Acknowledgments

Contents

Chapter 1

Global navigation satellite systems

1.1 GNSS principles

1.2 Galileo spreading codes

We calculate the cross correlation of all different E1-b codes. We get that the maximum of the absolute value of the cross correlations is **244**. This could be our design criterion. Figure 2 shows some circular cross correlations.

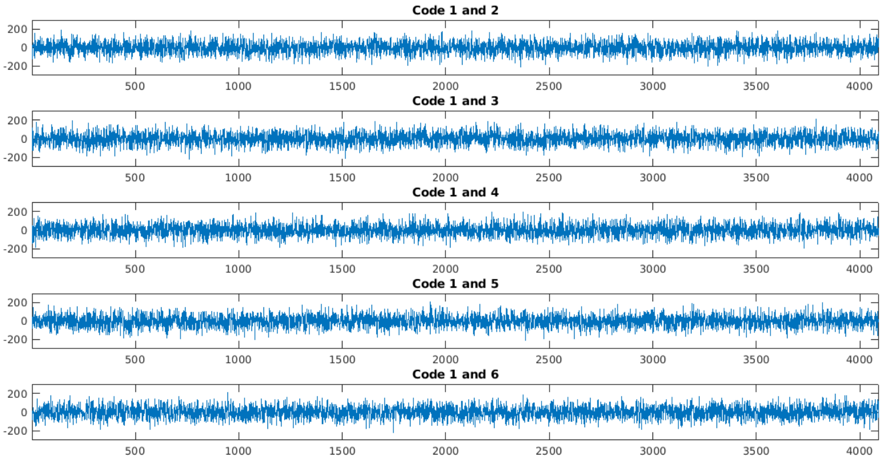

Figure 1.1: circular cross correlations of code 1 with codes 2 through 6.

Values of all cross correlations of different E1-b codes are distributed according to the histogram in figure 3. We cross correlate random unitary power gaussian noise with all different spreading codes and plot the distribution of the resulted values in figure 4.

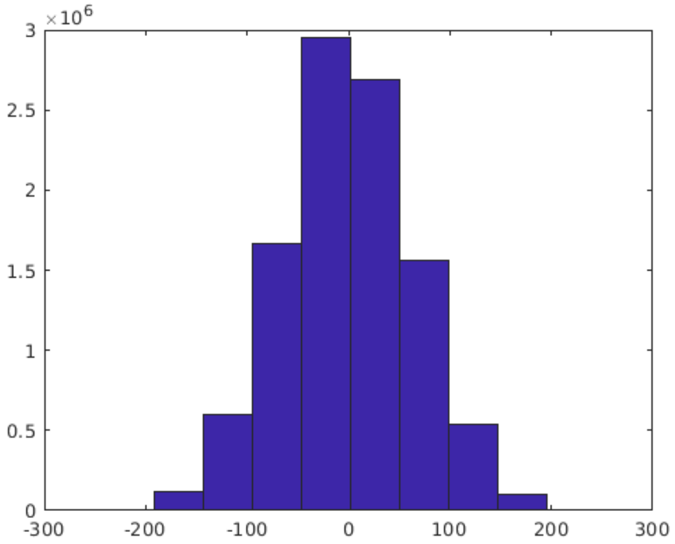

Figure 1.2: Distribution of all circular cross correlation values of different codes

We suppose that there are 25 free spreading sequences. We use them to build noise. We construct a unitary power noise sequence by spreading a random gaussian value with 25 unused spreading codes. We sample the noise and add further noise on different samples such that the sum of the 4 noise samples is equal to sum of the 4 samples without added noise.

We plot the distribution of cross correlation values of the noise with the 25 other used codes.

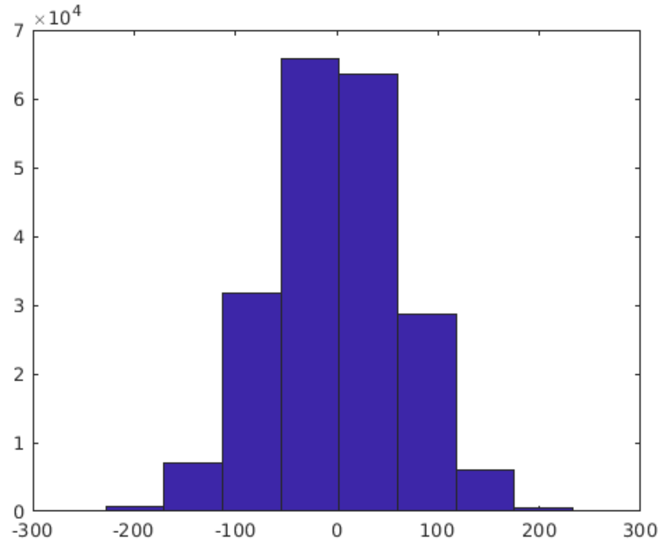

Figure 1.3: Distribution of all cross correlation values of different codes with random unitary power gaussian noise

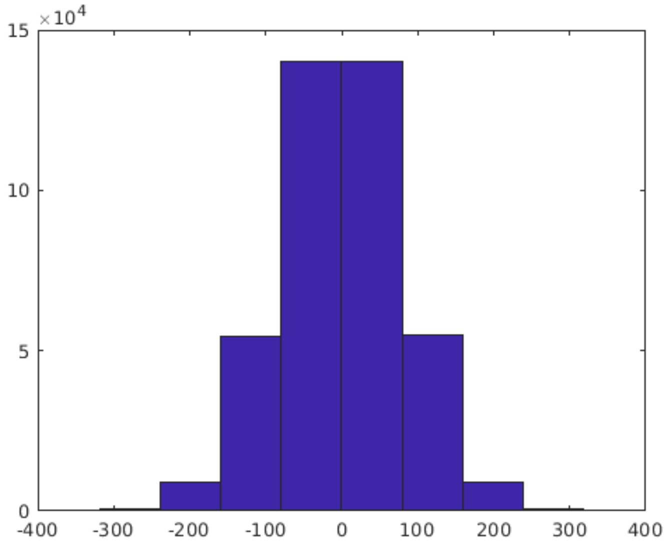

Figure 1.4: Distribution of all circular cross correlation values of the AN and the 25used codes

Chapter 2

Authentication protocols

2.1 System model

Our system model consists of N_B satellites, a receiver and a spoofer. Where N_B denotes the number of visible satellites to the receiver. The satellites provide timing and positioning services by continuously broadcasting navigation signals to the users. The receiver must have in view at least four different satellites in order to successfully calculate it's space and time coordinates. The spoofer aims to mislead the receiver by transmitting to it false navigation signals. We assume that the spoofer has high-end receiving equipment enabling it to receive navigation signals with high SNR.

From now on we will refer to the receiver by the name Bob, and to the spoofer by the name Eve. The model comprises different communication channels. First off, the wireless navigation channels though which the satellites broadcast their signals $s_i(t)$ to Bob. Since the distances separating Bob from each satellite are different, Bob receives the superposition of these signals with random delays δ_i. Next, the attack channel through which propagates the spoofing signal $s_E(t)$ transmitted by Eve to mislead Bob. Finally, An authenticated channel that connects the users including Eve to the ground segment. We assume that this channel has high bandwidth and that Eve cannot interfere with it. For example it could be a secure Internet connection. In an additive white Gaussian noise channel the received signals by Bob and Eve could be written as

$$r_B(t) = \sum_{i=1}^{N_B} s_i(t - \delta_i) + s_E(t) + \omega_B(t) \tag{2.1}$$

$$r_E(t) = \sum_{i=1}^{N_E} s_i(t - \mu_i) + \omega_E(t), \tag{2.2}$$

where $\omega_B(t)$ and $\omega_E(t)$ are the zero mean AWGN signals that model the effects of thermal noise and interfering signals with power $\sigma^2_{\omega_B}$ and $\sigma^2_{\omega_E}$, respectively. N_E is the number of satellites visible to Eve. δ_i and μ_i are the propagation delays from satellite i to Bob and Eve, respectively.

We delimit our model to the Galileo E1 band which is composed of two signals, data and pilot. We focus on the data signal $p_i(t)$ carrying the unitary power data stream d_{ij} with period T_s which could be written as

$$p_i(t) = \sum_{j=-\infty}^{+\infty} d_{ij} r_i(t - jT_s), \tag{2.3}$$

where

$$r_i(t) = \sum_{k=0}^{N_c-1} c_{ik} u(t - kT_c) \tag{2.4}$$

is the pulse used to spread navigation data of satellite i with chip period $T_c = T_s/N_c$ where N_c is the spreading factor, $c_{ik} = \pm 1$ and $u(t)$ is the chip pulse and can be written as

$$u(t) = \begin{cases} 1, & 0 \leqslant t \leqslant T_c \\ 0 & otherwise. \end{cases} \tag{2.5}$$

2.2 Artificial noise at symbol level

In the following section we describe an authentication protocol for the navigation signals based on the addition of an authentication signal corrupted by artificial noise at symbol level to the navigation signal. Adding AN at symbol level means adding noise on top of the symbols of the authentication message before spreading them.

Each satellite generates an authentication message V_i. This message is encoded and modulated and x_{ij} denotes the modulated symbols. Artificial noise ω^*_{ij} is then added to each authentication symbol. Then both are spread using a spreading pulse $r_{A,i}(t)$ orthogonal to all navigation spreading pulses $r_i(t)$. The authentication signal could be written as

$$z_i(t) = \sum_{j=-\infty}^{+\infty} (x_{ij} + \omega^*_{ij}) r_{A,i}(t - jT_s), \tag{2.6}$$

where

$$r_{A,i}(t) = \sum_{k=0}^{N_c-1} c_{A,ik} u(t - kT_c) \tag{2.7}$$

is the pulse used to spread the authentication signal of satellite i where $c_{A,ik} = \pm 1$.

Every satellite superimposes synchronously this authentication signal $z_i(t)$ to it's data signal $p_i(t)$. So the final transmitted signal from each satellite could be written as

$$s_i(t) = p_i(t) + z_i(t). \tag{2.8}$$

Bob saves all of the received authentication symbols. Then through the authenticated channel the ground segment reveals to all users the authentication messages V_i and the artificial noise ω_{ij}^* that was added. Bob checks the authenticity by removing the artificial noise from the saved received symbols and extracting the authentication messages V_i and comparing them to those revealed to him by the ground segment. where