Time to Rethink the Design of Qi Standard? Security and Privacy Vulnerability Analysis of Qi Wireless Charging

Yi Wu
University of Tennessee
Knoxville, TN, USA
ywu83@vols.utk.edu

Zhuohang Li
University of Tennessee
Knoxville, TN, USA
zli96@vols.utk.edu

Nicholas Van Nostrand
University of Tennessee
Knoxville, TN, USA
nvannost@vols.utk.edu

Jian Liu
University of Tennessee
Knoxville, TN, USA
jliu@utk.edu

ABSTRACT

With the ever-growing deployment of Qi wireless charging for mobile devices, the potential impact of its vulnerabilities is an increasing concern. In this paper, we conduct the first thorough study to explore its potential security and privacy vulnerabilities. Due to the open propagation property of electromagnetic signals as well as the non-encrypted Qi communication channel, we demonstrate that the Qi communication established between the charger (i.e., a charging pad) and the charging device (i.e., a smartphone) could be non-intrusively interfered with and eavesdropped. In particular, we build two types of attacks: 1) *Hijacking Attack*: through stealthily placing an ultra-thin adversarial coil on the wireless charger's surface, we show that an adversary is capable of hijacking the communication channel via injecting malicious Qi messages to further control the entire charging process as they desire; and 2) *Eavesdropping Attack*: by sticking an adversarial coil underneath the surface (e.g., a table) on which the charger is placed, the adversary can eavesdrop Qi messages and further infer the device's running activities while it is being charged. We validate these proof-of-concept attacks using multiple commodity smartphones and 14 commonly used calling and messaging apps. The results show that our designed hijacking attack can cause overcharging, undercharging, and paused charging, etc., potentially leading to more significant damage to the battery (e.g., overheating, reducing battery life, or explosion). In addition, the designed eavesdropping attack can achieve a high accuracy in detecting and identifying the running app activities (e.g., over 95.56% and 85.80% accuracy for calling apps and messaging apps, respectively). Our work brings to light a fundamental design vulnerability in the currently-deployed wireless charging architecture, which may put people's security and privacy at risk while wirelessly recharging their smartphones.

ACSAC '21, December 6–10, 2021, Virtual Event, USA

ACM ISBN 978-1-4503-8579-4/21/12…$15.00
https://doi.org/10.1145/3485832.3485839

CCS CONCEPTS

• **Security and privacy → Systems security**.

KEYWORDS

wireless charging, side-channel attack, Qi standard, vulnerability analysis

ACM Reference Format:
Yi Wu, Zhuohang Li, Nicholas Van Nostrand, and Jian Liu. 2021. Time to Rethink the Design of Qi Standard? Security and Privacy Vulnerability Analysis of Qi Wireless Charging. In *Annual Computer Security Applications Conference (ACSAC '21), December 6–10, 2021, Virtual Event, USA.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3485832.3485839

1 INTRODUCTION

Wireless charging is making inroads in the mobile and Internet of Things (IoT) industries as it offers the promise of increased mobility and freedom while charging devices. For instance, Qi-certified [44] wireless chargers for smartphones have become common in various locations around the home, workplace, hotels, airports, and coffee shops [4]. Plugless [34] offers wireless charging for many of the electrical vehicles on the road today. Medium Power Standard [6] supports wireless power delivery to portable tools (e.g., electric drills), robotic vacuum cleaners, drones, and e-bikes. In addition, many companies, such as Powermat [35] and WiTricity [46], provide wireless power solutions for medical implants and diagnostic instruments, etc.

With the ever-growing deployment of such wireless charging systems, it is essential to have a deep understanding of their vulnerabilities and the severity of the associated risks. In this paper, we dissect the fundamental vulnerabilities underlying Qi wireless charging standard [44] for mobile devices and reveal a set of severe threats which may put people's security and privacy at risk in practice. We believe such a vulnerability analysis can not only prioritize required mitigations in wireless charging for mobile devices but also shed light on the potential security and privacy issues of other wireless power transfer systems/standards which share many common technologies with Qi standard, such as the Ki Cordless Kitchen Standard [5] and the Medium Power Standard [6], etc.

Prior Research on Charging Attacks. Existing efforts have mainly focused on exploring the vulnerabilities of wired charging attacks. For instance, existing studies [23, 24, 28, 42, 50, 51] have shown that wired charging stations could expose users to serious

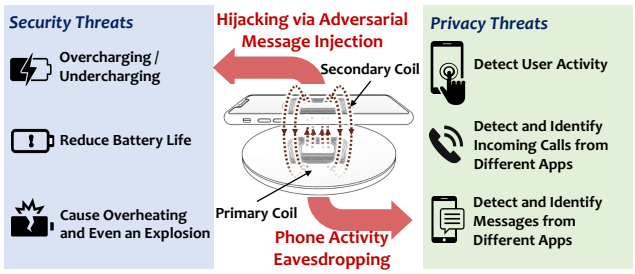


Figure 1: Illustration of the discovered privacy and security threats of Qi wireless charging.

privacy threats, ranging from deploying malware on the smartphones to inferring the browsing activity (i.e., which webpages are loaded) and exfiltrating privacy data (e.g., IMEI, contacts' phone number, and chatting records). As for wireless charging systems, although a survey paper [27] briefly mentioned the possibility of eavesdropping attacks (e.g., stealing the identity of the charging device) and man-in-the-middle attacks (e.g., a malicious device manipulates charging status), only initial thoughts have been provided, with no further discussion or technical solutions proposed. A recent study QID [49] showed the possibility of identifying different Qi-compliant smartphones while being wirelessly charged. However, this work only focused on the device identification while ignoring other potential vulnerabilities in Qi wireless charging systems. Moreover, denial-of-charging attacks (a.k.a, jamming attacks) have been proposed against a variety of wireless rechargeable sensor networks [25, 32, 33]. However, none of these attacks considered Qi protocol for mobile devices. To the best of our knowledge, there has yet to be research focusing on exploring the feasibility of a more severe attack where the adversary could interfere with and even take over the charging process.

Qi and its Possible Vulnerabilities. Qi, developed by Wireless Power Consortium (WPC), is the leading wireless charging standard for providing 5-15 watts of wireless power transfer to portable mobile devices [44]. As illustrated in Figure 1, the charger (e.g., a charging pad) and the charging device (e.g., a smartphone) have primary and secondary coils, respectively. During the power transfer phase, the primary coil generates an electromagnetic field that induces a current in the secondary coil to transfer energy. In addition, to allow the charging device to take control of the charging procedure, Qi specifies interoperable wireless power transfer and data communication between the charger and the charging device. The charger thus is able to adjust the transmit power density as requested by the charging device. However, there exists two fundamental vulnerabilities: *(1)* No encryption scheme has been used to secure the data communication channel, making the transmitted data (a.k.a., Qi messages) more susceptible to being interfered with or eavesdropped; and *(2)* The requested power transfer density of the charging device is highly correlated with the device's activities (e.g., receiving messages while being charged). This opens opportunities for the adversary to detect and identify the charging device's activities using the eavesdropped Qi messages as well as the inductive voltage of the charger. We describe how the adversary can leverage these vulnerabilities to launch attacks in the perspectives of security and privacy threats as follows:

Security Threats. Due to the open propagation property of electromagnetic signals, using the magnetic field to deliver Qi messages has fundamental vulnerabilities. From a security perspective, we show the potential of hijacking the communication channel by stealthily placing an adversarial coil between the charger and the charging device. Through a well-crafted alternating current acting on the adversarial coil, the adversary can inject arbitrary malicious Qi messages so as to take control of the entire charging process, such as starting/terminating charging, manipulating the amount of power being transferred per charging cycle, etc. As a consequence, the adversary can cause overcharging, undercharging, pause charging, which may reduce charging efficiency, battery life and cause overheating and even an explosion.

Privacy Threats. The Qi wireless charger needs to adjust its transmit power density to meet the charging device's requested amount according to the received Qi messages (more details are in Section 2). As all the Qi messages are transmitted via amplitude modulation (AM) in a non-encrypted form, we show that they can be easily eavesdropped by measuring the induced voltage on a nearby hidden adversarial coil (e.g., stuck underneath the surface on which the charger is placed). More importantly, *Control Error* messages (introduced in Section 2.2) indicate the difference between the actual transmit power density and the device's requested one, which would lead to lots of fluctuations while the charging device changes its status or is triggered by an activity such as turning on/off the screen, receiving an incoming phone call or a pop-up notification from an app. This is because when an activity is triggered while charging, the battery will charge at a slower rate than inactive to allow enough power for the ongoing usage [38]. As different activities associated with different apps rely on distinct sets of hardware modules, we experimentally demonstrate that they do induce *identifiable* power-consumption patterns which are reflected on the transmitted Qi messages and the inductive voltage sensed by the adversarial coil. Leveraging this side-channel, the adversary can demodulate Qi messages and identify whether the charging device receives a message notification, a phone call, or the screen is manually turned on by the user. Additionally, the adversary can further identify the specific apps (e.g., WhatsApp, Viber, and Twitter) triggering the activities.

Our main contributions are summarized as follows:

- To the best of our knowledge, we conduct the first thorough vulnerability assessment of Qi wireless charging to identify common malicious threats and the associated risks, which we believe is an essential step to prioritize required mitigations.
- Relying on a hidden adversarial coil stuck on the charger's surface, our validation experiments demonstrate that the adversary can completely take control of the charging process through injecting deliberately manipulated Qi messages in the communication channel, which may lead to more severe consequences (e.g., terminate the charging process, reduce battery life, overheating, or even an explosion).
- Due to the non-encryption characteristic of the communication channel, we show that the Qi messages can be non-intrusively snooped by simply sticking an adversarial coil underneath the surface on which the charger is placed. These messages carry a variety of sensitive information, such as device ID, charging state,

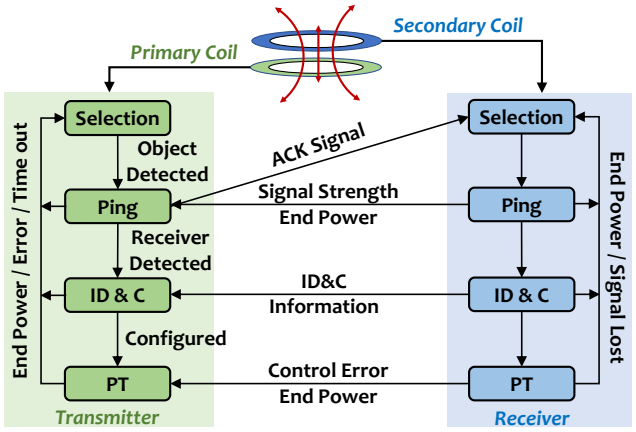


Figure 2: Overview of Qi wireless charging protocol.

and control error information, which highly correlates with the charging device's activities.

- Relying on the inductive voltage of the adversarial coil and its derived Qi messages, we validate these proof-of-concept attacks using multiple commodity smartphones. The results demonstrate that we can detect and identify phone calls from 4 most commonly used calling apps and phone notification messages from 10 messaging apps with high accuracies of over 95.56% and 85.80% accuracy, respectively.
- We analyze and evaluate several defense mechanisms including frequency-based hijacking signal detection and chaotic noise addition that can mitigate the effects of the proposed attacks. A few more potential directions about defense are also discussed.

2 BACKGROUND

2.1 Qi Wireless Charging

Generally, the charging process involves two main components: a power transmitter (e.g., a charging pad) and a compatible power receiver (e.g., a smartphone). Relying on the oscillating electromagnetic field, the power can be transferred wirelessly between the two coils (i.e., *primary coil* and *secondary coil*) embedded in the power transmitter and receiver, respectively. Specifically, an alternating current in the primary coil produces an oscillating magnetic field which in turn induces an alternating current in the secondary coil in close proximity. By attaching a load (e.g., a battery) to the secondary coil, the induced alternating current can be used for charging purposes.

To enable interoperable and efficient wireless power transfer, Qi allows the power receiver to be in control of the charging procedure. The Qi-compliant transmitter is capable of communicating with the receiver and adjusting its transmit power density as requested by the receiver. A systematic overview of Qi wireless charging protocol is illustrated in Figure 2. Specifically, it has four different phases as follows:

Selection. The transmitter continuously monitors its surface for the presence of any object. If the presence of an object is detected, the transmitter will move to the *Ping* phase and also send out an acknowledgment (ACK) signal to inform the receiver to move to the next phase.

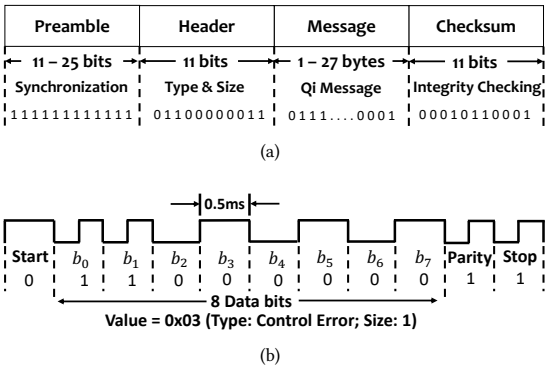


Figure 3: Illustration of the Qi communication packet: (a) the format of the Qi communication packet; and (b) an example of the *control error* packet's *Header*.

Ping. The transmitter determines whether the detected receiver is in need of power. If the receiver has a need for power, the receiver will send a *Signal Strength* packet which indicates the strength of the signal (i.e., how well the two coils are coupled) to the transmitter.

ID & C. The receiver sends the ID & C packets which carry its specific manufacturer, model, and configuration information to the transmitter. If the transmitter agrees to transfer power to the receiver, the Power Transfer (PT) phase would be reached.

PT. In order to decrease the internal power consumption and reach the best operating conditions in terms of power transfer efficiency, Qi makes the receiver take control of the system [44]. Specifically, the receiver needs to send *Control Error* messages, which indicate the difference between the requested operating point (e.g., load voltage) and the actual one to the transmitter. After receiving the control error message, the transmitter would adjust the primary coil's alternating current, thereby making the transmit power density match the receiver's need and satisfying its battery management's requirements.

2.2 Qi Message

In the Qi standard, all the communication packets (e.g., identification, configuration, and control error) transmitted between the transmitter and the receiver are in a non-encrypted form and are generated by means of load modulation. Specifically, the receiver changes its load through switching a capacitor between the secondary coil and (full bridge) rectifier, which would induce changes in the primary coil's alternating current.

The format of Qi communication packets is shown in Figure 3(a). It contains a *Preamble* for synchronization, a *Header* which indicates the type and size of the packet, a *Message* which contains the Qi message, and a *Checksum* that aims to check the integrity of the packet. Save for the *Preamble* consisting of 11-25 all ONE bits, the other three fields use an 11-bit asynchronous serial format. They all begin with a *Start* bit set to ZERO and end with a *Stop* bit set to ONE. Eight data bits (LSB first) and a *Parity* bit are followed by the *Start* bit, which are used to carry the data and check the data's integrity, respectively. If there is an even number of ONE bits in the data bits, the *Parity* bit will be set to ONE, otherwise it will be set to ZERO. These bits are bi-phase encoded and have a period of $0.5ms$. An example of the control error packet's *Header*

is shown in Figure 3(b)[1], with the messages being transmitted using AM modulation by switching a resistive dummy load on the power receiver side. The carrier voltage signal of AM modulation is operated at around 125 kHz.

Among all types of Qi messages, the *control error* message is the most critical for adaptively controlling power transfer. The transmitter uses the received *control error* value C^i in the i^{th} *control error* packet to adjust its primary coil's alternating current: $I^i = I^{i-1} \cdot (1 + C^i/128)$, where I^i is the new primary coil current, and I^{i-1} is the previous primary coil current constrained by both I^{i-2} and C^{i-1}.

2.3 Electromagnetic Induction

Based on electromagnetic induction, a wireless charging system can be represented using Maxwell Equations (differential form):

$$\nabla \cdot D = \rho_f, \quad (1a) \qquad \nabla \cdot B = 0, \quad (1b)$$

$$\nabla \times E = -\frac{\partial B}{\partial t}, \quad (1c) \qquad \nabla \times B = \mu_0 J + \mu_o \epsilon_0 \frac{\partial E}{\partial t}, \quad (1d)$$

where D is the electric displacement field, E is the electric field ($E = \frac{D}{\epsilon_0}$), B is the magnetic field, ρ_f is the electric charge density, μ_0 is the magnetic permeability, ϵ_0 is the electric permittivity, and J is the charging current density. Since Qi messages are transmitted via AM modulation, a change on the primary coil voltage will influence ρ_f and thereby further change the electric field strength. According to Equation 1d, a changing electric field will also generate an induced magnetic field and further produce induced voltage on a nearby coil. Since ZERO and ONE in Qi messages are transmitted using differential coding (as shown in Figure 3 (b)), they would exhibit different patterns on the induced voltage on the adversarial coil. On the other side, adding an external magnetic field to the charging system will change the strength of its magnet field and further influence the electric field, according to Equation 1c. The primary coil voltage of the charger would thus be affected, thereby interfering with or even fully controlling the Qi message transmission channel.

3 THREAT MODEL

3.1 Possible Attack Scenarios

Due to the open propagation properties of oscillating magnetic signals, Qi wireless charging gives attackers various opportunities to inject adversarial magnetic signals on the power transmitter to hijack the communication channel and further alter the power transfer. Moreover, the current design of the Qi wireless charging does not provide any encryption or authentication mechanisms to protect the transmitted Qi messages, which in turn can be easily snooped by the adversary. It thus incurs potential privacy concerns of monitoring smartphone activity while being charged. Given these fundamental vulnerabilities, we consider the following two attack scenarios:

(1) Hijacking Attack: In this scenario, the adversary can hijack the Qi communication channel by injecting adversarial magnetic signals using a disguised adversarial coil to alter the power transfer as desired. Through modulating the alternating current flowing through the adversarial coil, the coil can produce well-crafted magnetic signals to perturb the electromagnetic field between the power transmitter and receiver, which serves as the medium for power transfer and the Qi message transmission. In consequence, the adversary can reduce the power transfer efficiency (e.g., increasing charging time) or directly terminate the charging process. One step further, the adversary can even take control of the power transmission, such as intentionally manipulating the values of Qi messages, making the transmitter transmit any amount of power they want. This charging process may cause significant damage to the battery (e.g., overheating, reducing battery life, or even an explosion). It's important to note that an adversary may be capable of directly adding power to the receiver via coupling energy in an analog manner leveraging the adversarial coil. However, the charging system may become much more unstable in the presence of two "power transmitters", making the receiver reverse back to the selection phase and end up power transfer. We leave this scenario as our future work.

(2) Eavesdropping Attack: In this scenario, the adversary can non-intrusively and passively derive Qi messages using a nearby hidden adversarial coil (e.g., stuck underneath the table) and further infer the activities of the power receiver (e.g., a smartphone) while being charged. Due to the sudden increase in the power consumption associated with phone notifications (e.g., receiving a SMS message, or receiving an incoming phone call), the gap between the desired and actual operating point during the power transfer (PT) phase would have to be changed accordingly. Through capturing the values of the control error messages, the adversary can detect the exact time when the smartphone receives these notifications. More importantly, different types of notifications (e.g., receiving a SMS message, receiving an incoming phone call, and turning on the screen by the user himself) or even the same type of notifications from different apps would have a unique impact on the power transfer control as they all rely on different set of hardware modules (e.g., vibration motor, screen on/off, WiFi module, cellular module, and sensor module). Therefore, when a notification is received, different apps would show a discriminative power consumption pattern and have distinguishable reflections on the biasing of the operating point, further leading to different control error messages and primary coil voltage patterns. Additionally, by deriving Qi *ID & C* messages carried on the inductive coil voltage, the adversary can obtain the basic device identifier, which can be further used to identify users. The potential security & privacy threats we discovered are summarized in Table 1.

3.2 Assumptions & Adversary's Capability

Given a charging pad that the victim might use in a coffee shop, hotel, airport, library, commercial office, or home, we assume the adversary should have the following capabilities as per each attack scenario:

(1) Hijacking Attack: In this scenario, the adversary is assumed to be able to stealthily place an adversarial coil between the charging pad and the charging device. For instance, the add-on adversarial coil could be stuck on the surface of the charger and made to resemble a lookalike sticker, such as the one shown in Figure 4(a) which looks like an ultra-thin film (i.e., 0.7 mm thickness) and can be attached on the charging pad's surface without drawing suspicion.

[1]The data bits (LSB first) *0x03* indicates the packet type is *control error*, and the message size can be calculated as $1 + (Header - 0)/32$=1 [7].

Table 1: Potential security and privacy threats of Qi wireless charging.

Attack Scenario	Information/Action Needed	Security&Privacy Threats
Hijacking attack	Inject adversarial magnetic signals	Start/stop charging
		Manipulate the amount of power being transferred (e.g., overcharging/undercharging)
		Reduce charging efficiency, cause overheating and battery damage
Eavesdropping attack	Inductive voltage on a nearby hidden coil	Recognize basic device identifier and manufacturer ID
		Detect & identify the basic phone activities (e.g., Phone is unlocked and the screen is on)
		Detect & identify the category of incoming notifications (e.g., phone calls or messages)
		Identify the specific app triggering the notification (e.g., WhatsApp, and Messenger)

(a) Stealthily sticking an ultra-thin adversarial coil on the surface of the charger

(b) Hiding the adversarial coil underneath the surface

Figure 4: Examples of Possible attack scenarios: (a) [Hijacking] sticking an ultra-thin adversarial coil to the charger's surface; and (b) [Eavesdropping] sticking the adversarial coil underneath the surface on which the charging device is placed.

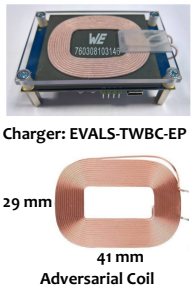
In practice, the adversary can make the color of the sticker closer to the charger's color to make it even more unnoticeable. The voltage of the controlled adversarial coil can be provided by a signal generation back end, which could be concealed in an instrumented power outlet.

(2) Eavesdropping Attack: In this scenario, as the adversary only needs to passively receive the magnetic signals, he/she can place the ultra-thin adversary coil farther away, such as hiding the coil underneath the surface on which the charging pad is placed, as shown in Figure 4 (b). The coil also requires a logging back end to capture the inductive voltage. We used a 312 kHz sample rate with 8-bit samples in this work, showing a reasonable throughput of 2.5 Mbps for logging via a modern cellular network, WiFi, or a local SD card.

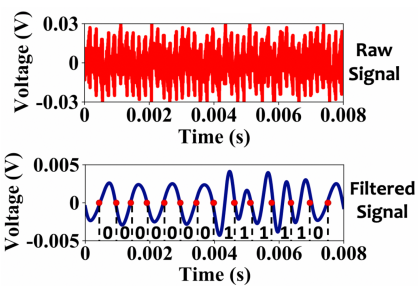
For both attack scenarios, the adversary is not required to get physical access to the charger. In other words, the adversary does not need to disassemble the charger or modify the internal circuit board. We believe that these non-intrusive attacks are under very practical threat models and can be surreptitiously and easily launched in practice.

4 SNOOPING QI MESSAGE THROUGH A NEARBY HIDDEN ADVERSARIAL COIL

In this section, we describe how an adversary can snoop Qi messages through a nearby hidden adversarial coil. Specifically, once the adversary gets access to the inductive voltage of the adversarial coil, the time-series voltage readings need to be fed into the following components to derive Qi message data bits: *Voltage Denoising & Filtering*, *Packet Detection & Segmentation*, and *Data Bits Demodulation*.



(a) EVALSTWBC-EP charging board [31] and the adversarial coil



(b) Signal denoising & filtering

Figure 5: Illustration of signal collection and filtering using an EVALSTWBC-EP evaluation board.

4.1 Voltage Denoising & Filtering

In order to isolate Qi-message-relevant signals from the adversarial coil voltage, we apply a moving-average filter and a low-pass filter to smooth the signal and eliminate irrelevant frequency components, respectively. Figure 5 shows a segment of the measured adversarial coil voltage (raw signal) and the corresponding denoising and filtering processing (filtered signal) in our *eavesdropping attack* scenario. In the experiment, the wireless charger (i.e., EVALSTWBC-EP provided by STMicroelectronics [31]) is placed on a wooden table which has a thickness of 3.2 cm. To snoop Qi messages, a tiny and ultra-thin adversarial coil (Figure 5(a)) is stuck underneath the table, and the horizontal distance between the charger and the coil is around 2 cm. A logging backend (e.g., a digital oscilloscope) is connected to the adversarial coil for measuring inductive voltage.

To extract the modulated data bits, we first apply a *moving-average filter* which only keeps the average value within a sliding window. We set the window length as $\lceil f_s/f_c \rceil$, where f_s and f_c are the sampling rate of our logging backend (i.e., 312 kHz) and the measured carrier frequency (around 4 kHz), respectively. We then apply a *third-order low-pass Butterworth filter* with a cut-off frequency at 2 kHz (modulation frequency) to further eliminate irrelevant frequency components, . After filtering, only the packet segments carrying the data bits are preserved. Figure 5(b) illustrates a fragment of the raw signal and the filtered signal in a packet segment for visualization purposes. Qi message data can then be detected and decoded according to the modulating frequency (i.e., ZERO is 1kHz, ONE is 2kHz).

4.2 Packet Detection & Segmentation

After filtering, the carrier signal can be filtered out and the signal that does not contain Qi packets would approximately become a

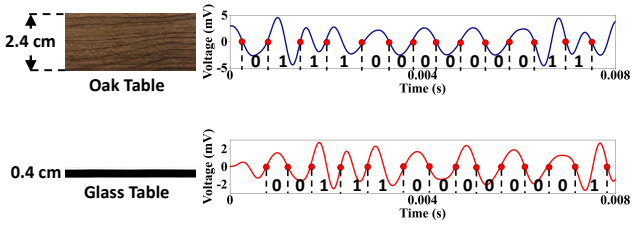
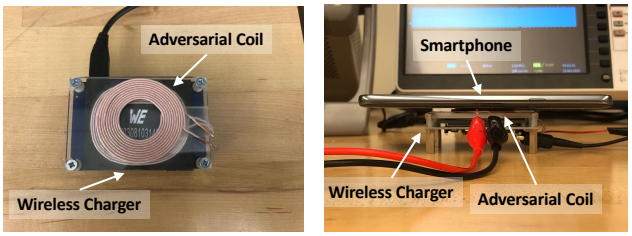


Figure 6: Filtered waveform on different tables.



(a) Experimental setup (b) Side view

Figure 7: Experimental setup for hijacking attack: the adversarial coil is stuck on the charger surface.

constant DC wave. To detect and separate each Qi packet segment, we apply a sliding window on the filtered signal and calculate the variance of each sliding window centered at time t, which is represented as $winVar(t)$. The length of the sliding window is set to $\lceil f_s/2000 \rceil$ to ensure the difference is sufficiently distinct. Therefore, by setting a threshold τ, we can easily determine whether t is in a packet segment or not. As the duration of a single packet transmission (i.e.,~30 ms) is significantly shorter than the gap between two adjacent packets (i.e.,~150 ms), we can detect the start time t_s and end time t_e of each segment by solving the following objective function:

$$\begin{aligned} &\arg\max_{t_s,t_e} t_e - t_s, \\ &s.t., winVar(t_s), winVar(t_e) > \tau, t_p < t_e - t_s < t_g, \end{aligned} \tag{2}$$

where t_p is the minimum length of a Qi packet (i.e., 22 ms as shown in Figure 3)[2], and t_g represents the maximum length of a Qi packet which is empirically set to 70 ms to detect and segment *ID & C* packets containing relatively more data bits than *Control Error* packets. The *argmax* function is used to ensure the completeness of a single packet segment.

4.3 Data Bits Demodulation

As illustrated in Figure 5(b), ZERO bits and ONE bits in a message segment can be identified leveraging their different modulating frequency. In order to derive the bi-phase encoded data bits, we further leverage the zero-crossing points in the filtered signal to decode the bi-phase bits. To detect these zero-crossing points, we first calculate the mean value m and the max value M of all the digital samples in the packet segment and then find out all the digital samples that are within a distance $\zeta = \frac{M}{100}$ to m. Given that each bi-phase bit has a period of 0.5 ms according to the Qi standard [44], the possible distance between two adjacent zero-crossing points should be 0.25 ms or 0.5 ms. We thus adopt a minimum acceptable

[2]A packet contains at least 44 data bits, which takes 22 ms [7].

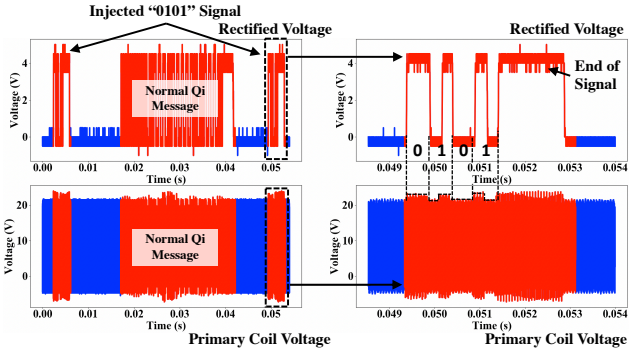


Figure 8: Illustration of injecting a "0101" signal.

interval $\sigma = 0.2$ ms to remove the detected zero-crossing points that are too close to each other.

After detecting all the zero-crossing points on the filtered coil voltage signal, we can follow the bi-phase decoding mechanism to derive the bi-phase data bits according to the distance between two adjacent points. Specifically, as shown in Figure 5(b), two zero-crossing points with a 0.5 ms distance ($1T$) indicates a ZERO bit, while three zero-crossing points with a 0.25 ms distance ($0.5T$) between each adjacent pair represents a ONE bit. Following this rule, the data bits sequence could be obtained. In the practical implementation, we increase the distance threshold to $1.5T$ and $0.75T$ respectively, in case of the inevitable biases and time delay caused by the manufacturing imperfection.

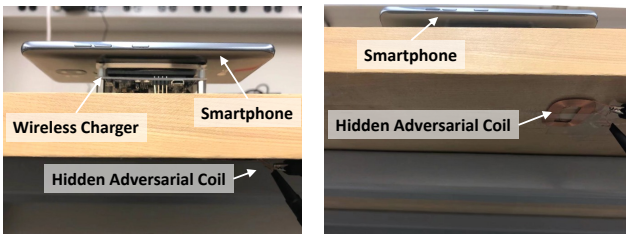
We further conduct the same type of experiment on two other tables with different materials & thickness to demonstrate the generalizability of the attack. The results are shown in Figure 6. We can observe similar patterns from an oak table which has a thickness of 2.4 cm and a glass table which has a thickness of 0.4 cm. This demonstrated that our attack can be extended to various surfaces with different materials & thickness.

5 VALIDATION OF ADVERSARY'S CAPABILITIES

5.1 Hijacking via Adversarial Message Injection

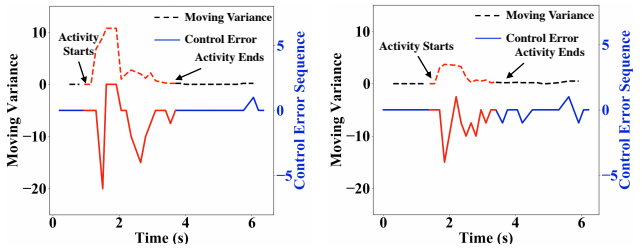
To verify whether the adversary is capable of injecting manipulated Qi messages by using an adversarial coil and further hijack the charging process, we conduct an experiment where the adversarial coil is stuck on the surface of the wireless charger (i.e., EVALSTWBC-EP board [31]) while a smartphone (i.e., LG G7) is being charged, as shown in Figure 7. We use a Keysight 33522B waveform generator to produce the well-crafted alternating signal on the adversarial coil while the oscilloscope is used to monitor the charging process.

In order to communicate with the wireless charger, Qi requires the perceived AM modulated signal to change significantly in the primary coil voltage (i.e., > 200 mV) of the charger [44]. To verify the adversary's capability, we add a 80 kHz sinusoidal wave with a 20 V peak-to-peak voltage on the adversarial coil, and we observe that the primary coil voltage is increased up to 3 V, which is much greater than 200 mV. By switching off the signal, the primary coil voltage returns to its original level. Thus, to inject manipulated Qi



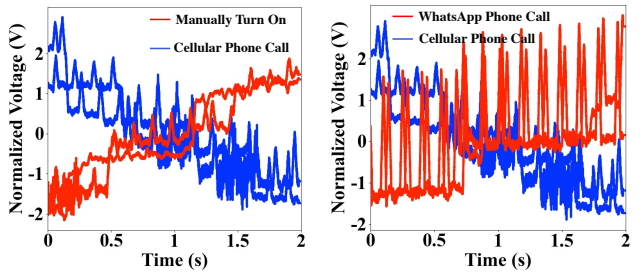
(a) Experimental setup (b) Upward view

Figure 9: Experimental setup for eavesdropping attack: the adversarial coil is stuck underneath the table.



(a) Receiving a SMS msg. (b) Receiving a Wechat msg.

Figure 10: Examples of the control error sequences with different activities.



(a) Manually turn on. vs. cellular phone call (b) Cellular phone call. vs. WhatsApp phone call

Figure 11: Normalized moving abs-mean voltage of the captured adversarial coil among different activities & apps.

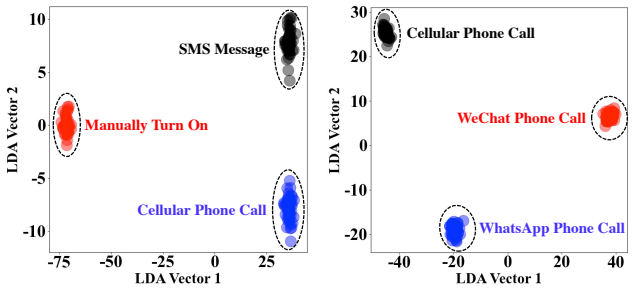
messages, the adversary can follow the bi-phase encoding mechanism to regulate the voltage of the adversarial coil (i.e., switching between LOW and HIGH states): When the signal is added on the adversarial coil, it's a LOW to HIGH switch, while it's a HIGH to LOW switch when it's removed from the adversarial coil. Figure 8 shows the primary coil voltage and rectified voltage when we inject "0101" signals in intervals into the normal Qi messages. Note that the rectified voltage is measured using the test point provided by the wireless charger board, which can better visualize pre-demodulated Qi messages to verify whether the signal is successfully injected. We can observe the bi-phase encoded "0101" signal (the following High voltage represents the end of the injected bit sequence that was intentionally added by us) from the rectified coil voltage clearly, which confirms our hypothesis that the adversary can inject any malicious communication packets to control the charging process by just using a tiny adversarial coil.

5.2 Eavesdropping via Inductive Voltage

Our attack is built on the hypothesis that the inductive voltage of a nearby hidden adversarial coil and its derived Qi *Control Error* messages carry rich information of the phone activities while being charged. This is because when an activity is triggered while charging, the battery will charge at a slower rate than inactive to allow enough power for the ongoing usage [38]. As a consequence, the charging device will adjust its desired operating point and further transmit corresponding *Control Error* messages to the charger to adjust the transmit power density. Different activities usually rely on different sets of hardware modules, thus they have different initial power consumptions while being triggered. This would cause the charging device to skew from the operating point at different scales, leading to an *identifiable* pattern on the control error sequences as well as the inductive voltage. We experimentally validate our hypothesis by addressing the following questions: *(1)* Does the occurrence of an activity have an impact on the control error sequence & the nearby hidden coil's inductive voltage? *(2)* Do different kinds of activities (i.e., receiving a phone call, a notification message, and manually turning on the screen by the user) generate unique patterns on the control error values and the inductive voltage? *(3)* For the same kind of activity, do different apps (e.g., receiving a SMS message or a WeChat message) still have distinguishable patterns?

The experimental setup is shown in Figure 9. Specifically, we use the EVALSTWBC-EP board [31] (Figure 5(a)) and a smartphone (i.e., LG G7) as the wireless charger and charging device, respectively. The adversarial coil is hidden underneath the surface on which the charger is placed. The coil is connected to the probe of a Tektronix TBS2102 digital oscilloscope, which serves as the data logging backend. The surface is a wooden table which has a thickness of 3.2 cm. Figure 10 shows the extracted control error sequences and its moving variance when the smartphone receives a SMS message and a WeChat message respectively, while being charged. As these activities trigger various actions on the smartphone (e.g., turning on the screen, popping up a notification, and running necessary background services), we observe that the values of the control error messages, which are for power density adjustment, change greatly while the moving variance is approximately zero when there is no activity. In addition, we find that the received control error sequence exhibits different patterns of these two activities, which confirms that control error messages carry information that can be used to distinguish different phone activities. To further verify the distinguishability of the inductive voltage on the adversarial coil during phone activities, we measure the inductive voltage while the smartphone receives a cellular phone call, a WhatsApp phone call, and is unlocked manually (twice for each activity) as shown in Figure 11. To better visualize the voltage pattern, we perform Z-score normalization [22] on the measured voltage. We can see the voltage curves of the same activity have a very similar pattern, while the curves of different activities exhibit distinguishable patterns.

To further confirm our hypothesis, we collect the inductive voltage on the adversarial coil and the decoded control error sequences when the smartphone (i.e., LG G7) is triggered by *(1) three types of activities*: receiving a cellular phone call, a SMS message, and manually turning on the screen (50 times for each activity); and



(a) Three types of activities (b) Three types of *phone calls*

Figure 12: Illustration of the extracted features of inductive coil voltage and control error sequence to distinguish different activities.

(2) three apps of the same activity (i.e., receiving phone calls): cellular phone call, WeChat phone call, and WhatsApp phone call (50 times for each activity). We then extract 14 time-domain features (i.e., length, minium, maximum, median, variance, std, abs-mean, cv, skewness, kurtosis, first quartiles, second quartiles, third quartiles, inter quartile-range) from both the voltage signal and the decoded control error sequence on each activity segment (using the segmentation method introduced in Section 7.1). We also calculate the FFT of the voltage signal for each segment and divide the frequency range into 100 equal-size frequency bins. The average amplitude in each bin is used, resulting in a total of 100 frequency-domain features. We apply linear discriminant analysis (LDA) [12] for dimensionality reduction and plot the extracted features in a 2-dimensional domain as shown in Figure 12. We observe that different activities and apps can be easily distinguished and the collected samples of each activity are densely clustered. These findings have addressed the three questions we raised and validate the hypothesis of our proposed attacks.

6 ATTACK DESIGN AND EVALUATION: HIJACKING VIA ADVERSARIAL MESSAGE INJECTION

6.1 Malicious Qi Packet Generation

As described in Section 5.1, through the stealthy placement of an adversarial coil, the adversary is capable of injecting manipulated Qi messages. To achieve this, we generate the following two types of Qi messages: *(1) End Power Transfer (EPT) Packet*: After the EPT packet has been received, the charger will terminate the power transfer immediately. To be specific, the EPT packet has a header value of 2, and the data in the message byte indicates the reason for the power transfer end (e.g., overheating, logic error, battery failure). *(2) Control Error Packet*: The control error packet carries the information about the difference between the charging device's desired transmit power density and the actual density. This is used by the charger to adaptively control its power transfer. The adversary thus can manipulate the values of control error messages to control the power transfer. A positive control error value indicates that an increase in transmit power density will be triggered and vice versa. By controlling the power transfer, the adversary can cause overcharging or undercharging, leading to a reduction in charging efficiency and significant damage to the battery (e.g., overheating, reducing battery life, or even an explosion).

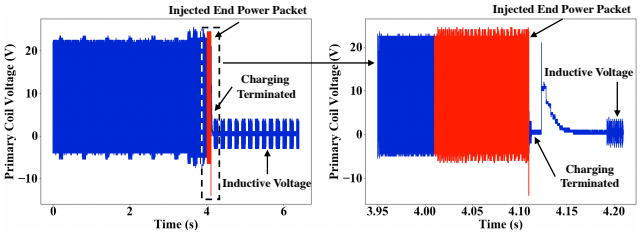


Figure 13: Terminate charging process via injecting end power transfer packets.

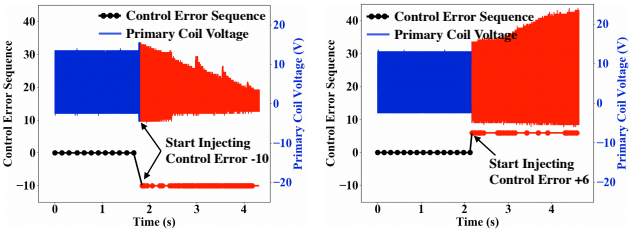
6.2 Experimental Methodology

The experimental setup is similar to the setup shown in Figure 7. An ultra thin adversarial coil (i.e., 0.7 mm) [10] is placed between the charger and the charging device (i.e., a smartphone), with the alternating signal being generated by a wave generator. We validate our attack under three scenarios in order to terminate the charging process, reduce charging efficiency and transfer excess power (causing overheating, battery life reduction, or even an explosion). The experiments are conducted using 5 different commodity smartphones (i.e., Samsung Galaxy Note 5, Samsung Galaxy S7, LG G7, Google Pixel 3, and iPhone 8) and two chargers (i.e., an EVALSTWBC-EP board [31] and a commercial Yootech charger [2], which has more than 106,034 customer ratings on Amazon by May, 2021). Our attack has been successful on attacking all these devices. To illustrate the attack's success, we use the experiment with an EVALSTWBC-EP charger [31] due to its convenience for monitoring the charging process and a Samsung Galaxy Note 5 as an example in the rest of this section.

6.3 Attack Effectiveness

Charging Process Termination. In order to terminate the charging process, the adversary can modulate an EPT packet in the communication channel with an arbitrary value in the message byte. In our experiment, we set the value to 3, which indicates the charging device is overheating (but actually not). As shown in Figure 13, as soon as the malicious EPT packet is injected, the charging process is terminated instantly (i.e., in 0.05 seconds). If an end power event occurs, both the power transmitter and the receiver will move back to the *selection* phase, trying to restart the power transfer again. Therefore, in order to stop the charging process permanently, the adversary has to continuously (repeatedly) inject EPT packets, in turn generating an inductive voltage on the primary coil, as shown in Figure 13, and disturbing the ACK signal sent to the power receiver to make the charging process unable to restart. Our experiment validates the effectiveness of this type of attack, which can make wireless chargers stop working and cause great inconvenience to their users. Additionally, although we show the feasibility of such denial-of-service (DOS) attack in Qi wireless charging, we believe this threat could be extended to other wireless-charging-enabled devices as well, making the device incapable of operating, such as an EV failing to start, or cause a wireless cardiac pacemaker to stop working.

Charging Efficiency Reduction. To reduce charging efficiency, the adversary can flood a bunch of manipulated *control error packets*



(a) Charging efficiency reduction (b) Excess power transfer

Figure 14: Injecting malicious Qi control error messages to take control of the wireless charging.

with a negative value in the communication channel. Since these fake packets will cause an unexpected primary coil voltage, the receiver will try to make the voltage back to normal via sending legitimate control error messages. To prevent the charging system from completing self-calibration and to take full control of the charging process, we inject the malicious Qi messages at a nearly maximum frequency (i.e., approximately 40 packets per second, as each packet lasts for around 25 ms), which is much higher than legitimate Qi communication (i.e., 6-7 messages per second). This ensures each legitimate Qi packet may have an overlap with our injected packets, which can break the integrity of the legitimate Qi packets so as to make them lose effectiveness.

Figure 14(a) shows the experimental result of injecting a set of control error packets with a value of -10 in the communication channel. We can clearly observe that, during the normal power transfer phase (before injecting malicious Qi packets), the primary coil voltage is maintained at a very stable stage with all the control errors equal to 0. However, after we start injecting malicious packets, the demodulated control errors become −10 and the primary coil voltage starts to linearly decrease and is reduced to only half of its original amplitude within 2 seconds. Some of the peaks during the decrease are caused by the alternating signal of the adversarial coil, as the signal itself also has an impact on the amplitude, but it won't influence the overall trend. This example validates the effectiveness of the injected malicious Qi messages, significantly reducing the charging efficiency. In other words, the adversary can control the charger and transmit any amount of power they want, such as transmitting a very low amount of power per cycle. Outside of increasing the amount of time it takes to charge a device, existing studies [15, 17] demonstrate that undercharging can damage the chemical properties of the battery and shorten the life of battery cells.

Excess Power Transfer. To transfer excess power, we periodically inject malicious control error packets with a positive value in the communication channel. Similarly, we inject these malicious packets at a high frequency (i.e., approximately 40 packets per second). For safety concerns, we set the value of the control error messages to a relatively small number (i.e., 6). With a larger value of the control error messages, the transmit power density will increase more quickly. As shown in Figure 14(b), after the malicious control errors 6 starts being injected, the primary coil begins increasing and can nearly reach twice its original peak-to-peak voltage within 2 seconds with all of the demodulated control errors from the charger are equal to 6. In the normal operation of Qi wireless charging, the charging device will send an EPT packet to the charger to request "stop charging" if it is overheating, however such a packet will be dropped under this attack due to the collision with the continuously injected malicious control error packets. During the experiment, we could obviously feel the excessive heat of the smartphone and even heard an electric hum when the primary voltage was increased to 25 V. Due to safety concerns, each round of experiments was only performed for a short time, yet we successfully demonstrated the attack's potential to make the charger transfer excess power through the manipulated Control Error packets. Existing studies have empirically demonstrated the serious consequences in more safety-controlled lab environments when the battery undergoes overcharging. For instance, when a lithium-ion battery keeps being overcharged, thermal runaway would ensue, inducing the battery to vent with smoke, fire, or an explosion [8, 11, 13, 20]. All these results show that this type of attack poses a very serious threat to public safety, and we believe that the potential threat may be more serious in other wireless charging systems, such as medical implants, electrical vehicles, etc.

7 ATTACK DESIGN AND EVALUATION: EAVESDROPPING VIA INDUCTIVE COIL VOLTAGE

7.1 Activity Detection & Segmentation

As mentioned in Section 5.2, when an activity is triggered on the phone, the values of the transmitted control error messages will be changed accordingly. To detect and segment the initialized control error pattern associated with each activity, we first apply a sliding window on the control error sequence and calculate the variance of each window. The window length is set to 5 as the receiving rate of Qi messages is approximately 6-7 packets per second. Similar to Equation 2, we detect the start time and end time of each segment using two pre-defined thresholds (i.e., minimum and maximum segment lengths). We empirically set these two thresholds to 1 second and 4 seconds, which can filter out most of the unexpected instantaneous fluctuations on the control error when there is no activity occurred. Moreover, after a period of inactivity, the screen of the smartphone will automatically turn off, which also leads to some fluctuations on the control error. However, compared with the segment when an activity is triggered, the sum of control error values is always a negative value, while we find that the segment associated with the screen turned off is a positive value. We therefore restrict that the sum of all the control error values in an activity segment has to be a negative value.

7.2 Activity Classification

Time-frequency Feature Extraction. Once we have obtained each activity segment, we need to extract its representative feature set. To be specific, we use time-frequency domain features consisting of 14 statistical time-domain features (i.e., length, minium, maximum, median, variance, std, abs-mean, cv, skewness, kurtosis, first quartiles, second quartiles, third quartiles, inter quartile-range) extracted from both the control error sequence and the adversarial coil voltage. Frequency domain features are calculated using the Fast Fourier Transform (FFT) on the adversarial coil voltage of each segment. We divide the frequency range into 100 equal-size

frequency bins and use the average amplitudes in each bin as frequency domain features. Therefore, we can obtain a total of 128 time-frequency features for each activity segment.

Feature Selection & Classification. To identify each activity, we apply a hierarchical classification scheme. Specifically, we first perform *activity category classification* to identify the type of the activity (i.e., calling, messaging, or the screen turned on by the user manually). Then we conduct *app classification* to identify the specific involved app if it's a calling or messaging activity. To minimize the adversary's attacking efforts and make our work developable/exploitable in the real world, we use a standard classifier to differentiate these activities. We have tried Linear Discriminant Analysis (LDA), Random Forest, Support Vector Machine (SVM), and a 2-dense-layer Deep Neural Network (DNN) with 50 neurons in each layer. We find that Random Forest outperforms other classifiers. Additionally, we observe that not all of the 128 time-frequency features are unique enough to make different activities distinguishable from each other. To further improve the performance, we first train the random forest classifier on the complete dataset with 128 features, and calculate the overall contribution of each feature to the decision made by the classifier. The prediction function of a forest is the average of the prediction of its child trees, which can be decomposed into a sum of each feature [21]:

$$F(x) = \frac{1}{J}\sum_{j=1}^{J} c_{j_{full}} + \sum_{k=1}^{K}(\frac{1}{J}\sum_{j=1}^{J} contrib(x,k)), \tag{3}$$

where $F(x)$ is the predict outcome for the instance x of the random forest classifier and J is the number of decision trees. $c_{j_{full}}$ is the value at the root of the node for the jth decision tree, which is determined during the training phase. K is the number of features and $contrib(x,k)$ is the contribution of the feature k in the instance x. We only preserve a subset of features that have relatively larger contributions than the average of all the features. By applying this feature selection method, the number of features being used is reduced to around 30-40. These selected features through training are used in the following test phase.

7.3 Experimental Methodology

Experimental Setup. The experimental setup is similar to the setup shown in Figure 9. A smartphone is placed on the charger (i.e., an EVALSTWBC-EP board [31]), and the adversarial coil is stuck underneath the table and connected to a Tektronix TBS2102 digital oscilloscope. The table has a thickness of 3.2 cm, and the horizontal distance between the charger and the adversarial coil is around 2 cm. In the experiment, we use 3 different commodity smartphones including a Samsung Galaxy Note 5, a Samsung Galaxy S7, and a LG G7.

Data Collection. While the smartphone is being charged, we manually send messages to it from 10 commonly used social apps (i.e., SMS, WhatsApp, Viber, WeChat, QQ, Skype, Tumblr, Twitter, Instagram, and Messenger). 50 messages are send to each app on each phone. We also deliver phone calls to each smartphone using 4 common calling apps (i.e., cellular phone call, WhatsApp, Skype and WeChat), and 50 phone calls are made to each app on each phone. Additionally, we manually turn on the screen of each smartphone 50 times by pressing the power button, which indicates the user manually operates the phone. In total, we collect 2250 activities from these phones and the whole experiment is conducted over a two-month time period. During the experiment, the battery levels of these phones were between 5% to 100% without manual controls.

Table 2: Activity classification performance among 3 types of activities.

	10-fold cross-validation			Train & Test (2 : 1)		
	Accuracy	Precision	Recall	Accuracy	Precision	Recall
Note 5	95.00%	95.85%	95.83%	95.00%	92.59%	95.23%
S7	98.00%	97.33%	97.33%	98.00%	98.33%	97.78%
G7	95.33%	96.67%	96.67%	96.00%	96.29%	96.49%

Table 3: Phone call classification performance of 4 commonly used calling apps.

	10-fold cross-validation			Train & Test (2 : 1)		
	Accuracy	Precision	Recall	Accuracy	Precision	Recall
Note 5	90.00 %	89.38%	89.37 %	96.22%	96.77%	95.56%
S7	98.00%	97.65%	97.99%	98.78%	98.81%	98.53%
G7	95.20%	93.95%	94.00%	95.18%	95.65%	95.65%

Evaluation Method & Metrics. We use both 10-fold cross-validation and training & testing for classification. Specifically, 10-fold cross-validation divides the whole dataset randomly into 10 disjoint subsets, using 9 subsets for training and the retaining 1 subset for testing. For training & testing, we divide the whole dataset into a training set and a testing set, with a size ratio of 2:1. In addition, we use *Accuracy*, *Precision* and *Recall* to evaluate our attack. Specifically, the accuracy is defined as the percentage of the correctly identified activities among all the triggered activities. The precision of identifying the class k is defined as $P_k = \frac{TP_k}{TP_k+FP_k}$, where TP_k and FP_k are the true positive rate and the false positive rate for the class k, respectively. The recall of identifying the class k is defined as $R_k = \frac{TP_k}{TP_k+FN_k}$, where FN_k is the false negative rate for the class k.

7.4 Attack Performance

Activity Category Classification. As shown in Table 2, we observe that our attack is able to distinguish different types of activities with a substantial degree of accuracy. For the 10-fold cross-validation setup, the accuracy for all smartphones reach at least 95%, in which the S7 achieves the best accuracy of 97.33% precision/recall. Although there is no app being triggered for the class "screen turned on manually by user", our attack can still distinguish this activity. As a baseline, a random guess attack could only achieve 33.3% which is significantly worse than our attack.

Calling App Classification. As shown in Table 3, the reported classification accuracy, precision, and recall for all three phone models achieve more than 89% in both the 10-fold cross-validation and train & test models. The attack on the Samsung Galaxy S7 phone achieves the best accuracy with over 98.00% and 98.78% for the 10-fold cross-validation and train & test models, respectively. These results are much higher than a random guess attack (25% in distinguishing 4 calling apps), leading to the conclusion that the privacy threat of our attack is indeed serious. The results demonstrate the adversary's ability to detect and identify these calling activities by merely relying on the inductive adversarial coil voltage.

Messaging App Classification. As shown in Table 4, even if these types of activities are the same, we still achieve a very high performance for the Samsung S7 and LG G7 phones with the accuracy over 84% and 89%, and precision/recall over 86% and 90%,

Table 4: Message classification performance of 10 commonly used messaging apps.

	10-fold cross-validation			Train & Test (2 : 1)		
	Accuracy	Precision	Recall	Accuracy	Precision	Recall
Note 5	82.50%	82.17%	81.94%	80.67%	84.05%	83.63%
S7	86.81%	86.27%	83.35%	84.57%	86.34%	86.34%
G7	90.48%	90.83%	90.83%	89.80%	90.06%	90.06%

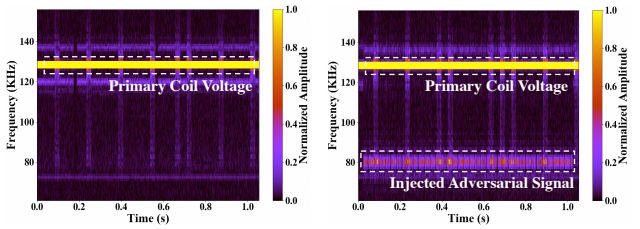
respectively, in both 10-fold cross-validation and train & test models. For the Note 5, we also have a relatively good result of over 80% accuracy, which is still much higher than a random guess (i.e., 10% in distinguishing 10 messaging apps). These experimental results showed that all these activities triggered by different apps exhibit unique and distinguishable patterns in the adversarial coil voltage and its derived Qi control error sequence, which can put people's privacy at risk while recharging their smartphones wirelessly.

8 DEFENSE STRATEGIES

Defense Against Hijacking Attack. When there is an alternating current flowing in the adversarial coil, the primary coil voltage will exhibit a different pattern due to the generated inductive power. Therefore, it's feasible to defend against the hijacking attack through detecting this external energy and swiftly terminate the charging process or reject the incoming messages once it's detected. Figure 15 (a) and 15 (b) show the power spectrogram of the primary coil voltage with and without malicious message injection, respectively. We can observe from Figure 15(a) that only the frequency response of the primary coil voltage is displayed, while the frequency response of the 80kHz sine wave, which serves as the carrier wave of the injected Qi messages in our implementation, is revealed on Figure 15(b). We thus propose the following sliding-window based automatic anomaly detection mechanism: the transmitter shall calculate the FFT of the primary coil voltage in each sliding window and use a peak detection algorithm to detect the number of peaks in the FFT spectrum. If there's an extra peak detected in addition to the operating frequency, it's highly likely there's an ongoing hijacking attack. To prove the feasibility of such a defense mechanism, we use the peak detection algorithm provided by the Scipy toolkit [45] and collect the primary coil voltage traces under two different scenarios: the first is where the smartphone is charging at a normal state while the other is under an overcharging attack, with the frequency of the adversarial signal set as 80kHz. Although we choose 80kHz as the carrier frequency in our implementation, there would always be an extra peak on the FFT spectrum even if the adversary uses other frequencies. We set the sliding window size as 20ms, with each scenario having a total of 32 seconds trace with 1600 samples. The anomaly-detection algorithm reaches a 100% true positive rate and a 0% false positive rate. This promising result demonstrate the effectiveness of the proposed mechanism, which can be used as a reference in the future design of Qi standard.

If the adversary sets the frequency exactly the same as the operating frequency of the primary coil, a legitimate charging profile containing a FFT spectrum collected from normal charging processes, would be created. The spectrum with message injection can thus be detected using outlier detection algorithms, such as 1-class SVM [40], isolation forest [26], and local outlier factor [36].

Defense Against Eavesdropping Attack. For the eavesdropping attack, adding noises to the primary coil voltage would directly introduce additional distortion on the inductive voltage of a nearby adversarial coil, making its correlation between the smartphone activities tampered, further downgrade the classification accuracy. To validate our thoughts, we collect 500 traces of the primary coil voltage while the smartphone (i.e., Note 5) is triggered by 10 message apps (50 times each) in our eavesdropping attack setting. We further perform the same classification methods as aforementioned and achieve a 10-fold cross-validation accuracy of 91.98% serving as the baseline accuracy. We then add random noises to parts of the collected primary coil voltage traces where there are no modulated communication packets. Specifically, for each gap between two adjacent packets, we add a Gaussian white noise with a random mean and standard deviation. This approach cause the 10-fold cross-validation accuracy to drop from 91.98% to 44.37%, indicating that adding random noises can indeed thwart eavesdropping attack.



(a) Normal charging state (b) Under hijacking attack

Figure 15: Spectrogram of the primary coil voltage at normal charging state and under hijacking attack.

In our current approach, we add noises to the collected voltage traces from the software side. We would also like to try some existing hardware based approaches, such as masking the voltage signal via a randomizer [3] and the DES encryption algorithm [39]. Dynamically switching the frequency and amplitude of the coil voltage [52] and duplication methods [14] may also be helpful on perturbing the integrity of the collected voltage traces. This would be considered for our future work.

Other Potential Approaches. In addition to the anomaly detection algorithm, another possible approach to defend against the hijacking attack is to detect the in-correlation between the control error message and the sudden rise of primary coil voltage. The adversarial alternating current will cause a sudden rise on the amplitude of the primary coil voltage, however, the transmitter will not receive a corresponding control error message at that moment. Thus, this conflict could be used for anomaly detection. Moreover, due to the self-calibration characteristic of Qi standard, the adversary has to inject malicious messages continuously at a very high frequency to ensure the attack is effective. The transmitter can thus monitor the message receiving rate and terminate the charging process once a sudden increase is detected. Wireless charger identification\authentication could be also possible to defend against hijacking attacks, though additional efforts are required in detecting the successfully injected Qi messages on the charger's primary coil. A recent study [53] showed that it could identify wireless chargers via fingerprinting based on the intrinsic nonlinear distortion effects of the underlying charging circuit. We will also follow this to explore if we could use these fingerprints at the circuit level to design a more resilient charging system.

For the eavesdropping attack, besides adding irregular noises on the primary coil voltage, another possible procedure is to add light-weight encryption mechanisms (e.g., lightweight block ciphers, hash functions [41], and AES [16]) to the Qi communication channel, which helps avert Qi messages from being eavesdropped. Some other existing studies [1, 18, 19, 54, 55] proposed to chaotically regulate the frequency of the power source to encrypt the energy, so that only legitimate power receivers can acquire the energy. As Qi uses AM modulation to modulate data bits on its carrier signal, we can possibly leverage this chaotic frequency regulation technique in a reverse way to protect the Qi messages (kind of energy) sent from the charging device to the charger. We leave these potential approaches as our future work.

9 DISCLOSURE

We are working with the industry to resolve the identified threats. We have already informed the Wireless Power Consortium (WPC) [47] of the potential security and privacy threats of Qi wireless charging. The fix of the identified threats is ongoing.

10 RELATED WORK

Security and Privacy Threats on Wired Charging. Due to the limited lifespan of smartphone batteries, a number of USB charging stations have been set up in public areas, such as airports, hotels, and hospitals, etc. Although these charging stations provide a great convenience, existing studies [23, 24, 42, 50, 51] have shown that the charging stations also expose users to serious privacy threats. For instance, Mactans [24] showed the success of deploying malware on iOS devices within one minute of being plugged into a malicious USB wall charger. Tian *et al.* [43] demonstrated AT commands issued through USB charging interfaces can launch various types of attacks on Android devices (e.g., unlock screens, inject touch events). KeySweeper [23] uses a malicious USB wall charger to passively sniff, decrypt, and log all keystrokes from wireless keyboards in the vicinity. Moreover, Yang *et al.* [51] showed that webpage browsing activity (i.e., which webpages are loaded) on smartphones while the phone is being charged can be collected via power trace analysis. Relying on the power consumption information, Yang *et al.* [50] also proposed a new attack on Tor to identify which website is being visited. Spolaor *et al.* [42] demonstrated the potential of using a (power-only) USB charging cable to exfiltrate data (e.g., IMEI, and contacts' phone number) from a smartphone through installing a malicious app on the device. Additionally, Meng *et al.* proposed a set of juice filming attacks which can automatically monitor and record the phone screen during the charging process [28–30].

Security and Privacy Threats on Wireless Charging. Compared with the security research on wired charging, the research efforts in exploring the vulnerabilities of wireless charging are still in the early stage. Several studies explored the security and safety issues of wireless powered communication networks. For instance, Dai *et al.* [9] proposed an algorithm that maximize the charging utility of far-field, radio frequency-based wireless rechargeable sensor networks (WRSNs), while assuring human safety under the electromagnetic radiation (EMR) exposure. Lin *et al.* [25] proposed a denial-of-charging attack on WRSNs for wireless charging vehicles. Through generating fake charging requests, the attack can make the rechargeable sensor nodes in the network exhaust faster than usual. Moreover, Niyato *et al.* [32, 33] formulated theoretical models (e.g., game theoretic models) in wireless powered communication networks to analyze the energy request and data transmission policy under jamming attacks. Additionally, given the security requirements in many applications, such as preventing unauthorized electric vehicles (EVs) from obtaining the energy, several studies [18, 19, 54, 55] proposed energy encryption mechanisms to ensure the power is only transmitted to an authorized receiver. There has been limited discussion on security and privacy threats of these wireless charging systems. Regarding wireless charging for mobile devices, few studies have investigated its underlying vulnerabilities. A survey paper [27] only briefly mentioned the possibility of launching eavesdropping and man-in-the-middle attacks against Qi. Neither technical details nor proof-of-concept experiments were provided. The discussion on eavesdropping attack was only limited to identity leakage (i.e., the manufacture of the smartphone), while the possibility of hijacking attacks and revealing more sensitive private information such as smartphone's activities have not been discussed. Roychowdhury [37] proposed an encryption method to protect the transmitted communication packets (i.e., ID & C packets) via simulation, while Yang *et al.* [49] proposed QID, a system which could identify different charging devices leveraging the unique features extracted from coil activities. Similar to the survey paper [27], only identity leakage had been taken into consideration in these papers. In general, the underlying threats of Qi wireless charging deserve to have greater attention.

Different from existing studies, we want to bring to public attention the potential vulnerabilities of wireless charging, particularly Qi wireless charging for mobile devices, to prioritize its mitigations under attacks. We analyze Qi standard from both security and privacy perspectives and demonstrate the capability of an adversary to take over the entire charging process and infer various phone activities while it is being charged.

11 CONCLUSION

In this paper, we conducted the first thorough study to explore the potential security and privacy vulnerabilities of Qi wireless charging. We demonstrated that due to the open propagation characteristic of electromagnetic signals, the Qi communication channel can be easily hijacked by injecting malicious Qi messages through stealthy placement of an adversarial coil on the charger. Additionally, an adversary is capable of snooping Qi messages transmitted between the wireless charger and the charging device to further detect and identify the device's activities (e.g., incoming phone calls and messages from different apps) while being charged. We validated that the adversary can reduce charging efficiency, stop power transfer, cause overcharging, which may lead to significant damage to the battery by injecting malicious Qi messages. Moreover, extensive experiments using multiple different commodity smartphones and 14 commonly used social apps demonstrated the effectiveness of the proposed eavesdropping attack.

ACKNOWLEDGMENTS

We would like to thank our anonymous reviewers for their insightful feedback. Some preliminary results of this work were presented in part at the poster session of ACM SenSys 2020 [48].

REFERENCES

[1] Emmanuel Ahene, Mark Ofori-Oduro, and Brighter Agyemang. 2017. Secure energy encryption for wireless power transfer. In *2017 IEEE 7th International Advance Computing Conference (IACC)*. IEEE, 199–204.

[2] Amazon. 2021. Yootech Wireless Charger,Qi-Certified 10W Max Fast Wireless Charging Pad. https://www.amazon.com/Wireless-Qi-Certified-Charging-Compatible-Qi-Enabled/dp/B079KZ49PJ. Accessed November, 2020.

[3] Luca Benini, Elvira Omerbegovic, A Macii, Massimo Poncino, E Macii, and Fabrizio Pro. 2003. Energy-aware design techniques for differential power analysis protection. In *Proceedings 2003. Design Automation Conference (IEEE Cat. No. 03CH37451)*. IEEE, 36–41.

[4] Businesswire. 2020. Consumers Seek Wireless Charging On the Go, New International Survey Shows. https://www.businesswire.com/news/home/20191016005007/en/Consumers-Seek-Wireless-Charging-New-International-Survey. Accessed March, 2020.

[5] Wireless Power Consortium. 2020. Ki Cordless Kitchen Standard. https://www.wirelesspowerconsortium.com/kitchen/

[6] Wireless Power Consortium. 2020. Medium Power Standard. https://www.wirelesspowerconsortium.com/medium-power/

[7] Wireless Power Consortium et al. 2016. The Qi wireless power transfer system power class 0 specification, part 1 and 2: Interface definitions.

[8] Garth P Corey. 2010. Nine ways to murder your battery (These are only some of the ways). *Battcon'10* (2010).

[9] Haipeng Dai, Yunhuai Liu, Guihai Chen, Xiaobing Wu, and Tian He. 2014. SCAPE: Safe charging with adjustable power. In *2014 IEEE 34th International Conference on Distributed Computing Systems*. IEEE, 439–448.

[10] DigiKey. 2020. WT505090-10K2-A11-G Wireless Power Transfer Tx (transmitting) Coil Units. https://www.digikey.com/product-detail/en/tdk-corporation/WT505090-10K2-A11-G/445-16095-ND/4702661

[11] Chil-Hoon Doh, Dong-Hun Kim, Hyo-Suck Kim, Hye-Min Shin, Young-Dong Jeong, Seong-In Moon, Bong-Soo Jin, Seung Wook Eom, Hyun-Soo Kim, Ki-Won Kim, et al. 2008. Thermal and electrochemical behaviour of C/LixCoO2 cell during safety test. *Journal of Power Sources* 175, 2 (2008), 881–885.

[12] Richard O Duda, Peter E Hart, and David G Stork. 2012. *Pattern classification*. John Wiley & Sons.

[13] Denzil Ferreira, Anind K Dey, and Vassilis Kostakos. 2011. Understanding human-smartphone concerns: a study of battery life. In *International Conference on Pervasive Computing*. Springer, 19–33.

[14] Louis Goubin and Jacques Patarin. 1999. DES and differential power analysis the "Duplication" method. In *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 158–172.

[15] Mahammad A Hannan, Md Murshadul Hoque, Aini Hussain, Yushaizad Yusof, and Pin Jern Ker. 2018. State-of-the-art and energy management system of lithium-ion batteries in electric vehicle applications: Issues and recommendations. *Ieee Access* 6 (2018), 19362–19378.

[16] Simon Heron. 2009. Advanced encryption standard (AES). *Network Security* 2009, 12 (2009), 8–12.

[17] MM Hoque, MA Hannan, A Mohamed, and A Ayob. 2017. Battery charge equalization controller in electric vehicle applications: A review. *Renewable and Sustainable Energy Reviews* 75 (2017), 1363–1385.

[18] NH Hussin, MM Azizan, A Ali, and MAM Albreem. 2017. Comparison of Performance based on Power of Energy Encryption in Medium Field for Wireless Power Transfer System. *International Journal on Advanced Science, Engineering and Information Technology* 7 (2017), 1805–1810.

[19] Nur Hazwani Hussin, MM Azizan, A Ali, and MAM Albreem. 2018. Encryption Techniques and Wireless Power Transfer Schemes. *Indonesian Journal of Electrical Engineering and Computer Science* 9, 1 (2018), 183–190.

[20] Masahiro Ichimura. 2007. The safety characteristics of lithium-ion batteries for mobile phones and the nail penetration test. In *INTELEC 07-29th International Telecommunications Energy Conference*. IEEE, 687–692.

[21] Diving into data blog. 2020. Interpreting random forests. http://blog.datadive.net/interpreting-random-forests/

[22] Anil Jain, Karthik Nandakumar, and Arun Ross. 2005. Score normalization in multimodal biometric systems. *Pattern recognition* 38, 12 (2005), 2270–2285.

[23] Samy Kamkar. [n.d.]. KEYSWEEPER. https://samy.pl/keysweeper/. Accessed March, 2020.

[24] Billy Lau, Yeongjin Jang, Chengyu Song, Tielei Wang, Pak Ho Chung, and Paul Royal. 2013. Mactans: Injecting malware into iOS devices via malicious chargers. *Black Hat USA* 92 (2013).

[25] Chi Lin, Zhi Shang, Wan Du, Jiankang Ren, Lei Wang, and Guowei Wu. 2019. CoDoC: A Novel Attack for Wireless Rechargeable Sensor Networks through Denial of Charge. In *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*. IEEE, 856–864.

[26] Fei Tony Liu, Kai Ming Ting, and Zhi-Hua Zhou. 2008. Isolation forest. In *2008 Eighth IEEE International Conference on Data Mining*. IEEE, 413–422.

[27] Xiao Lu, Dusit Niyato, Ping Wang, Dong In Kim, and Zhu Han. 2015. Wireless charger networking for mobile devices: Fundamentals, standards, and applications. *IEEE Wireless Communications* 22, 2 (2015), 126–135.

[28] Weizhi Meng, Fei Fei, Wenjuan Li, and Man Ho Au. 2017. Harvesting smartphone privacy through enhanced juice filming charging attacks. In *International Conference on Information Security*. Springer, 291–308.

[29] Weizhi Meng, Wang Hao Lee, SR Murali, and SPT Krishnan. 2015. Charging me and I know your secrets! Towards juice filming attacks on smartphones. In *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security*. 89–98.

[30] Weizhi Meng, Wang Hao Lee, SR Murali, and SPT Krishnan. 2016. JuiceCaster: towards automatic juice filming attacks on smartphones. *Journal of Network and Computer Applications* 68 (2016), 201–212.

[31] ST Microelectronics. 2020. EVALSTWBC-EP: Qi MP-A15 15W wireless charger TX evaluation kit based on STWBC-EP. https://www.st.com/en/evaluation-tools/evalstwbc-ep.html. Accessed September, 2020.

[32] Dusit Niyato, Ping Wang, Dong In Kim, Zhu Han, and Lu Xiao. 2015. Game theoretic modeling of jamming attack in wireless powered communication networks. In *2015 IEEE International Conference on Communications (ICC)*. IEEE, 6018–6023.

[33] Dusit Niyato, Ping Wang, Dong In Kim, Zhu Han, and Lu Xiao. 2015. Performance analysis of delay-constrained wireless energy harvesting communication networks under jamming attacks. In *2015 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 1823–1828.

[34] Plugless. 2021. Plugless Power. https://www.pluglesspower.com/

[35] Powermat. 2021. Powermat. https://powermat.com/

[36] Peter J Rousseeuw and Katrien Van Driessen. 1999. A fast algorithm for the minimum covariance determinant estimator. *Technometrics* 41, 3 (1999), 212–223.

[37] Priyankar Roychowdhury. [n.d.]. Trustable Digital Design Counter-Measures against Eavesdropping and Man-in-the-Middle Attacks in Qi Wireless Power Transfer Protocol. ([n. d.]).

[38] Samsung. 2020. Can you use your phone while charging? https://www.samsung.com/ca/support/mobile-devices/can-you-use-phone-while-charging/

[39] Hendra Saputra, Narayanan Vijaykrishnan, Mahmut Kandemir, Mary Jane Irwin, R Brooks, Soontae Kim, and Wei Zhang. 2003. Masking the energy behavior of DES encryption [smart cards]. In *2003 Design, Automation and Test in Europe Conference and Exhibition*. IEEE, 84–89.

[40] Bernhard Schölkopf, John C Platt, John Shawe-Taylor, Alex J Smola, and Robert C Williamson. 2001. Estimating the support of a high-dimensional distribution. *Neural computation* 13, 7 (2001), 1443–1471.

[41] Saurabh Singh, Pradip Kumar Sharma, Seo Yeon Moon, and Jong Hyuk Park. 2017. Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. *Journal of Ambient Intelligence and Humanized Computing* (2017), 1–18.

[42] Riccardo Spolaor, Laila Abudahi, Veelasha Moonsamy, Mauro Conti, and Radha Poovendran. 2017. No free charge theorem: A covert channel via usb charging cable on mobile devices. In *International Conference on Applied Cryptography and Network Security*. Springer, 83–102.

[43] Dave Jing Tian, Grant Hernandez, Joseph I Choi, Vanessa Frost, Christie Raules, Patrick Traynor, Hayawardh Vijayakumar, Lee Harrison, Amir Rahmati, Michael Grace, et al. 2018. Attention spanned: Comprehensive vulnerability analysis of AT commands within the android ecosystem. In *27th USENIX Security Symposium (USENIX Security 18)*. 273–290.

[44] Dries Van Wageningen and Toine Staring. 2010. The Qi wireless power standard. In *Proceedings of 14th International Power Electronics and Motion Control Conference EPE-PEMC 2010*. IEEE, S15–25.

[45] Pauli Virtanen, Ralf Gommers, Travis E Oliphant, Matt Haberland, Tyler Reddy, David Cournapeau, Evgeni Burovski, Pearu Peterson, Warren Weckesser, Jonathan Bright, et al. 2020. SciPy 1.0: fundamental algorithms for scientific computing in Python. *Nature methods* 17, 3 (2020), 261–272.

[46] WiTricity. 2021. WiTricity. https://witricity.com/

[47] WPC. 2020. Wireless Power Consortium. https://www.wirelesspowerconsortium.com/

[48] Yi Wu, Zhuohang Li, Nicholas Van Nostrand, and Jian Liu. 2020. Security and privacy in the age of cordless power world. In *Proceedings of the 18th ACM Conference on Embedded Networked Sensor Systems (SenSys)*. 717–718.

[49] Deliang Yang, Guoliang Xing, Jun Huang, Xiangmao Chang, and Xiaofan Jiang. 2020. QID: Identifying Mobile Devices via Wireless Charging Fingerprints. In *2020 IEEE/ACM Fifth International Conference on Internet-of-Things Design and Implementation (IoTDI)*. IEEE, 1–13.

[50] Qing Yang, Paolo Gasti, Kiran Balagani, Yantao Li, and Gang Zhou. 2018. USB side-channel attack on Tor. *Computer Networks* 141 (2018), 57–66.

[51] Qing Yang, Paolo Gasti, Gang Zhou, Aydin Farajidavar, and Kiran S Balagani. 2016. On inferring browsing activity on smartphones via USB power analysis side-channel. *IEEE Transactions on Information Forensics and Security* 12, 5 (2016), 1056–1066.

[52] Shengqi Yang, Wayne Wolf, Narayanan Vijaykrishnan, Dimitrios N Serpanos, and Yuan Xie. 2005. Power attack resistant cryptosystem design: A dynamic voltage and frequency switching approach. In *Design, Automation and Test in Europe*. IEEE, 64–69.

[53] Jiayu Zhang, Zhiyun Wang, Xiaoyu Ji, Wenyuan Xu, Gang Qu, and Minjian Zhao. 2020. Who Is Charging My Phone? Identifying Wireless Chargers via Fingerprinting. *IEEE Internet of Things Journal* (2020).

[54] Zhen Zhang, KT Chau, Chunhua Liu, Chun Qiu, and Fei Lin. 2014. An efficient wireless power transfer system with security considerations for electric vehicle applications. *Journal of Applied Physics* 115, 17 (2014), 17A328.

[55] Zhen Zhang, KT Chau, Chun Qiu, and Chunhua Liu. 2014. Energy encryption for wireless power transfer. *IEEE Transactions on Power Electronics* 30, 9 (2014), 5237–5246.