POWDER REU
Intro to the Physical Layer
Presentation Notes
11 May 2020

Authors:
Neal Patwari
Washington University in St. Louis
McKelvey School of Engineering

Ayaz Mahmud, Shamik Sarkar, Sneha K. Kasera
University of Utah
School of Computing

Contents

Presentation 1

In This Presentation: (1) RF Measurements, (2) Propagation, (3) Multipath Channels

1 Overview

My job in this overview is largely to motivate research into the physical layer of wireless communication systems, and in particular, the radio channel.

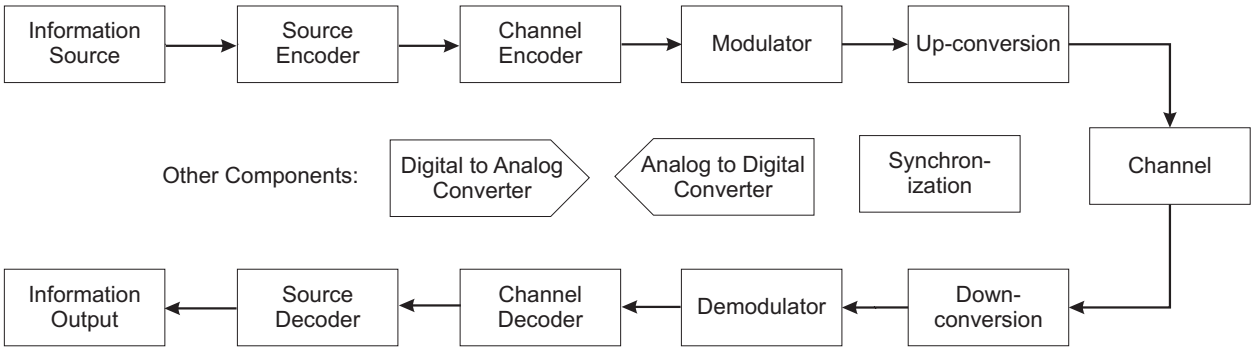


Figure 1: Block diagram of a single-user digital communication system, including (top) transmitter (TX), (middle) channel, and (bottom) receiver (RX).

The physical layer of the networking stack has inputs of bits and outputs of bits. In between, there is *coding*, which rearranges bits, and *modulation*, which takes discrete-time discrete-valued bits and changes them to an analog-valued, continuous-time signal (which is required because it is sent on EM waves in the real world), and *the channel*, which adds noise and attenuates and changes the shape of the signals which pass through it.

The reasons why I am so interested in studying the channel in Powder are:

- The channel is what we have the least control over. It causes significant changes in the signals researchers send from a transmitter. But the channel does not stay the same from one minute to the next (or even ms to the next in mobile radio), so our goal of *repeatable experimentation* can be foiled by the channel. It is important to understand it and to know what it was like during an experiment. Everything else in Figure 1 can be exactly repeated.
- We can't accurately recreate everything about the channel in a simulation or emulation environment. The channel is also what makes actual wireless communications so challenging. Thus the channel is exactly why we *need* Powder.

2 Power

Radio frequency (RF) engineers talk about power, power gains and losses. Here are some key concepts when we talk about RF channels.

First, power on a channel is in part limited by the maximum transmit power. Sometimes this is limited by how much power the transmit amplifier can produce, and sometimes by regulation (US

FCC). For example, the max EIRP of a "category B" CBSD base station is 47 dBm (for a 10 MHz channel).

1. Effective isotropic radiated power (EIRP) is the power that would have to be sent to an isotropic antenna to achieve the same power in the direction of maximum gain of the antenna actually in use. That is, is is the transmit power (dBm) plus the antenna gain (dB).

2. One must be able to convert between dBm and mW or dBW and W; also, to understand how dBX units add and subtract.

2.1 Decibel Notation

We often use a decibel (dB) scale for power. If P_{lin} is the power in Watts, then the power in dBW is

$$P\,[\text{dBW}] = 10\log_{10}\frac{P_{lin}}{1\text{ W}}.$$

We convert from dB to linear by inverting the above formula,

$$P_{lin} = (1\text{ W})10^{P[\text{dBW}]/10}.$$

The standard in the RF area is to consider power gains and losses, not voltage gains and losses. So if we say, for example, the channel has a loss of 20 dB, this refers to a loss in power. In particular, the output of the channel has 100 times less power than the input to the channel.

Remember these two dB numbers:

- 3 dB: This means the number is double in linear terms.
- 10 dB: This means the number is ten times in linear terms.

And maybe this one:

- 1 dB: This means the number is a little over 25% more (multiply by 5/4) in linear terms.

With these three numbers, you can quickly convert losses or gains between linear and dB units without a calculator. Just convert any dB number into a sum of multiples of 10, 3, and 1.

Example: Convert dB to linear values:

1. 30 dBW
2. 47 dBm
3. -20 dB
4. 4 dB

Solution:

1. $(1\text{ W})10^{30[\text{dBW}]/10} = 10^3\text{W} = 1000\text{ W}$.
2. 47 dBm = 30 dBm + 20 dB - 3 dB = 1000 mW $\times 100/2 = 50$ W.

3. -20 dB = $10^{-20[\text{dBW}]/10} = 10^{-2} = 0.01$.
4. 4 dB = 3 dB + 1 dB $\approx 2(1.25) = 2.5$.

Example: Convert linear values to dB:

1. 0.2 W
2. 40 mW

Solution:

1. 0.2 W = (0.1W)(2) = ([dBW] − 10) + 3 [dB] = −7 dBW
2. 40 mW = (10mW)(2)(2) = 10 [dBm] + 3 [dB] + 3 [dB] = 16 [dBW].

Example: Convert power relationships to dB:
Convert the expression to one which involves only dB terms.

1. $P_{y,lin} = 100 P_{x,lin}$
2. $P_{r,lin} = P_{t,lin} \frac{G_{t,lin} G_{t,lin} \lambda^2}{(4\pi d)^2}$, where λ is the wavelength (m), d is the path length (m), and $G_{t,lin}$ and $G_{t,lin}$ are the linear gains in the antennas, $P_{t,lin}$ is the transmit power (W) and $P_{r,lin}$ is the received power (W). This is the Friis free space path loss formula.

These last two are what we need to start to discuss path loss models.

2.2 SDR Unknown Reference

In software-defined radio, we often will have the power measured with respect to an unknown reference. That is, a receiver provides a dB measurement of power, but there is no known reference. That is, there is some power value X Watts that will result in a 0 dB measurement, but we don't know X. I refer to this as dBX,

$$P\,[\text{dBX}] = 10 \log_{10} \frac{P_{lin}}{X}, \tag{1}$$

where X is the power reference in Watts that corresponds to 0 dBX.

The advantage of denoting the power as dBX is that, it is clear that you're refering to a power value rather than a gain or loss. When one takes the difference of two dBX values, one gets a gain or loss in dB.

A transmitter or receiver calibration can then be used to obtain the value of X. Please note that two different SDRs will have different values for X, even if they are the same model and manufacturer. If you want to know the power received by the antenna, then the cable losses and RF front end will also play a part in this calibration.

3 Received Power Models

A universal model for received power is:

$$P_r(\text{dBW}) = P_t(\text{dBW}) + \sum \text{dB Gains} - \sum \text{dB Losses} \tag{2}$$

Of course, a dB Gain is just (-1) times a dB Loss. So whether we include something the Gains or Losses column is just a matter of our perspective. We typically think of an antenna as being a gain; and we think of path loss as being a loss. Note that when we say "path loss", by calling it a loss, we will express it as a positive value when it causes the received power to go down. If we had called it a "path gain" (as is sometimes done), then we will express it as a negative value when it causes the received power to go down.

1. There's no particular reason I chose dBW instead of dBm for P_r and P_t. But they must be the same, otherwise you'll have a 30 dB error!
2. *If using EIRP transmit power*, it includes $P_t(\text{dBW}) + G_t(\text{dB})$, so don't double count G_t by also including it in the dB Gains sum.
3. **Gains** are typically the antenna gains, compared to isotropic antennas.
4. **Losses** include large scale path loss, or reflection losses (and diffraction, scattering, or shadowing losses, if you know these specifically), losses due to imperfect matching in the transmitter or receiver antenna, any known small scale fading loss or "margin" (what an engineer decides needs to be included to be robust for fading), etc.

Path loss models are either (1) empirical or (2) theoretical. We've already studied one empirical model, the *path loss exponent model*. Below we describe one theoretical, and one empirical model.

3.1 Free Space Model

In the "far field" (distances many wavelengths from the antenna), the received power P_r in free space at a path length d is given by the "Friis Equation" as

$$P_r = P_t G_t(\theta) G_r(\theta) \left(\frac{\lambda}{4\pi d}\right)^2 \tag{3}$$

where G_t and G_r are the transmitter and receiver antenna gains, respectively; P_t is the transmit power; and λ is the wavelength. Notes:

- Wavelength $\lambda = c/f$, where $c = 3 \times 10^8$ meters/sec is the speed of light, and f is the frequency. We tend to use the center frequency for f, except for UWB signals, it won't really matter.
- All terms in (3) are in linear units, not dB.
- The effective isotropic radiated power (EIRP) is $P_t G_t$.
- The path loss is $L_p = \left(\frac{4\pi d}{\lambda}\right)^2$. This term is called the "free space path loss".
- The received power equation (3) is called the Friis transmission equation, named after Harald T. Friis [2].

- Free space is useful for space communications systems, or radio astronomy. Not for cellular telephony.

In dB, the expression from (3) becomes

$$P_r(\text{dBm}) = P_t(\text{dBm}) + G_t(\text{dB}) + G_r(\text{dB}) - L_p(\text{dB}), \tag{4}$$

where

$$L_p(\text{dB}) = 20 \log_{10} \left(\frac{4\pi d}{\lambda} \right) \tag{5}$$

I like to leave $L_p(\text{dB})$ in terms of d/λ, which is a unitless ratio of how many wavelengths the signal has traveled. The terms $G_t(\text{dB})$ and $G_r(\text{dB})$ are gains (when they are positive, the received power increases). And as distance increases, $L_p(\text{dB})$ increases, which because of the negative sign, reduces the received power.

3.2 Empirical: Path Loss Exponent Model

The path loss exponent model is a simple generalization of (3) and (4) in which the distance exponent of 2 in the Friis model is allowed to change to an arbitrary value. This generalization takes into account that obstructions exist in our real world (non free-space propagation environment) that cause transmission, diffraction, and scattering losses in addition to the simple radiative losses expressed by the Friis equation.

$$P_r(\text{dBm}) = P_0(\text{dBm}) - 10\nu \log_{10} \frac{d}{d_0} \tag{6}$$

where $P_0(\text{dBm})$ is still given by the Friis equation,

$$P_0(\text{dBm}) = P_t(\text{dBm}) + G_t(\text{dB}) + G_r(\text{dB}) - 20 \log_{10} \left(\frac{4\pi d_0}{\lambda} \right) \tag{7}$$

but now the path loss after d_0 term has changed to include a factor 10ν instead of 20. Typically d_0 is taken to be on the edge of near-field and far-field, say 1 meter for indoor propagation, and 10-100m for outdoor propagation.

Because environments have different densities of obstructions, the path loss exponent ν is determined by empirical measurements for the particular area in which the link resides. The value of ν will be higher:

1. in dense cities;
2. in buildings with highly attenuating walls;
3. in varying terrain;
4. when antennas are closer to the ground.

Thus we find the parameters $P_0(\text{dBm})$ and ν from measurements. For example, two measurement campaigns I did in office areas resulted in the estimates of $\nu = 2.30$ and 2.98 as shown in Figure 2.

As another example, consider the path loss exponent model on the University of Utah campus in the CBRS band (3.5 GHz). A campaign was conducted by Alex Orange and others using Powder.

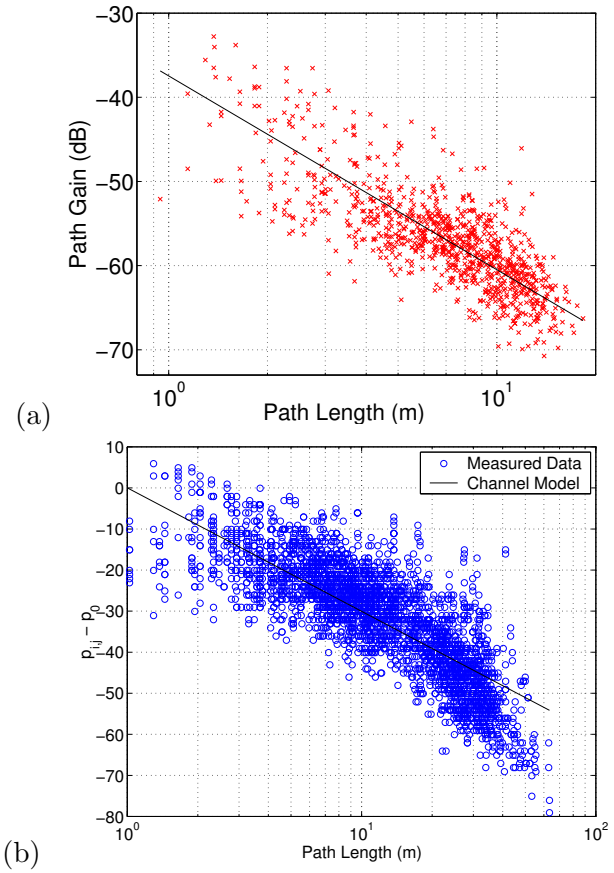


Figure 2: (a) Wideband path gain measurements (×) at 2.4 GHz as a function of path length d. Linear fit (—) is with $d_0 = 1$m, $\nu = 2.30$, and $\sigma_{dB} = 3.92$. (b) Narrowband measurements of received power minus P_0(dBm) (o) at 925 MHz as a function of path length d. Linear fit (—) is with $d_0 = 1$m, $\nu = 2.98$, with standard deviation $\sigma_{dB} = 7.38$. From [9].

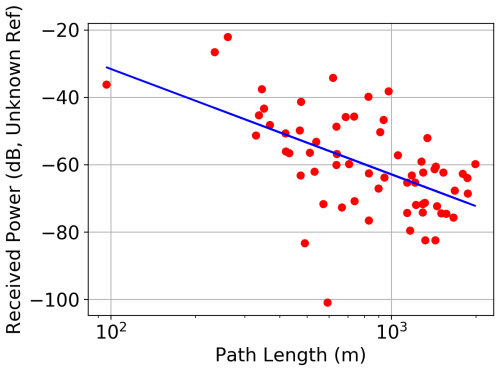


Figure 3: Narrowband received power (with unknown reference) • at 3.5 GHz as a function of log distance d. Linear fit (—) is with $\nu = 3.13$, and $\sigma_{dB} = 12.1$ dB. Data collected by Alex Orange and Jonathon Duerig.

In this campaign, base station (BS) locations were used as transmitters and fixed endpoints (FE) were used as receivers. There were $8 \times 8 = 64$ links measured. The received power values are plotted in Figure 3 as a function of log distance between the BS and FE.

Empirical measurement studies sometimes show a change in slope of the L_p vs. distance curve a certain distance [4]. You can see this effect in Figure 2(b) for $d > 20$ meters; the path gains at $d = 50$ meters are all lower than the model, and one can see the slope changing to an ν higher than 2.98. We can model the path loss as experiencing more than one slope in different segments of the $\log d$ axis. See [4] for more details.

We will conduct another measurement study at a different frequency band in Powder during the hands-on part of this tutorial.

4 Multipath Effects

Powder is a real-world set of radio channels. That is, it is both time-varying, and has many multipath components. The effects we will discuss in this brief tutorial are that:

- There will be time dispersion in the received signal; you'll receive a filtered version of the signal that you transmit. This may limit your data rate or require a more robust modulation.
- There will be frequency selectivity: The results on one frequency channel will be different from the results on a neighboring frequency channel, even within the same band. The received power can readily vary by 20 dB within one band.

Multipath radio wave propagation as a term groups together various ways for waves to propagate in the environment; via reflection, transmission, diffraction, and scattering. Many individual propagating waves arrive at the receiver, these waves are called *multipath components*, or collectively, *multipath*.

The challenges caused by multipath fading in wireless communication systems are one the most significant challenges addressed by wireless engineers. Engineers have developed a variety of modulation and diversity schemes in order to counteract the negative influence of multipath fading; as well as those methods which take advantage of multipath in particular ways as a benefit for communication systems

4.1 Voltage and Power in Multipath

As we discussed, many multipath wave components arrive at the receiver. *They add together as voltages.* DO NOT add the powers of the multipath together – there is no such physical antenna that add together the powers of multipath.

Let's say there are M multipath components, numbered 0 through $M-1$. Component i has amplitude V_i and phase $\theta_i(f)$ at frequency f. Then the total voltage at the receiver antenna will be:

$$V_{TOT}(f) = \sum_{i=0}^{M-1} V_i e^{j\theta_i(f)}$$

We then refer to the received power as $|V_{TOT}(f)|^2$. Technically the power is scaled by a resistance, we tend to omit this.

If you transmit a single frequency f, then the received power can vary by 10 to 20 dB or more due to the exact amplitudes and phases of the M multipath components. We often talk about the phases in particular, for given $\{V_i\}_i$.

- If the multipath have phases that are approximately the same, the $|V_{TOT}(f)|^2$ will be relatively high. We call this *constructive interference*.
- If the multipath have phases that are approximately 180^o out of phase, the sum of them will tend to bring the sum close to the origin, and $|V_{TOT}(f)|^2$ will be relatively low. We call this *destructive interference*, or *being in a deep fade*.

4.2 Temporal

Let's expand on where these phase angles come from. Recall that $V_i e^{j\theta_i(f)}$ is the representation of $V_i \cos(2\pi f t + \theta_i)$ where f is the carrier frequency. If $V_i \cos(2\pi f t)$ is transmitted from the transmitter antenna, how do the phases of the multipath components behave with respect to each other? Well, each component has its own path length. It really did travel that length. And EM waves travel (in air) at $c = 3 \times 10^8$ m/s. So some waves arrive later than others. Let τ_i denote the time delay of arrival for multipath i relative to the transmit time. It is d_i/c, where d_i is the length of component i. What happens when a function is delayed by τ_i? We replace t with $t - \tau_i$ in the function. So $V_i \cos(2\pi f(t - \tau_i))$ is received. Well, not the full story – reflections and diffractions also cause phase changes (we discussed specifics for reflection in Section 4.5). Really,

$$V_i \cos(2\pi f(t - \tau_i) + \phi_i)$$

is received, where ϕ_i is the sum of all phase changes caused by the physical propagation phenomena. The above equation is in baseband notation, what is the complex baseband notation? It is:

$$V_i e^{j(-2\pi f \tau_i + \phi_i)}.$$

So what is the total received voltage from all multipath?

$$V_{TOT} = \sum_{i=0}^{M-1} V_i e^{j(-2\pi f \tau_i + \phi_i)} \tag{8}$$

In other words, $\theta_i = -2\pi f \tau_i + \phi_i$. We've now written it in terms of its temporal delay, τ_i. Note that V_{TOT} is a function of frequency f. It is also a function of time delays $\{\tau_i\}_i$ which are a function of TX and RX antenna positions.

On your own "homework" problem: Prove that the expected value of the power, that is, $E\left[|V_{TOT}|^2\right]$, is equal to the sum of the power of the individual paths, *i.e.*, $\sum_{i=0}^{M-1} |V_i|^2$. Assume that the phases $\{\phi_i\}$ are independent and identically distributed uniform $[0, 2\pi)$ random variables.

4.3 Channel Impulse Response

What we have in (8) is a frequency response as a function of frequency f. The equation can show the frequency response at *any* frequency. So (8) is a frequency-domain representation of the total voltage. Let's convert to the time domain. How? Using the inverse Fourier transform:

$$\begin{aligned} \mathfrak{F}^{-1}\left\{\sum_{i=0}^{M-1} V_i e^{j(-2\pi f \tau_i + \phi_i)}\right\} &= \sum_{i=0}^{M-1} V_i \mathfrak{F}^{-1}\left\{e^{j(-2\pi f \tau_i + \phi_i)}\right\} \\ &= \sum_{i=0}^{M-1} V_i e^{j\phi_i} \delta(\tau - \tau_i) \end{aligned} \tag{9}$$

This says, in the *time delay domain*, multipath i arrives at delay τ_i.

This leads to how we frame the channel. **The channel is an echo-causing filter, with an impulse response that is a sum of time-delayed impulses.** Let $s(t)$ be the transmitted signal and $r(t)$ be the received signal. Then

$$r(t) = \frac{1}{2} s(t) \star h(t)$$

where $h(t)$ or $h(\tau)$ is called the *channel impulse response* (CIR), and is given by

$$h(\tau) = \sum_{i=0}^{M-1} a_i e^{j\phi_i} \delta(\tau - \tau_i) \tag{10}$$

The a_i are proportional to V_i but are unitless – the units are contained in $s(t)$, which has units of Volts. The amplitude $|a_i|$ is the amplitude gain in that path; the squared magnitude $|a_i|^2$ is the power gain in that path. Researchers often plot the squared magnitude of $h(\tau)$ in the dB domain and call it the *power delay profile*, or PDP. We also denote this power in the ith path as $P(\tau_i) = |a_i|^2$. Fig. 4 shows three examples measured by Dustin Mass [8].

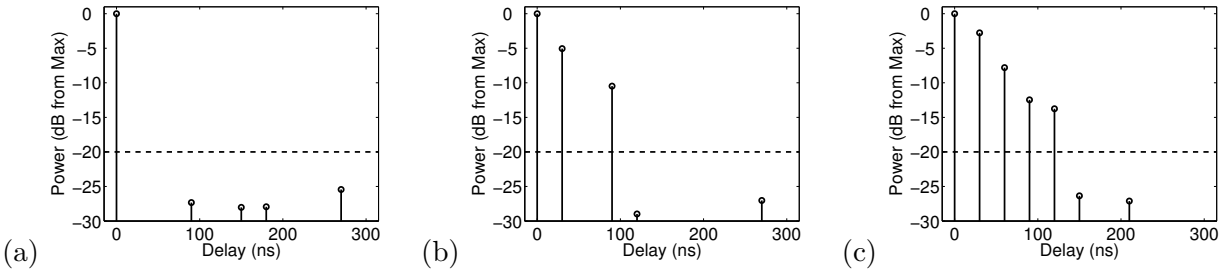


Figure 4: Measured PDPs (power gain normalized to the maximum power gain) in SLC (a) in residential area West of the Univ. of Utah; (b) 4th South in Salt Lake City (c) Main St. in Salt Lake City [8].

Summer project idea: A good piece of meta-data for a researcher would be the CIR of the channel. They could use this as a measure of the multipath channel in which they are running their experiment. If it changes from one run of their experiment to another, that might be a reason that their experiment results change.

You can measure this with a Powder transmitter and receiver. There are multiple ways to accomplish this. One standard way is to send a known wideband signal that is nearly constant in in $|S(f)|$, measure the received signal $r(t)$ at a receiver, and estimate that the channel $|H(f)|$ (the filter in between the two) must have been proportional to $|R(f)|$ to result in your measurement. This is the method used in [8].

Another method is the sliding correlator [12]. This is useful because it does not require as much synchronization between transmitter and receiver; also it is lower in computational complexity, so it can be used for real-time CIR plotting.

4.4 Channel Frequency Response

The received power as a function of frequency is simply given by the magnitude squared of the total voltage from (8). The channel frequency response (CFR) is the normalized version of this

(normalized to the total transmitted power):

$$|H(f)|^2 = \left| \sum_{i=0}^{M-1} \alpha_i e^{j(-2\pi f \tau_i + \phi_i)} \right|^2 \tag{11}$$

where $\alpha_i = |V_i|^2/P_{TX}$, that is, the normalized received power in path i. An example of a CFR is shown in Figure 5.

If the bandwidth of your signal is not relatively flat, that is, there are nulls within it, you are operating in a frequency-selective channel. This will tend to happen when multipath 1) arrive from many different angles, and 2) arrive with large time delays.

In general, $H(f)$ is a correlated random process, and we talk about a *correlation bandwidth*, that is, the frequency separation which makes $H(f)$ have a correlation coefficient of $1/e$. The correlation coefficient is inversely proportional to the RMS delay spread, which can be calculated from the channel impulse response.

Presentation 2

In This Presentation: (1) Modulation Basics, (2) OFDM

5 Modulation Basics

5.1 Orthogonality

Digital communications systems send and receive linear combinations of orthogonal signals. In short, we use orthogonal signals for:

1. *Multiple Access*: Multiple users can access the same medium, and a receiver can separate one user's signal from the rest.

2. *Increasing Signal Dimension*: A single device can send information along multiple dimensions at the same time, which is useful for increasing the bit rate or fidelity.

3. *Sending Symbols over Time*: We use a symbol waveform (function) that is orthogonal to itself at integer multiples of T_s, the symbol period, so that we can repeatedly send symbols that don't interfere with others we sent previously.

My "engineering" definition of a set of orthogonal waveforms: *They are waveforms that can be separated at the receiver.* Note that a waveform is defined as a finite-energy function (with units of Volts) of time. Now, let's provide the mathematical definition of orthogonal waveforms.

Def'n: *Orthogonal*
Two complex-valued waveforms $\phi_0(t)$ and $\phi_1(t)$ are orthogonal if

$$\int_{-\infty}^{\infty} \phi_0(t)\phi_1^*(t)dt = 0,$$

where $\phi_1^*(t)$ is the complex conjugate of $\phi_1(t)$.

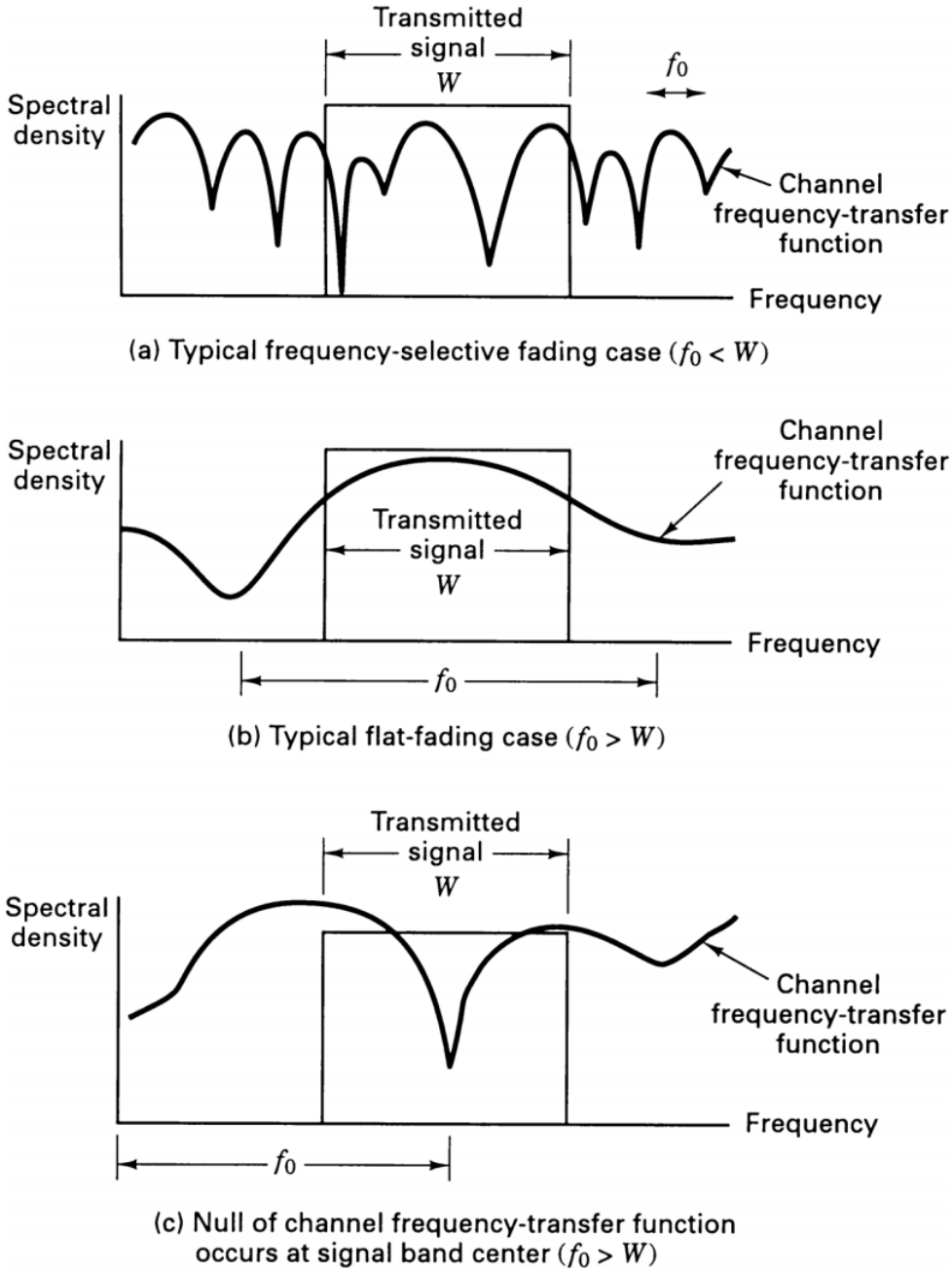


Figure 5: Example channel frequency responses; the example transmitted signal PSD is shown as a rectangle. The resulting PSD of the received signal is the product of the two. In (a) the *frequency selective fading* case, the frequency selectivity will result in a received signal with a very different shape (in time and frequency domains) than the transmitted signal; whereas in (b) the *flat fading* case, the shape of the received signal will be nearly the same as the transmitted signal. From [16].

Def'n: *Orthogonal Set*
K waveforms $\phi_0(t), \ldots, \phi_{K-1}(t)$ are mutually orthogonal, or form an orthogonal set, if every pair of waveforms $\phi_i(t)$, $\phi_j(t)$, for $i \neq j$, is orthogonal.

Example: Sine and Cosine
Let

$$\begin{aligned} \phi_0(t) &= \begin{cases} \cos(2\pi t), & 0 < t \leq 1 \\ 0, & o.w. \end{cases} \\ \phi_1(t) &= \begin{cases} \sin(2\pi t), & 0 < t \leq 1 \\ 0, & o.w. \end{cases} \end{aligned}$$

Are $\phi_0(t)$ and $\phi_1(t)$ orthogonal?
Solution: Using $\sin 2x = 2\cos x \sin x$,

$$\begin{aligned} \int_{-\infty}^{\infty} \phi_0(t)\phi_1(t)dt &= \int_0^1 \cos(2\pi t)\sin(2\pi t)dt \\ &= \int_0^1 \frac{1}{2}\sin(4\pi t)dt \\ &= \frac{-1}{8\pi}\cos(4\pi t)\Big|_0^1 = \frac{-1}{8\pi}(1-1) = 0 \end{aligned}$$

So, yes, $\phi_0(t)$ and $\phi_1(t)$ are orthogonal.

Example: Frequency Shift Keying
Assume $T_s >> 1/f$, and show that these two are orthogonal.

$$\begin{aligned} \phi_0(t) &= \begin{cases} \cos(2\pi f t), & 0 \leq t \leq T_s \\ 0, & o.w. \end{cases} \\ \phi_1(t) &= \begin{cases} \cos\left(2\pi\left[f + \frac{1}{T_s}\right]t\right), & 0 \leq t \leq T_s \\ 0, & o.w. \end{cases} \end{aligned}$$

Solution: The integral of the product of the two must be zero. Checking, and using the identity for the product of two cosines,

$$\begin{aligned} & \int_0^{T_s} \cos(2\pi f t)\cos\left(2\pi\left[f + \frac{1}{T_s}\right]t\right)dt \\ = \; & \frac{1}{2}\int_0^{T_s} \cos(2\pi t/T_s)\,dt + \frac{1}{2}\int_0^{T_s} \cos(4\pi f t + 2\pi t/T_s)\,dt \\ = \; & 0 + \frac{1}{2}\left[\frac{1}{2\pi(2f + 1/T_s)}\sin(2\pi(2f + 1/T_s)t)\right|_0^{T_s} \end{aligned}$$

The remaining term has a $\frac{1}{2\pi(2f+1/T_s)}$ constant out front. Because f is very high, this term will be very very low. The sine term is limited to between -1 and +1 so it will not cause the second term to be large. Thus,

$$\int_{-\infty}^{\infty} \phi_0(t)\phi_1(t)dt \leq \frac{1}{\pi(2f + 1/T_s)} \approx 0$$

Thus the two different frequency waveforms are orthogonal.

5.2 Linear Combinations

What is a linear combination of orthogonal waveforms? Well, consider the orthogonal set $\phi_0(t), \ldots, \phi_{K-1}(t)$. A linear combination $s_m(t)$ is

$$s_m(t) = a_{m,0}\phi_0(t) + a_{m,1}\phi_1(t) + \cdots + a_{m,K-1}\phi_{K-1}(t) = \sum_{m=k}^{K-1} a_{m,k}\phi_k(t)$$

We also call the linear combination a *symbol*. We use subscript m to indicate that it's not the only possible linear combination (or symbol). In fact, we will use M different symbols, so $i = 0, \ldots, M-1$, and we will use $s_0(t), \ldots, s_{M-1}(t)$. A transmitter repeatedly looks at the bits to be sent, takes $\log_2 M$ of them, looks up the linear combination $s_m(t)$ corresponding to the mth symbol, and creates that signal and adds it to the analog signal being sent out of the antenna, as shown in Figure 6.

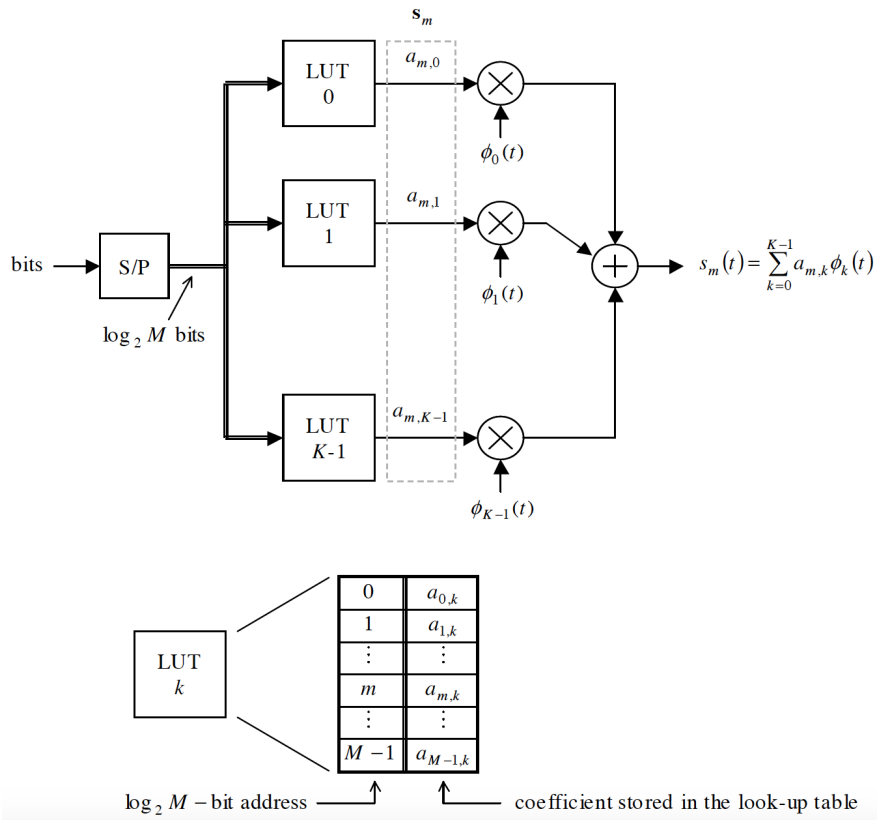


Figure 6: (Taken from Rice Figure 5.5 [14]): Block diagram of a modulator for M-ary linear modulation based on the synthesis equation.

We represent the mth symbol (linear combination of the orthogonal waveforms), $s_m(t)$, as a vector for ease of notation:

$$\mathbf{s}_m = [a_{m,0}, a_{m,1}, \ldots, a_{m,K-1}]^T$$

The superscript T is for transpose – $\mathbf{s}_m$ is a column vector. Vectors are easy to deal with because they can be plotted in vector space, to show graphically what is going on. We call the plot of all

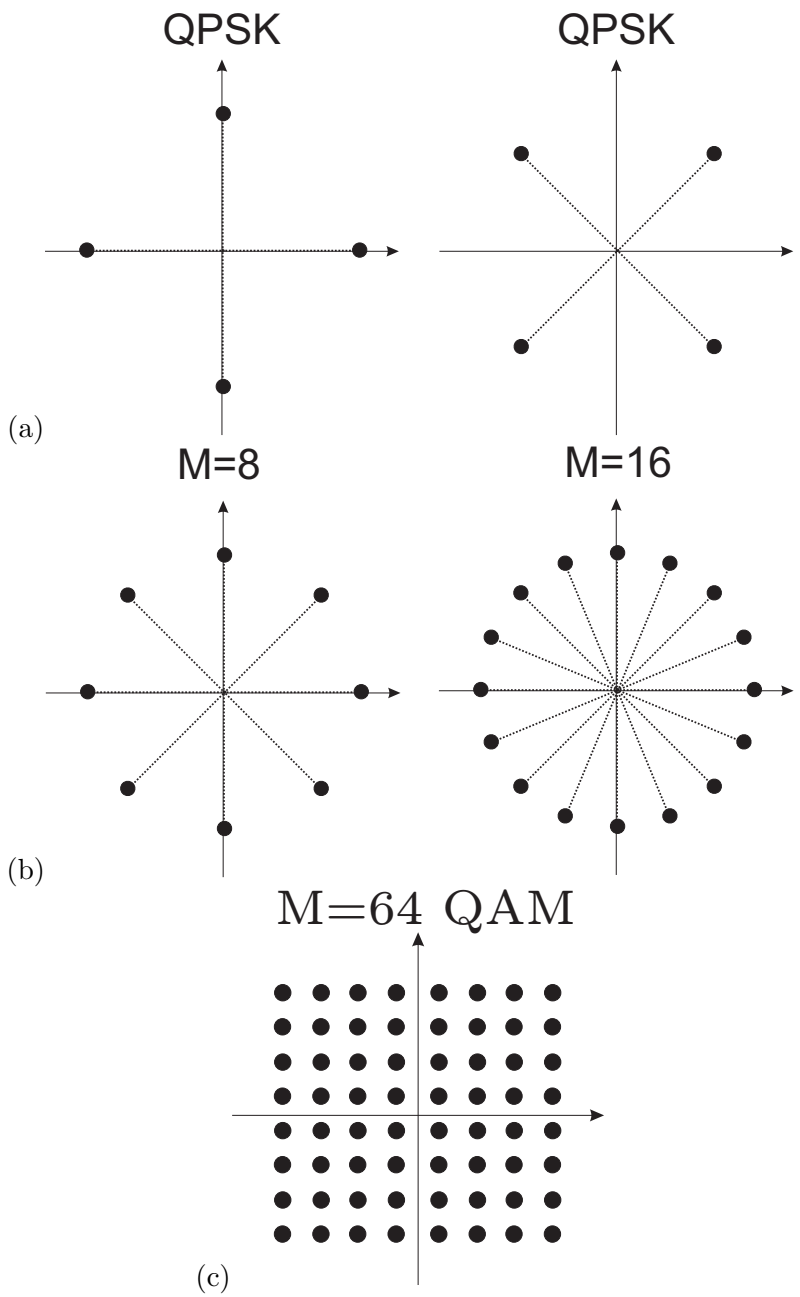


Figure 7: Signal constellations for (a) $M = 4$ PSK (a.k.a. BPSK), (b) $M = 8$ and $M = 16$ PSK, and (c) 64-QAM.

possible $\mathbf{s}_m$, that is, for $m = 0, \ldots M-1$, the *constellation diagram*. Some examples are shown in Figure 7.

Here is how a transmitter *uses* the different linear combinations to convey digital bits to the receiver. First, consider that there are M different symbols for the TX to chose from. Each symbol is described by a $\log_2 M$-length bit sequence. For example, if there are 8 possible combinations, we would label them 000, 001, 011, 010, 110, 111, 101, 100.

The transmitter knows which $\log_2 M$-bit sequence it wants to send. It picks the symbol that corresponds to that bit sequence, let's call it symbol m. Then it sends $s_m(t)$.

If the receiver is able to determine that symbol m was sent, it will correctly receive those $\log_2 M$ bits of information. In this example, it will receive three bits of information.

6 Orthogonal Frequency Division Multiplexing (OFDM)

This is Section 5.5 in the Rice book [14].

In FSK, we use a single basis function at each of different frequencies. In QAM, we use two basis functions at the same frequency. *Multicarrier modulation* is the combination, using two basis functions at K different frequencies. Each frequency is called a *subcarrier* or *subchannel*. There are K subcarriers, and thus $2K$ orthogonal waveforms:

$$\begin{aligned}
\phi_{0,c}(t) &= \sqrt{2}p(t)\cos(\omega_0 t) \\
\phi_{0,s}(t) &= -\sqrt{2}p(t)\sin(\omega_0 t) \\
\phi_{1,c}(t) &= \sqrt{2}p(t)\cos(\omega_0 t + 2\pi\Delta f t) \\
\phi_{1,s}(t) &= -\sqrt{2}p(t)\sin(\omega_0 t + 2\pi\Delta f t) \\
&\vdots \\
\phi_{K-1,c}(t) &= \sqrt{2}p(t)\cos(\omega_0 t + 2\pi(K-1)\Delta f t) \\
\phi_{K-1,s}(t) &= -\sqrt{2}p(t)\sin(\omega_0 t + 2\pi(K-1)\Delta f t)
\end{aligned}$$

where $\Delta f = \frac{1}{T_s}$. Multi-carrier modulation is a general type of modulation, of which *orthogonal frequency division multiplexing* (OFDM) is a specific version which uses the NRZ (rectanguar)

pulse, equal to $1/\sqrt{T_s}$ between 0 and T_s, and zero otherwise. OFDM is thus represented as:

$$\begin{aligned}
\phi_{0,c}(t) &= \begin{cases} \sqrt{\frac{2}{T_s}}\cos(\omega_0 t), & 0 \le t \le T_s \\ 0, & o.w. \end{cases} \\
\phi_{0,s}(t) &= \begin{cases} -\sqrt{\frac{2}{T_s}}\sin(\omega_0 t), & 0 \le t \le T_s \\ 0, & o.w. \end{cases} \\
\phi_{1,c}(t) &= \begin{cases} \sqrt{\frac{2}{T_s}}\cos(\omega_0 t + 2\pi\Delta f t), & 0 \le t \le T_s \\ 0, & o.w. \end{cases} \\
\phi_{1,s}(t) &= \begin{cases} -\sqrt{\frac{2}{T_s}}\sin(\omega_0 t + 2\pi\Delta f t), & 0 \le t \le T_s \\ 0, & o.w. \end{cases} \\
&\vdots \\
\phi_{K-1,c}(t) &= \begin{cases} \sqrt{\frac{2}{T_s}}\cos(\omega_0 t + 2\pi(K-1)\Delta f t), & 0 \le t \le T_s \\ 0, & o.w. \end{cases} \\
\phi_{K-1,s}(t) &= \begin{cases} -\sqrt{\frac{2}{T_s}}\sin(\omega_0 t + 2\pi(K-1)\Delta f t), & 0 \le t \le T_s \\ 0, & o.w. \end{cases}
\end{aligned}$$

where again $\Delta f = \frac{1}{T_s}$.

These waveforms, for multicarrier modulation and for OFDM in particular, are all mutually orthogonal, as you can show using the definition for orthogonality. (Note we have $2K$ basis functions here in the same bandwidth as K-ary FSK!)

The signal on subcarrier k for OFDM might be represented as:

$$x_k(t) = \sqrt{\frac{2}{T_s}}\left[a_{k,I}(t)\cos(\omega_0 t + 2\pi f_k t) - a_{k,Q}(t)\sin(\omega_0 t + 2\pi f_k t)\right]$$

On the kth channel, the signal could be described as some kind of QAM or PSK modulation. Regardless, over all channels, the modulation is called OFDM. The OFDM signal of the sum of all K signals might then be represented as:

$$\begin{aligned}
x(t) &= \sqrt{\frac{2}{T_s}}\mathbb{R}\left\{\sum_{k=1}^{K}(a_{k,I}(t) + j a_{k,Q}(t))e^{j(\omega_0 + 2\pi k\Delta f)t}\right\} \\
x(t) &= \sqrt{\frac{2}{T_s}}\mathbb{R}\left\{e^{j\omega_0 t}\sum_{k=1}^{K}A_k(t)e^{j2\pi k\Delta f t}\right\} \qquad (12)
\end{aligned}$$

where $A_k(t) = a_{k,I}(t) + j a_{k,Q}(t)$. Does this look like an inverse discrete Fourier transform? If yes, than you can see why it might be possible to use an IFFT and FFT to generate the transmitted signal.

FFT implementation: There is a particular implementation of the transmitter and receiver that use FFT/IFFT operations. This avoids having K independent transmitter chains and receiver chains. The FFT implementation (and the speed and ease of implementation of the FFT in hardware) is why OFDM became so hugely popular.

The only downside of the FFT implementation is that the FFT and IFFT assume that the signal is *perfectly periodic*. But we don't send the same data over and over again — that wouldn't be communication. To enable use of the FFT, we add a period called the *cyclic prefix* which actually

does repeat the signal. This is overhead because it does not convey new information, however, it makes implementation easier.

Since the K carriers are orthogonal, the signal is like K-ary FSK. But, rather than transmitting on one of the K carriers at a given time (like FSK) we transmit information in parallel on all K channels simultaneously. An example state space diagram for $K = 3$ and PAM on each channel is shown in Figure 8.

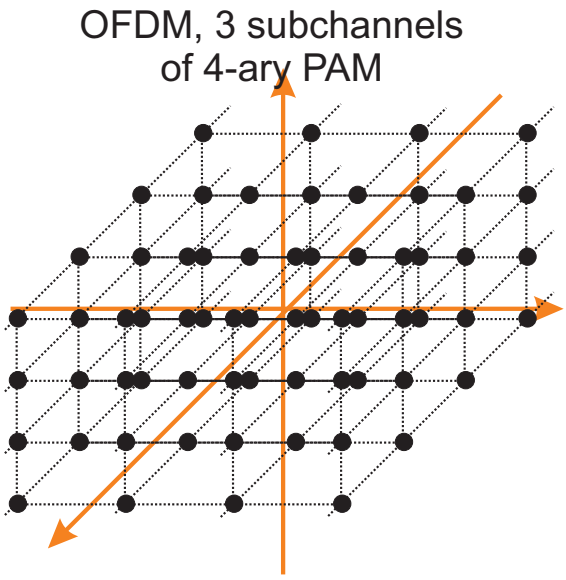


Figure 8: Signal space diagram for $K = 3$ subchannel OFDM with 4-PAM on each channel.

Example: 802.11a
IEEE 802.11a uses OFDM with 52 subcarriers. Four of the subcarriers are reserved for pilot tones, so effectively 48 subcarriers are used for data. Each data subcarrier can be modulated in different ways. One example is to use 16 square QAM on each subcarrier (which is 4 bits per symbol per subcarrier). The symbol rate in 802.11a is 250k/sec. Thus the bit rate is

$$250 \times 10^3 \frac{\text{OFDM symbols}}{\text{sec}} 48 \frac{\text{subcarriers}}{\text{OFDM symbol}} 4 \frac{\text{coded bits}}{\text{subcarrier}} = 48 \frac{\text{Mbits}}{\text{sec}}$$

Presentation 3

In This Presentation: (1) Source Localization

7 Source Localization from Received Power

Applications of source localization in Powder:

- We may measure a source that would interfere with our system-under-test, or that we would possibly interfere with. To better know what the signal is, we could try to locate it. For example, if we find it originates near a Crown Castle tower, we might ask them.

- We may be investigating source localization as our research question itself. Cognitive radio depends on sensors which measure and then locate and classify the transmitter. Mobile devices often need to be located for navigation or for logistics purposes.

For a motivating example, consider Tampa Florida driver Jason Humphreys, who bought a cell phone jammer and used it every day while he was commuting [7]. He used it for two years with the intention that he was improving his personal safety by kicking drivers off of their phones. Because he was mobile, the FCC's standard triangulation methods were insufficient to locate the source, and it took considerable person-hours to identify the vehicle. We predict that as jamming becomes more possible with a change in software, that such illegal use of the spectrum will increase.

There are several methods for source localization:

1. *Angle*: Receiver at multiple locations can estimate the angle to the source, using a rotating directional antenna, or a antenna array. The angular accuracy increases with the directionality or the number of antenna elements in the array. Such methods are not appropriate for physically small devices such as UEs.

2. *Time*: Receivers can compare the relative time delay between signals recorded at multiple locations. This requires a means to synchronize the receivers. Sometimes synchronization is performed using a "beacon transmitter" at a known location. Alternatively, synchronization can be achieved with a GPS-derived oscillator, or SyncE, as long as the received samples are traceable back to the synchronous oscillator.

3. *Power*: As the received power is, on average, a function of distance, one can use power to estimate the source location.

4. *Doppler*: A moving source can be more challenging to locate, but it additionally provides a Doppler shift in frequency that is proportional to its velocity relative to the receiver. This additional information can be helpful in its localization.

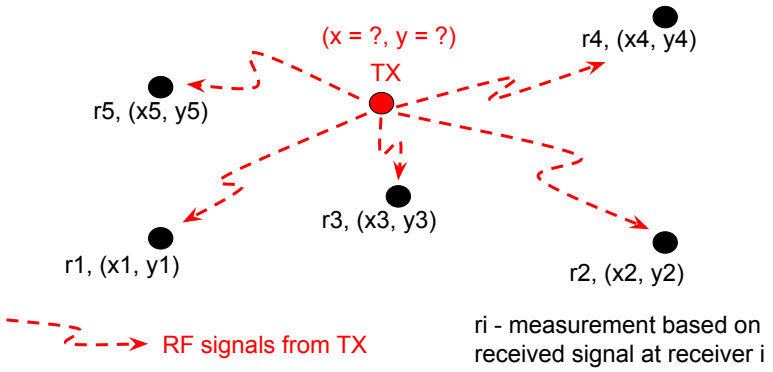


Figure 9: The source localization problem.

We focus on this section on received power-based localization because:

- Powder is currently capable of power measurements.
- It does not require frequency or time synchronization or angle measurements.

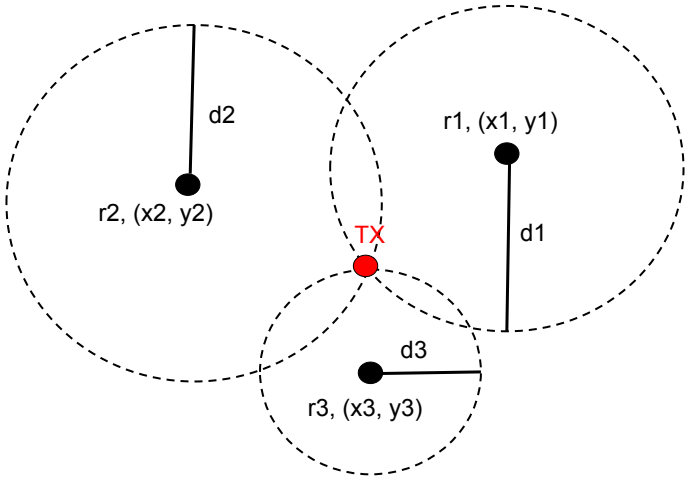


Figure 10: Localization using trilateration, a method that uses range estimates from each receiver to locate a transmitter.

- The bandwidth from the receivers is lower – only power measurements must be sent to an algorithm.
- It does not record the raw samples of any transmitted signal. While you are not in danger from the FCC unless you de-encrypt a received signal not intended for you, it is safer not to store raw received signals to drive at all.

7.1 Range Estimation

From (6), we can invert the expression to find an estimate of distance:

$$\hat{d} = d_0 10^{\frac{P_0(dBm) - P_r(dBm)}{10\nu}} \tag{13}$$

Although this happens to be the maximum likelihood estimator of distance, this is a poor estimate of distance because of the large standard deviation in the P_r [dBm] as a function of distance. The estimate has a huge standard deviation, and is also biased, typically on the order of 20% longer than the actual distance [10]. That is, *even on average*, this $\hat{d} \approx 1.20d$ for actual distance d.

Another major problem is that, for finding an unknown transmitter, the transmit power is unknown, and P_0(dBm) is equal to the transmit power minus a constant. Thus the two problems of transmit power estimation and distance estimation are fundamentally coupled.

Note that (13) also assumes that there is only one source.

7.2 Modified Maximum Likelihood Method

One method for model-based localization is the maximum likelihood estimator (MLE). When the transmit power is known, this has been presented in [11]. The difference in locating an unknown source is that the transmit power is also unknown.

The MLE is a model-based method that has a few assumptions:

- The average received power at distance d is given by the path loss exponent model in (6).

- The distribution of the model error is Gaussian in dB, or log-normal in linear terms.

We are not making assumptions about the transmit power in this formulation. (Note that you could assume P_t [dBm] is Gaussian, for example, and this would lead to a different estimator.)

The MLE does just what its name says — it maximizes a likelihood function:

$$\hat{x}_{MLE}, \hat{P}_t = \arg\max_{\mathbf{x}, P_t} f\left(\{P_{r,i}\}_i;\, \{\bar{P}_{r,i}(P_t, \mathbf{x})\}_i, \sigma^2_{dB}\right) \tag{14}$$

where $f(\mathbf{y};\, \mu, \sigma^2)$ is the multi-variate Gaussian distribution function; $\bar{P}_{r,i}(\mathbf{x}, P_t)$ is what the path loss exponent model predicts for received power $P_{r,i}$ at transmitter location $\mathbf{x}$ and power P_t.

$$\bar{P}_{r,i}(P_t, \mathbf{x}) = P_t(\text{dBm}) + G_t(\text{dB}) + G_r(\text{dB}) - 20\log_{10}\left(\frac{4\pi d_0}{\lambda}\right) - 10\nu\log_{10}\frac{\|\mathbf{x} - \mathbf{r}_i\|}{d_0}, \tag{15}$$

where $\mathbf{r}_i$ is the ith receiver location. Equation (15) shows the model's dependence on transmitter location $\mathbf{x}$ and power P_t.

While it is possible to use optimization techniques to solve 14, we can also simply calculate the likelihood for each possible transmitter coordinate $\mathbf{x}$ on a grid. This also has the benefit of giving us an image of the likelihood.

For a particular coordinate $\mathbf{x}$, we estimate the transmit power as

$$\hat{P}_t(\mathbf{x}) = P_d + \frac{1}{N}\sum_{i=1}^{N}\left(P_{r,i} - \bar{P}_{r,i}(P_d, \mathbf{x})\right) \tag{16}$$

where P_d is an arbitrary *default* transmit power level. It actually cancels out, but we use it to provide a more intuitive solution. That is, we start with the default transmit power, and add in the average difference between the measured received powers and what the model would predict for TX at $\mathbf{x}$ with power P_d.

Then we can calculate the MLE location by removing constants that are not a function of $\mathbf{x}$ and thus simplifying (14) to be:

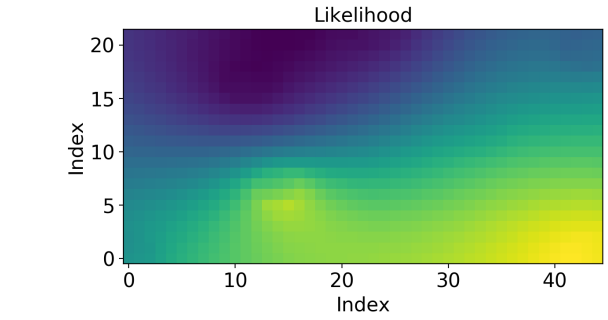
$$\hat{x}_{MLE} = \arg\min_{\mathbf{x}} \exp\left\{-\sum_i \left[P_{r,i} - \bar{P}_{r,i}(\hat{P}_t, \mathbf{x})\right]^2 / (2\sigma^2_{dB})\right\} \tag{17}$$

For an implementation, see my code `ml_source_imaging.py`. I ran this code using the 'madsen' fixed endpoint as a transmitter, and eight base stations as receivers. The results are shown in Figure 11.

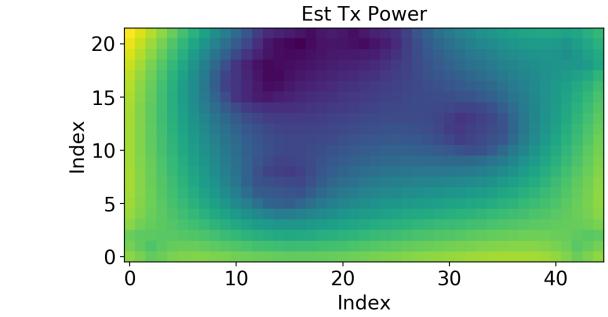
7.3 Source Localization: Related Work

A wide variety of algorithms have been proposed that can localize the transmitter based on the received power and the receivers' locations. In the following, we briefly summarize some well-known received power based transmitter localization algorithms. At a high level, power-based localization algorithms can be classified in two broad categories:

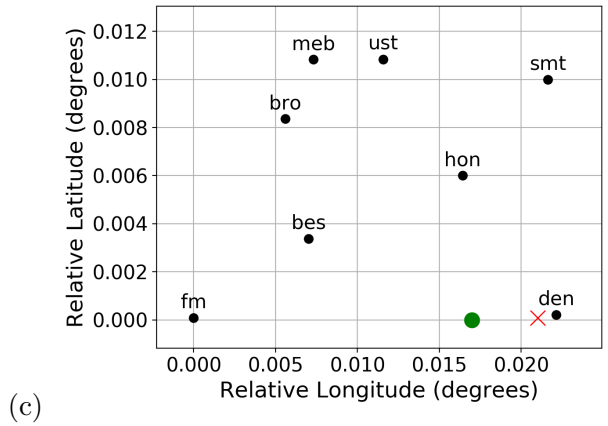
- Model-based algorithms,
- Learning-based algorithms.



(a)



(b)



(c)

Figure 11: Given measurements at the 8 BS receivers, (a) Likelihood image (probability of measurements given TX at each position) with yellow=high likelihood, blue=low likelihood; (b) estimated transmit power if the transmitter is at each position, yellow=high TX power and blue=low TX power; (c) MLE (×) and actual (●) position of transmitter, on a map of base station locations (●), in a map of lat/long (GPS) coordinates w.r.t. Friendship Manor, our bottom-leftmost device.

7.3.1 Model-based localization

In case of model-based localization algorithms, the fundamental idea is to use a radio wave propagation path loss model (PLM) for localization. Both deterministic and probabilistic methods have been investigated for this category of localization algorithms.

Trilateration: A conceptually simple model-based localization algorithm is trilateration, as shown in Fig 10. In this method, each receiver, i, estimates its range, d_i, from the transmitter using the PLM and then draws a circle of radius d_i, with receiver i at the center of the circle. The location where the three circles intersect is estimated as the transmitter's location. This method needs at least 3 receivers whose x-y coordinates do not form a line. Due to shadowing and multipath fading in the RF environment, the estimate of d_i is very inaccurate. Consequently the three circles do not have a common intersection point, and some sort of non-linear optimization is required to produce an estimate of the transmitter's location. One such popular algorithm is EZ [3], that uses a genetic optimization algorithm.

Echolocation (EL) [20]: The distance estimates of the transmitter using the PLM are often inaccurate. EL is an algorithm that tries to counter this problem by applying a non-parametric method popular in statistics, called ranking. The EL method creates an ordered sequence of the measured received power values. Then for every location in the area of interest, it creates an ordered sequence of the distances to the receivers. Finally, it estimates the location of the transmitter as the one that has maximum match between the ordered sequence of received powers and that location's ordered sequence of distances. Essentially, the method does not depend directly on the PLM but uses the intuition that the measured received power reduces monotonically as the distance of the receiver, from the transmitter, increases. While monotonicity is not always valid, it is more robust than assuming a particular PLM function.

Matrix inversion (MI): One recent algorithm, the matrix inversion method [5], addresses the problem that all of the previously described methods assume there is exactly one transmitter. The MI method discretizes the area of interest in voxels, describes a linear model for what the received power would be from a transmitter in each voxel, inverts the model, and declares the voxel center with maximum transmit power field as the (greedy) location of one transmitter.

7.3.2 Learning-based localization

In case of learning-based localization methods, the general idea is to collect many received power measurements for known transmitter and receivers' locations and then use supervised learning techniques to learn a model that is more data-driven than the traditional PLM. Learning-based localization has been studied most extensively in the context of WiFi fingerprinting.

RADAR: The basic idea of WiFi fingerprinting was first introduced in the RADAR paper [1]. The basic idea is to capture received power fingerprints from a number of static access points (AP) at many locations in a grid in an indoor area. Subsequently, the location of a mobile node, in the same area, is obtained by searching for a match between the current received power fingerprint from the APs and the previously collected received power fingerprints. Fig 12 shows a very small example of the training campaign in the context of Wi-Fi fingerprinting. Nearest neighbor algorithms are well suited for finding the fingerprint match in a fast way.

Horus [21]: Instead of using fixed received power fingerprints, it is also possible to store information about the signal strength distributions from the APs and use probabilistic methods to estimate the

user location during the online phase, as done in the Horus system.

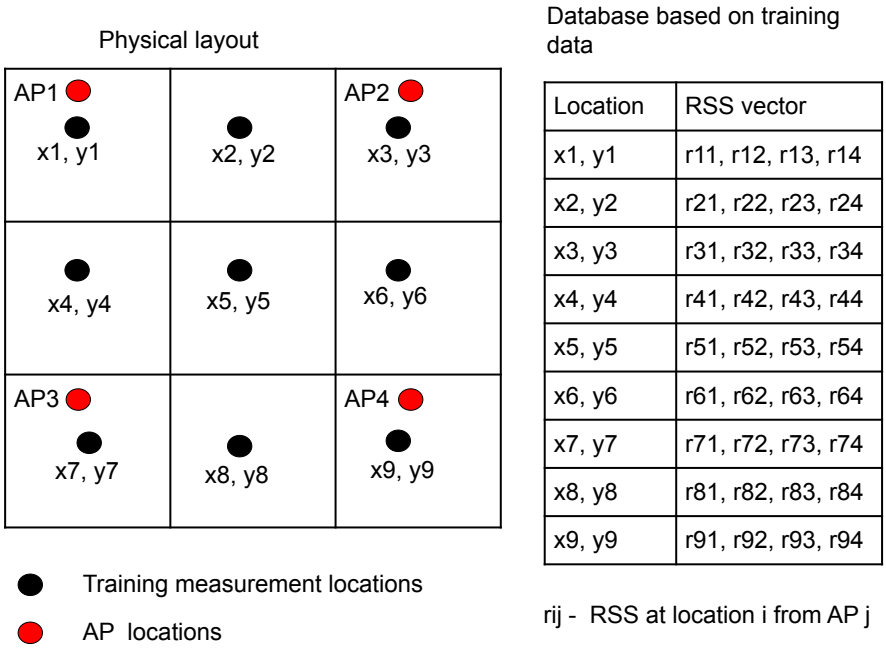


Figure 12: WiFi fingerprinting database [21].

Reducing calibration effort in WiFi fingerprinting: Traditional WiFi fingerprinting methods require extensive manual effort in collecting the fingerprints during training. To circumvent this problem, researchers have investigated ways to make the system work even if the fingerprints are spatially sparse. The basic idea explored by these works is to marginally compromise the accuracy of localization at the cost of significantly reduced training overhead. For example, in the radial basis interpolation method (RBF interpolation) [6] authors collect the training data at room level granularity and then learn a model using the sparsely collected training data. Researchers have also looked at reducing training efforts by collecting sparse training data at strategically important locations. The idea is to exploit the correlation in high dimensional data-space between the locations used for training and the remaining ones [18, 17].

Crowdsourced WiFi fingerprinting: Another interesting idea, in this context of WiFi fingerprinting, is to use crowdsourcing for collecting the training fingerprints [13, 19]. The advantage of this approach is that no dedicated effort is required for creating the fingerprinting database; all the participants contribute towards the data collection effort while engaging in their regular activities.

Almost all learning-based localization algorithms perform better than model-based localization algorithms. However, this advantage of learning-based algorithms comes at a price — irrespective of the approach, all of the existing learning-based localization methods ultimately depend on a static infrastructure. learning-based algorithms assume a constant (or at least known) transmit power from transmitters. On the contrary, the model-based approaches can work with mobile infrastructure, and can be adjusted for unknown or changing transmit powers. One exception is our recent work which attempts to bridge this gap by use a model-based interpolation method to accurately learn both about the infrastructure and the transmitters [15].

References

[1] P. Bahl and V. N. Padmanabhan. RADAR: An In-building RF-based User Location and Tracking System. In *IEEE INFOCOM*, 2000.

[2] J. E. Brittain. Electrical engineering hall of fame: Harald T. Friis. *Proceedings of the IEEE*, 97(9):1651–1654, Sept. 2009.

[3] K. Chintalapudi, A. Padmanabha Iyer, and V. N. Padmanabhan. Indoor localization without the pain. In *Proceedings of the sixteenth annual international conference on Mobile computing and networking*, pages 173–184. ACM, 2010.

[4] M. Feuerstein, K. Blackard, T. Rappaport, S. Seidel, and H. Xia. Path loss, delay spread, and outage models as functions of antenna height for microcellular system design. *Vehicular Technology, IEEE Transactions on*, 43(3):487–498, Aug 1994.

[5] M. Khaledi, M. Khaledi, S. Sarkar, S. Kasera, N. Patwari, K. Derr, and S. Ramirez. Simultaneous power-based localization of transmitters for crowdsourced spectrum monitoring. In *Proc. 23rd Annual ACM International Conference on Mobile Computing and Networking (MobiCom 2017)*, pages 235–247, Oct 2017.

[6] J. Krumm and J. Platt. Minimizing Calibration Effort for An Indoor 802.11 Device Location Measurement System. *Microsoft Research, November*, 2003.

[7] D. Love. A florida man was busted for allegedly using a cell phone jammer to stop people from using their phones while driving, June 2014.

[8] D. Maas, M. H. Firooz, J. Zhang, N. Patwari, and S. K. Kasera. Channel sounding for the masses: Low complexity GNU 802.11b channel impulse response estimation. *IEEE Trans. Wireless Communications*, 11(1):1–8, Jan. 2012.

[9] N. Patwari. *Location Estimation in Sensor Networks*. PhD thesis, University of Michigan, Ann Arbor, MI, Sept. 2005.

[10] N. Patwari, J. Ash, S. Kyperountas, R. L. Moses, A. O. Hero III, and N. S. Correal. Locating the nodes: Cooperative localization in wireless sensor networks. *IEEE Signal Process.*, 22(4):54–69, July 2005.

[11] N. Patwari, A. O. Hero, M. Perkins, N. S. Correal, and R. J. O'dea. Relative location estimation in wireless sensor networks. *IEEE Transactions on signal processing*, 51(8):2137–2148, 2003.

[12] R. J. Pirkl and G. D. Durgin. Optimal sliding correlator channel sounder design. *IEEE Trans. Wireless Communications*, 7(9):3488–3497, September 2008.

[13] A. Rai, K. K. Chintalapudi, V. N. Padmanabhan, and R. Sen. Zee: Zero-effort crowdsourcing for indoor localization. In *Proceedings of the 18th annual international conference on Mobile computing and networking*, pages 293–304. ACM, 2012.

[14] M. Rice. *Digital Communications: a Discrete-Time Approach*. Pearson Prentice Hall, 2009.

[15] S. Sarkar, A. Baset, H. Singh, P. Smith, N. Patwari, S. Kasera, K. Derr, and S. Ramirez. LLOCUS: Learning-based localization using crowdsourcing. In *Proceedings of the 10th Intl. Conf. on Mobile Systems, Applications, and Services (MobiHoc 2020)*, 2020. (to appear).

[16] B. Sklar. The characterization of fading channels, 2002. Course Material, Department of Electrical and Computer Engineering, Eastern Mediterranean University, Cyprus.

[17] S. Sorour, Y. Lostanlen, and S. Valaee. RSS based indoor localization with limited deployment load. In *2012 IEEE Global Communications Conference (GLOBECOM)*, pages 303–308. IEEE, 2012.

[18] S. Sorour, Y. Lostanlen, S. Valaee, and K. Majeed. Joint indoor localization and radio map construction with limited deployment load. *IEEE Transactions on Mobile Computing*, 14(5):1031–1043, 2015.

[19] H. Wang, S. Sen, A. Elgohary, M. Farid, M. Youssef, and R. R. Choudhury. No need to war-drive: Unsupervised indoor localization. In *Proceedings of the 10th international conference on Mobile systems, applications, and services*, pages 197–210. ACM, 2012.

[20] K. Yedavalli, B. Krishnamachari, S. Ravula, and B. Srinivasan. Ecolocation: A sequence based technique for RF-only localization in wireless sensor networks. In *Proc. 4th Int. Conf. on Information Processing in Sensor Networks (IPSN '05)*, April 2005.

[21] M. Youssef and A. Agrawala. The Horus WLAN Location Determination System. In *ACM MobiSys*, 2005.