2004 International Symposium on Nonlinear
Theory and its Applications (NOLTA2004)
Fukuoka, Japan, Nov. 29 - Dec. 3, 2004

Exact Bit Error Rates of Multi-user Differential Chaos-Shift-Keying Communication Systems

Ji Yao and Anthony J. Lawrance

School of Mathematics, The University of Birmingham, Birmingham B15 2TT, United Kingdom
Department of Statistics, The University of Warwick, Coventry, Warwickshire CV4 7AL, United Kingdom
Email: yaoji@maths.bham.ac.uk, A.J.Lawrance@bham.ac.uk

Abstract–Theory giving the nearly exact bit error rates (BER) of multi-user chaos-shift-keying digital communication systems is derived analytically in the differential non-coherent case. Accurate approximation and numerical integration are then used to give the required results; these are demonstrated to conform with a pure-simulation study and thus inductively verify their correctness. A condition is deduced for the BER to be independent of the mix of transmitted bit types. The modulation scheme provides a possible choice for multi-access communication.

1. Introduction

Chaos-based communication has attracted intensive research interest over recent years, much dealing with chaos-shift-keying systems for single users. The wideband property of many chaotic wave forms indicates that a similar approach is particularly suitable for multi-access schemes but for these the theory is less developed. In this paper, focus is therefore on the performance analysis of multi-user differential-chaos-shift-keying (DCSK) digital communication systems with correlation decoding, following on from the corresponding single-user systems [1]. The differential, alternatively called non-coherent, aspect makes the systems realistic without problematic chaotic synchronization.

There have been some DCSK multi-access schemes considered in the previous publications [2]-[5]. The general advantage of DCSK schemes over the corresponding coherent schemes is the reduction by one-half of channel resources, and therefore the doubling of system efficiency. Of course, the performance of the system is thereby reduced. However, due to the complication of the dynamics of chaotic sequences, performance analysis of such systems is usually based on applying the Central Limit Theorem (CLT) to dependent variables, with its consequent slow convergence behaviour. This paper demonstrates the advantages of knowing the *exact* performance of such systems.

2. Multi-user DCSK Communication Systems

In this section, general configurations of multi-user differential-chaos-shift-keying (DCSK) communication systems are described. Because there are several possible conventional multi-access schemes available to implement this system, a relatively abstract model is considered. The block diagram of this model is given in Fig. 1.

2.1. The DCSK Modulation Scheme

Assume there are L users within the multi-user DCSK system. Analysis is focused on the transmission of one bit for each user, i.e. b_l for the l^{th} user, over the same time duration.

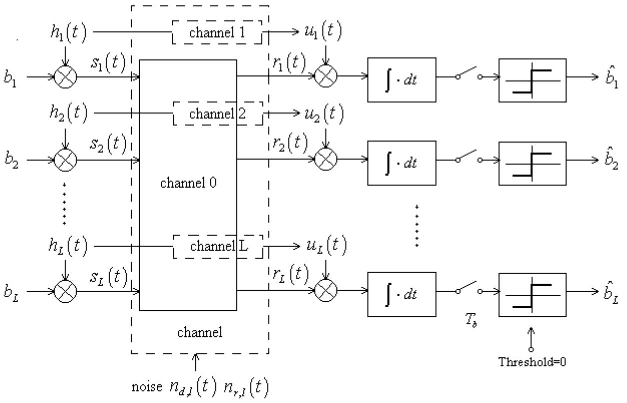

Fig. 1. Block diagram of multi-user DCSK communication system.

In a single-user DCSK communication system, a typical bit uses two time slots. In the first slot (the reference slot) a *reference sample* is transmitted and in the second slot (the data slot) a *data sample* is transmitted by modulating the reference sample with the information bit. In a multi-user system, it is possible to transmit the data samples of all users through the same channel, however, in order to achieve an acceptable performance, the reference samples no longer share the same channel [2]-[5], as shown in Fig. 1. But this doesn't mean that a real channel have to be allocated to each to user to transmit the reference sample. Any multi-access technology can be applied here. For example, in the case of only one real channel available, the reference samples can be transmitted during different time slot and the data samples are transmitted in same time slot. The advantage og this scheme is that it apparently saves half time than the pure time-division system.

To transmit the bit information b_l , the reference sequence takes a segment $x_l = \left\{ x_{l,i} \middle| i = 0,1,2,...,N-1 \right\}$ of N successive values from a chaotic waveform $\{X_l\}$; N is termed the *spreading factor*. These segments are generated by a common chaotic map $\tau(\cdot)$ irrespective of the user, that is

$$x_{l,i+1} = \tau\left(x_{l,i}\right)\ i = 0,1,2,...,N-1 \text{ and } l = 1,2,...,L. \quad (1)$$

The chaotic sequence $\{X_l\}$ is assumed to have been started with a random initial value $x_{l,0}$ which is chosen from the natural invariant distribution $\rho(x)$ of the map. The mean of $\{X_l\}$ is denoted by μ and the variance by σ_X^2. As it is always possible to move the map to achieve $\mu = 0$ without changing the dynamical properties of the map, $\mu = 0$ is assumed throughout the paper.

The output of the chaotic signal generator used by the l th user, denoted by $h_l(t)$, is given by

$$h_l(t) = \sum_{i=0}^{N-1} x_{l,i} g_{T_c}\left(t - iT_c\right), \quad (2)$$

where T_c is the time interval between change of x_i, which is always a constant; $g_{T_c}(t)$ is a rectangular pulse of unit amplitude and width T_c, i.e.

$$g_{T_c}(t) = \begin{cases} 1, & 0 \le t < T_c \\ 0, & elsewhere \end{cases}.$$

In the reference slot, the chaos sequence is transmitted directly as the reference sample, i.e. the reference sample for the l th user is

$$h_l(t) = \sum_{i=0}^{N-1} x_{l,i} g_{T_c}\left(t - iT_c\right). \quad (3)$$

In the data slot, the information bit is modulated by $b_l h_l(t)$. To avoid the modulated values being out of range of the map, the domain of chaotic map $\tau(x)$ is assumed to be symmetric about its mean $\mu = 0$. Thus, denoted by $s_l(t)$, the transmitted data sample of the l th user is

$$s_l(t) = \sum_{i=0}^{N-1} \left(b_l x_{l,i}\right) g_{T_c}\left(t - iT_c\right). \quad (4)$$

2.2. Channel Model

An additive white Gaussian noise (AWGN) channel is considered in this paper. Although the reference sample and data sample may transmitted through different channels, it is assumed that the noise in the reference channel and data channel has the same two-sided power spectral density given by $S_n(f) = N_0/2$.

Let $n_{r,l}(t)$ be the AWGN to the reference sample of the l th user. For convenience, we replace $n_{r,l}(t)$ by an equivalent noise source $n'_{r,l}(t)$, given by

$$n'_{r,l}(t) = \sum_{i=0}^{\infty} \eta_{l,i} g_{T_c}\left(t - iT_c\right),$$

where $\eta_{l,i}$ $(i = 0,1,...,N-1)$ are modeled as Gaussian random variables with mean 0 and variance $\sigma_n^2 = N_0/(2T_c)$. Because the reference sample is transmitted through different channels for different users, as previously explained, the transmitted reference sample of the l th user is only contaminated by its own channel AWGN. So the received reference sample of the l th user, denoted by $u_l(t)$, is

$$u_l(t) = \sum_{i=0}^{N-1} \left(x_{l,i} + \eta_{l,i}\right) g_{T_c}\left(t - iT_c\right) \equiv \sum_{i=0}^{N-1} y_{l,i} g_{T_c}\left(t - iT_c\right). \quad (5)$$

where $y_{l,i} = x_{l,i} + \eta_{l,i}$.

In the data slot, let $n_{d,l}(t)$ be the AWGN contaminating the data sample of the l th user. Thus, as with the reference slot, we replace $n_{d,l}(t)$ by an equivalent noise source $n'_{d,l}(t)$, given by

$$n'_{d,l}(t) = \sum_{i=0}^{\infty} \varepsilon_{l,i} g_{T_c}\left(t - iT_c\right), \quad (6)$$

where $\varepsilon_{l,i}$ $(i = 0,1,...,N-1)$ are independent Gaussian random variables with zero mean and same variance σ_n^2.

The data samples of each user are transmitted through the same channel, and so each is corrupted by both AWGN and the transmitted waveforms of the other $L-1$ users, termed as *interference.* The received data sample the of the l th user, denoted by $r_l(t)$, is thus

$$r_l(t) = s_l(t) + \sum_{k=1,k\neq l}^{L} s_k(t) + n'_{d,l}(t) \equiv \sum_{i=0}^{N-1} z_{l,i} g_{T_c}\left(t - iT_c\right), (7)$$

where $z_{l,i} = b_l x_{l,i} + \sum_{k=1,k\neq l}^{L} b_k x_{k,i} + \varepsilon_{l,i}$. Note that the only difference in $r_l(t)$ for different users is the channel noise; the sum of data samples of all users is received by each user.

The signal-to-noise energy ratio (SNR) of the system is

$$E_b/N_0 \equiv \left(2NT_c\sigma_X^2\right)/N_0 = \left(N\sigma_X^2\right)/\sigma_n^2, \quad (8)$$

which is different from the coherent case.

2.3. Demodulation Scheme

With the commonly used correlation decoder, demodulation takes the form

$$C\left(r_l, u_l\right) = \int_0^{NT_c} r_l(t) u_l(t) dt, \quad (9)$$

which calculates the covariance between $r_l(t)$ and $u_l(t)$, and takes a sample over time NT_c to make the demodulation decision. By (5) and (7), (9) can be simplified as

$$C\left(r_l, u_l\right) = T_c \sum_{i=0}^{N-1} y_{l,i} z_{l,i} \equiv T_c C\left(y_l, z_l\right), \quad (10)$$

where $C\left(y_l, z_l\right)$ is the discrete covariance $\sum_{i=0}^{N-1} y_{l,i} z_{l,i}$. With the correlation decoder, the transmitted bit b_l is estimated as $\hat{b}_l$ by

$$\hat{b}_l = \begin{cases} +1 & if\ C(y_l, z_l) \geq 0 \\ -1 & if\ C(y_l, z_l) < 0 \end{cases}. \tag{11}$$

3. Exact Bit Error Rates

The *bit error rates* (BER) of the l th user are the probabilities that this user estimates a bit value as –1 given +1 is transmitted or that the user estimates a it value as +1 given that –1 was transmitted. So the overall BER of the l th user takes the form

$$\begin{aligned} BER_l &= P(b_l = +1) \cdot BER_l \big| (b_l = +1) \\ &\quad + P(b_l = -1) \cdot BER_l \big| (b_l = -1), \end{aligned} \tag{12}$$

in which, following (10) and (11) is

$$\begin{aligned} &BER_l \big| (b_l = +1) = P\left(\hat{b}_l = -1 \mid b_l = +1\right) \\ &= P\left[C(Y_l, Z_l) < 0 \mid b_l = +1\right] \\ &= P\left\{\sum_{i=0}^{N-1}\left\{\left[\tau^{(i)}(X_l) + \sum_{k=1,k\neq l}^{L} b_k \tau^{(i)}(X_k) + \varepsilon_{1,i}\right]\left[\tau^{(i)}(X_l) + \eta_{l,i}\right]\right\} < 0\right\} \end{aligned} \tag{13}$$

and $BER_l \big| (b_l = -1)$ has a similar expression. In (13) upper case letters are used to denote continuous random variables and b_k $(k = 2,3,...,L)$ are discrete random variables taking value –1 or +1. It is interesting to note that the two conditional probabilities of (13) are not trivially equal, but see Section 4. A two-stage approach [6] is used to calculate the BER.

3.1. Two-stage Exact Analysis (TSE) Approach

Consider the BER of the 1st user, as being typical, in this DCSK system. In stage I of dealing with channel noise, the spreading sequence of all users and the transmitted bits of all users except the demodulating user, are considered known; only the $\varepsilon_{1,i}$ and $\eta_{1,i}$ are random variables. Therefore, from (13), the BER of the 1st user conditional on $b_1 = +1$ is

$$\begin{aligned} &BER_1(L,N) \big| (b_1 = +1, x_1, x_2, ..., x_L, b_2, b_3, ..., b_L) \\ &= P\left\{\sum_{i=0}^{N-1}\left\{\left[\tau^{(i)}(x_1) + \sum_{k=2}^{L} b_k \tau^{(i)}(x_k) + \varepsilon_{1,i}\right]\left[\tau^{(i)}(x_1) + \eta_{1,i}\right]\right\} < 0\right\}. \end{aligned} \tag{14}$$

Let

$$Z_{1i} = \left(\varepsilon_{1,i}/\sigma_n + \eta_{1,i}/\sigma_n\right)\big/\sqrt{2} \tag{15}$$

and

$$Z_{2i} = \left(\varepsilon_{1,i}/\sigma_n - \eta_{1,i}/\sigma_n\right)\big/\sqrt{2}, \tag{16}$$

then Z_{1i} and Z_{2i} are independent standard Gaussian random variables because $\varepsilon_{1,i}$ and $\eta_{1,i}$ are independent. From (15) and (16), one gets

$$\varepsilon_{1,i} = \sigma_n (Z_{1i} + Z_{2i})\big/\sqrt{2} \tag{17}$$

and

$$\eta_{1,i} = \sigma_n (Z_{1i} - Z_{2i})\big/\sqrt{2}. \tag{18}$$

Further let

$$a_i = \frac{\sqrt{2}}{\sigma_n}\tau^{(i)}(x_1) \tag{19}$$

and

$$c_i = \frac{\sqrt{2}}{\sigma_n}\left[\tau^{(i)}(x_1) + \sum_{k=2}^{L} b_k \tau^{(i)}(x_k)\right]. \tag{20}$$

With these definitions (17), (18), (19) and (20), (14) becomes

$$\begin{aligned} &BER_1(L,N) \big| (b_1 = +1, x_1, x_2, ..., x_L, b_2, b_3, ..., b_L) \\ &= P\left\{\sum_{i=0}^{N-1}\left[Z_{1i}^2 - Z_{2i}^2 + (a_i + c_i)Z_{1i} + (a_i - c_i)Z_{2i} + a_i c_i\right] < 0\right\} \\ &= P\left\{\sum_{i=0}^{N-1}\left[\left(Z_{1i} + \frac{a_i + c_i}{2}\right)^2 - \left(Z_{2i} + \frac{c_i - a_i}{2}\right)^2\right] < 0\right\} \\ &= P\left\{\sum_{i=0}^{N-1}\left(Z_{1i} + \frac{a_i + c_i}{2}\right)^2 \Big/ \sum_{i=0}^{N-1}\left(Z_{2i} + \frac{c_i - a_i}{2}\right)^2 < 1\right\} \\ &= F_{DNCF}\left[1; N, N, \sum_{i=0}^{N-1}\left(\frac{a_i + c_i}{2}\right)^2, \sum_{i=0}^{N-1}\left(\frac{a_i - c_i}{2}\right)^2\right], \end{aligned} \tag{21}$$

where $F_{DNCF}(x; r_1, r_2, \lambda_1, \lambda_2)$ is the cumulative distribution function of the doubly non-central F-distribution with degrees of freedom r_1, r_2 and non-centrality parameters λ_1, λ_2. With (19), (20) and (21), the BER can be calculated if the chaos sequences and other users' transmitted bits are known.

Define the random variables

$$\lambda_1 = 2\sigma_n^2 \sum_{i=0}^{N-1}\left(\frac{a_i + c_i}{2}\right)^2 = \sum_{i=0}^{N-1}\left[2\tau^{(i)}(X_1) + \sum_{k=2}^{L} b_k \tau^{(i)}(X_k)\right]^2,$$

and

$$\lambda_2 = 2\sigma_n^2 \sum_{i=0}^{N-1}\left(\frac{a_i - c_i}{2}\right)^2 = \sum_{i=0}^{N-1}\left[\sum_{k=2}^{L} b_k \tau^{(i)}(X_k)\right]^2. \tag{22}$$

In stage II, dealing with dynamical properties of the chaotic map, the joint distribution of (λ_1, λ_2) is first assumed known exactly as $f_{(\lambda_1,\lambda_2)}(y,z)$; then the BER conditional on $b_1 = +1$ is

$$\begin{aligned} &BER_1(L,N) \big| (b_1 = +1) \\ &= \int_0^{+\infty}\int_0^{+\infty} F_{DNCF}\left(1; N, N, \frac{y}{2\sigma_n^2}, \frac{z}{2\sigma_n^2}\right) f_{(\lambda_1,\lambda_2)}(y,z)\,dydz\ . \end{aligned} \tag{23}$$

The BER conditional on $b_1 = -1$ can be calculated in a similar manner; it is easy to show that

$$\begin{aligned} &BER_1(L,N) \big| (b_1 = -1) \\ &= \int_0^{+\infty}\int_0^{+\infty} F_{DNCF}\left(1; N, N, \frac{y}{2\sigma_n^2}, \frac{z}{2\sigma_n^2}\right) f_{(\lambda_1',\lambda_2')}(y,z)\,dydz \end{aligned} \tag{24}$$

where $f_{(\lambda_1',\lambda_2')}(y,z)$ is the joint distribution of

$$\lambda_1' = \sum_{i=0}^{N-1}\left[-2\tau^{(i)}(X_1) + \sum_{k=2}^{L} b_k \tau^{(i)}(X_k)\right]^2 \tag{25}$$

and $$\lambda_2' = \sum_{i=0}^{N-1}\left[\sum_{k=2}^{L} b_k \tau^{(i)}\left(X_k\right)\right]^2 = \lambda_2 .$$

In theory, we now have the exact BER of the communication system, but the joint distributions of $\left(\lambda_1, \lambda_2\right)$ and $\left(\lambda_1', \lambda_2'\right)$ are difficult to calculate. So approximation may be necessary.

3.2. Approximation

Calculation of the double non-central F-distribution function is time-consuming. A quite satisfying approximation based on the central limit theorem is

$$F_{DNCF}\left(1; r, r, y, z\right) \approx \Phi\left(\frac{z-y}{2\sqrt{(r+y+z)}}\right). \qquad (26)$$

Another key and difficult problem is calculating the joint probability density function of $\left(\lambda_1, \lambda_2\right)$. There are several approaches to approximate this distribution. However, due to the complicated structure of $\left(\lambda_1, \lambda_2\right)$, few approaches provide accurate approximations. One of these is to approximate λ_2 with a χ^2-distribution due its structure as a sum of squares, and then approximate

$$\lambda_1 = \lambda_2 + \sum_{i=0}^{N-1}\left\{\left[2\tau^{(i)}\left(X_1\right)\right]^2 + 4\tau^{(i)}\left(X_1\right)\sum_{k=2}^{L} b_k \tau^{(i)}\left(X_k\right)\right\}$$

with a Gaussian distribution conditional on λ_2.

Another approach to calculate the exact BER by (23) is by *semi-simulation*, that is, to obtain the joint distribution of $\left(\lambda_1, \lambda_2\right)$ by simulation and then evaluate (23) by numerical integration. As the joint distribution of $\left(\lambda_1, \lambda_2\right)$ and does not depend on SNR, a very accurate but time-consuming simulation need only be done once for each value of N. This is the approach that will be exemplified in Section 5.

4. BER not dependent on transmitted bit mix

The results of the two-stage approach not only provide a BER calculation, but also allow a further important qualitative conclusion. As shown in (23) and (24), the conditional BERs are not necessarily equal. But when $\left(\lambda_1, \lambda_2\right)$ has exactly the same joint distribution as $\left(\lambda_1', \lambda_2'\right)$, the overall BER does not depend on the mix of transmitted bit values. If the chaotic map $\tau\left(\cdot\right)$ is an odd-symmetry map, and therefore has a natural invariant distribution symmetrical about zero, then the minus sign before $2\tau^{(i)}\left(X_1\right)$ in λ_1' of (25) can be absorbed into $\tau^{(i)}\left(X_1\right)$; for any initial value x_1 there is a $-x_1$. The symmetric invariant distribution then guarantees the equality. There is no requirement on the distribution of b_k, so $\left(\lambda_1, \lambda_2\right)$ always has the same joint distribution as $\left(\lambda_1', \lambda_2'\right)$. In other cases, including even-symmetry maps, the BER is dependent on the mix of transmitted bit values.

5. Simulation Results and Conclusions

Analytical BER results by (23), (33) and semi-simulation in the case of Bernoulli shift map spreading are compared with *pure-simulation* results. The Bernoulli shift map applied here is

$$\tau_1\left(x\right) = \begin{cases} 2x+1 & \mathit{if}\ -1 \le x < 0 \\ 2x-1 & \mathit{if}\ 0 \le x \le 1 \end{cases}.$$

For this map, the mean and the variance of its invariant distribution are $\mu = 0$ and $\sigma_X^2 = 1/3$, respectively. For a given E_b/N_0, σ_n^2 is $N\sigma_X^2/10^{\left[\left(E_b/N_0\right)/10\right]}$.

The analytical and simulated BERs are plotted against E_b/N_0 in Fig. 2 for fixed $L = 2,5$. In the pure-simulation, for every different L and N, 100,000 bits have been transmitted in the whole system. Fig. 2 shows that the nearly exact analytical BERs always provide excellent results compared with the pure-simulation BERs.

Fully analytical approaches, avoiding semi-simulation, will be published later in a more complete account of this work.

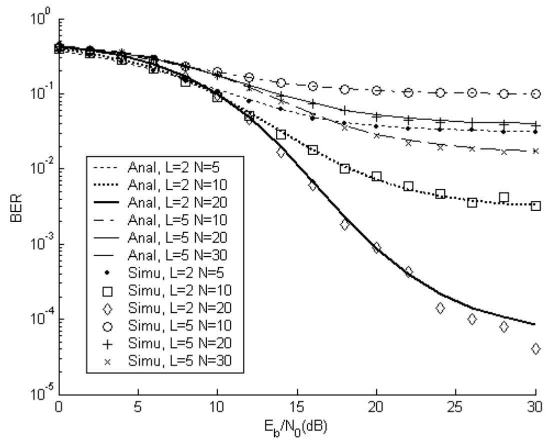

Fig. 2. Analytical and pure-simulation BERs plotted against E_b/N_0.

References

[1] G. Kolumban, B. Vizvazi, W. Schwarz, and A. Abel, "Differential chaos shift keying: A robust coding for chaos communication," in *Proc. 4th Int. Workshop of Nonlinear Dynamics of Electronics Systems,* Seville, Spain, June 1996, pp.87-92.

[2] W. M. Tam, F. C. M. Lau, and C. K. Tse, "Analysis of bit error rates for multiple access CSK and DCSK communication," IEEE Trans. Circuits Syst. I, vol. 50, pp. 702-707, May. 2003.

[3] F. C. M. Lau, M. M. Yip, C. K. Tse, and S. F. Hau, "A multiple access technique for differential chaos shift keying," in Proc. IEEE-ISCAS'2001, vol. III, Sydney, Australia, May 6-9, 2001, pp. 317-320.

[4] F. C. M. Lau, K. Y. Cheong, and C. K. Tse, "Permutation-based DCSK and multiple-access DCSK," IEEE Trans. Circuits Syst. I, vol. 50, pp. 733-742, June. 2003.

[5] W. M. Tam, F. C. M. Lau, and C. K. M. Tse, "An improved multiple access scheme for chaos-based digital communications using adaptive receivers," in Proc. IEEE-ISCAS'2004, vol. IV, Vancouver, Canada, May 23-26, 2004, pp. 605-608.

[6] J. Yao and A. J. Lawrance, "Bit error rate calculation for multi-user coherent chaos-shift-keying communication systems," IEICE Trans. Fundamentals, 2004, to appear.