Technicity of Radio Signal Transmissions

Carl Colena

Carl Colena works as a research engineer, running the Signal Identification Guide (SIGID) wiki as a hobby. His interest in signal identification developed during his studies in computer engineering at the City College of New York.

The SIGID wiki website was started in 2014 during the so-called 'RTL-SDR boom': the discovery that small USB dongles, made for digital television (DTV) reception, could be used as computer-based radio scanners. Several people including Antti Palosaari, Eric Fry and group gathered around Osmocom,[1] hacked the driver on the RTL2832U chipset and found a way to access the raw IQ data from the analogue to digital converter, which samples the radio frequency space. The tuner on the DTV device can tune into a very wide range of frequencies. The discovery of this affordable software-defined radio (SDR) was still made in a professional research domain. Still, the use of RTL-SDR proliferated and a community formed around it, curious to explore the radio space.

The SIGID wiki website documented different signals that could be recorded using this equipment. Within three to four years, the wiki grew from about 80 signals to over 300. We have a community of individuals who use the website for a variety of purposes. There are amateur radio operators who focus on shortwave transmissions (SWLs). They listen for the purposes of listening, to discover new signals and track the patterns

1 See https://sdr.osmocom.org/trac/wiki/rtl-sdr (accessed 01.06.2021).

of different transmissions in their area. Other users come from the information security space, seeking to understand more on wireless and baseline some of their designs. Then there are tech hobbyists who are interested in the radio space in general, in radio frequency and the ability to transmit information in various different ways.

Signal engineering

A comparison with acoustic waves is useful to understand radio signals: acoustic waves, such as the sound of the human voice, are generated by longitudinal waves, which transmit information by compressing air in the direction of travelling (Figure 2, top). Radio waves, a combination of an electric and a magnetic field, are transverse waves: they oscillate orthogonally to the direction to that which the wave travels. These are physically different phenomena, but they are both about the propagation of energy going in a specific direction.

We receive a radio signal in the digital domain using analogue to digital converters (ADCs) that sample the analogue space of the wave at a certain frequency. What is typically done in SDR, is to use an I and Q generator that takes the end phase component, and then simultaneously sample both in-phase (I) and quadrature (Q) waveforms as a single wave, saving the two pieces of data as a single sample in time. The digitally quantized form of the received signal is the accumulation of these samples. An IQ plot shows each individual component and complex form as a given magnitude: a polar circle of both magnitude and angle. This is the process typically used to sample and process signals.

Radio signals have a specific frequency associated with them, In the physical space, there can only be as many different signals as there are different frequencies, without interference. This is based on the Fourier theory of the frequency domain and the translation between time and frequency domains. When it comes to radio signals that transmit information, we can think of transmission frequencies as channels, and the derivatives of this frequency as bandwidth or the quantity of information being sent. In the domain of telecommunication and radio engineering, we talk about carrier frequencies. This is a baseband signal that has information embedded into it. It could be voice, digital data, or anything else. The bandwidth or the width of the signal, is usually much lower than the carrier frequency. Human voice, for example, is typically between 100Hz and 3KHz, making its bandwidth about 3KHz wide. The actual frequency of the signal partitions signal space, so that different transmissions can be individually tuned into and received without overlapping and distortion. Understanding carrier frequencies as 'channels' paints radio signals as a finite resource.

Consistent with the Fourier theory, instead of frequency, time division can be used to avoid interference and overlaps. Multiple signals could share the same frequency, sliced into different time chunks. Successful communication in this case requires coordination between operators.

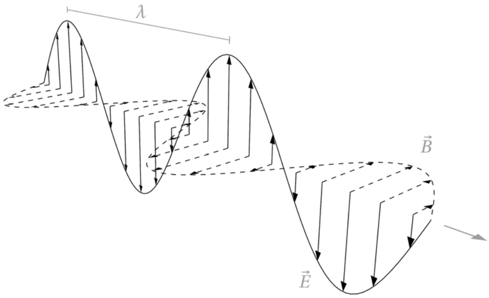
Intentionality of radio signal transmissions

A radio wave is an oscillation of energy (Figure 1). Signal engineers have come up with ways to use this to transmit information by modulating the radio wave. Two very common types of modulation are amplitude (AM) and frequency modulation (FM). With AM, the channel is the carrier frequency at which this wave is actually oscillating, and then data itself is the overlaid signal, in form of a changing amplitude. With FM, amplitude is fixed and the frequency is changing: the compression between the oscillations gets narrower and wider, corresponding to the actual amplitude of the original signal.

By simply changing the domain at which the signal is transported, for example by using an FM demodulator on that AM signal and plotting the received information, we would just get a flat line because the frequency in AM is constant. The same would be the other way around, using an AM demodulator on the FM signal. If we were to receive the signal with incorrect or unintended method of reception, it would contain no information. Whether or not a signal has informational content, therefore depends on how it is received, and how the signal was intended to be transmitted.

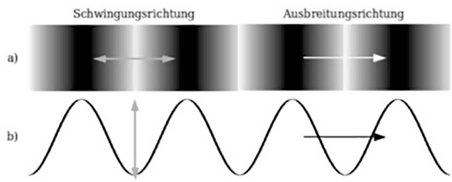
Two primary modalities that are used in signal analysis are acoustic and visual. Both are interpretations which can bring out different perspectives on radio signals, as we could see with AM and FM demodulation. It is important to gather multiple perspectives on a radio wave in order to fully understand it.

Figure 1: Electromagnetic wave.



Author Lennart Kudling, 2010. CC-BY-SA-3.0.

Figure 2: Direction of oscillation and propagation of a longitudinal wave (a) and a transverse wave (labels in German).



Author Debianux, 2018. CC-BY-SA-3.0.

Figure 3: Three types of modulation. Left: Frequency-shift keying modulation. An example demonstrating binary FSK. Middle: Phase-shifting keying modulation. Right: Digital Amplitude Modulation Signals (OOK – On-Off Keying).

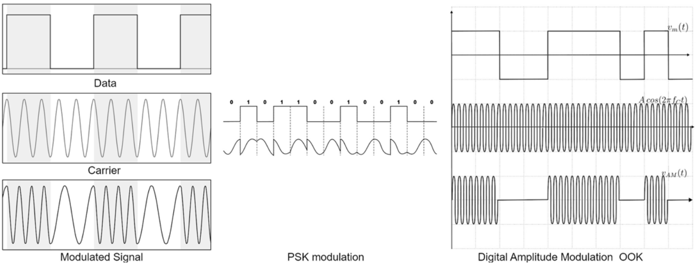


Image redrawn by Selena Savić based on sources: Left: Author Ktims, 2006, CC-BY-SA-3.0; Middle: Author Maria Moura Malburg, 2004 CC BY-SA 4.0; Right: Author Ramjar, 2014, CC BY-SA 4.0.

In terms of signal understanding, we typically try to look for patterns, signatures and tonalities that exist in the signal. This is combined with the visual component in order to have multiple perspectives on the signal at once, while also using a variety of modes, for example the upper-side band, which is probably the closest to raw listening or listening to the signal as it was sent. AM and FM modes are often used as well, depending on the way that the signal was meant to be received. With digital methods of signal transmission such as FSK (Figure 3, left), frequency shifts with respect to the carrier as the data is overlaid, resulting in periods of higher and lower frequency. In PSK (Figure 3, middle), frequency and amplitude stay the same, but the phase of the signal shifts (efficient for transmissions in a populated frequency space). In ASK (Figure 3, right) the signal can be modulated or not, it simply switches on and off.

One extreme perspective on radio signals is an encoding technique called ‘spectrum painter’, which uses the spectrum of a certain bandwidth and a digital analogue converter (DAC), to paint images on the spectrum. If we were to listen to this on the radio, it would sound like digital noise, but when it is received with a spectrum analyser tool, it plots a picture. With regards to intentionality, this signal is clearly not meant to be listened to, but it transports intentional visual information.

An interesting case of intentionality is the intention not to be seen, typically used for InfoSec such as pseudo random hopping signals. This makes it very difficult for a receiver to capture and decode a message broadcast on shifting frequencies.

Ultra-wide band signals lend themselves to another form of intentionality. These signals exist below the noise floor. For example, Driftnet Radio Buoys, used by fishing boats in open seas to locate and collect fishing nets. The beacon normally sends out a variety of dots and tones at a stable frequency, but the signal begins drifting, sounding almost like a dolphin, when the batteries become weak. A signal can therefore have many different forms, not just due to the intention of the transmission, but also to factors that may just be physical, such as battery power.

Natural radio

Natural radio phenomena include spherics and whistlers. These are transmitted at a very low frequency (VLF) range and are purely natural transmissions. They are induced by natural events, such as lightning. Spherics come from lightnings which cause strong bursts of electromagnetic energy, such that you can actually hear them as simultaneous bursts in the acoustic domain. Their electromagnetic emissions sound like crackles. Whistlers are reverberations from lightning that have passed through the magnetosphere. You can think of them as shooting stars.

There are a lot of natural phenomena that produce radio signals at very low frequency (VLF) level. Two forms of listening are of interest here. One is media scattering: hobbyists listening for a manmade transmitter, one that they know they could not actually receive under normal circumstances, due to distance. They point their receiver up to the sky and they do something similar to passive coherent radar (PCR) technique, listening for reflections. This is typically done at a very high frequency (VHF), 141 MHz. When meteorites travel or burn up in the upper atmosphere, they leave behind this ionizing particle cloud. Under the right circumstances, the transmitted signals from the Earth hit this ionization cloud and bounce down, over the horizon, so that they can be heard on the other side of the planet. These are called meteor echoes, because a transmitter gets echoed off of a meteor trail. Whether or not this is a natural or manmade signal is an interesting discussion, but the role of natural phenomena in the transmission of a manmade emission is clearly important.

Discussion

Miro Roman: I imagine taking the database of radio signals to compare all the sounds, or to create a context where they can live together. According to what Carl Colena is saying, the first move would be to translate them to the same modality. How would you work with sounds of different duration? I have an idea how to do this with text and with images, but not with sound.

Carl Colena: When it comes to comparison, you certainly want to compare signals from the same perspective. You do not want to compare the AM demodulation of one signal and the FM demodulation of another. But when it comes to what forms, what kind of signatures you can think of, look for, I know one of particular interest. It is the autocorrelation function (ACF), going into the order of frequency. You can compress the actual frequency of the modulating signal itself into a single number (or a much lower dimensionality piece of data), if a signal has that sort of periodicity. For example, what is the frequency of your modulating signal? That itself could be a single attribute. This is obviously depending on whether or not the signal has periodicity, as well as what is the form of this periodicity.

Some signals, like the FSK, have a minimum spacing between the tones, which could be considered a comparative attribute. There are certain things that we do in identification, we look for factors that would be common throughout the signals, and then use that to reduce the dimensionality space.

Signals that are not well structured, such as natural phenomena, make it hard to find a regularity because there may not be any periodicity in the signal. What you may need to do then, is look for signal differentiation: taking a derivative of the signal or looking at the rate of change of different properties throughout. For example, with the whistlers, there was a frequency change in the sound, which could be mapped as a function and as frequency of response in these signals. In spherics, there might be a high impulse between samples.

In general, you would look for different ways to 'signaturize' or come up with some sort of categorization that you can use upon multiple signals, such that you can find similar patterns in many signals. You first have to bring them to the same level and then, when it comes to radio, do the additional modality on top, so that you can process the sounds in a similar fashion.

Simone Conforti: If I were to compare radio signals to words, or other things with widespread accepted meaning, working with radio signals completely depends on what you are searching for. We can generalize and compare with looking for words and putting those words in a context or in another. This can give us something comparable.