synchronization scheme used. For simulation purposes, take $d(t) = 0.05$. As seen in Fig. 4, the decryption error $s(t) - s_d(t)$ is so significant that the recovered signal $s_d(t)$ is quite different from the message signal $s(t)$ over the time interval $[20,\ 20.6]$.

IV. Concluding Remarks

In this brief, a novel two-channel communication scheme using chaotic systems has been presented and illustrated in Lorenz system. A highly nonlinear encryption function, involving all chaotic states, is used and can be chosen to yield strong sensitivity to the encryption error and therefore guarantee higher security/privacy.

References

[1] G. Chen and X. Dong, *From Chaos to Order: Perspectives, Methodologies and Applications*. Singapore: World Scientific, 1998.

[2] N. J. Corron and D. W. Hahs, "A new approach to communications using chaotic signals," *IEEE Trans. Circuits Syst. I*, vol. 44, pp. 373–382, May 1997.

[3] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, "Synchronization of Lorenz-based chaotic circuits with applications to communications," *IEEE Trans. Circuits Syst. II*, vol. 40, pp. 626–633, Oct. 1993.

[4] G. Grassi and S. Mascolo, "A system theory approach for designing cryptosystems based on hyperchaos," *IEEE Trans. Circuits Syst. I*, vol. 46, pp. 1135–1138, Sept. 1999.

[5] C. Grebogi, Y.-C. Lai, and S. Hayes, "Control and applications of chaos," *Int. J. Bifurc. Chaos*, vol. 7, no. 10, pp. 2175–2197, 1997.

[6] S. Hayes, C. Grebogi, and E. Ott, "Communicating with chaos," *Phys. Rev. Lett.*, vol. 70, pp. 3031–3034, 1993.

[7] H. Huijberts, H. Nijmeijer, and R. Willems, "System identification in communication with chaotic systems," *IEEE Trans. Circuits Syst. I*, vol. 47, pp. 800–808, June 2000.

[8] T. Kapitaniak, *Chaos for Engineers: Theory, Applications, and Control*. New York: Springer-Verlag, 1998.

[9] Y. C. Lai and C. Grebogi, "Synchronization of chaotic trajectories using control," *Phys. Rev. E*, vol. 47, no. 4, pp. 2357–2360, 1993.

[10] T.-L. Liao and N.-S. Huang, "An observer-based approach for chaotic synchronization with applications to secure communications," *IEEE Trans. Circuits Syst. I*, vol. 46, pp. 1144–1150, Sept. 1999.

[11] H. Nijmeijer and I. Mareels, "An observer looks at synchronization," *IEEE Trans. Circuits Syst. I*, vol. 44, pp. 882–890, Oct. 1997.

[12] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.*, vol. 64, no. 8, pp. 821–824, 1990.

[13] K. Short, "Unmasking a modulated chaotic communication scheme," *Int. J. Bifurcation Chaos*, vol. 6, no. 2, pp. 367–375, 1996.

[14] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 2nd ed. Upper Saddle River, NJ: Prentice-Hall, 1999.

[15] C. W. Wu and L. O. Chua, "A simple way to synchronize chaotic systems with applications to secure communication systems," *Int. J. Bifurcation Chaos*, vol. 3, pp. 1619–1627, 1993.

[16] T. Yang and L. O. Chua, "Secure communication via chaotic parameter modulation," *IEEE Trans. Circuits Syst. I*, vol. 43, pp. 817–819, Sept. 1996.

[17] T. Yang, C. W. Wu, and L. O. Chua, "Cryptography based on chaotic systems," *IEEE Trans. Circuits Syst. I*, vol. 44, pp. 469–472, May 1997.

A Multiple-Access Technique for Differential Chaos-Shift Keying

F. C. M. Lau, M. M. Yip, C. K. Tse, and S. F. Hau

***Abstract*—A multiple-access technique for use with differential chaos shift keying is proposed and analyzed in this paper. A simple one-dimensional iterative map is used to generate the chaotic signals for all users and the average data rates for the users are identical. Bit-error rates are derived numerically for different number of users and computer simulations are performed to verify the results.**

***Index Terms*—Chaos communication, chaos shift keying, multiple access.**

I. Introduction

Due to their continuous broadband feature, chaotic signals are useful for encoding information in spread spectrum communications. When a narrowband signal is spread over a much wider bandwidth, the average power spectral density (psd) becomes lower. As a consequence, the signal psd becomes comparable with the background noise. Thus, without prior knowledge of the transmission system, it is not easy to detect the presence of the signal. Even if an unintended user detects the presence of the signal, in the case where coherent detection is required, it is very difficult to decode the data without prior knowledge of the encoding scheme. Recently, the application of chaotic signals in communications has received much attention. Chaotic masking [1] and chaotic modulation [2] spread analog signals by chaotic signals, while in chaos shift keying (CSK) [3]–[7] and predictive Poincaré control modulation [8], binary data are spread. The basic CSK maps different symbols to different chaotic attractors, which are produced by a dynamical system for different values of a bifurcation parameter or by completely different dynamical systems [5], [6]. A coherent correlation CSK receiver is then required at the receiving end to decode the signals. Noncoherent detection is also possible provided the signals generated by the different attractors have different attributes, such as mean of the absolute value, variance and standard deviation. The optimal decision level of the threshold detector will depend on the signal-to-noise ratio in general, although specific examples with noise-invariant threshold can be designed for CSK. As in other communication systems, its performance increases with the symbol energy or equivalently, the signal-to-noise ratio [9].

To overcome the threshold level shift problem, differential CSK (DCSK) has been proposed [3]–[6]. The advantage of DCSK over CSK is that the threshold level is always set at zero and is independent of the noise effect. It has been shown by Kis [7] that for a given noise level, the variance in the estimation of the parameters of chaotic sample functions can be reduced by increasing the length of the chaotic sample or the bandwidth of the carrier. Unfortunately, the variance in the estimation depends on both the characteristics of the chaotic carrier and the channel noise. In the differentially coherent DCSK system, the longer the bit duration or the wider bandwidth of the transmitted signal corrupts the noise performance [10], [11]. Optimum values for the bit duration have been investigated by Sushchik *et al.* [12].

Manuscript received June 8, 2000; revised January 20, 2001 and June 14, 2001. This work was supported in part by the Hong Kong Research Grants Council under the competitive earmarked research grant PolyU5124/01E and in part by the Hong Kong Polytechnic University under a research grant.This paper was recommended by Associate Editor G. Setti.

The authors are with the Department of Electronic and Information Engineering, Hong Kong Polytechnic University, Kowloon, Hong Kong, China (e-mail: encmlau@polyu.edu.hk).

Publisher Item Identifier S 1057-7122(02)00287-8.

In conventional communication systems, the allocated spectrum is shared by a number of users. Multiple-access techniques such as frequency-division multiple access (FDMA), time-division multiple access (TDMA) and code-division multiple access (CDMA) are commonly used. Similar to CDMA, CSK/DCSK spreads the spectrum of the data signal over a much larger bandwidth as compared to FDMA and TDMA. As a result, multiple access becomes an essential feature for practical implementation of the system. Furthermore, it is imperative that more users are included in the same bandwidth without causing excessive interference to one another.

A few multiple-access schemes have been proposed recently for chaos-based communication systems. In Carroll *et al.* [13], a method based on multiplexing chaotic signals has been proposed. Also, novel approaches for generating spreading codes using chaotic functions have been applied to conventional CDMA systems [14]–[16]. Furthermore, multiple access using DCSK has been introduced by Kolumbán *et al.* [17], [18] and the multiple-access capability of frequency-modulated DCSK (FM-DCSK) has been studied by Jáko *et al.* [19]. In both cases, two chaotic basis functions have been used as an illustration to transmit two streams of data at the same time in the same frequency band. The bit period is first divided into four time slots. For the first signal, the reference sample is divided into two parts which are sent in the first and third time slots. Similarly, the data sample is also divided into two parts which are sent in the second and fourth time slots. In order to obtain orthogonality between the transmitted signals, the order of transmission is changed for the second signal. Its reference sample is sent in the first two slots while the data sample is transmitted in the third and fourth slots. If the two chaotic basis functions are uncorrelated, the two signals will not affect each other when appropriate demodulation techniques are used. When the number of users increases, however, the number of time slots created in each bit duration would also increase, implying that switching between the reference and data samples will be performed more frequently within the same bit period. This will impose more stringent requirements on the switching circuits in both the transmitter and the receiver.

In this paper, an alternative multiple-access technique for use with DCSK (MA-DCSK) is proposed and analyzed. The proposed scheme gives equal average data rates of all users. As in a single-user DCSK system, each bit duration is always divided into two time slots for all users. Hence, the requirements on the switching circuits in the transmitter and the receiver will be similar compared with the single-user system. To minimize the correlation between signals, the frame periods and the arrangements of the reference and sample waveforms of all users are different. To evaluate the effectiveness of the scheme, a simple one-dimensional (1–D) iterative map is used to generate the chaotic signals for all users. As would be expected, the proposed scheme achieves similar error probabilities for all users and the error performance degrades as the number of users increases. However, we show that when the correlation between samples of the same/different chaotic signals is low, achieved by using a large spreading factor, a low bit-error rate (BER) can be achieved. Numerical BERs are also derived and compared with the simulation results. In Section II, the operation of DCSK is briefly reviewed. Section III describes the system model and the proposed multiple-access technique in detail. The statistical properties of the detected signal and a numerical analysis are discussed in Section IV. The BERs and the overall system capacity are presented in Section V. Finally, a comparison between the proposed scheme and the one by Jáko *et al.* [19] is given in Section VI.

II. Review of Differential Chaos-Shift Keying (DCSK)

DCSK was first proposed by Kolumbán *et al.* [3]. By using a chaotic carrier to spread the digital signal over a large bandwidth, the spread signal possesses some of the advantages of spread spectrum communications such as mitigation of multipath fading and low probability of detection. In DCSK, the signal can also be decoded using noncoherent detection. This section briefly reviews the basic operation of DCSK which will be helpful in understanding the multiple-access scheme that follows.

In DCSK, each bit duration is first divided into two equal time slots and every transmitted symbol is represented by a pair of chaotic signal samples sent in the two slots. The first sample serves as the reference (reference sample) while the second one carries the data (data sample) [3]–[6]. If a "+1" is to be transmitted, the data sample will be identical to the reference sample, and if a "−1" is to be transmitted, an inverted version of the reference sample will be used as the data sample. Assume the system is discrete and starts at $k = 0$. Let 2α be the spreading factor, defined as the number of time units occupied by a binary symbol, where α is an integer. Fig. 1 shows a typical transmitted waveform, denoted by $s(k)$, for a spreading factor of 10. At the receiving end, the reference sample and the corresponding data sample are correlated. Depending on whether the output is larger or smaller than the threshold zero, a "+1" or "−1" is decoded. Fig. 2 shows the block diagram of a DCSK correlator receiver and the output waveform of the correlator, which is sampled at multiples of 2α time units.

III. System Model and Multiple Access Technique

In a multiple-access system, to avoid excessive interference and hence mis-detection, the separation between the reference and data samples must be different for different users. Here, we propose a multiple-access scheme where the separation between the reference and data samples differs for different users, as illustrated in Fig. 3. For all users, the bit durations are first divided into 2 slots. For user i, $2i$ consecutive slots are collected to form a frame. Hence, the slot duration (half of bit duration) is the same for all users but the frame periods are different for different users. In each frame of user i, the first i slots (slots 1 to i) will be used to transmit i reference samples while the remaining i slots (slots $i+1$ to $2i$) are used to transmit i data samples. If a binary symbol "+1" is to be transmitted in slot $i+1$, the sample in slot 1 is repeated in slot $i+1$, otherwise, an inverted copy is sent. Similarly, in slot $i+2$, the same or inverted copy of the sample in slot 2 is sent, and so on. As a result, the reference and data samples of user i will be separated by i slots. Therefore, within a frame of length i bit periods (or $2i$ time slots), i bits of information will be sent. This corresponds to 1 bit per bit period. The data rates of all users are thus the same. However, a buffer is required to store the data before transmission. Fig. 4(a) shows the transmitter for the ith user whose chaotic series is denoted by $\{x_i(l)\}$. Fig. 5 depicts a typical transmitted waveform for user 3 with a spreading factor of 10.

Without loss of generality, consider the output of the ith transmitter at time k during the first frame. If it belongs to one of the reference samples, i.e.

$$k = \alpha(m_i - 1) + n \text{ for some } n \in \{1, 2, \ldots, \alpha\} \tag{1}$$

where $m_i \in \{1, 2, \ldots, i\}$ denotes the slot number, the output, denoted by $z_i(k)$, will equal to

$$z_i(k) = x_i(\alpha(m_i - 1) + n). \tag{2}$$

On the other hand, if the output lies in one of the data sample slots, i.e.

$$k = \alpha(m_i + i - 1) + n \text{ for some } n \in \{1, 2, \ldots, \alpha\} \tag{3}$$

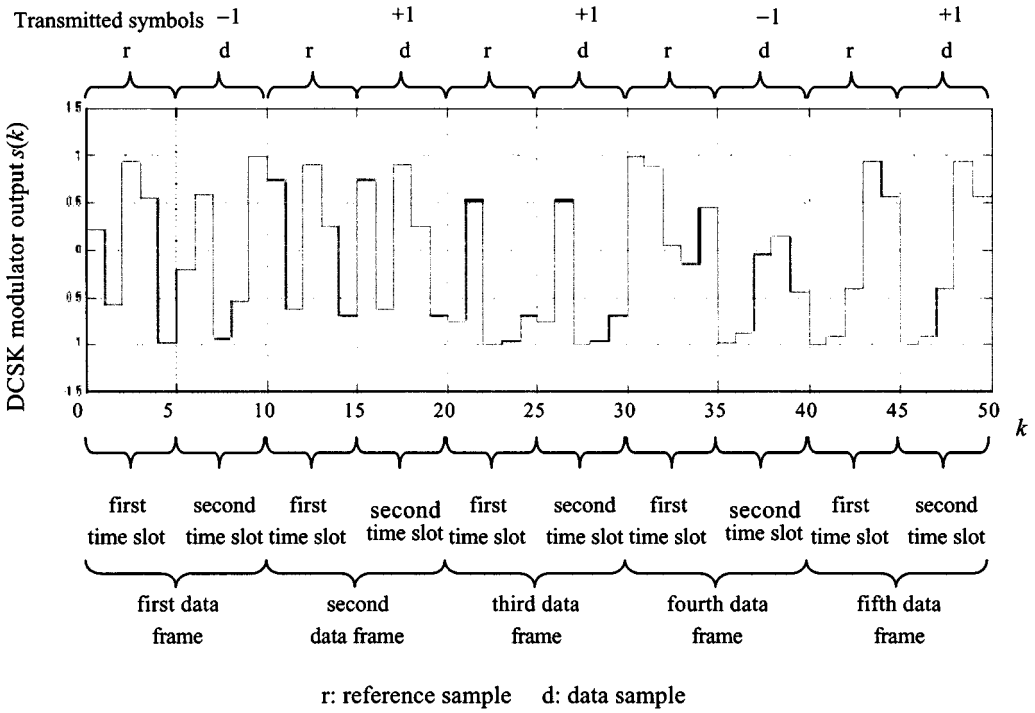

Fig. 1. A typical DCSK signal (spreading factor = 10).

where $m_i+i(m_i \in \{1, 2, \ldots, i\})$ denotes the slot number, the output becomes

$$z_i(k) = x_i(\alpha(m_i - 1) + n)b_i(m_i) \tag{4}$$

where $b_i(j) \in \{-1, +1\}$ denotes the jth transmitted symbol of user i.

Using the aforementioned notations, the output of transmitter i at time k equals

$$z_i(k) = \begin{cases} x_i(\alpha(m_i - 1) + n) \\ \quad \text{when } k = \alpha(m_i - 1) + n \\ x_i(\alpha(m_i - 1) + n)b_i(m_i) \\ \quad \text{when } k = \alpha(m_i + i - 1) + n \end{cases} \tag{5}$$

for some $m_i \in \{1, 2, \ldots, i\}$ and $n \in \{1, 2, \ldots, \alpha\}$. The overall transmitted signal of the whole system at time k, denoted by $z(k)$, is derived by summing the signals of all individual users, i.e.

$$z(k) = \sum_{i=1}^{N} z_i(k) \tag{6}$$

where N represents the number of users in the system.

Fig. 4(b) shows the receiver of user i in a multi-user DCSK system. At the receiving end, the time slots in the first half of each frame, i.e., first i slots, will correlate with those in the second half, i.e., $(i + 1)$th to $(2i)$th slots. During the same time, the correlator output is sampled every α time units before the correlator is reset. The output is then compared with the threshold zero to determine whether a "+1" or "−1" has been received. Fig. 6 depicts the correlator output and the decoded symbols of user 3 in a five-user system, assuming a spreading factor of 2000. If the correlation between different samples from the same user or samples from different users is low, a low BER is expected.

IV. Numerical Analysis

As derived in the previous section, the overall transmitted signal is given by $z(k) = \sum_{i=1}^{N} z_i(k)$. Ignoring the effect of noise and filters, the same signal will arrive at each receiver input. Without loss of generality, consider the m_ith transmitted symbol of user i during the first frame, $m_i \in \{1, 2, \ldots, i\}$. To recover the data, the received signal in the m_ith slot will correlate with that i slots later, i.e., the $(m_i + i)$th slot. The output of the correlator, denoted by O_i, is given by

$$O_i = \sum_{k=\alpha(m_i-1)+1}^{\alpha(m_i-1)+\alpha} z(k)z(k + \alpha i). \tag{7}$$

Substituting (6) in (7) gives

$$\begin{aligned} O_i &= \sum_{k=\alpha(m_i-1)+1}^{\alpha(m_i-1)+\alpha} \sum_{u=1}^{N} \sum_{v=1}^{N} z_u(k)z_v(k + \alpha i) \\ &= \sum_{u=1}^{N} \sum_{v=1}^{N} \sum_{k=\alpha(m_i-1)+1}^{\alpha(m_i-1)+\alpha} z_u(k)z_v(k + \alpha i) \end{aligned} \tag{8}$$

where $z_u(k)$ and $z_v(k)$ denote the signals of users u and v, respectively. For brevity, we define $X_{i,u,v}$ as

$$X_{i,u,v} = \sum_{k=\alpha(m_i-1)+1}^{\alpha(m_i-1)+\alpha} z_u(k)z_v(k + \alpha i). \tag{9}$$

Hence, O_i can be written as

$$O_i = \sum_{u=1}^{N} \sum_{v=1}^{N} X_{i,u,v}. \tag{10}$$

The mean of O_i, denoted by $\overline{O_i}$, is evaluated from

$$\begin{aligned} \overline{O_i} &= \overline{\sum_{u=1}^{N} \sum_{v=1}^{N} X_{i,u,v}} = \sum_{u=1}^{N} \sum_{v=1}^{N} \overline{X_{i,u,v}} \\ &= \overline{X_{i,i,i}} + \sum_{\substack{u=1 \\ u \neq i}}^{N} \overline{X_{i,u,u}} + \sum_{\substack{u=1 \\ u \neq v}}^{N} \sum_{v=1}^{N} \overline{X_{i,u,v}}. \end{aligned} \tag{11}$$

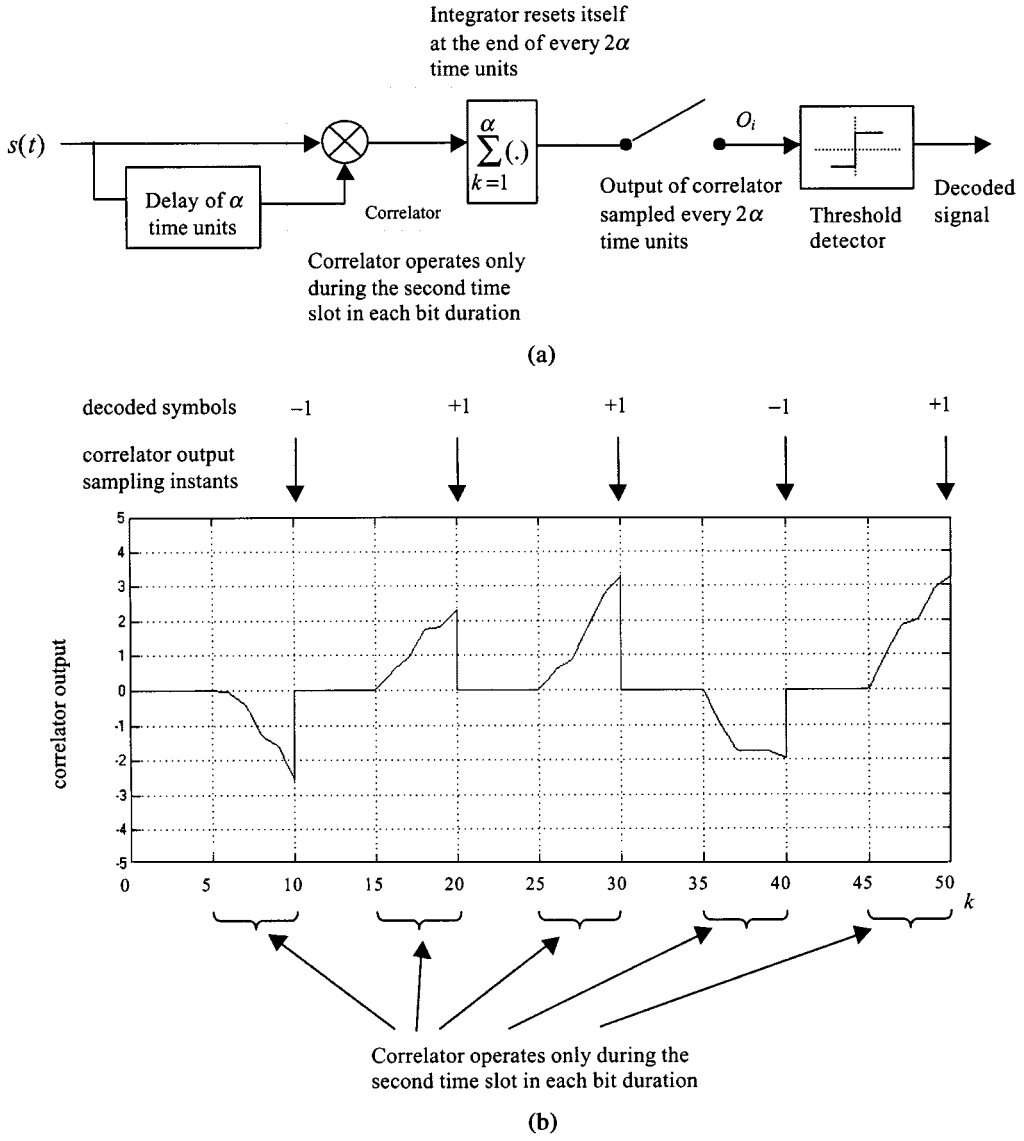

Fig. 2. (a) Block diagram of a DCSK correlator receiver. (b) Output of the correlator and the decoded symbols (spreading factor = 10).

Furthermore, if the $X_{i,u,v}$s are all uncorrelated normal random variables, O_i, being the sum of these variables, is also normal with variance given by

$$\begin{aligned}\mathrm{var}(O_i) &= \sum_{u=1}^{N}\sum_{v=1}^{N}\mathrm{var}(X_{i,u,v}) \\ &= \mathrm{var}(X_{i,i,i}) + \sum_{\substack{u=1\\u\neq i}}^{N}\mathrm{var}(X_{i,u,u}) + \sum_{\substack{u=1\\u\neq v}}^{N}\sum_{v=1}^{N}\mathrm{var}(X_{i,u,v})\end{aligned} \tag{12}$$

where $\mathrm{var}(Y)$ denotes the variance of Y [20], [21].

In the sequel, we assume that the map

$$x(l+1) = g(x(l)) = 4x^3(l) - 3x(l) \tag{13}$$

is used to generate the chaotic signals for all users but with different initial conditions. With this choice of $g(.)$, it can be shown that the probability density function (pdf) of $x(l)$ is symmetrical along the y-axis. As a result, the expected value of $x(l)$ is zero. The means and variances of the variables $X_{i,u,v}$s under three different cases (see Appendix) are derived by extensive computer simulations and the values are tabulated in Table I for spreading factors 200 and 2000.

Applying the central limit theorem [9] to each of the $X_{i,u,v}$s, the $X_{i,u,v}$s can be shown to be approximate normal with the approximation getting better with increasing α. Assume that all $X_{i,u,v}$s are uncorrelated random variables. Therefore, we can apply (11) and (12) to obtain, for $\alpha = 100$ and 1000

$$\overline{O_i} = \begin{cases} 0.5\alpha, & \text{“+1” is transmitted} \\ -0.5\alpha, & \text{“−1” is transmitted} \end{cases} \tag{14}$$

and

$$\mathrm{var}(O_i) = 0.125\alpha + 0.25\alpha(N^2 - 1). \tag{15}$$

Since the output of the correlator is approximate normal with mean $\overline{O_i}$ and variance $\mathrm{var}(O_i)$, the bit error rate (BER), denoted by BER, can be obtained by

$$\begin{aligned}\mathrm{BER} = {} & \mathrm{Prob}(O_i < 0 | \text{“+1” is transmitted})/2 \\ & + \mathrm{Prob}(O_i > 0 | \text{“−1” is transmitted})/2\end{aligned}$$

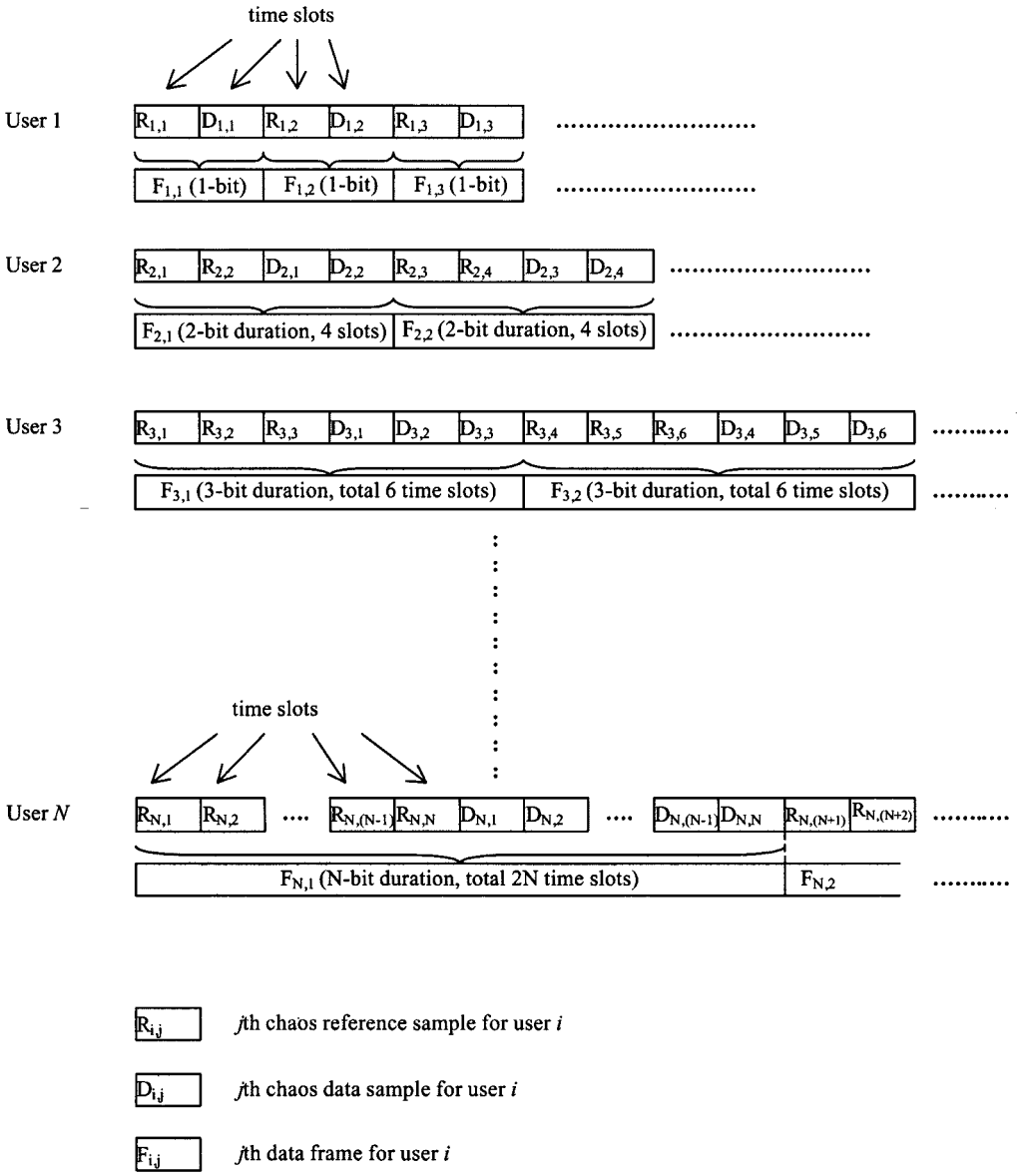

Fig. 3. Transmission scheme in a multiple-access differential chaos shift keying (MA-DCSK) system.

$$= \frac{1}{2}Q\left(\frac{0.5\alpha}{\sqrt{0.125\alpha + 0.25\alpha(N^2-1)}}\right) + \frac{1}{2}Q\left(\frac{0-(-0.5\alpha)}{\sqrt{0.125\alpha + 0.25\alpha(N^2-1)}}\right) = Q\left(\frac{0.5\alpha}{\sqrt{0.125\alpha + 0.25\alpha(N^2-1)}}\right). \quad (16)$$

The Q-function in (16) is defined as [9]

$$Q(x) = \int_x^\infty \frac{1}{\sqrt{2\pi}} \exp\left(\frac{-t^2}{2}\right) dt. \quad (17)$$

It can be observed from (15) that $\mathrm{var}(O_i)$ increases with N^2. Hence, the performance of the system will degrade quite rapidly with the number of users, as indicated in Fig. 7.

V. Results on Error Performance and Overall Capacity

Simulations have been carried out to confirm the feasibility of the proposed multiple-access scheme and to verify the foregoing numerical analysis. Spreading factors 200 and 2000 are used. The number of users in the system is assigned up to 50 and different initial conditions are assigned to different users to generate the chaotic signals. 10 000 bits are first sent from each user. Then, the number of errors received by each user and the average number of errors among all users are noted. Fig. 8 shows some typical results obtained. In this example, there are 10 users in the system. The average number of errors is 1562.3 and 6.8 for $\alpha = 100$ and $\alpha = 1000$, respectively. It can be observed that all users receive similar number of errors. In other words, the scheme achieves unbiased error probabilities for all users. The reason is that all users are suffering from similar amount of interference from all other users. Hence, the error rates are similar.

Fig. 7 compares the numerical BERs computed using (16) with the simulation results. It can be observed that the simulation results match very closely with the numerical ones. As mentioned in Section IV, the

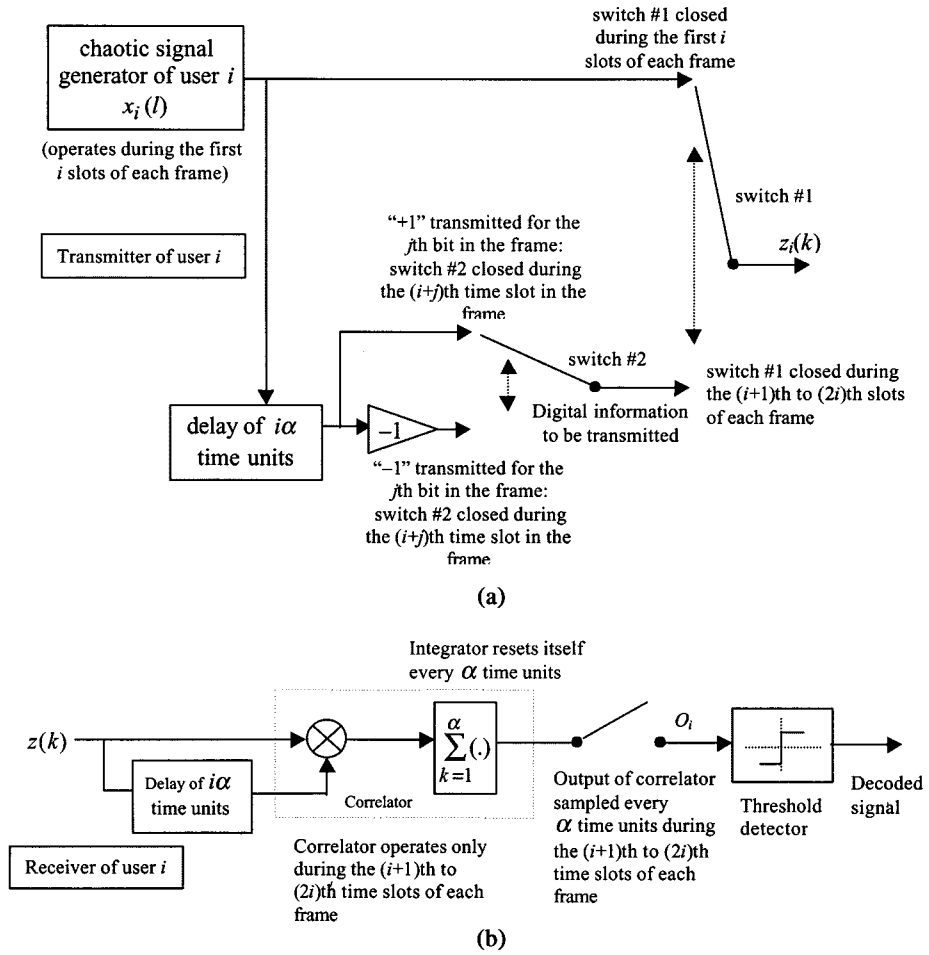

Fig. 4. (a) Transmitter of user i in a multiuser DCSK system with a spreading factor 2α. (b) Receiver of user i in a multiuser DCSK system with a spreading factor 2α.

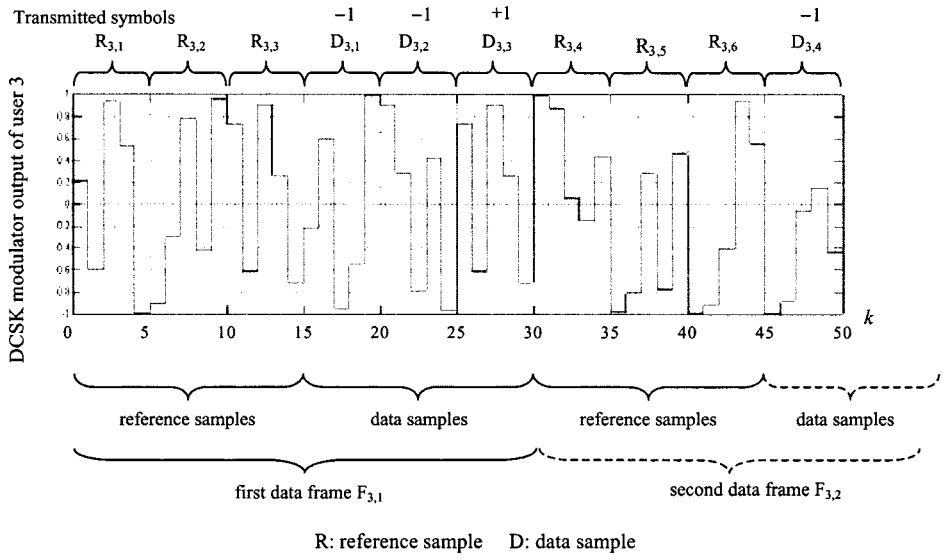

Fig. 5. A typical transmitted signal for user 3 in a multiple-access DCSK system (spreading factor = 10).

variance of the output of the correlator, $\mathrm{var}(O_i)$, increases with N^2. Hence, the BER becomes high when the number of users is large. On the other hand, by using a higher spreading factor and hence lower autocorrelation and cross-corrrelation values, the system performance can be drastically improved under a noise free environment.

The overall capacity of the system is also evaluated for different number of users and plotted in Fig. 7. The capacity of each user, denoted by C, is given by $C = 1 - H(\mathrm{BER})$ where $H(.)$ represents the entropy function. The overall capacity of the system is simply N times the individual capacity. As shown in Fig. 7, when the number of users

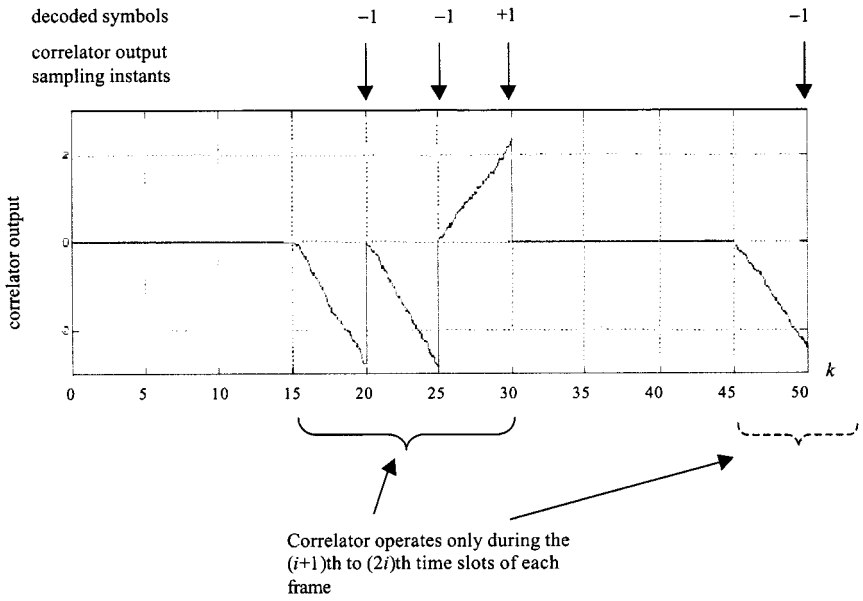

Fig. 6. Output of the correlator and the decoded symbols of user 3 in a five-user system (spreading factor = 2000).

TABLE I
STATISTICAL PROPERTIES OF $X_{i,u,v}$ FOR SPREADING FACTORS 200 AND 2000

Spreading factor 2α	Statistical properties	Case I: $u=v=i$	Case II: $u=v$, $u\neq i$	Case III: $u\neq v$
200	Mean	$\overline{X_{i,i,i}}=\begin{cases}50 & \text{"+1" is transmitted}\\ -50 & \text{"−1" is transmitted}\end{cases}$	$\overline{X_{i,u,u}}=0$	$\overline{X_{i,u,v}}=0$
	Variance	$\text{var}(X_{i,i,i})=12.5$	$\text{var}(X_{i,u,u})=25$	$\text{var}(X_{i,u,v})=25$
2000	Mean	$\overline{X_{i,i,i}}=\begin{cases}500 & \text{"+1" is transmitted}\\ -500 & \text{"−1" is transmitted}\end{cases}$	$\overline{X_{i,u,u}}=0$	$\overline{X_{i,u,v}}=0$
	Variance	$\text{var}(X_{i,i,i})=125$	$\text{var}(X_{i,u,u})=250$	$\text{var}(X_{i,u,v})=250$

increases, the overall capacity increases initially because the small reduction of capacity of each individual is compensated by the additional capacity of extra users. After reaching a maximum value (4.3 and 13.8 bits/bit duration for $\alpha = 100$ and $\alpha = 1000$ respectively), the overall capacity starts to decrease because the extra capacity of an additional user cannot compensate for the total reduction of capacity of the existing users.

VI. COMPARISONS AND DISCUSSION

In this section, we compare our proposed multiple-access scheme with the one reported earlier by Jáko *et al.* [18]. First of all, in both schemes, one reference sample will correlate with the corresponding data sample in order to decode the data. Similar interference will be received by each user in both systems and hence similar BERs are expected. On the other hand, due to the different arrangements of the reference/data samples, the requirements for the two schemes are different and each scheme has its own advantages and disadvantages.

Suppose there are N users in the system. In the multiple-access scheme proposed by Jáko *et al.* each bit period is divided into 2^N time slots. One reference/data sample pair of each user is first divided into 2^N parts and then transmitted in the 2^N time slots. The arrangement of the parts in the time slots will be different for different users. The scheme ensures that data can be decoded in every bit duration. When the number of users increases, the number of time slots created in each bit duration would increase exponentially, implying that switching between the reference and data samples will be performed more frequently within the same bit period. This will impose more stringent requirements on the switching circuits in both the transmitter and the receiver. In our proposed scheme, each bit period is always divided into two slots for all users. The requirements on the switching circuits in the transmitter and the receiver will be similar compared with the single-user system. The price to pay, however, is that the frame periods of different users are different. Since the user has to receive half of the frame before demodulation can begin, different users will experience different demodulation delay although the average bit rates of all users are identical. Moreover, a buffer is required at the transmitter side to store the arriving data when the transmitter is sending the reference samples during the first half of the frame.

VII. CONCLUSIONS

In this paper, we have proposed a simple multiple-access scheme for use with differential chaos shift keying (MA-DCSK). The access scheme of different users has been described and the corresponding noncoherent receiver has also been designed to decode the signals. As

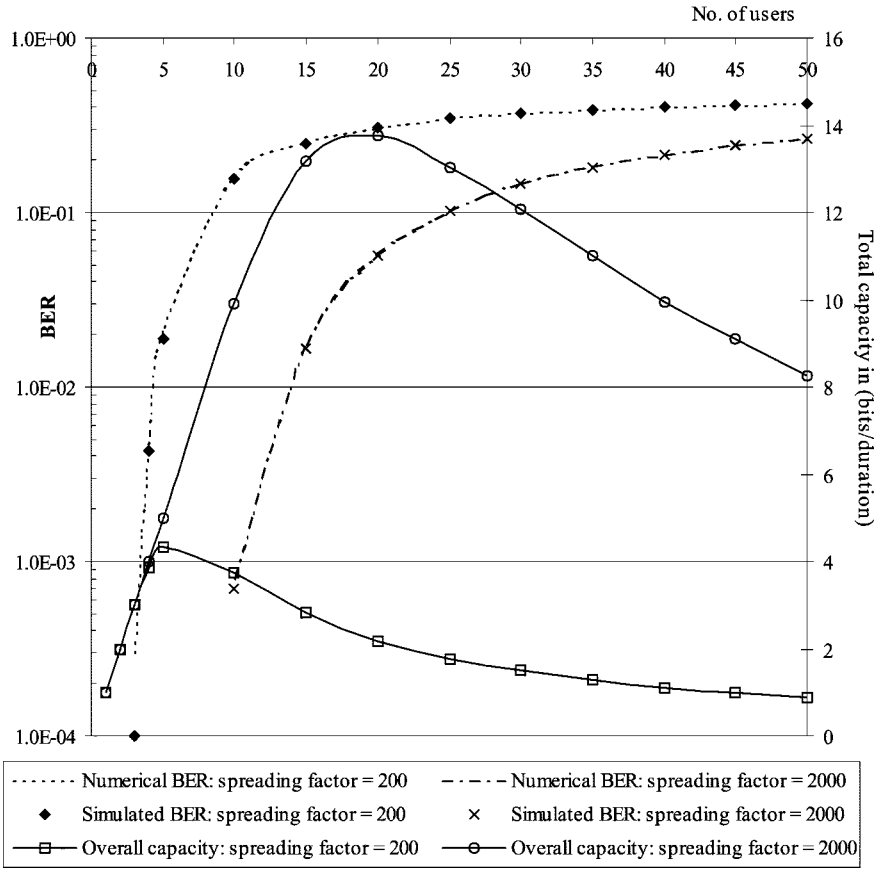

Fig. 7. Numerical and simulated bit error probabilities, and total system capacity against number of users in a multiuser DCSK system.

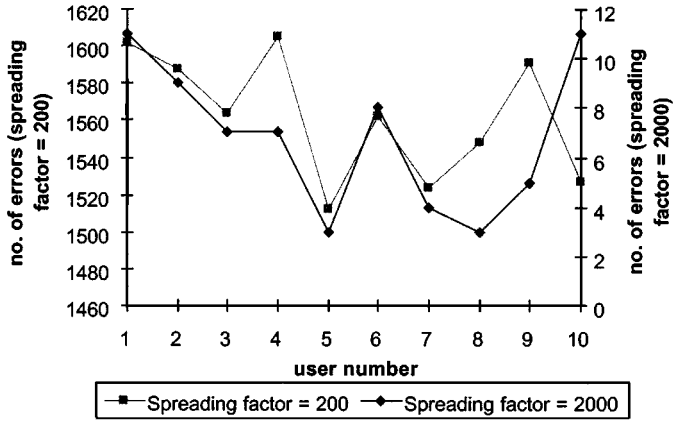

Fig. 8. Number of errors received for different users out of 10 000 transmitted symbols.

in a single-user DCSK system, each bit period is always divided into two slots for all users. Hence, the requirements on the switching circuits in the transmitter and the receiver is similar compared with the single-user system. The trade-off, however, is that the frame periods of different users are different. The user has to receive half of the frame before demodulation can begin. As a consequence, different users will experience different demodulation delays although the average bit rates of all users are the same.

In order to evaluate the performance of the system, a simple 1-D iterative map has been used to generate the chaotic signals for all N users. For this particular choice of map where the probability density function of the chaotic signal is symmetrical with zero mean, it is found that the correlator output follows an approximate normal distribution with variance increases with N^2, provided the probabilities of a "$+1$" or "-1" being transmitted are equal for all users. As a consequence, the numerical BER of the system is derived. As would be expected, the proposed scheme achieves similar error probabilities for all users because all users are suffering from similar amount of interference from all other users. Moreover, the error performance degrades as the number of users increases. Simulations are then carried out and the results match very closely with the numerical BER. It is observed that by using a higher spreading factor and hence lower autocorrelation and cross-corrrelation values, the BER can be reduced under a noiseless environment. The overall system capacity has also been evaluated and it is found that different optimal values are obtained for different spreading factors.

The proposed scheme can be applied to the downlink (base station to mobile station) as well as the uplink (mobile station to base station) in wireless communications. If the scheme is applied in the uplink, slot synchronization among all participating users may be required, which unfortunately is very difficult to maintain in practice. In the case when the time slots among users are not synchronized, it is anticipated that the interference between users will not vary much. As a result, the BER performance should not be affected substantially. Detailed analysis and more simulations are required to verify the conjecture. Finally, noise appears in all communication systems. It is therefore of interest to study the effect of noise in the MA-DCSK system and to derive similar numerical solutions. This will be left to a future publication. On the other hand, the DCSK scheme is known to be suboptimal in the amplitude modulated version. An extension of the present numerical analysis to the frequency modulated DCSK would also be worth studying.

APPENDIX

The statistical properties of $X_{i,u,v}$, as defined in Section IV, are investigated here for different combinations of u, v and i. All symbols have their meanings as defined in the paper.

Case I: $u = v = i$: The reference sample of the ith user correlates with the corresponding data sample. Since the data sample is derived from the reference sample, with a possible factor of -1 due to the binary symbol, a high correlation value is expected. $X_{i,u,v}$ is now re-expressed as

$$X_{i,i,i} = \sum_{k=\alpha(m_i-1)+1}^{\alpha(m_i-1)+\alpha} z_i(k)z_i(k+\alpha i) = b_i(m_i) \sum_{l=\alpha(m_i-1)+1}^{\alpha(m_i-1)+\alpha} x_i^2(l). \quad \text{(A1)}$$

For brevity, we let $W_{i,i,i} = \sum_{l=\alpha(m_i-1)+1}^{\alpha(m_i-1)+\alpha} x_i^2(l)$. Hence, we have

$$X_{i,i,i} = b_i(m_i)W_{i,i,i}. \quad \text{(A2)}$$

Applying the central limit theorem to $W_{i,i,i}$ shows that $W_{i,i,i}$ is approximate normal with the approximation getting better with increasing α.

Case II: $u = v$, $u \neq i$: One reference/data sample of the uth user correlates with another reference/data sample i slots away. For the uth user, the reference sample and its corresponding data sample are separated by u slots. Therefore, if $u \neq i$, low correlation is expected between the reference/data samples separated by i slots. $X_{i,u,v}$ is now re-expressed as

$$X_{i,u,u} = \sum_{k=\alpha(m_i-1)+1}^{\alpha(m_i-1)+\alpha} z_u(k)z_u(k+\alpha i). \quad \text{(A3)}$$

It is obvious that for a zero-mean symmetrical pdf, a multiplication of $+1$ or -1 does not change the shape of the pdf. Hence, for $x_u(l)$ which has a symmetrical pdf with zero mean, the two signals $z_u(k)$ and $z_u(k+\alpha i)$, derived from multiplying $x_u(l)$s with $+1$ or -1 for some ls, would have the same pdf of $x_u(l)$. Define $W_{i,u,u}$ as

$$W_{i,u,u} = \sum_{m=1}^{\alpha} x_u(l_1+m)x_u(l_2+m) \quad \text{(A4)}$$

for some unequal values l_1 and l_2. The pdf of $X_{i,u,u}$ would then have the same pdf of $W_{i,u,u}$. Applying the central limit theorem again, $W_{i,u,u}$ and hence $X_{i,u,u}$ can be shown to be approximate normal with better approximation with increasing α.

Case III: $u \neq v$: One reference/data sample of the uth user correlates with the reference/data sample of another user (vth user) i slots away. Since the samples are generated by chaos generators with different initial conditions [22], low correlation is expected. Rewrite (9) here again

$$X_{i,u,v} = \sum_{k=\alpha(m_i-1)+1}^{\alpha(m_i-1)+\alpha} z_u(k)z_v(k+\alpha i). \quad \text{(A5)}$$

Similar to the previous case, for $x_u(l)$ which has a symmetrical pdf with zero mean, the two signals $z_u(k)$ and $z_v(k+\alpha i)$, derived from multiplying $x_u(l_1)$ and $x_v(l_2)$ with $+1$ or -1 for some l_1 and l_2, would have the same pdf of $x_u(l)$. Define $W_{i,u,v}$ as

$$W_{i,u,v} = \sum_{m=1}^{\alpha} x_u(l_1+m)x_v(l_2+m) \quad \text{(A6)}$$

for some values l_1 and l_2. The pdf of $X_{i,u,v}$ would have the same pdf of $W_{i,u,v}$. Applying the central limit theorem again, $W_{i,u,v}$ and hence $X_{i,u,v}$ can be shown to be approximate normal with better approximation with increasing α.

Extensive simulations have been carried out on the chosen map (13) to calculate the means and variances of $W_{i,i,i}$, $W_{i,u,u}$ and $W_{i,u,v}$ in the above three cases with spreading factors 200 and 2000. From the results, the means and variances of $X_{i,u,v}$s are derived, as tabulated in Table I.

REFERENCES

[1] L. Kocarev, K. S. Halle, K. Eckert, L. O. Chua, and U. Parlitz, "Experimental demonstration of secure communications via chaotic synchronization," *Int. J. Bifurcation Chaos*, vol. 2, pp. 709–713, 1992.

[2] M. Itoh and H. Murakami, "New communication systems via chaotic synchronizations and modulation," *IEICE Trans. Fund.*, vol. E78-A, no. 3, pp. 285–290, 1995.

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

[4] G. Kis, Z. Jáko, M. P. Kennedy, and G. Kolumbán, "Chaotic communications without synchronization," in *Proc., 6th IEE Conf. Telecommunications*, Edinburgh, U.K., Mar. 1998, pp. 49–53.

[5] M. P. Kennedy, "Chaotic communications: From chaotic synchronization to FM-DCSK," in *Proc., 6th Int. Specialist Workshop on Nonlinear Dynamics of Electronics Systems (NDES 98)*, Budapest, Hungary, July 1998, pp. 31–40.

[6] G. Kolumbán, M. P. Kennedy, and L. O. Chua, "The role of synchronization in digital communications using chaos—Part II: Chaotic modulation and chaotic synchronization," *IEEE Trans. Circuits Syst. I*, vol. 45, pp. 1129–1140, Nov. 1998.

[7] G. Kis, "Required bandwidth of chaotic signals used in chaotic modulation schemes," in *Proc., 6th Int. Specialist Workshop on Nonlinear Dynamics of Electronics Systems (NDES 98)*, Budapest, Hungary, July 1998, pp. 113–117.

[8] J. Schweizer and M. P. Kennedy, "Predictive Poincaré control modulation: A new method for modulating digital information onto a chaotic carrier signal," in *Proc. Irish DSP and Control Colloquium*, Dublin, Ireland, 1994, pp. 125–132.

[9] J. G. Proakis and M. Salehi, *Communication Systems Engineering*. Englewood Cliffs, NJ: Prentice-Hall, 1994.

[10] G. Kolumbán, "Theoretical noise performance of correlator-based chaotic communications schemes," *IEEE Trans. Circuits Syst. I*, vol. 47, pp. 1692–1701, Dec. 2000.

[11] M. P. Kennedy, G. Kolumbán, G. Kis, and Z. Jáko, "Performance evaluation of FM-DCSK modulation in multipath environments," *IEEE Trans. Circuits Syst. I*, vol. 47, pp. 1702–1711, Dec. 2000.

[12] M. Sushchik, L. S. Tsimring, and A. R. Volkovskii, "Performance analysis of correlation-based communication schemes utilizing chaos," *IEEE Trans. Circuits Syst. I*, vol. 47, pp. 1684–1691, Dec. 2000.

[13] T. L. Carroll and L. M. Pecora, "Using multiple attractor chaotic systems for communication," *Chaos*, no. 9, pp. 445–451, 1999.

[14] T. Yang and L. O. Chua, "Chaotic digital code-division multiple-access (CDMA) communication systems," *Int. J. Bifurcation Chaos*, vol. 7, pp. 2789–805, 1997.

[15] G. Mazzini, G. Setti, and R. Rovatti, "Chaotic complex spreading sequences for asynchronous DS-CDMA. Part I: System modeling and results," *IEEE Trans. Circuits Syst. I*, vol. 44, pp. 937–947, Oct. 1997.

[16] ——, "Chaotic complex spreading sequences for asynchronous DS-CDMA. Part II: Some theoretical performance bounds," *IEEE Trans. Circuits Syst. I*, vol. 45, pp. 496–506, Apr. 1998.

[17] G. Kolumbán, M. P. Kennedy, and G. Kis, "Multilevel differential chaos shift keying," in *Proc., 5th International Specialist Workshop on Nonlinear Dynamics of Electronics Systems (NDES'97)*, Moscow, Russia, June 1997, pp. 191–196.

[18] M. P. Kennedy, G. Kolumbán, G. Kis, and Z. Jáko, "Recent advances in communicating with chaos," in *Proc., IEEE Int. Symp. Circuits and Systems, (ISCAS'98)*, vol. 4, Monterey, CA, May 1998, pp. 461–464.

[19] Z. Jáko, G. Kis, and G. Kolumbán, "Multiple access capability of the FM-DCSK chaotic communications system," in *Proc., 8th Int. Specialist Workshop on Nonlinear Dynamics of Electronics Systems (NDES'2000)*, Cantania, Italy, May 2000, pp. 52–55.

[20] M. D. Springer, *The Algebra of Random Variables*. New York: Wiley, 1979.

[21] S. M. Ross, *Introduction to Probability Models*, 5th ed. New York: Academic, 1993.

[22] K. T. Alligood, T. D. Sauer, and J. A. Yorke, *Chaos: An Introduction to Dynamical Systems*. New York: Springer-Verlag, 1996.