MagFingerprint: A Magnetic Based Device Fingerprinting in Wireless Charging

Jiachun Li*, Yan Meng*, Le Zhang*, Guoxing Chen*, Yuan Tian†, Haojin Zhu*§, and Xuemin (Sherman) Shen‡
*Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China
†Electrical and Computer Engineering Department, University of California, Los Angeles, USA
‡Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Canada
Email: {jiachunli, yan_meng, sj-16-zl, guoxingchen, zhu-hj}@sjtu.edu.cn, yuant@ucla.edu, sshen@uwaterloo.ca

***Abstract*—Wireless charging is a promising solution for charging battery-driven devices pervasively. However, the wide deployment of wireless charging stations is vulnerable to the *device masquerade attack*, which causes financial loss when billing or charging system damages like overheating and explosion. Device fingerprinting is a classical technique to thwart the device masquerade attack. But existing works either are vulnerable to forging or require specialized equipment, which is not suitable for wireless charging.**

In this paper, we design a magnetic based fingerprinting system MAGFINGERPRINT, which utilizes the alternating magnetic signals as the fingerprint and is compatible with existing wireless charging systems. MAGFINGERPRINT is convenient for the user since it only employs commercial-off-the-shelf (COTS) magnetic sensors and requires no action from users. In particular, for the charging device, based on its intrinsic manufacturing errors, MAGFINGERPRINT generates a unique fingerprint according to the distinct magnetic changes during the wireless charging process. It is shown that MAGFINGERPRINT can achieve an accuracy of 98.90% on wireless charging exposed coils, while it is also effective on different commercial wireless charging pads of Apple, Huawei, and Xiaomi.

***Index Terms*—Device Fingerprinting, Wireless Charging, Magnetic Signal, Device Masquerade Attack**

I. INTRODUCTION

Numerous battery-driven devices (*e.g.*, smartphones, electric toothbrushes, home appliances) in emerging IoT scenarios [1] face the urgent demand of charging anywhere and anytime. Wireless charging, due to its convenience and user-friendliness, is being increasingly deployed in public infrastructures, such as airports, subway stations, cafeterias, and electric vehicle charging stations. According to the report published by Allied Market Research [2], the global wireless charging market will reach 40.24 billion in 2027 with a compound annual growth rate of 22.2% from 2020.

Despite the great benefits that wireless charging has brought, recent studies [3] point out that it opens a door for the adversary to launch a severe attack named *device masquerade attack* [4], [5]. In this attack, the adversary can threaten the security of both users and wireless charging systems (*e.g.*, wireless power banks, public charging pads). As for the threat toward the user, the attacker can masquerade as the victim's identity when billing, which will lead to the financial loss of the victim user [4], [5]. Concerning attacking the whole charging system, the attacker can stick an adversary coil on malicious devices to damage the wireless charging system [6], which will cause overheating or even an explosion when charging. As a result, the device masquerade attack poses a great threat to deploying the wireless charging system.

The main cause of the device masquerade attack is that current wireless charging systems lack an authentication mechanism for the device's identity. Device fingerprinting is a typical candidate authentication scheme, which builds a fingerprint (*i.e.*, unique identifier) for each device to defend against the device masquerade attack. In current device fingerprinting mechanisms, a device's fingerprint is always derived from the following factors: password [7], mobile identification number [8], location [9] (*e.g.*, Received Signal Strength (RSS), the Channel State Information (CSI) [9]), and hardware difference [10], [11], [12] (*e.g.*, accelerator, gyroscope) [10], [11], [12], [13]. However, password [7] and mobile identification number [8] can be forged by the adversary. Other schemes like location [9] and hardware difference [10], [11], [12] either require users to actively conduct actions unrelated to charging or deploy non-commercial specialized equipment inside the charging system for data collection which increases the user's burden during the deployment. In summary, existing works can not be fitted into the wireless charging process non-invasively and conveniently. Thus, it is crucial to propose a user-friendly method to realize the device fingerprinting while keeping the wireless charging working normally.

In this study, to overcome the aforementioned challenges when applying existing schemes in wireless charging, we propose MAGFINGERPRINT, a passive device fingerprinting system that leverages COTS sensors to collect the magnetic signals as a unique fingerprint without interrupting the normal charging process or requiring the user's participation. Furthermore, it can also serve as an alternative solution for two-factor authentication based on hardware characteristics, which can be compatible with existing authentication solutions.

Our basic insight is based on the phenomenon that wireless charging signals can be served as a unique factor for device fingerprinting. More specifically, when the device is undergoing wireless charging, the changeable wireless signal (*i.e.*, the magnetic signal) has a unique characteristic related to the device's inherent hardware properties. Thus, via contact-less collecting and analyzing the wireless signals, the unique device

[§] Haojin Zhu is the corresponding author.

979-8-3503-3414-2/23/$31.00 ©2023 IEEE

fingerprint can be passively constructed without requiring any special actions from the device's owner and the device itself. However, it is still quite challenging to build such a convenient, effective, and robust device fingerprinting scheme based on this phenomenon. Particularly, we need to answer the following research challenges: *(1)* How to collect useful data conveniently? *(2)* How to effectively capture the distinct and inherent factors inside devices when charging? *(3)* Considering our MAGFINGERPRINT is the first magnetic based device fingerprinting scheme in wireless charging, how to verify its robustness in real world environments?

In this paper, we address these challenges as follows. Firstly, for *challenge 1*, when a new device is placed at the charging station, we collect the alternating magnetic signals leveraging an array with four commercially available and tiny magnetic sensors, which do not need to modify the internal circuit for convenience consideration. Secondly, for *challenge 2*, to capture the characteristics effectively, MAGFINGERPRINT performs the pre-processing and noise filtering schemes to improve the collected data quality. We also propose a combined feature, which consists of temporal features, frequency features, observed features, and auxiliary features. Finally, for *challenge 3*, we implement MAGFINGERPRINT on widely-adopted real world commercial wireless charging systems, in which various factors (*e.g.*, battery level, placement, background applications, training dataset size) are considered and evaluated.

As for the performance of MAGFINGERPRINT, it can achieve an accuracy of 98.90% when conducting the task of identifying 20 smart devices with three popular commercial charging pads, including Apple, Huawei, and Xiaomi. Considering the impacts of various environmental factors, MAGFINGERPRINT maintains a high accuracy of 91.95% even in the worst case. Besides, the proposed MAGFINGERPRINT is superior to existing systems in the experimental evaluations. The contributions of this work are summarized as follows:

- We propose a novel passive magnetic based device fingerprinting system MAGFINGERPRINT, which is convenient and user-friendly. To the best of our knowledge, MAGFINGERPRINT is the first device fingerprinting system based on magnetic changes in wireless charging.
- We establish a wireless charging circuit system and conduct case studies to verify the motivation of MAGFINGERPRINT. Then, we design a novel array based data collection method to extract the precise real time alternating magnetic signals and propose effective fingerprinting features (*e.g.*, time-frequency information, device characteristics).
- We implement MAGFINGERPRINT on three commercial wireless charging pads developed by Apple, Huawei, and Xiaomi. The real world experimental results with 20 devices show that MAGFINGERPRINT achieves above 91.95% under various occasions, which proves its robustness.

The remainder of this paper is organized as follows. The background is introduced in Section II. We introduce the insights for designing MAGFINGERPRINT in Section III. In Section IV, we elaborate the details of MAGFINGERPRINT which is followed by evaluation, discussion, related works, and conclusion in Section V, VI, VII, and VIII respectively.

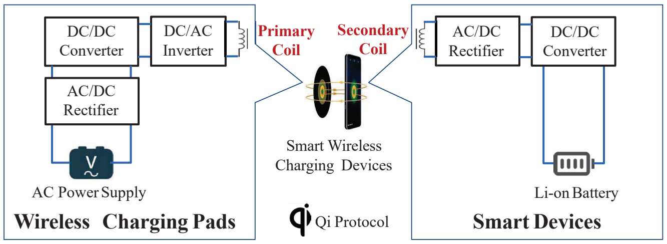


Fig. 1. Illustration of wireless charging system.

II. BACKGROUND

In this section, we introduce the preliminaries of this study, including the details of the wireless charging process (*i.e.*, the mainstream protocol — Qi protocol and the electromagnetic induction).

The development of wireless charging can be categorized into two directions, radiative wireless charging and coupling based wireless charging [14]. Radiative wireless charging leverages the electromagnetic waveform to transmit the energy in the electric field. Considering the coupling based wireless charging, the insight is that the energy can be transmitted by the coupling between the two coils (*i.e.*, the primary coil, the secondary coil in Fig. 1). The latter techniques are widely used in terms of the IoT devices' wireless charging, which follows the open interface standard Qi [15] developed by the Wireless Power Consortium (WPC).

Qi messages. The Qi standard developed by the WPC is the mainstream protocol in the range of wireless charging, which is widely used in smart devices when conducting wireless charging. It can be divided into 5 phases, which are the start phase, the ping phase, the identification and configuration phase (ID&C), the power-transfer phase (PT), and the ending phase. Firstly, the power transmitter sends a packet to verify whether a device is valid. Secondly, a ping packet is transmitted to receive an adequate replying packet with enough density. Thirdly, the ID&C phase is used to set up the configuration by packet transmission for the next phase (*i.e.*, power transferring). Then, in the PT phase, the energy is transferred to charging devices. It also sends the "Control Error" packet to optimize the charging progress. Finally, when the receiver mutes the transmission, the charging process will be ended simultaneously.

Electromagnetic induction. In the charging progress, the electric field changes satisfy Faraday's law of electromagnetic induction[16], which is represented as $\nabla \times E = -\frac{\partial B}{\partial t}$, where B refers to the magnetic flux density, and E denotes the electric field. Besides, the displacement field D is calculated as $D = \epsilon_0 E$, where ϵ_0 represents the electric permittivity.

The magnetic changes are restricted to Ampere's law.

$$\begin{aligned} \nabla \times H &= J + \frac{\partial D}{\partial t}, \\ \nabla \times B &= \mu_0 J + \mu_0 \epsilon_0 \frac{\partial E}{\partial t}, \end{aligned} \tag{1}$$

where H represents the magnetic flux density, and J denotes the charging current density. And the derivation of the magnetic flux density B and the electric field E follows $H = \mu_0 B$, where μ_0 refers to the magnetic permeability.

As shown in Fig. 1, the charging process can be clarified as follows. After the prepossessing of the alternating current/direct current (AC/DC) rectifier, the DC/DC converter, and the DC/AC inverter [14], the high-frequency alternating current (AC) will be sent to the primary coil, which will generate an alternating magnetic field according to the Faraday's law. Simultaneously, the induced voltage will be generated in the secondary coil due to the alternating magnetic field relying on Ampere's law in (1). The induced voltage is processed by the rectification and filtering techniques and finally replenished at the load (*e.g.*, Li-on battery in smartphones).

III. Threat Model and Motivation

In this section, we introduce the threat model, and elaborate the insight of this study by circuit analysis, then validate the insight on case studies.

A. Threat Model

When conducting wireless charging, the adversary in the device masquerade attack can threaten user and wireless charging systems on both software and hardware sides. On the software side, the attacker is capable of leveraging the broadcast nature of wireless signals and the programmability of smart devices to forge the devices. More specifically, the attacker can control the devices and masquerade them as legitimate identities [4], [5]. Thus, the malicious deduction can be performed when billing since the attacker can charge the device using other victims' financial accounts [4], [5], especially in electric vehicle charging. On the hardware side, the attacker can bypass the authentication and stick an adversary coil on the malicious devices when conducting wireless charging [6]. It may cause overheating or even an explosion to threaten the user and the system. Therefore, device fingerprinting should be proposed to ensure the security of wireless charging.

B. Motivation

Based on the fact that there are subtle hardware differences introduced by manufacturing errors in smart devices[17], our study is based on the following insights: *"subtle hardware differences" in smart devices can lead to the unique alternating current or magnetic changes during wireless charging, which can be leveraged as fingerprints.* To validate this insight, we firstly develop a novel circuit based wireless charging demo system by following the standardized Qi protocol. Then we perform two case studies, which are designed to answer the following questions: 1. Given a specific device, will the magnetic field have significant changes if slightly modifying the electrical unit (*i.e.*, "test equipment") in the circuit? 2. Given commercial devices even with the same brand and type, is it possible to distinguish one from others by only exploiting the magnetic device fingerprints?

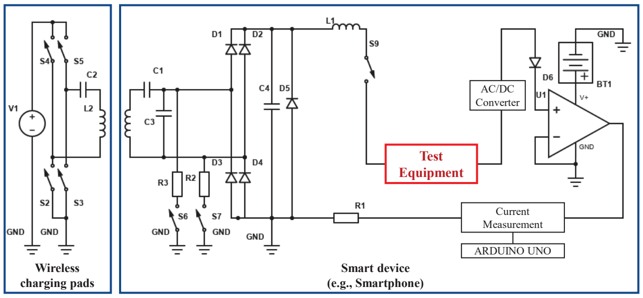
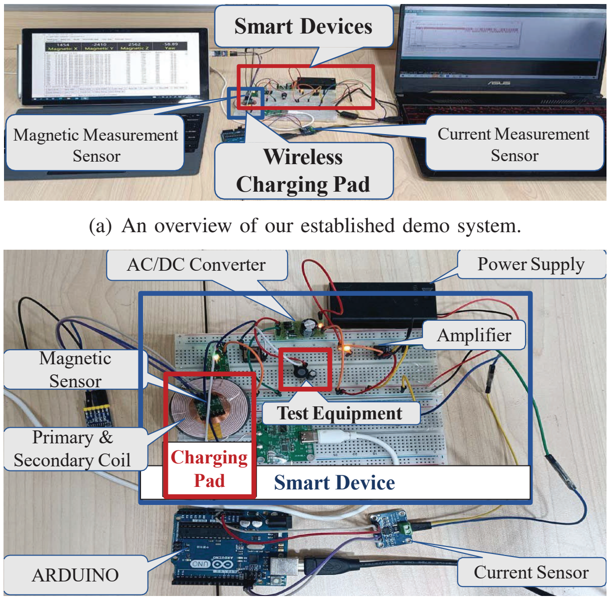


Fig. 2. The circuit diagram of our established wireless charging demo system following Qi protocol.



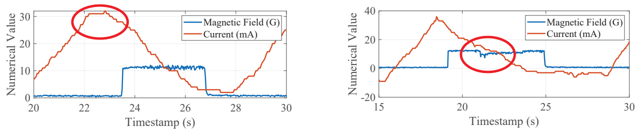
(a) An overview of our established demo system.

(b) A close look at the demo system components.

Fig. 3. Wireless charging demo system.

1) Case Study 1: Demonstrating Impact of Subtle Hardware Differences on Magnetic Field: When investigating the impact of "subtle hardware differences" inside smart devices when charging, to eliminate the distortion caused by various electrical components (*e.g.*, resistance, capacitance, specialized sensor) types and running applications in commercial devices, we establish an open and "clean" wireless charging circuit system. We use a small component called "test equipment" of the smart device circuit to model the "subtle hardware difference", which is set as the capacitive circuit (*i.e.*, $R + \frac{1}{jwC}$) or the pure resistance circuit (*i.e.*, R). Note that, the settings of the wireless charging system in Fig. 3(a), and 3(b), follow the aforementioned wireless charging protocol — Qi protocol.

The settings of case studies. In Fig. 3(a), we implement two personal computers to measure the magnetic intensity and the current value respectively. The current measurement devices consist of an INA219 sensor and an ARDUINO UNO for



(a) Test equipment: $R+\frac{1}{j\omega C}$, $R = 1.00K\Omega$, $C = 4.7\mu F$.

(b) Test equipment: R, $R = 1.00K\Omega$.

Fig. 4. Changing ”test equipment“ to model the subtle hardware differences.

controlling. The QMC5883 sensor is utilized for measuring magnetic intensity. In Fig. 3(b), the secondary coil receives the energy from the primary coil and transmits it to the next component. We implement the AC/DC converter to generate the direct current. The magnetic sensor is upon the secondary coil to evaluate the magnetic intensity. The current sensor is also connected in series in the circuit to measure the real time current value. To show the results more obviously, LM358 is used as an amplifier for current. In experiments, the two conditions of smart devices are set as the capacitive circuit (*i.e.*, $R+\frac{1}{j\omega C} = 1.00K\Omega + \frac{1}{j\omega \times 4.7\mu F}$) and the pure resistance circuit (*i.e.*, $R = 1.00K\Omega$).

Results. The evaluation results well answer our first question on the impact of subtle hardware differences on the magnetic fingerprint. As shown in Fig. 4(a) and Fig. 4(b), when the test equipment changes from $R + \frac{1}{j\omega C}$ to R, which models the subtle hardware differences in the circuit (*e.g.*, manufacture errors and user usage in commercial devices), lead to observable differences of current and magnetic when charging.

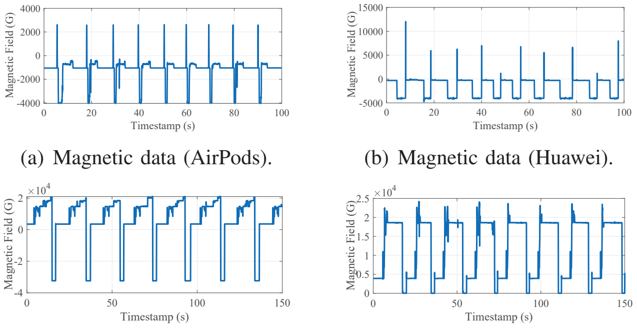
2) *Case Study 2: Demonstration of Magnetic Fingerprint Differences for Commercial Devices:* To further validate the insight that the magnetic difference when charging can be leveraged as fingerprints to distinguish commercial smart devices, we perform the case studies on commercial smartphones. We choose devices of different brands (*i.e.*, an Apple AirPods and a Huawei Mate40Pro) and devices of the same brand and type (*i.e.*, two iPhoneXRs).

According to Fig. 5(a) and Fig. 5(b), the magnetic field changes have significant differences, which can be leveraged as fingerprints among devices of different brands. Besides, it is observed in Fig. 5(c) and Fig. 5(d) that even if the smartphones are of the same brand and type, the differences between magnetic field changes are still distinguishable for device fingerprinting. This result well answers question Q2.

Thus, the above two case studies demonstrate the correctness of the insight, which motivates our proposed MAGFINGERPRINT in the next section.

IV. THE DESIGN OF MAGFINGERPRINT

In this section, we introduce the technical details of MAGFINGERPRINT, which consist of four modules, the *Data Collection Module*, the *Pre-processing Module*, the *Feature Extraction Module*, and the *Classification Module* as shown in Fig. 6.



(a) Magnetic data (AirPods).

(b) Magnetic data (Huawei).

(c) Magnetic data (iPhoneXR 1).

(d) Magnetic data (iPhoneXR 2).

Fig. 5. Magnetic field changes during the plug-in-plug-out charging.

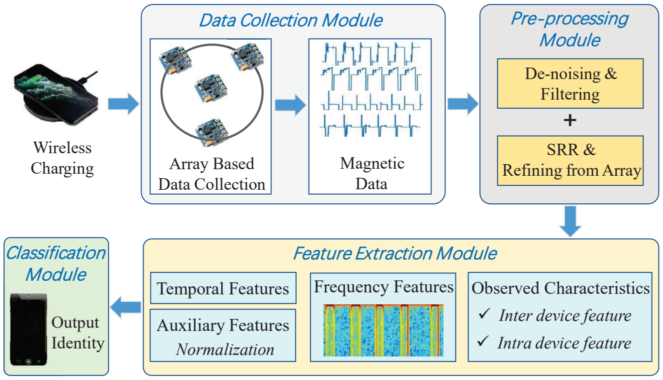


Fig. 6. System overview of MAGFINGERPRINT.

A. Data Collection Module

In this module, MAGFINGERPRINT collects alternating magnetic changes in wireless charging. To capture tiny changes accurately, we first conduct the sensor calibration and design an array with four magnetic sensors in Fig. 7. Note that, the magnetic sensor [18] is vertical to the coil plane and it is placed beneath the primary coil on the charging pad.

Preparation phase: calibrating magnetic sensors. To mitigate the impact of the external environment and the sensor placement, MAGFINGERPRINT calibrates the four magnetic sensors before data collection. Specifically, we rotate the magnetic sensors and gather the results together. As shown in Fig. 8(a) and Fig. 8(b), after the calibration, the re-collected calibrated data is more concentrated around 0, and the noise of the external environment can be significantly mitigated.

Data collection phase: array based scheme. Considering the fact that magnetic fields from various positions could provide more fine-grained information about the target charging smart device, we utilize a magnetic sensor array during data collection. As shown in Fig. 7, given a magnetic sensor $Sensor_i$ (*i.e.*, the i-th magnetic sensor), the sampling rate is set to F_s and the collected magnetic signal is denoted as M_i. When the duration time is T, the collected sampled data M_i has P sampling points, where $P = F_s \times T$. Finally, the collected sampled data with multiple sensors is transmitted to the *Pre-processing Module*.

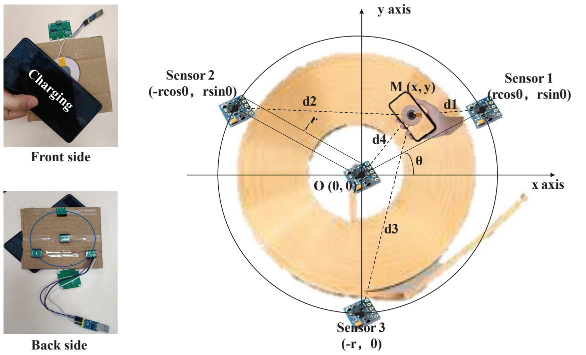
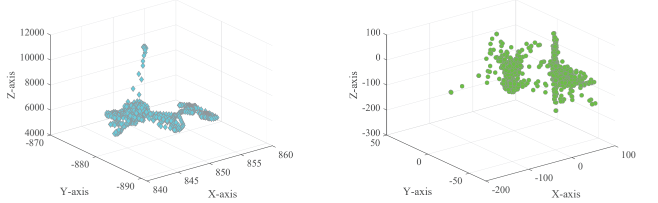


Fig. 7. Real world settings of MAGFINGERPRINT and array based data collection.



(a) Before calibration (time a).

(b) After calibration (time b).

Fig. 8. Collected data before/after the sensor calibration in the first sensor.

B. Pre-processing Module

After obtaining the raw data, to eliminate the influence of noises and low sampling rate, we design the *Pre-processing Module*, which consists of three steps: de-noising, super-sampling rate [19], and array based signal aggregation.

1) De-noising & Filtering: Since the collected data contains external noises which shield the signal component related to the device's inherent characteristics, it is important for MAGFINGERPRINT to conduct de-noising and filtering. We implement a pre-emphasis mechanism and a moving average filter for de-noising and filtering. More specifically, we denote original sampled discrete data (*i.e.*, the collected magnetic signals) as M_i and the pre-emphasis process is as follows:

$$E[n] = M_i[n] - \epsilon M_i[n-1], \quad n \geq 2 \tag{2}$$

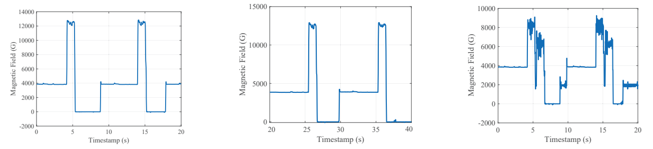
where $E[n]$ is the data after the pre-emphasis process and ϵ is set as 0.9 empirically [20].

Furthermore, the moving average filter is used to smooth the signal curves. The filtered data is calculated as follows:

$$FE[n] = \frac{\sum_{m=n}^{m=n-N+1} E[m]}{N}, \quad n \geq 2 \tag{3}$$

where $FE[n]$ represents the pre-emphasized data filtered by the moving average filter. In this study, we empirically set the window size N as 10. After conducting de-noising and filtering, most noises existing in the collected signal are removed.

2) Super-sampling Rate Reconstruction (SRR): Due to the hardware constraint, the sampling rate of the commercial magnetic sensor is limited as 100 Hz, which causes it hard to capture the tiny signal changes and extract the characteristics of the tested devices when charging. Thus, we implement super-sampling rate reconstruction (SRR), which is used to reconstruct the signal by using more samples from other time periods involved [19]. Fig. 9 shows the collected magnetic data before and after the super-sampling rate reconstruction. It is observed that the reconstructed data contains more fine-grained information, which shows the efficiency of SRR.



(a) Before SRR (time period a).

(b) Before SRR (time period b).

(c) After SRR (time period a).

Fig. 9. Magnetic data reconstruction before/after SRR in the first sensor.

3) Refining Magnetic Signals from the Sensor Array: In a practical charging case, the charging device is placed arbitrarily, which causes the signal collected by a single sensor inevitably deviates from its original form. Thus, we propose a signal refining mechanism based on the data collected from the sensor array deployed in Fig. 7. We first conduct a theoretical analysis to prove the superiority of the sensor array. Then, the signal refining process is introduced.

Theoretical analysis. As shown in Fig. 7, for the four-sensor array, the first one is at $(0, 0)$, and the k-th sensors' coordinates as $(X_k, Y_k) = (r \cdot cos(\theta + \frac{2\pi(k-2)}{N}), r \cdot sin(\theta + \frac{2\pi(k-2)}{N})), k = 2, 3, 4$. In this study, N is set to 3.

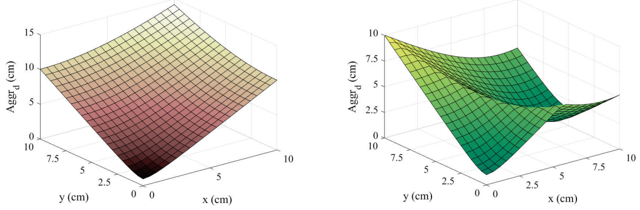
when charging, the secondary coil in the smart device is regarded as a particle magnetic field, which is denoted as $M(x, y)$. When M is not directly right above the primary coil in $O(0, 0)$, in the single sensor scenario, the magnetic sensor locates at $O(0, 0)$. The distance between the single sensor and secondary coil is $d_1 = \sqrt{x^2 + y^2}$. In the sensor array scenario, the distances (*i.e.*, d_1, d_2, d_3, d_4) is calculated as follows:

$$d_1 = \sqrt{x^2 + y^2}, d_k = \sqrt{(x - X_k)^2 + (x - Y_k)^2}. \tag{4}$$

To measure the impact of the location of M on the collected magnetic field, we define the aggregating distance as $Aggr_d$. In the single sensor condition, $Aggr_d = d_1$. When deploying the sensor array, $Aggr_d$ denotes the minimum of the four distances (*i.e.*, $Aggr_d = min(d_1, d_2, d_3, d_4)$).

When M changes in the ranges of $-r \leq x \leq r$, $-r \leq y \leq r$, we conduct a simulation experiment to prove the robustness of $Aggr_d$. For the settings, as shown in Fig. 7, the radius r is set to 10 cm and the thickness of smart device h is 1 cm. As the coil can be placed at any angle when charging, we set θ to $\frac{\pi}{6}$. Fig. 10(a) and Fig. 10(b) show the simulation results. It is observed that $Aggr_d$ in the sensor array condition is much more stable than that in a single sensor condition. Thus, according to the Biot–Savart law [21], the magnetic field calculated in sensor array scenarios will be much more accurate due to the stable $Aggr_d$.

Signal refining mechanism. According to the theoretical analysis, it is proved that the array based scheme can provide more accurate data than that from a single sensor. Thus,



(a) Single magnetic sensor.

(b) Magnetic sensor array.

Fig. 10. Simulation results of $Aggr_d$ in two scenarios.

MagFingerprint dynamically selects the data from the sensor $Sensor_i$ in which $d_i = Aggr_d$ as the main signal and regards other signals as assistance during the feature generation in the next subsection.

C. Feature Extraction Module

In this subsection, we introduce the details of the features, which consist of the temporal features, the frequency features, the observed characteristics, and the auxiliary features.

1) Temporal Features: As defined in the *Pre-processing Module*, the pre-processed collected data is defined as $FE[1:P,i]$ for the i-th magnetic sensor, which contains the sampling points P. As for the charging curve, MagFingerprint captures the high peaks $hp = [hp_1, hp_2, ..., hp_k]$ and the low peaks $lp = [lp_1, lp_2, ..., lp_k]$, where k denotes the number of peaks. Then, MagFingerprint exploits the segmentation schemes to divide the data according to the hp and lp. The divided data for the i-th magnetic sensor is as follows:

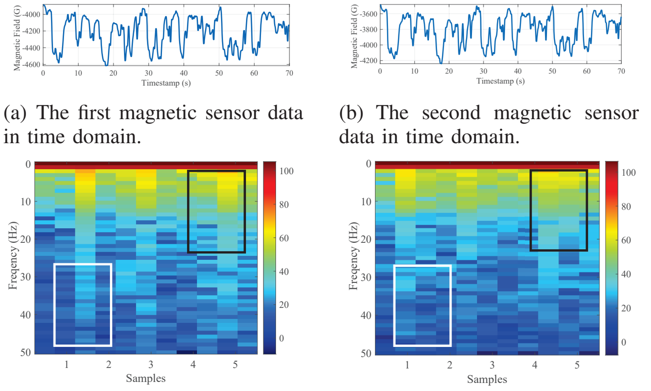
$$FE[:,i] = [FE[hp_1 : lp_1, i], ..., FE[hp_k : lp_k, i]], \tag{5}$$

which is set as the temporal features F_{Temp}.

2) Frequency Features: Besides temporal features, MagFingerprint also extracts features from the perspective of frequency. For instance, as shown in Fig. 11(a) and Fig. 11(b), when performing screen unlocking and locking operations, the magnetic field will change in the wireless charging scene. However, it is observed that the magnetic data changes in the given time period are similar, which demonstrates that simply utilizing the temporal features is not enough. Therefore, MagFingerprint extracts frequency features via the following two steps.

Exhibiting the device's characteristics via frequency analysis. To extract frequency features, we first perform a Short Time Fourier Transform (STFT) on the divided frames and generate the corresponding frequency spectrum as $S[:,:,i] = [S[\frac{hp_1\times N_{FFT}}{F_s} : \frac{lp_1\times N_{FFT}}{F_s}, :, i], ..., S[\frac{hp_k\times N_{FFT}}{F_s} : \frac{lp_k\times N_{FFT}}{F_s}, :, i]]$.

During the STFT process, for the i-th magnetic sensor, S represents the frequency spectrum. A Hanning window is implemented on the magnetic signals $FE[:,i]$. The overlap window size is set as 48, which is the half size of the Hanning window. To reduce the overhead of calculation, we implement the cut-off frequency f_{band} filter on $S[:,:,i]$. For the i-th magnetic sensor, the processed S_{cut} is represented as $S_{cut}[:,:,i] = S[1:Freq,:,i]$, where $Freq = (f_{band} \times N_{FFT})/F_s$, where FFT points $N_{FFT} = 96$, the F_s is set as 100 Hz in this study. $Freq$ denotes the number of the samples which are limited by the frequency band f_{band}. The size of $S[:,:,i]$ is calculated as $width_{spec[i]} \times height_{spec[i]}$, and the size of $S_{cut}[:,:,i]$ is calculated as $Freq \times height_{spec[i]}$.



(a) The first magnetic sensor data in time domain.

(b) The second magnetic sensor data in time domain.

(c) The first magnetic sensor data in frequency domain.

(d) The second magnetic sensor data in frequency domain.

Fig. 11. The magnetic data from different sensors in time domain and frequency domain (when performing screen on and off).

After performing the STFT, the collected data from Fig. 11(a) and Fig. 11(b) are processed, and the generated spectrums are shown in Fig. 11(c) and Fig. 11(d). It is observed that the energy distribution in the spectrum diagram is different, which is obvious in the white block and the black block. Thus, STFT is useful for the collected data in this study.

Refining and finalizing the frequency features. After performing STFT, MagFingerprint transforms the processed data $S[1:Freq,:,i]$ to the grid matrix, which is represented as $G[:,:,i]$ for the data collected by the i-th magnetic sensor, where $i = 1,2,3,4$ in this study. For a given data collected by the i-th sensor, the spectrum $S[1:Freq,:,i]$ is divided into $M_{grid} \times N_{grid}$ chunks, then MagFingerprint calculates the sum of elements in $S[1:Freq,:,i]$ in the range of the corresponding generated grid matrix, which is as follows:

$$G[m,n,i] = \sum_{k_w=(m-1)\times w_{g[i]}}^{m\times w_{g[i]}} \sum_{k_h=(n-1)\times h_{g[i]}}^{n\times h_{g[i]}} S[k_w,k_h,i], \tag{6}$$

where w_g and h_g represent the width and the height of each divided chunk, which is calculated as follows:

$$w_{g[i]} = \lfloor \frac{Freq}{M_{grid}} \rfloor, h_{g[i]} = \lfloor \frac{height_{spec[i]}}{M_{grid}} \rfloor. \tag{7}$$

In this study, M_{grid} and N_{grid} are set as 80 and 100 respectively. Then, the frequency features matrix is calculated as the average value of the grid matrix from 4 different magnetic sensors. The chunks in this matrix are still $M_{grid} \times N_{grid}$. Finally, we obtain the frequency features F_{Freq} and its j-th element can be represented as:

$$F_{Freq}[j] = \sum_{k=1}^{N_{grid}} \sum_{i=1}^{4} \frac{G[j,k,i]}{4}. \tag{8}$$

3) Observed Characteristics: To investigate the characteristics between inter-type devices (*i.e.*, different devices of different types) and intra-type devices (*i.e.*, different devices of the same types), we design the observed characteristics, which are denoted as F_{Cha}. As for the inter-type characteristics, it consists of the mean value, the Root Mean Square amplitude, and the spread of the spectrum. Considering the intra-type characteristics, it contains the roll-off, the average value, and the standard deviation of the spectrum.

4) Auxiliary Features: To further improve the effectiveness of MAGFINGERPRINT, besides the aforementioned features, we propose the auxiliary features. Firstly, for the processed data $FE[:,i]$ collected by the i-th magnetic sensor, we first choose the magnetic field according to the array based analysis. Then we perform the normalization operation to generate the reconstructed data $ReFE[:]$ as follows:

$$Norm_{ReFE}[:] = \frac{ReFE[:] - min(ReFE[:])}{max(ReFE[:]) - min(ReFE[:])}. \tag{9}$$

Then we exploit a light-weighted feature extraction library, LibXtract[22] on the normalized data $Norm_{ReFE}[:]$ to generate the auxiliary features (*i.e.*, F_{Aux}).

5) Feature Aggregation: After generating all necessary features, MAGFINGERPRINT aggregates the features X as $X = [F_{Temp}, F_{Freq}, F_{Cha}, F_{Aux}]$. Then, MAGFINGERPRINT exploits the FEAST toolbox [23] to rank the features and select the top k features to reduce the calculation load. Then, the generated features of the j-th devices $X_j[1:k]$ are transmitted to the *Classification Module*.

D. Classification Module

In this subsection, after obtaining X from a given charging device, MAGFINGERPRINT utilizes a classifier to determine the device's identity. We elaborate on the classifier building and execution processes below.

Classifier construction. To build an effective and robust classifier, we follow Section IV-A and Section IV-B to collect data from various charging devices. Then, we extract the features and label the identity of devices, which is built as the feature dataset $F = [X_0[1:k], ..., X_j[1:k]]$. After that, we input training data into four classifiers (*i.e.*, Support Vector Machines (SVM)-Linear, SVM-rbf, SVM-poly, Naive Bayes). The generated classifier is used in device verification.

Device verification. After obtaining a classifier by training, for a given device, the classifier outputs the predicted identity. If the predicted label is as it claimed, MAGFINGERPRINT regards the device as benign and charges the given devices. Otherwise, MAGFINGERPRINT regards it as the device masquerade attack and declines the charging requirement. Note that, compared with the deep neural networks, the light-weighted classifiers in MAGFINGERPRINT can fingerprint quickly.

V. EVALUATION

In this section, we elaborate on the details of the experiments. To demonstrate the robustness of MAGFINGERPRINT, we evaluate the impact of environmental factors (*e.g.*, battery level, placement, background applications) and MAGFINGERPRINT's configurations (*e.g.*, training dataset size). Furthermore, we also validate the performance on different commercial charging pads.

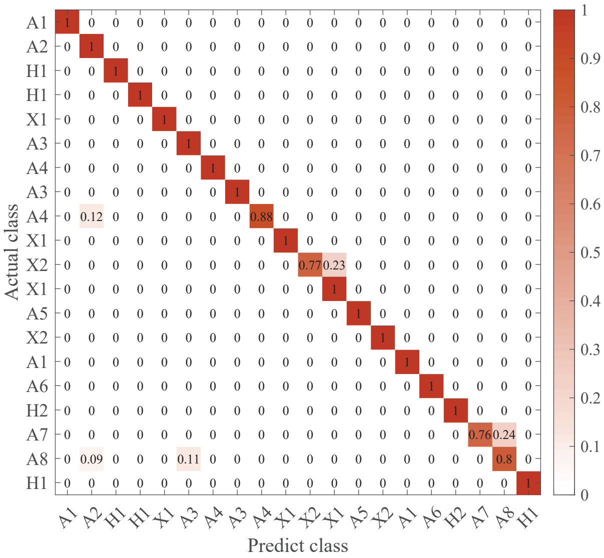


Fig. 12. Confusion matrix of the evaluated devices.

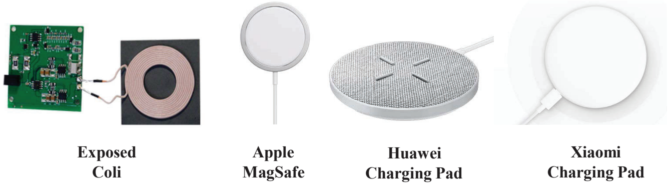


Fig. 13. Charging pad produced by different developers.

A. Experiment Settings

The experiment setting of data collection has been clarified in Section IV-A. The magnetic data collected by QMC5883 [18], is transferred to the serial converter, which is visualized on a personal computer. We implement MAGFINGERPRINT on a desktop with 64-bit Ubuntu 18.04 OS, Intel Core i7 CPU, and 64 GB RAM. As for the ethnic consideration, there are no human participants. Thus it is exempt from the institutional review board (IRB).

In this study, we evaluate 20 devices in total. The charged devices include smartphones from Apple, Huawei, Xiaomi, and the AirPods from Apple. For the charging pad, the experiments are conducted on the exposed coil and the other three commercial charging platforms (*i.e.*, MagSafe developed by Apple, the charging pad developed by Huawei, and Xiaomi) shown in Fig. 13. Note that, the tested devices are from different manufacturers and follow the Qi protocol. As for the settings, the charging process is set as 50 times per device, and the battery level is set as 60%. All the background applications are muted down, and the feature dimension is 200.

In summary, we collect 1740 samples from 20 devices on 4 different charging pads. The collected data is divided to generate the training dataset and the testing dataset according to the split ratio (*i.e.*, 7:3), which is selected according to the

TABLE I
OVERALL PERFORMANCE OF MAGFINGERPRINT

Classifier	Accuracy (%)	F-score	Time Overhead (s)
SVM-Linear	98.90	0.98	0.30
SVM-Rbf	97.80	0.97	0.48
SVM-Poly	88.60	0.89	0.43
Naive Bayes	98.90	0.99	0.21

TABLE II
THE DETAILS OF THE EVALUATED DEVICES

Devices	Details	Producer	Devices	Details	Producer
A1	AirPods3	Apple	**A2**	iPhone11	Apple
H1	Mate40Pro	Huawei	**H1**	Mate40Pro	Huawei
X1	Mi9	Xiaomi	**A3**	P40Pro	Apple
A4	iPhone12	Apple	**A3**	P40Pro	Apple
A4	iPhone12mini	Apple	**X1**	Mi9	Xiaomi
X2	Mi10	Xiaomi	**X1**	Mi9	Xiaomi
A5	iPhoneXR	Apple	**X2**	Mi10	Xiaomi
A1	AirPods3	Apple	**A6**	iPhoneSE	Apple
H2	Mate20Pro	Huawei	**A7**	iPhoneXR	Apple
A8	iPhone8	Apple	**H1**	Mate40Pro	Huawei

evaluations in Section V-D. Besides, the classification module will select the best results among all the involved classifiers if not clarified in Section V.

B. Overall Performance

The overall accuracy and time overhead are shown in TABLE I. We implement the lightweight classification algorithms (*i.e.*, SVM-Linear, SVM-rbf, SVM-poly, Naive Bayes) in Section IV-D.

The details of the participated devices are shown in TABLE II. Besides, the overall time overhead (*i.e.*, $Time_{overall}$) is comprised of the data collection (*i.e.*, 17.05 seconds), the feature generation (*i.e.*, 0.74 seconds), and the classification overhead (*i.e.*, 0.30 seconds), which occupies 94.25%, 4.09%, and 1.66%. The registration time is 18.09 seconds per device, which is acceptable for device fingerprinting compared with existing works (*e.g.*, 55.50 seconds in [24]). As shown in TABLE I and Fig. 12, MAGFINGERPRINT can classify the devices with low time latency and high accuracy according to the magnetic signals via wireless charging.

C. Impact of Environmental Factors on MAGFINGERPRINT

In this subsection, we evaluate the impact of various environmental factors on MAGFINGERPRINT to demonstrate the robustness of the proposed system. Except for the evaluation of the given factors, all the experiments follow the same configuration in Section V-A.

1) Battery Level: Since the process of wireless charging is related to the current battery level [3], it is crucial to evaluate the impact of battery level on MAGFINGERPRINT. To evaluate this factor, we set the battery level of all devices as 20%, 40%, 60%, and 80%.

As illustrated in TABLE III, the accuracy decreases when the battery level is increasing from 60% to 80% and 80% to 90%. It is because when the battery is nearly full, the charging process will slow down [3], and fewer characteristics inside the evaluated devices will be revealed during the testing time period. However, the accuracy is still above 97.00%, which is acceptable and stable to realize the function of fingerprinting.

TABLE III
IMPACT OF THE BATTERY LEVEL

Battery Level	20%	40%	60%	80%	90%
Accuracy (%)	98.70	98.90	98.90	97.80	97.20
F-score	0.99	0.99	0.99	0.98	0.98

TABLE IV
IMPACT OF THE PLACEMENT ANGLE

Placement Angles	Accuracy (%)	F-score	Placement Angles	Accuracy (%)	F-score
0°**&** 360°	93.05	0.94	180°	93.15	0.94
45°	91.95	0.93	225°	92.90	0.94
90°	95.80	0.94	270°	95.95	0.95
135°	99.90	0.99	315°	99.90	0.99

2) Placement: In the real world environment, It is known that the user can place the smart devices randomly on the wireless charging pad. To explore the impact of different placements, we set the tested device at different angles. Each tested device is rotated 45° in every trial, which is set as 0°, 45°, 90°, 135°, 180°, 225°, 270°, 315°.

As depicted in TABLE IV, the experimental results demonstrate that MAGFINGERPRINT can maintain the fingerprinting performance under various placements of the target device. It reveals that the accuracy is above 91.00% regardless of the changes in the placement angles, which demonstrates the robustness and effectiveness of MAGFINGERPRINT in wireless charging scenarios.

3) Background Applications: The state-of-the-art works have proved that background application impacts the wireless charging process [3]. When running background applications, the charging rate will slow down [25]. The consumption of energy when running the aforementioned applications is different, which will affect the wireless charging process differently. In this study, to evaluate the impact of background running applications, we choose 4 typical applications, which are TikTok, Chrome browser, WeChat, and Messages. More specifically, we categorize the occasions into the single application running and multiple application running.

As depicted in TABLE V, compared with the situation in the overall evaluation (*i.e.*, all the applications are muted down), the accuracy of MAGFINGERPRINT will decrease when the background applications are running. When the number of the background running applications increase or more energy-consuming applications are running, the accuracy will decrease too. The reason is that, if the applications consume more energy, fewer characteristics will be captured in the same time period since less energy is distributed to wireless charging. In summary, MAGFINGERPRINT still performs stably under the occasion of background applications running.

4) Different Pads: To evaluate the performance of MAGFINGERPRINT on the commercial charging platforms, we deploy MAGFINGERPRINT on various charging pads (*i.e.*, Apple MagSafe, Huawei, Xiaomi Charging Pad) in Fig. 13.

It is observed in Fig. 14 that the performance of MAGFINGERPRINT is still above 80%, which is also effective on the other commercial wireless charging platforms.

TABLE V
IMPACT OF THE BACKGROUND APPLICATION

Single App Running	Accuracy (%)	F-score	Multiple App Running	Accuracy (%)	F-score
Messages (App1)	94.30	0.95	**App1 & App2**	93.25	0.94
Chrome Browser (App2)	93.10	0.94	**App3 & App4**	92.25	0.92
WeChat (App3)	93.30	0.94	**App1 & App2 & App3**	92.10	0.92
TikTok (App4)	93.15	0.94	**App1 & App2 & App3 & App4**	92.85	0.92

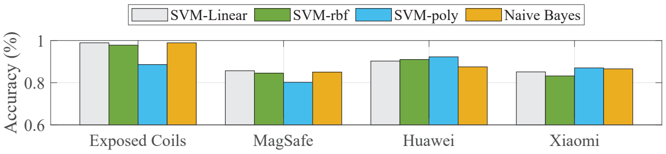


Fig. 14. Performance on different commercial charging pads.

D. *Impact of Configurations on* MagFingerprint

In this subsection, we evaluate the impact of configurations on the performance of MagFingerprint.

1) Size of the Training Dataset: To evaluate the cost of the registration process, we change the proportion of the training dataset in this subsection. It is adjusted from 30% to 90%.

TABLE VI shows that when the size of the training dataset increases, the performance of MagFingerprint gets improved, and the time overhead of training MagFingerprint increases simultaneously. However, the overall performance of MagFingerprint is above 93.00% and the time overhead of MagFingerprint is 18.09 seconds for each participating device, which demonstrate the efficiency of MagFingerprint when the bootstrapping time is limited.

VI. Discussions

In this section, we discuss the limitations and the future work of MagFingerprint.

Shapes and Sizes of Devices. In this study, the selected wireless charging coil is in a round shape, which supports most smartphones and some earphones. However, some Qi-supported devices with no regular shapes (*e.g.*, the charging belt in smart toothbrushes) are not considered in this study. For further study, we will implement MagFingerprint on a larger dataset with more devices.

Signal obfuscation. As the device fingerprint is built according to the alternating magnetic signal when charging, it is required that the charging process should be normal. If it is interrupted by signal obfuscation [26], [27], (*e.g.*, the adversarial coil attack [6]), the performance of MagFingerprint will decrease due to the signal obfuscation. In future work, we will consider overcoming this problem.

Long range transmission. Wireless charging techniques implemented on smart devices are still limited to the range of less than 30 cm, which is caused by the fundamental principle of electromagnetic induction currently. In the future, we will study how to enable MagFingerprint to work in a long range transmission charging scenario [28].

TABLE VI
IMPACT OF THE SIZE OF TRAINING DATASET

Training dataset proportion	Accuracy (%)	F-score	Time Overhead (s)
30%	93.10	0.94	0.86
50%	95.00	0.95	0.91
70%	98.90	0.99	0.94
90%	98.95	0.99	0.97

Temporal stability of the tested devices. In this study, temporal stability (*i.e.*, fingerprints may change for a long time) is an inherent drawback, but it does not hinder the deployment of MagFingerprint. To overcome this issue, MagFingerprint can update the device fingerprinting adaptively. Since the process can be conducted passively when charging, the overhead is acceptable.

VII. Related Work

In this section, we present the related works about charging and device fingerprinting.

Existing works have shown the threat to charging. For instance, [29], [30], [31] can deploy malicious applications and steal user privacy via the wired power line. [3], [6], [32], [33] also perform similar side channel attacks in wireless charging. Thus, device fingerprinting is a crucial solution for security consideration recently, like [7], [9], [10], [11], [34], [35], [36], [37], [38], [39], [40]. It can be categorized into the following kinds, identifying based on passwords [7], identifying based on location [9], and identifying based on hardware differences [10], [11], [12], [24], [41]. However, the generation of fingerprinting by existing schemes is either easy to be forged, or requires specialized equipment.

To the best of our knowledge, MagFingerprint is the first work to construct the fingerprint by capturing the magnetic signal changes in the wireless charging scenario, which is convenient, effective, and robust.

VIII. Conclusion

In this study, we propose MagFingerprint, a novel magnetic signal based fingerprinting system in wireless charging scenarios. MagFingerprint is the first work to utilize magnetic signal changes via wireless charging to build unique device fingerprints. Specifically, we establish a circuit based wireless charging demo system to verify motivation and propose novel mechanisms (*e.g.*, array based data collection, feature extraction) for designation. Various experiments are conducted to evaluate the impact of possible factors (*e.g.*, the environmental factors, the configurations) to prove the usability. In summary, MagFingerprint is a convenient, effective, and robust solution for device fingerprinting, which is believed to be effective for identification.

Acknowledgment

This research was supported in part by National Natural Science Foundation of China under Grants No. 62132013 and 61972453, and NSERC of Canada. Yuan Tian is partially supported by NSF award #1943100 and Facebook Faculty Award.

References

[1] D. Minoli, K. Sohraby, and B. Occhiogrosso, "Iot considerations, requirements, and architectures for smart buildings—energy optimization and next-generation building management systems," *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 269–283, 2017.

[2] A. market research, "Wireless charging market outlook-2027," https://www.alliedmarketresearch.com/wireless-charging-market, 2022.

[3] A. S. La Cour, K. K. Afridi, and G. E. Suh, "Wireless charging power side-channel attacks," in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '21, 2021, pp. 651–665.

[4] Q. Xu, R. Zheng, W. Saad, and Z. Han, "Device fingerprinting in wireless networks: Challenges and opportunities," *IEEE Communications Surveys Tutorials*, vol. 18, no. 1, pp. 94–104, 2016.

[5] N. T. Nguyen, G. Zheng, Z. Han, and R. Zheng, "Device fingerprinting to enhance wireless security using nonparametric bayesian method," in *2011 Proceedings IEEE INFOCOM*, 2011, pp. 1404–1412.

[6] Y. Wu, Z. Li, N. Van Nostrand, and J. Liu, "Time to rethink the design of qi standard? security and privacy vulnerability analysis of qi wireless charging," in *Annual Computer Security Applications Conference*, 2021, pp. 916–929.

[7] W. Meng, W. Li, L. Jiang, and L. Meng, "On multiple password interference of touch screen patterns and text passwords," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, ser. CHI '16, 2016, pp. 4818–4822.

[8] S.-H. Seo, A. Gupta, A. Mohamed Sallam, E. Bertino, and K. Yim, "Detecting mobile malware threats to homeland security through static analysis," *Journal of Network and Computer Applications*, vol. 38, pp. 43–53, 2014.

[9] M. Li, Y. Meng, J. Liu, H. Zhu, X. Liang, Y. Liu, and N. Ruan, "When csi meets public wifi: Inferring your mobile phone password via wifi signals," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '16, 2016, pp. 1068–1079.

[10] Y. Cheng, X. Ji, J. Zhang, W. Xu, and Y.-C. Chen, "Demicpu: Device fingerprinting with magnetic signals radiated by cpu," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '19, 2019, pp. 1149–1170.

[11] X. Xu, J. Yu, Y. chen, Q. Hua, Y. Zhu, Y.-C. Chen, and M. Li, "Touchpass: Towards behavior-irrelevant on-touch user authentication on smartphones leveraging vibrations," in *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking*, 2020, pp. 1–13.

[12] G. Baldini and G. Steri, "A survey of techniques for the identification of mobile phones using the physical fingerprints of the built-in components," *IEEE Communications Surveys Tutorials*, vol. 19, no. 3, pp. 1761–1789, 2017.

[13] M. Foruhandeh, A. Z. Mohammed, G. Kildow, P. Berges, and R. Gerdes, "Spotr: Gps spoofing detection via device fingerprinting," in *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WiSec '20, 2020, pp. 242–253.

[14] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless charging technologies: Fundamentals, standards, and network applications," *IEEE Communications Surveys Tutorials*, vol. 18, no. 2, pp. 1413–1452, 2016.

[15] D. van Wageningen and T. Staring, "The qi wireless power standard," in *Proceedings of 14th International Power Electronics and Motion Control Conference EPE-PEMC 2010*, 2010, pp. S15–25–S15–32.

[16] J. Selvaraj, G. Y. Dayanıklı, N. P. Gaunkar, D. Ware, R. M. Gerdes, and M. Mina, "Electromagnetic induction attacks against embedded systems," in *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, ser. ASIACCS '18, 2018, pp. 499–510.

[17] A. Das, N. Borisov, and M. Caesar, "Do you hear what i hear? fingerprinting smart devices through embedded acoustic components," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '14, 2014, pp. 441–452.

[18] S. Technology, "Qmc5883," https://surtrtech.com/2018/02/01/interfacing-hmc8553l-qmc5883-digital-compass-with-arduino/, 2018.

[19] Y. Huang, K. Chen, Y. Huang, L. Wang, and K. Wu, "Vi-liquid: Unknown liquid identification with your smartphone vibration," in *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '21, 2021, pp. 174–187.

[20] W. Han, C.-F. Chan, C.-S. Choy, and K.-P. Pun, "An efficient mfcc extraction method in speech recognition," in *2006 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2006, pp. 145–148.

[21] Wiki, "Biot-savart." https://en.wikipedia.org/wiki/BiotSavart_law, 2022.

[22] J. Bullock, "Libxtract: A lightweight library for audio feature extraction," https://www.jamiebullock.com/LibXtract/documentation/, 2014.

[23] G. Brown, "Feast: A feature selection toolbox for c and matlab." https://github.com/Craigacp/FEAST, 2017.

[24] D. Yang, G. Xing, J. Huang, X. Chang, and X. Jiang, "Qid: Identifying mobile devices via wireless charging fingerprints," in *2020 IEEE/ACM Fifth International Conference on Internet-of-Things Design and Implementation (IoTDI)*, 2020, pp. 1–13.

[25] Samsung, "Phone charging?" https://www.samsung.com/ca/support/mobile-devices/can-you-use-phone-while-charging/, 2020.

[26] Z. Xu, R. Hua, J. Juang, S. Xia, J. Fan, and C. Hwang, "Inaudible attack on smart speakers with intentional electromagnetic interference," *IEEE Transactions on Microwave Theory and Techniques*, vol. 69, no. 5, pp. 2642–2650, 2021.

[27] X. Ji, Y. Cheng, W. Xu, Y. Chi, H. Pan, Z. Zhu, C.-W. You, Y.-C. Chen, and L. Qiu, "No seeing is also believing: Electromagnetic-emission-based application guessing attacks via smartphones," *IEEE Transactions on Mobile Computing*, pp. 1–1, 2021.

[28] X. Chen, H. Wang, F. Wu, Y. Wu, M. C. González, and J. Zhang, "Multimicrogrid load balancing through ev charging networks," *IEEE Internet of Things Journal*, vol. 9, no. 7, pp. 5019–5026, 2022.

[29] B. Lau, Y. Jang, C. Song, T. Wang, P. H. Chung, and P. Royal, "Mactans: Injecting malware into ios devices via malicious chargers," *Black Hat USA*, vol. 92, 2013.

[30] D. J. Tian, G. Hernandez, J. I. Choi, V. Frost, C. Raules, P. Traynor, H. Vijayakumar, L. Harrison, A. Rahmati, M. Grace, and K. R. B. Butler, "ATtention spanned: Comprehensive vulnerability analysis of AT commands within the android ecosystem," in *27th USENIX Security Symposium (USENIX Security 18)*, 2018, pp. 273–290.

[31] Q. Yang, P. Gasti, G. Zhou, A. Farajidavar, and K. S. Balagani, "On inferring browsing activity on smartphones via usb power analysis side-channel," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 5, pp. 1056–1066, 2017.

[32] D. Niyato, P. Wang, D. I. Kim, Z. Han, and L. Xiao, "Game theoretic modeling of jamming attack in wireless powered communication networks," in *2015 IEEE International Conference on Communications (ICC)*, 2015, pp. 6018–6023.

[33] 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*, pp. 1–1, 2022.

[34] S.-Y. Park, S. Lim, D. Jeong, J. Lee, J.-S. Yang, and H. Lee, "Pufsec: Device fingerprint-based security architecture for internet of things," in *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*, 2017, pp. 1–9.

[35] B. Mager, P. Lundrigan, and N. Patwari, "Fingerprint-based device-free localization performance in changing environments," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 11, pp. 2429–2438, 2015.

[36] A. Ostberg, M. Sheik-Nainar, and N. Matic, "Using a mobile device fingerprint sensor as a gestural input device," in *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, ser. CHI EA '16, 2016, pp. 2625–2631.

[37] Z. Zhou, W. Diao, X. Liu, and K. Zhang, "Acoustic fingerprinting revisited: Generate stable device id stealthily with inaudible sound," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '14, 2014, pp. 429–440.

[38] P. Cronin, X. Gao, C. Yang, and H. Wang, "Charger-Surfing: Exploiting a power line Side-Channel for smartphone information leakage," in *30th USENIX Security Symposium (USENIX Security 21)*, 2021, pp. 681–698.

[39] Y. Meng, J. Li, M. Pillari, A. Deopujari, L. Brennan, H. Shamsie, H. Zhu, and Y. Tian, "Your microphone array retains your identity: A robust voice liveness detection system for smart speakers," in *31st USENIX Security Symposium (USENIX Security 22)*, 2022.

[40] L. Xie, Y. Shi, Y. T. Hou, W. Lou, H. D. Sherali, H. Zhou, and S. F. Midkiff, "A mobile platform for wireless charging and data collection in sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 8, pp. 1521–1533, 2015.

[41] J. Zhang, Z. Wang, X. Ji, W. Xu, G. Qu, and M. Zhao, "Who is charging my phone? identifying wireless chargers via fingerprinting," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2992–2999, 2021.