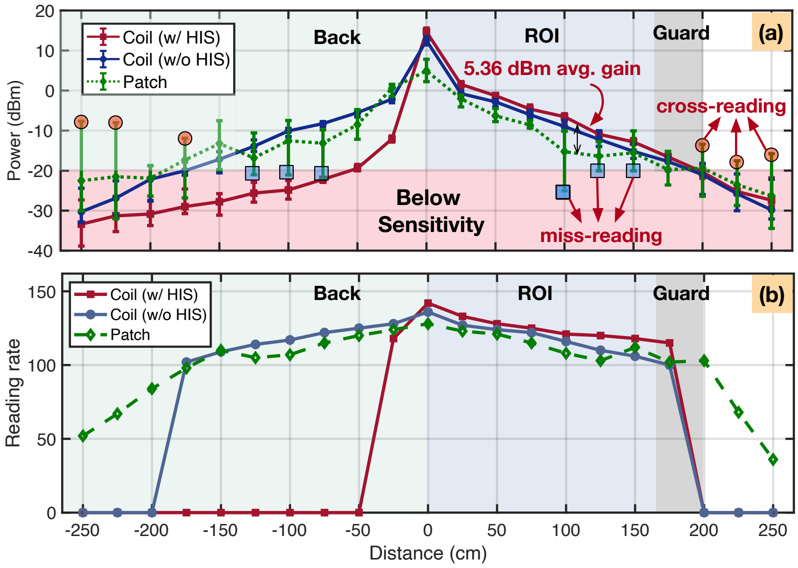


Fig. 5.20: Controllability Analysis across Different Antennas.(a) and (b) show the signal strength and reading rate as a function of distance, respectively.

Next, we characterize the coil array by analyzing the engineered coil antenna's attributes. We examined three distinct configurations: the novel coil array with and without an HIS, and a traditional electrical patch antenna devoid of a reflector. For experimental purposes, the antenna was positioned on the XOY plane. Here, positive (or negative) distances signify locations either ahead of (or behind) the antenna along Z-axis. Each configuration was subjected to 20 trials. The reader's transmitting power was consistently maintained at 30dBm.

- **Strength Distribution**. We analyzed the magnetic field distribution in radiative regions using a spectrum analyzer [224] coupled with magnetic field probes, as depicted in Fig. 5.20(a). (1) Frontside: In front of our coil antenna, magnetic strength gradually decreased with little variation. Conversely, the EM field from the patch antenna fluctuated significantly, with strengths ranging from -25 to 11dBm@100cm.

Table 5.1: Each Components' Impact on H-Field Boost.

Elements	Segmented	Multi-turn	HIS	**Total**
Gain (dB)	3.01	1.96	1.68	**6.65**

Considering a sensitivity threshold of -20dBm [225], the patch antenna could cause miss-readings @100-200cm and potential cross-readings @200-250 cm due to EM field unpredictability. (2) Backside: Behind the coil, the strength quickly fell below the sensitivity level, attributed to null-phase-shift reflections from the HIS. These reflections added an average 1.68dB gain to the frontside magnetic field, equivalent to a 1.5 times power gain. Our findings emphasized the heightened issues of miss-reading and cross-reading in traditional RFID antennas. In contrast, magnetic antennas exhibited enhanced controllability due to reduced multipath propagation effects. This study underscores the superiority of the proposed coil antenna and HIS in spatial control.

- **Effective Coverage**. Reading rates, defined as the number of readings recognized per second (r/s), were gathered across a range of -250 to 250 cm. The results are portrayed in Fig. 5.20(b). Frontside: Within 25-175 cm, the coil antenna consistently showed high reading rates of 115-133 r/s. Beyond 175 cm, this rate drops to zero, mirroring the observed decline in magnetic strength and indicating precise ROI control. Conversely, the patch antenna's reading capability persists beyond 200 cm, capturing nearly 36 r/s at 250 cm. Backside: Beyond -50 cm, the coil antenna w/ HIS reading rate swiftly drops to zero. However, both the coil w/o HIS and the patch antenna display similar reading rates on the backside as seen on the frontside.

Summary. The outcomes of these two experiments emphatically demonstrate the heightened controllability presented by the proposed coil array in both the physical and application dimensions relative to traditional electronic patch antennas. Further, the data suggests a maximum effective range of 175cm plus a 25cm guard zone.

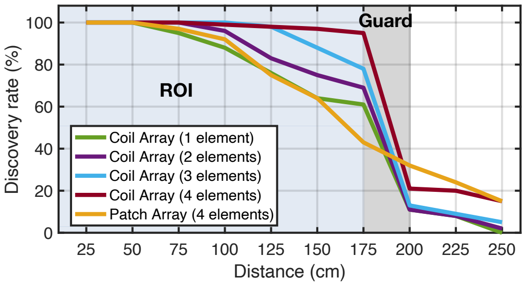


Fig. 5.21: Inventory Accuracy

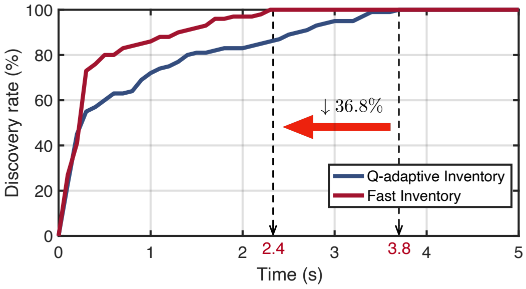


Fig. 5.22: Inventory Efficiency

5.7 Evaluation

In this section, we conduct a group of experiments within a sizable office measuring 50 m^2 full of multipath reflectors to evaluate RFID+ comprehensively.

5.7.1 Inventory Accuracy

We conducted a comparative analysis of RFID+ versus conventional RFID systems, centered on inventory accuracy. Both systems employed a 2×2 antenna array, with the former utilizing the proposed coil and the latter using a conventional patch antenna. In our test, a dense collection of 100 tags were fixed to a flat surface. The accuracy was measured based on the discovery rate, i.e., the percentage of unique tags identified from the total of 100 tags.

The results are shown in Fig. 5.21. From the figure, we have two main findings: First, RFID+ boasts near-perfect detection within the ROI, identifying almost all tags for distances up to 175cm. Beyond this zone, the detection drops drastically. Traditional RFIDs maintain a good detection rate only up to 100cm, and their performance diminishes past this point, mostly due to environmental reflections. Second, the number of coils in the array influences detection reach. Distances of flawless detection were reduced to 125cm, 100cm, and 75cm for arrays with 3, 2, and 1 coils, respectively. Overall, RFID+ offers better ROI management than standard RFIDs.

5.7.2 Inventory Efficiency

We introduce a Bloom Filter-enhanced fast inventory algorithm to expedite the near-field reader's inventory process as discussed in Sec. 5.5. Leveraging prefetched tags, the far-field reader constructs Bloom Filters to ascertain tags within the ROI swiftly. We compared this approach against conventional inventory methods. Initially, an electronic antenna gathers EPCs from 100 tags, out of which only 30 prefetched and 20 miss-read tags arrived at the near-field ROI. The efficiency is gauged by the discovery rate over time. As illustrated in Fig. 5.22, our fast inventory approach completes the discovery in 2.4 seconds, contrasted with the 3.8 seconds by the Q-adaptive algorithm. This marks a 36.8% efficiency boost, primarily due to the omission of anti-collision procedure.

5.7.3 Spatial Controllability

Next, we examine RFID+'s capability in finely tuning the beamforming focal point using the coil array. The focal point represents the peak of energy concentration derived from the coordinated quartet of coils. We directed the system's focus to five positions along the Z-axis: 40, 60, 80, 100, and 120cm. For each position, a tag was moved from 10cm to 120cm, and the backscattered signal strength was measured.

The findings are illustrated in Fig. 5.23. As anticipated, signal strength peaked exactly at the 40cm, 60cm, and 80cm marks when directed there. Beamforming focal point increases the average received signal strength (RSS) by approximately 7.73 dB at these locations. However, at 100cm and 120cm, the peaks lagged by 10cm, likely due to power dissipation effects, namely, the combined power from the four coils is unable to compensate for the losses experienced over extended distances. This observation is further mirrored in the peak values decreased with distances, i.e., from -42.3dBm to -46.5dBm, -50.2dBm, -51.5dBm, and -53.7dBm. Such precision in focal adjustments is unparalleled, making it invaluable for specialized scenarios like detecting tags in

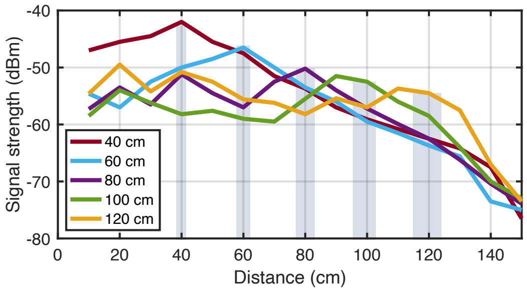


Fig. 5.23: Spatial Manipulation

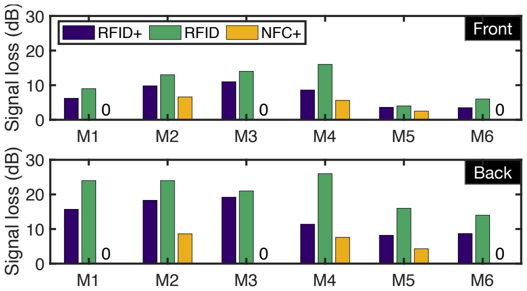


Fig. 5.24: Penetrability

containers or conveyors.

5.7.4 Penetrability

We assess the penetration capabilities of RFID+, NFC+ [70], and traditional RFID when tags are positioned on the front (LoS) and backside (NLoS) of various liquid products. Our experiment evaluates six distinct products: M1 (64mm-thick bottled water), M2 (48mm-thick canned Coke), M3 (40mm-thick bottled Coke), M4 (85mm-thick boxed milk), M5 (45mm-thick boxed milk), and M6 (64mm-thick Bottled beer). Such liquid bottles are placed 50cm ahead of the antenna array, which is linked to an Impinj R420 reader used to measure the signal strength.

Fig. 5.24 illustrates the difference of signal strengths (i.e., loss) acquired when a tag is either affixed to a product or not, respectively. Notably, NFC+, operating at 13.56MHz, exhibits superior performance in most scenarios due to its reduced vulnerability to water interference. Conversely, UHF frequency signals experience higher absorption by water molecules, leading to increased signal loss. Yet, RFID+ surpasses standard RFID systems, registering average losses of 7.1dB and 13.5dB on the product's front. These losses rise to 13.5dB and 20.8dB for RFID+ and RFID, respectively, on the back. In summary, RFID+ demonstrates potent penetration for liquid products with thicknesses less than 60mm, particularly near the ROI.

5.7.5 Versatility

To underscore the versatility of the magnetically-driven approach, we tested ten tags from leading manufacturers such as Impinj [226], Alien [227], NXP [228], and Laxcen [229]. Their performance is reflected in reading rates, outlined in Table. 5.2. Reading rates ranged from 105 to 129, with Impinj's H47 tag outperforming the rest and Alien's 9654 tag at the lower end. These differences are likely due to variations in the tags' internal loop structures. Broadly speaking, tags with larger loop diameters tend to register a heightened coupling coefficient, leading to better reading rates. However, every tag was effectively recognized by the magnetically driven reader, highlighting the universal efficacy of our solution.

5.7.6 Compared with Related Systems

In a parallel comparison, RFID+ outperforms the state-of-the-art RFID inventory solution RFGo [82] with respect to generality, cost, and deployment ease: First, RFID+ enables seamless plug-and-play functionality in dynamic environments without the extensive data collection and training RFGo requires. Moreover, RFID+ proves to be more budget-friendly, employing a limited number of lower-cost hardware compo-

Table 5.2: The configuration and reading rate of different tags.

Tag(#)	MFR.	IC	Model	Size(mm^2)	Reading rate
T1	Impinj	Monza 4QT	H47	50 × 50	129
T2		Monza R6	ER62	74 × 18	119
T3	Alien	Higgs 3	9662	70 × 17	121
T4		Higgs 3	9640	94.8 × 8.25	126
T5		Higgs 3	9654	93 × 19	105
T6		Higgs 3	9962	73.5 × 20.2	117
T7	NXP	Ucode8	U9624	98 × 27	105
T8		UR108	U7015	70 × 15	126
T9	Laxcen	Monza 4QT	C90G	90 × 20	107
T10		Monza 5	C50D	50 × 30	106

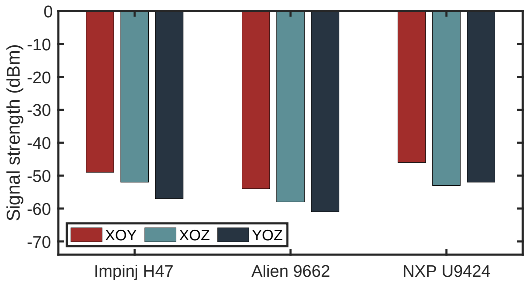


Fig. 5.25: Impact of tag orientation

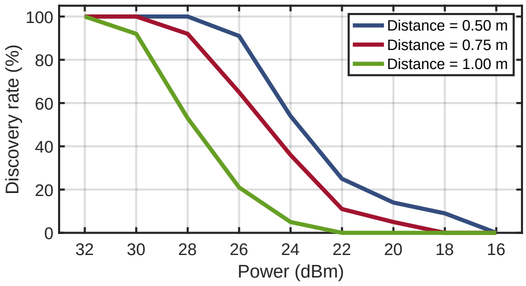


Fig. 5.26: Impact of Tx power

nents like magnetic coils, phase shifters, and HIS reflectors (see cost breakdown in Tab. 5.3), in contrast to RFGo's intricate setup involving 11 USRP X310 units and numerous antennas. Lastly, setting up RFID+ is straightforward, requiring only two perpendicular surfaces, unlike RFGo's complex three-dimensional antenna configuration.

5.7.7 Impact Analysis

Finally, we consider the two potential factors that affect the performance of RFID+.

- **Impact of Tag Orientation.** We investigate the role of tag orientation in determining RSS. Three distinct tags, namely Impinj H47, Alien 9662, and NXP U9424 are positioned 50cm from the coil array. These tags are aligned parallel to the XOY, XOZ, and YOZ planes, with the coil array set on the XOY plane. Fig. 5.25 presents the RSS from the backscatter signals for each tag across the three configurations. Clearly, optimal RSS is achieved when the tag orientation is parallel to the coil array

Table 5.3: Pricing Estimation for BOM List of One Antenna Unit

Item (#)	Component	Description	Quantity	Price ($)
1	Coil Antenna	Two-layer PCB	1	5.42
2	HIS Reflector	Two-layer PCB	1	3.06
3	RF Amplifier	SKY65111-348LF	1	2.64
4	Phase Shifter	SPHSA-152+	1	50.41
5	Micro Controller	Raspberry Pi Pico	1	4.00
Total Cost				**65.53**

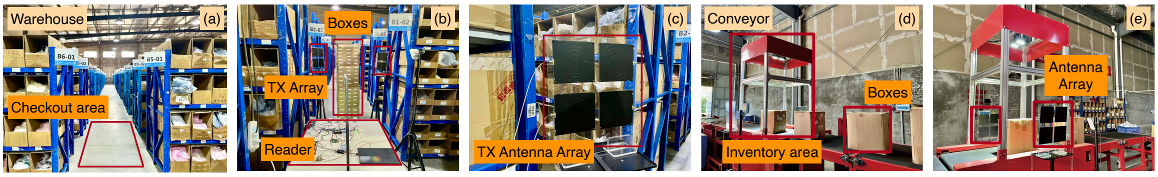


Fig. 5.27: Deploying RFID+ in real-world logistics networks. (a-c) show the application in warehouse management, whereas (d-e) illustrate the application in supply chain planning.

(i.e., XOY), as this allows maximum magnetic flux to traverse the tag's matching loops. Conversely, the least favorable setup is the YOZ orientation, where minimal flux interacts with the coils. This orientation sensitivity poses a recurring challenge in RFID systems, attributed to the use of planar antennas in tags. A practical workaround involves deploying multiple coils in varied orientations to mitigate such orientation-based discrepancies.

- **Impact of Transmission Power**. We investigated the influence of transmission power on the discovery rate, situating tags at intervals between 0.5 m and 1 m from the reader. As depicted in Fig. 5.26, the discovery rate correlates inversely with decreasing power levels from 32 dBm to 16 dBm. Notably, when transmission power diminishes below 26 dBm, the discovery rate plunges to under 20% for a 1 m distance setting. Moreover, an increased separation between the reader and tags further depresses the rate. For example, at a robust transmission power of 28 dBm, the discovery rate remains optimal at 100% for a 0.5 m distance. Yet, when the distances extend to 0.75 m and 1 m, the rates taper off to 70% and 48%, respectively. This underscores that RFID+, akin to traditional RFID systems, is power-sensitive, primarily because energizing the passive tags consumes a significant portion of the transmitted energy.

5.8 Pilot Study: Logistic Network Evaluation

5.8.1 Warehouse Management

We tested RFID+ in a textile factory warehouse with an annual revenue of 100 million USD for contact manufacturing of branded apparel. The factory uses both RFID and barcodes for identification, shown in Fig. 5.27 (a-c). We set up two 2 × 2 RFID+ antenna arrays near storage shelves. Over 200 tags were attached to clothing items like T-shirts and jeans, packed in garment boxes, and moved on a Manual Hand Pallet Jack. The number of tags is subject to the Manual Hand Pallet Jack's maximum capacity and aligns with values reported in earlier studies [72, 82]. As items passed through the scanning zone, RFID+ logged the detected products. Fig. 5.28 depicts the performance of RFID+, as determined by the mean outcome of ten replicated trials that collectively involved more than 2,000 tags. It detected 98.94% of tags at the gateway, outperforming the commercial radiatively-coupled RFID system's 77.14%. This is because approximately 10% of the regions are blind spots for reading with conventional radiatively-coupled RFID electrical antennas [201, 230, 231]. When five volunteers, including two students and three workers, manually counted with barcode scanners, the traditional optical barcode identification system noted about 97%. Hence, RFID+ demonstrated superior accuracy against both commercial RFID and manual counts. For cross-reading accuracy, we established a 2m×2m ROI around the coils/antennas and placed tags randomly at its edges. The results in Fig. 5.28 show RFID+ had a negligible 0.09% cross-reading rate, significantly less than the UHF RFID system's 42%. The manual method registered 1.4%, a number potentially increasing with working overtime. In summary, RFID+ excels in minimizing cross-reading and miss-reading when contrasted with both traditional RFID systems and manual inventory methods. It is even capable of approaching the performance of the state-of-the-art (SOTA) system, NFC+ [70], which records a mere 0.03% rate of miss-readings and a zero cross-reading rate for randomly oriented objects. The

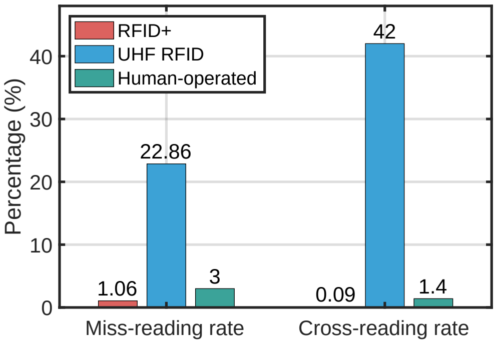


Fig. 5.28: Performance in Warehouse

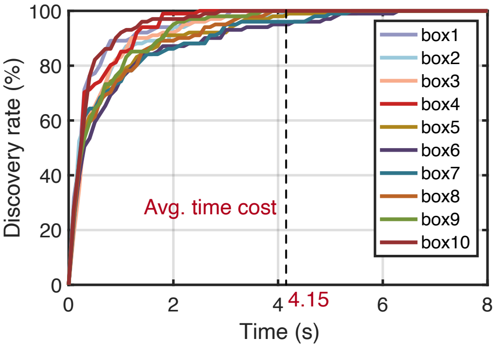


Fig. 5.29: Performance in Logistics

comparison in Appendix 5.7.6 also highlights RFID+'s outperformance over another SOTA system RFGo [82] in terms of generality, affordability, and ease of deployment.

5.8.2 Supply Chain Planing

We further explored RFID+'s efficacy in a supply chain setting, wherein boxed products traverse through a conveyor scanning gateway. This conveyor bridges the warehouse and the truck's cargo hold. We demarcated an inventory zone (i.e., ROI) on the conveyor, dimensions being $1.5 \times 0.5 \times 1.6\text{m}^2$, as visualized in Fig. 5.27(d-e). Each box, housing around 150-200 garments based on the apparel type, is strategically positioned on the conveyor at 1.5m gaps. Whenever a box enters the designated zone, the conveyor intuitively reduces its speed for inventory purposes. Given the tags' movement on the conveyor and the minimal interference risk from neighboring tags due to the deliberate spacing, our system consistently showcased flawless performance without any miss-reading or cross-reading instances. Fig. 5.29 portrays the discovery rate vis-a-vis the time expenditure for ten sequential boxes. An average time consumption of roughly 4.15 seconds is observed for each box. This testing underscores RFID+ 's prowess to seamlessly integrate into real-world industrial settings, where UHF RFID consistently sidesteps both miss-reading and cross-reading, all within a reasonable timeframe.

5.9 Conclusion

This work introduces RFID+, a highly accurate and reliable system for RFID tag inventory. RFID+ utilizes the tailored magnetic field to achieve a 99% discovery rate within the ROI, simultaneously preventing cross-reading of tags outside this area. Our warehouse analysis indicates that RFID+ has the potential to revolutionize the logistics industry.

Chapter 6

Conclusions and Future Works

6.1 Conclusions

Controllable magnetic inductive coupling techniques have garnered significant interest across both academic and industrial spheres, driven by the rapid evolution of advanced mobile systems. The potential applications of controllable magnetic coupling extend far beyond just wireless charging and NFC technologies. There is a pressing need to explore broader applications of this technology within current mobile systems, particularly in the context of the burgeoning Internet of Things era. Expanding the scope of controllable magnetic inductive coupling could unlock the full potential of magnetic fields, enhancing connectivity, functionality, and security across a diverse range of devices and platforms. This expansion is not only imperative for technological advancement but also critical in meeting the increasing demands for smarter and more integrated digital ecosystems.

This dissertation delves into the security challenges and introduces innovative applications in mobile systems through the use of temporally and spatially controllable magnetic inductive coupling, spanning frequencies from the LF to the UHF band. It extends the traditional scope of magnetic inductive coupling, demonstrating its versatility and utility in enhancing mobile system interoperabilities and addressing security vulnerabilities. Specifically, this research makes contributions by developing methodologies that not only improve the robustness of mobile systems against security threats but also pioneer the use of magnetic inductive coupling in new application domains. These contributions are detailed as follows:

- ***Controlled Magnetic LF Coupling**: Inaudible Voice Attacks and Countermeasures.* This work has uncovered a significant vulnerability in voice systems caused by LF magnetic coupling during wireless charging. It has been shown that conventional protective measures are inadequate to counter low-frequency magnetic interference, which can be exploited to inject malicious voice commands into smart devices. Through the introduction of HeartwormAttack and ParasiteAttack, this study demonstrated how compromised wireless chargers can act as vectors for security breaches. The success of these attacks highlights the urgent need for more effective electromagnetic compatibility strategies at lower frequencies. By proposing robust countermeasures that incorporate both software and hardware approaches, this research aims to strengthen the security architecture of smart devices against emerging electromagnetic threats, raising awareness and advocating for more secure designs in the rapidly evolving IoT landscape.
- ***Controlled Magnetic HF Coupling**: NFC-to-Camera Mobile Payment System.* This work has introduced an innovative physical side-channel communication system called MagCode, which utilizes magnetic interference from NFC readers to enable mobile payments through camera-based barcode-like stripe recognition. This approach overcomes the limitations of NFC functionality in legacy smartphones, significantly increasing the accessibility of secure mobile payment solutions. Through extensive testing on multiple devices, we validated the efficiency and speed of the MagCode system, demonstrating its superiority over existing magnetometer-based solutions. This groundbreaking application of magnetic inductive coupling not only enhances the capabilities of mobile devices but also opens new avenues

for secure, high-frequency communication, improving user experience in contactless transactions.

- ***Controlled Magnetic UHF Coupling***: *Spatially Controllable RFIDs Inventory.* This work has presented RFID+, a UHF near-field communication system that establishes a new standard in traditional RFID technology by achieving unparalleled spatial precision in RFID tag identification, drastically reducing miss-reading and cross-reading rates. Central to this advancement is the development of a specialized multi-turn, capacitor-segmented coil antenna, which successfully replicates the near-field characteristics of LF/HF systems within the UHF spectrum, addressing long-standing challenges in RFID technology. This innovation not only improves the accuracy and efficiency of RFID systems but also demonstrates the system's resilience in identifying materials that have traditionally posed difficulties. By extending controllable magnetic inductive coupling into the UHF band, RFID+ provides a transformative solution for complex logistical applications, paving the way for future breakthroughs in RFID technology.

Through these diverse applications—ranging from protecting voice command systems against novel attacks, enabling NFC-like payments on devices without NFC capabilities, to transforming UHF RFID near-field communication for logistical applications—this dissertation has made substantial advancements in the field of controllable magnetic inductive coupling. By extending the boundaries of what is possible in both established and emerging mobile technologies, this research not only enriches academic understanding but also delivers practical solutions with tangible real-world benefits. It establishes a solid foundation for further exploration and innovation in controllable magnetic inductive coupling technologies, with the goal of enhancing security and advancing the seamless integration of intelligent systems into everyday life.

6.2 Future Works

6.2.1 LF Magnetic Coupling-Driven Attacks & Countermeasure for Acoustic Sensing

Research Background

Recently, acoustic sensing on smartphones has attracted significant attention from both industry and research communities due to its distinct advantages. One of the key benefits of acoustic signals is their relatively low propagation speed in air, approximately 340 m/s, compared to electromagnetic signals, which travel at 3×10^8 m/s. This slower propagation speed allows acoustic sensing to achieve much finer sensing granularity. The foundation of acoustic sensing lies in the use of Frequency-Modulated Continuous Wave (FMCW) sonar. FMCW sonar transmits a chirp signal with an instantaneous frequency that increases linearly over a predefined sweeping period. When these signals encounter objects in the environment, they reflect back to the sonar with a time delay. By comparing the frequencies of the transmitted and received signals, the sonar calculates the time delay, enabling it to extract detailed information about the surrounding environment.

Commodity microphones and speakers embedded in widely available devices like smartphones and laptops enable powerful acoustic sensing capabilities. For example, studies have demonstrated sub-millimeter precision in monitoring vital signs, supporting applications such as fine-grained heartbeat monitoring [232, 233] and eye-blink motion detection [234]. These advancements highlight the potential of acoustic sensing to transform everyday devices into versatile sensing platforms. However, the security considerations for these techniques remain largely underexplored. Despite their utility in applications like health monitoring and environmental sensing, acoustic sensing systems are susceptible to vulnerabilities such as privacy breaches from unauthorized data access and spoofing attacks that mimic legitimate signals to disrupt functionality. Investigating potential security threats is essential to ensure the safe and dependable integration of acoustic sensing into consumer devices and critical systems.

Future Direction: Exploiting Vulnerabilities in Acoustic Sensing Systems

One notable application scenario of acoustic sensing involves utilizing the internal microphone and speaker of a smartphone to assist in clinical diagnoses. This technology helps assess a patient's overall health, monitoring whether their physical condition is improving or deteriorating during sleep. With the rapid adoption of wireless charging technologies in smart homes, many people now use wireless chargers to power their smartphones while sleeping. This shift presents an opportunity to exploit controllable LF magnetic inductive coupling from wireless chargers to launch attacks on acoustic sensing systems while the victim charges their phone overnight.

To inject inaudible voice commands into smartphones, two potential attack schemes can be employed: intrusive and non-intrusive approaches.

- **Intrusive Attack:** In this scenario, the attacker compromises the wireless charger by hacking its internal MCU and peripheral circuits. By manipulating these components, the attacker can inject inaudible voice commands into the smartphone's microphone. Similar to the *HeartwormAttack*, this method exploits the nonlinearity of the microphone's amplifier, allowing magnetic interference signals from the charging frequency to downconvert into the microphone operating spectrum, thereby disrupting the recorded chirp signals used for normal acoustic sensing. An adversary might install malware into the wireless charger during the manufacturing process. Once compromised, the charger can opportunistically interfere with, forge, or tamper with acoustic sensing signals, undermining the system's integrity.
- **Non-intrusive Attack:** Alternatively, an attacker can attach a parasite-like label

to the wireless charger to mislead victims. This parasite device is placed between the host wireless charger and the smartphone and operates as a compact, battery-free device designed to be inconspicuous. The parasite consists of an inner RX coil and multiple outer TX coils. Once the power transfer contract is established, the parasite harvests energy from the underlying charger using its inner RX coil and boosts its attack through the outer TX coils. The outer TX coils are arranged in a ring formation, ensuring that at least one coil is positioned near the smartphone's microphone, regardless of the device's orientation. This method directly generates a magnetic field at the voice frequency, which further induces magnetic interference signals at the microphone, enabling the non-intrusive attack.

These attack strategies highlight the vulnerabilities of smartphone-based acoustic sensing systems to LF-band magnetic inductive coupling, particularly in wireless charging scenarios. Mitigating these risks is essential to ensure the security and reliability of acoustic sensing applications, providing a valuable direction for future research and development.

6.2.2 UHF Magnetic Coupling-Driven RFID Inventory Acceleration Optimization

Research Background

The UHF magnetic coupling-driven RFID inventory system demonstrated in [235] has shown its ability to support spatially controllable identification through precise magnetic focus points. This capability arises from the use of a tailored magnetic antenna, which maintains a uniform magnetic field distribution across the near-field zone, even at UHF frequencies. However, despite these advancements, magnetically-driven RFID systems are inherently limited by near-field zone properties, achieving a maximum range of approximately 1.5 meters—significantly shorter than the 12-

meter range of radiatively-driven RFID systems. As a result, their application is largely confined to smaller regions of interest (ROIs), such as gates or checkout lanes. Within these restricted areas, achieving a high reading rate, defined as the number of tags identified per second, becomes crucial. Low reading speeds increase the risk of missing tags that move quickly through the ROI.

Currently, most RFID systems utilize the Q-adaptive anti-collision protocol, a time-division-based derivative of the ALOHA protocol. As highlighted in [216], the peak efficiency of these protocols is only about 36.8%, meaning nearly 74% of the time is lost to channel contention, posing a significant challenge to overall efficiency. To address this issue, Section 5.5 proposes a prefetching mechanism that integrates radiatively-driven and magnetically-driven RFID systems to enhance reading speed within the ROI. However, this approach has several limitations. First, it is not cost-effective, as it requires the simultaneous deployment of both near-field and far-field RFID readers, significantly increasing system complexity and expense. Second, the prefetching mechanism relies on prior knowledge of tag information (i.e., `EPC`) to construct a Bloom filter. Newly added tags that are not pre-registered will be immediately overlooked, reducing the system's flexibility. Additionally, current fast inventory algorithms are primarily suited for "roll-call" scenarios, where only one-bit [217] or RN-16 responses are used as indicators of tag presence. In cases where the full EPC data is required for inventory purposes, these algorithms fail to meet the demands.

To meet the demands of narrow inventory zones with high throughput requirements, it is imperative to explore more efficient and cost-effective fast inventory schemes. Developing faster and more adaptive strategies will be critical to addressing these challenges and unlocking the full potential of magnetically-driven RFID systems in constrained environments.

Future Direction: Minimizing Retransmissions in RFID Communication

In scenarios requiring full EPC data for inventory purposes, the absence of an effective forward error correction (FEC) mechanism presents a significant limitation in current RFID systems, leading to time-consuming retransmission processes. FEC improves error control in data transmission by incorporating redundant data at the transmitter (e.g., tags), enabling the receiver (e.g., a reader) to decode the original information with the help of these additional bits. However, the existing cyclic redundancy check (CRC) mechanism used in traditional RFID systems' EPC only verifies data integrity by checking the correctness of received bits. When bit errors occur, the CRC cannot correct them, resulting in the need for tags to retransmit their EPCs in subsequent rounds, which causes considerable communication time overhead. This issue is exacerbated in low SNR conditions, where decoding reliability decreases significantly. For example, in warehouse environments, the decoding success rate for EPC is typically lower than that for RN16. Ideally, these rates should be equal, as each EPC request relies on a preceding successful RN16 acknowledgment. At low SNR levels, the success decoding rate for RN16 remains around 90%, whereas the success rate for EPC drops sharply to just 60%, resulting in substantial retransmission delays during inventory processes. Despite its critical consequences, the issue of unreliable transmission has not been adequately addressed.

To enable a faster inventory, a potential solution is incorporating FEC into the EPC decoding process. Polar code [236], introduced by Erdal Arikan, is a type of error correction code that can achieve the capacity of binary-input discrete memoryless channels, making it an ideal candidate for reducing retransmissions and enhancing reliability. However, implementing polar codes in RFID systems poses challenges due to hardware incompatibility. In conventional communication systems like Wi-Fi or 5G, dedicated circuits for FEC encoding and decoding are present in the frontend. RFID tags, however, lack encoder circuits for polar codes, making it challenging to directly adopt polar-coded EPCs using commercial off-the-shelf tags.

A promising direction for future research is the concept of "EPC tunneling," inspired by IPv6 tunneling, which encapsulates IPv6 packets within IPv4 packets to ensure compatibility with existing infrastructure. In a similar vein, EPC tunneling enables existing RFID tags to transmit polar-coded `EPC`s without requiring hardware modifications. This process involves two main steps: First, the original 96-bit `EPC` is pre-encoded into a 128-bit (or optionally 256-bit) polar code. The `EPC` length in tags can be extended by modifying the *protocol-control* word as defined in the Gen2 protocol. Second, a software-defined RFID reader [237] overwrites the tag's memory with the `PolarEPC`, a polar-coded representation of the `EPC`. When the reader requests the `EPC`, the tag directly transmits the `PolarEPC`, bypassing the need for onboard encoding. Then, the received `PolarEPC` is processed through a polar code decoder at the application layer level to correct potential bit errors and retrieve the original `EPC` information. As a result, polar codes provide robust protection against interference that might otherwise introduce bit errors, allowing the reader to reliably reconstruct the intended data from the corrupted `PolarEPC`. This innovative technique can enable polar-coded transmissions while ensuring full compatibility with current RFID systems.

The advantages of EPC tunneling are evident. It maintains high compatibility with the Gen2 protocol and remains transparent to upper-layer applications, ensuring seamless integration with existing RFID infrastructure. Moreover, polar-coded packets transmitted over the air exhibit enhanced resilience to channel interference, significantly improving reliability in environments with high noise or interference. Consequently, EPC tunneling effectively meets the fast inventory requirements of near-field RFID communication by eliminating the time overhead associated with retransmissions. By addressing key limitations of current RFID technologies, EPC tunneling represents a significant step forward in developing robust, fast, and future-proof RFID inventory solutions.

References

[1] International Data Corporation (IDC), "Idc report on mobile technology trends," https://www.idc.com/getdoc.jsp?containerId=prUS52655324, 2024.

[2] L. Dodds, I. Perper, A. Eid, and F. Adib, "A handheld fine-grained rfid localization system with complex-controlled polarization," in *Proc. of ACM MobiCom*, 2023, pp. 1–15.

[3] Z. Zhang, Y. Liu, Z. Wang, X. Mu, and J. Chen, "Physical layer security in near-field communications," *IEEE Transactions on Vehicular Technology*, 2024.

[4] Y. Liu, C. Ouyang, Z. Wang, J. Xu, X. Mu, and A. L. Swindlehurst, "Near-field communications: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, 2024.

[5] NFC Forum, "Use cases for wireless charging," https://nfc-forum.org/learn/use-cases/wireless-charging/, 2024.

[6] E. Strommer, M. Jurvansuu, T. Tuikka, A. Ylisaukko-Oja, H. Rapakko, and J. Vesterinen, "Nfc-enabled wireless charging," in *2012 4th International Workshop on Near Field Communication.* IEEE, 2012, pp. 36–41.

[7] Z. Zhang, Y. Liu, Z. Wang, X. Mu, and J. Chen, "Simultaneous wireless information and power transfer in near-field communications," *IEEE Internet of Things Journal*, 2024.

[8] T. Imura and Y. Hori, "Maximizing air gap and efficiency of magnetic resonant coupling for wireless power transfer using equivalent circuit and neumann formula," *IEEE Transactions on industrial electronics*, vol. 58, no. 10, pp. 4746–4752, 2011.

[9] N. Oodachi, K. Ogawa, H. Kudo, H. Shoki, S. Obayashi, and T. Morooka, "Efficiency improvement of wireless power transfer via magnetic resonance using transmission coil array," in *2011 IEEE International Symposium on Antennas and Propagation (APSURSI)*. IEEE, 2011, pp. 1707–1710.

[10] A. Berger, M. Agostinelli, S. Vesti, J. A. Oliver, J. A. Cobos, and M. Huemer, "A wireless charging system applying phase-shift and amplitude control to maximize efficiency and extractable power," *IEEE Transactions on Power Electronics*, vol. 30, no. 11, pp. 6338–6348, 2015.

[11] Y. Chen, S. He, B. Yang, S. Chen, Z. He, and R. Mai, "Reconfigurable rectifier-based detuned series-series compensated ipt system for anti-misalignment and efficiency improvement," *IEEE Transactions on Power Electronics*, vol. 38, no. 2, pp. 2720–2729, 2022.

[12] Z. Zhang, H. Pang, A. Georgiadis, and C. Cecati, "Wireless power transfer—an overview," *IEEE transactions on industrial electronics*, vol. 66, no. 2, pp. 1044–1058, 2018.

[13] K. F. Warnick, R. B. Gottula, S. Shrestha, and J. Smith, "Optimizing power transfer efficiency and bandwidth for near field communication systems," *IEEE transactions on antennas and propagation*, vol. 61, no. 2, pp. 927–933, 2012.

[14] Y. Zhao, H. Li, S. Naderiparizi, A. Parks, and J. R. Smith, "Low-cost wireless power efficiency optimization of the nfc tag through switchable receiver antenna," *Wireless Power Transfer*, vol. 5, no. 2, pp. 87–96, 2018.

[15] P. Lathiya and J. Wang, “Near-field communications (nfc) for wireless power transfer (wpt): An overview,” *Wireless Power Transfer–Recent Development, Applications and New Perspectives*, pp. 95–122, 2021.

[16] Q. Huang, Z. Ma, S. Wang, and Y. Yang, “Integration of near field communication (nfc) antenna and wireless charging coil for portable electronic products,” *IEEE Journal of Emerging and Selected Topics in Power Electronics*, 2024.

[17] M. Wang, Q. Luo, Y. Iravantchi, X. Chen, A. Sample, K. G. Shin, X. Tian, X. Wang, and D. Chen, “Automatic calibration of magnetic tracking,” in *Proc. of ACM MobiCom*, 2022, pp. 391–404.

[18] D. Chen, Q. Luo, X. Chen, X. Wang, and C. Zhou, “Magdot: Drift-free, wearable joint angle tracking at low cost,” *Proc. of ACM UbiComp*, vol. 7, no. 4, pp. 1–25, 2024.

[19] D. Chen, M. Wang, C. He, Q. Luo, Y. Iravantchi, A. Sample, K. G. Shin, and X. Wang, “Magx: wearable, untethered hands tracking with passive magnets,” in *Proc. of ACM MobiCom*, 2021, pp. 269–282.

[20] B. Tao, E. Sie, J. Shenoy, and D. Vasisht, “Magnetic backscatter for in-body communication and localization,” in *Proc. of ACM MobiCom*, 2023, pp. 1–15.

[21] Z. Yu, F. T. Alrashdan, W. Wang, M. Parker, X. Chen, F. Y. Chen, J. Woods, Z. Chen, J. T. Robinson, and K. Yang, “Magnetoelectric backscatter communication for millimeter-sized wireless biomedical implants,” in *Proc. of ACM MobiCom*, 2022, pp. 432–445.

[22] J. Shi, X. Qing, Z. N. Chen, and C. K. Goh, “Electrically large dual-loop antenna for uhf near-field rfid reader,” *IEEE Transactions on Antennas and Propagation*, vol. 61, no. 3, pp. 1019–1025, 2012.

[23] Y. Guo, Y. Zhang, Z. Wang, and Y. Liu, “Wideband beamforming for near-field communications with circular arrays,” *IEEE Transactions on Wireless Communications*, 2024.

[24] H. Li, Z. Wang, X. Mu, P. Zhiwen, and Y. Liu, “Near-field integrated sensing, positioning, and communication: A downlink and uplink framework,” *IEEE Journal on Selected Areas in Communications*, 2024.

[25] V. R. Gowda, O. Yurduseven, G. Lipworth, T. Zupan, M. S. Reynolds, and D. R. Smith, “Wireless power transfer in the radiative near field,” *IEEE Antennas and Wireless Propagation Letters*, vol. 15, pp. 1865–1868, 2016.

[26] D. M. Dobkin, S. M. Weigand, and N. Iyer, “Segmented magnetic antennas for near-field uhf rfid,” *Microwave Journal*, vol. 50, no. 6, p. 96, 2007.

[27] B. Sim, S. Jeong, Y. Kim, S. Park, S. Lee, S. Hong, J. Song, H. Kim, H. Kang, H. Park *et al.*, “A near field analytical model for emi reduction and efficiency enhancement using an nth harmonic frequency shielding coil in a loosely coupled automotive wpt system,” *IEEE Transactions on Electromagnetic Compatibility*, vol. 63, no. 3, pp. 935–946, 2020.

[28] C. Song, H. Kim, Y. Kim, D. Kim, S. Jeong, Y. Cho, S. Lee, S. Ahn, and J. Kim, “Emi reduction methods in wireless power transfer system for drone electrical charger using tightly coupled three-phase resonant magnetic field,” *IEEE Transactions on Industrial Electronics*, vol. 65, no. 9, pp. 6839–6849, 2018.

[29] J. Liu, X. Zou, L. Zhao, Y. Tao, S. Hu, J. Han, and K. Ren, “Privacy leakage in wireless charging,” *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 2, pp. 501–514, 2022.

[30] T. Ni, J. Li, X. Zhang, C. Zuo, W. Wang, W. Xu, X. Luo, and Q. Zhao, “Exploiting contactless side channels in wireless charging power banks for user

privacy inference via few-shot learning," in *Proc. of ACM MobiCom*, 2023, pp. 1–15.

[31] D. Dai, Z. An, Q. Pan, and L. Yang, "Magcode: Nfc-enabled barcodes for nfc-disabled smartphones," in *Proc. of ACM MobiCom*, 2023, pp. 1–14.

[32] W. Jiang, D. Ferreira, J. Ylioja, J. Goncalves, and V. Kostakos, "Pulse: low bitrate wireless magnetic communication for smartphones," in *Proc. of ACM UbiComp*, 2014, pp. 261–265.

[33] N. Roy, H. Hassanieh, and R. Roy Choudhury, "Backdoor: Making microphones hear inaudible sounds," in *Proc. of ACM MobiSys*, 2017, pp. 2–14.

[34] N. Roy, S. Shen, H. Hassanieh, and R. R. Choudhury, "Inaudible voice commands: The long-range attack and defense," in *Proc. of USENIX NSDI*, 2018, pp. 547–560.

[35] G. Zhang, C. Yan, X. Ji, T. Zhang, T. Zhang, and W. Xu, "Dolphinattack: Inaudible voice commands," in *Proc. of ACM CCS*, 2017, pp. 103–117.

[36] C. Yan, G. Zhang, X. Ji, T. Zhang, T. Zhang, and W. Xu, "The feasibility of injecting inaudible voice commands to voice assistants," *IEEE Transactions on Dependable and Secure Computing*, 2019.

[37] M. Zhou, Z. Qin, X. Lin, S. Hu, Q. Wang, and K. Ren, "Hidden voice commands: Attacks and defenses on the vcs of autonomous driving cars," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 128–133, 2019.

[38] Q. Yan, K. Liu, Q. Zhou, H. Guo, and N. Zhang, "Surfingattack: Interactive hidden attack on voice assistants using ultrasonic guided waves," in *Network and Distributed Systems Security (NDSS) Symposium*, 2020.

[39] X. Ji, J. Zhang, S. Jiang, J. Li, and W. Xu, "Capspeaker: Injecting sounds to microphones via capacitors," in *Proc. of ACM CCS*, 2021.

[40] G. Zhang, X. Ji, X. Li, G. Qu, and W. Xu, "Eararray: Defending against dolphinattack via acoustic attenuation," in *Network and Distributed Systems Security (NDSS) Symposium*, 2021.

[41] D. F. Kune, J. Backes, S. S. Clark, D. Kramer, M. Reynolds, K. Fu, Y. Kim, and W. Xu, "Ghost talk: Mitigating emi signal injection attacks against analog sensors," in *Proc. of IEEE S&P*. IEEE, 2013, pp. 145–159.

[42] C. Kasmi and J. L. Esteves, "Iemi threats for information security: Remote command injection on modern smartphones," *IEEE Transactions on Electromagnetic Compatibility*, vol. 57, no. 6, pp. 1752–1755, 2015.

[43] T. Sugawara, B. Cyr, S. Rampazzi, D. Genkin, and K. Fu, "Light commands: laser-based audio injection attacks on voice-controllable systems," in *Proc. of USENIX Security*, 2020, pp. 2631–2648.

[44] Y. Wang, H. Guo, and Q. Yan, "Ghosttalk: Interactive attack on smartphone voice system through power line," *Network and Distributed Systems Security (NDSS) Symposium*, 2022.

[45] Infineon Technologies, "AN558: MEMS microphone electrical implementation.pdf," https://www.infineon.com/, 2018.

[46] D. Dai, Z. An, and L. Yang, "Inducing wireless chargers to voice out for inaudible command attacks," in *Proc. of IEEE S&P*. IEEE, 2023, pp. 1789–1806.

[47] Infineon Technologies, "IM69D130: High performance digital XENSIVTM MEMS microphone.pdf," https://www.infineon.com/cms/en/product/sensor/mems-microphones/mems-microphones-for-consumer/im69d130/#!documents, 2017, Last accessed October 22, 2021.

[48] C.-H. Ko, H.-L. Lee, and C.-H. Wang, "The emi suppression of ultra thin mems microphone package," in *2010 5th International Microsystems Packaging Assembly and Circuits Technology Conference*. IEEE, 2010, pp. 1–3.

[49] G. Reitsma, M. Kouwenhoven, and A. Mosterd, “A low-power microphone preamplifier with emi canceling,” in *Proc. of the 26th European Solid-State Circuits Conference.* IEEE, 2000, pp. 296–299.

[50] T. Shijo, K. Ogawa, M. Suzuki, Y. Kanekiyo, M. Ishida, and S. Obayashi, “Emi reduction technology in 85 khz band 44 kw wireless power transfer system for rapid contactless charging of electric bus,” in *2016 IEEE Energy Conversion Congress and Exposition (ECCE).* IEEE, 2016, pp. 1–6.

[51] M. Suzuki, K. Ogawa, F. Moritsuka, T. Shijo, H. Ishihara, Y. Kanekiyo, K. Ogura, S. Obayashi, and M. Ishida, “Design method for low radiated emission of 85 khz band 44 kw rapid charger for electric bus,” in *2017 IEEE Applied Power Electronics Conference and Exposition (APEC).* IEEE, 2017, pp. 3695–3701.

[52] K. Inoue, K. Kusaka, and J.-I. Itoh, “Reduction in radiation noise level for inductive power transfer systems using spread spectrum techniques,” *IEEE Transactions on Power Electronics*, vol. 33, no. 4, pp. 3076–3085, 2017.

[53] L. Tan, Z. Tang, S. Wang, Z. Li, W. Zhao, R. Zhong, and X. Huang, “Design and optimization of parameters of electric vehicle’s wireless power transmission system to decrease the influence of coexistence interference,” in *2019 IEEE 2nd International Conference on Electronics Technology (ICET).* IEEE, 2019, pp. 315–319.

[54] D. Dai, Z. An, Q. Pan, and L. Yang, “Harnessing nfc to generate standard optical barcodes for nfc-missing smartphones,” *IEEE Transactions on Mobile Computing*, 2024.

[55] A. Schwarz, Y. Sanhedrai, and Z. Zalevsky, “Digital camera detection and image disruption using controlled intentional electromagnetic interference,” *IEEE*

transactions on electromagnetic compatibility, vol. 54, no. 5, pp. 1048–1054, 2012.

[56] A. Richelli, “Emi susceptibility issue in analog front-end for sensor applications,” *Journal of Sensors*, vol. 2016, 2016.

[57] F. Fiori, “Emi-induced distortion of baseband signals in current feedback instrumentation amplifiers,” *IEEE Transactions on Electromagnetic Compatibility*, vol. 60, no. 3, pp. 605–612, 2017.

[58] ams OSRAM, “Imager Sensor Solutions,” https://www.mouser.com/datasheet/2/588/CMOSImageSensors_PD000121_2-00-1519004.pdf, 2022.

[59] S. Kovář, J. Valouch, and M. Adámek, “Electromagnetic susceptibility of ip camera,” *Przeglad Elektrotechniczny*, 2016.

[60] ams OSRAM, “NANEYE IMAGE SENSOR MODULES,” https://www.application-datasheet.com/pdf/ams/ne2d-rgb-v90f4-0-2m.pdf, 2022.

[61] C. Microwave, “Shielded Cameras,” https://www.castlemicrowave.com/technologies/shielded-cameras/, 2022.

[62] P. E. Product, “Shielded Cameras,” https://www.pontis-emc.com/products/shielded-cameras/, 2022.

[63] R. Nandakumar, K. K. Chintalapudi, V. Padmanabhan, and R. Venkatesan, “Dhwani: secure peer-to-peer acoustic nfc,” *ACM SIGCOMM Computer Communication Review*, vol. 43, no. 4, pp. 63–74, 2013.

[64] N. Roy, M. Gowda, and R. R. Choudhury, “Ripple: Communicating through physical vibration,” in *Proc. of USENIX NSDI*, 2015, pp. 265–278.

[65] M. Gao, F. Lin, W. Xu, M. Nuermaimaiti, J. Han, W. Xu, and K. Ren, “Deafaid: mobile iot communication exploiting stealthy speaker-to-gyroscope channel,” in *Proc. of ACM MobiCom*, 2020, pp. 1–13.

[66] H. Pan, Y.-C. Chen, G. Xue, and X. Ji, "Magnecomm: Magnetometer-based near-field communication," in *Proc. of ACM MobiCom*, 2017, pp. 167–179.

[67] H. Huang and S. Lin, "Met: a magneto-inductive sensing based electric toothbrushing monitoring system," in *Proc. of ACM MobiCom*, 2020, pp. 1–14.

[68] V. Coskun, B. Ozdenizci, and K. Ok, "A survey on near field communication (nfc) technology," *Wireless personal communications*, vol. 71, no. 3, pp. 2259–2294, 2013.

[69] M. Taguchi and H. Mizuno, "Analysis of dead zone of rfid system," in *2006 IEEE Antennas and Propagation Society International Symposium.* IEEE, 2006, pp. 4759–4762.

[70] R. Zhao, P. Wang, Y. Ma, P. Zhang, H. H. Liu, X. Lin, X. Zhang, C. Xu, and M. Zhang, "Nfc+ breaking nfc networking limits through resonance engineering," in *Proc. of ACM SIGCOMM*, 2020, pp. 694–707.

[71] Z. Wang, M. Xu, N. Ye, R. Wang, and H. Huang, "Rf-focus: Computer vision-assisted region-of-interest rfid tag recognition and localization in multipath-prevalent environments," in *Proc. of ACM IMWUT*, 2019.

[72] B. Liang, P. Wang, R. Zhao, H. Guo, P. Zhang, J. Guo, S. Zhu, H. H. Liu, X. Zhang, and C. Xu, "Rf-chord: Towards deployable rfid localization system for logistic networks," in *Proc. of USENIX NSDI*, 2023.

[73] L. Dodds, N. Naeem, A. Eid, and F. Adib, "Software-controlled polarization for longer-range rfid reading and localization," in *2023 IEEE International Conference on RFID (RFID).* IEEE, 2023, pp. 90–95.

[74] L. Dodds, I. Perper, A. Eid, and F. Adib, "A handheld fine-grained rfid localization system with complex-controlled polarization," in *Proc. of ACM MobiCom*, 2023.

[75] J. Wang, J. Zhang, R. Saha, H. Jin, and S. Kumar, “Pushing the range limits of commercial passive rfids,” in *Proc. of USENIX NSDI*, 2019, pp. 301–316.

[76] Y. Ma, Z. Luo, C. Steiger, G. Traverso, and F. Adib, “Enabling deep-tissue networking for miniature medical devices,” in *Proc. of ACM SIGCOMM*, 2018, pp. 417–431.

[77] S. Chen, S. Zhong, S. Yang, and X. Wang, “A multiantenna rfid reader with blind adaptive beamforming,” *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 986–996, 2016.

[78] D. Vasisht, G. Zhang, O. Abari, H.-M. Lu, J. Flanz, and D. Katabi, “In-body backscatter communication and localization,” in *Proc. of ACM SIGCOMM*, 2018, pp. 132–146.

[79] Z. An, Q. Lin, Q. Pan, and L. Yang, “Turbocharging deep backscatter through constructive power surges with a single rf source,” in *Proc. of IEEE INFOCOM*, 2021.

[80] S. Sabesan, M. J. Crisp, R. V. Penty, and I. H. White, “Wide area passive uhf rfid system using antenna diversity combined with phase and frequency hopping,” *IEEE Transactions on Antennas and Propagation*, vol. 62, no. 2, pp. 878–888, 2013.

[81] M. Bolic, M. Rostamian, and P. M. Djuric, “Proximity detection with rfid: A step toward the internet of things,” *IEEE Pervasive Computing*, vol. 14, no. 2, pp. 70–76, 2015.

[82] C. Bocanegra, M. A. Khojastepour, M. Y. Arslan, E. Chai, S. Rangarajan, and K. R. Chowdhury, “Rfgo: a seamless self-checkout system for apparel stores using rfid,” in *Proc. of ACM MobiCom*, 2020.

[83] HUAYUAN RFID NFC Manufacturer, "Dual frequency rfid cards," https://www.huayuansh.com/products/rfid-smart-cards/dual-frequency-rfid-cards/, 2024, accessed: 2024-02-27.

[84] B. Shrestha, A. Elsherbeni, and L. Ukkonen, "Uhf rfid reader antenna for near-field and far-field operations," *IEEE Antennas and Wireless Propagation Letters*, vol. 10, pp. 1274–1277, 2011.

[85] X. Qing, C. Goh, and Z. Chen, "Segmented loop antenna for uhf near-field rfid applications," *Electronics letters*, vol. 45, no. 17, pp. 872–873, 2009.

[86] P. V. Nikitin, K. Rao, and S. Lazar, "An overview of near field uhf rfid," in *2007 IEEE international conference on RFID.* IEEE, 2007, pp. 167–174.

[87] A. Diet, Y. Le Bihan, C. Conessa, F. Alves, M. Grzeskowiak, M. Benamara, G. Lissorgues, M. Biancheri-Astier, and A. Pozzebon, "Lf rfid chequered loop antenna for pebbles on the beach detection," in *2016 46th European Microwave Conference (EuMC).* IEEE, 2016, pp. 41–44.

[88] M. Benamara, M. Grzeskowiak, A. Diet, G. Lissorgues, Y. Le Bihan, S. Protat, and C. Conessa, "A twisted loop antenna to enhance hf rfid detection for different tag positioning," in *2016 10th European Conference on Antennas and Propagation (EuCAP).* IEEE, 2016, pp. 1–5.

[89] X. Qing, Z. N. Chen, and A. Cai, "Multi-loop antenna for high frequency rfid smart shelf application," in *2007 IEEE Antennas and Propagation Society International Symposium.* IEEE, 2007, pp. 5467–5470.

[90] W. L. Stutzman and G. A. Thiele, *Antenna theory and design.* John Wiley & Sons, 2012.

[91] Y. Zeng, Z. N. Chen, X. Qing, and J.-M. Jin, "Modeling and characterization of zero-phase-shift lines and optimization of electrically large zpsl loop antennas for

near-field systems," *IEEE Transactions on Antennas and Propagation*, vol. 64, no. 11, pp. 4587–4594, 2016.

[92] Z. N. Chen, X. Qing, J. Shi, and Y. Zeng, "Review of zero-phase-shift-line loop antennas for uhf near-field rfid readers," *IEEE journal of radio frequency identification*, vol. 1, no. 4, pp. 245–252, 2017.

[93] Y. S. Ong, X. Qing, C. K. Goh, and Z. N. Chen, "A segmented loop antenna for uhf near-field rfid," in *2010 IEEE Antennas and Propagation Society International Symposium.* IEEE, 2010, pp. 1–4.

[94] A. L. Borja, A. Belenguer, J. Cascon, and J. R. Kelly, "A reconfigurable passive uhf reader loop antenna for near-field and far-field rfid applications," *IEEE Antennas and Wireless Propagation Letters*, vol. 11, pp. 580–583, 2012.

[95] Y. Zeng, X. Qing, Z. N. Chen, and J.-M. Jin, "Directional uhf near-field rfid reader antenna with an improved magnetic field distribution," in *2016 IEEE Region 10 Conference (TENCON).* IEEE, 2016, pp. 135–137.

[96] Z. D. Wang, Y. Z. Yin, X. Yang, and J. J. Wu, "Design of a wideband horizontally polarized omnidirectional antenna with mutual coupling method," *IEEE Transactions on Antennas and Propagation*, vol. 63, no. 7, pp. 3311–3316, 2015.

[97] A. Kurs, A. Karalis, R. Moffatt, J. D. Joannopoulos, P. Fisher, and M. Soljacic, "Wireless power transfer via strongly coupled magnetic resonances," *science*, vol. 317, no. 5834, pp. 83–86, 2007.

[98] J. Jadidian and D. Katabi, "Magnetic mimo: How to charge your phone in your pocket," in *Proc. of ACM MobiCom*, 2014, pp. 495–506.

[99] L. Shi, Z. Kabelac, D. Katabi, and D. Perreault, "Wireless power hotspot that charges all of your devices," in *Proc. of ACM MobiCom*, 2015, pp. 2–13.

[100] K. Niotaki, N. B. Carvalho, A. Georgiadis, X. Gu, S. Hemour, K. Wu, D. Matos, D. Belo, R. Pereira, R. Figueiredo *et al.*, "Rf energy harvesting and wireless power transfer for energy autonomous wireless devices and rfids," *IEEE Journal of Microwaves*, vol. 3, no. 2, pp. 763–782, 2023.

[101] "Find out what siri can do on iphone," https://support.apple.com/en-hk/guide/iphone/ipha48873ed6/ios, 2022.

[102] "Google Now," https://www.androidcentral.com/google-now, 2016.

[103] "Amazon Alexa," https://developer.amazon.com/en-US/alexa, 2017.

[104] L. Palisek and L. Suchy, "High power microwave effects on computer networks," in *10th International Symposium on Electromagnetic Compatibility*. IEEE, 2011, pp. 18–21.

[105] F. Sabath, "Classification of electromagnetic effects at system level," in *Ultra-Wideband, Short Pulse Electromagnetics 9*. Springer, 2010, pp. 325–333.

[106] C. Kasmi, J. Lopes-Esteves, N. Picard, M. Renard, B. Beillard, E. Martinod, J. Andrieu, and M. Lalande, "Event logs generated by an operating system running on a cots computer during iemi exposure," *IEEE Transactions on Electromagnetic Compatibility*, vol. 56, no. 6, pp. 1723–1726, 2014.

[107] M. Guri, B. Zadov, and Y. Elovici, "Odini: Escaping sensitive data from faraday-caged, air-gapped computers via magnetic fields," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1190–1203, 2019.

[108] "Inaduible voice attacks demo," https://anplus.github.io/magsound/, 2022.

[109] "Ansys maxwell," https://www.ansys.com/products/electronics/ansys-maxwell, 2021.

[110] "Apple smart watch model," https://grabcad.com/library/apple-smart-watch-1, 2021.

[111] "Apple iphone 13 model," https://grabcad.com/library/tag/iphone13, 2021.

[112] "Qi Standard v1.3," https://www.wirelesspowerconsortium.com/knowledge-base/specifications/download-the-qi-specifications.html, 2020.

[113] M. Maaß, A. Griessner, V. Steixner, and C. Zierhofer, "Reduction of eddy current losses in inductive transmission systems with ferrite sheets," *Biomedical engineering online*, vol. 16, no. 1, pp. 1–18, 2017.

[114] "Mi 80W Wireless Charging Stand," https://www.mi.com/global/product/mi-80w-wireless-charging-stand/, 2020.

[115] "Tdk analog mems microphone t4086," https://invensense.tdk.com/download-pdf/t4086-datasheet/, 2021.

[116] "Infineon digital mems microphone im69d130," , 2021.

[117] "Tdk corporation overview mems microphone t4064/t4081," https://product.tdk.com/en/techlibrary/productoverview/mems-microphone.html, 2021.

[118] A. Vander Vorst, A. Rosen, and Y. Kotsuka, *RF/microwave interaction with biological tissues.* John Wiley & Sons, 2006, vol. 181.

[119] "ST EMIF02-MIC03F2 datasheet," https://www.st.com/en/emi-filtering-and-signal-conditioning/emif02-mic03f2.html, 2021.

[120] B. B. Monson, E. J. Hunter, A. J. Lotto, and B. H. Story, "The perceptual significance of high-frequency energy in the human voice," *Frontiers in psychology*, vol. 5, p. 587, 2014.

[121] "Knowles tda1308 silicon microphone," https://www.aliexpress.com/item/1005001415977347.html, 2021.

[122] "Zero-height sisonic mems microphone," https://www.knowles.com/docs/default-source/model-downloads/spv1840lr5h-b-rev-b-datasheet.pdf, 2014.

[123] "Max9812: fixed-gain microphone amplifiers," https://www.maximintegrated.com/en/products/analog/audio/MAX9812.html, 2022.

[124] "Google assistant," https://assistant.google.com/explore?hl=en_us, 2022.

[125] "Samsung bixby," https://www.samsung.com/hk_en/apps/bixby/, 2022.

[126] "Vocloner: standard voice cloning tool." https://vocloner.com/, 2022.

[127] J. Shen, R. Pang, R. J. Weiss, M. Schuster, N. Jaitly, Z. Yang, Z. Chen, Y. Zhang, Y. Wang, R. Skerrv-Ryan *et al.*, "Natural tts synthesis by conditioning wavenet on mel spectrogram predictions," in *Proc. of IEEE ICASSP*. IEEE, 2018, pp. 4779–4783.

[128] S. Arik, J. Chen, K. Peng, W. Ping, and Y. Zhou, "Neural voice cloning with a few samples," *Advances in neural information processing systems*, vol. 31, 2018.

[129] "Guidelines for automotive aftermarket qi chargers," https://www.wirelesspowerconsortium.com/data/downloadables/9/5/3/20121001-guidelines-for-automotive-aftermarket-chargers-v-10.pdf, 2012.

[130] "Get google assistant on your android lock screen," https://support.google.com/assistant/answer/9134021?hl=en, 2022.

[131] C. J, "Real-time voice cloning," https://github.com/CorentinJ/Real-Time-Voice-Cloning, 2024, accessed: 2024-07-16.

[132] X. Tan, T. Qin, F. Soong, and T.-Y. Liu, "A survey on neural speech synthesis," *arXiv preprint arXiv:2106.15561*, 2021.

[133] Y. Jia, Y. Zhang, R. Weiss, Q. Wang, J. Shen, F. Ren, P. Nguyen, R. Pang, I. Lopez Moreno, Y. Wu *et al.*, "Transfer learning from speaker verification to multispeaker text-to-speech synthesis," *Advances in neural information processing systems*, vol. 31, 2018.

[134] MathWorks, “Mel spectrogram - matlab melspectrogram,” https://ww2.mathworks.cn/help/audio/ref/melspectrogram.html, 2024, accessed: 2024-03-12.

[135] L. Wan, Q. Wang, A. Papir, and I. L. Moreno, “Generalized end-to-end loss for speaker verification,” in *Proc. of IEEE ICASSP*. IEEE, 2018, pp. 4879–4883.

[136] S. Hochreiter and J. Schmidhuber, “Long short-term memory,” *Neural computation*, vol. 9, no. 8, pp. 1735–1780, 1997.

[137] A. Van Den Oord, S. Dieleman, H. Zen, K. Simonyan, O. Vinyals, A. Graves, N. Kalchbrenner, A. Senior, K. Kavukcuoglu *et al.*, “Wavenet: A generative model for raw audio,” *arXiv preprint arXiv:1609.03499*, vol. 12, 2016.

[138] W. contributors, “Mean opinion score,” 2024, accessed: 2024-07-28. [Online]. Available: https://en.wikipedia.org/wiki/Mean_opinion_score

[139] D. Piotrowski, R. Korzeniowski, A. Falai, S. Cygert, K. Pokora, G. Tinchev, Z. Zhang, and K. Yanagisawa, “Cross-lingual knowledge distillation via flow-based voice conversion for robust polyglot text-to-speech,” in *International Conference on Neural Information Processing*. Springer, 2023, pp. 252–264.

[140] S.-F. Huang, C.-P. Chen, Z.-S. Chen, Y.-P. Tsai, and H.-y. Lee, “Personalized lightweight text-to-speech: Voice cloning with adaptive structured pruning,” in *Proc. of IEEE ICASSP*. IEEE, 2023, pp. 1–5.

[141] “Ti QI Standard Wireless Charger BQ500210,” https://www.ti.com.cn/product/cn/BQ500210?qgpn=bq500210, 2021.

[142] “STWBC: Digital controller for wireless battery charger transmitters supporting Qi A11 topology,” https://www.st.com/en/power-management/stwbc.html, 2021.

[143] J. Sun, "Pulse-width modulation," in *Dynamics and control of switched electronic systems.* Springer, 2012, pp. 25–61.

[144] L. Malesani, L. Rossetto, P. Tenti, and P. Tomasin, "Ac/dc/ac pwm converter with reduced energy storage in the dc link," *IEEE Transactions on Industry Applications*, vol. 31, no. 2, pp. 287–292, 1995.

[145] X. Chen and M. Kazerani, "Space vector modulation control of an ac–dc–ac converter with a front-end diode rectifier and reduced dc-link capacitor," *IEEE Transactions on power electronics*, vol. 21, no. 5, pp. 1470–1478, 2006.

[146] V. MURATOV, "Methodsfor foreign object detection in inductive wireless charging. qi developer forum, 2017."

[147] "STC12C2052AD," http://www.stcmicro.com/STC/STC12C2052AD.html, 2021.

[148] "IRF540NPBF," https://www.mouser.com/datasheet/2/196/Infineon_IRF540N_DataSheet_v01_01_EN-1732489.pdf, 2021.

[149] "TDK A11 Coil," https://product.tdk.com/en/search/wireless-charge/wireless-charge/tx-coil-module/info?part_no=WT505090-10K2-A11-G, 2021.

[150] "TDK Rx Coil," https://product.tdk.com/en/search/wireless-charge/wireless-charge/rx-coil-module/info?part_no=WRM483265-10F5-12V-G, 2021.

[151] "1N4002G," https://www.mouser.hk/ProductDetail/Taiwan-Semiconductor/1N4002G-R0G?qs=%2FQ2qp2Z%2FWFyOCLsW3PjwYQ%3D%3D, 2018.

[152] "Wireless Charging PWM Controller," https://www.semtech.com/products/wireless-charging/linkcharge-ics/ts61005, 2021.

[153] "ESP32-C3-DevKitC-02," https://docs.espressif.com/projects/esp-idf/en/latest/esp32c3/hw-reference/esp32c3/user-guide-devkitc-02.html, 2021.

[154] "LM7805," https://www.ti.com/lit/ds/symlink/lm340.pdf, 2021.

[155] "AR824 Sound Level Meter," https://www.amazon.com/SENSOR-Digital-Handheld-Decibel-Monitor/dp/B07RJDWK93, 2019.

[156] "Designing a Qi-compliant receiver coil for wireless power systems," https://www.mouser.com/pdfDocs/TI-Designing-a-Qi-compliant-receiver-coil.pdf, 2018.

[157] "HT201 Tesla Meter Surface Magnetic Field Gauss Meter Tester," https://www.amazon.com/Surface-Magnetic-Tester-Digital-Gaussmeter/dp/B018MPFF6I, 2018.

[158] C. C. Finlay, S. Maus, C. Beggan, T. Bondar, A. Chambodut, T. Chernova, A. Chulliat, V. Golovkov, B. Hamilton, M. Hamoudi *et al.*, "International geomagnetic reference field: the eleventh generation," *Geophysical Journal International*, vol. 183, no. 3, pp. 1216–1230, 2010.

[159] "Samsung 15W Fast Charge," https://www.amazon.com/Samsung-Charge-Wireless-Charger-Stand/dp/B07VG9JMG1, 2019.

[160] "Baseus Wireless Charger Station 15W," https://amz.run/56lZ, 2018.

[161] "UGREEN Qi Wireless Charger," https://www.amazon.com/UGREEN-Qi-Wireless-Charger-Compatible/dp/B096SC2ZQK, 2021.

[162] "Apple MagSafe Charger," https://www.amazon.com/Apple-MHXH3AM-A-MagSafe-Charger/dp/B08L5NP6NG, 2020.

[163] "Wireless charging test module tester," https://www.aliexpress.com/item/1005002014025696.html, 2021.

[164] "Google Cloud: Speech-to-Text," https://cloud.google.com/speech-to-text, 2021.

[165] "Product Overview MEMS Microphone T4064/T4081," https://product.tdk.com/en/techlibrary/productoverview/mems-microphone.html, 2021.

[166] L. Blue, L. Vargas, and P. Traynor, "Hello, is it me you're looking for? differentiating between human and electronic speakers for voice interface security," in *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, 2018, pp. 123–133.

[167] K. S. Tharayil, B. Farshteindiker, S. Eyal, N. Hasidim, R. Hershkovitz, S. Houri, I. Yoffe, M. Oren, and Y. Oren, "Sensor defense in-software (sdi): Practical software based detection of spoofing attacks on position sensors," *Engineering Applications of Artificial Intelligence*, vol. 95, p. 103904, 2020.

[168] S. Grotta, "COVID-19 and Debit and Alternative Payments Products," https://www.mercatoradvisorygroup.com/covid-19-and-debit-and-alternative-payments-products/, 2020.

[169] H. Keni, M. Earle, and M. Min, "Product authentication using hash chains and printed qr codes," in *2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 2017, pp. 319–324.

[170] V. Mavroeidis and M. Nicho, "Quick response code secure: a cryptographically secure anti-phishing tool for qr code attacks," in *International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security*. Springer, 2017, pp. 313–324.

[171] S. Sung, J. Lee, J. Kim, J. Mun, D. Won *et al.*, "Security analysis of mobile authentication using qr-codes," in *Computer Science & Information Technology-Computer Science Conference Proceedings*, 2015.

[172] X. Bai, Z. Zhou, X. Wang, Z. Li, X. Mi, N. Zhang, T. Li, S.-M. Hu, and K. Zhang, "Picking up my tab: Understanding and mitigating synchronized

token lifting and spending in mobile payment," in *26th USENIX Security Symposium (USENIX Security 17)*, 2017, pp. 593–608.

[173] F. Times, "China moves to impose order on mobile payments boom," https://www.ft.com/content/b7866e7c-eb8e-11e7-bd17-521324c81e23, 2017.

[174] Bluebite.com, "The State of NFC in 2021," https://bluebite.medium.com/the-state-of-nfc-in-2020-2a512e83774b, 2021.

[175] "Worldwide NFC Technology Use Surges Over Last 24 Months," https://nfc-forum.org/news/2022-07-worldwide-nfc-technology-use-surges-over-last-24-months/, 2022.

[176] "MagCode Demo," https://donghui-dai.github.io/magcode/, 2023.

[177] R. Technologies, "RIGOL DG2052 50 MHz Arbitrary Waveform Generator ," https://www.amazon.com/Rigol-DG2052-Function-Arbitrary-Generator/dp/B08228CY5X, 2019.

[178] Y. Zhao, J. R. Smith, and A. Sample, "Nfc-wisp: A sensing and computationally enhanced near-field rfid platform," in *2015 IEEE International Conference on RFID (RFID)*. IEEE, 2015, pp. 174–181.

[179] STMicroelectronics, "ST25 NFC guide," https://www.st.com/resource/en/technical_note/dm00190233-st25-nfc-guide-stmicroelectronics.pdf, 2016.

[180] H. Marouani and M. R. Dagenais, "Internal clock drift estimation in computer clusters," *Journal of Computer Systems, Networks, and Communications*, vol. 2008, 2008.

[181] J. Buchner, "ImageHash —A Python Perceptual Image Hashing Module," https://github.com/JohannesBuchner/imagehash, 2021.

[182] B. Yang, F. Gu, and X. Niu, “Block mean value based image perceptual hashing,” in *2006 International Conference on Intelligent Information Hiding and Multimedia.* IEEE, 2006, pp. 167–172.

[183] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, “Image quality assessment: from error visibility to structural similarity,” *IEEE transactions on image processing*, vol. 13, no. 4, pp. 600–612, 2004.

[184] Z. Wang, E. P. Simoncelli, and A. C. Bovik, “Multiscale structural similarity for image quality assessment,” in *The Thrity-Seventh Asilomar Conference on Signals, Systems & Computers, 2003*, vol. 2. Ieee, 2003, pp. 1398–1402.

[185] V. Muratov, “Methods for foreign object detection in inductive wireless charging,” in *Qi Developer Forum Nov*, vol. 16, 2017.

[186] D. J. MacKay, “Fountain codes,” *IEE Proceedings-Communications*, vol. 152, no. 6, pp. 1062–1068, 2005.

[187] A. Khisti, “Tornado codes and luby transform codes,” *SemanticScholar Org. web-site*, pp. 1–12, 2003.

[188] M. Luby, “Lt codes,” in *The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings.* IEEE Computer Society, 2002, pp. 271–271.

[189] A. Shokrollahi, “Raptor codes,” *IEEE transactions on information theory*, vol. 52, no. 6, pp. 2551–2567, 2006.

[190] G. T. Chen, L. Cao, F. Zhao, H.-f. Zheng, and M. Pan, “Analysis of robust soliton distribution for lt code,” in *2012 IEEE 11th International Conference on Signal Processing*, vol. 2. IEEE, 2012, pp. 1546–1549.

[191] “LTcode Matlab,” https://github.com/william-zk/LT_code/tree/master/LT_matlab, 2021.

[192] F. Gardner, "A bpsk/qpsk timing-error detector for sampled receivers," *IEEE Transactions on communications*, vol. 34, no. 5, pp. 423–429, 1986.

[193] L. E. Peterson, "K-nearest neighbor," *Scholarpedia*, vol. 4, no. 2, p. 1883, 2009.

[194] J. Carrère, S. Place, J. Oddou, D. Benoit, and F. Roy, "Cmos image sensor: Process impact on dark current," in *2014 IEEE International Reliability Physics Symposium.* IEEE, 2014, pp. 3C–1.

[195] "Imformation capacity and versions of QRcode," https://www.qrcode.com/en/about/version.html, 2021.

[196] "ClearImage Barcode Reader SDK," https://www.inliteresearch.com/barcode-recognition-sdk.php, 2022.

[197] "System usability scale," https://en.wikipedia.org/wiki/System_usability_scale, 2022.

[198] E. C. Jones and C. A. Chung, *RFID in logistics: a practical introduction.* CRC press, 2007.

[199] Z. Zhang, G. Xu, and E. C. Kan, "Outlooks for uhf rfid-based autonomous retails and factories," *IEEE Journal of Radio Frequency Identification*, 2022.

[200] S. Pradhan, E. Chai, K. Sundaresan, S. Rangarajan, and L. Qiu, "Konark: A rfid based system for enhancing in-store shopping experience," in *Proceedings of the 4th International on Workshop on Physical Analytics*, 2017, pp. 19–24.

[201] C. Loo, A. Elsherbeni, F. Yang, and D. Kajfez, "Experimental and simulation investigation of rfid blind spots," *Journal of Electromagnetic Waves and Applications*, vol. 23, no. 5-6, pp. 747–760, 2009.

[202] J. Wang, L. Chang, O. Abari, and S. Keshav, "Are rfid sensing systems ready for the real world?" in *Proc. of ACM MobiSys*, 2019, pp. 366–377.

[203] Y. Ma, N. Selby, and F. Adib, "Minding the billions: Ultra-wideband localization for deployed rfid tags," in *Proc. of ACM MobiCom*, 2017, pp. 248–260.

[204] Impinj, "Rain rfid readers, connectivity devices for iot solutions," https://www.impinj.com/products/readers, accessed: 2024-02-27.

[205] Ettus Research, "Usrp x310 high performance software defined radio," https://www.ettus.com/all-products/x310-kit/, accessed: 2024-02-27.

[206] Mike Lenehan, "Monza 4 datasheet – impinj support portal," https://support.impinj.com/hc/en-us/articles/202756908-Monza-4-Datasheet, accessed: 2024-02-27.

[207] Ansys, "Ansys hfss: 3d high frequency simulation software," https://www.ansys.com/products/electronics/ansys-hfss, 2024, accessed: 2024-02-27.

[208] A. H. Muqaibel, A. Safaai-Jazi, and S. M. Riad, "Fork-coupled resonators for high-frequency characterization of dielectric substrate materials," *IEEE transactions on instrumentation and measurement*, vol. 55, no. 6, pp. 2216–2220, 2006.

[209] R. Dewan, M. Rahim, M. Hamid, M. Yusoff, N. A. Samsuri, N. Murad, and K. Kamardin, "Artificial magnetic conductor for various antenna applications: An overview," *International Journal of RF and Microwave Computer-Aided Engineering*, vol. 27, no. 6, p. e21105, 2017.

[210] T. H. Loh, "High impedance surface electromagnetic band gap metamaterials: Design approach and applications for antenna engineering," *Invited Paper*, 2011.

[211] P. Nepa and A. Buffi, "Near-field-focused microwave antennas: Near-field shaping and implementation." *IEEE Antennas and Propagation Magazine*, vol. 59, no. 3, pp. 42–53, 2017.

[212] A. Buffi, P. Nepa, and G. Manara, "Design criteria for near-field-focused planar arrays," *IEEE Antennas and Propagation Magazine*, vol. 54, no. 1, pp. 40–50, 2012.

[213] Wikipedia, "Fresnel diffraction," https://en.wikipedia.org/wiki/Fresnel_diffraction, 2024, accessed: 2024-02-27.

[214] J. Wang and D. Katabi, "Dude, where's my card? rfid positioning that works with multipath and non-line of sight," in *Proc. of ACM SIGCOMM*, 2013, pp. 51–62.

[215] L. Yang, Y. Chen, X.-Y. Li, C. Xiao, M. Li, and Y. Liu, "Tagoram: Real-time tracking of mobile rfid tags to high precision using cots devices," in *Proc. of ACM MobiCom*, 2014, pp. 237–248.

[216] D. Tse and P. Viswanath, *Fundamentals of wireless communication.* Cambridge university press, 2005.

[217] L. Yang, Q. Lin, C. Duan, and Z. An, "Analog on-tag hashing: Towards selective reading as hash primitives in gen2 rfid systems," in *Proc. of ACM MobiCom*, 2017, pp. 301–314.

[218] Z. An, Q. Lin, L. Yang, and W. Lou, "Embracing tag collisions: Acquiring bloom filters across rfids in physical layer," in *Proc. of IEEE INFOCOM*, 2019, pp. 1531–1539.

[219] B. Sheng, Q. Li, and W. Mao, "Efficient continuous scanning in rfid systems," in *Proc. of IEEE INFOCOM*, 2010.

[220] L. Xie, Q. Li, X. Chen, S. Lu, and D. Chen, "Continuous scanning with mobile reader in rfid systems: An experimental study," in *Proc. of ACM MobiHoc*, 2013, pp. 11–20.

[221] Z. An, Q. Lin, L. Yang, W. Lou, and L. Xie, “Acquiring bloom filters across commercial rfids in physical layer,” *IEEE/ACM Transactions on Networking*, vol. 28, no. 4, pp. 1804–1817, 2020.

[222] Mini-Circuits, “Sphsa-152+ datasheet,” https://www.minicircuits.com/pdfs/SPHSA-152+.pdf, 2024, accessed: 2024-02-27.

[223] Raspberry Pi Foundation, “Raspberry pi 4 model b,” https://www.raspberrypi.com/products/raspberry-pi-4-model-b/, accessed: 2024-02-27.

[224] Rohde & Schwarz, “Hameg hms3010 3 ghz spectrum analyzer,” https://scdn.rohde-schwarz.com/ur/pws/dl_downloads/dl_common_library/dl_brochures_and_datasheets/pdf_1/HAMEG_DB_EN_HMS3000_3010.pdf, accessed: 2024-02-27.

[225] D. Dobkin, *The rf in RFID: uhf RFID in practice.* Newnes, 2012.

[226] Impinj, “Rain rfid tag chips for the internet of things,” https://www.impinj.com/products/tag-chips, 2024, accessed: 2024-02-27.

[227] Alien Technology, “Tags,” https://www.alientechnology.com/products/tags/, accessed: 2024-02-27.

[228] NXP Semiconductors, “Ucode rain rfid uhf,” https://www.nxp.com/products/rfid-nfc/ucode-rain-rfid-uhf:MC_50483, 2023, accessed: 2024-02-27.

[229] Laxcen, “RFID,” http://www.laxcen.com/rfid.html, 2023, accessed: 2024-02-27.

[230] L. Ukkonen, D. Engels, A. Sydanheimo, and M. Kivikoski, “Reliability of passive rfid of multiple objects using folded microstrip patch-type tag antenna,” in *2005 IEEE Antennas and Propagation Society International Symposium*, vol. 2. IEEE, 2005, pp. 341–344.

[231] R. H. Clarke, D. Twede, J. R. Tazelaar, and K. K. Boyer, “Radio frequency identification (rfid) performance: the effect of tag orientation and package contents,” *Packaging Technology and Science: An International Journal*, vol. 19, no. 1, pp. 45–54, 2006.

[232] K. Qian, C. Wu, F. Xiao, Y. Zheng, Y. Zhang, Z. Yang, and Y. Liu, “Acousticcardiogram: Monitoring heartbeats using acoustic signals on smart devices,” in *Proc. of IEEE INFOCOM*. IEEE, 2018, pp. 1574–1582.

[233] F. Zhang, Z. Wang, B. Jin, J. Xiong, and D. Zhang, “Your smart speaker can“hear” your heartbeat!” *Proc. of ACM UbiComp*, vol. 4, no. 4, pp. 1–24, 2020.

[234] J. Liu, D. Li, L. Wang, and J. Xiong, “Blinklistener: “listen” to your eye blink using your smartphone,” *Proc. of ACM UbiComp*, vol. 5, no. 2, pp. 1–27, 2021.

[235] D. Dai, Z. An, Z. Gong, Q. Pan, and L. Yang, “RFID+: Spatially controllable identification of UHF RFIDs via controlled magnetic fields,” in *Proc. of USENIX NSDI*, 2024, pp. 1351–1367.

[236] E. Arikan, “Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels,” *IEEE Transactions on information Theory*, vol. 55, no. 7, pp. 3051–3073, 2009.

[237] E. A. Keehr, “A low-cost software-defined uhf rfid reader with active transmit leakage cancellation,” in *2018 IEEE International Conference on RFID (RFID)*. IEEE, 2018, pp. 1–8.