A Privacy Leakage Issue in Qi-compatible Cellphone Wireless Charging by Stray Magnetic Field Sniffing

Yirui Yang[1], Zihao Zhan, Honggang Yu, Qinghui Huang, Shuo Wang[2]
Department of Electrical and Computer Engineering
University of Florida
Gainesville, FL, USA
yirui.yang@ufl.edu[1] and shuowang@ieee.org[2]

2024 IEEE Applied Power Electronics Conference and Exposition (APEC) | 979-8-3503-1664-3/24/$31.00 ©2024 IEEE | DOI: 10.1109/APEC48139.2024.10509303

***Abstract*— This research uncovers that wireless charging of mobile phones generates a leakage magnetic field in the surrounding space, containing information about charging power. Using longwave radio technology with a ferrite rod antenna, signal detection extends to 1.5 meters, enabling inconspicuous measurement. Extracting features from the magnetic field waveforms, machine learning trains a Deep Neural Network model to distinguish user's activities on the phone with 100% accuracy. This highlights the privacy risks posed by this wireless charging technology, providing valuable insights into potential privacy concerns.**

Keywords*— *security and privacy, side channel attacks, wireless charging.

I. Introduction

In today's digital landscape, cellphones play a pivotal role in our daily lives, serving as our primary means of communication, information access, and task management. The growing reliance on mobile devices for both personal and professional purposes has made them indispensable tools. However, this increasing integration of smartphones into every aspect of our lives has raised substantial concerns about data privacy and security [1-4]. With an abundance of personal information stored on these devices, the digital age has brought about heightened awareness of the need to safeguard our data from potential threats and breaches.

The continuous advancements in power electronics techniques [5][6][7] and the emergence of novel power electronic devices [8][9] have propelled our smartphones to new levels of performance and functionality. These innovations have not only made our phones more capable but have also introduced convenient wireless charging methods [10]. However, the increasing switching frequency [11][12] and faster switching speed [13] also results in an unintended consequence: the generation of electromagnetic interference (EMI) noises [14] during their operation. While EMI receives extensive research attention within the field of electromagnetic compatibility (EMC)[15], its significance in the context of cybersecurity should not be underestimated. Recent research has illuminated the notion that these EMI noises can carry information relevant to users' activities [1-4]. And it has been shown that hackers can potentially exploit this avenue to infer sensitive information, thereby exposing vulnerabilities in the security [2][3] and privacy [1] of smartphone users.

In the past, hackers typically had to physically access a phone, its cables, or directly connected devices to collect EMI noises for information gathering [1][2]. Remote collection of these noises for eavesdropping was challenging [3] due to the weak strength of the radiated EMI produced by phones. However, the widespread use of wireless charging techniques may change this situation.

Cellphone wireless charging solutions utilize magnetic field to transfer power to the phone. However, a fundamental challenge arises due to the inherent gap between the phone and the charger, preventing the magnetic circuit from being a perfect closed system and resulting in leakage fields [16] extending into the surrounding space [17]. These leakage fields effectively mirror the characteristics of the charging waveform. Consequently, hackers have the capability to sense variations in the charging waveform by monitoring this leakage field [18][19] from a distance, enabling them to infer fluctuations in the charging power.

Furthermore, the leakage field can contain more detailed power-related data. For instance, the widely adopted Qi standard, commonly used in consumer electronics for wireless charging, employs in-band communication to transfer data between the phone and the charger [20]. That means, the phone and the charger transmit the data by modulating the transmitted power waveform. By eavesdropping on the leakage field, hackers gain access to the communication contents, including commands and reports about the power close-loop control process within the Qi system. It's crucial to note that this data is typically not encrypted, and the protocol is publicly available in the Qi standard documents accessible online [20]. In summary, through remote sensing of the leakage field emitted by a wirelessly charged phone, hackers can deduce trends in the phone's charging power, revealing a previously unrecognized security vulnerability in the wireless charging process.

Allowing hackers to gain access to the user's phone power trend has direct consequences, enabling them to infer users' activities on the device. Research has already shown that a user's actions on a smartphone leave recognizable features in the phone's charging power. By extracting and identifying these features, hackers can make practical guesses about the types of apps running on the phone and potentially other more detailed information. An emerging trend in wireless charging technology is to minimize disruptions to users' regular phone usage during the charging process. Compact wireless chargers like MagSafe, for instance, allow users to hold their phones while charging, while other designs enable users to place their phones at an angle on a tabletop for ease of operation. Ongoing research is also exploring extending the range of wireless charging and enhancing the flexibility of phone positioning during the charging process. This trend makes scenarios where people use their phones during wireless charging more common.

Consequently, if there is a higher risk of leaked behavioral information during wireless charging, the resulting privacy concerns will become increasingly severe as wireless charging technology matures.

The leakage of information regarding a user's app usage poses significant threats to an individual's privacy [3] and cybersecurity [2]. Even the seemingly innocuous timeline of apps accessed can unveil substantial insights into a person's personal life, preferences [1], and behaviors. This information forms the building blocks for creating a detailed profile of the victim, potentially resulting in a severe invasion of their privacy. Moreover, this knowledge becomes a potent tool for hackers in devising convincing phishing attacks. By leveraging their understanding of the victim's app preferences, attackers can tailor deceptive messages that appear to originate from trusted sources, such as a recently used app, increasing the chances of successful social engineering. Furthermore, there is a risk of the collected data being traded or shared with third parties, exacerbating concerns related to personal privacy and exposing individuals to potential exploitation. These threats underscore the importance of safeguarding personal data and devices in an increasingly interconnected digital landscape [19]. In this context, comprehensive cybersecurity measures and user education become imperative to mitigate these emerging risks.

It should be noted that distinguishing subtle differences in the power waveform of a phone when running various apps is a challenging task for humans. Identifying the specific characteristics of charging power fluctuations is also a complex and difficult task.

This is where Deep Neural Networks (DNN) offer a significant advantage [21]. DNN excels in complex data analysis and pattern recognition. So, this research employs DNN technique in this task. By training a DNN on a dataset of power waveforms associated with different app usage scenarios, the network can learn to recognize and classify the slight variations in the charging power waveform associated with different app activities with a high degree of accuracy.

This paper is organized as follows. Section II-A will introduce the characteristics of power waveforms in a Qi-compatible wireless charging system and the relevant communication protocols. In Section II-B, the physical mechanism of the eavesdropping will be covered. Section III will introduce the DNN technique utilized to analyze collected signals and infer user activities. The experimental validation of the proposed threat scenario is presented in Section IV. Section V will conclude this paper.

II. Physical Principles of Power-Relevant Information Leakage in Wireless Charging Sysytem

A. Magntic Field for Wireless Charging Carries Information.

As the most widely used industry standard for wireless charging in the consumer electronics sector, the Qi standard specifies the structure of wireless charging systems. Figure 1 illustrates a typical main circuit structure of a wireless charging system as outlined in the Qi standard.

The inverter contained within the Wireless charger generates an AC square wave voltage V_{inv} in the range of 100kHz to 200kHz. This voltage V_{inv} is applied to a primary coil connected to the charger, producing a current I_p and then generating a magnetic field around the primary coil. Most of the magnetic flux crosses the gap between the charger and the charged phone, reaching the location of the secondary coil inside the phone. According to Faraday's electromagnetic induction law, this periodically changing magnetic field induces voltage and current in the secondary coil. After subsequent processing such as rectification and regulation, it charges the phone's battery.

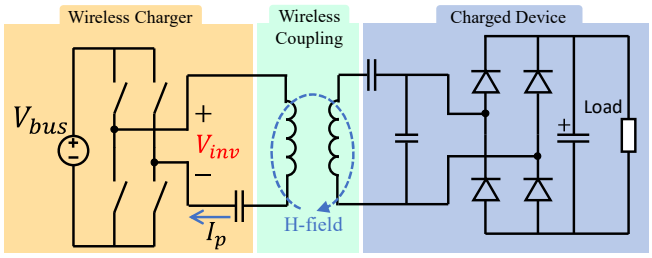


Fig. 1. Schematic of a wireless power transfer system.

There are two ways in which a wireless charging system can change its charging power. First, after communication and negotiation between the phone and the charger, the charger can initiate a change in the charging power. The charger changes the transmission power by altering the frequency and duty cycle of V_{inv}. Because the structure of the wireless charging system exhibits the characteristics of a resonant converter, its transmission gain is frequency-dependent, and, therefore, changing the frequency of V_{inv} can modify the power of transmission. This alteration is reflected in the alternating magnetic field generated around the primary coil in the form of changes in amplitude and frequency.

In the second scenario, V_{inv} of the charger remains unchanged, but the load of the phone itself undergoes a change. This change can result in variations in the amplitude or phase of the current in the primary coil. Since the current in the primary coil is the source of the magnetic field, the amplitude and phase of the magnetic field will also change accordingly.

In summary, because the magnetic field at the wireless coupling stage serves as the medium for transferring power from the wireless charger to the phone, changes in wireless charging power will manifest in corresponding alterations in the frequency, amplitude, or phase of the magnetic field. In other words, the information about changes in wireless charging power is contained within the waveform of the magnetic field.

In addition, the waveform of the magnetic field also contains communication information, the content of which is directly related to changes in charging power. Figure 2 illustrates the communication structure designed by the Qi standard for data exchange between the phone and the charger. Since the phone and the charger are not physically connected, when the phone needs the charger to adjust V_{inv} to help changing the charging power, it needs to transmit messages wirelessly to the charger.

The Qi standard specifies that the way a phone transmits data to the charger is by overlaying binary disturbances on its load impedance, thereby causing fluctuations in I_p in the charger's coil. The charger detects these special fluctuations in I_p to

obtain the information sent by the phone. Since the current in the primary coil is directly related to the magnetic field, this communication information is reflected in the magnetic field as well.

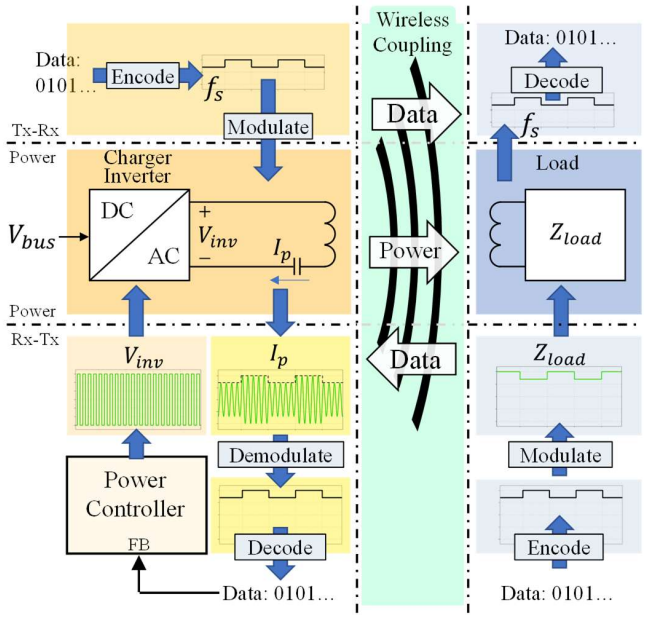


Fig. 2. A block diagram of the communication structure in a Qi-compatible wireless charging system.

When the charger needs to respond to the phone's requests or send data to the phone, it does so by adding small deviations to the frequency of V_{inv}. This causes V_{inv}'s frequency to jitter around the frequency required for power transmission. The phone detects changes in the system's operating frequency to obtain the data sent by the charger. Since the frequency of the magnetic field is the same as that of V_{inv}, this communication information is also reflected in the magnetic field.

According to the Qi standard, for the communication between the phone and the charger, the encoding relationship between the physical signal and binary values follows Differential Bi-phase Encoding Scheme". Binary bits are composed in a Least-Significant-Bit (LSB) 11-bit asynchronous serial format to form a byte. Bytes are structured in a "Header+Message+Checksum" format to create a data packet. Communication is not encrypted, and the meaning of the content within the data packet is detailed in the publicly available Qi standard. Therefore, once the communication waveform is obtained, its content can be completely decoded.

Among the data packets, two types of data packets have the closest relationship with charging power: the Control Error (CE) packet and the Received Power (RP) packet. Both are data packets sent by the phone to the charger. The CE packet contains a value that measures the deviation between the actual received power of the phone and the target charging power. The charger uses the CE data packet to adjust V_{inv}, enabling closed-loop control of the charging power. The RP packet contains real-time information about the actual charging power that the phone is receiving. The phone reports real-time power to the charger to help the charger calculate power losses during transmission and determine if there are any safety concerns. By detecting the content of these CE and RP data packets through the magnetic field, the charging power fluctuation curve of the phone can also be outlined.

In summary, during the wireless charging process, fluctuations in transmission power are reflected in changes in the amplitude, phase, and frequency of the magnetic field waveform. Communication content related to power adjustment is also mirrored in the magnetic field waveform. By measuring changes in the magnetic field, it is possible to understand the variations in wireless charging power.

B. Detect Magnetic Field with Radio Reception Technology.

Due to the inevitable air gap in the magnetic path between the charger and the phone, there is significant leakage of the magnetic field into the surrounding space. The leaked magnetic field exhibits a waveform very similar to the original magnetic field. As a result, the information contained in the original magnetic field, as described earlier, also exists in the leaked magnetic field. Therefore, for a phone being wireless charged, hackers can extract the information from the leaked magnetic field measured from a distance without physical contact. Then they obtain the phone's charging power curve, and ultimately infer the user's activities on the phone.

Due to the operation frequency of wireless charging ranges from 100kHz to 200kHz, and the coil dimensions are in the centimeter range, the electromagnetic radiation in the far field is extremely weak. The leaked magnetic field distributed within a few meters of the phone is mainly in the near field, and its field strength rapidly attenuates with distance. So, it will be more practical for the hackers to eavesdrop on the leakage field is within several meters. When measuring the field strength of the leaked magnetic field within this range, radio reception technology is needed to enhance the quality of signal reception. A typical radio reception solution is illustrated in Fig. 3.

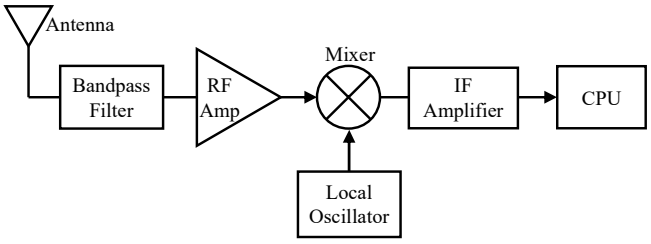


Fig. 3. A block diagram of a signal reception system for the measurement of the leakage field.

The main components in Fig. 3 include the receiving antenna, bandpass filter, active signal amplifier, mixer, intermediate frequency (IF) amplifier, and the chips for subsequent signal analysis or decoding. Since the frequency of the leaked field is low and majorly magnetic field, a ferrite rod antenna can be used as the receiving antenna, and the coil winding should use Litz wire to improve the quality factor. The bandpass filter is used to block signals from unwanted frequency ranges, with the passband designed between 100kHz and 200kHz. The received signal is amplified by the RF amplifier, then the mixer raises the signal frequency to the intermediate frequency. In practical applications, the Local Oscillator's frequency is dynamically adjusted to precisely select the

operating frequency, ensuring real-time tracking of the wireless charging process. This enables the most effective measurement of the actual leaked magnetic field waveform.

As described in Section II-A, the relationship between the leakage magnetic field signal and the charging power is reflected in two aspects. On one hand, it involves the analog characteristics of the signal itself, such as frequency, phase, and amplitude. On the other hand, the magnetic field's waveform carries digital communication contents related to the charging power control.

Once the leaked magnetic field signal is measured using the previously mentioned radio reception device, its analog signal characteristics can be directly extracted. The extraction of communication content can be accomplished using amplitude demodulation method for the following reasons: In cases where the phone sends data to the charger, the Qi standard specifies that the phone controls the load to toggle between two values near the actual load, carrying binary data in the form of load fluctuations, which is to be detected by the charger. This modulation method primarily affects the amplitude of the magnetic field, which also fluctuates with the modulation signal. Therefore, amplitude demodulation method is suitable for the extraction of the communication signal. The subsequent processors will digitize the signal and decode for its contents.

In cases where the charger sends data to the phone, the Qi standard specifies that the charger controls its operating frequency to superpose an intermittent shift upon the normal operation frequency, and the phone receives the signal by detecting frequency fluctuations. Since the above described receiving circuit utilizes the Local Oscillator, Mixer, and narrowband IF amplifier to selectively detect the signal at the normal operating frequency, its gain at frequencies beyond the passband is significantly lower than that at the operation frequency. Thus, when the charger shifts the operation frequency, the output of the IF amplifier will significantly reduce in amplitude. So, the charger's frequency modulation also results in changes in the output amplitude of the IF amplifier. In this case, amplitude demodulation is also a preferable method for signal extraction.

Based on the analysis provided, a common longwave radio with a ferrite rod antenna is well-suited for receiving this signal. In the field of radio, the longwave (LW) band typically refers to the frequency range of 100kHz to 300kHz and employs Amplitude Modulation (AM). So, LW radios come with circuits for Amplitude Demodulation. Additionally, the advantage of a ferrite rod antenna is its smaller size compared to an electric field antenna when receiving low-frequency electromagnetic waves. This makes it a common choice in the design of LW radios, and suitable ferrite rod LW radios are readily available in the market.

As a result, modifying a ferrite rod LW radio for the detection of leakage magnetic field is a convenient choice, which also reduces the barrier for hackers to use this eavesdropping technique. This experiments in study will be based on a modified ferrite rod LW radio.

III. Design of Deep Neural Networks for Waveform Analysis and Phone Activity Inference

Section II introduces the techniques to obtain leakage magnetic field waveforms and extract communication contents from these waveforms. The ultimate objective is to utilize this collected information to infer user activities on the phone. However, identifying the intricate waveform characteristics and establishing the connection between charging power trends and specific app activities presents considerable challenges for human analysis. To address this, Deep Neural Networks emerge as a promising solution. In this section, an exploration is conducted into the effective utilization of deep neural networks (DNN) to address this particular task, providing valuable insights into how DNNs can be applied and their potential to overcome the intricate hurdles associated with it.

As an overview of the model, it is trained using waveform data from the leakage magnetic field that is acquired while various apps are running on the phone. Once the training is complete, the model is expected to tell which app is currently running on the phone based on the given leakage field waveform.

Data preprocessing is a crucial step in our training process. As discussed in Section II, the waveform carries information in two ways: through the inherent characteristics of the raw traces at the operation frequency and via the CE Packets and RP Packets. To maximize the utility of these potential features within the traces, a two-fold data preprocessing approach is employed. This approach is common in machine learning workflows to ensure that the data used for training and testing models is appropriately cleaned, transformed, and organized.

The first step, Data Cleaning and Preprocessing, comprises two key aspects. First, the Short-Time Fourier Transform (STFT) technique is used to generate spectrograms from the raw traces. This step extracts both time-domain and frequency-domain features within the trace, enabling a more comprehensive analysis. Moreover, only the spectrums around the operation frequency is included for the training, reducing unrelated interferences. Second, to take full advantages of the prior knowledge about the communication protocol, the CE packets and the RP packets in the waveforms are decoded. Using this information, a charging power curve is generated, which is then input into the DNN for further exploration of its relationship with app usage.

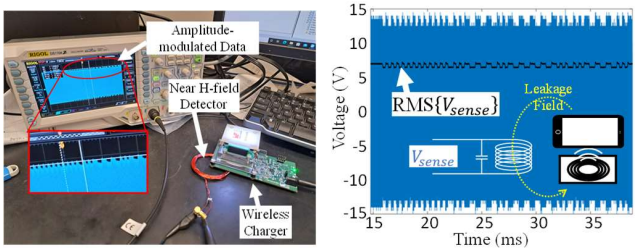
In the second step, namely the Data Splitting, the preprocessed data is split into training sets and test sets. This is essential to evaluate the machine learning model's performance properly. This two-fold data preprocessing approach effectively prepares the model for the subsequent data analysis and characteristic identification.

The preprocessed data will be used to train a Convolutional Neural Network (CNN) to extract features. Since two types of data are generated during the data preprocessing stage, either one type of data or both types can be used when training the model. When using one type of data, the data goes through four convolutional layers to extract features, and then three fully connected layers are used for classification and regression, completing the model training. When training the CNN model

using both types of data, a multi-channel CNN structure is used to process the two data types. Each data type goes through four convolutional layers to extract features and is organized for classification using one fully connected layer. The features extracted from the two channels are merged through a Concatenation Layer to form a larger feature vector. The merged feature information is input into two additional fully connected layers for final classification and regression, mapping the features to the model's output, completing the model training.

IV. Experiment Verification

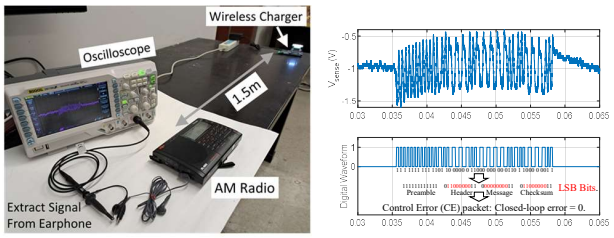
To verify the presence of communication information in the near magnetic field around the wireless charger, the Renesas WP15WBD-RK Wireless Charging Kit [22] was examined. The evaluation kit adhered to the Qi standard, with a steady-state operating frequency of 141kHz. A circular coil with 20 turns, wound using AWG20 wire and having a diameter of 5cm, was utilized for magnetic field detection. The coil was tuned by connecting a parallel resonant capacitor for a high gain at 141kHz. The setup is shown in Fig. 4(a), a voltage of 141kHz was measured across the terminals of the coil, as shown in Fig. 4(b), which is induced by the leakage field. The amplitude of the voltage waveform varied over time, indicating the presence of amplitude modulation (AM) communication.



(a) (b)

Fig. 4. Experimental validation of the presence of communication information in the leakage field. (a) Experiment setup. (b) Communication binary bits present in the induced voltage.

To verify that the leakage magnetic field strength is sufficient for remote eavesdropping, the second phase of the experiment utilized an LW radio reception circuit of a TECSUN TL-660 radio receiver to detect the signal, as shown in Fig. 5(a). The radio was tuned to the operation frequency of the charger (141kHz). The charging power command packet is fully recovered from the voltage sensed 1.5m from the charging device, as shown in Fig. 5(b).

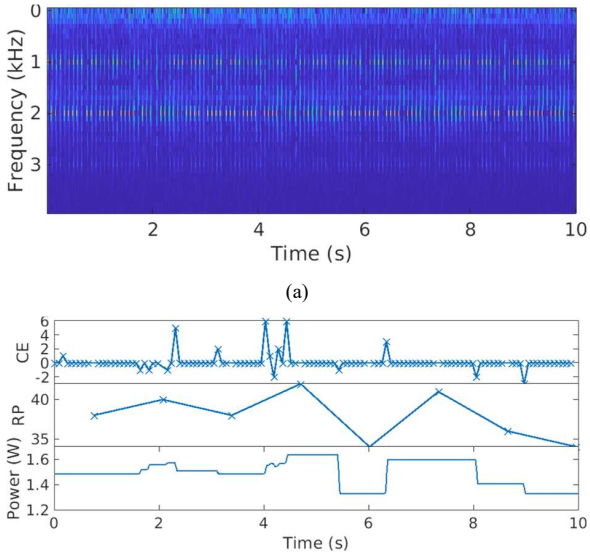


(a) (b)

Fig. 5. Experimental validation of distant eavesdropping. (a) Experiment setup. (b) Sensed voltage and the recovered digital waveform.

After confirming the feasibility of the distant measurement of leakage magnetic fields, the next phase of the experiment aims to validate the capability of using DNN to analyze the measured waveforms and subsequently infer the user's activities on the phone. The experiments were conducted under six distinct cellphone activities, which included the use of five different apps - Amazon, X, YouTube, Safari, and Recorder - as well as a scenario in which the cellphone remains idle. For each activity, 100 data traces were gathered for training and an additional 10 data traces were gathered for testing. Each data trace was collected at a sampling rate of 200kHz and spanned a duration of 10 seconds.

The gathered waveforms go through the preprocessing steps explained in Section III. Figure 6 provides an illustration of the preprocessed data. Figure 6(a) is an example of the spectrograms obtained through STFT. And Fig. 6(b) shows the values extracted from the CE and RP packets decoded from the waveform. The power curve generated by these values is also shown in Fig. 6(b).



(a)

(b)

Fig. 6. An example of two types of information extracted from the measured magnetic field waveforms during the data preprocessing steps. (a) Spectrogram obtained through STFT. (b) values of decoded CE and RP packets and the estimated power curve.

To evaluate the importance of two different types of information - spectrograms and Qi messages - in reflecting cellphone activities, three distinct CNN models were trained. These models were configured to use either spectrograms exclusively, Qi messages exclusively, or a combination of both types of information during training. The model architecture adheres to the design described in Section III. All three models were trained using a batch size of 100 for 200 epochs. Subsequently, the performance of each of the three models was assessed.

The classification results are illustrated in Fig. 7 using confusion matrices. When trained only on spectrograms or Qi messages, the classifier achieves accuracy levels of 86.67% and 76.67%, respectively. However, the classifier attains a 100% accuracy rate when employing a multi-channel CNN model with

both spectrogram and Qi message data. This enables accurate identification of all six distinct activities based on their corresponding power traces, affirming the robustness and effectiveness of our approach in inferring user activities on cellphones under wireless charging.

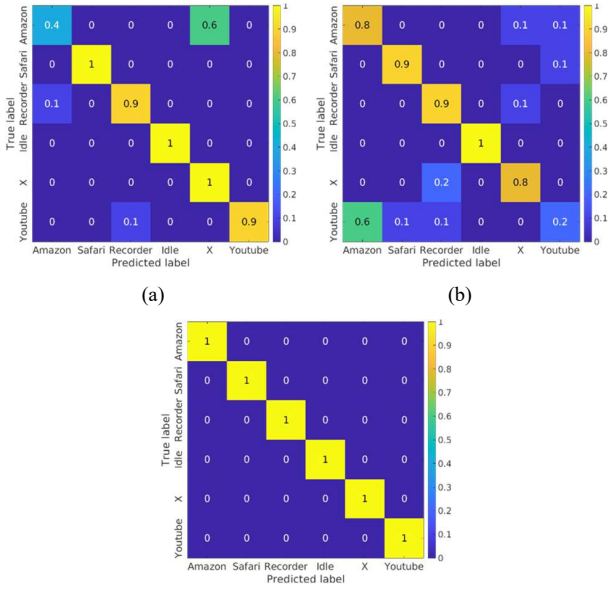


Fig. 7. Confusion matrices obtained when using different data for model training. (a) Model is trained only with spectrogram data. (b) Model is trained only with Qi message (CE/RP packets) data. (c) Model is trained with both kinds of data.

V. Conclusion

This study reveals that when charging a mobile phone through wireless charging technology, it generates a leakage magnetic field in the surrounding space that contains information about the phone's charging power. Because the phone's charging power trend is related to the user's activities on the phone, the information contained in this leakage magnetic field may lead to privacy concerns. Through theoretical analysis and practical experiments, this research confirms that the leakage magnetic field can be measured in close proximity to the phone using a simple magnetic field receiving coil. By employing ferrite-rod-antenna based longwave radio reception technology, the signal detection range can be extended to 1.5 meters, which is sufficient for measuring the leakage magnetic field without the victim's awareness.

Based on the acquired magnetic field waveforms, this study indicates that information related to charging power is embedded in the original waveform and the in-band communication data designed by the Qi standard that can be extracted from the waveform. Machine learning techniques are used to extract features from this information and train a Deep Neural Network model. In the experiments, the final DNN model is capable of distinguishing between the phone's idle state and running five different apps based on the measured magnetic field waveforms, achieving an accuracy rate of 100%. This demonstrates the privacy risks associated with the wireless charging technology proposed in this study.

References

[1] Alexander S. La Cour, Khurram K. Afridi, and G. Edward Suh. 2021. Wireless Charging Power Side-Channel Attacks. In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (CCS '21). Association for Computing Machinery, New York, NY, USA, 651–665.

[2] Cronin, Patrick et al. "Charger-Surfing: Exploiting a Power Line Side-Channel for Smartphone Information Leakage." USENIX Security Symposium (2021).

[3] Ni, Tao, et al. "Uncovering User Interactions on Smartphones via Contactless Wireless Charging Side Channels." 2023 IEEE Symposium on Security and Privacy (SP). IEEE Computer Society, 2022.

[4] 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). Association for Computing Machinery, New York, NY, USA, 916–929.

[5] Y. He et al., "Control Development and Fault Current Commutation Test for the EDISON Hybrid Circuit Breaker," in IEEE Transactions on Power Electronics, vol. 38, no. 7, pp. 8851-8865, July 2023.

[6] Y. He, Y. Li, B. Zhou, Y. Zou and F. Z. Peng, "An Ultra-Fast Inrush-Current-Free Startup Method for Grid-tie Inverter without Voltage Sensors," 2023 IEEE Applied Power Electronics Conference and Exposition (APEC), Orlando, FL, USA, 2023, pp. 2874-2880.

[7] S. Fan et al., "Inherent SM Voltage Balance for Multilevel Circulant Modulation in Modular Multilevel DC–DC Converters," in IEEE Transactions on Power Electronics, vol. 37, no. 2, pp. 1352-1368, Feb. 2022.

[8] Z. Gao et al., "A GaN-Based Integrated Modular Motor Drive for Open-Winding Permanent Magnet Synchronous Motor Application," 2018 1st Workshop on Wide Bandgap Power Devices and Applications in Asia (WiPDA Asia), Xi'an, China, 2018, pp. 73-79.

[9] X. Liu et al., "FPGA-Based Forced Air-Cooled SiC High-Power-Density Inverter for Electrical Aircraft Applications," 2023 IEEE Applied Power Electronics Conference and Exposition (APEC), Orlando, FL, USA, 2023, pp. 3169-3173.

[10] M. Gao, H. L. Herrera and J. Moon, "Optimization of Core Size and Harvested Power for Magnetic Energy Harvesters based on Cascaded Magnetics," 2023 IEEE Applied Power Electronics Conference and Exposition (APEC), Orlando, FL, USA, 2023, pp. 2926-2932.

[11] Z. Lu et al., "Medium Voltage Soft-Switching DC/DC Converter With Series-Connected SiC MOSFETs," in IEEE Transactions on Power Electronics, vol. 36, no. 2, pp. 1451-1462, Feb. 2021.

[12] Q. Yang, A. Nabih, R. Zhang, Q. Li and Y. Zhang, "A Converter Based Switching Loss Measurement Method for WBG Device," 2023 IEEE Applied Power Electronics Conference and Exposition (APEC), Orlando, FL, USA, 2023, pp. 8-13.

[13] Y. Zhang et al., "A SiC and Si Hybrid Five-Level Unidirectional Rectifier for Medium Voltage Applications," in IEEE Transactions on Industrial Electronics, vol. 69, no. 8, pp. 7537-7548, Aug. 2022.

[14] H. Jie et al., "VNA-Based Fixture Adapters for Wideband Accurate Impedance Extraction of Single-Phase EMI Filtering Chokes," in IEEE Transactions on Industrial Electronics, vol. 70, no. 8, pp. 7821-7831, Aug. 2023.

[15] Y. Cao et al., "A Three-Level Buck–Boost Converter With Planar Coupled Inductor and Common-Mode Noise Suppression," in IEEE Transactions on Power Electronics, vol. 38, no. 9, pp. 10483-10500, Sept. 2023.

[16] L. Yi and J. Moon, "Direct in-situ Measurement of Magnetic Loss in Power Electronic Circuits," in IEEE Transactions on Power Electronics, vol. 36, no. 3, pp. 3247-3257, March 2021.

[17] A. Zajic, M. Prvulovic and D. Chu, "Path loss prediction for electromagnetic side-channel signals," 2017 11th European Conference on Antennas and Propagation (EUCAP), Paris, France, 2017, pp. 3877-3881.

[18] J. Danial, D. Das, S. Ghosh, A. Raychowdhury and S. Sen, "SCNIFFER: Low-Cost, Automated, Efficient Electromagnetic Side-Channel Sniffing," in IEEE Access, vol. 8, pp. 173414-173427, 2020.

[19] Giovanni Camurati, Sebastian Poeplau, Marius Muench, Tom Hayes, and Aurélien Francillon. 2018. Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS '18). Association for Computing Machinery, New York, NY, USA, 163–177.

[20] Qi-v1.3-comms-protocol and Qi-v1.3-power-delivery, in"Qi specifications", [online] Available: https://www.wirelesspowerconsortium.com.

[21] X. Liu et al., "Convolutional Neural Network (CNN) based Planar Inductor Evaluation and Optimization," 2022 IEEE Applied Power Electronics Conference and Exposition (APEC), Houston, TX, USA, 2022, pp. 1506-1511.

[22] Renesas WP15WBD-RK evaluation kit user manual, [online] Available: https://www.renesas.com/eu/en/products/power-powermanagement/wireless-power/wireless-power-transmitters/wp15wbd-rk-15w-wireless-charging-solution-bi-directional-data-communication.