Performance of a new Chaos-based Communication Scheme: the Reduced-Delay-Masked-DCSK

Rhouma Rhouma and Safya Belghith
Unit 6'tel , Sup'com Tunis, Tunisia
Ecole Nationale d'Ingnieurs Tunis, tunisia
e-mail: rhoouma@yahoo.fr safya.belghith@enit.rnu.tn

Abstract— *Using chaotic signals in spread-spectrum communications has a few clear advantages over traditional approaches. Chaotic signals are non-periodic, wideband, and more difficult to predict, to reconstruct, and to characterize than periodic carriers. These properties of chaotic signals make it more difficult to intercept and decode the information modulated upon them. In this paper, we introduce modifications on DCSK to enhance the privacy by eliminating the similarity in the output samples by a chaotic mask, and faster by reducing the delay time. We analyze then the performance of the proposed modulation for different parameters and by comparison with other variants of DCSK.*

Keywords: DCSK, UWB, Chaos, Chaotic mask, security.

I. INTRODUCTION

The chaotic signal based UWB system [1] was proposed to satisfy the requirement of the IEEE 802.15.4a standard for low power consumption, low complexity, and low data rate communication. Many chaos-based communication schemes have been proposed and studied in recent years, including chaos masking [2, 3], chaotic switching or chaos-shift-keying (CSK) [4, 5], differential CSK (DCSK) [6] and frequency modulated DCSK (FM-DCSK) [7]. Among the digital communication techniques proposed, CSK and DCSK are the most widely studied [8, 9]. In DCSK, each bit duration is divided into two equal slots. In the first slot, a reference chaotic signal is sent. Dependent upon the symbol being sent, the reference signal is either repeated or multiplied by the factor "-1" and transmitted in the second slot.

However, some disadvantages in the modulation DCSK make it less secure than other chaos-based communications schemes: there are similarity between data and reference, so the information and the bit rate can be guessed easily. In [10], Francis *et al* have proposed a method to eliminate this similarity, which is the "permutation-based DCSK" or "P-DCSK". Another drawback of the DCSK system is the difficulty of implementing long delay line. To deal with that, Lee *et al* have proposed in [11] a method to reduce the delay by dividing a bit interval into S slots and the method is called the "reduced-delay DCSK".

In this paper, we propose to keep on the modification in [11], that is to reduce the delay, and mask the output with a chaotic signal to eliminate the similarity. We call this method : the "Reduced-Delay-Masked DCSK" (RDM-DCSK).

II. THE DIFFERENTIAL CHAOS SHIFT KEYING DCSK

In Differential Chaos Shift Key (DCSK) one half of the transmitted symbol is a reference chaotic waveform, and the second half of the transmitted symbol is the modulated reference, as illustrated in Figure 1. The advantage in using differential chaos shift keying is that in the case of severe channel distortions, both the reference portion and the message portion of the transmitted symbol undergo the same kind of distortion. Also, coherent detectors require synchronization between transmitter and receiver, and synchronization is susceptible to noise. The use of DCSK does not require the receiver to synchronize to the transmitter.

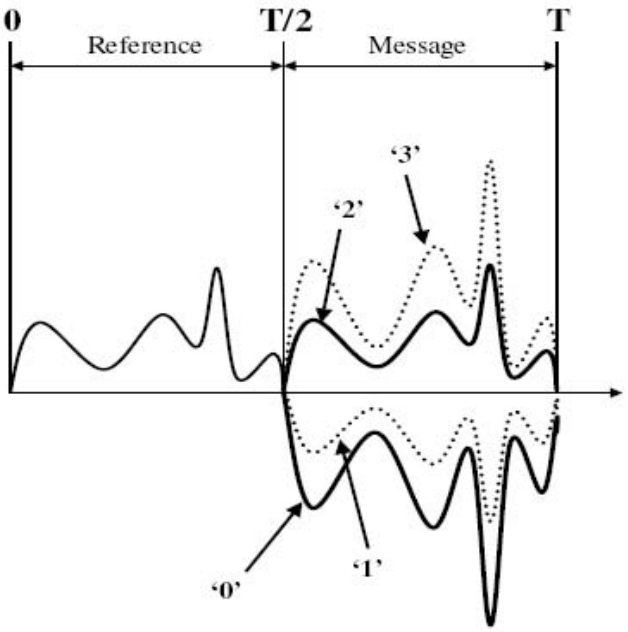

Fig. 1. Differential Chaotic Shift Key. The first half of the symbol is used as a reference, while the second half is a modulated version of the reference.

In the case of transmitting a binary information ± 1, the operation of the DCSK modulator is illustrated in Figure 2. For every bit of information, the transmitter outputs a chaotic sequence x_i of length M followed by the same sequence $b_l = \pm 1$ multiplied by the information signal, where l is the bit counter (see Figure 3). Thus, the transmitted signal for a single bit is given by:

$$s_i = \begin{cases} x_i, & if \ \ 0 < i < M \\ b_l x_{i-M}, & if \ \ M < i < 2M \end{cases} \qquad (1)$$

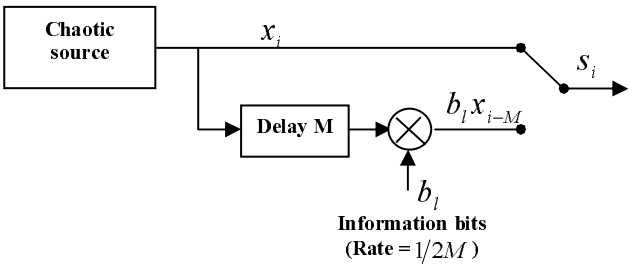

Fig. 2. Signal structure for the DCSK.

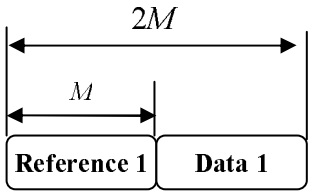

Fig. 3. DCSK operation in the transmitter.

In order to recover the information, the received signal r_i is multiplied by the received signal delayed by M,r_{i-M}. The product is then averaged over the spreading sequence length M.

the output of the correlator can be written as $S = \sum_{i=M}^{2M} r_i r_{i-M}$.

The operation of the DCSK demodulator is illustrated in Figure 4.

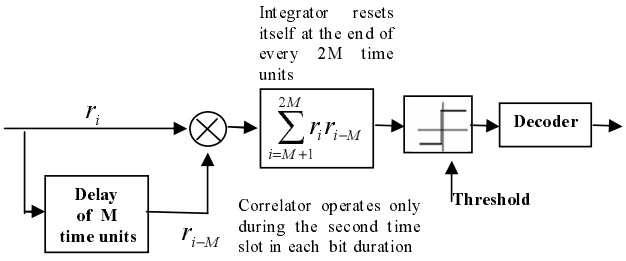

Fig. 4. DCSK operation in the receiver.

The correlation is made only in the second time slot in each bit duration. If the result of correlation is positive then the bit transmitted was 1, if not, the bit was -1. So, the entire binary message can be deduced from the correlation signal. Let us make the standard assumptions that the received signal r_i is given by $r_i = s_i + \xi_i$, where ξ is a stationary random process with $E(\xi_i) = 0$, that ξ_i and ξ_j are statistically independent for any $i \neq j$. And x_i and ξ_j are statistically independent. Then the correlator output can be written as:

$$S = \sum_{i=M+1}^{2M} (s_i + \xi_i)(s_{i-M} + \xi_{i-M})$$

$$= \sum_{i=M+1}^{2M} (b_l x_{i-M} + \xi_i)(x_{i-M} + \xi_{i-M})$$

$$= b_l \sum_{i=1}^{M} x_i^2 + \sum_{i=M+1}^{2M} (x_{i-M}(\xi_i + b_l \xi_{i-M}) + \xi_i \xi_{i-M}) \quad (2)$$

Let's note U the quantity $b_l \sum_{i=1}^{M} x_i^2$, and V the quantity $\sum_{i=M+1}^{2M} (x_{i-M}(\xi_i + b_l \xi_{i-M}) + \xi_i \xi_{i-M})$. U represent the correlation of the useful signal x_i, and the quantity V is a zero-mean random quantity:

$$E(V) = \sum_{i=M+1}^{2M} E(x_{i-M}\xi_i) + b_l \sum_{i=M+1}^{2M} E(x_{i-M}\xi_{i-M}) + \sum_{i=M+1}^{2M} E(\xi_i \xi_{i-M})$$

if ξ_i is a stationary random process, so ξ_{i-M} is also, and the terms $x_{i-M}\xi_i$, $x_{i-M}\xi_{i-M}$ and $\xi_i\xi_{i-M}$ are also stationary random process. So $E(V) = 0$.

III. PROPOSED SCHEME : THE REDUCED-DELAY MASKED-DCSK

A. Improve the speed of DCSK

To solve the long delay line in the conventional DCSK, we introduce the "reduced-delay DCSK", which uses shorter delay line. We divide one bit duration T_b by S slots. Assume that M is an even number, and if M is 2, it is reduced to the conventional DCSK. With the reduced-delay DCSK, delay line can reduce to $\frac{2M}{S}$ samples. The reduced-delay DCSK transmitted signal for $S = 4$ is shown in Figure 5. In other words, the delay length reduces to $\frac{M}{2}$ samples.

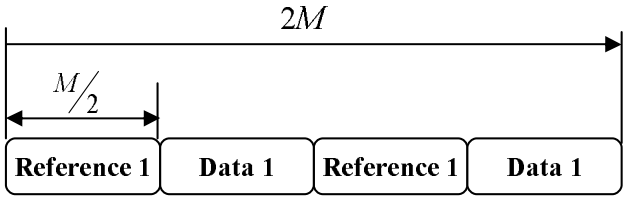

Fig. 5. Signal structure for the reduced-delay DCSK for $S = 4$.

$$s_k = \begin{cases} x_k & reference\,signal \\ a_l x_{k+\frac{2M}{S}} & data\,signal \end{cases} \quad (3)$$

where

$$k \in \{2M(l-1)+1, 2M(l-1)+2, \ldots, 2M(l-1)+(\frac{2M}{S})\}$$

$2M$: the total number of samples consisting of one bit.
a_l : l^{th} transmitted symbol $\{\pm 1\}$.
$\frac{2M}{S}$: delay length (S : even).

The reduced-delay DCSK receiver performs multiplication of received signal with $\frac{2M}{S}$ delayed signal.

B. Enhance the privacy of DCSK

The output s_k is composed of similar signals (data and reference) so, to destroy this similarity between the data and reference samples in a reduced-delay DCSK system, we propose to make transformation in the output of the DCSK signal. We mask the output by a chaotic sequence $\{c_k\}$ generated from the map described by Eq. (4), with α as parameter and c_0 is the initial condition:

$$c_{k+1} = \begin{cases} \frac{2c_k+1-\alpha}{1+\alpha} & for\ -1 \le c_k \le \alpha \\ \frac{-2c_k+1+\alpha}{1-\alpha} & for\ \alpha \le c_k \le 1 \end{cases} \quad (4)$$

At the receiver, the same chaotic sequence $\{c_k\}$ is generated with the same couple (c_0, α). the modulated signal is obtained by subtracting $\{c_k\}$ from the received signal. The output of the substracter r_l is then passed to a reduced-delay DCSK demodulator to retrieve the information signal.

C. Diagram of the RDM-DCSK

The diagram of the proposed method RDM-DCSK (reduced-delay masked-DCSK) is presented in Figure 6. We give now the equations that describe the whole system.

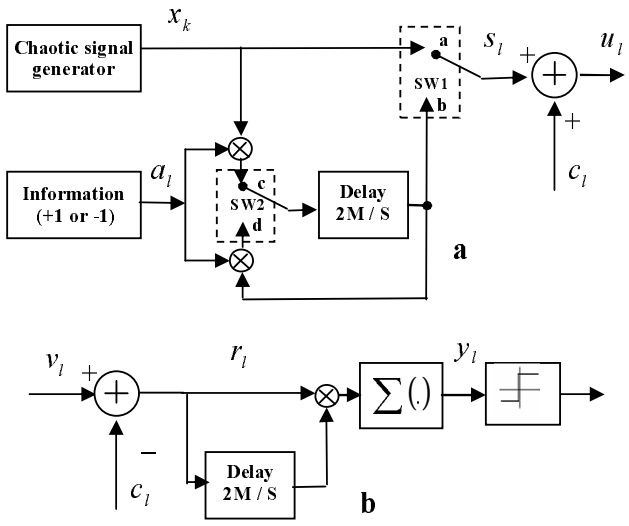

Fig. 6. The block diagram of the proposed DCSK alternative. (a) Modulator, (b) Demodulator

To simplify the notations, we define the chaotic sequence x_l used to modulate the signal in DCSK form:

$$x_l = (x_{2M(l-1)+1}, x_{2M(l-1)+2}, \ldots, x_{2M(l-1)+2M/S}) \quad (5)$$

The additive Gaussian noise:

$$\Psi_n = (\xi_{Mn+1}, \xi_{Mn+2}, \ldots, \xi_{Mn+2M/S}) \quad (6)$$

The transmitted signal before the mask operation:

$$s_l = (s_{2M(l-1)+1}, s_{2M(l-1)+2}, \ldots, s_{2Ml})$$

The transmitted signal :

If we admit that $S = 4$, then, during the l^{th} symbol duration, the transmitted signal block, s_l, can be denoted by :

$$s_l = (x_l\ a_l x_l\ x_l\ a_l x_l) \quad (7)$$

The chaotic sequence c_l used to mask each l block of the modulated signal x_l

$$c_l = (c_{2M(l-1)+1}, c_{2M(l-1)+2}, \ldots, c_{2M(l-1)+2Ml}) \quad (8)$$

The masked signal u_l :

$$u_l = s_l + c_l \quad (9)$$

The transmitted signal with noise:

$$v_l = u_l + (\Psi_{2l-2}\ \Psi_{2l-\frac{3}{2}}\ \Psi_{2l-1}\ \Psi_{2l-\frac{1}{2}}) \quad (10)$$

Whereas the received signal block, r_l, is now represented :

$$r_l = v_l - c_l \quad (11)$$

IV. PERFORMANCE ANALYSIS

A. DCSK Performance

The output of the correlator for DCSK[12] is given by Eq. (2). It can be written in the form:

$$S = b_l A + b_l \zeta + \eta$$

avec $A > 0$

$$A = \sum_{i=1}^{M} x_i^2,\ \ \zeta = \sum_{i=1}^{M} x_i^2 - A$$

$$\eta = \sum_{i=1}^{M} x_i \xi_{i+M} + b_l \sum_{i=1}^{M} x_i \xi_i + \sum_{i=1}^{M} \xi_i \xi_{i+M}$$

In DCSK, $A = \frac{E_b}{2}$, we shall require that x_i is stationary, and that the correlation between x_i and x_{i+k} decay quickly as $|k|$ increases (which is standard for chaotic systems). We assume that M is much larger than the characteristic correlation decay times. Under these assumptions, as M increases, the distributions of ζ and η approach Gaussian distributions. So, it is sufficient to compute the variance of $\eta + \zeta$ to fully characterize the distribution of the interference. The cross-correlations of ζ and η is zero. Therefore, $\sigma^2_{\eta+\zeta} = \sigma^2_\eta + \sigma^2_\zeta$.

$$\sigma^2_\eta = E_b \frac{N_0}{2} + \frac{N_0^2}{4} M$$

Authors in [12] have used the $symmetric\, tent\, map$:
$x_{i+1} = 1 - 2|x_i|$,
and find:

$$\sigma^2_\zeta = \frac{E_b^2}{5M}$$

so

$$\sigma^2 = \sigma^2_\eta + \sigma^2_\zeta = E_b \frac{N_0}{2} + \frac{E_b^2}{5M} + \frac{N_0^2}{4} M$$

The expression of BER will be :

$$BER = P((\zeta + \eta) > A) = \frac{1}{2} erfc(\frac{A}{\sqrt{2}\sigma}) \quad (12)$$

with

$$erfc(x) = \frac{2}{\sqrt{\pi}} \int_x^{\infty} exp(-t^2)dt.$$

After evaluating Eq. (12), the expression of BER[12] will be:

$$BER = \frac{1}{2} erfc(\sqrt{\frac{E_b}{4N_0}(1 + \frac{2}{5M}\frac{E_b}{N_0} + \frac{N_0}{2E_b}M)^{-1}}) \quad (13)$$

In Figure 7, we present the results of numerical simulations with different values of $M(M = 4, M = 8, M = 16)$. Channel noise ξ_i was taken to be Gaussian. The bit error rate for conventional binary phase-shift keying (BPSK) is also shown for comparison.

The BER of BPSK is given by :

$$BER_{BPSK} = \frac{1}{2} erfc(\sqrt{\frac{E_b}{N_0}}) \quad (14)$$

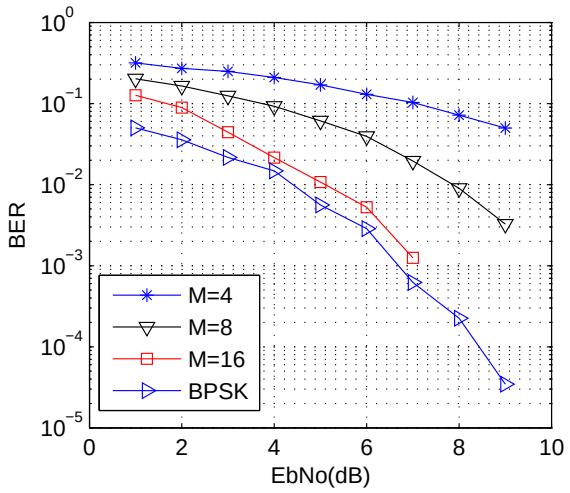

Fig. 7. Performance of DCSK for differents values of M.

B. Performance of the proposed method

The output of the correlator in RDM-DCSK is :

$$y_l = \sum_{2M(l-1)+1}^{2M(l-1)+2M/S} (x_k + c_k + \xi_k)(a_l x_{k+2M/S} + c_{k+2M/S} + \xi_{k+2M/S}) \quad (15)$$

To analyze performance of the RDM-DCSK on AWGN channel, assume that correlator output signal y_l follows the Gaussian distribution. Calculation of the bit error rate requires mean and variance of each slot. Equation (16) shows the mean of y_l :

$$E[y_l] = a_l \frac{2M}{S} E[x_k^2] = a_l A. \quad (16)$$

The chaotic signal from the reference signal and the data signal is the same, hence $x_k = x_{k+2M/S}$. Also x_k, ξ_k and c_k are uncorrelated each other. We require also to assume that $E(x_k) = E(c_k) = 0$.

Assuming that c_k is generated from the same map of x_k, then $E[c_k^2] = E[x_k^2]$. We shall require also that the correlations between x_k and $x_{k+2M/S}$ decay quickly as $|2M/S|$ increases (which is standard for chaotic systems). By applying Eq. (15), the variance of y_l can be represented as Eq. (17) :

$$Var(y_l) = \frac{2M}{S}(Var[x_k^2] + 3E^2[x_k^2] + 4E[x_k^2]\frac{N_0}{2} + (\frac{N_0}{2})^2] = \sigma^2 \quad (17)$$

The error rate can be calculated using the mean and the variance of each slot. Equation (18) represents error rate for each slot.

$$P_s(e) = P(y_l \leq 0 | a_l = 1).P(a_l = 1) + P(y_l > 0 | a_l = -1).P(a_l = -1) = \frac{1}{2} erfc(\frac{A}{\sqrt{2}\sigma}) \quad (18)$$

Using the definition of bit energy $E_b = 2ME[x_k^2]$, equation (18) is simplified as follows :

$$= \frac{1}{2} erfc((\frac{S}{4M}\Psi + \frac{3S}{4M} + S(\frac{E_b}{N_0})^{-1} + \frac{SM}{4}(\frac{E_b}{N_0})^{-2})^{-\frac{1}{2}}) \quad (19)$$

with $\Psi = Var[x_i^2]/E^2[x_i^2]$.

Figure 8 shows the bit error rate performance for the four methods: the proposed scheme, the conventional DCSK, the "P-DCSK" called also the "permutation-based DCSK proposed in [10] and the "reduced-delay DCSK" proposed in [11]. It can be seen that the two methods: the proposed one and the reduced-delay DCSK are better in performance than the others.

Figure 9 shows the bit error rate performance of the RDM-DCSK as function of the slot S when M is 40, in the AWGN channel.

V. CONCLUSION

In this paper, we have proposed modifications to enhance the security of a base-band chaos-based spread-spectrum communication scheme: the DCSK. It involves the transmission of a segment of chaotic signal twice, first as a reference signal, and second, polarity-modulated by the information bit. First, we have eliminated the similarity in the output signal by masking it with a chaotic signal, so we increase the security of the DCSK modulation. Second, we have reduced the delay time which make the demodulation faster. Simulations show that the proposed method (RDM-DCSK) and the "reduced-delay DCSK" give slightly better results in performance compared to the conventional DCSK and the "P-DCSK".

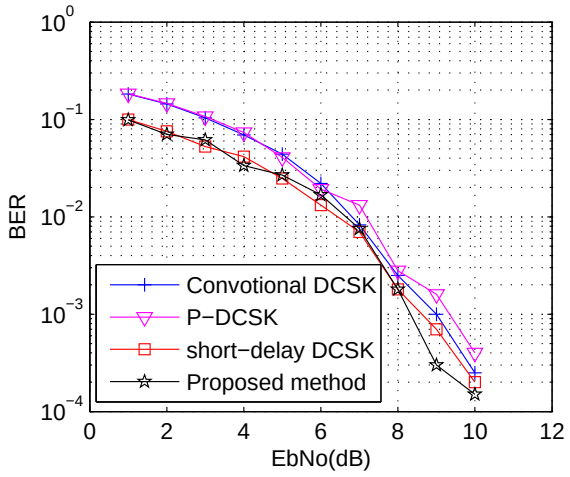

Fig. 8. Comparison of the performance of four DCSK variants: traditional DCSK,the reduced-delay DCSK, the P-DCSK and the proposed method (RDM-DCSK).

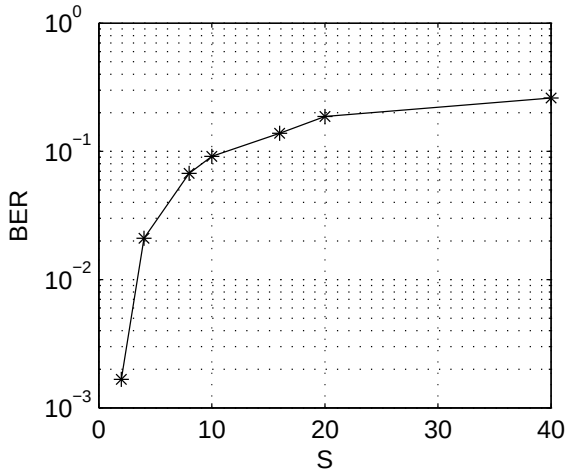

Fig. 9. Performance of the proposed method (RDM-DCSK) as function of the parameter S.

REFERENCES

[1] Y. H. Kim, et. al. Chaotic UWB System, In *IEEE 802.15-05-0132-03-004a, Monterey, CA, USA, Mar. 2005*. Available: http://grouper.ieee.org/groups/802/15/pub/05/15-05- 0132-03-004 a-merged-proposal-chaotic-uwb-system- 802-15-4a.pdf

[2] L. Kocarev, K. S. Halle, K. Eckert, L. O. Chua, U. Parlitz. Experimental demonstration of secure communications via chaotic synchronization. In *Int. J. Bifurcat. Chaos*,vol. 2, no. 3, pp. 709–713. 1992.

[3] K. M. Cuomo, A. V. Oppenheim. Circuit implementation of synchronized chaos with applications to communications. In *Physics. Rev. Let.* , vol. 71, pp. 65–68. 1993.

[4] U. Parlitz, L. O. Chua, L. Kocarev, K. S. Halle, A. Shang.Transmission of digital signals by chaotic synchronization. In *Int. J. Bifurcat. Chaos*,vol. 2, pp. 973–977, 1992.

[5] H. Dedieu, M. P. Kennedy, M. Hasler. Chaos shift keying: Modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuit. In *IEEE. Trans. Circ. Syst. -Part II*,vol. 40, pp. 634–642, Oct. 1993.

[6] G. Kolumban, B. Vizvari,W. Schwarz, A. Abel. Differential chaos shift keying: A robust coding for chaos communications. In *Proc., 4th Int. Workshop on Nonlinear Dynamics of Electronics Systems, (NDES'96), Seville, Spain, June 1996, pp. 87–92.*

[7] G. Kolumban, G. Kis, M. P. Kennedy, Z. Jako. FM-DCSK: A new and robust solution to chaos communications. In *Proc. Int. Symp. Nonlinear Theory and Its Applications (NOLTA'97) Hawaiian Village, HI*, 1997, pp. 117–120.

[8] G. Kolumban, G. Kis, Z. Jako, and M. P. Kennedy. A robust modulation scheme for chaotic communications. In *IEICE Trans. Fund.*, vol. E81-A, pp. 1798–1802, 1998.

[9] T. Schimming and M. Hasler. Optimal detection of differential chaos shift keying. In *IEEE. Trans. Circ. Syst. -Part I*, vol. 47, pp. 1712–1719, Dec. 2000.

[10] Francis C. M. Lau, Kai Y. Cheong, Chi K. Tse. Permutation-Based DCSK and Multiple-Access DCSK Systems. In *IEEE. Trans. Circ. Syst. -Part I*, vol. 50, no. 6,pp. 733–742, JUNE 2003.

[11] K. Lee, J. Son, J. Kim, Y. Kim, H. Park. Performance analysis of the reduced-delay DCSK UWB System. In *The 21st International Technical Conference on Circ. Syst. Comput. Comm.*, ISBN 974-94418-9-3, 2006, ECTI,pp. 137–140.

[12] M. Sushchik, Lev S. Tsimring, A. R. Volkovskii. Performance Analysis of Correlation-Based Communication Schemes Utilizing Chaos. In *IEEE. Trans. Circ. Syst. -Part I:Fundamental Theory and Applications.*, VOL. 47, NO. 12, DECEMBER 2000.