# Laboratory 3: DSSS

Niclas Scheuing and Vasileios Dimitrakis

November 27, 2015

## 1 Introduction

The goal of this laboratory exercise is to study the spread spectrum techniques. Spread spectrum schemes spread the signal over a large frequency band. 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 preferred 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 3 we used *MATLAB*, a vector- and numerical computing environment.

# 4 Theory

Some basic concepts need to be discussed first.

## 4.1 Signal analysis

To reason about the power spectrum of a signal $s(t)$ we need to study its Fourier transform $F(s)$. Let's assume $s$ consists of block functions

$$b_{\sigma,T}(t) = \begin{cases} 1 & \text{if } \sigma - \frac{T}{2} < t < \sigma + \frac{T}{2} \\ 0 & \text{else} \end{cases} \tag{1}$$

where $\sigma$ is the center of the block function, $T$ the width and $n$ the number of blocks. So our signal is the following

$$s(t) = \sum_{i=1}^{n} b_{\sigma_i,T}(t) \tag{2}$$

. Looking at the Fourier transform we get

$$\begin{aligned}
F(s(t)) &= \int_{-\infty}^{\infty} s(t) e^{-2i\pi t\xi} dt && (3)\\
&= \int_{-\infty}^{\infty} \sum_{i=1}^{n} s(t) e^{-2i\pi t\xi} dt && (4)\\
&= \sum_{i=1}^{n} \int_{-\infty}^{\infty} s(t) e^{-2i\pi t\xi} dt && (5)\\
&= \sum_{i=1}^{n} \int_{t_i-\frac{T}{2}}^{t_i+\frac{T}{2}} e^{-2i\pi t\xi} dt && (6)\\
&= \sum_{i=1}^{n} \frac{1}{-2\pi i\xi} \left[e^{-2i\pi t\xi}\right]_{t_i-\frac{T}{2}}^{t_i+\frac{T}{2}} && (7)\\
&= \sum_{i=1}^{n} \frac{1}{-2\pi i\xi} \left[e^{-2i\pi(t_i+\frac{T}{2})\xi} - e^{-2i\pi(t_i-\frac{T}{2})\xi}\right] && (8)\\
&= \sum_{i=1}^{n} \frac{1}{-2\pi i\xi} \left[e^{-2i\pi t_i\xi} e^{-i\pi T\xi} - e^{-2i\pi t_i\xi} e^{i\pi T\xi}\right] && (9)\\
&= \sum_{i=1}^{n} e^{-2i\pi t_i\xi} \frac{1}{\pi\xi} \left[\frac{e^{-i\pi T\xi} - e^{i\pi T\xi}}{-2i}\right] && (10)\\
&= \sum_{i=1}^{n} e^{-2i\pi t_i\xi} \frac{T}{T\pi\xi} \sin(\pi T\xi) && (11)\\
&= \sum_{i=1}^{n} e^{-2i\pi t_i\xi} T\mathrm{sinc}(T\xi) && (12)\\
& && (13)
\end{aligned}$$

The power spectrum is the $s(t)$ is the function $|F(s)|$, which yields

$$|F(s)| = \left| \sum_{i=1}^{n} e^{-2i\pi t_i \xi} T \text{sinc}(T\xi) \right| = T \sum_{i=1}^{n} |\text{sinc}(T\xi)| \tag{14}$$

There are two main observations to be made.

**Observation 1** *The maximum of the power spectrum of a block shape signal $s(t)$ is proportional to the width of one block $T$.*

**Observation 2** *The width of the first lobe of the power spectrum of a block function $b_{t_0,T}(t)$ is proportional to $\frac{1}{T}$. More formally: $2\,|t - t_0| \propto \frac{1}{T}$ where $t_0$ is the center of the block function and for $t$ holds $b_{t_0,T}(t) = 0$ and $|t - t_0|$ is minimal.*

### 4.2 Processing gain

In a spread spectrum system, the process gain $P$ (or 'processing gain') is the ratio of the DSSS signal bandwidth to the `data` bandwidth. It is usually expressed in decibels (dB). This is equivalent to the ratio of the maximum of the `data`'s power spectrum to the maximum of the DSSS signal's power spectrum. Observation1 thus yields $P = \frac{T_d}{T_c}$

## 5 Terminology

The data array, representing our block signal, is denoted as `data` and the chip sequence `chip`. The length on the time axis of a `data` bit is named $T_d$ where the length on the time axis of a `code` bit is $T_c$.

The total length of `data` in bits is called `DL` and of the `code` `CL`.

## 6 Tasks

The following steps were done when working with the MATLAB implementation of DSSS.

Executing it for the firsttime resulted in the despreading to fail. This was due to the fact that despreading with a different code than the one used for spreading, does not restore the original message.

We then fixed the code and made it use the same key for spreading and despreading. The reconstruction of the DSSS signal succeeded.

**Configuring the DSSS system** `DL` and `CL` were used in the following four configurations.

1. `DL`= 10bit , `CL`= 10bit. See Figure 1 and Figure 2.
   `data = [1 -1 1 -1 1 -1 1 -1 1 -1]`
   This results in a one chip per symbol modulation, which means $T_d = T_c$ and for the processing gain $P = \frac{10}{10} = 1$ Accordingly, as seen in Figure 2, the power spectra of `data` and the DSSS signal is almost the same.

2. `DL`= 10bit , `CL`= 100bit. See Figure 3 and Figure 4.
   `data = [1 -1 1 -1 1 -1 1 -1 1 -1]`
   $P = \frac{100}{10} = 10$. By looking at the plots, we observed a processing gain that is rather 3.5. The calculated value is for a block signal and the measurements were made on a BPSK modulated signal. The observed deviations might root in this difference.
   Figure 4 shows that the power spectra of `data` is much smaller than the the DSSS signal's because $T_c << T_d$.

3. `DL`= 5bit , `CL`= 100bit. See Figure 5 and Figure 6.
   `data = [1 -1 1 -1 1 ]`
   $P = \frac{100}{5} = 20$. The same observation as previously are made.
   The power spectra seen in Figure 6 look almost the same as for `DL`=10 and `CL` = 100. The `data` power spectrum for `DL`=5 is slightly lower than for `DL`=10 since $T_{d_5} > T_{d_{10}}$ The DSSS signal power spectrum is very similar since the $T_c$ does not change.

4. When using `DL`=5 and `CL` = 300 we observe some weird behavior in the MATLAB implementation. We assume this is a bug. See Figure 7.

# 7 Questions

## 7.1 Jamming resistance of DSSS

The broadband signaling schemes are more difficult to jam, because their energy is spread through a broad span of frequencies. The receiver has the same spreading code that the transmitter used to spread the signal and he is able to retrieve the message.

**Narrow-band jamming** Resistant, because the jamming signal gets spread while despreading.

**Wide-band** Resistant because the jamming signal is not correlated to code and thus does not get despread. Except if the jamming power is high enough to cover the despread signal.

## 7.2 Security introduced by DSSS

The CIA security properties and the possibility to detect a DSSS signal under noise are discussed in this section.

**Confidentiality** In a noise-less setup DSSS does not provide IND-CPA, because it is deterministic. An chosen plaintext attack will immediately reveal the code when the plaintext message gets XORed to the ciphertext. The DSSS signal looks random to anyone not knowing the code. In presence of noise the signal is said to be *hidden below the noise*. An eavesdropper can not distinguish between the noise and the DSSS signal. But this still does not provide IND-CPA, since noise has some statistical properties that can be used filtering. Also the position in time can just be brute-forced by multiplying the observed DSSS signal with the plaintext message using different time shifts.

**Integrity** DSSS does not provide strong integrity. Th receiver cannot verify that the message has not been altered by an attacker or a very unlucky noise constellation.

**Availability** DSSS does assure availability in presence of a jammer as discussed in page 5.

**Detection** [1] In the presence of noise a DSSS signal is hard to detect. It has some static properties that make it distinguishable from random noise, such as a constant chip length, though. Also by monitoring the energy level of the electro magnetic waves, the presence of an additional sender can be revealed.

## 7.3 Advantages and uses of DSSS

Beyond the property of avoiding intended or unintended jamming and the other security properties that DSSS provides, it has also some other uses and advantages[2]:

- First of all, the United States GPS, the European Galileo and the Russian GlONASS satellite navigation systems use DSSS, when they

transmit their data, as they can share the same channel for multiple users using different codes.

- DS-CDMA is a multiple access scheme based on DSSS, by spreading the signals from/to different users with different codes.
- Cordless phones operating in 900 MHz, 2.4 GHz and 5.8 GHz bands use DSSS.
- DSSS is also used for IEEE 802.11b 2.4 GHz Wi-Fi, its predecessor 802.11-1999 and for IEEE 802.15.4.

# 8 Analysis

Summarizing all above, we conclude our report with the following statements

- Observations 1 and 2 were clearly visible in section 6, but with some deviations. We assume these are due to using BPSK modulation instead of a block signal. We summarize our observations about the processing gain and the reasoning from Observation 1 and 2 as a dependency not on `CL` or `DL` but on the ratio $\frac{CL}{DL}$
- DSSS is robust against intended and unintended jamming, as it is able to hide the signal below the noise level. Finally, broadband jamming can be effective, if the attacker has enough power to use, in order to achieve his goal.
- Eavesdroppers cannot simply retrieve the original signal if they do not have the spreading code. Some of the basic security properties are not given though.

# References


[1] R.A. Dillard. Detectability of spread-spectrum signals. *Aerospace and Electronic Systems, IEEE Transactions on*, AES-15(4):526–537, July 1979.

[2] Wikipedia. Direct-sequence spread spectrum. `http://en.wikipedia.org/wiki/Direct-sequence_spread_spectrum`, 2015.

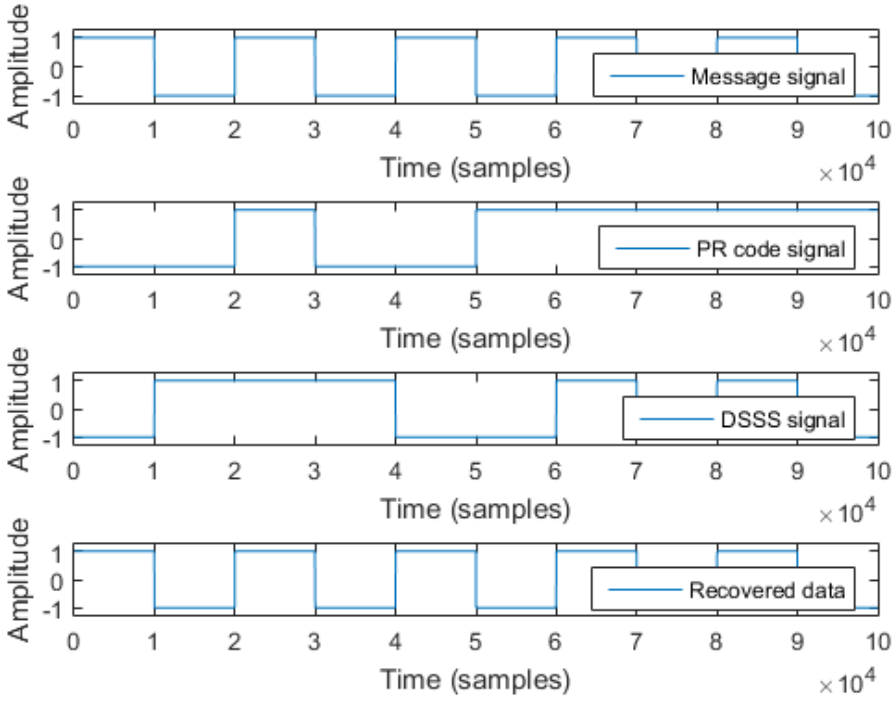


Figure 1: Original, spread and despread signal and code. Code length: 10bit, data length: 10bit

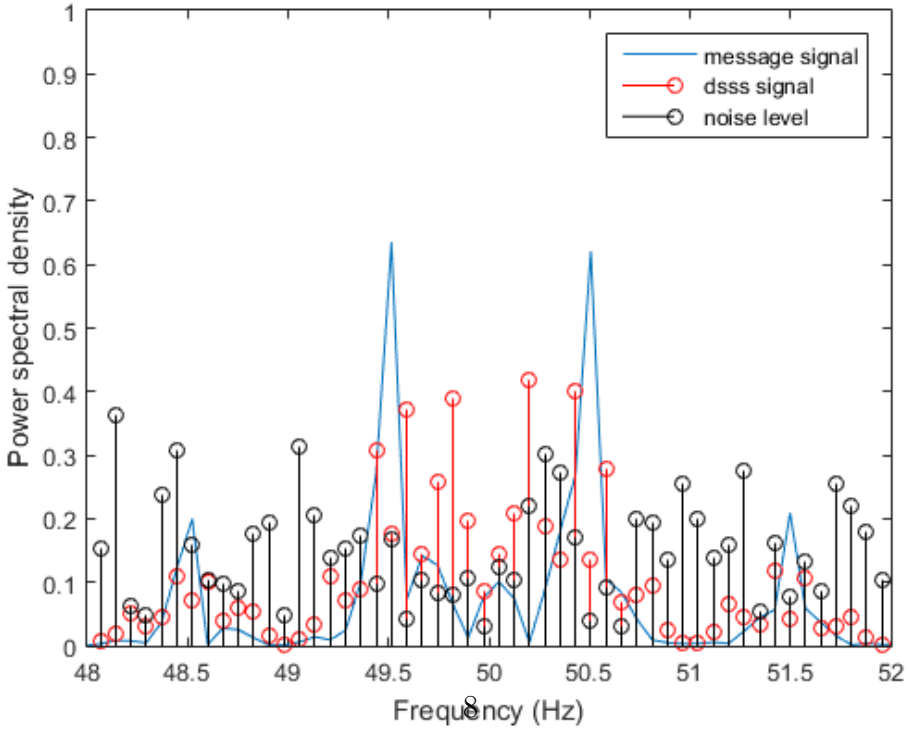


Figure 2: Original, spread and noise power spectra. Code length: 10bit, data length: 10bit

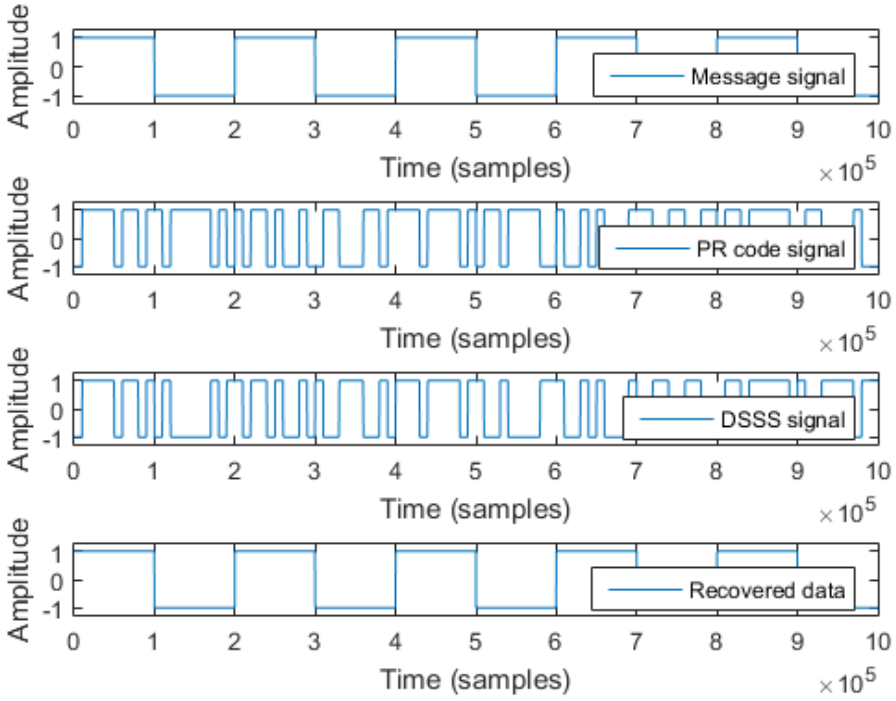


Figure 3: Original, spread and despread signal and code. Code length: 100bit, data length: 10bit

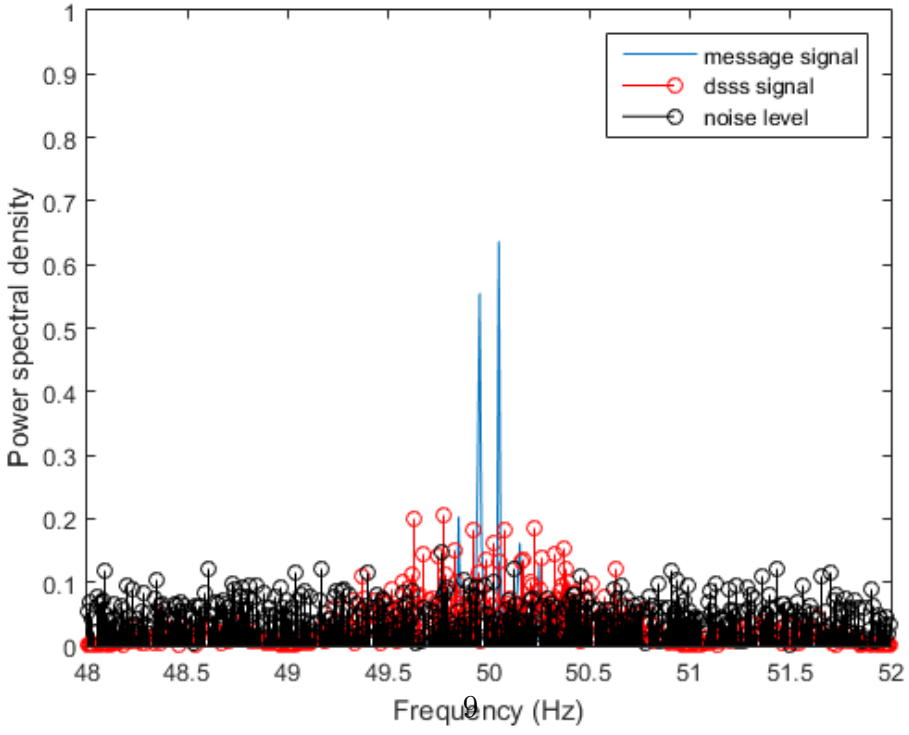


Figure 4: Original, spread and noise power spectra. Code length: 100bit, data length: 10bit

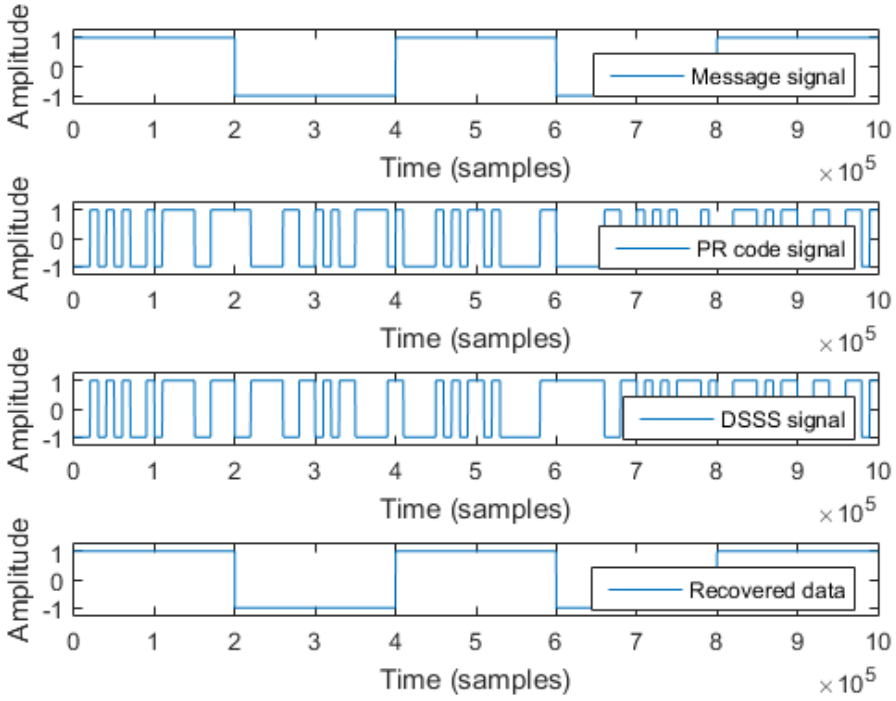


Figure 5: Original, spread and despread signal and code. Code length: 100bit, data length: 5bit

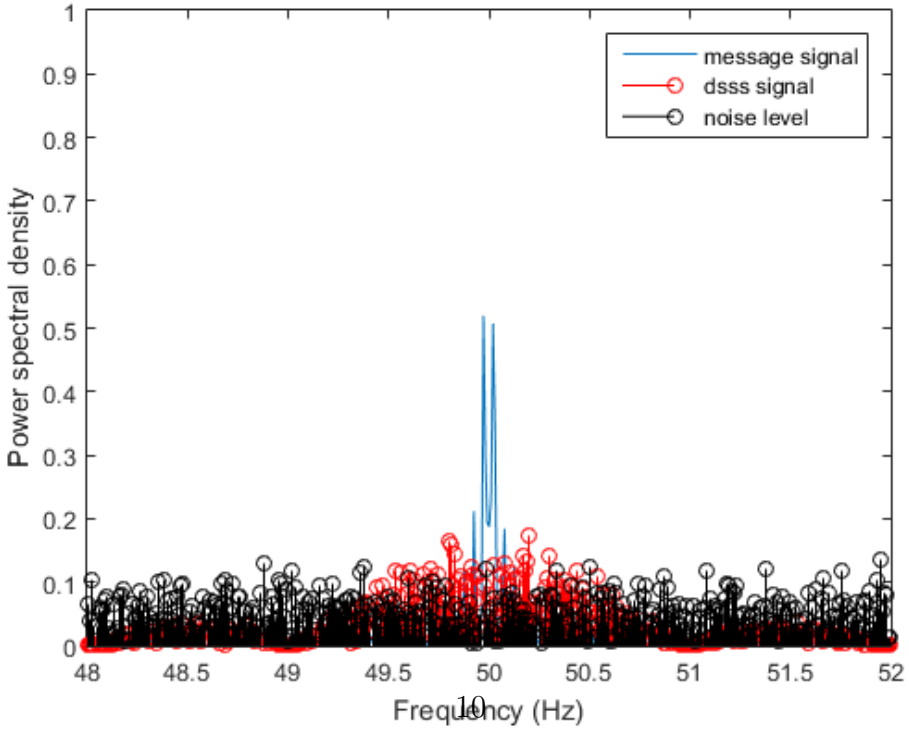


Figure 6: Original, spread and noise power spectra. Code length: 100bit, data length: 5bit

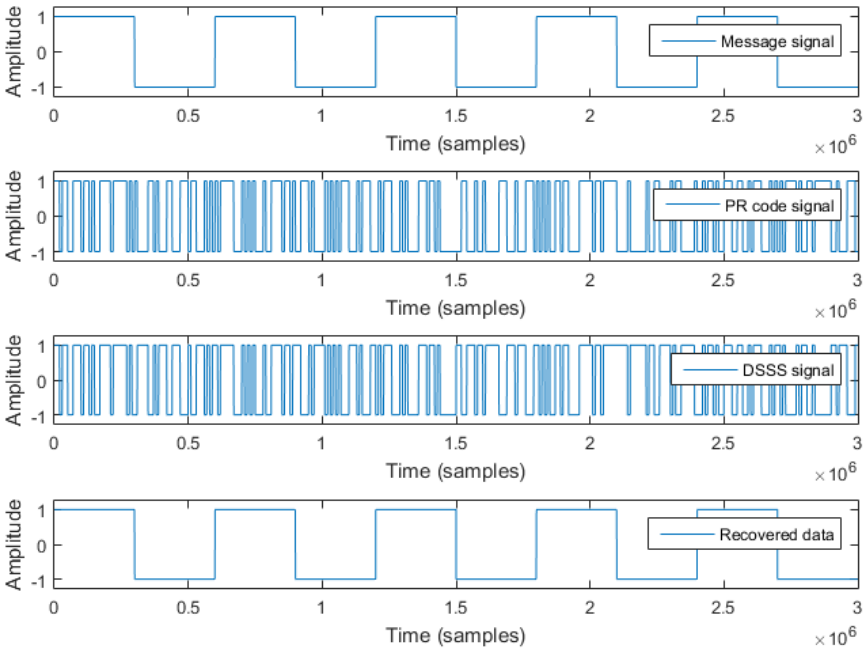


Figure 7: Original, spread and despread signal and code. Code length:300bit, data length: 10bit. The time axis seems to be buggy. The data array labeling is wrong.