Power-Positive Networking Using Wireless Charging: Protecting Energy Against Battery Exhaustion Attacks

Sang-Yoon Chang
University of Colorado Colorado Springs
Colorado Springs, CO
schang2@uccs.edu

Sristi Lakshmi Sravana Kumar
Advanced Digital Sciences Center
Singapore, Singapore
sravana.s@adsc.com.sg

Bao Anh N. Tran
Advanced Digital Sciences Center
Singapore, Singapore
baoanh.t@adsc.com.sg

Sreejaya Viswanathan
Advanced Digital Sciences Center
Singapore, Singapore
sreejaya.v@adsc.com.sg

Younghee Park
San Jose State University
San Jose, CA
younghee.park@sjsu.edu

Yih-Chun Hu
University of Illinois at Urbana-Champaign
Urbana, IL
yihchun@illinois.edu

ABSTRACT

Energy is required for networking and computation and is a valuable resource for unplugged embedded systems. Energy DoS attack where a remote attacker exhausts the victim's battery by sending networking requests remains a critical challenge for the device availability. While prior literature proposes mitigation- and detection-based solutions, we propose to eliminate the vulnerability entirely by offloading the power requirements to the entity who makes the networking requests. To do so, we build communication channels using wireless charging signals, so that the communication and the power transfer are simultaneous and inseparable, and use the channels to build power-positive networking (PPN). PPN also offloads the computation-based costs to the requester, enabling authentication and other tasks considered too power-hungry for battery-operated devices. Furthermore, because we use the charging signal for bidirectional networking, the design requires no additional hardware beyond that for wireless charging. In this paper, we present PPN, implement a Qi-compatible prototype, and use the prototype to analyze the performance.

1 INTRODUCTION

Wireless networking and wireless power transfer enable device connectivity in broad applications by letting the devices be free of cables and are the driving forces behind the Internet of Things (IoT). For example, both technologies are used in mobile phones, implantable medical devices, wearable devices, sensors for environment and structure monitoring, electric vehicles, and so on. For unplugged devices which operate on batteries and do not have a stable power supply source, energy (generally required for networking, computations, and other operations of electronic devices) is a valuable resource and its constraint is often the fundamental bottleneck to the system design (e.g., the size of the battery becoming the dominating factor of the physical size of the devices or requiring frequent and periodic power transfer). Thus, researchers in electronics and computing are vigorously pursuing to advance the energy constraint/use of networked devices.

While the experts in electronics and computing understand that energy is a valuable resource and focus on optimizing and increasing the efficiency of energy use, transfer, and storage, there has been relatively little effort to protect the integrity of the energy use. *Energy denial-of-service* (energy DoS) occurs when the attacker exhausts the battery by purposely draining the energy, thus making the device incapable of its operations. Such threats can be carried out by a compromised component of the system (e.g., malware) which triggers intra-host computations or performs them itself; alternatively, an easier attack that does not require a priori system compromise is merely engaging the device by sending repeated network requests via wireless communications (in an otherwise legitimate manner), e.g., sleep deprivation attacks [26] on wireless sensor networks.

We focus on the latter networking-based energy DoS with an external attacker (our work also addresses the processing tasks, such as authentication, associated with the networking session). Such attack can be especially devastating for embedded and sensor device availability because such networking events are designed to occur sporadically, e.g., for system maintenance and upgrade, and the power is budgeted accordingly (much lower than the power budget for the devices' primary functions of sensing and control) [12, 26]. Prior solutions assume that receiving network inputs consumes the device's power (which assumption is also pervasively established in the general energy-saving research in a non-security context, e.g., [8, 19, 33]) and thus focus on detection and mitigation of such attacks; Section 5.1 reviews such literature in energy DoS in greater details. However, we take a fundamentally different approach to addressing energy DoS and eliminate the attack entirely; we break the assumption that network inputs result in net-negative energy to the receiver and build a networking channel where the network inputs that have been received through that channel increases the device's energy. To the best of our knowledge, this is a novel approach.

We build communication on the wireless charging signal, so that the power transfer and the information transfer are coupled and occur simultaneously. For consistency, and because we develop

WiSec '17 , Boston, MA, USA

978-1-4503-5084-6/17/07…$15.00
DOI: 10.1145/3098243.3098265

Baseline	Awake	Paired	Receive	Transmit	Authentication
1.144 (1x)	1.348 (1.178x)	1.347 (1.177x)	1.419 (1.240x)	1.631 (1.431x)	1.85 (1.617x)

Table 1: The power costs in Watt (W) depending on the networking states: Baseline (networking is disabled), Awake (networking is enabled), Paired (the requester is identified and resolved), Receive, Transmit, and Authentication. The values inside of the parentheses are the power cost gains with respect to the Baseline.

bidirectional communication, we call the node that is actively sending networking requests the *requester* (possibly malicious and the subject of the energy DoS) and the node that receives those network requests the *receiver* (energy-constrained and possibly under the energy-DoS attacks). Because we modulate data information using the charging signal, our design requires minimal hardware (beyond that for wireless charging) on both the requester and the receiver and no power consumption on the receiver (in fact, the receiver is actually being charged and replenishing its battery while receiving the networking requests). Even though our solution (providing practically free communication and networking channel) can be applied in general contexts, we focus on its security application and show the effectiveness against energy DoS in this paper.

We construct *power-positive networking* (PPN), so that all the power cost is offloaded to the requester and the net-power of the receiver increases after the networking/authentication operations, by building communication channels on the power subsystem frontend, because the networking operations using the RF subsystem frontend consume power. PPN is thus orthogonal to the networking operations from the traditional RF-based networking subsystem, for example, it does not interfere with the receiver initiating communications via RF for emergency communications.

2 ENERGY DENIAL-OF-SERVICE THREAT

2.1 Threat Model

We consider a malicious and external attacker. The attacker is *malicious* as its sole goal is to expend the energy of the victim node as much as possible, and it is *external* as it resides outside of the victim receiver and interacts with the victim receiver via communications. Thus, the attacker repeatedly sends networking requests to the receiver, triggering power consumption on the receiver. The attack is generic and can apply to any networking protocol; independent of the lower-layer details, the attacker merely activates the networking and continues sending request packets.

In the Resurrecting Duckling model [26] (designed for general wireless ad hoc networking), attacker's request triggers "distinct auxiliary function" which is triggered externally and supposed to occur sporadically; in contrast, the cost of the primary functions (e.g., of regularly updating the authority) is relatively fixed and accounted for at the system design stage. The attackers' requests are otherwise legitimate (e.g., the attacker is intelligent enough to learn the networking protocol by Kerchkoff's principle) and the receiver cannot distinguish between a legitimate requester and an attacker (e.g., we do not rely on attacker detection, which are described in Section 5.1).

We do not consider the cases of the requester being subjected to attack, and the networking session initiator assumes power cost. The requester acts as the power transfer source in PPN and thus its power is inherently cheaper (more abundant) than the receiver's.

2.2 Threat Impact

To motivate our work, we study the energy DoS impact on the receiver and analyze the networking costs for communicating with the requester using more traditional RF-based networking channels (which is fundamentally different from our proposed scheme). In particular, we analyze the networking cost and the authentication cost; the networking corresponds to establishing a connection, receiving the requests, and transmitting other packets (e.g., if the requester asks for transmitting or relaying), and the digital authentication accounts for verifying the requester entity from the claimed identity, which is a necessary step before further processing the requests in secure networking and computing.

We use a Raspberry Pi 3 Model B, which is representative of physically smaller embedded system applications, and experiment using IEEE 802.11n (WiFi) networking protocols, which capability is already built-in on the Raspberry Pi board. For authentication, AES-CCM-128 is used due to its use in IoT-friendly Zigbee [13] and wireless body area network [16]. For measuring power, we physically tap the power supply cord of the platforms and injected a multimeter, measuring the current that is drawn from the power source; it thus accounts for the cost of the entire system.

The networking cost measurements and the authentication cost measurement are in Table 1. For reference, we define *Baseline* costs as when the networking (both communications and authentication) is disabled; this accounts for the power costs from the rest of the operations un-related to networking. We separate the networking and the authentication costs; while networking incurred costs at both the networking frontend and the backend processor, the authentication's was limited to the backend processor. Networking and authentication can occur simultaneously and, if so, the costs are additive.

Because power-conscious applications optimize the power use in general, significantly lowering the Baseline cost, and because we make no such power-optimization effort at the platforms in our experiments, the threat impact values here are conservative, and the impact on power-conscious applications will be much more severe. Even with our conservative measurements, the additional power costs of the receiver is significant; for example, against a straightforward threat from a requester who keeps sending packets with legitimate packet headers (so that the receiver processes authentication before dropping the packets), the power increases by 85.7% (the aggregate cost for Receiving and Authentication). Our observations agree with Martin et al. [20] in that, for general-purpose computers (which we use here), the cost for networking does not outweigh that of the rest of the system. However, for sensor/embedded applications for dedicated tasks, RF-based networking dominates the power consumptions [17, 20], and energy DoS threat can cut the battery life by one to two orders of magnitude [15].

The actual threat impact will heavily depend on the application context and the system implementation. We purposely distance ourselves from a particular application or the system backend and design our prototype frontend to be modular to the backend processor, as described in Section 4.1.

3 POWER-POSITIVE NETWORKING

3.1 PPN Overview

Our scheme offers power-positive networking (PPN) where the receiver node's power cost is offloaded to the requester (who initiates the networking session) by coupling the power and the information transfer process and making them inseparable. PPN is built in three parts. First, the communication from the requester to the receiver is built on wireless charging signals, which are generated by the requester. Second, the requester's signal continues until the receiver has sufficient power to perform the relevant networking tasks, such as authentication; the receiver withholds transmitting the session-ending acknowledgement back to the requester until then. Third, the communication for the feedback (from the receiver to the requester) uses backscattering with passive components and is power-free.

To accommodate lossy environments, there are three types of feedback responses that the receiver makes: the initial feedback for establishing connection, the periodic feedback for relaying the networking/power-transfer status (as is typical in power transfer process), and the session-ending acknowledgment for the networking request. Only when the requester delivers sufficient power to perform the networking tasks (communication, authentication, and so on) to the receiver, the receiver sends the last acknowledgement feedback to the requester and further process the networking packets beyond the networking stack. In other words, the requester's request does not get accepted and processed if it fails to deliver sufficient amount of power. In the case of a malicious requester, it either needs to pay off the required energy cost to the receiver or cannot engage the victim receiver. Therefore, PPN both eliminates the communication cost and powers the relevant intra-host networking-relevant computation operations such as the requester authentication; such computation has been a challenge in the general context of resource-constrained networking systems and is particularly devastating in the presence of energy DoS.

3.2 PPN Applications and Scope

PPN can prevent energy DoS in many applications (as long as the application device supports wireless power transfer and storage/battery), because it requires minimal hardware and avoids power-consuming radio hardware at the frontend (e.g., the receiver does not need to generate its own signal) and is only enabled when the possibly malicious requester initiates the networking by generating the charging signal (e.g., it does not interfere with the receiver initiating networking). For example, for mobile or wearable applications, our scheme provides a networking channel that the nodes can rely on when the battery is running low or energy DoS is detected; for wireless sensor networks, our solution provides a separate networking channel even when the node is *sleeping* and the RF subsystem is disabled; and for devices that traditionally have not supported networking (but may want to for emerging IoT applications), it offers a communication channel with minimal hardware overhead and practically no power consumption (net-positive power). Also, our scheme does not interfere with the receiver initiating networking, e.g., emergency communications.

PPN operates within the wireless charging distance range, which is in the order of centimeters and is comparable to the near-field communication (NFC) range. However, in contrast to NFC/RFID (which is further discussed in Section 5.2), PPN has a greater focus on power-active devices utilizing such near-field data networking. Example applications are implantable device networking, cordless token/key exchange for mobile/wearable devices, and enabling IoT connectivity for systems with no RF hardware.

Because PPN has a shorter range than that of a typical RF-based data transfer, we recommend using it in conjunction with the more traditional RF-based networking in *normal* situations when the battery is relatively full and is not draining in an abnormally fast rate; in this case, the primary control and sensing functionalities of the embedded system and the networking and cryptographic computations share the same energy resource (battery) and directly compete with each other. However, when the battery is running low or the receiver detects abnormal battery-draining behavior (e.g., building on prior work in Section 5.1), the receiver can opt for PPN only and turn off the traditional RF networking subsystem; otherwise, our analyses and experiments in Section 2.2 show that repeated networking sessions (e.g., from energy DoS threat) can drain the battery quickly.

The design for such decision engine triggering PPN-only mode (investigating threshold for low battery and algorithms for abnormal-behavior detection, e.g., prior work in Section 5.1) depends heavily on the embedded applications and how critical the networking is compared to the control/sensing functionalities of the device. PPN design is orthogonal to such decision engine and can actually be used broadly across applications supporting wireless charging (more specifically, our prototype is compatible to Qi technology which is widely used in mobile, wearable, and implantable applications), and we leave the application-specific investigations as future work.

3.3 PPN Implementation

PPN provides simultaneous power and data transfer. For *power transfer*, PPN builds on wireless charging, invented in the 20th century [27]. Wireless charging uses inductive coupling to transfer power from one circuit to another. Since current (electric field propagation) generates electromagnetic field and vice versa, running AC current on one node generates change in magnetic flux around it and, in turn, generates alternating current on a nearby node. For the devices being charged, this alternating current is used to store the electrical power on a battery.

For *communication*, we build on the power transfer design and add information entropy by varying the charging parameters which affect the inductive coupling. The bidirectional communication uses the same signal used for power transfer. For the forward-direction from the requester to the receiver, we vary the frequency of the signal, i.e., frequency-shift keying (FSK). For for the reverse-direction communication from the receiver to the requester, we use backscattering by varying the electrical properties of the receiver, which affect the inductive coupling field and thus the electrical field amplitude on the transmitter, i.e., amplitude-shift keying (ASK). Since the modulations operate in orthogonal dimensions (one in frequency/phase and the other in amplitude), the communications can coexist (enabling full duplex, which development is left for future

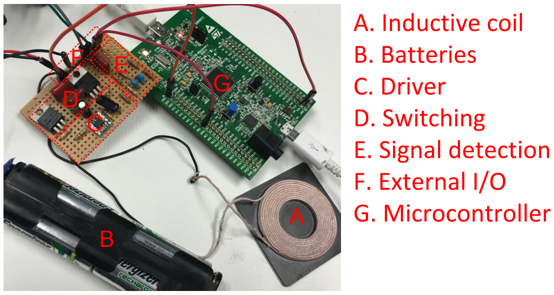

Figure 1: The transmitter prototype (soldered)

work). In addition to being orthogonal to backscattering, we use frequency modulation for requester-to-receiver communication due to its channel noise resistance.

Most of the communication circuit overlaps with the power transfer circuit as communication piggybacks on the charging signal. The only additions to the power transfer design are the following components (comprised only with passive elements): the backscattering circuit and the voltage divider and translator/shifter (to make the receiving signal compatible to the system backend) at the receiver side and the band-pass filter and the envelope detector at the requester side for receiving the receiver-to-requester communication. The rest of the logic is at the digital level and implemented at the device backend.

4 EVALUATION

We build our prototype as described in Section 3.3. Our parameter choices are driven to minimally impact the power transfer due to its importance in PPN. Communication is also affected by the parameter choices. More specifically, communication performance monotonically increases as the frequency separation between the FSK signals increases and as the data communication rate decreases; these phenomena agree with the prior work in wireless communications/networking, and we omit the results in this paper.

In our prototype, we use the center frequency of 155kHz (which complies with the Qi standard and maximizes the power transfer) with a frequency separation of 1kHz (which keeps the power transfer within 1.9% of the optimal performance). For the communication rate, we use 7kbps for the requester-to-receiver communication and 2kbps for receiver-to-requester communication.

4.1 Modular Design to Backend Processor

Our PPN prototype implementation supports modular design to the system backend and can be applied in various applications. We test and verify the charging/communication prototype's functionality and the compatibility to Raspberry Pi, a microcontroller (STM32F4 Discovery board), Samsung Galaxy phone and a laptop. Figure 1 displays the transmitter prototype with the microcontroller and the charging coil (which acts like an antenna for networking). We focus on our prototype's performance when using the Raspberry Pi for processing in Section 4.2 and Section 4.3.

4.2 Reliable Communication Range

As the distance between the requester and the receiver increases, PPN's performance in both power transfer and data transfer decrease. More specifically, for power transfer, the power transfer efficiency (the ratio between the received power and the transmitted power) and the received power itself monotonically decrease in distance. For data transfer, the signal-to-noise ratio (SNR) decreases in distance while the bit error rate (BER) increase in distance (the higher the signal quality the lower the error probability, i.e., higher communication reliability); these hold for both FSK-modulated requester-to-receiver communication and backscattering-based receiver-to-requester communication.

We define the *reliable communication range* to be when the reliability performance limits the BER to 2% (such communication range can be controlled by adding redundancy in error control, e.g., error correction code, to allow more bit errors while still decoding the message). Taking measurements over 0.5cm intervals, our prototype's reliable communication range is 15cm for the requester-to-receiver communication and 2.5cm for the receiver-to-requester communication. The receiver-to-requester communication range is much shorter than the requester-to-receiver communication range because the reverse-direction communication for feedback uses backscattering, which relies on the reflection of the forward-direction signal generated by and transmitted from the requester. Therefore, the bottleneck communication is the reverse-direction receiver-to-requester communication, and it limits the reliable communication range to be within 2.5cm. At the end of our reliable communication range, i.e., when the receiver is 2.5cm away from the requester, the power efficiency (the ratio of the received power measured at the receiver and the transmitted power measured at the transmitter) is 10%.

In the more typical case when the receiver is 0.5cm away from the requester (which is the target distance for many wireless charging prototype and product design), the power efficiency is 67% and there is no bit error observed for communications. Section 4.3 measures the PPN cost when the requester-receiver distance is 0.5cm. Our prior work in Cognitive Wireless Charger for improving power transfer [5] provides greater details about our prototype and power transfer performance (CWC algorithm is disabled here).

4.3 Security Cost in Time Delay

PPN is effective in preventing energy DoS, as it forces the attacker to provide the very resource (energy) that it is targeting for DoS. However, PPN can cause time delay in accepting legitimate network requests, because the receiver does not process the requests until it receives sufficient power from the requester, as described in Section 3.1.

We conduct experiments when PPN is enabled and the receiver simultaneously performs various RF-based networking tasks, including Baseline (disabling RF), Awake (enabling RF but being idle), Paired (after identifying and resolving the requester), Receiving, Transmitting, and Authentication. In contrast, Section 2.2 measured the power consumption with no PPN.

We compute the delay of PPN using the power consumption and the power delivery measurements when the receiver is processed by a Raspberry Pi and it is 0.5cm away from the requester; PPN provides stable power supply across different networking tasks and the power delivery fluctuate only slightly ranging from 1.107W to 1.109W. The receiver only asks for the cost incurred by the requester's networking/authentication requests, e.g., its main purpose is not to replenish its battery. Figure 2 presents the delay of using our prototype for PPN, and the authentication cost is additive to

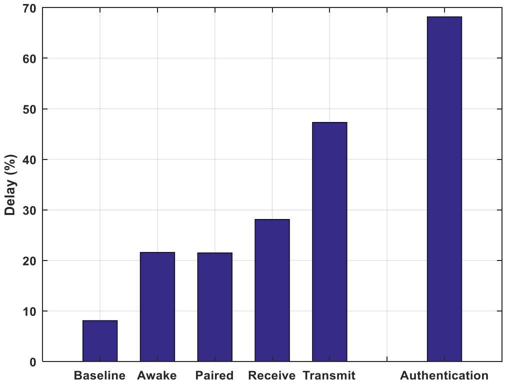

Figure 2: Security cost (time delay) of PPN. The delay is in percentage (%) and with respect to real-time processing. For example, if the delay is 50%, then for every task that takes 1 second, PPN takes 1.5 seconds.

the other RF networking tasks if it is triggered simultaneously (e.g., receiving and authenticating a packet simultaneously).

When energy is critical, e.g., as described in Section 3.2, the receiver can only rely on PPN (and no RF) to listen for networking. In such case, the PPN cost corresponds to Baseline (8.1%) or, if authentication is also required, Baseline/Authentication (76.2%). The Baseline cost being greater than 0% indicates that merely having Raspberry Pi on is too expensive to be charged using our current prototype, as 0% corresponds to real-time processing with no delay.

Power optimization in both transfer and use will lower these costs and help to support PPN in real-time with no delay cost. Such cost will be even lower in embedded system applications designed for power efficiency (as opposed to having a general-purpose device at the backend), in which case the excessive power (beyond that used for networking) can be used to charge the battery. We leave prototype optimization and experiments on power-sensitive systems for future work.

5 RELATED WORK

5.1 Energy Denial-of-Service

The remote networking-based energy DoS threat[1] has garnered greater attention in computer security with the increased connectivity and networking capabilities of the devices, e.g., IoT, and will become even more devastating in wireless sensor network applications [2, 20, 24], which typically have much simpler hardware architecture than other computing devices and the overall power consumption is dominated by the RF subsystem.

Proposed solutions against energy DoS can be divided into the following classes: *detection* based on energy-monitoring [4, 20, 21], *mitigation* based on lightweight authentication [9, 20] and sleeping-based medium access control (MAC) [3] (which is vulnerable [23] especially against an attacker who knows the MAC-layer information).

The closest to our approach in defending against energy DoS is done by Halperin et al. [12], which not addresses the remote vulnerabilities of deployed implantable medical devices but also presents *zero-power* cyber-defense designs relying on RF-energy harvesting. However, their definition of zero-power differs from ours in that they focus only on the power cost of their responsive security designs of authentication and notification (which designs are modular to the rest of the system) and separates those power from that coming from the system's primary battery dedicated for the device's body control functions of pacing and defibrillation. Our work shows that the cost of interfacing and triggering such defenses can also be non-trivial under energy DoS attacks in Section 2.2; the mere networking functions of pairing and receiving packets, even if dropping those packets immediately without further processing, consumes additional power and can be used for energy DoS by a radio-equipped attacker. Therefore, we take a fundamentally different approach and build networking on power transfer; greater power efficiency enables our work to power the entire system including control, networking, and security.

5.2 Backscattering and RFID

Backscattering modulates the reflected signal for data communication, i.e., the signal source receives the signal reflection with the modulated data. Since the node transmitting the data message does not need to generate its own signal, backscattering is especially helpful when the node is power constrained, e.g., RFID tags.

The receiver-to-requester communication component of our scheme builds on backscattering. However, in contrast to more conventional backscattering technologies such as RFID, we use the power transfer signal and not the RF signal, actively add power to the receiver during the communications, and target embedded systems with power-active components (whose operations rely on the power drawn from the battery).

Others have also used the power subsystem for backscattering communications to avoid additional networking hardware [10, 28] but not for simultaneous power and data transfer (as PPN does); they provide time-interleaved power transfer control communication in order to increase the power transfer efficiency.

5.3 Combining Networking and Power Transfer

Prior to our work, researchers designed bidirectional communication using charging signals in non-security contexts [7, 18]. Other work adopted communication-inspired concepts to boost the efficiency of wireless power transfer, e.g., MIMO can be used for power transfer improvement [14, 30].

Researchers also explored using the networking signal for power transfer. Prior literature uses ambient radio-frequency (RF) signals to harvest power [12, 25, 29]. While it may become useful for sustainable and long-distance power transfer, the technology targets battery-less applications and is too early to determine its practicality, especially with the low power efficiency [22] (even with respect to the wireless charging standard [1]). So far, power transfer based on RF radiation has not been adopted for standards for consumer electronics, and it is rather unclear how they can comply with FCC regulations. In contrast, inductive-coupling based power transfer is

[1] In addition to DoS attack on the device's energy, prior work in wireless/mobile network security includes DoS attacks on networking/channel resources, preventing channel access by sending channel control requests (e.g., [6, 11]), by jamming, and so on. Our work focuses on energy/battery resource.

already standardized for wireless power transfer (e.g., the Qi standard by Wireless Power Consortium [31] and Rezence standard by Alliance for Wireless Power (A4WP)) and has been deemed safe and compliant to FCC standards [32]. Thus, we use inductive coupling signals and not RF signals.

6 CONCLUSION

We build power-positive networking (PPN) and use it to dispatch energy DoS threat. By building communications on wireless charging signals, our scheme is not only lightweight in hardware but also replenishes the receiving node's energy, thwarting energy DoS from its vulnerability surface. Our prototype offers 7kbps communication in the requester-to-receiver direction and 2kbps communication in the reverse direction while using near-field Qi-standard-compatible wireless charging.

ACKNOWLEDGMENTS

This study is supported by the research grant for the Human-Centered Cyber-physical Systems Programme at the Advanced Digital Sciences Center from Singapore's Agency for Science, Technology and Research (A*STAR).

REFERENCES

[1] Rhett Allain. 2015. Wi-Fi Charging Works, But it Can'fit Really Power Your Phone. *Wired* (June 2015). http://www.wired.com/2015/06/power-wifi-isnt-think/

[2] R. Anderson, Haowen Chan, and A. Perrig. 2004. Key infection: smart trust for smart dust. In *Network Protocols, 2004. ICNP 2004. Proceedings of the 12th IEEE International Conference on.* 206–215. DOI: https://doi.org/10.1109/ICNP.2004.1348111

[3] M. Brownfield, Yatharth Gupta, and N. Davis. 2005. Wireless sensor network denial of sleep attack. In *Information Assurance Workshop, 2005. IAW '05. Proceedings from the Sixth Annual IEEE SMC.* 356–364. DOI: https://doi.org/10.1109/IAW.2005.1495974

[4] T. K. Buennemeyer, M. Gora, R. C. Marchany, and J. G. Tront. 2007. Battery Exhaustion Attack Detection with Small Handheld Mobile Computers. In *Portable Information Devices, 2007. PORTABLE07. IEEE International Conference on.* 1–5. DOI: https://doi.org/10.1109/PORTABLE.2007.35

[5] S.Y. Chang, S. Kumar, and Y.C. Hu. 2017. Cognitive Wireless Charger: Sensing-Based Real-Time Frequency Control For Near-Field Wireless Charging. In *IEEE International Conference on Distributed Computing Systems (ICDCS) 2017.*

[6] S. Y. Chang, Y. C. Hu, and Z. Liu. 2015. Securing wireless medium access control against insider denial-of-service attackers. In *Communications and Network Security (CNS), 2015 IEEE Conference on.* 370–378. DOI: https://doi.org/10.1109/CNS.2015.7346848

[7] W.P. Choi, W.C. Ho, X. Liu, and S.Y.R. Hui. 2010. Bidirectional communication techniques for wireless battery charging systems & portable consumer electronics. In *Applied Power Electronics Conference and Exposition (APEC), 2010 Twenty-Fifth Annual IEEE.* 2251–2257. DOI: https://doi.org/10.1109/APEC.2010.5433550

[8] Girisha De Silva, Binbin Chen, and Mun Choon Chan. 2016. Collaborative Cellular Tail Energy Reduction: Feasibility and Fairness. In *Proceedings of the 17th International Conference on Distributed Computing and Networking (ICDCN '16).* ACM, New York, NY, USA, Article 25, 10 pages. DOI: https://doi.org/10.1145/2833312.2833451

[9] R. Falk and H. J. Hof. 2009. Fighting Insomnia: A Secure Wake-Up Scheme for Wireless Sensor Networks. In *Emerging Security Information, Systems and Technologies, 2009. SECURWARE '09. Third International Conference on.* 191–196. DOI: https://doi.org/10.1109/SECURWARE.2009.36

[10] Xiang Gao. 2013. *Demodulating Communication Signals of Qi-Compliant Low-Power Wireless Charger Using MC56F8006 DSC.* Technical Report. Freescale Semiconductor.

[11] Nico Golde, Kevin Redon, and Jean-Pierre Seifert. 2013. Let Me Answer That for You: Exploiting Broadcast Information in Cellular Networks. In *Presented as part of the 22nd USENIX Security Symposium (USENIX Security 13).* USENIX, Washington, D.C., 33–48. https://www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/golde

[12] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel. 2008. Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. In *2008 IEEE Symposium on Security and Privacy (sp 2008).* 129–142. DOI: https://doi.org/10.1109/SP.2008.31

[13] M. Healy, T. Newe, and E. Lewis. 2009. Security for wireless sensor networks: A review. In *Sensors Applications Symposium, 2009. SAS 2009. IEEE.* 80–85. DOI: https://doi.org/10.1109/SAS.2009.4801782

[14] Jouya Jadidian and Dina Katabi. 2014. Magnetic MIMO: How to Charge Your Phone in Your Pocket. In *Proceedings of the 20th Annual International Conference on Mobile Computing and Networking (MobiCom '14).* ACM, New York, NY, USA, 495–506. DOI: https://doi.org/10.1145/2639108.2639130

[15] Noboru Kamijoh, Tadanobu Inoue, C. Michael Olsen, M. T. Raghunath, and Chandra Narayanaswami. 2001. Energy Trade-offs in the IBM Wristwatch Computer. In *Proceedings of the 5th IEEE International Symposium on Wearable Computers (ISWC '01).* IEEE Computer Society, Washington, DC, USA, 133–. http://dl.acm.org/citation.cfm?id=580581.856575

[16] M. Kaur and S. Singh. 2015. A Study on Networking Techniques of WBAN System. In *International Research Journal of Engineering and Technology(IRJET).* 80–85.

[17] Bryce Kellogg, Vamsi Talla, Shyamnath Gollakota, and Joshua R. Smith. 2016. Passive Wi-Fi: Bringing Low Power to Wi-Fi Transmissions. In *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16).* USENIX Association, Santa Clara, CA, 151–164. https://www.usenix.org/conference/nsdi16/technical-sessions/presentation/kellogg

[18] U.K. Madawala, J. Stichbury, and S. Walker. 2004. Contactless power transfer with two-way communication. In *Industrial Electronics Society, 2004. IECON 2004. 30th Annual Conference of IEEE*, Vol. 3. 3071–3075 Vol. 3. DOI: https://doi.org/10.1109/IECON.2004.1432302

[19] Justin Manweiler and Romit Roy Choudhury. 2011. Avoiding the Rush Hours: WiFi Energy Management via Traffic Isolation. In *Proceedings of the 9th International Conference on Mobile Systems, Applications, and Services (MobiSys '11).* ACM, New York, NY, USA, 253–266. DOI: https://doi.org/10.1145/1999995.2000020

[20] Thomas Martin, Michael Hsiao, Dong Ha, and Jayan Krishnaswami. 2004. Denial-of-Service Attacks on Battery-powered Mobile Computers. In *Proceedings of the Second IEEE International Conference on Pervasive Computing and Communications (PerCom'04) (PERCOM '04).* IEEE Computer Society, Washington, DC, USA, 309–. http://dl.acm.org/citation.cfm?id=977406.978701

[21] Alessio Merlo, Mauro Migliardi, and Luca Caviglione. 2015. A survey on energy-aware security mechanisms. *Pervasive and Mobile Computing* 24 (2015), 77 – 90. DOI: https://doi.org/10.1016/j.pmcj.2015.05.005 Special Issue on Secure Ubiquitous Computing.

[22] John Perzow. 2015. Measuring Wireless Charging Efficiency in the Real World. *WPC Trade Conference* (November 2015). https://www.wirelesspowerconsortium.com/data/downloadables/1/5/2/7/john-perzow-efficiency-of-wireless-charging.pdf

[23] D. Raymond, R. Marchany, M. Brownfield, and S. Midkiff. 2006. Effects of Denial of Sleep Attacks on Wireless Sensor Network MAC Protocols. In *Information Assurance Workshop, 2006 IEEE.* 297–304. DOI: https://doi.org/10.1109/IAW.2006.1652109

[24] S. Slijepcevic, M. Potkonjak, V. Tsiatsis, S. Zimbeck, and M. B. Srivastava. 2002. On communication security in wireless ad-hoc sensor networks. In *Enabling Technologies: Infrastructure for Collaborative Enterprises, 2002. WET ICE 2002. Proceedings. Eleventh IEEE International Workshops on.* 139–144. DOI: https://doi.org/10.1109/ENABL.2002.1030000

[25] Joshua R. Smith, Alanson P. Sample, Pauline S. Powledge, Sumit Roy, and Alexander Mamishev. 2006. A Wirelessly-powered Platform for Sensing and Computation. In *Proceedings of the 8th International Conference on Ubiquitous Computing (UbiComp'06).* Springer-Verlag, Berlin, Heidelberg, 495–506. DOI: https://doi.org/10.1007/11853565_29

[26] Frank Stajano and Ross J. Anderson. 2000. The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks. In *Proceedings of the 7th International Workshop on Security Protocols.* Springer-Verlag, London, UK, UK, 172–194. http://dl.acm.org/citation.cfm?id=647217.760118

[27] N. Tesla. 1914. Apparatus for transmitting electrical energy. (Dec. 1 1914). http://www.google.com/patents/US1119732 US Patent 1,119,732.

[28] D. van Wageningen and T. Staring. 2010. The Qi wireless power standard. In *Power Electronics and Motion Control Conference (EPE/PEMC), 2010 14th International.* S15–25–S15–32. DOI: https://doi.org/10.1109/EPEPEMC.2010.5606673

[29] R. Vyas, H. Nishimoto, M. Tentzeris, Y. Kawahara, and T. Asami. 2012. A battery-less, energy harvesting device for long range scavenging of wireless power from terrestrial TV broadcasts. In *Microwave Symposium Digest (MTT), 2012 IEEE MTT-S International.* 1–3. DOI: https://doi.org/10.1109/MWSYM.2012.6259708

[30] B.H. Waters, B.J. Mahoney, V. Ranganathan, and J.R. Smith. 2015. Power Delivery and Leakage Field Control Using an Adaptive Phased Array Wireless Power System. *Power Electronics, IEEE Transactions on* 30, 11 (Nov 2015), 6298–6309. DOI: https://doi.org/10.1109/TPEL.2015.2406673

[31] Wireless Power Consortium. 2013. *Qi System Description, version 1.1.2.* Technical Report.

[32] WiTricity. 2012. *Highly resonant wireless power transfer: safe, efficient, and over distance.* Technical Report.

[33] X. Zhang and K. G. Shin. 2012. E-MiLi: Energy-Minimizing Idle Listening in Wireless Networks. *IEEE Transactions on Mobile Computing* 11, 9 (Sept 2012), 1441–1454. DOI: https://doi.org/10.1109/TMC.2012.112