

Leveraging the Powerline to Support Very Low Power, Whole-House Wireless Sensing

Please note: we have created a supplementary video, available at <http://www.youtube.com/powerlinesensors> demonstrating the phenomenon explored in this work. We have made every effort to respect the double-blind process in posting this material and would very much appreciate if reviewers of this work were able to watch the video. If the program committee objects, we are happy to remove this note from the manuscript on request.

Abstract. A persistent concern of wireless sensor networks is the power consumption for communication, which presents a significant adoption hurdle. This work explores the use of the home powerline as a distributed reception antenna capable of receiving signals from very low-power wireless sensors and thus allowing these sensors to be detected at ranges that are otherwise impractical with over-the-air reception. We present several experiments that test the home powerline at various frequencies and show that the unlicensed 27.12 MHz band is an optimal choice for this task. We then demonstrate a wireless sensor network platform for the home that leverages this phenomenon and is able to be sensed throughout a home with just a 6.3 μ A average current draw for the radio.

1 Introduction

A consistently emerging theme in ubiquitous computing for the home is that while it is possible to think of the home as a sensor-rich environment, there are practical roadblocks to widespread deployment. Though our research community and others have begun to define more and more compelling applications of sensor-enabled environments, there remain too many obstacles to adoption by average householders. One constant concern is that of power requirements, particularly for wireless sensor networks. Wireless sensors are appealing because they can be placed in a variety of interesting locations, but the argument against them is that their current power consumption, largely attributed to wireless communication, limits the battery life to several months. Deploying tens and hundreds of these sensors in a home will result in weekly or daily requirements to change batteries.

In this paper, we present a technique to drastically reduce the power consumption requirements for transmission within a wireless sensor network. Inspired by recent work in ubicomp that has shown how the in-built infrastructure of a home can be used to simplify whole-house sensing [15, 17, 13, 14, 12, 7], we looked to find a way to use that infrastructure, specifically the domestic powerline, to support communication within a wireless sensor network. The PLP and WPLP work specifically used the powerline as a transmitting antenna for location tags around the home. PL-Tags showed a short-range, passive RFID-like

communication between the powerline, as a receiving antenna, and mobile tags [14]. Here we will show how an ultra low-power transmitting radio can wirelessly couple to the powerline to a directly coupled receiver, thus enabling a gateway receiver for a dense, distributed network of in-home sensors. Most importantly, the power requirements for this transmitter, measured in the range of tens of microwatts, drastically alters the design trade-off for energy consumption in a wireless sensor network. No longer will communication be the dominant feature in calculating power consumption. In the rest of this paper, we will develop the idea of using the domestic powerline as a conduit for wireless transmission of sensor data. In Section 2, we will explore how the powerline can be used as a conduit for HF, VHF and UHF radio transmissions and examine how frequencies in the unlicensed spectrum can be exploited for direct coupling communication via the powerline. In Section 3, we will establish why 27.12 MHz is the best alternative for exploiting wireless coupling from a transmitting sensor to the powerline. We provide empirical evidence from a home testbed that helps to characterize the range and limitations of this approach. In Section 4 we will provide evidence for how this powerline-assisted wireless transmission supports a platform for in-home wireless sensing, providing a comparison of power and data transmission efficiency compared to commercial alternatives and exploring application opportunities and security concerns.

2 The Powerline as a High-Frequency Signal Conduit

In this section, we explore the home powerline as a transmission line (no wireless communications, both transmitter and receiver directly connected) for signals at frequencies significantly higher than the power signal they were designed for. In order to act as a conduit for very low power wireless sensors, the powerline must be reasonably efficient at conducting signals of the frequency used by the sensor network. This section presents experimental data to demonstrate the feasibility of transmitting HF (3 - 30 MHz), VHF (30 - 300 MHz), and UHF signals (300 MHz - 3 GHz) over the powerline. We begin with a brief introduction to existing powerline communications technologies, and then explore the feasibility of using specific frequencies within these higher frequency ranges (HF, VHF, and UHF). This largely empirical process will lead to a small set of frequencies to explore within the radio spectrum for unlicensed communication.

2.1 Background: Powerline Communications

The home powerline, despite being designed to transmit low-frequency electrical power (typically at 50 - 60 Hz depending on the country), has been used successfully for communication at a variety of higher frequencies for various purposes. Home automation with X10, and more recently Insteon, has been a popular use of powerline communication. These standards utilize carrier frequencies of 120 kHz for X10 and 131.65 kHz for Insteon [23, 9]. Commercial home networking solutions, such as the Netgear XET1001 Ethernet-over-powerline system, show

the practicality of the powerline as a high-speed data transmission medium. Many of these solutions, including the XET1001, operate in accordance with the HomePlug standard, providing data rates up to 200 Mbps over the powerline and operating in the standard's defined 2-28 MHz range [8].

A benefit of using higher frequency signals on the powerline is their propagation range. In the US and Europe, homes are typically configured with a multi-phase power system which separates the home powerline into several isolated branches. This creates problems for X10 signals, since a controller may be plugged into one phase while a device it intends to control may be on another. The solution to this is to install a phase coupler either at the circuit breaker box or at a high voltage outlet (such as for a clothes dryer) where the phases come together. This allows the low frequency 120 kHz signals to propagate across the phases. Higher frequency signals (> 1 MHz) do not have this problem, however, as they are able to wirelessly couple between the phases at points where wiring from both phases runs close to one another (such as at the circuit breaker box). This is why Ethernet-over-powerline devices are able to cover an entire house without the use of a phase coupler.

2.2 Unlicensed Wireless Communications

We now motivate the frequencies at which we chose to explore the powerline as a signal conduit with a discussion on regulations regarding unlicensed wireless communications. The majority of the radio spectrum is reserved for licensed use. This ensures that wireless services such as mobile telephones, television and radio broadcasting, and radio-navigation services are generally free from interference. The International Telecommunication Union (ITU), a United Nations agency responsible for coordination of the radio spectrum on a global level, has specified several areas of radio spectrum that local governments should make available for unlicensed devices. These spectrum areas are commonly referred to as the Industrial, Scientific, and Medical (ISM) bands. Common ISM devices include WiFi (IEEE 802.11a/b/g) devices, Bluetooth devices such as wireless headsets, and wireless keyboards and mice with proprietary radio protocols. A list of the ITU suggested ISM spectrum is shown in Table 1.

Although in some countries, such as the United States, use of spectrum outside of the ISM regions is permitted (for example, under Part 15 of the US Federal Communications Commission regulations), we chose to focus our exploration on the ISM spectrum to make the work more globally applicable. Given this, we also chose to avoid utilizing the 433.92 MHz and 915.00 MHz bands since they are not globally available. Additionally, a large number of consumer electronic devices, such as cordless telephones and garage door openers, already operate in these bands and might cause interference for low-powered wireless sensors. Given this, we chose to explore five frequencies on the powerline: 6.78 MHz, 13.56 MHz, 27.12 MHz, 40.68 MHz, and 2.45 GHz.

Table 1. ITU specified Industrial, scientific, and medical (ISM) spectrum up to 2.4 GHz[5, 10].

Center Frequency	Range (MHz)	FCC Regulated Max. Field Strength	FCC Max. EIRP (dBm)
6.78 MHz ^a	±0.015	15 $\mu V/m$ @ 30 m	-51.71 dBm
13.56 MHz	±0.007	15,848 $\mu V/m$ @ 30 m	+8.77 dBm
27.12 MHz	±0.163	10,000 $\mu V/m$ @ 3 m	-15.23 dBm
40.68 MHz	±0.020	1,000 $\mu V/m$ @ 3 m	-35.23 dBm
433.92 MHz ^b	±0.870	—	—
915.00 MHz ^c	±13.000	—	+36.00 dBm ^d
2.45 GHz	±50.000	—	+36.00 dBm ^d

^a Subject to approval by the local regulatory body in the country of interest.

^b ITU Region 1 only (Europe, Africa, the Middle East west of the Persian Gulf, the former Soviet Union, and Mongolia).

^c ITU Region 2 only (The Americas, Greenland, and some eastern Pacific Islands).

^d For digital modulation schemes having bandwidth of at least 500 kHz.

2.3 Testing the Powerline at ISM Frequencies

To test the powerline as a transmission line at the selected frequencies, we built a high-frequency coupling box that allowed us to connect a spectrum analyzer to the powerline. This coupling box isolates the test equipment from the low-frequency, high-voltage power signal, but allows high frequency signals to pass through. A circuit diagram of this box is shown in Fig. 1. We utilized two of these coupling boxes: one to inject a high-frequency signal into the powerline using an Agilent E4433B signal generator, and one to measure the received signal with a Rhode & Schwarz FSH8 spectrum analyzer.

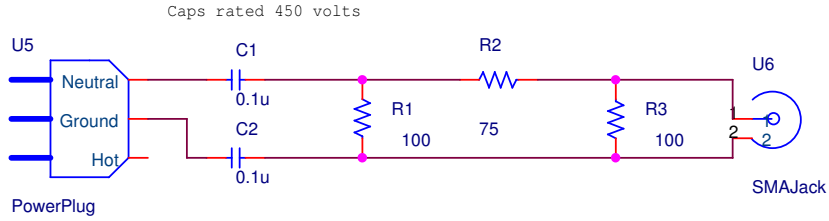


Fig. 1. The custom-built powerline coupling box. This box is used to connect a high-frequency receiver to the powerline while isolating it from the 50-60 Hz power signal.

Our experiments, the results of which are presented in Table 2, were performed in a 3-story, 371 square meter home built in 2003. A floor plan of the test environment is shown in Fig. 5. Data was obtained by using the signal generator to inject a 0 dBm (1 mW) signal into the powerline at each of the five frequencies. The signal generator was connected to the powerline via the coupling box plugged into an outlet in the dining room. During the tests the signal generator was powered by a UPS to isolate any signal leakage from its power supply. The received signal strength was then measured using the spectrum analyzer by connecting it to a single, representative outlet in each of nine listed rooms on the three floors. Average attenuation for the ISM frequencies from 6.78 MHz through 40.68 MHz ranged from 47 to 53 dB. At 2.45 GHz, no signal could be detected over the powerline in any of the rooms. Given this, we limit further exploration to 6.78 MHz, 13.56 MHz, 27.12 MHz, and 40.68 MHz.

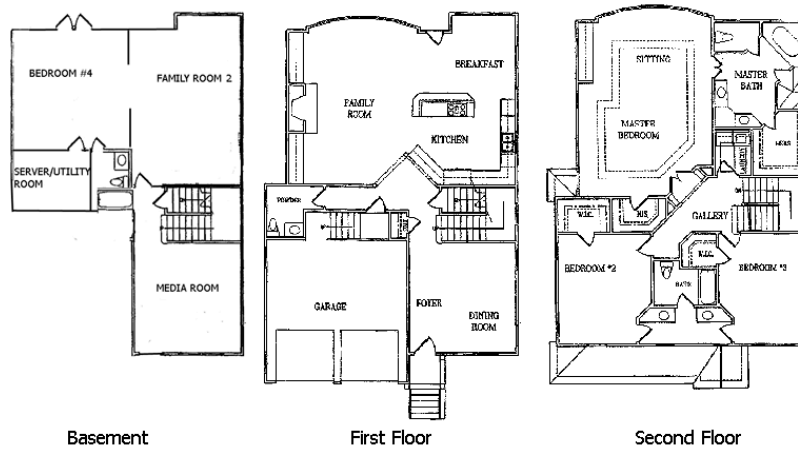


Fig. 2. Floor plan of the home that was utilized as one of the test environments. The home was constructed in 2003 and is 371 square meters.

Since, as noted in Section 2.1, Ethernet-over-powerline devices utilize spectrum from 2 to 28 MHz, we tested interference caused by these devices at the three ISM bands that fall within this range. To do so, we utilized two Netgear XET1001 HomePlug-based Ethernet-over-powerline devices, a laptop to generate traffic over the powerline-based network, and the spectrum analyzer to detect interference caused by the XET1001. We noted that the device generated significant interference at 6.78 MHz and 13.56 MHz when transmitting data, but that the 27.12 MHz band was clear.

Table 2. Received signal strength of a signal directly injected into the powerline, as sensed in each of nine rooms of the test home. The signal was injected in the dining room (see Fig. 5) at a power of 0 dBm, thus the numbers in this table represent the amount of attenuation caused by the powerline. No signal was detected over the powerline in any room for 2.45 GHz. The measured loss induced by the two powerline coupling boxes at each frequency was subtracted from these figures to give only the loss caused by the powerline.

Frequency (MHz)	Signal Strength (dBm)								
	Basement			1st Floor			2nd Floor		
	Media	Family #2	Bed #4	Dining	Kitchen	Family #1	Master Bed	Bed #2	Bed #3
6.780	-41.2	-57.5	-44.9	-19.2	-51.6	-50.8	-69.0	-72.0	-45.5
13.56	-56.8	-60.8	-61.1	-33.3	-53.1	-55.9	-57.1	-54.3	-50.2
27.12	-43.3	-53.5	-61.6	-21.7	-55.9	-61.6	-58.1	-50.4	-40.7
40.68	-38.3	-46.2	-66.7	-35.5	-44.6	-55.2	-53.9	-51.6	-31.1
2450	—	—	—	—	—	—	—	—	—

2.4 Summary

We summarize our exploration of the ISM bands we initially considered. 6.78 MHz and 13.56 MHz were eliminated due to interference from HomePlug-based Ethernet-over-powerline networks. 433.92 MHz and 915.00 MHz were eliminated since neither band is globally available and each is crowded with consumer devices that might cause interference. 2.45 GHz was eliminated since signals of this frequency did not transmit over the powerline. This leaves us with two ISM bands to consider: 27.12 MHz and 40.68 MHz. We will now explore the performance considerations of wireless transmission coupling at those frequencies.

3 Exploring The Powerline as a Receiving Antenna

3.1 Background and Related Work

Our exploration of the powerline as an antenna for receiving wireless signals is motivated by the PowerLine Positioning (PLP) and Wideband PowerLine Positioning (WPLP) work, which leverage the powerline as the infrastructure for a real-time indoor localization system [15,17]. PLP and WPLP utilize the powerline to wirelessly transmit signals, ranging in frequency from 400 kHz to 20 MHz and produced by one or more signal injector modules plugged into an outlet throughout a home. The principle of reciprocity in antenna design, that is, any given antenna is equally good at receiving and transmitting [11], suggests that the powerline would be a good receiver for at least the 400kHz - 20MHz range that was explored in the earlier work.

Additionally, inexpensive AM and FM clock radios often utilize a line cord antenna [21,6], which is comprised of a transformer and several capacitors to couple the radio’s input to the powerline (similar to our coupling box in Fig. 1).

We verified the capability of our test home’s powerline to receive signals in the US AM radio broadcast band by connecting the spectrum analyzer to the powerline and monitoring the 520 - 1610 kHz band (see Fig. 3). Line cord antennas have also been utilized for over-the-air VHF and UHF television reception [22].

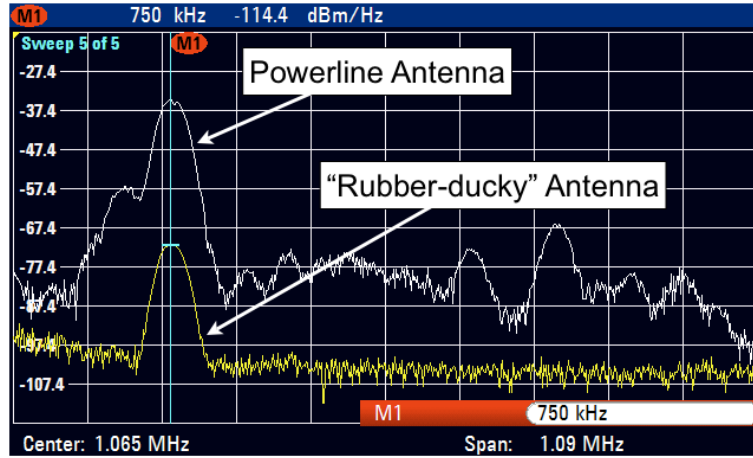


Fig. 3. The AM radio broadcast spectrum (520 - 1610 kHz in the US) as sensed by the spectrum analyzer when connected to the powerline through the coupling box of Fig. 1 and a standard “rubber ducky” antenna typical of hand-held radio scanners. Note that AM radio stations are received with much greater signal strength over the powerline antenna than with the rubber ducky antenna. A marker is placed at 750 kHz, which is a local AM radio station.

3.2 Factors leading to selection of 27.12 MHz

We begin our exploration of the powerline as a receiving antenna for low-power wireless signals originating within the home by making a final selection of a frequency to explore, between 27.12 MHz and 40.68 MHz, as discussed in Section 2. Since our objective is to use the powerline for receiving very low-power wireless transmissions, we need to select a frequency band that is relatively quiet on the powerline. Figure 3.2 illustrates the powerline background noise from 100 kHz to 42 MHz and specifically points out the two frequencies still in consideration (27.12 MHz and 40.68 MHz). Both of these fall in relatively quiet regions of the powerline, and so background noise levels did not influence our selection of one of these two.

Another consideration in selecting a frequency is the size of an efficient antenna at that frequency. For example, although the powerline has proven to be a reasonably reliable conduit for signals in the 100 kHz range (X10 and Insteon), frequencies this low are not practical for wireless communication. Although both X10 and Insteon offer wireless remote controls for operation of

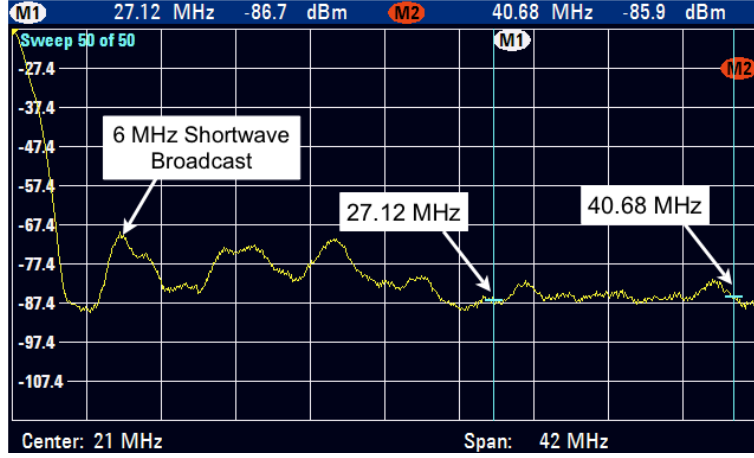


Fig. 4. Noise floor of the powerline from 100 kHz to 42 MHz using the coupling box shown in Fig. 1 and the R&S FSH-8 spectrum analyzer. The sample was taken in the kitchen of the test home, as shown in Fig. 5. The peaks generally represent various radio broadcasts from outside the home. The second from left, for example, is a 6 MHz shortwave-radio AM broadcast. Note that the noise floor is artificially raised by several dB when sampling such a large chunk of spectrum at once.

any X10 or Insteon-enabled device, these wireless remotes operate at higher frequencies (310 MHz in the US, under FCC Part 15 regulations) and do not directly couple with the powerline — a bridge between the high-frequency wireless channel and the low-frequency powerline channel is needed. There is a simple explanation for this. The size of an efficient antenna at any given frequency is proportional to the wavelength of the frequency. A common antenna design is the $\frac{1}{2}\lambda$ or $\frac{1}{4}\lambda$ dipole, where λ represents the wavelength of the frequency the antenna is designed to operate at. At 120 kHz, a $\frac{1}{4}\lambda$ dipole antenna would be 625 m long. In contrast, the higher frequencies utilized by HomePlug devices (2 - 28 MHz) are much more applicable to wireless communication. As a comparison, a $\frac{1}{4}\lambda$ dipole antenna at 28 MHz is 2.7 m, vs. 625 m at 120 kHz. The shorter wavelength of these higher frequencies is important in that the transmitting antenna for wireless sensors can be smaller, and also in that a typical home will contain numerous segments of powerline in the walls on the order of several meters, but certainly no segments of hundreds of meters.

We ultimately selected 27.12 MHz as the optimal frequency for powerline-based low-power wireless signal reception due to regulatory constraints. Revisiting Table 1, the third and fourth columns now become important. Within each frequency band, the FCC has specified a maximum power at which devices may operate [5]. This is typically specified as a maximum field strength in $\mu V/m$ at some distance from the transmitter. Equation 1 expresses the electric field as a function of the transmitter power (P_T), the antenna gain (T_G), and the distance from the transmitting antenna (r) [16].

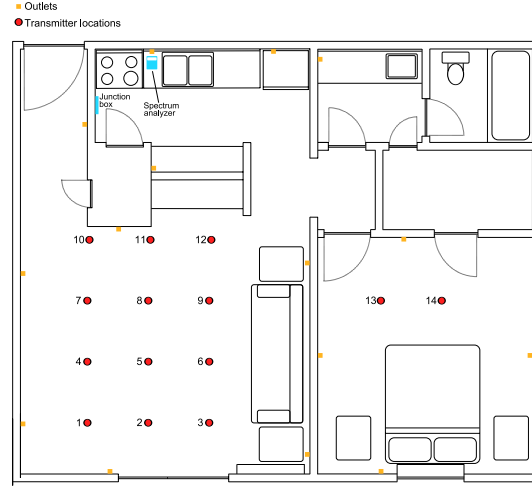


Fig. 5. Floor plan of the apartment used for tests. The building was constructed in approximately 1969 and the apartment is approximately 37 square meters. Numbered dots indicate test points for the heat-map shown later.

Table 3. ITU specified Industrial, scientific, and medical (ISM) spectrum up to 2.4 GHz[5, 10].

Center Frequency	Range (MHz)	Potential for Powerline-based Low-power Wireless Communication
6.78 MHz	± 0.015	Rejected: HomePlug devices interfere.
13.56 MHz	± 0.007	Rejected: HomePlug devices interfere.
27.12 MHz	± 0.163	Selected.
40.68 MHz	± 0.020	Rejected: FCC regulated maximum output power too low (-35.23 dBm).
433.92 MHz	± 0.870	Rejected: Not globally available.
915.00 MHz	± 13.000	Rejected: Not globally available.
2.45 GHz	± 50.000	Rejected: Experiments show powerline does not carry signals of this frequency.

$$E = \frac{\sqrt{30P_T G_T}}{r} \quad \text{Volts/meter} \quad (1)$$

$$P_T = \frac{E^2 r^2}{30} \quad (2)$$

Power in radio systems is often quoted as EIRP (Effective Isotropic Radiated Power), which refers to the power output of the system from a hypothetical isotropic antenna (a point-source which radiates equally in all directions). We can calculate EIRP from Equation 1 by setting G_T to 1 and rearranging to solve for P_T , giving Equation 2. These equations are how the fourth column of Table 1 was calculated. This column provides us with a good estimate of the maximum output power a wireless transmitter can have at each of these frequencies and still be within regulations. 40.68 MHz was ultimately eliminated from consideration based on this band's very low output power constraint of -35.23 dBm.

Table 3 now reflects our reasoning that leads to a selection of 27.12 MHz as the frequency for a very low-power wireless sensor network.

3.3 Receiving 27.12 MHz Signals Within the Home Using the Powerline

We first wanted to establish that strictly over-the-air communication was not possible at 27.12 MHz throughout our test home. We configured a transmitter, which consisted of a signal generator, producing a 27.12 MHz carrier signal at -35 dBm ($0.32 \mu\text{W}$) and AM modulated with a 550 Hz tone, connected to a 27 MHz Citizens' Band antenna that was placed close to an outlet in the dining room. The receiver consisted of a hand-held radio scanner (a RadioShack PRO-97) tuned to 27.12 MHz and used to listen to the 550 Hz tone. We did a quick survey of the test home using the "rubber-ducky" antenna that came with the scanner.

Where the 550 Hz tone can be heard clearly, the 27.12 MHz carrier signal is considered to be strong enough; where the tone cannot be heard indicates that the signal is too weak to be detected there. We quickly observed that outside of the dining room/foyer area where the transmitting antenna was placed, the signal was generally too weak to be detected by the scanner. We noticed, however, that when bringing the scanner's antenna close to an outlet, wall switch, or other plugged-in electrical device, the signal could be heard faintly. This indicates that the 27.12 MHz signal coupled from the transmitting antenna onto the powerline and was being radiated, albeit weakly, by the powerline at various other points in the home.

In practice, the receiver will be connected directly to the powerline, so the next step was to connect the scanner to the powerline via the coupling box of Fig. 1. We did this at a variety of outlet locations throughout the home and noted that the signal could be easily detected in every room of the home by directly connecting to the powerline. Not every outlet resulted in good reception, but the vast majority of outlets were satisfactory.

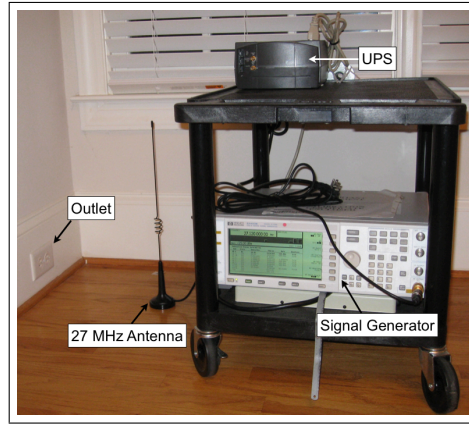


Fig. 6. Setup for initial testing of the powerline as a receiving antenna. The signal generator was electrically isolated by being placed on a plastic cart and powered by a UPS. A 27 MHz antenna (a Cobra HG A1000 designed for Citizens' Band radio use) was used to transmit a 27.12 MHz signal AM modulated at 550 Hz and at a power of -35 dBm ($0.32 \mu\text{W}$).

Given this empirical evidence suggesting that the 27.12 MHz signal coupled to the powerline over the air, we wanted to see how far away the transmitting antenna could be from the powerline and still be sensed by a powerline connected receiver at most outlets within the home. To do this, we moved the antenna away from an outlet in increments of 2.5 cm and used the powerline coupled scanner to check for the signal at various outlets throughout the home. We found that at a transmitter output power of -35 dBm, the antenna could be up to 60 cm away from the outlet before the signal was too weak to be detected by the receiving scanner. Generally, the further the antenna was away from the powerline, the weaker the signal detected by the scanner. Coupling is not limited to outlets, however. We noted that a similar effect could be observed by bringing the transmitting antenna close to other electrical wiring, such as a wall switch.

As a final test, we observed that some of the outlets in the test home served as particularly good coupling locations for the receiver. One of these, located in the basement, is near to the circuit breaker for the entire house, and so is in close proximity to every circuit in the home as result. Connecting the receiver to this outlet allowed us to test the range of the transmitting antenna in a best-case scenario. Fig. 7 shows a heat-map of the received signal strength along the first floor of the test home, indicating that the antenna's signal was strong enough throughout almost the entire first floor. We also repeated this test in a small apartment, as shown in Fig. 8. While there are some important limitations to this test (we only took measurements from a fixed height of approximately one foot off the ground), it does reveal great promise for using this solution to support a whole-house wireless sensing solution. We explore the larger systems issues of whole-house, low-power sensing in the next section.



Fig. 7. A heat-map of the test home first floor indicating the Signal-to-Noise Ratio (SNR) for a 27.12 MHz wireless transmitter at each indicated location as received by a fixed powerline coupled receiver in the basement. The transmitter utilized an output power of -25 dBm ($3.2 \mu\text{W}$) and a custom-built 27 MHz loop antenna.

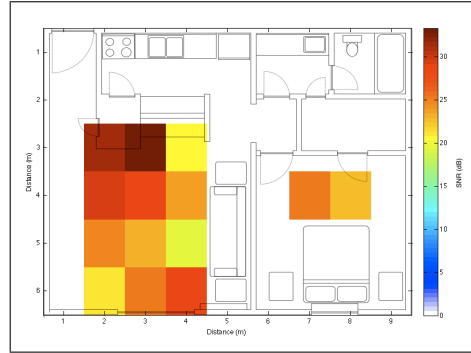


Fig. 8. A heat-map of the test apartment indicating the Signal-to-Noise Ratio (SNR) for a 27.12 MHz wireless transmitter at each indicated location as received by a fixed powerline coupled receiver in the kitchen. The transmitter utilized an output power of -35 dBm ($0.32 \mu\text{W}$) and a custom-built 27 MHz loop antenna.

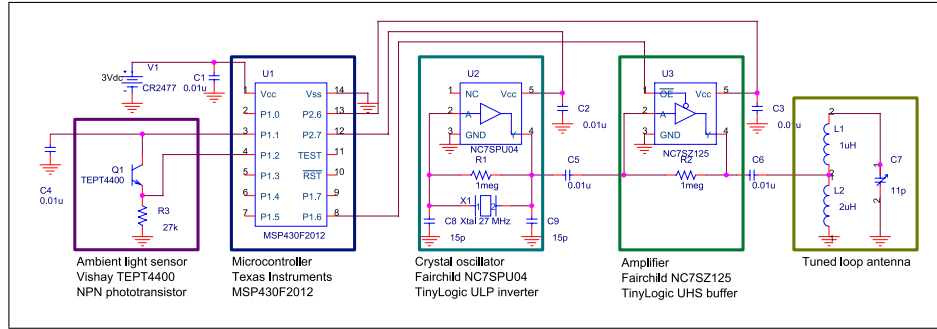


Fig. 9. A circuit diagram of our custom-built powerline-based wireless sensor.

4 Whole-House, Low-Power Sensing

4.1 A Platform For Powerline-Based Sensing

Given our success in detecting an AM modulated 27 MHz carrier signal from a wireless transmitter over the powerline, we wanted to build a real platform for sensing around this phenomenon. We used a Texas Instruments MSP430 microcontroller [20] with an attached light sensor and a custom-built 27 MHz radio. The radio consisted of a 27.12 MHz crystal with a low-power amplifier. The crystal and amplifier could be turned on and off by adjusting the voltage on a control pin, which was driven by the MSP430’s serial bus output.

We chose On-Off-Keying (OOK) as the modulation scheme for transmitting data from the sensor. On-Off-Keying — wherein the transmitter is on to transmit a one and off to transmit a zero — is a very efficient modulation scheme for low-power devices as the transmitter does not expend any energy to transmit a zero. Our sensor transmitted a packet of 16 bits once per second at a bit rate of 62.5 kilobits per second. The 16 bits consisted of five bits for the sensor’s ID, followed by ten bits for the value of the light sensor, followed by one stop bit — if more than 32 sensors are needed per home, or if more granularity is desired in the sensor reading, additional bits can easily be added to the packet as appropriate.

Since the objective of the sensor node is to transmit readings from its sensor, we elected not to include the ability for the node to receive data. This keeps the hardware cost and complexity down, as well as reduces power consumption of the node. The sensor, radio, and antennas are shown in Fig. 10, and a circuit diagram of the sensor and radio is shown in Fig. 9.

Our custom 27 MHz radio operates on just 1.5 mA at 1.2 V (this is in addition to the $165\mu A$ used by the MSP430 microcontroller). We programmed the microcontroller to transmit a sensor reading once per second and to shut off the oscillator during the interim sleep period, making the sensor’s duty cycle 0.941 milliseconds. With the amplifier and oscillator we used, the transmit power was actually more than sufficient to be sensed everywhere in the house, and so the power draw could actually be made less by utilizing more efficient oscillators and amplifiers.

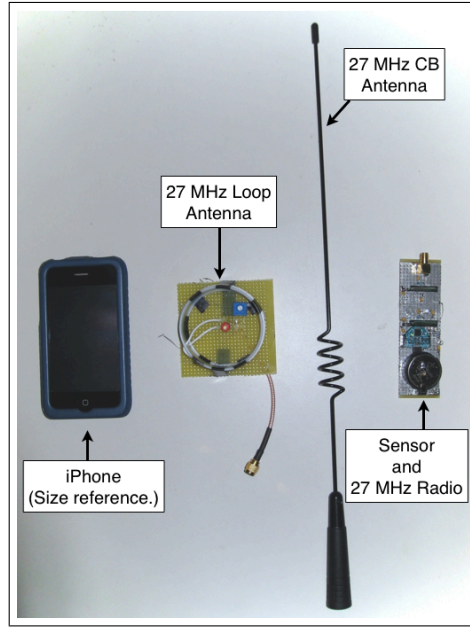


Fig. 10. Our wireless sensor platform along with two 27 MHz antennas.

We tested two types of antennas with the sensor, both pictured in Fig. 10. One was a CB antenna measuring 43 cm tall and the other a custom-built loop antenna measuring 6.5 cm long x 6.5 cm wide x 2 cm tall. The transmit power necessary for sensor data reception is a function of the efficiency of the antenna. Clearly the loop antenna has a size advantage in terms of enabling a compact form factor for in-home sensors, however both of these antennas are relatively small compared to the 11.06 m wavelength at 27.12 MHz, meaning that both are reasonably inefficient at this frequency. The efficiency of the powerline as a receiving antenna at 27 MHz largely makes up for this, but since we desire to operate the sensors at as low a power output as possible so as to increase their lifespan, a more efficient antenna will allow a lower transmit power. Thus, longevity of the sensor is a direct tradeoff with antenna size. We found that a sensor built around the larger 43 cm CB antenna was able to transmit at a power level of about 2 dB less on average in order to be detected with the same SNR as with the loop antenna.

4.2 Range & Power Efficiency - PL Sensing vs. Existing Technologies

Powerline-based wireless sensors should be evaluated against existing wireless sensing technologies on two fronts — range and power efficiency. Communication range of wireless sensors is an important consideration since sensors must be able to communicate with a base-station to transmit readings. The primary

model of enabling low power wireless sensor networks to date has been multi-hop mesh networking [2], wherein if a sensor can not directly communicate with a base-station, it forwards its readings through other sensors within range until the packet reaches the base-station. Although this potentially allows sensors to operate at a lower transmit power than if they had to directly reach the base-station, it also requires other sensors to receive data and then re-transmit it. Interestingly, the Texas Instruments CC2420, a popular 2.4 GHz ZigBee-compliant RF transceiver used in the Sun Microsystems SunSPOTs and Crossbow MicaZ wireless sensors, uses more power in receive mode (19.7 mA) than in transmit mode (17.4 mA @ 0 dBm) [19, 4].

To make a direct comparison between our powerline-based sensors and existing sensor network technology, we tested the communication range of two SunSPOT ([18]) wireless sensors within the test home. One SunSPOT continually transmitted packets at a power of -25 dBm, while the other continually listened for packets and flashed an LED when it received them. -25 dBm was chosen since a powerline connected receiver was able to detect a 27 MHz transmitter at that power level throughout the house (in fact, -35 dBm was sufficient power to sense a transmitter within 60 cm of a powerline when using a powerline connected receiver anywhere in the home). We left the transmitting SunSPOT in a fixed location (to simulate a fixed wireless sensor) and walked around the test home with the receiving SunSPOT (to test possible locations for the sensor base-station). We found that at -25 dBm, while the powerline-based sensors were able to be detected at any room in the home by connecting a receiver to the outlet, the SunSPOTs could generally only communicate within the same room. We also tested whether the SunSPOTs' range could be extended by coupling to the powerline (despite Sec. 2 showing that 2.4 GHz signals do not transmit over the powerline) by placing both SunSPOTs near an outlet. This actually *decreased* their range. To give the SunSPOTs' whole-house coverage, we needed to increase their transmit power to 0 dBm (1 mW).

Besides utilizing the powerline to extend the range of our low-power sensors, an additional source of power efficiency is the low complexity of our data transmission protocol. As mentioned earlier, our powerline-based sensors are designed only to transmit sensor readings periodically and do not need to receive data or forward data for other sensors. This allows our data transmission protocol to be extremely simple. Instead of the 256 bits of overhead in every ZigBee packet ([3]), our protocol needs only six bits of overhead (five bits for the sensor address and one stop bit). Thus, although our sensor has a lower data transmission rate than Zigbee (62.5 kbps vs. 250 kbps), the time the transmitter must be active to transmit a 10 bit sensor reading is actually less for our powerline-based sensor, thus requiring less energy.

A direct comparison metric for the two technologies is milliamp-hours per bit transmitted (mAh / bit). This can be calculated as:

$$\frac{NumberOfBits}{bits/sec} \cdot RadioPower \cdot \frac{1hr}{3600sec} \quad (3)$$

We provide this data for our powerline-based 27 MHz wireless sensors and for 2.4 GHz Zigbee sensors in Table 4. This table shows two configurations for Zigbee: no mesh and mesh. No mesh is a more direct comparison with our technology since here we only account for the power that a Zigbee-based sensor must use to transmit a 10-bit sensor reading with similar coverage to powerline-based sensing. The mesh Zigbee configuration, however, considers that Zigbee may need to forward packets in a mesh network configuration from sensors not within direct communication range of the basestation. These values account for a sensor that must receive a packet from one of these out-of-range sensors and then forward it on to the basestation, in addition to sending one of its own packets with a sensor reading for each forwarded packet. These calculations show that our powerline-based wireless sensors use just 2% – 7% of the power that a Zigbee-based wireless sensor requires for similar coverage. In fact, the actual results are potentially better since this calculation does not account for the fact that on-off-keying uses no power when transmitting a zero and represents the power necessary to transmit 16 ones.

Table 4. 27 MHz powerline-based wireless sensing compared with 2.4 GHz Zigbee. Power requirements for the CC2420 Zigbee radio can be found in [4].

	PowerLine	Zigbee (no mesh)	Zigbee (mesh)
Total bits for a 10-bit Sensor Reading	16	272	544
Bit Rate (kbps)	62.5	250	250
Transmit Current (mA)	1.5	17.4	17.4
Receive Current (mA)	—	—	19.7
mAh / bit	$1.07 \cdot 10^{-7}$	$52.6 \cdot 10^{-7}$	$164.7 \cdot 10^{-7}$
%age of Powerline-sensing	100%	4,930%	15,442%

4.3 Multiple-Access Protocol

At the current data rate of 62.5 kilobits per second, each sensor needs 0.03% of a second to transmit its data. When each sensor transmits a 16-bit packet once per second, this leads to a theoretical maximum of 3,906 sensors per home. Our system currently utilizes what can be considered a uni-directional version of the ALOHA protocol for multiple access on the channel [1]. Since sensors are not capable of receiving, we rely upon the various sensors within a home to transmit at different times so as not to interfere. This can be done reasonably well without synchronization when the number of sensors does not approach the theoretical maximum by having the sensors add a randomized delay each time to the one second interval between transmitting packets.

4.4 Security

Although our current data transmission protocol does not use encryption, the nature of the system has a basic level of security built-in. By utilizing extremely low transmit powers on the sensors, the reception range is greatly limited for anyone attempting to overhear the sensors from outside the home. Although, as with any wireless technology, these devices are susceptible to snooping with high-gain antennas, this is generally expensive and impractical.

The powerline also has a natural security mechanism built-in — transformers. Electric power is distributed at a higher voltage than is utilized in the home. Transformers convert this higher voltage to the voltage carried on the home powerline. Transformers work well for low frequency signals like the 50-60 Hz power signal, but their high inductance causes them not to pass higher frequency signals like 27 MHz. Since one transformer can typically serve just a few homes, they act as a natural barrier to the sensors' signals propagating too far along the powerline and being sensed by neighbors from within their homes.

We concede that these sensors are susceptible to snooping via physical access to outlets on the outside of the home, but believe that the security implications of being able to snoop such low-level sensors as this system was designed for are quite limited.

5 Conclusion

The objective of this work was to effectively take power consumption for wireless data transmission in sensor networks out of the lifespan equation for a sensor by making it negligible compared to power consumption for sensors and microcontrollers. To do so, this paper has demonstrated a new model for building in-home wireless sensor networks that leverages the naturally occurring phenomenon of the existing home powerline infrastructure acting as an antenna for 27.12 MHz devices. This allows wireless sensors to transmit at a much lower output power than would otherwise be necessary to cover a typical house.

We demonstrated a custom-designed sensor platform built around this phenomenon that used a light sensor as an example. The 27 MHz radio in this device was able to communicate with a powerline connected receiver anywhere in the home while using just $6.3 \mu\text{A}$ on average, with a peak current draw of 1.5 mA. We believe that leveraging this phenomenon will finally enable us to overcome the power constraints that have always been the roadblock in realizing the community's vision of ubiquitous sensing.

References

1. Abramson, N.: The ALOHA System: Another Alternative for Computer Communications. In: The Proceedings of the Fall Joint Computer Conference 1970 (1970).
2. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: Wireless Sensor Networks: A Survey. *Computer Networks* vol. 38 (2002).

3. Burchfield, T. R., Venkatesan, S., Weiner, D.: Maximizing Throughput in ZigBee Wireless Networks through Analysis, Simulations and Implementations. In: The Proceedings of the International Workshop on Localized Algorithms and Protocols for Wireless Sensor Networks (2007).
4. Crossbow MPR-MIB Users Manual, Revision A. (June 2007). (http://www.xbow.com/support/support_pdf_files/mpr-mib.series_users_manual.pdf)
5. Federal Communications Commission: Part 15 Regulations (July 2008). (<http://www.fcc.gov/oet/info/rules/part15/PART15.07-10-08.pdf>)
6. Fleming, R. United States Patent #3324473: Line Cord Antenna (1965).
7. Froehlich, J., Larson, E., Campbell, T., Haggerty, C., Fogarty, J., Patel, S.: HydroSense: Infrastructure-Mediated Single-Point Sensing of Whole-Home Water Activity. In: The Proceedings of UbiComp 2009 (2009).
8. Homeplug Powerline Alliance: Frequently Asked Questions. (<http://www.homeplug.org/about/faqs/>)
9. Insteon. (<http://www.insteon.net>)
10. International Telecommunication Union: Frequently Asked Questions. (<http://www.itu.int/ITU-R/terrestrial/faq/index.html>)
11. Milligan, T.: Modern Antenna Design, 2nd edition (2003).
12. Patel, S.N., Reynolds, M.S., Abowd, G.D.: Detecting Human Movement by Differential Air Pressure Sensing in HVAC System Ductwork: An Exploration in Infrastructure Mediated Sensing. In: The Proceedings of Pervasive 2008 (2008).
13. Patel, S.N., Robertson, T., Kientz, J.A., Reynolds, M.S., Abowd, G.D.: At the Flick of a Switch: Detecting and Classifying Unique Electrical Events on the Residential Power Line. In the Proceedings of UbiComp 2007 (2007).
14. Patel, S.N., Stuntebeck, E.P., Robertson, T.: PL-Tags: Detecting Batteryless Tags through the Power Lines in a Building. In: The Proceedings of Pervasive 2009 (2009).
15. Patel, S., Truong, K., Abowd, G.: PowerLine Positioning: A Practical Sub-Room-Level Indoor Location System for Domestic Use. In: The Proceedings of UbiComp 2006 (2006).
16. Semtech: TN1200.04: Calculating Radiated Power and Field Strength for Conducted Power Measurements (2007). (<http://www.semtech.com/pc/downloadDocument.do?navId=H0,C1,P2613&id=2561>)
17. Stuntebeck, E., Patel, S., Robertson, T., Reynolds, M., Abowd, G.: Wideband PowerLine Positioning for Indoor Localization. In: The Proceedings of UbiComp 2008 (2008).
18. Sun Microsystems SunSPOT wireless sensors. (<http://www.sunspotworld.com/>)
19. Texas Instruments CC2420 Datasheet. (<http://focus.ti.com/lit/ds/symlink/cc2420.pdf>)
20. Texas Instruments MSP430 Ultra-Low-Power Microcontrollers Datasheet. (<http://focus.ti.com/lit/sg/slab034q/slab034q.pdf>)
21. Thompson, M. United States Patent #2581983: Line-Cord Antenna (1947).
22. Tulli, T. United States Patent #4401989: Television Line Antena Apparatus (1982).
23. X10: Standard and Extended X10 Protocol. (<http://software.x10.com/pub/manuals/xtddcode.pdf>)