WPT Overview:

**General WPT:**

X. Lu, P. Wang, D. Niyato, D. I. Kim and Z. Han, "Wireless Charging Technologies: Fundamentals, Standards, and Network Applications," in *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1413-1452, Secondquarter 2016, doi: 10.1109/COMST.2015.2499783.

The authors provide a high-level overview of the technology surrounding wireless charging capabilities as well as a brief history of these developments. They also provide foreseen future routes for the technology to progress as well as proposed problems with the technology.

Q. Liu, K. S. Yildirim, P. Pawełczak and M. Warnier, "Safe and secure wireless power transfer networks: challenges and opportunities in RF-based systems," in IEEE Communications Magazine, vol. 54, no. 9, pp. 74-79, September 2016, doi: 10.1109/MCOM.2016.7565191.

The article discusses several vulnerabilities and ways WPT networks can be attacked. Harvested energy is very sensitive to environmental conditions – “the existence of a person in the deployment area can change the harvested energy considerably.” Handful of attacks – safety, charging, interference, spoofing, software, and monitoring attacks. Countermeasures should be implemented as small and energy-efficient protocols to ensure safe and secure energy transfer.

H. Zhang, N. Shlezinger, F. Guidi, D. Dardari, M. F. Imani and Y. C. Eldar, "Near-Field Wireless Power Transfer for 6G Internet of Everything Mobile Networks: Opportunities and Challenges," in IEEE Communications Magazine, vol. 60, no. 3, pp. 12-18, March 2022, doi: 10.1109/MCOM.001.2100702.

This article highlights opportunities and challenges arising from radiating near-field WPT. It also reviews design challenges and research directions from this paradigm including simultaneous operation with wireless communication, radiating waveform considerations, hardware aspects, and operation with typical antenna architecture. 6G wireless tech will use large-scale antenna arrays to communicate with user devices at bands offering higher bandwidth and energy transfer efficiency. Near-field refers to ranges of a few centimeters to several tens of meters.

**Technical Sources:**

Demodulating Communication Signals of Qi-Compliant Low-Power Wireless Charger Using MC56F8006 DSC by: Xiang Gao

The author provides a very technical report on the specifics of how messages are received and demodulated by the hardware and the software in the wireless charger with the MC56F8006 DSC. This solution to the problem of demodulation can be expounded upon and transferred to other DSC technology as claimed by the author in their conclusion.

**Attack Applications:**

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](https://sites.ucmerced.edu/files/wdu/files/2019infocom-codoc.pdf). In

IEEE INFOCOM 2019-IEEE Conference on Computer Communications. IEEE, 856-864

Wireless rechargeable sensor networks have seen improved performance in recent years due to wireless power transfer breakthroughs. These systems remain susceptible to Denial of Charge (DoC) attacks that have the ability to disrupt network reliability, network functionality, and possible trigger event loss. By manipulating and sending false charging request packets, the attack is able to disrupt the charging sequence and cause nodes to exhaust all of their energy before being recharged. The attack is limited by the Wireless Charging Vehicle (WCV), which has a larger charging capability than the maximum number of requests that can be generated. This lead too many tests resulting in minor to moderate network disruption with only a few causing significant impacts.

**Defense Applications:**

Priyankar Roychowdury. [n.d.]. [Trustable Digital Design Counter-Measures against Eavesdropping and Man-in-the-Middle Attacks in Qi Wireless Power Transfer Protocol](https://www.researchgate.net/publication/305041183_Trustable_Digital_Design_Counter-Measures_against_Eavesdropping_and_Man-in-the-Middle_Attacks_in_Qi_Wireless_Power_Transfer_Protocol) ([n.d.])

This article addresses the inherent authentication and confidentiality weaknesses associated with the Qi wireless power transfer protocol. Attackers can spoof packets to appear as if they are sent from the power receiver (authentication) and an attacker is able to intercept packets transmitted from both the receiver and transmitter as no encryption mechanism is employed by default (confidentiality). The article explores a hardware-based solution to this problem. To provide confidentiality a symmetric key cryptographic algorithm is proposed to be implemented in the power receiver and decrypted in the power transmitter. To address the authentication issue the usage of an authentication packet associated with each packet transmission is proposed as a way to verify communications as being valid.

J. Zhang, Z. Wang, X. Ji, W. Xu, G. Qu and M. Zhao, "Who is Charging My Phone? Identifying Wireless Chargers via Fingerprinting," in IEEE Internet of Things Journal, vol. 8, no. 4, pp. 2992-2999, 15 Feb.15, 2021, doi: 10.1109/JIOT.2020.3024572.

This journal discusses a potential solution for defending against wireless charging-based attacks. This potential solution is in the form of a digital fingerprint system for wireless charging devices. The hope is that the fingerprints will be able to verify the integrity of the messages sent in between charging devices to prevent malicious users from

**Additional Experiments:**

Ilter, Mehmet Cagri et al. “Information Harvesting for Far-Field Wireless Power Transfer.” ArXiv abs/2105.12838 (2021): n. pag.

This article introduces Information Harvesting for WPT systems. Information Harvesting aims to transmit information through existing WPT mechanisms without interfering power transfer. Only intended information receiver can decode the transmitted information after an information transfer process is initiated while energy harvesters continue the energy harvesting procedure. The key point here is designing a system where energy harvesters cannot detect ongoing information broadcasting since harvested energy is not affected by the information seeding mechanism.

Deliang Yang, Guoliang Xing, Jun Huang, Xiang Chang, and Xianfan Jian. 2020QIDL

[Identifying Mobile Devices via Wireless Charging Fingerprints](https://par.nsf.gov/servlets/purl/10168832). In 2020 IEE.ACN Fifth

International Conference on Internet of THings Design and Implementation (IoTDI).

IEEE, 1-13

QID or Qi Identification is a system that can identify Qi-compliant mobile devices while wirelessly charging in real-time. This system allows unique classification and identification of the device based on features such as the oscillator, coil, and controller of a Qi-compliant power receiver. This fingerprinting ability has tracking implications and for both tracking mobile users and providing location based services through WPT base stations.

J. Liu *et al*., "Privacy Leakage in Wireless Charging," in *IEEE Transactions on Dependable and Secure Computing*, doi: 10.1109/TDSC.2022.3173063.

This journal expands on the idea of using the changing amount of current detected from wireless charging to gain access to more personal information. The authors conducted experiments where they were able to achieve up to 99% accuracy in detecting a user’s passcode, keystrokes, app information, and speech content within the mobile device.

Charger-Surfing: Exploiting a Power Line Side-Channel for Smartphone Information Leakage Patrick Cronin, Xing Gao, and Chengmo Yang, University of Delaware; Haining Wang, Virginia Tech

The authors provide an in-depth explanation of a side-channel attack for USB charging mobile devices in order to acquire touchscreen specific data such as passwords. This requires a high sampling rate with an oscilloscope (hence the USB tap), however with a 125KHz sampling rate on voltage this could be achieved potentially through other means (i.e., wireless charging). Through adept training techniques the authors claimed an average greater than 90% prediction of button press and order on a lock screen.

La Cour, Alexander S., Khurram K. Afridi, and G. Edward Suh. "Wireless charging power side-channel attacks." *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*. 2021.

This journal describes experiments that demonstrate how vulnerable modern day mobile devices are to attacks via wireless charging. Specifically, the authors discuss how the amount of current being drawn from the charger can be used to determine which applications are being used by the mobile device. It also discusses the weaknesses of such attacks. For example, the longer a device is being used, the less accurate the estimate is. Additionally, when a device is on low battery, the estimates are the least accurate