Cybersecurity
Electronic and Communication Technologies
(Secure) Spread Spectrum Communications

Giacomo Bacci, Marco Luise
marco.luise@unipi.it

Dip. Ingegneria dell’Informazione, Univ. Pisa, Pisa, Italy
Baseband Data (PAM) Signal

\[ s(t) = \sum_{k=\infty}^{\infty} a_k \cdot p(t - kT) \]

Binary Pulse-Amplitude Modulation (PAM)

Symbol Interval: \( T = \) Bit Interval: \( T_b \)

Symbol Rate: \( R = 1/T = \) Bit Rate: \( R_b = 1/T_b \)

Antipodal Format

\( \{ a_k \} = \pm 1 \) Binary Data

Basic Pulse \( p(t) \):

A

<table>
<thead>
<tr>
<th>+A</th>
<th>a_0</th>
<th>a_1</th>
<th>a_2</th>
<th>a_3</th>
<th>a_4</th>
</tr>
</thead>
<tbody>
<tr>
<td>-A</td>
<td>T</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Electronic and Communication Technologies
Cybersecurity
Power Spectral Density (PSD) of the PAM Signal

\[ S_s(f) = \frac{A^2}{T} |P(f)|^2 \]
Spreading the Spectrum

The Spread-Spectrum signals «runs» at the same clock (the chip-rate) as the spreading code

\[ s(t) \rightarrow \times \rightarrow x_{SS}(t) \]

\[ c(t) \]

\[ M=8 \]

\[ s(t) \]

\[ c(t) \]

\[ T \]

\[ T_c \]

\[ t \]
The data symbols are *chipped* at the chip-rate: the resulting signal is faster and the spectrum is *wider-bandwidth* by a factor $M$. 

$$s(t)$$

$$c(t)$$

$$x_{SS}(t)$$

$$(+A, -A, +1, -1)$$

$$(T_T, T_c)$$

$$(s(t), c(t), x_{SS}(t))$$

SPREADING CODE
Direct-Sequence Spread Spectrum

\[ s(t) = \sum_{k=-\infty}^{\infty} a_k \cdot p(t - kT) \]

PAM Signal

M=Spreading Factor

\[ c(t) = \sum_{m=-\infty}^{\infty} c_m q(t - mT_c) \]

PSEUDO-NOISE Sequence

Chip Pulse

\[ T_c = T/M \]

Chip Time
Spread Spectrum !!

**Linear Scale**

**Log (dB) Scale**

GPS: chip rate $R_c$: 1.023 Mchip/s

bit rate $R_b$: 50 bit/s $\Rightarrow M=20460$
The DS/SS Receiver

\[ z(t) = s(t)c(t) + w(t) \]

\[ c(t) = s(t)c^2(t) + w'(t) \]

\[ = 1! \]
NO difference w.r.t a narrowband modulation!

Spectrum spreading/despreading is a transparent operation (but the bandwidth is much larger)
The overall spectrum is partitioned in $2^M$ bins

The spreading factor is LARGER

HOP Pattern

MT_c  2MT_c  Time

The spreading factor is LARGER
The receiver just demodulates the SS signal via a hopping oscillator with the same hop pattern.

Not used in multiple-access communications or positioning – commonplace in secure (military) communications.
Just to know..

Who’s invented Spread-Spectrum?
Can you believe?

Hedy Lamarr,
actress
The Cybersecurity Play & Characters

ALICE → BOB

EVE

MALLORY

Cybersecurity

Electronic and Communication Technologies

Dip. Ingegneria dell’Informazione
University of Pisa, Pisa, Italy

Marco Luise

(Secure) Spread-Spectrum Communications
In-band Interfering Power

\[ P_i = \frac{P}{\sqrt{T_c}} \cdot \frac{1}{T} = \frac{P T_c}{T} = \frac{P}{M} \]

\[ P_i = \frac{P}{T_c} \cdot \frac{1}{T} = \frac{PT_c}{T} = \frac{P}{M} \]

Narrowband Interference

Power \( P \)

SS signal

Before Despreading

\( 1/T_c \)

Frequency

After Despreading
The Cybersecurity Play & Characters

- **ALICE**
- **BOB**
- **EVE**
- **MALLORY**

Diagram with electronic and communication technologies and cybersecurity characters.
**Linear Feedback Shift-Register LFSR**

*with P delay elements*

The **CODE POLYNOMIAL** describes the outputs that are to be XORed:

\[ G(x) = 1 + x + x^2 + x^4 + x^6 \]
Maximal-Length Sequences

**Def:** $G(x)$ has no prime factors and divides $1+x^L$ in $GF(2^P)$

**Properties:**

- *M*-sequences have the maximum possible periodicity: $L=2^P-1$
- They contain $2^P/2$ 1s and $2^P/2-1$ 0s (BALANCED sequences)
- XORing an M-sequences with a delayed replica of itself gives the same M-sequence with a third phase
- If you slide a P-bit window on the sequence, you get all of the numbers between 1 and $2^P$
- There is a limited number of M-sequences for a given $P$
Gold Codes

- Family of $L+2$ codes with period $L=2^p-1$
- (Logical) sum of two $M$-sequences of length $L$
- May be done balanced (preferentially phased)
- Used in GPS, UMTS
- Good spectrum
- The average cross-correlation is low (quasi-orthogonal codes)

$$\mu = \frac{1}{N-1} \sum_{k=2}^{N} \left( \frac{1}{L} \sum_{m=0}^{L-1} C_m^{(1)} C_m^{(k)} \right)^2 = 1$$
**Autocorrelation Function of a PN sequence**

**Code Autocorrelation**

\[ R_p[k] = \frac{1}{L} \sum_{m=0}^{L-1} C_mC_{m+k} \]

Scan the values of \( k \) and find that one that maximizes the cross-correlation between the noisy received signal \( r_m = c_m + w_m \) and the local replica code \( C_{m+k} \).
Optimum code acquisition

Maximum Likelihood = Simple correlation processing:

\[ \hat{\tau} = \arg\max_{\delta} \left\{ \int_{0}^{T_0} r(t) s(t - \delta) dt \right\} \]

Scan the values of \( \delta \) and find that one that maximizes the cross-correlation between the received signal \( r \) and the local replica code \( s \).
Multiplexing: Time- and Frequency-Division

**TDMA:** The user signals are separated in **TIME** (overlapped in frequency)

**FDMA:** The user signals are separated in **FREQUENCY** (overlap in time)

- **User data signals to be multiplexed**
Code Division Multiplexing

Each user is assigned a signature code used to spread his/her own data signal.

The users are overlapped both in time and frequency. They can be separated only via de-spreading with the appropriate code.
\[
\int_0^T c^{(i)}(t) c^{(k)}(t) \, dt = 0, \quad i \neq k
\]

\[
H_2 = \begin{bmatrix}
1 & 1 \\
1 & -1
\end{bmatrix}
\]

\[
H_4 = \begin{bmatrix}
1 & 1 & 1 & 1 \\
1 & -1 & 1 & -1 \\
1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1
\end{bmatrix}
\]

\[
H_H = \begin{bmatrix}
H_{H/2} & H_{H/2} \\
H_{H/2} & -H_{H/2}
\end{bmatrix}
\]
The user signals are ORTHOGONAL (but synchronicity is needed)

$$\int w_i(t)w_k(t)dt = 0, \ i \neq k$$

Table of Walsh-Hadamard Functions $L=8$

<table>
<thead>
<tr>
<th>Code</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>$w_0(t)$</td>
<td>[Graph]</td>
</tr>
</tbody>
</table>
**Code-Division Multiplexing and Multiple Access**

**Synchronous multiplexing:** All users share the same data and chip clock.

- Co-located user signals
- Broadcast Pilot Signal

**Asynchronous MULTIPLE ACCESS:** No need of user synchronization (sort of random access)
GPS constellation

• 24+4 satellites about 1 ton each
• Average height 20,192 km (period about 12 h)
• Average speed 3874 m/s (14,000 km/h)
• 6 orbits
• 55 deg wrt the Equator
GPS constellation

- 24+4 satellites about 1 ton each
- Average height 20,192 km (period about 12 h)
- Average speed 3874 m/s (14,000 km/h)
- 6 orbits
- 55 deg wrt the Equator
### GPS Carriers

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>C/A SIGNAL</th>
<th>P SIGNAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>CODE CLOCK RATE - $R_c$</td>
<td>1.023 MCHIPS/SEC</td>
<td>10.23 MCHIPS/SEC</td>
</tr>
<tr>
<td>CODE LENGTH</td>
<td>1023 CHIPS (1 ms)</td>
<td>≈ 6 TRILLION CHIPS (1 WEEK)</td>
</tr>
<tr>
<td>DATA RATE</td>
<td>50 BITS/SEC</td>
<td>50 BITS/SEC</td>
</tr>
<tr>
<td>TRANSMISSION FREQUENCY</td>
<td>$L_1 = 1575.42$ MHz, $= 1540 R_c$</td>
<td>$L_1 = 1575.42$ MHz, $= 154 R_c$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$L_2 = 1227.6$ MHz, $= 120 R_c$</td>
</tr>
</tbody>
</table>

**Data includes:**

- **TELEMETRY**
- **SYNCHRONIZATION INFORMATION (PREAMBLE, TIME)**
- **SATELLITE CLOCK AND EPHEMERIS PARAMETERS**
- **ALMANACS**
- **IONOSPHERIC DELAY AND UTC TIME MODELS**
GPS L1

- **Carrier frequency (MHz):** 1575.42
- **Multiple Access Technique:** CDMA
- **Services:** PPS, SPS
- **Signal Bandwidth (MHz):** 20.46
- **PRN code rate (Mcps):** 10.23 (P), 1.023 (C/A)
- **PRN code length (c):** 2.35E+14 (P), 1023 (C/A)
- **NAV data rate (bps):** 50
- **NAV symbol rate (sps):** 50
- **Modulation:** BPSK