Recent Theory and New Applications in Chaos Communications

Anthony J Lawrance
Department of Statistics
University of Warwick
Coventry, United Kingdom
Email: A.J.Lawrance@warwick.ac.uk

Abstract—This paper will begin the Special Session by introducing the topics to be covered and then more particularly will present some of the author’s recent work on exact and accurate conditional Gaussian approximations for BER, likelihood decoding, and the communications use of optical chaos. There will be two general themes to the session, one of improving existing theory of BER performance and one covering the latest application developments of chaos-based communications to ultra wide-band radio and cooperative personal networks. The main system used for exemplification will be multi-user antipodal chaos shift-keying, both in coherent and noncoherent forms, and also with some modifications including frequency modulated chaos shift-keying and error correcting. Other topics of the session include highly accurate approximate BER results with channel fading, the role of non-constant bit energy, and optimal spreading.

I. INTRODUCTION

There has been a substantial body of work in chaos communications over the last decade or so, the evidence being in the monographs [1], [2], [3], [4] and [5]. Motivation of this interest derives from the advantages offered by chaotic signals in terms of highly spread spectrum, non-periodicity, robustness in multipath environments, coexistence with other systems, resistance to jamming, apparent randomness, non-predictability, and low cost. The possibility of generating an infinite number of sequences from a given chaotic map, electronic circuit or optical laser makes for attractive application of these signals. However, there has also been criticism that the bit error performance of chaos-based systems is often inferior to that conventional sinusoidal systems. This point may be lessened by optimized coding and decoding which means not following the conventional approaches, but using statistically efficient ones, Lawrance [6]. Alternatively, as first pointed out by Kolumban [7] and continued by Kolumban [8] and Wang [9] in this session, the applications should be ones where the perceived criticisms are irrelevant, such as ultra wide-band radio, low data rate personal networks and optical laser systems.

II. MULTI-USER ANTIPODAL CSK COMMUNICATION

The first concern is to define for the rest of the paper the meaning to be applied to basic chaos shift keying (CSK) communication systems, which feature strongly in this session; there are a number of versions in the literature, several of which could equally be used. The block diagram in Figure 1 illustrates the system to be considered, assuming \( L \) users.

The system is concerned with the simultaneous transmission of a single binary bit message for each user. Dynamic or statistical linkage between successive bits is not considered in the basic model, but is useful when error correcting is the concern, as shown by Arai et al in [10] of this session. The binary messages \( b_i = \pm 1, i = 1, 2, \ldots, L \) are to be simultaneously transmitted by the \( L \) users to \( L \) receivers. The focus is on an individual user, the so-called active-user, in the presence of the other-users, accepted as interferers. To carry a binary message, user \( i \) has a chaotic generator which provides

![Fig. 1. Block diagram of a multi-user coherent antipodal CSK communication system.](image-url)
a spreading segment $X_j^T = (X_{j1}, \ldots, X_{jN})$ of chosen spreading factor length $N$ and which is modulated (multiplied in the antipodal case) by the bit to be transmitted $b_j$ and then called the message segment. Thus, the binary bit $b_j$ is transmitted $N$ times in the message segment which has values $b_j, j = 1, 2, \ldots, N$. All the $L$ bit-modulated spreading segments are transmitted additively in the same time slot through the noisy channel and arrive at all receivers but with additive individual Gaussian channel noise, of variance $\sigma_x^2$. In the basic model, described as coherent, the individual spreading segment of the $l$th user is available without error at the $l$th receiver, either by chaotic synchronization or by identical chaotic generation; this is often called the reference segment since the received message segment is compared with it in order to decode $b_j$, or in statistical language, to estimate $b_j$. In the so-called non-coherent case, sometimes called the differential case, the spreading segments are separately and additionally transmitted and are received with channel noise or synchronization error. The main motivation of all the subsequent modelling is the assessment of wrongly decoding $b_j$, the bit error rate; this means the average probability of erroneously decoding a transmitted bit.

For the $l$th and active-user transmitting a single bit, the message segment containing the bit information arriving at the $l$th receiver is

$$R_j = b_jX_j + \sum_{k=1}^{L} b_kX_k + \epsilon_{lj}, j = 1, 2, \ldots, N \quad (1)$$

where $\epsilon_{lj}$ is the channel noise, for $l = 1, 2, \ldots, L$. The summation term represents interference by the message bits of other users. The decoding of the received message bit $b_j$ in the transmitted segment (1) at the receiver is an essentially statistical task of estimation and is done in conjunction with knowledge of the $l$th spreading segment, the reference segment, but without knowledge of the other spreading segments at the receiver. In the coherent case there is exact knowledge of the spreading segment, but in the non-coherent case it is received un-modulated as

$$Y_j = X_j + \epsilon_{lj}, j = 1, 2, \ldots, N \quad (2)$$

and $\epsilon_{lj}$ is the channel noise; $\epsilon_{lj} \equiv 0$ can be regarded as the coherent case. The message bit $b_j$ is best treated as a statistical parameter and then the optimum decoder is a likelihood-based estimate of $b_j$; on the other hand, the bits of the other users are not of interest to the $l$th user and are treated as random variables.

The spreading segments are required to be part of a chaotic sequence, although this is not a fundamental requirement to shift-keying communication as being described here. It is just that chaotic segments can have the previously mentioned desirable properties, and can easily be mathematically generated, and by electronic circuits and optical lasers. However, the connection between these three is not close and worthy of future examination, as will be mentioned.

However, as a model for theoretical study, and also a practical method, the generation by a chaotic map $\tau(\cdot)$ is mathematically convenient. Thus, for the $l$th user, the chaotic segment $\{X_{lj}\}$ is assumed to have been started with a random initial sample value $X_{l1}$ from the natural invariant distribution of $\tau(\cdot)$. As random variables, the chaotic segments of the $l$th user are arranged have zero mean, common variance $\sigma_x^2$ and they are of course dependent, both functionally and statistically.

For both the coherent and non-coherent cases, the correlation decoder using

$$R_l = (R_{lj}, j = 1, 2, \ldots, N) \text{ and } Y_l = (Y_{lj}, j = 1, 2, \ldots, N) \quad (3)$$

is the standard choice, and given by

$$\hat{b}_l = \begin{cases} +1 & \text{if } C(R_l, Y_l) \geq 0 \\ -1 & \text{otherwise} \end{cases} \text{, } C(R_l, Y_l) = \sum_{j=1}^{N} R_{lj}Y_{lj} \quad (4)$$

Much of the earlier theory is concerned with the bit error rate (BER) of this decoder in the single user case; the earliest approximations were given by Kolumban [11], and later exact results were given by Lawrance [12]. The optimal choice of chaotic spreading is crucial, Yao [15], Papamarkou [16], but not really considered in the early work. Much more could be said about the significant contributions of earlier work, but the next section will be mainly focused on the more recent work of the author.

### III. RECENT RESULTS FOR COHERENT CSK SYSTEMS

Remaining with correlation decoders to begin this section, some recent results for coherent multi-user CSK are presented. The distribution of $C(R_l, Y_l)$ is required but the mathematics is not exactly tractable. Earlier approaches, see [2], much advanced the topic by giving simple Gaussian approximation (SGA) to the distribution. But to improve on this, Lawrance [13], [6], introduced the conditional Gaussian approximation (CGA). This gave two useful equivalent expressions of the result as

$$\text{BER} = E_x \times \Phi \left[ \sum_{i=0}^{N-1} X_i^2 \right] \left\{ \frac{1}{\text{SNR}} + 1 \left( \frac{1}{\text{SOR}} + 1 \right) \right\} + \frac{2}{\text{SOR}} \sum_{i=1}^{N-1} \left\{ \frac{\sum_{j=0}^{N-1} X_j X_{j+i}}{\sum_{j=0}^{N-1} X_j^2} \right\} \rho_x(k) \right\}^{1/2}$$

$$\text{BER} = E_x \times \left[ \Phi \left( -\frac{\left( \sum_{i=0}^{N-1} X_i^2 \right)^{1/2}}{\left( \sum_{i=0}^{N-1} X_i^2 \right) \sigma_x^2} \left( \frac{1}{\text{SNR}} + 1 \left( \frac{1}{\text{SOR}} + 1 \right) \right) \right) \right]$$

where $\text{SNR} = N \sigma_x^2 / \sigma_x^2$ is the signal to noise ratio, $\text{SOR}$ is a new quantity, the spreading to other user interference ratio, defined as $N/(L-1)$. $\Phi$ is the cumulative standardized Normal distribution function, often expressed as an erf function. The form (5) shows the importance of the bit energy, a topic to be dealt with by Kaddoum [14] in this
session. The form (6) shows clearly the interpretable behaviour as $N$ becomes large and also when $SNR$ becomes large - there is still bit error because of interference by other users. These and similar results can be computed analytically for well-known chaotic maps for which there are explicit iterated forms, but can be computationally demanding for extensive spreading. Illustrations may be found in previous papers, such as Lawrance [13], [6] and others. The choice of maps is crucial, logistic being the best among the common maps, and with circular maps of Yao [15], Papamarkou [16] being optimal, these having strong negative quadratic correlation.

While the correlation decoder is standard, it is not optimal, except in the CSK single-user coherent case. This prompted Lawrance [6] to explore likelihood approaches, and this inactively led to the generalized correlation decoder

$$\hat{b}_i = \begin{cases} +1 & R_i^T \Sigma_x^{-1} Y > 0 \\ -1 & \text{otherwise} \end{cases}$$

(7)

where $\Sigma_x$ is the autocorrelation matrix of $X$ and known theoretically for many chaotic maps. This decoder gains performance, as confirmed by simulation, by utilizing prior information about the spreading; it has the CGA bit error result

$$BER = E_x \left\{ \Phi \left( - \frac{N^{-1}(X^T \Sigma_x^{-1} X)^{1/2}}{\sigma_x^2} \left[ \left( \frac{X^T \Sigma_x^{-1} X}{SNR} \right)^{1/2} + \frac{1}{SOR} \right] \right) \right\}.$$  

(8)

A point to be noted is that there is no explicit role for bit energy here, leading to the tentative conclusion that this is more associated with standard correlation decoding.

Although the corresponding SGA result to (6) is reported in [2], it is thought worthwhile to show the result in full generality and in the descriptive style

$$BER = \Phi \left[ - \frac{1}{SNR} + \frac{N^{-1} \sigma_x^2}{SNR} \left( 1 + 2 \sum_{i=1}^{N-1} \left( 1 - \frac{k}{N} \right) \rho_x(k) \right) \right] + \frac{1}{SOR} \left( 1 + 2 \sum_{i=1}^{N-1} \left( 1 - \frac{k}{N} \right) \left( \rho_x(k) \right)^2 \right)^{1/2}. \quad (9)$$

Here can be seen the influence of chaos through kurtosis of the invariant distribution, and through both the linear and quadratic autocorrelations. Each of these is a statistical property of chaos as opposed to a dynamical one. Also evident are the common communication aspects of SNR and SOR. The result (5) after replacing its last summation term by $(1 - k/N)\rho_x(k)$ is similar, but much more accurate.

IV. RECENT RESULTS FOR NON-COHERENT CSK SYSTEMS

From a theoretical point of view, non-coherent systems have an added complexity and poorer bit error performance, but are practically more realizable. To set the scene, continue with correlation decoding but restrict attention to single-user systems. Multi-user systems present a higher order of theoretical challenge. Exact analysis in Lawrance [12] gave the deceptively simple BER result as

$$BER = E_x \left\{ P \left( F_{x,X} \left( 2(\|X^T X\|^1/2)/\sqrt{SNR} \right) < 1 \right) \right\} \quad (10)$$

$$= (2\pi \sigma_x^2)^{-1} \exp \left( -\frac{1}{2} \sum_{i=1}^{N} \left( r_i - bx_i \right)^2 \right).$$

The quantity $F_{x,X}(\cdot)$ is a random variable with the so-called doubly non-central $F$-distribution with the indicated non-centrality parameter. The probability that it is less than 1 is then calculated as a function of $X^T X$, the sum of squares or bit energy of the spreading sequence. This probability is then averaged over the distribution of bit energy. The distribution of bit energy has been studied by Kaddour, as in [17]. Unlike the coherent case, the BER does not decrease as $N$ increases. The simple Gaussian approximation to this result, obtained computationally in Sushchik et al [18], is given more fully in the previous descriptive style by

$$BER = \Phi \left[ - \left( \frac{2}{SNR + SNR^2} + \frac{N}{SNR} \right) \rho_x(k) \left( 1 + 2 \sum_{i=1}^{N-1} \left( 1 - \frac{k}{N} \right) \rho_x(k) \right)^{1/2} \right]. \quad (11)$$

It can be seen that it tends to its highest value of one-half as $N$ tends to infinity, unlike the coherent case for which it tends to the BPSK lower limit; also, the near quadratic aspect in $N$ indicates there is an optimum degree of spreading for fixed SNR.

An extension of (11) to a multiple user result with broadly similar structure and conclusions is

$$BER = \Phi \left[ - \frac{2}{SNR + SNR^2} + \frac{2}{SNR} \rho_x(k) \left( 1 + 2 \sum_{i=1}^{N-1} \left( 1 - \frac{k}{N} \right) \rho_x(k) \right)^{1/2} \right]. \quad (12)$$

V. LIKELIHOOD DECODING

There is no doubt that this is the biggest theoretical challenge for non-coherent CSK systems, and it is by no means yet solved for practical use. Previous likelihood-based work, [19], [20], [6] assumed that the noise variance was known, not always the practical situation, and also under specialized assumptions. The full likelihood decoder should just use the received data pertaining to each bit, and not need knowledge of the channel noise variance. Early consideration of the full likelihood was given in Lawrance [12] but more recent progress has been made by T. Papamarkou (unpublished as yet) in his 2010 Warwick PhD thesis. Work is still limited to the single-user case.

By virtue of the Gaussian noise assumptions, the full joint probability density function of $R, Y, X$ for transmitted data $b, r, y$ and with $X$ unknown, is given by
\[
\begin{align*}
\hat{b} = \begin{cases} 
+1 & \text{if } likr(b | r, y) > 1 \\
-1 & \text{otherwise}
\end{cases}
\end{align*}
\]

The computational organization is considerable and as yet only manageable as a research methodology. Brute-force simulation has given BER curves, and these show that improvement over correlation decoding is increasingly evident as SNR becomes large.

VI. RECENT APPLICATIONS

Recent applications in the area of ultra-wide frequency band chaos communications will be covered in this Special Session by Kolumban & Krebesz [8] and by Wang [9]. Here the chaotic carriers, generated by electronic circuits, have extremely low power spectral density. They are beneficial for indoor and mobile applications where high data rates are not required, and where low bit error rates are achieved by acknowledgement protocols. Particular instances are UWB radio, networking devices of embedded systems, and personal or body area networks; they also have the advantage of being able to co-exist with other systems. In their papers, Kolumban recommends FM-DCSK with TR-based autocorrelation decoding, while Wang is more concerned with DCSK/FM-DCSK and a cooperative strategy.

A further emerging area is that of optical laser-based communications, currently being developed by the author. The extremely fast generation of laser waves and the ability to synchronize lasers by injection makes this an attractive possibility; one such system has already been experimentally tested, Argyris et al [21]. Uchida et al [22], envisaged another possibility with a chaotic on-off keying system. The author is analyzing synchronized pairs of sequences from lasers pumped via optical feedback; their nonlinearity has been established, but chaotic features have yet to be ascertained. The data have been kindly provided by Professor A. Uchida of Saitama University, Japan and colleagues. There are thus several promising new directions in which the area of chaos communications is still developing.

REFERENCES