Power-Positive Networking: Wireless-Charging-Based Networking to Protect Energy Against Battery DoS Attacks

SANG-YOON CHANG, University of Colorado Colorado Springs
SRISTI LAKSHMI SRAVANA KUMAR, Advanced Digital Sciences Center
YIH-CHUN HU, University of Illinois at Urbana-Champaign
YOUNGHEE PARK., San Jose State University

Energy is required for networking and computation and is a valuable resource for unplugged systems such as mobile, sensor, and embedded systems. Energy DoS attack where a remote attacker exhausts the victim's battery via networking 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 (as opposed to the traditional radio-frequency 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. In this paper, we study the energy DoS attack impacts on off-the-shelf embedded system platforms (Raspberry Pi and the ESP 8266 SoC module), present PPN, implement and build a Qi-charging-technology-compatible prototype, and use the prototype for evaluations and analyses. Our prototype, built on the hardware already available for wireless charging, effectively defends against energy DoS and supports simultaneous power and data transfer.

CCS Concepts: • **Networks → Network properties**; **Network security**; **Mobile and wireless security**;

Additional Key Words and Phrases: Wireless networking, denial-of-service, battery exhaustion attack, wireless charging, Internet of Things

ACM Reference Format:
Sang-Yoon Chang, Sristi Lakshmi Sravana Kumar, Yih-Chun Hu, and Younghee Park. . 2019. Power-Positive Networking: Wireless-Charging-Based Networking to Protect Energy Against Battery DoS Attacks. *ACM Trans. Sensor Netw.* 1, 1 (February 2019), 25 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

This study is supported by the research grant for the Human-Centered Cyber-physical Systems Programme at the Advanced Digital Sciences Center (ADSC) from Singapore's Agency for Science, Technology and Research (A*STAR). This paper is an extended version of the work published at ACM WiSec, Boston, Massachusetts, USA, July, 2017 [1]. The authors extend the previous work by improving the prototype, adding the analyses with ESP 8266 SoC module, including broader and more detailed analyses and performance measurements of the power and the data transfer, and discussing about future work and the potential of wireless-charging-based networking beyond PPN. The authors would also like to thank the anonymous reviewers and the Associate Editor, Gang Zhou for their feedback.

Authors' addresses: Sang-Yoon Chang University of Colorado Colorado Springs, schang2@uccs.edu; Sristi Lakshmi Sravana Kumar Advanced Digital Sciences Center, sravan.s@adsc.com.sg; Yih-Chun Hu University of Illinois at Urbana-Champaign, yihchun@illinois.edu; Younghee Park. San Jose State University, younghee.park@sjsu.edu.

1550-4859/2019/2-ART $15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

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). 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 bottleneck to the system design [2–4] (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 and the energy use/efficiency of the networked devices.

While the experts in electronics and computing are aware 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 and the energy availability. *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 [5] on wireless sensor networks.

We focus on the latter networking-based energy DoS with an external attacker (however, our work also addresses the processing tasks, e.g., 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 according to such design (much lower than the power budget for the devices' primary functions of sensing and control) [5, 6]. Prior solutions assume that receiving networking inputs consumes the device's power and reduces the battery energy (which assumption is also pervasively established in the general energy-saving research in a non-security context, e.g., [7–9]) and thus focus on the detection and mitigation of such attacks; Section 2.1 reviews such literature in energy DoS in greater details. However, we take a fundamentally different approach to address energy DoS and eliminate the attack entirely; we break the aforementioned assumption that the networking inputs result in net-negative energy to the receiver and build a networking channel so that the networking inputs which have been received through the channel increase the device's energy. In other words, we introduce a novel *power-positive networking* (PPN) channel which use for communications increase the device's energy.

We build communication on the wireless charging signal, so that the power transfer and the information transfer are coupled and occur simultaneously. Because we modulate data information using the charging signal, our design requires minimal hardware (minimal 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). To use the charging signal for data communications, we implement networking on the power subsystem. We build the PPN channels on the power subsystem (which is built for wireless charging and energy storage) because the networking operations using the RF subsystem frontend (built for data transfer) consumes power. PPN is thus orthogonal to the networking operations from the traditional RF-based networking subsystem; for example, PPN enables communications even when the RF-based frontend/antenna is turned off or does not interfere with the receiver

initiating communications via RF for emergency communications. Because it uses the power subsystem and the power transfer signals, PPN provides unique features distinct from other RF-based networking channels. We propose PPN to provide an orthogonal communication channel to RF-based networking (the PPN channel has minimal overhead in power and hardware and eliminates the vulnerability for energy DoS) as opposed to replacing RF networking, as described in Section 4.2.

Even though our scheme (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. To implement PPN and demonstrate its use, we assume that the device is under attack (energy-DoS attacker is present) and that the networking is only enabled when there is positive energy from the networking session (e.g., the victim device is running low in battery energy and cannot afford wasting it via unnecessary networking). Such use of PPN corresponds to a preventive measure in an energy-limited environment. However, while such measures would have merely turned off the networking previously/without PPN, PPN offers an orthogonal channel to RF networking which still enables communications with the device while providing power-positive property to the device; Section 4.2 provides greater details.

We construct bidirectional communications using the power-transfer signal. For consistency, 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). For the reverse direction from receiver to requester, we use backscattering for energy-saving communication.

The rest of the paper is organized as follows. We discuss related work in Section 2 and describe our energy DoS threat model (applicable to *any* networking-capable systems) and the impact of RF-networking-based threats through experimental measurements in Section 3. Section 4 presents power-positive networking (PPN), our scheme against energy DoS, and Section 5 describes the PPN implementation. We evaluate the power transfer performance, the communication performance, the communication-compatibility with radio hardware, and the effectiveness and the security cost of our PPN prototype in Section 6. Afterward, we discuss potential directions and future work in Section 7 and conclude our paper in Section 8.

2 RELATED WORK

2.1 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., Internet of Things (IoT), and will become even more devastating in wireless sensor network applications [17–19], which typically have much simpler hardware architecture than other general-purpose 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- and behavior-monitoring [18, 20–25], *mitigation* based on lightweight authentication [18, 26], and sleeping-based *medium access control (MAC)* [7–9, 27] (which is vulnerable especially against an attacker who knows the MAC-layer information [28]).

The closest to our approach in defending against energy DoS is by Halperin et al. [6], which not only 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

[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., [10–12]), by jamming (e.g., [13–16]), and so on. Our work focuses on energy/battery resource.

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 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 3.2; the mere networking functions of pairing and receiving packets, even if dropping those packets immediately after receiving without further processing, consume additional power and can be used for energy DoS by a radio-equipped attacker. Therefore, we take a fundamentally different approach from the prior work and build networking on power transfer. The greater power efficiency from using the power transfer signal enables our work to power the entire system including control, networking, and security.

2.2 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., radio-frequency identification (RFID) tags [29–31].

The receiver-to-requester communication component of our scheme, used for feedback and acknowledgment, 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).

2.3 Building Networking on Power Transfer

Both wireless communication and wireless charging rely on the electromagnetic (EM) field propagation over air, but the two fields are mostly studied separately. Prior to our work, a limited group of researchers designed bidirectional communication channels using the charging signals [32–34]. However, these work are not designed to be power-sensible to the receiver and actively draw energy from the receiver's battery.

In contrast, others have enabled receiver-to-requester communications by using the power subsystem for backscattering communications to avoid additional networking hardware and to conserve power on the receiver [35–37]. While we build on these prior work, these work are not designed for simultaneous power and data transfer (as PPN does). They rather provide time-interleaved power transfer control communication in order to increase the power transfer efficiency.

While the aforementioned work built communications using power transfer signals for networking purposes, other work adopted communication-inspired concepts to boost the efficiency of wireless power transfer. Jadidian and Katabi used multiple power transmitter coils to beamform the magnetic flux to one receiver [38] while their following work [39] and others [40] extended that notion to multiple receivers. Others proposed improving the power transfer efficiency via adaptive frequency control [41–43], inductance and capacitance control [43, 44], or the receiver coil placement control [45, 46]. While these work can be applied to build more sophisticated control of the requester transferring the power to the receiver and initiating networking, our contribution to construct PPN focuses on a single- and fixed-coil setup and is orthogonal to these prior work adopting coil control. Our work can be used in conjunction with them in principle, however the actual systems investigation to combine the multiple-coil approach is beyond the scope of this paper.

2.4 Building Power Transfer on Networking

Prior literature uses ambient radio-frequency (RF) signals to harvest power (which is a form of energy transfer but has significantly lower magnitude of energy being transferred than charging and is thus not utilized for replenishing a battery for storing energy) [6, 47–50]. 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 [51] (even with respect to the wireless charging standard [52]) and possible health concerns for human-proximate applications [53]. 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 Federal Communications Commission (FCC) regulations. In contrast, inductive-coupling based power transfer is already standardized for wireless power transfer (e.g., the Qi standard by Wireless Power Consortium [36] and Rezence standard by Alliance for Wireless Power (A4WP)) and has been deemed safe and compliant to FCC standards [54]. Thus, we use inductive coupling signals (designed for charging batteries of mobile and embedded devices) and not RF signals (designed for networking).

In wired networking, Power over Ethernet (PoE) is standardized by IEEE 802.3af and 802.3at and provides power and data over the Ethernet cable.

3 ENERGY DENIAL-OF-SERVICE THREAT

3.1 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 threat is analogous to the volumetric DoS attacks which flood the victim with repeated transmissions to exhaust their network bandwidth or system resources in the wired networking context, but the attacker in our threat model targets the energy resource and is based on wireless networking with direct communication link to the victim node. The attack is generic and can apply to any communication implementations at the physical layer; independent of the lower-layer details of coding and modulation, the attacker merely activates the networking and continues sending request packets. In this paper, we focus on the networking protocols based on one back-and-forth exchange and leave the other protocols (e.g., the protocols based on multiple exchanges or stateful protocols) as future work, as described in Section 7.

In the Resurrecting Duckling model [5] designed for general wireless ad hoc networking, the external/remote attacker's request causes a response and such response is classified as a "distinct auxiliary function". Because these distinct auxiliary functions are supposed to occur sporadically, the system design treats the cost of the primary functions (including not only the sensing and control costs but also those that regularly update the authority by networking) as the dominating cost factor of the system; in normal situations when an attacker is absent, the primary function cost dominates the distinct auxiliary function cost. Our threat model challenges this notion by increasing the cost of such networking-based "distinct auxiliary function" by flooding the victim with networking requests. The attackers' requests are otherwise legitimate (e.g., the attacker is intelligent enough to learn the networking protocol by Kerchkoff's principle and to generated and transmit the requests accordingly) and the receiver cannot distinguish between a legitimate requester and an attacker (e.g., we do not rely on attacker detection, which prior work are described in Section 2.1).

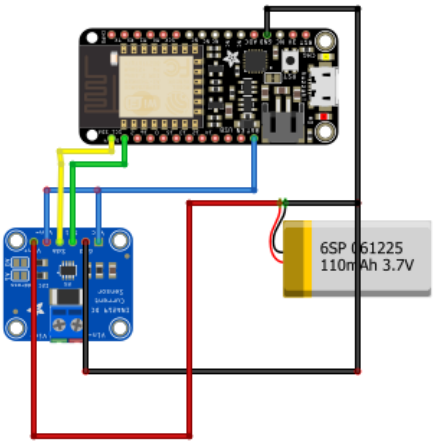


Fig. 1. ESP power measurement setup. The top is the Adafruit HUZZAH ESP 32 Feather board hosting the ESP 8266 SoC module; the bottom right is the battery; and the bottom left is the INA 219 current sensor (which interfaces with a processor, not drawn here).

We do not consider the cases of the requester being subjected to attack, and the networking initiator assumes the power cost (outside of our threat model, the victim node can also initiate networking with power costs, and PPN does not interfere with such networking). Furthermore, we do not consider the cases of the power transfer source (such as those having stable power supply from power outlet) being under attack because its energy is inherently cheaper and more abundant than the receiver's. If PPN is enabled, the requester either communicates when the receiver is in middle of a charging session or acts as the power source itself, as discussed in Section 4.2.

3.2 Threat Impact Analyses

To motivate our work, we study the energy DoS impact on the receiver and analyze the networking costs for communicating with the requester using the RF-based networking channels, which are the typical channels that a remote attacker would use to engage the victim; our proposed scheme using a fundamentally different technology/signal is not incorporated in the analyses in this section. In particular, we analyze the networking cost and the authentication cost; the networking corresponds to establishing a connection, receiving the requests/packets, 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 packets in secure networking and computing.

We use a *Raspberry Pi 3 Model B* (RasPi) and an *ESP 8266* (ESP) module, which are representative of physically smaller embedded system applications, and experiment using IEEE 802.11n (WiFi) networking protocols, which capability is already built-in on both boards. ESP 8266 is a system-on-chip (SoC) module designed for wireless sensor networking, in contrast to the general-purpose Raspberry Pi, and is equipped with multiple sleeping (power-saving) modes. For authentication, AES-CCM-128 is used due to its use in IoT-friendly Zigbee [55] and wireless body area network [56].

For measuring the power for Raspberry Pi (which is a general-purpose platform), we physically tap the power supply cord (connected to the power outlet) and inject a multimeter, measuring the current that is drawn from the power source. On the other hand, ESP 8266 interfaces with Adafruit

	Baseline	Awake	Paired	Receive	Transmit	Authentication
RasPi	1.144 (1x)	1.348 (1.178x)	1.347 (1.177x)	1.419 (1.240x)	1.631 (1.431x)	1.85 (1.617x)
ESP	0.0245 (1x)	0.304 (12.38x)	0.326 (13.25x)	0.343 (13.96x)	0.373 (15.20x)	0.363 (14.78x)

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.

HUZZAH ESP 32 Feather board for hosting the battery and the voltage regulator for the power supply for ESP 8266. For measuring power for ESP 8266, we monitor the power drawn directly from the battery using a current sensor (the INA 219 board which is designed for current/power monitoring), as depicted in Figure 1. Thus, our power measurements for ESP 8266 and Raspberry Pi account for the cost of the entire system and are reliable (more so than the software-based power measurement tools).

The networking cost measurements and the authentication cost measurement are in Table 1; the power values are shown upto the significant digits with minimal/no fluctuations according to our measurements. 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.

For Raspberry Pi, while the additional networking power costs are less than that of the Baseline (the aggregate cost of the rest of the functionalities), they are still significant, reaching up to 24% and 43.1% additional cost for receiving and transmitting, respectively, and 61.7% additional cost for the authentication computation.

Energy DoS impact becomes more dramatic for ESP 8266, because the power-efficient system optimizes the power use in general and significantly lowers the Baseline cost. For example, against a straightforward threat from a requester who sends signals according to the victim's physical-layer modulation (so that the victim receiver is forced to be awake), the power cost increases by 1238%; against another malicious requester who sends packets with legitimate packet headers and a spoofed identity, claiming to be another requester without the credential/key for the proper authentication (so that the receiver processes authentication, which fails, before dropping the packets), the power increases by 2874% (the aggregate cost for Receive and Authentication).

Comparing the general-purpose RasPi and the WiFi-dedicated ESP, our observations agree with Martin et al. [18] in that, for general-purpose computers, the cost for networking does not outweigh that of the rest of the system. However, for sensor/embedded applications for dedicated tasks and a dedicated SoC for networking, RF-based networking dominates the power consumptions [18, 57] and energy DoS threat can cut the battery life by one to two orders of magnitude [58].

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 6.1.

4 POWER-POSITIVE NETWORKING

4.1 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 processes 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 and the acknowledgment (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 in 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.

4.2 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/connectivity 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 using RF, e.g., for emergency communications.

Figure 2 illustrates the requester/attacker scenarios. Figure 2(a) corresponds to the traditional RF-based networking attacks, as experimented in Section 3.2. In this case, if PPN is enabled to achieve the power-positive property, the victim device goes in to sleep and turns off the RF networking, nullifying the energy DoS. The victim device still has the PPN communication channel opened, enabling data communications possibilities. An attacker can waste the victim device's power as long as the net power of the victim device is increasing, for example, the attacker can attack at times when the victim is getting charged, as in Figure 2(b). However, in such case, the attacker

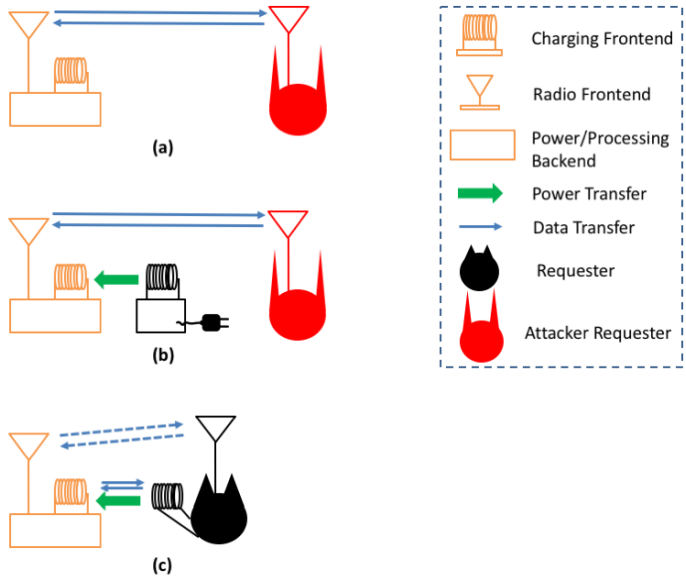


Fig. 2. PPN Networking Attack Scenarios: (a) RF-only attack results in the victim device sleeping/disabling the networking; (b) RF-only attack can get accepted by the victim device when the device is being charged; (c) Requester utilizes both RF networking and PPN networking (the dotted lines indicate that the RF-channel data transfer can be optional)

is significantly limited in both its feasibility (can only attack when the victim device is being charged) and impact (the attack decreases the charging rate as opposed to depleting the energy). In another scenario in Figure 2(c), the charging-capable requester can use PPN communication channel for data communications (which would also provide energy transfer); the requester can also optionally engage the victim device via RF networking. The requester can be either malicious or legitimate/benign, but PPN enforces that the power is positive and protected even if the requester is malicious. In our experiment in Section 6 to demonstrate the PPN effectiveness, we focus on the scenario in Figure 2(c) with a malicious attacker as the requester, which is a stronger threat model than Figure 2(b) because it provides the attacker with greater options (including the control of the charging source). In contrast, Figure 2(b) can actually be more of an attack on the charger as opposed to the victim device (because of its impact on the charger prolonging the power-charging duration with slower charging rate); the attack analyses on the charger is beyond the scope of our threat model since charger's energy is cheaper than the energy-constrained victim device.

PPN channel can also be used to facilitate security and control communications for the RF networking. For example, a key/seed can be exchanged to control the physical-layer parameters to randomize the RF channels against the attacker, e.g., spreading spectrum [10, 14, 19]. Such use of PPN channel is beyond the scope of this paper, and we rather focus on building the non-RF channel for PPN 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 2.2), 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 anomalous battery-draining behavior (e.g., building on the prior work in energy DoS detection in Section 2.1), the receiver can opt for PPN only and turn off the traditional RF networking subsystem; otherwise, our analyses and experiments in Section 3.2 show that repeated networking sessions (e.g., from energy DoS threat) can drain the battery and shut down the device operation quickly.

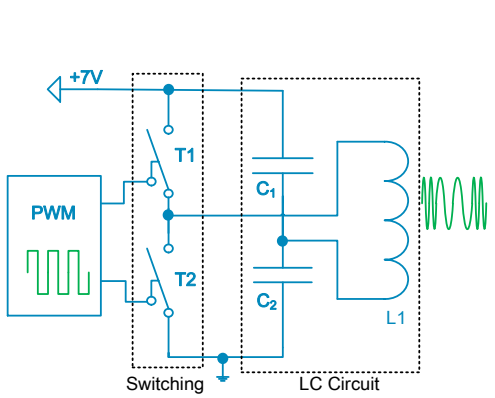
The design for such decision engine triggering PPN-only mode (investigating threshold for low battery and algorithms for anomaly detection, e.g., prior work in Section 2.1) depends heavily on the embedded applications and how critical the networking is compared to the control/sensing functionalities 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.

5 PPN IMPLEMENTATION

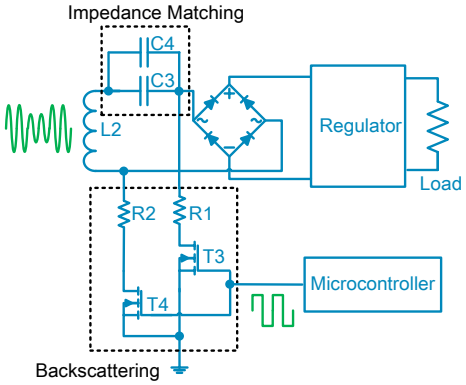
PPN provides simultaneous power and data transfer. For *power transfer*, PPN builds on wireless charging, invented in the 20th century [59]. Wireless charging uses inductive coupling to transfer power from one circuit to another. Since current (electric field propagation) generates EM field and vice 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. Our PPN prototype specifically builds on the Qi standard for inductive coupling charging [36], which is widely used in mobile and embedded systems.

For *communications*, we build on the power transfer design and modulate information 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 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 requester, 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 (potentially enabling full duplex, which is accessory to our work and whose development is left for future work). In addition to being orthogonal to the amplitude-based backscattering, we use frequency modulation for requester-to-receiver communication due to its channel noise resistance.

Figure 3 shows the circuit block diagrams of the requester and the receiver which have been used for power and communication transmission. Most of the communication circuit overlaps with the power transfer circuit as communication piggybacks on the charging signal. The only hardware 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



(a) Requester design for transmitting power and the forward-direction communication using FSK (simplified). The green signals illustrate the outputs of the the communication scheme. TPS28225 driver drives the T_1 and T_2 nMOSFETs; $C_1 = C_2 = 22$nF; and $L_1 = 24\mu$H. From left to right, the micro-controller and the driver generates the pulse width modulation (PWM) signal with frequency control; the half-H-bridge-based circuit follows for switching; the capacitors generate sinusoidal alternating current (AC); and the inductive coil generates (resonant) electromagnetic induction.



(b) Receiver design for receiving power and the reverse-direction communication using backscattering (simplified). The green signals illustrate the outputs of the the communication scheme. T_3 and T_4 are nMOSFETs, $C_3 = C_4 = 22$nF, and $L_2 = 24\mu$F. For receiving power, the LC circuit converts the inductive coupling signal to electrical current; the rectifier (full-wave rectifier based on diode bridge) converts the AC to DC; and the voltage regulator yields a constant voltage for stable power supply to the load. For backscattering, the receiver vary the inductive coupling strength by changing the effective resistance.

Fig. 3. Circuit Block Diagrams for Requester and Receiver

the envelope detector at the requester side for receiving the receiver-to-requester communication. However, modern mobile and embedded systems with wireless charging technologies are already equipped with such hardware and capabilities because they build networking on the power subsystem for the power control communications to improve the power transfer efficiency, as described in Section 2.3 and standardized in Qi by Wireless Power Consortium [35, 36]. The rest of the logic is at the digital level and implemented at the device backend.

For the forward-direction communication from requester to the receiver, we modulate the inductive coupling signal by varying its frequency, i.e., frequency shift keying (FSK). The micro-controller at the requester varies the frequency of the pulse width modulation (PWM), which affects the AC current, the inductive coupling field, and then the AC current generated at the receiver. From the AC current, the receiver digitally filters the signal and de-modulates the FSK signal (by comparing the phase to that of the reference).

Since they are mutually coupled, both the requester and the receiver affect the inductive coupling field and each other's electrical fields. Thus, we modulate the receiver's circuit for the reverse-direction communication (from the receiver to the requester). Specifically, as depicted in Figure 3(b), whether the message bit is "1" or "0" drives the binary switching circuit, which determines the effective resistance (and thus the effective impedance of the circuit) and varies the inductive coupling strength. This affects the current level at the requester; the two bits transmitted at the receiver yield two distinct current amplitude levels at the requester (the recipient of the reverse-direction communication), thus making the communication demodulation at the requester to be that of an

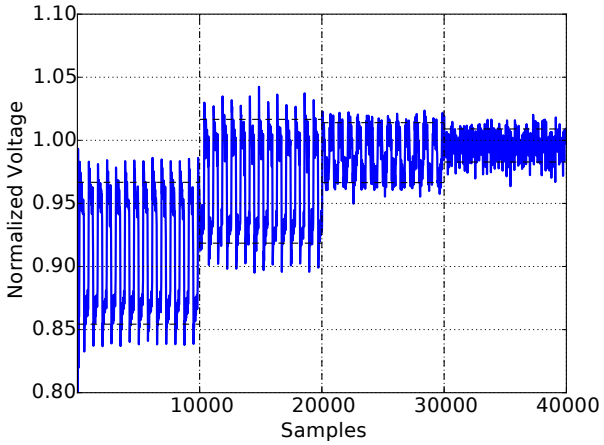


Fig. 4. The effect of backscattering (for reverse-direction communication) on the voltage level on the requester side. The voltage in the vertical axis is normalized by 3.3 Volts, which is the the upper bound of the dynamic range of the micro-controller (digitally processing the backscattering demodulation), and each of the 10,000 samples correspond to different requester-receiver distances (0.5cm, 1cm, 2cm, and 3cm from left to right). The dotted horizontal lines correspond to the average amplitudes for each bits.

amplitude-shift keying (ASK). The requester, in turn, samples the signal after the LC circuit, filters it with an analog band-pass filter, and then uses an envelope detector for the ASK demodulation

To demonstrate the reverse-direction communication and the effect of backscattering, Figure 4 shows the voltage level on the requester side (after the voltage divider, translator, the envelope detector and before the micro-controller, which digitally samples and processes the signal for backscattering demodulation) when the bits toggling between 1's and 0's ("10101010...") are transmitted at the reverse direction and there is no forward-direction communication. The first ten thousand samples correspond to the case when the requester and the receiver are 0.5cm apart (we avoid the case of 0cm when the coils are touching each other), the second ten thousand samples when they are 1cm apart, the third when they are 2cm apart, and the last when they are 3cm apart; these events are distinguished with vertical dotted lines. Because of the backscattering, there are amplitude shifts in the electrical voltage; the average difference (denoted with ΔV) between the reverse-direction communication bits "1" and "0" are shown in the figure. As distance increases, ΔV and consequentially the ASK signal power (which is proportional to the square of ΔV) decrease; this reduces the communication channel quality, as we will study in greater details in Section 6.3.2.

6 EVALUATION

We build our prototype as described in Section 5. We choose the parameters to minimally impact the power transfer due to the importance of the power resource in PPN. Communication is also affected by the parameter choices, and the prototype behaviors generally agree with the prior work in wireless communications/networking despite our use of inductive-coupling charging signal and not the RF signal. In this section, we detail our findings of PPN using our prototype.

In our prototype, we use the center frequency of 155kHz (which complies with the Qi standard and maximizes the power transfer for our prototype design) with a frequency separation of 1kHz for the FSK-based data transfer (which keeps the power transfer within 1.9% of the optimal performance).

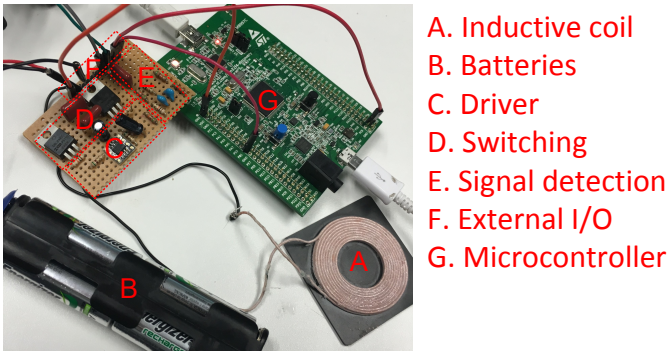


Fig. 5. The requester prototype

For the communication rate, we use 7kbps for the requester-to-receiver communication and 2kbps for receiver-to-requester communication.

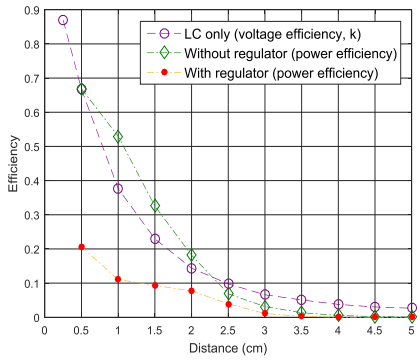
6.1 Modular Design to Backend Processor

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, Adafruit HUZZAH ESP 32 Feather board (hosting ESP 8266), Samsung Galaxy phone, and a laptop. Figure 5 displays the requester prototype with the microcontroller and the charging coil (which acts like an antenna for networking).

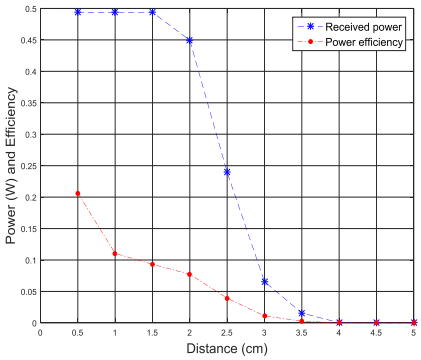
6.2 Power Transfer

We first empirically study the effect of the circuit blocks on the power transfer and then study the received power and the power transfer efficiency over the distance between the requester and the receiver. We operate at the resonance frequency that minimizes the impedance and optimizes the power transfer; the theoretical resonance frequency in our prototype design is: $f = \frac{1}{2\pi\sqrt{L \cdot C}} = \frac{1}{2\pi\sqrt{24\mu\text{H} \cdot (22+22)\text{nF}}} = 155\text{kHz}$; we also experimentally verified that this frequency yields the maximum power transfer. The power was computed from the voltage and current measurements using a multimeter when a 50-Ω load was connected. As is typical in power transfer performance analyses, we vary the distance between the requester and the receiver to vary the (inductive coupling) signal strength; we treat the case of requester-receiver distance being 0cm as an outlier, as the coils are touching each other and interfering with the inductive coupling, and exclude it from our analyses.

6.2.1 Coupling & Regulator. We study the inductive coupling channel quality over distance and the effect of regulator (designed for stable power transfer/supply and popularly implemented in wireless charging) in this section. First, to study the channel quality and the strength of the inductive coupling field, we only keep the LC circuit and open-circuit the rest of the receiver (in other words, we replace the rectifier, voltage regulator, load, backscattering, micro-controller, etc. from Figure 3(b)). The LC circuit determines the reactance, which quantifies the resistivity to the change in electrical current, and consequently the coupling coefficient between itself and the requester, which coefficient quantifies the strength of the inductive coupling field between the two nodes and varies between zero (no coupling) and one (full/maximum coupling). Figure 6(a)



(a) The coupling coefficient k (LC only), the power efficiency without the regulator (Without regulator), and the power efficiency with the regulator (With regulator)



(b) The received power and the power efficiency

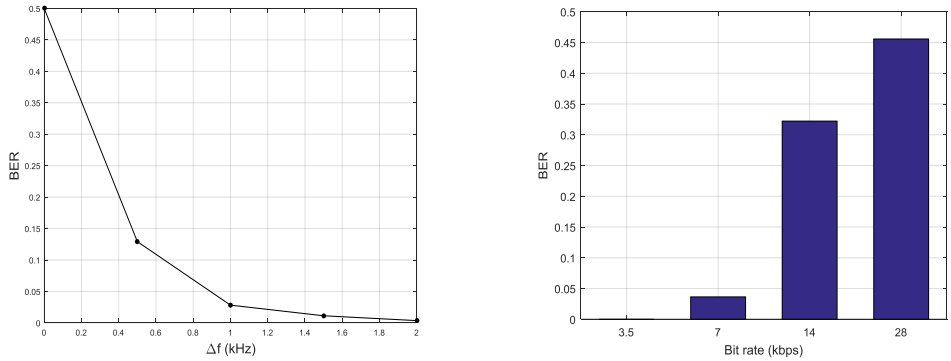
Fig. 6. The power transfer performance (the markers indicate the measurements)

presents our experimental results for the coupling coefficient, k, which is obtained from the voltage ratio between receiver and the requester/transmitter when $L_1 = L_2$ (which values are specified in Figure 3). The signal strength decreases as the two nodes are further apart.

We also study the effect of the rest of the circuit components beyond the LC. Restoring our prototype, depicted in Figure 3(b), we take the same power efficiency measurements (the ratio of the received power over requester's transmitted power) without and with the regulator and present our results in Figure 6(a). Both power-efficiency measurements decrease as the transmitter-receiver distance increases (because the inductive coupling field strength decreases, as discussed in the previous paragraph). Comparing between with and without regulator, the performance decreases by incorporating the regulator. Despite the reduced voltage performance, the use of regulator is critical in wireless charging because it provides stable power supply and protects the charging load from arbitrary electrical spikes; we further study the effect of the regulator on the received power in Section 6.2.2. Due to this reason, we study the performance of the complete circuit with the regulator in the rest of the paper.

6.2.2 Power and Requester-Receiver Distance. We analyze the power transfer performance over distance and present our experimental results in Figure 6(b). We measure two performance metrics with the probes across the load (e.g., the receiver's battery): the received power and the power efficiency (the ratio of received power to the transmitted power). The performance generally deteriorates as the receiver moves further away from the requester and the signal strength decreases, and the performance is the strongest at 0.5cm-1.5cm region, i.e., the magnetic flux is the strongest. At 0.5cm-1.5cm region (which is typical for wireless charging), our prototype supplies a constant 5V and 0.49W of power to the load; the power supply is constant due to the regulator (which has an input dynamic range of 7V-25V). The performance of our prototype is comparable to the state-of-the-art wireless charging for low power applications, and we test the compatibility with commercial-grade batteries and off-the-shelf wireless charging devices.

Besides the effect of the receiver regulator, the power efficiency and the received power are not proportional to each other because the transmitted power is not constant and actually increases



(a) The effect of FSK modulation-signal amplitude (the amplitude of frequency variation)

(b) The effect of communication rate

Fig. 7. Communication reliability performance (bit error rate) of the requester-to-receiver communication

with the requester-receiver distance before it reaches a steady-state (at which point and onward, the receiver presence has negligible impact on the requester power). The strength of the coupling between the requester and the receiver (and the effect of the receiver to the requester and vice versa) decreases as they become increasingly apart; the reflected impedance of the receiver, experienced by the requester, decreases as the receiver is farther away. In our experiment, from distance 0.5cm to 2.5cm, the transmitted power increases from 2.4W to 6.1W and then reaches the steady-state.

6.3 Communication

As discussed in Section 5, we use FSK to vary the frequency of the charging signal for the forward-direction communication (from the requester to the receiver) and ASK-based backscattering for the reverse-direction communication. We use two metrics for the communication performances and reliability: *bit error rate* (BER) measures the digital communication reliability and counts the number of errorneous bits relative to the number of total bits sent, and *signal-to-noise-ratio* (SNR) measures the analog signal quality and corresponds to the signal power relative to the noise power. BER and SNR are related to each other (in general, the higher the SNR the higher the reliability performance and lower the BER) but are measured at different points of the signal processing chain, as discussed in Section 6.3.1. For measurements, we generate random bits for the data transmission. We synchronize using a 4-byte-long header/footer (which does not count toward the performance), and the measurements were averaged over 10,000 communication bits in both directions.

6.3.1 Requester-to-Receiver Communication. As described in Section 5, we use binary FSK to modulate our bits to the charging signals, and the degree of difference in the charging signal (the frequency deviation amplitude in this case) between the two bits determines how reliable the information delivery is against channel noise, whose impact grows as the signal decreases by channel propagatoin/attenuation.

We study the effect of the FSK modulation amplitude (the frequency deviation amount, Δf) when the receiver is at a distance 0.5cm away from the requester and present our results in Figure 7(a). Δf is with respect to the reference frequency, and $\Delta f = 0$ is equivalent to when the communication is disabled and results in a random coin-toss to demodulate/decide between the

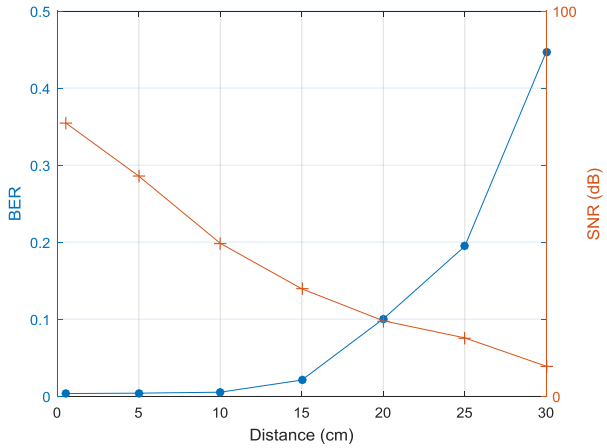


Fig. 8. The effect of distance for requester-to-receiver communication (the BER is marked with '.'markers, and the SNR in dB is marked with '+'markers)

two bits, i.e., BER=0.5. As Δf increases, BER decreases and thus the communication reliability (and the noise resistance) increases. However, we cannot keep increasing Δf if we are to enable both communication and power transfer, as increasing Δf will negatively impact the power transfer; as discussed in Section 6.2, the greater the deviation from the optimal frequency (155kHz in this case), the worse the power transfer performance and efficiency. For the rest of the paper, we make a design choice and use $\Delta f = 1$kHz which has an error rate of 0.025 and keeps the power transfer within 1.9% of the optimal power transfer; the system applications and requirements influence this choice.

The communication performance is also affected by the communication rate. With fixed sampling rate at the analog-to-digital converter (ADC) on the micro-controllers, increasing the bit rate decreases the samples that are used to process a bit and thus decreases the processing gain. Therefore, as shown in Figure 7(b) (which shows the BER performance with varying communication bit rate when the requester-receiver distance is at 15cm), choosing a more aggressive rate for higher communication efficiency deteriorates the reliability performance, e.g., the BER exceeds 0.32 when the bit rate is 14kbps or greater. Therefore, we use the forward-direction communication rate of 7kbps, which has an error performance of 0.0364 when the receiver is 15cm away from the requester.

We also analyze the impact of the charging signal attenuation (as it propagates through the air medium) on the communication performances; in Section 6.2.2, we studied its effect on the power transfer. We measure two different metrics at two different locations at the receiver, described in Figure 3(b), and show the results in Figure 8. First, we measure the physical signal-to-noise-ratio (SNR) after the LC circuit and before the signal enters the digital-processing domain (plotted at the right vertical axis); the noise power is measured when there is no transmission. Second, we measure the BER performance at the digital backend after the signal is processed (e.g., demodulation) and see whether the decision between the two bits matches the transmitted bits (plotted at the left vertical axis). The digital communication reliability performance, which is inversely correlated with the

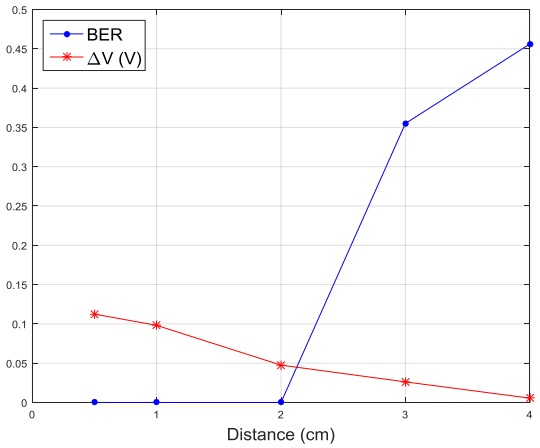


Fig. 9. The effect of distance for the backscattering-based receiver-to-requester communication

BER, behaves according to the physical/analog SNR measured toward the frontend. As requester-receiver distance increases, the communication performance gets worse, i.e., SNR decreases and BER increases.

6.3.2 Receiver-to-Requester Communication. We study the communication performance as the signal propagates through the medium air for the reverse-direction communication while the communication rate is 2kbps. To study the ASK signal strength and the communication channel quality at the requester, Figure 9 plots the difference in voltage amplitude level (ΔV) between the two modulated bits and the bit error rate (BER). As the requester-receiver distance increases, ΔV decreases, which also worsens the overall communication channel quality and increases the BER.

Although we study the communication parameters for the forward-direction communication in Section 6.3.1, we largely omit the analyses for the parameters for the reverse-direction communication because of the following two reasons. First, the data rate requirement is generally lower than the forward-direction channel. Second, it is more difficult to control and vary the modulation parameters at the receiver and therefore there is less motivation to deploy such control/degree-of-freedom; changing the circuit impedance (resistance or capacitance) either involves a manual effort in changing the circuit components or more components incorporated at the hardware to offer greater number of options (resulting in bulkier hardware). Thus, it is less practically relevant to study such parameter control effects than that of the forward-direction communication.

6.3.3 PPN and Radio/RF Networking. In addition to building bidirectional PPN communication channel for the transmitter and the receiver (both of which are built on the power subsystem supporting inductive-coupling wireless charging), we introduce radio nodes to receive the requester's PPN communication to test the PPN's communication compatibility with radio hardware. Such channel is for communications only and not for power transfer, as these radio hardware do not support wireless charging and consumes power. For the frontend of the radio nodes, we use RTL-SDR (composed of RTL2832U chipset and R820T tuner). RTL-SDR is a cheap, off-the-shelf software-defined radio (SDR) and takes the raw quadrature samples from a DVB-T TV tuner for passive operations. As the RTL-SDR can only access the frequency band of 25MHz-1750MHz, we

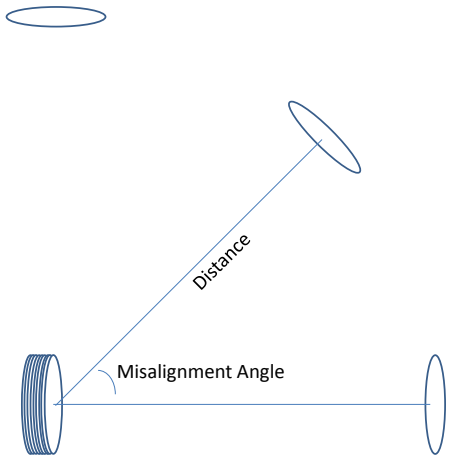
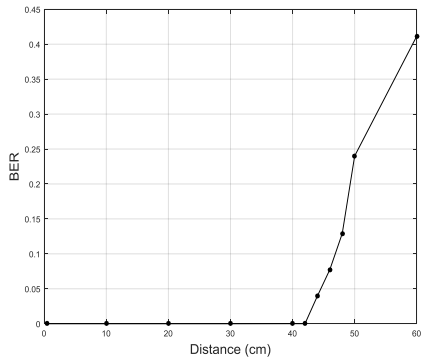
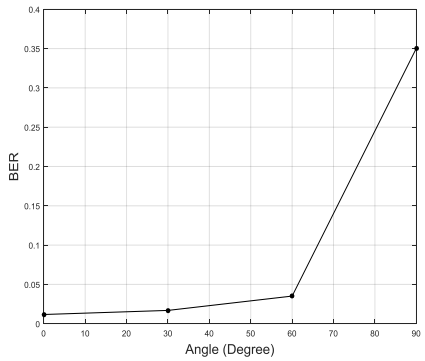


Fig. 10. The illustration of the relative node position, determined by the distance and the misalignment angle (the radio antennas are drawn at the misalignment angle of 0, 45, and 90 degrees)



(a) Bit error rate vs distance. We zoom in for our measurements between distance 40-50cm as is indicated with the markers.



(b) Bit error rate vs the misalignment angle.

Fig. 11. Radio receiver's performance for receiving the PPN communication

add a 125MHz upconverter that oversamples the upcoming stream before the RTL-SDR. We also use a loop antenna (similar to the inductive-coupling coils for wireless charging in shape) to introduce directionality for the radio nodes. We call these nodes receiving data from the requester using the PPN channel *radios* or *radio receivers* to distinguish them from the *receivers* built on wireless charging hardware we defined previously.

In Figure 11(a), we study the communication reliability performance in BER with respect to the distance between the radio receiver and the requester while the radio's loop antenna and the requester's inductive coil are aligned and facing each other. The communication begins to suffer as the distance exceeds 40cm.

To allow greater flexibility and mobility for the radios, we study the impact of misalignment between the requester's inductive coil and the radio's loop antenna and introduce *misalignment angle* (similarly to the angle in the polar coordinates), as described in Figure 10. For example, the misalignment angle of 0 degrees corresponds to when they are perfectly aligned and the radio receiver is located at the main direction of the requester's inductive coupling field propagation, and the misalignment angle of 90 degrees correspond to when the radio receiver is directly above or below the requester. In all cases (of the radio receiver's relative location), the radio antenna is facing the transmitter. Fixing the distance to be 35cm, Figure 11(b) shows the effect of misalignment on the communication reliability. The communication is robust to the radio receiver's (angle) location relative to the transmitter's mainbeam direction and that the side-lobes of the transmitter's beamforming offers relatively good signal. For example, BER stays below 5% up to misalignment angle of 60 degrees and, even when the radio is completely misaligned with an angle of 90 degrees, the error performance is still 35.0%. Thus, radio receivers can retrieve communication and their locations/orientations relative to the transmission source affect the level of signal processing effort required, e.g., for filtering out the noise and processing erroneous bits.

6.4 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). Based on our measurements in Section 6.3, 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 requester) 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 6.5 measures the potential PPN cost when the requester-receiver distance is 0.5cm.

6.5 PPN Delay Cost

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 potentially cause time delay for the receiver in accepting legitimate networking requests, because the receiver does not process the requests

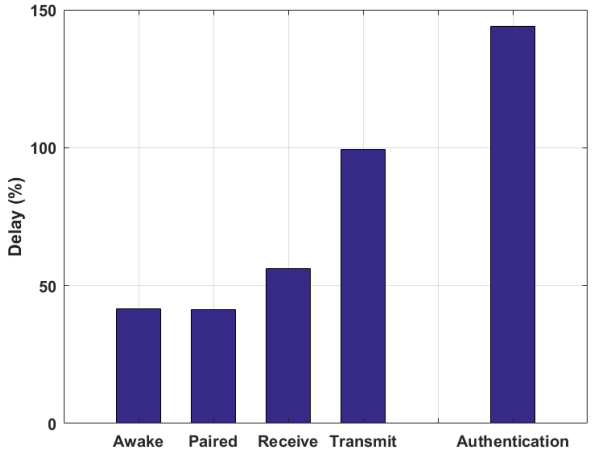


Fig. 12. Security cost (time delay) of PPN for Raspberry Pi. The delay is in percentage (%) and with respect to real-time processing. For example, if the delay is 50%, then for every task that takes 1 second, PPN takes 1.5 seconds.

until it receives sufficient power from the requester, as described in Section 4.1. Such security cost in time delay depends on the receiver's system platform (and its power requirement) and the networking operations requested by the requester.

We investigate the case when the requester sends requests triggering RF networking tasks using the PPN channel to show the effectiveness of PPN against RF-networking-based energy drainage attacks, as described in Figure 2(c). 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. These networking tasks are mirrored from Section 3.2 but, in that section, we measured the power consumption without PPN.

Hosting a Raspberry Pi for the processing, we compute the delay of PPN using the power consumption and the power delivery measurements when the receiver is 0.5cm away from the requester. The PPN receiver, described in Section 4.1, only asks for the incremental cost incurred by the requester's networking/authentication requests beyond that of the Baseline, e.g., its main purpose is not to replenish its battery, and the requester is only responsible for the additional power cost it will cause for the request and not for that of the Baseline. Our PPN prototype is insufficient to support the Raspberry Pi Baseline itself, as Raspberry Pi typically relies on wired charging and does not support wireless charging. Figure 12 presents the delay of using our prototype for PPN, and the authentication cost is additive to the other RF networking tasks if it is triggered simultaneously (e.g., receiving and authenticating a packet simultaneously).

On the other hand, when our prototype interfaces with ESP 8266 for processing and RF networking, it can support real-time processing of all the RF-networking requests and there is no delay cost. In fact, unlike Raspberry Pi (whose Baseline was not supported by our PPN prototype charging), ESP 8266 can be charged in its entirety by our prototype. Figure 13 shows the power performance when both PPN and the respective RF networking tasks occur simultaneously; the

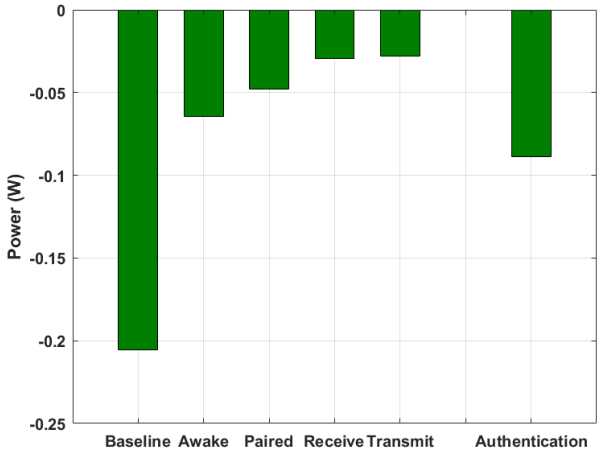


Fig. 13. The charging of the battery when PPN is enabled simultaneously with RF networking/authentication of ESP 8266. The vertical axis measures the aggregate power consumption (as is the case in Section 3.2), and negative power corresponds to the net-power increase.

power is negative because PPN provides excessive power (beyond that used for Baseline and the respective networking tasks) and charges the battery.

7 DISCUSSIONS & FUTURE WORK

We incorporate data communication to wireless charging and study the proposed design with system implementations and channel analyses. Because we build a communication link using inductive-coupling charging signal, designed for near-distance charging (e.g., the distance of 0.5cm is typical between the charging pad coil and the charging client coil), the communication is also appropriate for shorter distances; our prototype's communication range performance is in the order of tens of centimeters for the forward-direction communication and in the order of centimeters for the reverse-direction communication, as described in Section 6.3. Therefore, we do not envision nor advocate that our scheme replaces the traditional RF communications. We rather see it as an out-of-band and out-of-technique communication link, which provide unique features and can complement RF networking.

Adding communication channel links, practically free in power and hardware, to wireless charging opens up possibilities. In this section, we discuss about potential future directions from design improvement (beyond our current prototype) to other applications that can benefit from our work.

7.1 Design Improvement & Directions

7.1.1 Power Transfer Optimization. Although we studied the state-of-the-art literature in wireless charging (which influenced the design of our power transfer system), the power transfer improvement and optimization is not the main focus of this work. A more thorough optimization of power transfer will bridge our work closer to the power transfer community, as increasing power efficiency and transfer performance is one of the main focuses in the field. For example, recent

work in wireless charging uses dynamic control [38–40, 42] to make the charging signal stronger (which will therefore improve both the data and power transfer of our approach).

7.1.2 Joint Processing Development. Even though the modular design is generally a strength and offers easier deployment (and is thus the approach that we take in this work), a joint design between the backend and the frontend can offer greater performance gains in power transfer and information transfer. Such approach will especially be useful in the deployment phase when the application context is given and the node's functionality scope is defined, e.g., embedded systems (in contrast to a general-purpose system).

7.1.3 Networking Protocol Design. This paper focuses on providing the necessary networking/power channels for PPN. While PPN can be applied to any networking protocols in principle (because PPN is built on the power-transfer subsystem and uses the battery for energy storage), our current design prototype assumes a networking protocol based on one back-and-forth exchange (e.g., request and reply) and focuses on the instantaneous power load and that of the immediate response's. Designing networking protocols involving longer exchanges for PPN will provide a more complete solution which extends the scope of PPN. For example, for multiple-way protocols or longer responses, the PPN protocol would require the power-cost estimation of the following operations of the protocol and, for stateful protocol, PPN protocol could have the requester hold the state for power efficiency. Such protocols can use our PPN channel for power-positive property in principle (the requester only needs to provide enough power to store the energy on the battery for the impending operations) but may need adaptations on the networking protocols.

7.2 Interesting Use & Applications

7.2.1 More Connectivity. Our scheme builds networking from charging and not from the more traditional RF system. Thus, our scheme can not only provide an independent or redundant communication channel but can also enable connectivity for devices that cannot afford RF processing and hardware.

7.2.2 Multi-User Power Management. The current power transfer landscape largely operates under the model of one power source and one receiver. In the future power transfer landscape where the charging pads are implemented in the public sector (such as the airports, restaurants/cafes, and vehicular roads), multi-receiver cases can emerge. Our proposed communication link with minimal power and hardware overheads can facilitate better power transfer/management in such cases.

7.2.3 Security Services. Enabling communications for wireless charging devices can have security applications. For example, in addition to our focus of thwarting energy DoS (exhausting battery on resource-constrained devices), the geographical proximity (especially compared to the RF) and the inherent asymmetries between the transmitter and the receiver in the size, capability, and the infrastructure connection can be used for additional sources of security assurance.

8 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. PPN provides a preventive measure against energy DoS but, instead of merely disabling networking altogether, provides a RF-separate data communication channel with power-positive property which can be enabled/used even when under energy DoS attacks. Our PPN prototype offers 7kbps communication in the requester-to-receiver direction (which communication can also

be received using radio hardware) and 2kbps communication in the reverse direction while using near-field Qi-standard-compatible wireless charging. Using the prototype, we analyze the PPN channel performances (both in power transfer and data transfer) and validate its effectiveness against networking-based energy DoS.

REFERENCES

[1] S.-Y. Chang, S. L. S. Kumar, B. A. N. Tran, S. Viswanathan, Y. Park, and Y.-C. Hu, "Power-positive networking using wireless charging: Protecting energy against battery exhaustion attacks," in *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WiSec '17. New York, NY, USA: ACM, 2017, pp. 52–57. [Online]. Available: http://doi.acm.org/10.1145/3098243.3098265

[2] S. Saxena, G. Sanchez, and M. Pecht, "Batteries in portable electronic devices: A user's perspective," *IEEE Industrial Electronics Magazine*, vol. 11, no. 2, pp. 35–44, June 2017.

[3] S. Rothgang, T. Baumhöfer, H. van Hoek, T. Lange, R. W. de Doncker, and D. U. Sauer, "Modular battery design for reliable, flexible and multi-technology energy storage systems," *Applied energy*, vol. 137, no. 1, pp. 931–937, 2014. [Online]. Available: http://publications.rwth-aachen.de/record/459644

[4] T. Crompton, *Battery Reference Book*. Elsevier Science, 2000. [Online]. Available: https://books.google.com/books?id=QmVR7qiB5AUC

[5] F. Stajano and R. J. Anderson, "The resurrecting duckling: Security issues for ad-hoc wireless networks," in *Proceedings of the 7th International Workshop on Security Protocols*. London, UK, UK: Springer-Verlag, 2000, pp. 172–194. [Online]. Available: http://dl.acm.org/citation.cfm?id=647217.760118

[6] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *2008 IEEE Symposium on Security and Privacy (sp 2008)*, May 2008, pp. 129–142.

[7] J. Manweiler and R. Roy Choudhury, "Avoiding the rush hours: Wifi energy management via traffic isolation," in *Proceedings of the 9th International Conference on Mobile Systems, Applications, and Services*, ser. MobiSys '11. New York, NY, USA: ACM, 2011, pp. 253–266. [Online]. Available: http://doi.acm.org/10.1145/1999995.2000020

[8] X. Zhang and K. G. Shin, "E-mili: Energy-minimizing idle listening in wireless networks," *IEEE Transactions on Mobile Computing*, vol. 11, no. 9, pp. 1441–1454, Sept 2012.

[9] G. De Silva, B. Chen, and M. C. Chan, "Collaborative cellular tail energy reduction: Feasibility and fairness," in *Proceedings of the 17th International Conference on Distributed Computing and Networking*, ser. ICDCN '16. New York, NY, USA: ACM, 2016, pp. 25:1–25:10. [Online]. Available: http://doi.acm.org/10.1145/2833312.2833451

[10] S. Y. Chang and Y. C. Hu, "SecureMAC: Securing Wireless Medium Access Control Against Insider Denial-of-Service Attacks," *IEEE Transactions on Mobile Computing*, vol. 16, no. 12, pp. 3527–3540, Dec 2017.

[11] N. Golde, K. Redon, and J.-P. Seifert, "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)*. Washington, D.C.: USENIX, 2013, pp. 33–48. [Online]. Available: https://www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/golde

[12] S. Y. Chang, Y. C. Hu, and Z. Liu, "Securing wireless medium access control against insider denial-of-service attackers," in *Communications and Network Security (CNS), 2015 IEEE Conference on*, Sept 2015, pp. 370–378.

[13] X. Wei, Q. Wang, T. Wang, and J. Fan, "Jammer localization in multi-hop wireless network: A comprehensive survey," *IEEE Communications Surveys Tutorials*, vol. 19, no. 2, pp. 765–799, Secondquarter 2017.

[14] S.-Y. Chang, Y.-C. Hu, and N. Laurenti, "SimpleMAC: A Jamming-resilient MAC-layer Protocol for Wireless Channel Coordination," in *Proceedings of the 18th Annual International Conference on Mobile Computing and Networking*, ser. Mobicom '12. New York, NY, USA: ACM, 2012, pp. 77–88. [Online]. Available: http://doi.acm.org/10.1145/2348543.2348556

[15] T. D. Vo-Huu, T. D. Vo-Huu, and G. Noubir, "Interleaving Jamming in Wi-Fi Networks," in *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, ser. WiSec '16. New York, NY, USA: ACM, 2016, pp. 31–42. [Online]. Available: http://doi.acm.org/10.1145/2939918.2939935

[16] S. Lakshminarayana, J. S. Karachiwala, S.-Y. Chang, G. Revadigar, S. L. S. Kumar, D. K. Yau, and Y.-C. Hu, "Signal jamming attacks against communication-based train control: Attack impact and countermeasure," in *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, ser. WiSec '18. New York, NY, USA: ACM, 2018, pp. 160–171. [Online]. Available: http://doi.acm.org/10.1145/3212480.3212500

[17] S. Slijepcevic, M. Potkonjak, V. Tsiatsis, S. Zimbeck, and M. B. Srivastava, "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*, 2002, pp. 139–144.

[18] T. Martin, M. Hsiao, D. Ha, and J. Krishnaswami, "Denial-of-service attacks on battery-powered mobile computers," in *Proceedings of the Second IEEE International Conference on Pervasive Computing and Communications (PerCom'04)*, ser. PERCOM '04. Washington, DC, USA: IEEE Computer Society, 2004, pp. 309–. [Online]. Available: http://dl.acm.org/citation.cfm?id=977406.978701

[19] R. Anderson, H. Chan, and A. Perrig, "Key infection: smart trust for smart dust," in *Network Protocols, 2004. ICNP 2004. Proceedings of the 12th IEEE International Conference on*, Oct 2004, pp. 206–215.

[20] T. K. Buennemeyer, M. Gora, R. C. Marchany, and J. G. Tront, "Battery exhaustion attack detection with small handheld mobile computers," in *Portable Information Devices, 2007. PORTABLE07. IEEE International Conference on*, May 2007, pp. 1–5.

[21] A. Merlo, M. Migliardi, and L. Caviglione, "A survey on energy-aware security mechanisms," *Pervasive and Mobile Computing*, vol. 24, pp. 77 – 90, 2015, special Issue on Secure Ubiquitous Computing. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1574119215000929

[22] H. Kim, J. Smith, and K. G. Shin, "Detecting energy-greedy anomalies and mobile malware variants," in *Proceedings of the 6th International Conference on Mobile Systems, Applications, and Services*, ser. MobiSys '08. New York, NY, USA: ACM, 2008, pp. 239–252. [Online]. Available: http://doi.acm.org/10.1145/1378600.1378627

[23] X. Ma, P. Huang, X. Jin, P. Wang, S. Park, D. Shen, Y. Zhou, L. K. Saul, and G. M. Voelker, "edoctor: Automatically diagnosing abnormal battery drain issues on smartphones," in *Presented as part of the 10th USENIX Symposium on Networked Systems Design and Implementation (NSDI 13)*. Lombard, IL: USENIX, 2013, pp. 57–70. [Online]. Available: https://www.usenix.org/conference/nsdi13/technical-sessions/presentation/ma

[24] P. Huang, T. Xu, X. Jin, and Y. Zhou, "Defdroid: Towards a more defensive mobile os against disruptive app behavior," in *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services*, ser. MobiSys '16. New York, NY, USA: ACM, 2016, pp. 221–234. [Online]. Available: http://doi.acm.org/10.1145/2906388.2906419

[25] X. Gao, D. Liu, D. Liu, H. Wang, and A. Stavrou, "E-android: A new energy profiling tool for smartphones," in *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, June 2017, pp. 492–502.

[26] R. Falk and H. J. Hof, "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*, June 2009, pp. 191–196.

[27] M. Brownfield, Y. Gupta, and N. Davis, "Wireless sensor network denial of sleep attack," in *Information Assurance Workshop, 2005. IAW '05. Proceedings from the Sixth Annual IEEE SMC*, June 2005, pp. 356–364.

[28] D. Raymond, R. Marchany, M. Brownfield, and S. Midkiff, "Effects of denial of sleep attacks on wireless sensor network mac protocols," in *Information Assurance Workshop, 2006 IEEE*, June 2006, pp. 297–304.

[29] M. Keskilammi, L. Sydänheimo, and M. Kivikoski, "Radio frequency technology for automated manufacturing and logistics control. part 1: Passive rfid systems and the effects of antenna parameters on operational distance," *The International Journal of Advanced Manufacturing Technology*, vol. 21, no. 10, pp. 769–774, Jul 2003. [Online]. Available: https://doi.org/10.1007/s00170-002-1392-1

[30] C. Zhou and J. D. Griffin, "Accurate Phase-Based Ranging Measurements for Backscatter RFID Tags," *IEEE Antennas and Wireless Propagation Letters*, vol. 11, pp. 152–155, 2012.

[31] Q. Chai and G. Gong, "BUPLE: Securing Passive RFID Communication through Physical Layer Enhancements," in *RFID. Security and Privacy*, A. Juels and C. Paar, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 127–146.

[32] U. Madawala, J. Stichbury, and S. Walker, "Contactless power transfer with two-way communication," in *Industrial Electronics Society, 2004. IECON 2004. 30th Annual Conference of IEEE*, vol. 3, Nov 2004, pp. 3071–3075 Vol. 3.

[33] W. Choi, W. Ho, X. Liu, and S. Hui, "Bidirectional communication techniques for wireless battery charging systems & portable consumer electronics," in *Applied Power Electronics Conference and Exposition (APEC), 2010 Twenty-Fifth Annual IEEE*, Feb 2010, pp. 2251–2257.

[34] J. Wu, C. Zhao, Z. Lin, J. Du, Y. Hu, and X. He, "Wireless power and data transfer via a common inductive link using frequency division multiplexing," *IEEE Transactions on Industrial Electronics*, vol. 62, no. 12, pp. 7810–7820, Dec 2015.

[35] D. van Wageningen and T. Staring, "The Qi wireless power standard," in *Power Electronics and Motion Control Conference (EPE/PEMC), 2010 14th International*, Sept 2010, pp. S15–25–S15–32.

[36] Wireless Power Consortium, "Qi System Description, version 1.1.2," Tech. Rep., 2013.

[37] X. Gao, "Demodulating Communication Signals of Qi-Compliant Low-Power Wireless Charger Using MC56F8006 DSC," Freescale Semiconductor, Tech. Rep., 2013.

[38] J. Jadidian and D. Katabi, "Magnetic MIMO: How to Charge Your Phone in Your Pocket," in *Proceedings of the 20th Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '14. New York, NY, USA: ACM, 2014, pp. 495–506. [Online]. Available: http://doi.acm.org/10.1145/2639108.2639130

[39] L. Shi, Z. Kabelac, D. Katabi, and D. Perreault, "Wireless power hotspot that charges all of your devices," in *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '15. New York, NY, USA: ACM, 2015, pp. 2–13. [Online]. Available: http://doi.acm.org/10.1145/2789168.2790092

[40] B. Waters, B. Mahoney, V. Ranganathan, and J. Smith, "Power delivery and leakage field control using an adaptive phased array wireless power system," *Power Electronics, IEEE Transactions on*, vol. 30, no. 11, pp. 6298–6309, Nov 2015.
[41] A. Kurs, A. Karalis, R. Moffatt, J. D. Joannopoulos, P. Fisher, and M. Soljacic, "Wireless power transfer via strongly coupled magnetic resonances," *Science*, vol. 317, no. 5834, pp. 83–86, July 2007. [Online]. Available: http://dx.doi.org/10.1126/science.1143254
[42] S. Chang, S. Kumar, and Y. Hu, "Cognitive wireless charger: Sensing-based real-time frequency control for near-field wireless charging," in *IEEE International Conference on Distributed Computing Systems (ICDCS) 2017*, 2017.
[43] B. Waters, A. Sample, and J. Smith, "Adaptive impedance matching for magnetically coupled resonators," in *Progress in Electromagnetics Research Symposium*, 2012, pp. 694–701.
[44] S. O'Driscoll, A. S. Y. Poon, and T. H. Meng, "A mm-sized implantable power receiver with adaptive link compensation," in *IEEE International Solid-State Circuits Conference - Digest of Technical Papers*, Feb 2009, pp. 294–295.
[45] D. Baarman, S. McPhilliamy, and C. Houghton, "Inductively powered apparatus," Oct. 10 2006, US Patent 7,118,240. [Online]. Available: https://www.google.com/patents/US7118240
[46] K. Lee, Y. Kim, K. Byun, and S. YEO, "Method for controlling charging power and wireless charging apparatus for the same," Jun. 2 2015, US Patent 9,048,683. [Online]. Available: https://www.google.com/patents/US9048683
[47] V. Talla, B. Kellogg, B. Ransford, S. Naderiparizi, S. Gollakota, and J. R. Smith, "Powering the Next Billion Devices with Wi-Fi," *arXiv preprint arXiv:1505.06815*, 2015.
[48] R. Vyas, H. Nishimoto, M. Tentzeris, Y. Kawahara, and T. Asami, "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*, June 2012, pp. 1–3.
[49] J. R. Smith, A. P. Sample, P. S. Powledge, S. Roy, and A. Mamishev, "A wirelessly-powered platform for sensing and computation," in *Proceedings of the 8th International Conference on Ubiquitous Computing*, ser. UbiComp'06. Berlin, Heidelberg: Springer-Verlag, 2006, pp. 495–506. [Online]. Available: http://dx.doi.org/10.1007/11853565_29
[50] H.-J. Chae, M. Salajegheh, D. J. Yeager, J. R. Smith, and K. Fu, *Maximalist Cryptography and Computation on the WISP UHF RFID Tag*. New York, NY: Springer New York, 2013, pp. 175–187. [Online]. Available: http://dx.doi.org/10.1007/978-1-4419-6166-2_10
[51] J. Perzow, "Measuring wireless charging efficiency in the real world," *WPC Trade Conference*, November 2015. [Online]. Available: https://www.wirelesspowerconsortium.com/data/downloadables/1/5/2/7/john-perzow-efficiency-of-wireless-charging.pdf
[52] R. Allain, "Wi-Fi Charging Works, But it Can't Really Power Your Phone," *Wired*, June 2015. [Online]. Available: http://www.wired.com/2015/06/power-wifi-isnt-think/
[53] J. Nadakuduti, L. Lu, and P. Guckian, "Operating frequency selection for loosely coupled wireless power transfer systems with respect to rf emissions and rf exposure requirements," in *Wireless Power Transfer (WPT), 2013 IEEE*, May 2013, pp. 234–237.
[54] WiTricity, "Highly resonant wireless power transfer: safe, efficient, and over distance," Tech. Rep., 2012.
[55] M. Healy, T. Newe, and E. Lewis, "Security for wireless sensor networks: A review," in *Sensors Applications Symposium, 2009. SAS 2009. IEEE*, Feb 2009, pp. 80–85.
[56] M. Kaur and S. Singh, "A study on networking techniques of wban system," in *International Research Journal of Engineering and Technology (IRJET)*, Dec 2015, pp. 80–85.
[57] B. Kellogg, V. Talla, S. Gollakota, and J. R. Smith, "Passive Wi-Fi: Bringing Low Power to Wi-Fi Transmissions," in *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*. Santa Clara, CA: USENIX Association, Mar. 2016, pp. 151–164. [Online]. Available: https://www.usenix.org/conference/nsdi16/technical-sessions/presentation/kellogg
[58] N. Kamijoh, T. Inoue, C. M. Olsen, M. T. Raghunath, and C. Narayanaswami, "Energy Trade-offs in the IBM Wristwatch Computer," in *Proceedings of the 5th IEEE International Symposium on Wearable Computers*, ser. ISWC '01. Washington, DC, USA: IEEE Computer Society, 2001, pp. 133–. [Online]. Available: http://dl.acm.org/citation.cfm?id=580581.856575
[59] N. Tesla, "Apparatus for transmitting electrical energy." Dec. 1 1914, uS Patent 1,119,732. [Online]. Available: http://www.google.com/patents/US1119732