Side-Channel Based Device Authentication in Wireless Charging: An Experimental Study

Sung-Kyu Ahn
SysCore Lab
Sejong University
Seoul, Korea
yiimfn@gmail.com

Sang-Hoon Choi
SysCore Lab
Sejong University
Seoul, Korea
csh0052@gmail.com

Ki-Woong Park*
Department of Information Security
Sejong University
Seoul, Korea
woongbak@sejong.ac.kr

***Abstract*—As wireless technologies increasingly occupy the digital landscape, wireless charging services for smartphones and related accessories have taken a leap forward. In this context, the ability to authenticate and distinguish devices has become a paramount necessity for maintaining consistent service quality and user satisfaction. In this study, we implement an efficient and cost-effective side-channel based device authentication system. Our approach primarily focused on harvesting side-channel data from Qi wireless charger voltage measurements, thus developing a procedure that is not confined to a specific protocol. To implement this authentication framework, we developed a model that classifies devices by continuously monitoring voltage fluctuations in a wireless charging environment, and learns from these observations. We conducted validation experiments using four products from two different smartphone manufacturers. Our results show that the manufacturer of a mobile device can be identified with an exceptional 100% accuracy by relying solely on the voltage readings obtained from the Qi wireless charger. Moreover, our method can distinguish among four devices with different models with an accuracy of 92%. By adopting such a side-channel based device authentication system, service providers can mitigate the risks associated with unauthorized access by unauthenticated users. Our groundbreaking findings may also contribute to the development of a robust and scalable architecture for device classification and authentication in wireless charging environments.**

***Index Terms*—wireless charging, device authentication, side-channel data**

I. Introduction

Considering the ubiquitous presence of smartphones and the surge in ancillary accessories, individuals are normally equipped with mobile devices at all times. Most of these devices require battery power, thereby creating a demand for frequent battery charging to support continuous usage. To reduce this demand, battery capacity of mobile devices has been increased. However, this implies additional device weight. Moreover, considering that battery consumption is subject to fluctuations based on the nature of smartphone usage, numerous studies aimed at reducing battery consumption instead [1] [2]. Regardless of these efforts, smartphones in daily use still require regular charging. Sustaining a stable power supply for mobile devices and maintaining battery life require frequent connections to a charging cable. This burdensome process has propelled the development of various wireless charging technologies for mobile devices, which is also supported by a market share steadily increasing.

In 2023, the BIS Research CEO postulated that wireless charging technology will be adopted more extensively than the wired counterpart [3]. As advancements in wireless charging technology continue, numerous institutions and corporations are providing wireless charging services. Notably, public wireless charging services, as the ones shown in Fig.1, have made their way into venues such as airports and bus stops.

Fig. 1: Public Wireless Charging Service

Public wireless charging services aim to deliver user-friendly wireless charging options. To improve the quality of these services and mitigate potential malicious activities, service providers and institutions must implement device authentication technologies suitable for any device that utilizes their services. Therefore, in this study, we propose a swift and cost-effective side-channel based device authentication system that can be deployed within the service infrastructure of organizations and corporations offering wireless charging facilities. Specifically, we employ the technological blueprint of a side-channel based device authentication system compatible with the Qi standard technology landscape, which is prevalent in the wireless charging market. Additionally, we anticipate prospective enhancements of the proposed technology for future development.

The device authentication technology proposed in this study requires constant voltage measurements within the wireless charging transmitter throughout the charging process. Through

* Corresponding author.

2831-7203/23/$31.00 ©2023 IEEE
DOI 10.1109/AIKE59827.2023.00028

learning and classification of voltage fluctuation patterns, the system effectively classifies mobile devices during charging.

To implement this approach, we adopted a Atmega-based microcontroller, thus, bypassing the necessity for high-performance or cumbersome equipment to be installed in the transmitter. Furthermore, the proposed technology neither requires a physical connection between user and system nor additional procedures to be performed by the user. Lastly, our experimental evaluation targeted Qi standard-based wireless charging transmitters, which cater to multiple wireless charging-capable mobile devices, to demonstrate the versatile applicability of the proposed technology in various settings.

The structure of this paper is as follows. Section 2 presents background knowledge and related studies pertinent to this study. Section 3 describes experiments and results obtained using the proposed side-channel based device authentication technology. Section 4 addresses potential application and expandability of the proposed technology. Finally, Section 5 presents the conclusions of this study

II. Related work

In this section, wireless power transfer technologies are analyzed, and their classification and utilization in various applications are discussed. Prominent wireless power transfer technologies include magnetic induction and resonance, and radio frequency/optical based wireless charging methods [4]. Currently, the most widely commercialized technology is based on magnetic induction. Magnetic resonance-based methods are entering the commercialization phase, whereas radio frequency and optical-based methods are still in the experimental stage. The near-field wireless charging technology utilizes electromagnetic induction for power transfer [5]. Magnetic induction-based charging is implemented using two induction coils: one coil generates an alternating electromagnetic field while the other receives power from the field and converts it into current to supply the device. This technology enables wireless power transfer to devices within 40 mm. Samsung wireless chargers [6] and Apple wireless charging pads [7], for instance, employ this technology. Magnetic-induction-based charging offers the advantage of transmitting power with an efficiency exceeding 90% [8]. However, the efficiency decreases significantly if the two coils are not properly aligned. Consequently, users cannot move their devices freely while using near-field charging technologies. The near-field wireless charging environment based on magnetic induction is predominantly implemented using the well-established Qi wireless charging standard, which defines the characteristics of power and communication information in wireless charging environments.

Considerable research has been conducted on side-channel formation and information extraction through power analysis in charging environments, particularly for mobile devices. For instance, QID [8] is a system that extracts features from the control scheme of an oscillator and power receiver and uses lightweight algorithms to identify Qi-compatible mobile devices in real time during wireless charging. Guo [9] presented a battery parameter identification method that considers the battery load in wireless charging systems to estimate the battery power shortage and full- charge state, which can be applied for battery state-of-charge estimation. Qing Yang [10] presented a method to analyze the web pages loaded by a smartphone when a charging cable without a data cable attached is provided by leveraging a charging power side-channel attack. EM-Surfing strategies [11] build a theoretical model to detect activities and tasks performed on a smartphone by exploiting electromagnetic induction effects in a wireless charging environment. In their study, the authors demonstrated a 99%, 96%, 94%, and 97% accuracy in inferring passwords, keystrokes, application information, and voice content, respectively. Similarly, using charger-Surfing [12], touch locations on smartphone and tablet touchscreens can be inferred through power-tracking attacks in the presence of USB charging cables with an average accuracy of 98.7%. Lastly, Lin Yan [13] presented an approach to infer user behavior through power analysis based side-channel attacks in the Android smartphone environment.

III. Experiments and Results

A. Experimental environments

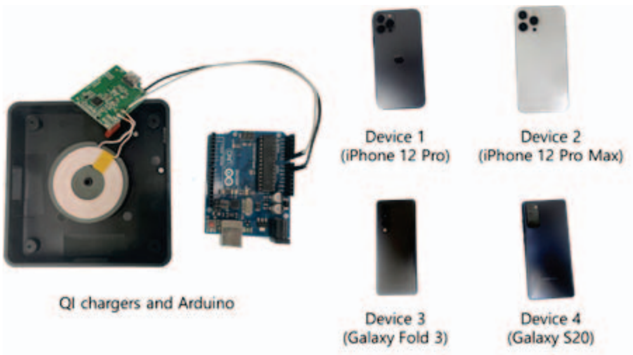


Fig. 2: Qi chargers and mobile devices used for our experiments

We used a cheap wireless charger that supports 5 W of power to perform our experiments. An Arduino was used to measure the voltage of the Qi charger, as shown in Fig.2. Experiments were conducted using four mobile devices. The purpose of our experiment was to quantify the voltage leaving the Qi charger to the mobile device and to classify the devices based on the measured voltage. Measurements were performed at 100 ms intervals

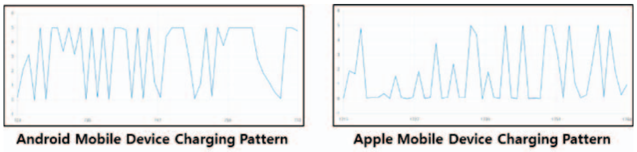


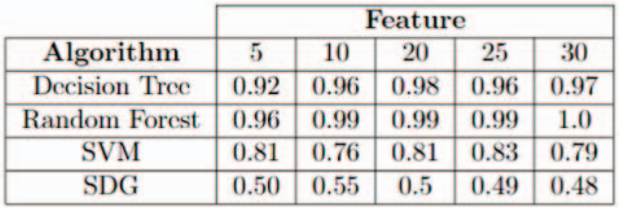
Fig. 3: Android and iOS smartphone voltage measurement

Fig.3 shows a graph of the voltage measured in the wireless charging environment for an Android OS-based Galaxy S22 Ultra mobile device and iOS-based iPhone 12 Pro Max mobile device. Hardware specifications and power consumption vary according to the type of mobile device and installed applications.

We used four machine learning algorithms to improve the accuracy of the voltage-based device classification. To overcome the limitation of using only one-dimensional feature information, we used the amount of voltage collected during x ms as a feature. For classification, we used 5, 10, 20, and 25 as feature labels, which correspond to the data collected for 500, 1000, 2,000, and 2,500 ms, respectively.

B. Evaluate the performance of device classification based on voltage measurement of Qi wireless chargers

TABLE I: Manufacturer-based classification accuracy (Apple and Samsung)

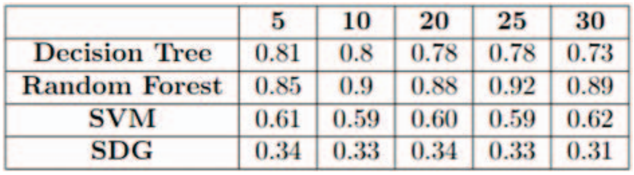


	Feature				
Algorithm	5	10	20	25	30
Decision Tree	0.92	0.96	0.98	0.96	0.97
Random Forest	0.96	0.99	0.99	0.99	1.0
SVM	0.81	0.76	0.81	0.83	0.79
SDG	0.50	0.55	0.5	0.49	0.48

Four experiments were conducted using voltage measurements obtained from the Qi wireless chargers. The first experiment classified mobile devices according to their manufacturer. We measured the voltages of Apple iPhone 12 Pro Max and Samsung Galaxy Fold while charging the batteries from 60% to 80%. The results are presented in Table I. The accuracy of the manufacturer-based classification increases proportionally with the number of features. Notably, the random-forest algorithm showed a 100% accuracy when the mobile device is charged for 3 s.

Although the accuracy of our results was high, we further investigated false-positive and false-negative rates. A low false positive rate ensures that we rarely misidentify a device manufacturer, whereas a low false negative rate confirms that we seldom overlook a correct identification. Analyzing these rates provides a more comprehensive understanding of the performance of our model and potential areas of improvement.

TABLE II: Different mobile devices classification accuracy



	5	10	20	25	30
Decision Tree	0.81	0.8	0.78	0.78	0.73
Random Forest	0.85	0.9	0.88	0.92	0.89
SVM	0.61	0.59	0.60	0.59	0.62
SDG	0.34	0.33	0.34	0.33	0.31

For our second classification experiment, we used two different models of Apple iPhone and two different models of Samsung Galaxy Phone, as the ones shown in Fig.2. Similarly, we measured the voltages of the four devices while the batteries were charging from 60% to 80%. The results of the classification are presented in Table II. The proposed method classified the four mobile devices with an accuracy of approximately 92% when measuring the voltage for 2.5 seconds. However, we observed that the classification accuracy decreased when the number of features exceeded 25. This decline can be attributed to an increase in false positives and negatives, which affects performance particularly when relying solely on one-dimensional voltage data. Further research will aim at addressing this issue to reduce the false positives and negatives rates.

IV. Use Case Scenarios and Research Directions

In this chapter, we present a method and its procedures to establish a secure user environment by constructing an authentication system utilizing the side-channel based device authentication scheme proposed in this study, within a paid wireless charging environment.

A. Paid Wireless Charging Service Environments

To utilize wireless charging services, users must provide upon the first usage the device charging patterns to the service provider and engage with the charging services after authentication, as shown in Fig.4.

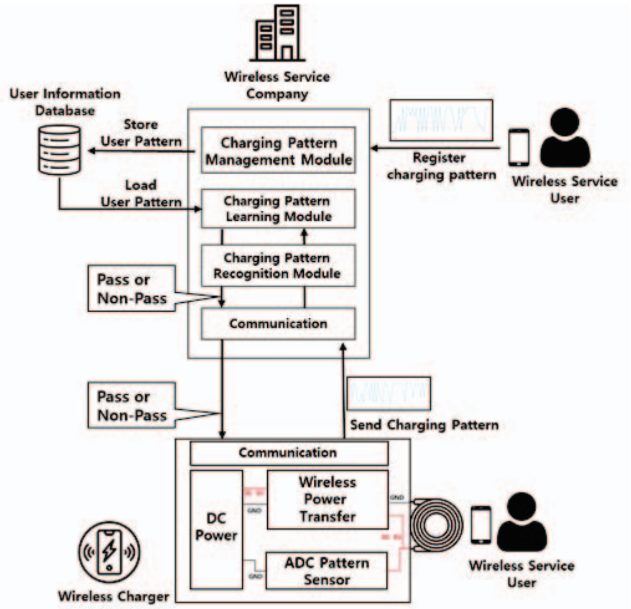


Fig. 4: Use case example of the proposed side-channel based device authentication technology

The provider then collates the device charging pattern, maps it to the associated user information, and archives it in a dedicated database. Stored charging patterns are continually processed by a charging pattern learning module, thereby constructing a dataset that can be used to identify the user's device accurately. The next time the user employs a wireless charging service for their mobile device, a brief charging process lasting 5 s is initiated. The voltage measurement signals acquired during this charging period are transmitted to the service provider, which authenticates the user registration based on the charging pattern data obtained from the wireless charger. Authenticated users are subsequently issued a continuous charging command for the wireless charger in use. Conversely, for unauthenticated users or potentially malicious entities, a charging termination command is dispatched to the pertinent wireless charger.

In summary, the wireless charger determines the next course of action, that is, whether to proceed with charging by implementing the command for a continuous power supply. Therefore, the proposed side-channel device authentication technology can respond to unauthorized charging attempts by both authenticated and unauthenticated users through real-time voltage consumption measurements.

B. Future Developments of Side-channel Device Authentication Systems

The operating landscape of mobile devices is intricate and incorporates several configurations and applications tailored for the specifics of each device, which results in unique power-consumption patterns. For example, a device running a resource-intensive application such as high-definition video streaming, along with several other background processes, presents a power consumption pattern that markedly diverges from that of a device operating a lightweight text-based application. For this reason, our future research will focus on power-consumption patterns during charging to enhance the precision and accuracy of device classification. By obtaining a comprehensive understanding of these patterns, we aim to streamline the authentication process to make it resilient and dependable by substantially improving device classification and overall authentication accuracy. Exploring the features of charging patterns will serve as a steppingstone towards more robust and reliable device authentication systems based on the information contained within the power consumption patterns of individual devices.

We also aim to conduct studies addressing security threats arising from vulnerabilities in the technological environment proposed in this study. To achieve this, we plan to analyze threat factors affecting the side-channel and research corresponding solutions.

V. Conclusion

The proposed side-channel based device authentication technology classifies devices based on voltage measurements obtained from a wireless charging transmitter in a near-field wireless charging environment. To ensure broad applicability, we extracted side-channel information from the voltage measurement of a Qi wireless charger without any protocol. The results of our experiments proved that the manufacturer of a mobile device can be classified with 100% accuracy based on the voltage of the Qi wireless charger alone. Moreover, our approach can discriminate among four devices of different models with an accuracy of 92%. In future research, we plan to implement a framework that analyzes the features of charging patterns in wireless charging service and authentication environments to establish a fast and cost-effective differentiation and authentication system.

Acknowledgment

This work was supported by the Institute of Information & Communications Technology Planning & Evaluation (IITP),(Project No. RS-2022-00165794, Development of a Multi-Faceted Collection-Analysis-Response Platform for Proactive Response to Ransomware Incidents, 30%), (Project No.2022-0-00701, 10%, Project No.RS-2023-00228996, 10%), the ICT R&D Program of MSIT/IITP, (Project No. 2021-0-01816, A Research on Core Technology of Autonomous Twins for Metaverse, South Korea, 10%), and a National Research Foundation of Korea (NRF), South Korea grant funded by the Korean government (Project No. RS-2023-00208460, 40%).

References

[1] Raffaele Bolla, Maurizio Giribaldi, Rafiullah Khan, and Matteo Repetto. Smart proxying: An optimal strategy for improving battery life of mobile devices. In *2013 International Green Computing Conference Proceedings*, pages 1–6. IEEE, 2013.

[2] Ranveer Chandra, Steve Hodges, Anirudh Badam, and Jian Huang. Offloading to improve the battery life of mobile devices. *IEEE Pervasive Computing*, 15(4):5–9, 2016.

[3] TNW Callum Booth. Wireless charging is cool, but won't replace cables anytime soon, 2019.

[4] Alexander S La Cour, Khurram K Afridi, and G Edward Suh. Wireless charging power side-channel attacks. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, pages 651–665, 2021.

[5] Young-Jin Park. Next-generation wireless charging systems for mobile devices, 2022.

[6] APPLE Electronics. Magsafe charger, 2019.

[7] Mohammad Haerinia and Reem Shadid. Wireless power transfer approaches for medical implants: A review. *Signals*, 1(2):209–229, 2020.

[8] Deliang Yang, Guoliang Xing, Jun Huang, Xiangmao Chang, and Xiaofan Jiang. Qid: Robust mobile device recognition via a multi-coil qi-wireless charging system. *ACM Transactions on Internet of Things*, 3(2):1–27, 2022.

[9] Yanjie Guo, Yuwang Zhang, Wenjie Zhang, and Lifang Wang. Battery parameter identification based on wireless power transfer system with rectifier load. *IEEE Transactions on Industrial Electronics*, 68(8):6893–6904, 2021.

[10] Qing Yang, Paolo Gasti, Gang Zhou, Aydin Farajidavar, and Kiran S. Balagani. On inferring browsing activity on smartphones via usb power analysis side-channel. *IEEE Transactions on Information Forensics and Security*, 12(5):1056–1066, 2017.

[11] Jianwei Liu, Xiang Zou, Leqi Zhao, Yusheng Tao, Sideng Hu, Jinsong Han, and Kui Ren. Privacy leakage in wireless charging. *IEEE Transactions on Dependable and Secure Computing*, 2022.

[12] Patrick Cronin, Xing Gao, Chengmo Yang, and Haining Wang. Charger-Surfing: Exploiting a power line Side-Channel for smartphone information leakage. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 681–698. USENIX Association, August 2021.

[13] Lin Yan, Yao Guo, Xiangqun Chen, and Hong Mei. A study on power side channels on mobile devices. In *Proceedings of the 7th Asia-Pacific Symposium on Internetware*, Internetware '15, page 30–38, New York, NY, USA, 2015. Association for Computing Machinery.