Wireless Power Authentication Protocol and System Design

Chin-Po Su
University of Michigan, EECS dept.

Pallavi M. Moghe
University of Michigan, EECS dept.

1 Abstract

Wireless charging is already becoming commonplace with more wireless powered products, and we are expecting this technology to be more public and have longer transmission distance. However, this brings new attack surfaces for security considerations, including how to prevent unauthorized devices from receiving power and prevent the attacks of stealing wireless energy. In this paper we combined theoretical analysis with simulations to show that fast frequency hopping is one of the possible methods to achieve secured wireless energy channel, while unauthorized devices can only receive $\approx 1\%$ of power compared to authorized devices. We also provided hardware and software design framework taking practical design issues into consideration and proposed a design for wireless power authentication protocol and hardware prototype.

2 Background

Inventor Nikola Tesla performed the first experiment in wireless power transmission. In the period 1891 to 1904 he experimented with Tesla coils, which generated high AC voltages, to transmit power for short distances without wires. In demonstrations at the 1893 Columbian Exposition in Chicago he lit light bulbs from across a stage. In 1901, he designed and built the Wardenclyffe Tower, which was intended to be a wireless signal and energy transmission station. The project's primary backer, financier J. P. Morgan, later refusing to fund further. Additional investment could not be found and the project was abandoned in 1906 and never became operational.[1]

In 2007, a team led by Marin Soljai at MIT used coupled tuned circuits made of a 25 cm resonant coil at 10 MHz to transfer 60 W of power over a distance of 2 meters (6.6 ft) (8 times the coil diameter) at around 40% efficiency[2] On July 2009, Eric Giler showcased Wireless Technology at TED Conference to power up a smart phone and the LCD screen on stage[3].

Wireless Power Consortium (WPC), Power Matters Alliance (PMA) and the Alliance for Wireless Power (A4WP) are three standardization bodies striving to take a leading position in the wireless charging market. Global technology leaders are now collaborating to make wireless power as ubiquitous as Wi-Fi.

The controlling device which houses the wireless power transmission circuitry and software protocol for device authentication, which we call in this paper the Power Access Point (PAP), is necessary to have a secure channel for the energy transmission as well as the authentication technology. Now we expect a new concept of simultaneous wireless information and power transfer (SWIPT)[4], also called wireless info-energy device has been proposed. Therefore, the need is to prevent rogue devices from harvesting the power supplied, to enable billing of authorized power users, and the management of wireless energy connections.

3 Related Work

Different wireless power technologies[5] including ones for short to mid range inductive coupling, resonance inductive coupling, capacitive coupling, magnetodynamic, or ones for further range transmission such as microwaves, and laser. Protocol in this paper focus on the short to mid range transmission while using the near-field technology.

"Wireless power transmission" is a collective term that refers to a number of different technologies for transmitting power by means of time-varying electromagnetic fields. In general a wireless power system consists of a "transmitter" device connected to a source of wired power, which converts the power to a time-varying electromagnetic field, and one or more "receiver" devices which receive the power and convert it back to DC or AC electric power which is consumed by an electrical device.

While the power transmission technology is relatively gaining progress, securing wireless transmission is not yet very mature. It is possible to use beamforming technique to achieve security energy transfer for some info-energy system[7]. However, beamforming requires signal to be directive, and is hard to achieve sharp beam in close range. On the other hand, the technique we propose is similar to Spread-spectrum signal structuring technique employing frequency hopping in telecommunications. Frequency-hopping spread spectrum (FHSS) is a method of transmitting radio signals by rapidly switching a carrier among many frequency channels, using a random sequence known to both transmitter and receiver[8]. The authentication technique we propose is similar to the one used in TLS/SSL authentication over the web.

4 Approach

The challenge for securing non-radiative wireless energy is, when transmitting EM waves in free space, its physical nature makes it hard to prevent near by devices from receiving or intercepting the signal in principle.

To prevent even receiving the signal energy, we propose a channel hopping protocol with the transmission frequency information being encrypted. The orthogonality of wave and the Coupled Mode Theory (CMT) make devices not in the resonance frequency can barely receive energy. Practically speaking, we first make two(or more) charging coils resonating when highly coupled and sensitive to incoming energy 's frequency(related to system's natural frequency). We tune the circuit selectivity, or Q factor, to a very high value, which means the energy being coupled is highly sensitive to this incoming frequency. If we model our load and charging pad as RLC series circuit, considering the case first without external coupling, then the selectivity can be tuned by selecting the total serial resistance in the system shown in Eq. 1

$$Q = \frac{1}{F_{\text{bw}}} = \frac{\omega_{res}}{\Delta\omega} = \frac{\omega_{res}L}{R} \tag{1}$$

$$\omega_{res} = \frac{1}{\sqrt{LC}} \tag{2}$$

To hop the system's natural frequency continually, we do it by changing the capacitance as shown in Eq. 2 by using variable capacitor. We then form a negative feedback control loop in order to set the system to the resonating frequency with high accuracy. Lastly the authentication protocol will share the transmission frequency information with the authorized devices and start the power transmission session between the resonating devices. This will induce all the authorized devices to resonate strongly and the other devices to remain loosely coupled and unable to receive the energy.

4.1 Building blocks of the system

- Resonant inductive coupling

  As one coil can be analyzed like an RLC oscillator, consider two coupled coils to together give us resonance.

  Resonant inductive coupling[2] is the resonance of EM field which occurs with two or more coils that transmit the energy wirelessly at near field. The linearization of resonance dynamics can be generalized using CMT as Eq. 3

$$\begin{aligned} \frac{da_1}{dt} &= -i(\omega_1 - i\Gamma_1)a_1 + i\kappa a_2 + f(t) \\ \frac{da_2}{dt} &= -i(\omega_2 - i\Gamma_2)a_2 + i\kappa a_1 \end{aligned} \tag{3}$$

  Where ω_1, ω_2 are the individual resonance frequencies (eigen frequencies), Γ_1, Γ_2 are the resonance widths due to the objects intrinsic (absorption, radiation etc.) losses, κ is the coupling coefficient, and $f(t)$ is the external driving term.

  We can show that using CMT, the resonant inductive mechanism allows for around Q^2 (10^6) times more power delivery for work at the device than the non-resonant ones[2], which is desired for our purpose of blocking non-resonating devices.

- Frequency-Locked Loop (FLL)

  A frequency-lock, or frequency-locked loop, is an electronic control system that generates a signal that is locked to the frequency of an input or "reference" signal, which will be used to lock the power source and power receiver with high accuracy.

  One thing noteworthy is that we are trying to change the system's natural frequency ω_{res}, rather than the frequency of a signal.

  We propose an analog filtering approach referencing the received power signal to form a self-resonating feedback loop to achieve high accuracy resonance. However, resonance sensing need measuring instruments with sweeping input. How to use compact sensors for very fast resonance detecting is still an research area in EE/MEMS/ME area and now lacking mature product for this purpose[9]. This makes our system security depend on this lacking of compact sensor or quick algorithm to measure the system's resonance frequency. We will discuss this effect in the Sec. 7.

- Phase-Locked Loop (PLL)

  Frequency hopping requires the power source and receiver to hop to new frequency in sync, otherwise

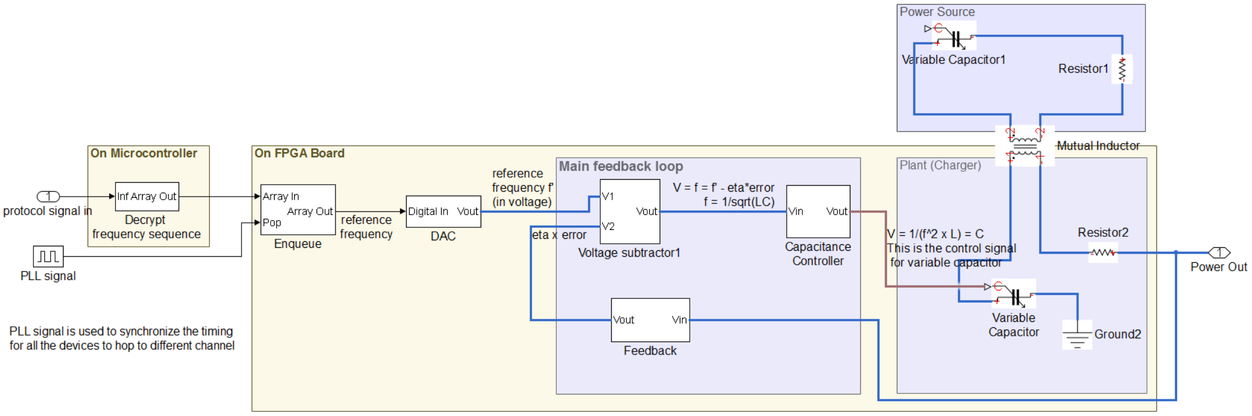


Figure 1: System Block Diagram

power transfer will remain lossy. This timing synchronization is achieved by using a phase-locked loop (PLL).

A PLL is a control system that generates an output signal whose phase is related to the phase of an input signal. It is an electronic circuit consisting of a variable frequency oscillator and a phase detector with feedback loop.

Our PLL signal is used to trigger a hardware queue to pop referencing frequency information toward the coil controlling circuit, and all the devices connected into our wireless power network are synchronized with the same PLL signal.

4.2 System Organization

The system shown in Fig.1 comprises of a microcontroller side, FPGA hardware and the coil circuit 3 parts.

The microcontroller can be any general purpose computing device such as a smartphone, a laptop or IoT nodes as well. The software protocol is implemented at this side and responsible for the decryption computation of the frequency key sequence, and the session handling for connection.

The FPGA comprises of real time logic components working as FLL and PLL for highly coupled resonance to work. In detail, this software defined radio like board has a hardware queue, digital to analog converter (DAC), and the main feedback loop including the capacitance controller and feedback controller. Moreover, in the real hardware, it also needs other power circuits to stabilize and regulate the voltage provided to our device which we ignore here now for simplicity sake.

The whole life cycle for a frequency hop protocol is as follows: First the protocol signal sends in p numbers of frequency sequence in 1 packet. The frequency sequence will be stored in the microcontroller memory with buffer size m, and the microcontroller will fetch a frequency key to do the decryption, and push it to the hardware queue.

The hardware queue has size q, and each time the FPGA, receives a PLL signal(the clock interval is the hopping interval time t_{hop}), the FPGA will pop a key from hardware queue, send it to DAC and into main feedback loop, and the capacitance value will be changed to the desired value as the system's resonating frequency.

We have provided an example setup in the evaluation section for a better understanding of this mechanism.

4.3 Circuit Design

The circuit in Fig.2 refers to our main control loop, and the charging coil. This circuit receives a voltage value as referencing capacitance value from DAC output, and will generate voltage signals to tune the variable capacitance for ω_{res}, and variable resistors for Q. ω_{res} can be computed by Eq. 2, and for choice of Q we will discuss in Sec. 5. Variable capacitor is connected to the charging coil and the device. The main control loop comprises of 2 parts: the parameter controller part, and the feedback part.

The feedback part references the power signal to form a self-resonating feedback loop to achieve high accuracy resonance. This works as we expect the power signal to be received at the band close to the system's natural frequency, but with small bandwidth across the spectrum. If there is only a small deviation from the correct resonating frequency, the receiver will be working at the "steep slope" of one side of the "resonance peak". Therefore, by sending the received power signal to a high and a low pass filter we can detect whether we are tuned at higher or lower than the desired resonance. By this analog approach, we can send this information as feedback signal without a compact sensor device being provided.

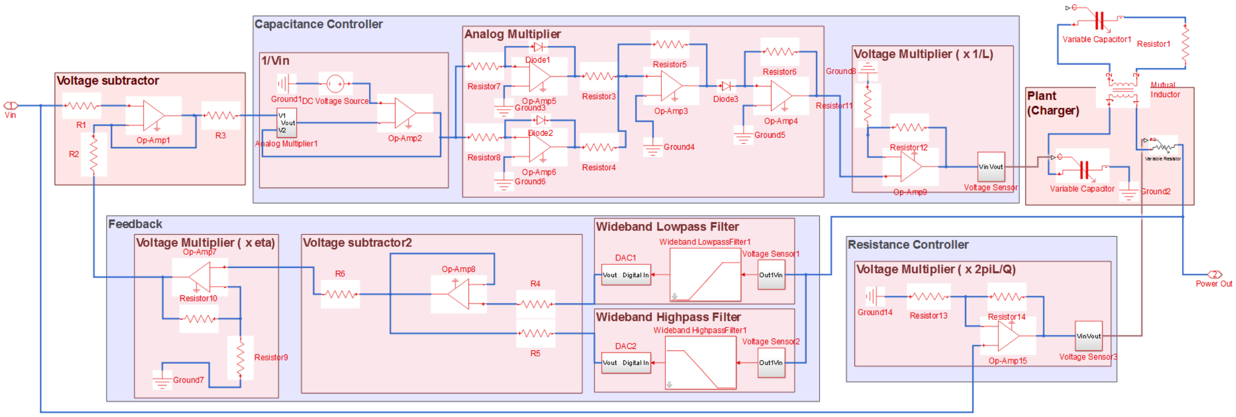


Figure 2: Circuit Block Diagram

4.4 Software Protocol Design

- Authentication

  The authentication process between the client and the PAP will use asymmetric key cryptography to share the symmetric/shared key. The client sends a probe making his presence known to the PAP. The PAP responds back with its public key. In response to this message, the client will generate a shared/symmetric key on his side and send it to the PAP. Henceforth, the messages between the client and the PAP will be encrypted using the symmetric key. The device will be authenticated based on a challenge response mechanism. When the authentication process succeeds i.e. when the user enters a valid response to the challenge, a power transmission session will be established. Figure below illustrates this authentication process.

- Frequency Hopping

  We propose a frequency hopping scheme in the power transfer module of the PAP to ensure secure power transmission. After the authentication succeeds, the power transmitter in our scheme will generate a string of random frequencies. The string will encompass an “optimal count” of randomly generated frequencies in the chosen band of power transmission.

  The PAP shares this string with the authenticated client device for synchronization. The PLL synchronizes the clocks on the client device and the PAP. Once done, the PAP starts transmission, switching to the next random frequency very rapidly after every “safe interval”. The sequence will be regenerated for use over the next set of safe intervals. An eavesdropper will have difficulty intercepting a transmission in real time if the random sequence is not known. The fast frequency hopping technique will also make the system resilient to deliberate jamming attempts by adversaries.

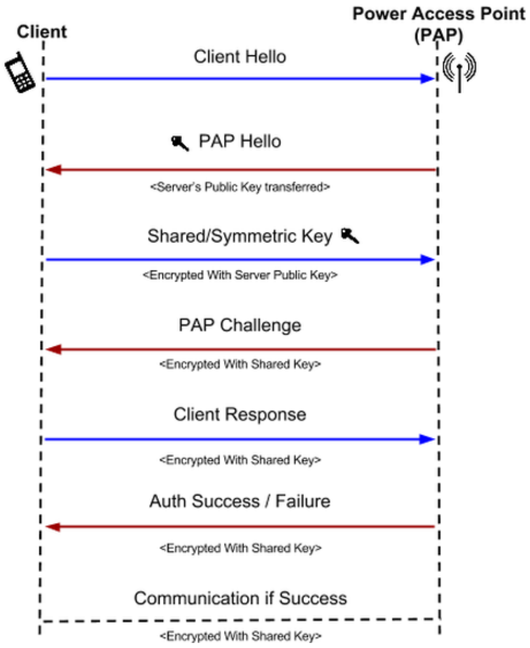

Client
Power Access Point (PAP)
Client Hello
PAP Hello
<Server's Public Key transferred>
Shared/Symmetric Key
<Encrypted With Server Public Key>
PAP Challenge
<Encrypted With Shared Key>
Client Response
<Encrypted With Shared Key>
Auth Success / Failure
<Encrypted With Shared Key>
Communication if Success
<Encrypted With Shared Key>

Figure 3: Authentication Protocol

5 Other Design Considerations

In order to make the system to work practically, we also need to take care of the following conditions:

- Band selection

  When designing the system, the efficiency, amount of power transferred and heat generated affected by the band should also be taken into consideration. We notice that the maximum efficiency point of the system is not necessarily the point of maximum power transfer, though they usually tend to be close.

From Eq. 3 we can derive the efficiency expression in Eq. 4, and by taking the derivative of it wrt. $\frac{\Gamma_2}{\Gamma_L}$, we can determine optimum resistor value[10] for $R_{L,opt} = \Gamma_{L,opt} L = \frac{\omega_{res} L}{Q_{L,opt}}$ as shown in Eq. 5

$$\eta = \frac{P_L}{P_S} = \frac{1}{1+\frac{\Gamma_2}{\Gamma_L}(1+\frac{\Gamma_2\Gamma_3}{\kappa}(1+\frac{\Gamma_L}{\Gamma_3}))} \tag{4}$$

$$\Gamma_{L,opt} = \frac{\Gamma_2}{\sqrt{(1+K_{12}^2/\Gamma_1\Gamma_2)}}. \tag{5}$$

We notice that if we fix Q-factor, the required optimum resistor value will change with the ω_{res}. We choose to have a fixed Q and variable resistor to simplify the design. However, a design with variable Q may give a better performance.

Consider R_1, and R_2, since they should be small for high Q, we can simply just use the serial resistance in the coil to be the lowest possible resistance in our band, and add variable serial resistor to change it.

After deciding the resistor value for optimum transfer efficiency, a simulation for different resonance frequency can be done Fig. 4. In this implementation, we choose two coils with $L = 10\mu H, R1 = 80m, R2 = 500m$, and we choose a band from 1MHz to 100MHz.

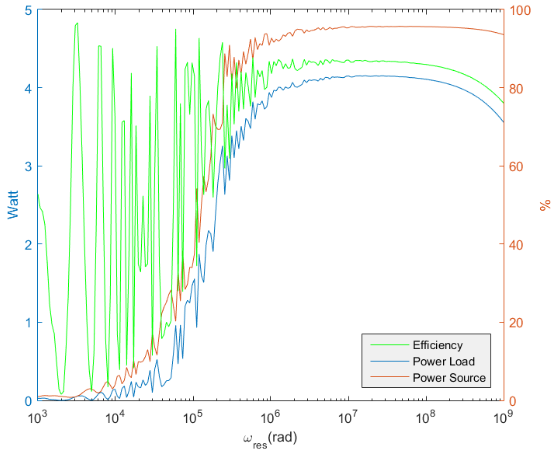


Figure 4: Analysis for efficiency / amount of power transferred at different frequency

- Number of Channels

  After the band selection, we can divide the band into n different channels. Despite it can be discrete as well, here we use the channel as a continuous number. Now we define channel coefficient in Eq. 6.

  $$n = \gamma Q_{res} \log BW = \gamma \log BW \frac{\omega_{res}}{\Delta\omega} \tag{6}$$

  This coefficient decides how close two channels will be, where BW is the total bandwidth, $\Delta\omega$ is the width of the resonant power curve at half maximum, which means a channel γ number away will be able to receive 50% of power compared at resonance peak. For our implementation, we pick n = 20 while $\gamma \approx 0.02$.

- Transient effect during hopping

  During the hopping, a larger hop will have worse transient effects such as spike in our design. When hopping toward a higher frequency, the settling time for circuit to reach resonance will be longer due to slow capacitor charging, which causes a drop in the amount of energy being delivered. When hopping toward a lower frequency, there will be a sharp voltage and energy spike that might damage the circuit, due to the fast decay of the magnetic energy in inductor.

  We will show in result section how these transient effects affect the performance of our system. To reduce the transient effect, we can either introduce voltage / current spike protection circuit, or change our random frequency sequence generation scheme.

- Real time issue for the protocol stability

  The protocol should not only be secure for power transmission, but also be stable with respect to power transmission and session maintenance. The following parameters should be optimized to prevent buffer overflows in real time, and the ability to restore transmission even after few hiccups on the resonance frequency sequence.

  Statistical analysis should be done to derive optimal values of the following parameters:

  - Packet Size p
    A single packet will have n number of frequency keys. This value will determine the size of the packet. We can send number of frequency hops per second to be proportional to the packet size.
  - Memory Buffer Size m
    This is the buffer size in the PAP and the client device. This should be defined in the standard,

and it would depend on the rate at which the system hops to the next frequency and packet transmission rate. The buffer should be large enough to prevent overwriting of frequency keys in queue.

- Hardware Queue Size q
  This will define the hardware queue size in the PAP and client device.

The process for determining these buffer size can be related to the router buffer problem[12], and they should be determined theoretically for preventing underflow, otherwise the energy transfer will not be stable[11].

- Correction for the theoretical model of the coil

  We notice that for a real coil, mostly in spiral or helix form, the value of inductance and capacitance will change with frequency and current, and radiation resistance needs to be considered together with ohmic resistance as well[6]. For simplicity's sake, we use static value for R,L,C value related with coil for all the discussion in this paper. However, we should know that for real implementation, the value need to be updated accordingly, so that the controller command need be calibration based on these calculation.

  Right now we just need to take a look at radiative resistance shown in Eq. 7 and make sure it is small enough for the design parameter we pick. Here R_r is the radiative resistance of the coil, with n turns, radius r, and height h.

$$R_r = \sqrt{\frac{\mu_0}{\varepsilon_0}}[\frac{\pi}{12}n^2(\frac{\omega r^4}{c} + \frac{2}{3\pi}(\frac{\omega h^2}{c}))] \tag{7}$$

6 Results

We simulated the system on MATLAB and this section describes the simulation results. However, we expect a hardware prototype to be finished soon as future work. Below in Fig. 5 and Fig. 6 we can see significant different amount of power being received between our target device, which with the decrypted frequency key to hop to correct channel, and the rogue device without the key.

The simulation showed two samples of how source and load systems hop between each channel. During the hopping, the resonance builds up with time and reaches a state of steady energy transmission.

The power transfer efficiency (PTE) we use here is the load power divided by the source power,$PTE = \frac{V_{in} \times I_{in}}{V_{out} \times I_{out}}$. However, we should notice that capacitor is no longer just a energy storage device that changing the capacitor value should also do work toward the capacitor, which is another power input. The reason we neglect it is the work made by capacitor should be small since δC is small in our design. Therefore the real PTE should be defined in Eq. 8:

$$PTE = \frac{V_{out}I_{out} - \frac{1}{2}\Delta C_2 V_{C2}^2}{V_{in}I_{in} + \frac{1}{2}\Delta C_1 V_{C1}^2} \tag{8}$$

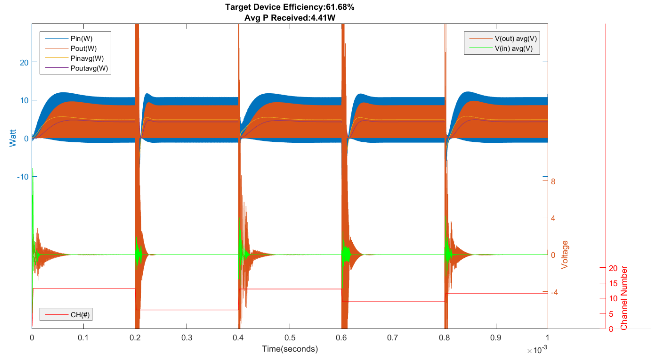


Figure 5: Target device during the hopping

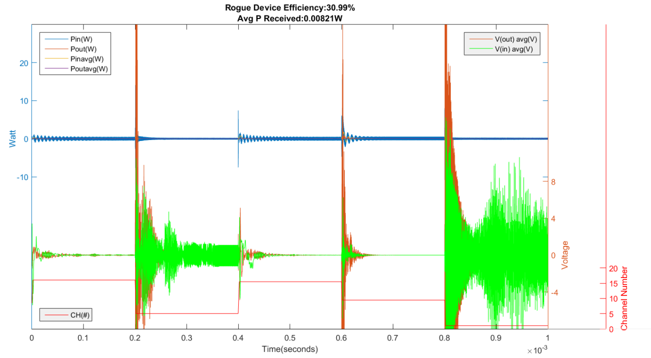


Figure 6: Rogue system during the hopping

We observed that during hopping, if the transient voltage spike peaks up high, it could be a potential problem to the circuit. However, these spikes appear in a very short period and do not carry substantial energy. One way to reduce the spike is reduce the resonance factor Q, since the spike should come from the mode changing of the resonance making large inductance energy coupled back to the coil. However, as long as we want a high resonance Q in this scenario, this might be a designing trade off problem. For a detailed results for a longer time simulation results is shown in table 6.

Table 1: Results for a longer Simulation

Simulation Period	100ms
P_{avg}	5.326W
PTE	82.33%
Data points	10^9
max step	$10^{(}-10)$
hops	1000
Band	1MHz - 100MHz
Number of channels	20
Q_1	1250
Q_2	200
Q_L	200
κ (coupling coefficient)	0.99

7 Security Feature Analysis

- Safe Interval t_{safe}

  In our scheme the hopping is done after a periodic interval $t_{hop} = \frac{1}{f_{hop}}$. The hopping frequency in a way determines the security of the system.

  Shorter the interval, the harder will be for the the attacker to use any kind of analysis methods to follow the resonating frequency. The safe interval is defined as the largest possible interval which guards the system against this attack. The defence lies is the fact that the transmitter will switch the carrier to the next random frequency by the time the attacker predicts the current frequency using any related mechanism.

  On the other hand, the system settling time is the time needed for an output to reach and remain within a specified error band following some input stimulus, usually symmetrical about the final value at the transient.

  The system should have a hopping interval smaller than the safe interval, but bigger than the system settling time t_{set}. We let the interval become t_{set} times coefficient K.

  $$t_{hop} = K \times t_{set} < t_{safe}, \qquad K > 1 \tag{9}$$

  Therefore, the effective percentage of time for energy transmission becomes $\frac{K-1}{K}$.

- Resonance sensitivity of the frequency

  We expect the energy gain to be fairly sensitive to the natural frequency of the system due to the resonance. However, in order to verify this, we deduced the state space expression for CMT in Eq. 10, which give us the solution for energy gain of a_2 in different system natural frequency ω_2.

  $$\begin{aligned} A &= \begin{bmatrix} -i(\omega_1 - i\Gamma_1) & i\kappa \\ i\kappa & -i(\omega_2 - i\Gamma_2) \end{bmatrix} \\ B &= \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad C = \begin{bmatrix} 0 & 1 \end{bmatrix}, \quad D = 0 \end{aligned} \tag{10}$$

  Solving the state space will give us the response with $Y(s)$ being the spectrum of the received EM wave, and $U(s)$ is the driving term, the frequency correspondents of the $f(t)$ in Eq. 3. We let this ratio to be $H(s)$.

  $$H(s) = \frac{Y(s)}{U(s)} = C(sI - A)^{-1}B \tag{11}$$

  We substitute s with $2\pi i f$ and integrate $H(f)$ from $-\infty$ to ∞ and plug into Eq. 12 and get the energy summation across the spectrum $E(f)$ on receiver.

  $$E(s) = |H(s)|^2 \tag{12}$$

  This gives us the energy gain for a specific natural frequency, we can do this and get all gain among different natural frequencies of the receiver, while source's natural frequency is given. We use ω_1 = 2000π, Γ_1 = Γ_2 = 0.001, and κ = 1 to model a near perfect resonance. In Figure 7 we see how energy gain changed highly sensitive to the correct resonance frequency as we desired.

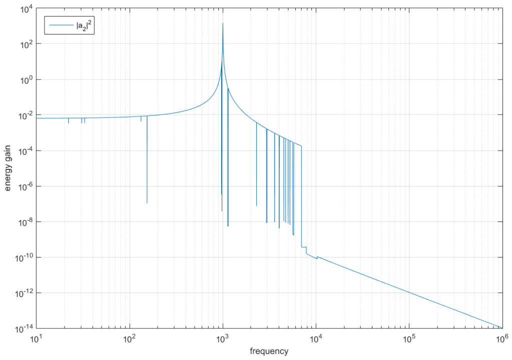


Figure 7: Resonance Sensitivity Simulation with different ω_2

- Wide Spectrum analysis attack

  Following up the discussion in 4.1, with dedicated instruments, it is possible to use a wide spectrum input pulse and detect the absorbed part to determine current system's resonating frequency at a high speed. Currently this type of equipment is bulky and expensive, but it is feasible to perform such interference and energy interception. For launching such an attack one may have to come up with compact sensor devices for detection of system natural frequency.

- Self-resonating convergence device attack

  As we mentioned before, a feedback loop design can be achieved for high accuracy frequency tracking. As can be observed in Figure 4, the two sides of the resonating curve are almost piecewise monotonically increasing / decreasing. The feedback loop will perform the real estimation of the frequency of the power source f, given the reference frequency f'. The difference between the two arises from the systematic error when in the hardware implementation. When the receiver coil couples with the energy on the spectrum, it will go through two analog filters and receive high and low parts of the energy amplitude. It will then determine the direction to update the real resonating frequency. The math has been illustrated in Eq. 13.

  $$f = f' + \eta \frac{dE(\omega_2)}{d\omega_2} \tag{13}$$

  It is possible to leverage this phenomenon and make a device to crack the resonance key with this mechanism. One can eventually restore the resonance frequency starting at an arbitrary initial frequency. However, since there is noise being introduced into the EM wave and circuit then to $E(\omega_2)$, we expect most of the estimation starting far away from the resonance frequency will be trapped at their adjacent local maximum, and only the starting point with the close enough reference starting frequency will be able to converge to true resonance frequency. Therefore the channel number shown in Eq. 6 together with the desired power transfer should be carefully pick to minimize the possibility to converge to correct resonance frequency to prevent this type of attacks.

8 Evaluation

8.1 Advantages of our approach

- Non-radiative: The energy transmitted by resonance inductive coupling is non-radiative, which means the energy not being received by the target will get coupled back into the resonance and not wasted and achieve high efficiency transmission.

- Short to mid range: Resonance inductive coupling is expected to be the primary technique in the new A4WP standard for mid-range power transmission. It will be compatible with close range charging pads as well as mid-range power transmission coming out in the near future.

- Supports information encryption: This frequency hopping technique can also be used on securing the information channel by simply let only target device able to receive the power of the signal. Therefore means it can add an additional layer of security upon cryptography.

- Easy to manufacture: The coil controller part Can be easily produced in chip form.

- Wireless communication can merge with power supply: For convenience of implementation, the band used for the traditional “communication carrier” and “energy carrier” should be different. However, theoretically, the band used to transmit information and energy can be the same. In the future, it can become possible to use the same coil / antenna to receive communication and power at the same time. The information part can be separated from the energy part and sent to two different components of the chip. This can reduce the need for extra hardware, reuse the power loss in the DSP procedure for communication, and save the band being occupied during transmission.

- Software defined ability: We propose building this mechanism into the hardware. However, the ability to change the crucial coupling parameters in software makes the design flexible in terms of updating the security protocols used underneath. Meanwhile, our implementation maintains some of the advantages of general wireless communication as mentioned ahead.

- Immune to traditional jamming: The channel hopping feature aids in preventing the low charging performance in a specific band if the background noise is not suitable for that band, and is naturally immune to a specific band transmission jamming attack or phenomenon.

- Allow multiple PAP in short range: This authentication method can allow multiple energy hot spots to transmit simultaneously in the same vicinity, while the receiving device would be able to select which source to connect to based on signal strength.

8.2 Shortcomings of our approach

- Authentication needs device to be alive: Since the authentication mechanism requires the device to be powered up, this mechanism will not be able to charge a completely drained device.

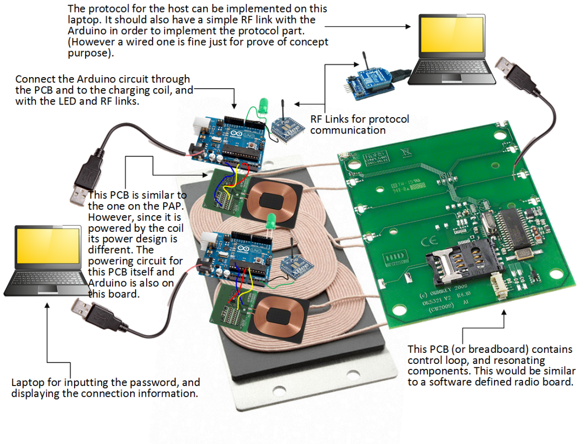
- Overhead energy usage: The frequency hopping, authentication and hardware tuning mechanisms have additional energy overheads.

- Decrease in available time for transmission: As we have elaborated in sec. 7, the valid time for transmitting energy is equal to $\frac{K-1}{K}$ as a result of the frequency hopping mechanism.

9 Future work

We plan to firstly test our authentication protocol on embedded systems charging. Eventually, we are working on a project to set up two Arduino devices with LEDs to indicate its on-off status both with charging modules, and another big charging pad connected with the embedded system to emulate the power distributing host. A more intuitive figure is shown in Fig. 8

While the power distributing host is always on and providing power to the charging pad, we will put two Arduino devices on the pad at same the time, and prove that without the correct password being provided, the device will not be able to harvest power even put adjacent enough to the source.



The protocol for the host can be implemented on this laptop. It should also have a simple RF link with the Arduino in order to implement the protocol part. (However a wired one is fine just for prove of concept purpose).

Connect the Arduino circuit through the PCB and to the charging coil, and with the LED and RF links.

RF Links for protocol communication

This PCB is similar to the one on the PAP. However, since it is powered by the coil its power design is different. The powering circuit for this PCB itself and Arduino is also on this board.

Laptop for inputting the password, and displaying the connection information.

This PCB (or breadboard) contains control loop, and resonating components. This would be similar to a software defined radio board.

Figure 8: Authentication Protocol

Other future works for theoretical ones including analysis for security robustness under convergence device attack with different noise level, analysis for optimum choice of channel number γ, analysis for resonance mode robustness under noisy environment, energy analysis for multiple device charging with multiple rogue devices, and analysis for trade off between resonance Q and transient voltage spike.

Besides, implementation future works including design for managing and maintaining wireless charging session, determining the real time issue parameters for stable transmission, designing better random sequence algorithm to reduce the transient voltage spike, and implementing and testing with convergence attack devices.

References

[1] Wikipedia, (2015). Wireless power. [online] [Accessed 25 Apr. 2015].

[2] Karalis, A., Joannopoulos, J. and Soljai, M. (2008). Efficient wireless non-radiative mid-range energy transfer. Annals of Physics, 323(1), pp.34-48.

[3] Giler, E. (2015). A demo of wireless electricity. [online] Ted.com. [Accessed 25 Apr. 2015].

[4] Chu, Z., Johnston, M. and Le Goff, S. (2015). SWIPT for wireless cooperative networks. Electronics Letters, 51(6), pp.536-538.

[5] Wu, K., Choudhury, D. and Matsumoto, H. (2013). Wireless Power Transmission, Technology, and Applications [Scanning the Issue]. Proc. IEEE, 101(6), pp.1271-1275.

[6] Kurs, Andr; Karalis, Aristeidis; Moffatt, Robert (July 2007). Wireless Power Transfer via Strongly Coupled Magnetic Resonances. Science 317: 8385

[7] Ng, D., Lo, E. and Schober, R. (2014). Robust Beamforming for Secure Communication in Systems With Wireless Information and Power Transfer. IEEE Transactions on Wireless Communications, 13(8), pp.4599-4615.

[8] Wikipedia, (2015). Spread spectrum. [online] [Accessed 25 Apr. 2015].

[9] Adams, T. and Layton, R. (2010). Introductory MEMS. New York: Springer. pp.184-186.

[10] Kiani, M. and Ghovanloo, M. (2012). The Circuit Theory Behind Coupled-Mode Magnetic Resonance-Based Wireless Power Transmission. IEEE Trans. Circuits Syst. I, 59(9), pp.2065-2074.

[11] Adan, I. and Resing, J. (2001). Queueing theory. Eindhoven: Eindhoven University of Technology. Department of Mathematics and Computing Science.

[12] Appenzeller, G., Keslassy, I. and McKeown, N. (2004). Sizing router buffers. SIGCOMM Comput. Commun. Rev., 34(4), p.281.