HARDWARE AND DEVICE-TO-DEVICE COMMUNICATION SECURITY

Notes about that

Fabio Lorenzato

Contents

Part I

Wireless

Chapter 1

Digital Communication

This first section is all about how to convert and transmit some signal.

1.1 Introduction

The goal of communication is to transmit some kind of data form a sender to a receiver. In order to do so, the physical layer defines the means of transmitting a stream of **raw bits** over a physical data link, which connects those two nodes.
Data is transmitted in the form of **signals**, which are a physical representation of the data. The signal is transmitted over a **channel**, which is the transmission medium that connects the sender and receiver. This can be both wired or wireless.
Whereas with wired channels, checking the device connected to the channel is easier to implement, with wireless ones security is a major when travelling in the channel. This is for may reasons:

- No inherent protection is applied to the channel(it is replaced by a logical association)

  sending and receiving messages do not need physical access to the network infrastructure

- the communication is in broadcast, which is intrinsic of radio nature.

  Transmission can be overheard by anyone in range(which can be quite big, depending on the situation), and anyone can generate a transmission, for example by jamming nearby transmissions.

As a result:

- Eavesdropping is easy
- Injecting fake messages into the communication in easy
- replaying previously recorded messages is easy(*meaconing*). This is actually very dangerous for gps positioning, so it is also a security concern.
- illegitimate access to the network and its services is easy
- Denial of service attacks are easy, achieved by jamming the channel.

1.2 Digital Communication System

The digital communication system in characterized by three sections:

- the **user section**, which consist in the transmitter and the receiver, that want to communicate.
- the **interface section**, which is the interface to conveying the signal from the user to the analog channel. It also transforms bits to analog signal, compressing and encoding them, also associating bits to signal waveforms, to transform bits to analog signal.
- the **channel section**, which is the physical medium, that can only propagate analog waveforms. In the end, we want to transmit digital signal but we are forced to use analog ones.

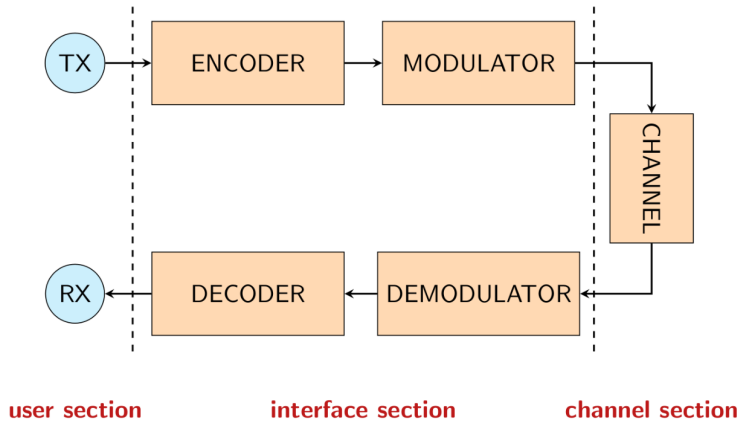

Figure 1.1: Digital Communication System

1.2.1 The transmitter chain

The transmitter chain is the part of the system that takes the digital signal, or an analog one converted to digital, and converts it to an analog signal, that can be transmitted over the channel.
It is basically composed by two parts. The first one being an **encoder**, which can limit the amount of bits transmitted(*source encoding*), and/or make the transmitted sequence more robust to errors(*channel encoding*).
The second one is the **modulator**, which is the part of the system that takes the digital signal and converts it to an analog one to transmit it over the channel.

1.2.2 The channel

The channel is the physical medium that transfers bits from interface to interface, from the sender to the receiver. Its operation is affected by different types of disturbances such as:

- frequency-domain distortion
- wireless fading

- additive noise
- impulsive noise
- interference from other frequency channels (interchannel interference)
- interference from the same frequency channel (cochannel interference)
- Intentional interference

1.2.3 The receiver chain

The receiver chain is the part of the system that takes the analog signal from the channel and converts it to a digital signal, that can be processed by the user.
It is composed by the dual counterpart of the transmitter chain, the **demodulator** and the **decoder**.
The demodulator takes the analog signal and converts it to a sequence of samples that can be processed by the decoder.
The decoder takes the sequence of samples and converts it to a digital signal. It implements *channel decoding*, to correct errors, and *source decoding*, to recover the original message.

1.3 Signal representation and Processing

> A **signal** is a (mathematical) function that conveys information about a phenomenon.

Basically, any quantity that varies over space or time can be used to represent a informations, allowing to describe the evolution of physical quantities over time(voltages, currents, ...).
Its mathematical representation is therefore a function of real variable (time) taking real or complex(more than one) values.
We will be mostly focused on Electromagnetic Signals (e.g. voltage), but the general concepts can be applied to any kind of signal

1.3.1 Energy of a signal

The energy of a signal is the integral of the squared modulus of the signal itself.

$$E(x) = \int_{-\infty}^{\infty} |x(t)|^2 dt \tag{1.1}$$

As we can see , the energy is a scalar value, and the whole function is made positive by the squared modulus.
A signal with a very large amplitude, over time, will have a very high energy, while a signal which assumes values close to zero will have a very low energy, being a very weak signal.
Furthermore, we can note that the more distant is the signal from the origin, the larger the energy.

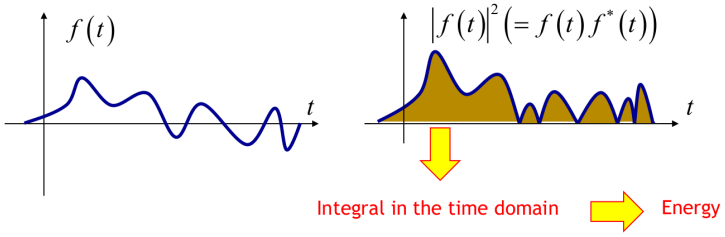

Figure 1.2: Energy of a signal

1.3.2 Power of a signal

When we refer to power we can refer to the **instantaneous power** of a signal, which is just the square module of a signal

$$P(x) = |x(t)|^2 \tag{1.2}$$

but much more commonly we refer to the average power of a signal, which is the time average of the instantaneous power of the whole signal.

$$P(x) = \lim_{a \to \infty} \frac{1}{2a} \int_{-a}^{a} |x(t)|^2 dt \tag{1.3}$$

This a again a scalar value.

1.3.3 Signal Representation

To analyze and process the signals, it is necessary to adequately represent them, and the definition of signals as "time functions" is NOT effective for many applications, for many reasons.
Generally, signals can become very complicated depending on our communication system, and we want different ways of representing them, to make them easier to process.
For instance, we can represent a signal as a sum of elementary signals, thanks to the scalar product of the signal with a basis of the space of signals.

The scalar product between signals is a scalar value, which is a measure of the similarity among signals.
If two function are quite similar we will get a large number. It it is zero, they are said to be orthogonal.

$$\langle x, y \rangle = \langle x(t), y(t) \rangle = \int_{-\infty}^{\infty} x(t) y^*(t) dt \tag{1.4}$$

So, if we have a set of elementary signals $w_1(t), w_2(t), \ldots, w_m(t)$, we write the signal $x(t)$ as a linear combination of the elementary signals:

$$x(t) = \sum_{i=1}^{m} \alpha_i w_i(t) \tag{1.5}$$

where α_i are the coefficients of the linear combination $\alpha_i = \langle x(t), w_i(t) \rangle$.

In a more down to hearth way, the coefficient α_i allows us to understand how much each individual signal is similar to any other elementary signal we are considering, and because the scalar product is higher for similar signals, we can understand how much each elementary signal is contributing to the whole signal.

Furthermore, by adjusting the coefficient, we are able to create a whole different signal using the same elementary signals.

A common example: In Phase and Quadrature Representation

Lets consider a very simple basis, or a set of elementary signals, which is actually more important that many other ones:

- the **in-phase** signal, which is a cosine function $w_1(t) = cos(2\pi f_o t)$
- the **quadrature** signal, which is a sine function $w_2(t) = sin(2\pi f_o t)$

where f_o is the frequency, in Hz, of the signal.
We can write any signal as a linear combination of these two signals, just by adjusting the coefficients:

$$x(t) = x_1 cos(2\pi f_o t) + x_2 sin(2\pi f_o t) \tag{1.6}$$

where x(t) is the signal we want to represent, and x_1 and x_2 are the coefficients of the linear combination.

A very simple representation of this complex signal is obtainable by representing each signal as an axes in a complex plane, for example in figure 1.3 the x-axis is the in-phase signal, and the y-axis is the quadrature signal.
Each signal can be represented as a point in the complex plane, because the distance from the origin signal(*axis*) is the amplitude of the signal. For example, choosing a point close to the x-axis, we are choosing a signal with a very low quadrature component, and a very high in-phase component.

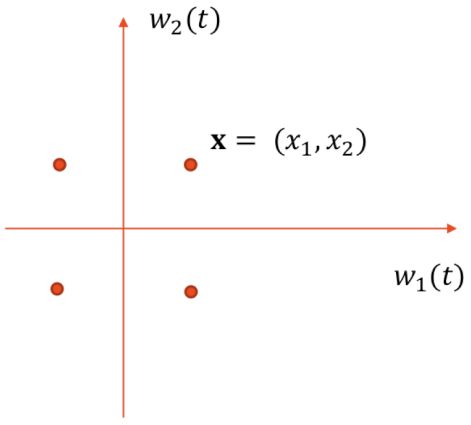

Figure 1.3: Some points that represent some signals in the I/Q representation

1.3.4 Fourier Analysis

Lets consider a signal with bases the complex exponential functions

$$e^{j2\pi\frac{n}{T}t} = cos(2\pi\frac{n}{T}t) + jsin(2\pi\frac{n}{T}t) \tag{1.7}$$

It is actually characterized by a frequency $f_n = \frac{n}{T}$, where T is the period of the signal. The higher the frequency, the more oscillations we will have in the same time interval.

We can use that function as a basis to decompose a signal, again.

Part II

Hardware