Laboratory 2: Unauthorized Access in Wireless Networks

Niclas Scheuing and Vasileios Dimitrakis

November 19, 2015

1 Introduction

The goal of this laboratory exercise is to introduce us to the spread spectrum techniques. Spread spectrum refers to a system developed to spread the signal over a large frequency band, in order to increase the security of the communication. The main idea behind this systems is to use more bandwidth and at the same time to maintain the same amount of power in the whole signal. These techniques offer increased resistance to interference, noise, jamming and channel multipath and fading effects. These properties make them very popular and frequently prefered in communication systems. There are three main spread spectrum techniques that are frequently used:

- *Frequency Hop Spread Spectrum*: Is a method of transmitting radio signals by rapidly switching a carrier among many frequency channels, using a pseudorandom sequence known to both transmitter and receiver.
- *Chirp*: Is a signal, which decreases or increases its frequency continuously over time. It has many applications and one of them is the property of spread spectrum that offers.
- *Direct Sequence Spread spectrum*: Is a spread spectrum technique whereby the original data signal is multiplied with a pseudo random noise spreading code.

In this exercise we will study the case of the Direct Sequence Spread Spectrum (DSSS). In DSSS the signal is used to modulate a bit sequence, which is known as Pseudo Noise (PN) code. This code consists of pulses that have much shorter duration than the one of original signal. Therefore, this

process chops up the pulses of the message signal and this leads to broader signal's bandwidth that tends to be equal to the one of the PN code. This spread spectrum technique is widely used, because it offers many benefits and for this reason, it is widely used in both military and civilian communication systems.

- Resistance to intended or unintended jamming.
- Multiple users can share the same channel.
- Robust against noise.
- It provides a way to determine relative timing between transmitter and receiver.
- DSSS spreads the signal over a wide range of frequency and the latter can be hidden below noise level.

2 Topology

In this exercise we have one DSSS transmitter and one DSSS receiver. In this system, we have two main signal components: the message signal m(t) and the pseudorandom code code(t).
Transmitter: First of all, the transmitter modulates the data signal with a primary modulator using a modulation scheme, e.g BPSK. After that it multiplies the outcome of the previous process with the PN code generator and the bandwidth of the signal is spread to a wider range of frequencies.
Receiver: On the other hand, in the receiver the reverse process is followed. Firstly, the receiver despreads the broadened signal using the appropriate PN code. In the next step, it demodulates the signal using the carrier, in order to retrieve the data.

3 Materials and Methods

Throughout the lab exercise 2 we used different materials and methods, that are presented below:

- *MATLAB*: Vector- and numerical computing environment.

4 Terminology

5 Tasks

6 Questions

6.1 System configuration

Length of message Length of code chips per symbol
Processing gain: In a spread spectrum system, the process gain (or 'processing gain') is the ratio of the spread (or RF) bandwidth to the unspread (or baseband) bandwidth. It is usually expressed in decibels (dB).

6.2 Jamming resistance of DSSS

Below noise multiband

6.3 Security introduced by DSSS

6.4

7 Analysis

In this lab we demonstrated that some widely used security mechanisms as MAC-filtering, WEP and WPA2 are prone to rather simple

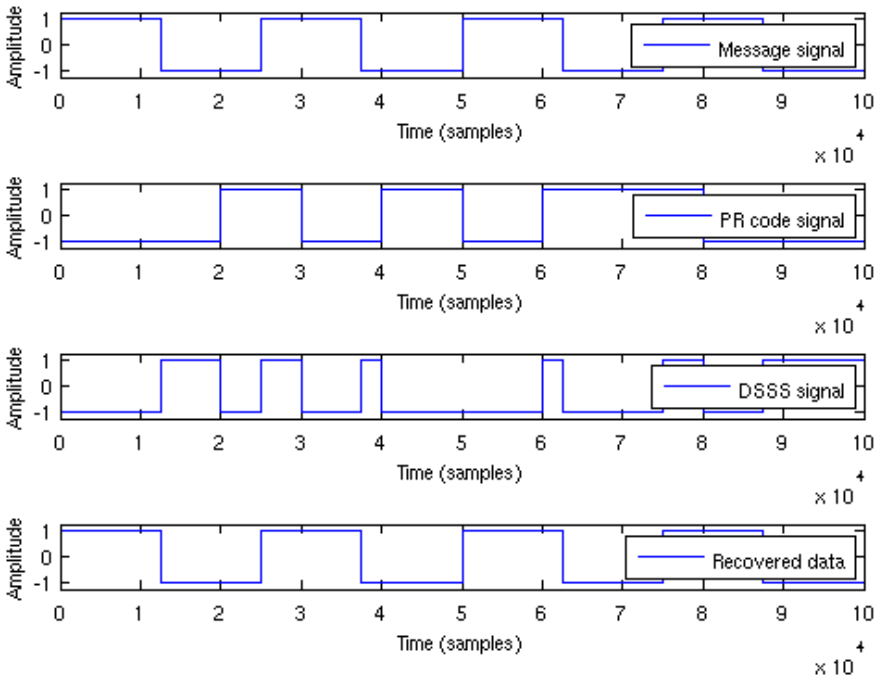

Figure 1: Capturing the traffic using source MAC address filtering.