Detection of Direct Sequence Spread Spectrum Transmissions without Prior Knowledge

G. Burel, C. Bouder and O. Berder
L.E.S.T. – FRE CNRS 2269
Université de Bretagne Occidentale, BP 809, 29285 Brest cedex, France
Email: Gilles.Burel@univ-brest.fr

Abstract – **Direct sequence spread spectrum transmissions (DS-SS) are now widely used for secure communications, as well as for multiple access. Since the transmission uses a large bandwidth, the power spectral density of a DS-SS signal can be below the noise level. Hence, such a signal is difficult to detect.**
In this paper, we propose a method which is able to detect a spread spectrum signal hidden in the noise. The method does not require a priori knowledge about the spreading sequence used by the transmitter. It is based on two parallel computations: the "theoretical path", in which we compute the theoretical behavior of the fluctuations of second order moments estimators in the case noise alone is present, and the "experimental path", in which we compute the actual fluctuations. When a DS-SS signal is hidden in the noise, the results provided by both paths diverge, hence the presence of the signal is detected. Experimental results show that the method can detect a signal far below the noise level.

I. Introduction

Spread spectrum signals have been used for secure communications for several decades [7]. Nowadays, they are also widely used outside the military domain, especially in Code Division Multiple Access (CDMA) systems [2][3]. Due to their low probability of interception, these signals increase the difficulty of spectrum surveillance.

In direct-sequence spread spectrum (DS-SS), the information signal is modulated by a periodic pseudo-random sequence [6] prior to transmission, resulting in a wideband signal with low probability of interception [1][4]. Indeed, the DS-SS signal can be transmitted below the noise level, because the receiver knows the pseudo-random sequence and therefore can use a correlator [5] to increase the signal-to-noise ratio (SNR). For instance, with a pseudo-random sequence length equal to 127, the correlation gain is 21dB. Hence, even if the DS-SS signal is received with $SNR = -10dB$, at the correlator output the SNR is $+11dB$.

In the context of spectrum surveillance, the pseudo-random sequence used by the transmitter is unknown (as well as other transmitter parameters such as duration of the sequence, symbol frequency, etc.). Hence, in that context, the presence of a DS-SS transmission is very difficult to detect. In this paper, we propose a method to detect DS-SS transmission far below the noise level. It is based on analysis of the fluctuations of second order statistics estimators. The method considers two parallel paths:

- The "theoretical path", in which we compute what these fluctuations should be if noise only were present. This path provides theoretical bounds: they are computed in order to ensure that, when noise only is present, the probability to get fluctuations outside these bounds is very low.
- The "experimental path", in which we compute the actual fluctuations. This is done by temporally dividing the received signal into analysis windows, applying estimators of second order statistics on each window, and then using the results to compute the fluctuations.

We prove that, when a DS-SS signal is hidden in the noise, the actual fluctuations go outside the noise-only bounds provided by the theoretical path.

Not only the method provides a detection of a DS-SS signal hidden in a noise, but it also provides a precise estimation of the duration of the pseudo-random sequence used by the transmitter.

The performance of the method increases with the number of windows (which itself increases with the duration of the signal used for computing statistics), and also with the length of the pseudo-random sequence used by the transmitter. For example, for pseudo-random sequences of length 127, and 400 analysis windows, the detection limit is, approximately, –12dB, and the computation time is only a few seconds on a PC.

The paper is organized as follows. In Section 2, we give the notations and hypotheses. Then, in Sections 3 and 4, the experimental and theoretical paths are described. The principle of the detection is explained in Section 5. Finally, experimental results are provided to illustrate the approach (Section 6) and a conclusion is drawn (Section 7).

II. Notations and Hypotheses

In a DS-SS transmission, the symbols a_k are multiplied by a pseudo-random sequence which spreads the bandwidth. The pseudo-random sequence, as well as the carrier and symbol frequencies, are known by the receiver. The receiver correlates the received signal with the pseudo-random sequence, in order to retrieve the symbols. A receiver which does not know these parameters cannot even detect the presence of a DS-SS signal, because it is usually under the noise level.

We will use the notations below:

g(t), $G(\nu)$: the receiver filter impulse response and its Fourier transform.

h(t): the convolution of the pseudo-random sequence with the transmitter filter (and with the channel echoes if they exist).

r(t): the convolution of *h(t)* with the receiver filter.

$\gamma_x(\nu)$: the power spectral density of a signal *x(t).*

T_s: the symbol period.

L: the length (number of bits) of the pseudo-random sequence.

T_c: the chip period ($T_c = T_s / L$)

T: the duration of the analysis window

$s_c(t)$ and *s(t):* the noise-free signal at the input and at the output of the receiver filter.

$n_c(t)$ and *n(t):* the noise at the input and at the output of the receiver filter.

σ_n^2 : the noise variance, at the output of the receiver filter.

σ_s^2 : the variance of the noise-free signal, at the output of the receiver filter.

The signal at the output of the receiver filter is then:

$y(t) = n(t)$

when no signal is hidden in the noise, and

$y(t) = s(t) + n(t)$

when a DS-SS signal is hidden in the noise.

The DS-SS signal is:

$$s(t) = \sum_{k=-\infty}^{+\infty} a_k h(t - kT_s) \qquad (1)$$

The following hypotheses are assumed:

- The symbols are centered and uncorrelated.
- The received noise $n_c(t)$ is white, gaussian, centered, and uncorrelated with the signal. Its power spectral density is $N_0 / 2$
- The signal to noise ratio (in *dB*) at the output of the receiver filter is negative (the signal is hidden in the noise).

III. THE EXPERIMENTAL PATH

The received signal is divided into non-overlapping windows of duration *T* (the exact value of *T* does not matter; ideally, the window should contain a few symbols, but the methods works over a large range of values). With each window, we compute an estimation of the correlation:

$$\hat{R}_{yy}^{(m)}(\tau) = \frac{1}{T}\int_0^T y(t)y^*(t-\tau)dt \qquad (2)$$

where m is the index of the window.

Using *M* windows, we can estimate the second order moment of the estimated autocorrelations:

$$\rho(\tau) = \frac{1}{M}\sum_{m=1}^{M}\left|\hat{R}_{yy}^{(m)}(\tau)\right|^2 \qquad (3)$$

This is a measure of the fluctuations of the autocorrelation estimator.

IV. THE THEORETICAL PATH

In the theoretical path, we assume that **noise only is present**, and we compute the theoretical average value and standard deviation of $\rho(\tau)$.

The theoretical average value of the fluctuations is (it does not depend on τ):

$$m_\rho^{(n)} = E\{\rho(\tau)\} = E\left\{\left|\hat{R}_{nn}(\tau)\right|^2\right\}$$

This is the average power of the estimated autocorrelation signal. Hence, we can write:

$$m_\rho^{(n)} = \int_{-\infty}^{+\infty}\gamma_{\hat{R}}(\nu)d\nu$$

If *T* is not too small, we have:

$$\gamma_{\hat{R}}(\nu) = \frac{1}{T}\left|\gamma_n(\nu)\right|^2$$

Hence:

$$m_\rho^{(n)} = \frac{1}{T}\int_{-\infty}^{+\infty}\left|\gamma_n(\nu)\right|^2 d\nu \qquad (4)$$

We can note that the power spectral density of the noise, at the output of the receiver filter is:

$$\gamma_n(\nu) = \left|G(\nu)\right|^2\frac{N_0}{2} \qquad (5)$$

The standard deviation of the fluctuations is:

$$\sigma_\rho^{(n)}(\tau) = \sqrt{\mathrm{var}\{\rho(\tau)\}}$$

Since the windows are independent, using equation 3 we obtain:

$$\sigma_\rho^{(n)}(\tau) = \sqrt{\frac{1}{M}\mathrm{var}\left\{\left|\hat{R}_{nn}(\tau)\right|^2\right\}}$$

where:

$$\mathrm{var}\left\{\left|R_{nn}(\tau)\right|^2\right\} = E\left\{\left|R_{nn}(\tau)\right|^4\right\} - \left(m_\rho^{(n)}\right)^2$$

The statistical behavior of $\hat{R}_{nn}(\tau)$ is almost gaussian, because it is the average of a large number of independent random variables (see eq. 2). Furthermore, its average value is zero (except for low value of τ, for which the short term coherence created by the receiver filter results in non-zero autocorrelation). Hence:

$$E\left\{\left|R_{nn}(\tau)\right|^4\right\} = 3\left(m_\rho^{(n)}\right)^2$$

The result does not depend on τ. Then, we obtain:

$$\sigma_\rho^{(n)} = \sqrt{\frac{2}{M}}\, m_\rho^{(n)} \qquad (6)$$

The theoretical path performs the computations below:

1. Compute the power spectral density $\gamma_n(\nu)$ of the signal at the output of the receiver filter.
2. Compute the theoretical average value $m_\rho^{(n)}$ of the fluctuations (eq. 4)
3. Compute the theoretical standard deviation $\sigma_\rho^{(n)}$ of the fluctuations (eq. 6)
4. Then, compute the theoretical upper bound of the fluctuations: $m_\rho^{(n)} + 4\sigma_\rho^{(n)}$. Strictly speaking, this is not an upper bound, but we know that the fluctuations will remain below this bound with a high probability.

V. Detection

The results provided by both paths are displayed to a human operator. The display shows the curve $\rho(\tau)$ computed by the "experimental path", and the upper bound computed by the "theoretical path". If no signal is present, the curve remains under the upper bound with a high probability. If a signal is hidden in the noise, the curve goes above the theoretical upper bound for every value of τ that is multiple of the symbol period.

Below, we show why, when a signal is present, high fluctuations are obtained for every τ multiple of the symbol period T_s. For simplicity, the proof is restricted to $\tau = T_s$, and only the most important intermediate results are given. Using equations 1 and 2, we can show that:

$$\widehat{R}_{ss}(T_s) = \frac{1}{T}\sum_{k=-\infty}^{+\infty} a_k a_{k-1}^* \int_0^T \left|r(t-kT_s)\right|^2 dt$$

After a few mathematical manipulations, the average value of its square modulus reduces to:

$$m_\rho^{(s)} = E\left\{\left|R_{ss}(\tau)\right|^2\right\} = \frac{T_s}{T}\sigma_s^4$$

This is the contribution of the noise-free signal. Now, let us evaluate the contribution of the noise. For simplicity, let us consider the case of a receiver filter with flat frequency response in [-*W*/2, +*W*/2] and zero outside. In that case, using equation (4), we can show that:

$$m_\rho^{(n)} = \frac{1}{TW}\sigma_n^4$$

Hence (from equation 6), the standard deviation of the fluctuations is:

$$\sigma_\rho^{(n)} = \sqrt{\frac{2}{M}}\frac{1}{TW}\sigma_n^4$$

Then:

$$\frac{m_\rho^{(s)}}{\sigma_\rho^{(n)}} = \sqrt{\frac{M}{2}}T_s W \frac{\sigma_s^4}{\sigma_n^4}$$

This is the ratio between the mean value of the peaks created by the DS-SS signal (if there is one such signal hidden in the noise), and the standard deviation of the fluctuations due to the noise. The reader must not be surprised to see a ratio between a mean and a standard deviation: indeed, it is this ratio which is significant to determine if the peaks due to the DS-SS signal may be hidden by the fluctuations due to the noise (see the display in the next section).

However, this formula is not easy to use as such because σ_s and σ_n depend on *W*. Here, to avoid going too deep into mathematical details, we will just give the expression corresponding to the optimal value of the receiver filter bandwidth. The bandwidth of the optimal receiver filter is approximately 1/Tc. In that case, we have:

$$\frac{m_\rho^{(s)}}{\sigma_\rho^{(n)}} = \sqrt{\frac{M}{2}}L\frac{\sigma_s^4}{\sigma_n^4} \qquad (7)$$

Let us consider the following example:

$\frac{\sigma_s^2}{\sigma_n^2} = 0.03$ (input SNR = $-15dB$)

M=800 (number of analysis windows)

L=255 (length of the pseudo-random sequence)

In that case, the output SNR is 5.1 (that is +7 dB).

Equation (7) shows that, from a theoretical point of view, the detector performances can be increased without limits, just by increasing the number of windows *M*. However, on a practical point of view, we must take into account the fact that computation time is approximately proportional to *M*, hence the value of *M* cannot be increased without limits: it depends on the available computation power, and it depends also on the time allocated for detection.

Equation (7) also shows that when the transmitter uses short spreading sequences (low value of L), the DS-SS signal is more difficult to detect. However, this is not really a problem, because in that case the DS-SS signal cannot be far below the noise level (otherwise, even the receiver which knows the sequence could not retrieve the symbols: indeed, when L is low, the correlation gain is low).

VI. Experimental Results

Figure 1 shows an example of detector output. The horizontal axis represents τ (in μs). The curve represents $\rho(\tau)$ (i.e. the estimated fluctuations of the autocorrelation estimator). The horizontal lines represent the theoretical mean fluctuation and the theoretical upper bound.

We can see that there are peaks above the theoretical upper bound. Furthermore, these peaks are located on multiples of a given period. This means that a DS-SS signal is hidden in the noise.

Here, there was indeed a DS-SS signal hidden in the noise. The parameters were: input SNR = $-10dB$, L = 31, and M = 255. Computation time on a PC with a 266 MHz processor: 5 seconds (with a non-optimized C program).

Furthermore, the location of the peaks provides an estimation of the symbol period.

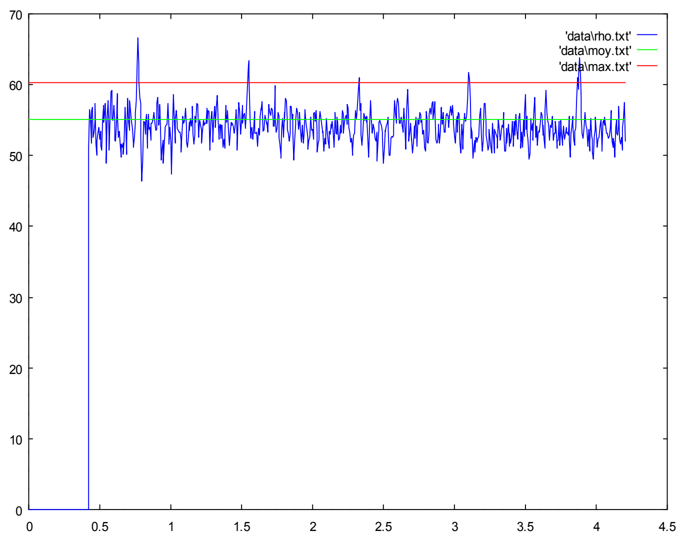

Fig. 1: Example of fluctuations curve.

VII. Conclusion

DS-SS signals are difficult to detect. Indeed, they are often transmitted below the noise level. Furthermore, a DS-SS signal is especially built to be similar to a noise, in order to have a low probability of interception. The autocorrelation of a spread spectrum signal is close to a Dirac function, as well as the autocorrelation of a white noise (this is due to the pseudo-random sequence).

The originality of the detector proposed in the paper is that it is based on the fluctuations of autocorrelation estimators, instead than on the autocorrelation itself. Although the autocorrelation of a DS-SS signal is similar to the autocorrelation of a noise, we have shown that the fluctuations of estimators are totally different.

The proposed method is interesting in any non-cooperative context such as spectrum surveillance. Furthermore, it is also able to estimate the symbol period of the DS-SS signal.

References

[1] C.E. Cook, H.S. Marsh, "An introduction to spread spectrum", *IEEE Communications Magazine*, March 1983, pp. 8-16.

[2] K.S. Kim et al., "Analysis of quasi-ML multiuser detection of DS/CDMA systems in asynchronous channels", *IEEE Trans. on Communications*, vol 47, No. 12, December 1999

[3] D.T. Magill, F. D. Natali, G. P. Edwards, "Spread-Spectrum Technology for Commercial Applications", Proceedings of the IEEE, Vol. 82, No. 4, April 1994, pp. 572- 584

[4] R.L. Picholtz, D.L. Schilling, L.B. Milstein, "Theory of Spread-Spectrum Communications - A Tutorial", IEEE Trans. on Communications, Vol. 30, No. 5, May 1982, pp. 855- 884.

[5] John G. Proakis, "Digital communications", Third Edition, Mac Graw Hill International Editions, 1995.

[6] Dilip V. Sarwate, Michael B. Pursley, "Crosscorrelation Properties of Pseudorandom and Related Sequences", Proceedings of the IEEE, Vol. 68, No. 5, May 1980, pp. 593-619.

[7] R.A. Scholtz, "The origins of spread spectrum communications", IEEE Trans. on Communications, vol 30, No. 5, May 1982