Wireless Signals

GSM, CDMA, 802.11 layer 1

Outline

- Signals and stuff
- GSM and CDMA
- OFDM and 802.11

Signals

- Some frequency fc is called the carrier frequency. Data is modulated by a carrier wave(sometimes in multiple steps)

$$s_i(t)\cos(2\pi f_c t) + s_q(t)\sin(2\pi f_c t)$$

- Easy to see when looking at the spectrum of the signal. <show spectrum img>

- We are just going to talk about the base band signal from here on out - $s(t)$

GSM Signals

- Frequency Division Duplex
  - Up and down, 25MHz bands
- 200kHz sub channels, each sub-channel can handle 8 users using a TDMA scheme, slot length is 577 micro seconds
- Users do not interfere with each other, separated in time and frequency.

GSM Signals 2

- We can decompose each user's transmissions into a time diversity scheme.
- More diversity is better - we want the different symbols to fade independently of each other.
- If you are walking, there is not enough diversity - the time between symbols is too fast and you don't get an independent fade.
- Solution: Frequency hopping - GSM can hop frequencies between channel frames - more diversity!

What's a GSM symbol?

- Gaussian minimum shift keying is used to be spectrally efficient and to reduce cross channel interference. huh?

$$a_n \in \{-1, +1\}$$

- Like PSK, with g(t) looking gaussian

$$s_i(t) = \sum_{-\infty}^{\infty} a_{2n} g_T(t - 2nT_b)$$
$$s_q(t) = \sum_{-\infty}^{\infty} a_{2n+1} g_T(t - 2nT_b - T_b)$$
$$g_T(t) = Ae^{\frac{t^2}{\sigma^2}}$$

So how do I interfere?

- It depends on what you want to do.
- Interfering is illegal, the bands are licensed and Verizon has paid a lot of money to lobby to get government to make sure frequencies are not available to anyone.
- Stop ALL GSM communications near you?
- Stop a specific user near you?

CDMA Signals

- Code Division Multiple Access is a really complicated system.
- Again, the system is decomposed into p2p links but not by time separation.
- Direct Sequence Spread Spectrum s.t. my signal is your noise.
- Lots and lots of ECC here, we can lose bits all over the place and still ensure that I get my txt messages.

CDMA Signals 2

- No math here, the formulas get too long.
- Convolutional Code (error correcting ability) and block interleaving
- Hadamard-Walsh Sequence (outputs some bits)
- PN code for spreading both I and Q channels
- Some signal shaping filters (for OQPSK)
- All users transmit on all channels all the time

Interfering is harder

- Each user's signal is designed so that it can accommodate all the other users as noise.
- The thing is - this is white noise, not specially designed noise to interfere.
- What do we need to stop CDMA? A lot of noise, on the entire bandwidth.

802.11 (OFDM)

- Orthogonal Frequency Division Multiplexing
- Does anyone care? This presentation is long.
-

Attacks on GSM

- Your voice is encoded, and then encrypted with a very special weak algorithm.
- If someone were to record all the GSM packets, and then later decide to try and decrypt yours it might not be all that hard.
- How sophisticated? $5-10k worth of hardware and the technical skills to use it. Plus some crypto background.

Attacks on 802.11

- WEP - Broken, happens fast. RC4 has issues when used like this besides the obvious WEP cracking fiasco.
- TKIP - Another WEP, just changes keys faster.
- WPA - TKIP + a broken hash function + 802.1x Authentication (RADIUS i think)
- 802.11i - backwards compat + AES option. totally new hardware.

Why is 802.11 Security Doooomed?

- This is my opinion: Protocols, Cryptographic implementations, and hash functions which are designed in a closed environment influenced by companies are always going to have big problems.
- Less testing, less theoretical backing, and more do what you can for the money.
- That is all. Use OpenVPN.