
Peer reviewed version

Link to published version (if available):
10.1109/TCSII.2004.835559

Link to publication record in Explore Bristol Research
PDF-document

University of Bristol - Explore Bristol Research

General rights

This document is made available in accordance with publisher policies. Please cite only the published version using the reference above. Full terms of use are available:
http://www.bristol.ac.uk/pure/about/ebr-terms.html
The Importance of Choosing Attractors for Optimizing Chaotic Communications

Martin E. Homer, S. John Hogan, Mario di Bernardo, and Chris Williams

Abstract—In this brief, we consider methods to improve the performance of chaotic communication schemes. We study a system using a receiver which explicitly includes the presence of noise in the channel. We show how the choice of chaotic dynamical system generating the transmitted signal is crucial. We observe a large variation in bit error rate performance of the system as parameters in the maps are changed, and we propose a simple explanation for this variation.

Index Terms—Bit error rate (BER), chaotic communication, optimal estimator, piecewise smooth systems.

I. INTRODUCTION

Following the discovery that two chaotic oscillators can be synchronized [1], there has been a considerable amount of speculation that chaotic dynamics could lead to the possibility of secure low power communication systems which are easy to build, and have low probability of interception and detection [2]–[5]. In practice, the use of chaos in communication systems has been limited because most schemes based on synchronization perform poorly in the presence of a distorting channel. Much recent work has concentrated in improving chaotic communication schemes to degradation by noise, band-pass filtering, attenuation, and parameter mismatch [6]–[12].

Clearly, how noise affects a chaotic communication scheme is vital. The most frequently used performance indicator for a communication scheme is the bit error rate (BER); although other measures, bandwidth or power efficiency for example, must also be considered.

We consider a scheme using a receiver that is explicitly designed to take account of channel distortion [13], and use piecewise-linear maps to generate the transmitted iterates. In particular, we show that the optimal BER performance of the optimal estimator scheme using the piecewise-linear maps is much lower than that obtained by using skew tent maps, and observe a wide variation in the BER performance of the system as parameters are varied in the piecewise-linear maps. Furthermore, we provide an explanation for this wide variation in performance with reference to any distribution of channel noise or choice of transmitter maps. This leads us to a method to reduce the BER still further.

The brief is organized as follows. In Section II we describe the notation used throughout the paper, review the synthesis of the optimal estimator in Section III, and describe the piecewise-linear map used to generate the transmitted iterates in Section IV. In Section V we consider the changes in the BER as parameters of the transmitter map are varied. In Section VI we provide an explanation for the differences in performance found in Section V. Finally, we provide conclusions and suggest possible areas for further work in Section VII.

II. DEFINITIONS

We follow the notation of [13]. Suppose that we wish to transmit an M-ary symbol \( \sigma_1, \sigma_2, \ldots, \sigma_M \). We suppose that the symbols are samples from a random variable \( \Sigma \). For simplicity we shall assume a uniform distribution for \( \Sigma \) so that

\[
P(\Sigma = \sigma) = \frac{1}{M}.
\]  

(1)

The chaos-shift keying (CSK) method transmits strings of \( N \) iterates \( \mathbf{x} = (x_1, x_2, \ldots, x_N)^T \in \mathbb{R}^N \) to represent one of the \( M \) possible symbols. The iterates are generated by one of \( M \) chaotic maps \( G_{\sigma_1}, G_{\sigma_2}, \ldots, G_{\sigma_M} \) depending on the symbol to be transmitted. Thus, to transmit the \( M \)-ary symbol \( \sigma \in \Sigma \) the transmitted string is

\[
\mathbf{x} = (x_1, G_{\sigma}(x_1), G_{\sigma}^2(x_1), \ldots, G_{\sigma}^{N-1}(x_1))^T
\]  

(2)

where \( G_{\sigma}^i \) denotes the \( i \)-fold composition of the map \( G \). Each string is generated by its first iterate \( x_1 \). We assume that each chaotic map has a unique stationary distribution, and that it can be described by a density (true for a wide class of dynamical systems: ergodic maps, for example, [14]). Thus the first iterates \( x_1 \) can be modeled as samples from a random variable \( X_1 \). The random variable of first iterates given a particular transmitted symbol, \( X_1|\Sigma = \sigma \), is central to our study; its density function \( \rho_{\sigma} \) is known as the invariant density or invariant measure [14]. We define \( I_{\sigma} \) to be the subset of \( \mathbb{R} \) for which \( \rho_{\sigma} \neq 0 \). The invariant density is known analytically for some maps. It needs to be computed numerically for others, for which efficient numerical algorithms exist [15].

Upon transmission, the signal \( \mathbf{x} \) is degraded by noise in the channel \( \mathbf{w} \in \mathbb{R}^N \), with random variable \( \mathbf{W} \), the components of a realization of the noise \( (w_{ij}) \) are assumed to be identically distributed, and independent of each other and the transmitted
signal. The iterates that arrive at the receiver we label as \( y \), so that
\[
\begin{align*}
y &= \Psi(x, w)
\end{align*}
\] (3)
for some function \( \Psi \), and hence, are samples from a random variable \( Y \). In the case of additive noise, we have
\[
\begin{align*}
y &= x + w
\end{align*}
\] (4)
or for multiplicative noise
\[
\begin{align*}
y &= Wx
\end{align*}
\] (5)
where \( W \) is a diagonal matrix with entries \( w_1, w_2, \ldots, w_N \).

The goal of the communication system is to estimate the transmitted symbol \( \sigma \) from the received signal \( y \) that is, to find a function \( \phi : \mathbb{R}^N \to \Sigma \)
\[
\begin{align*}
\sigma &= \phi(y).
\end{align*}
\] (6)
We shall review the construction of the function \( \phi \) in the next section.

III. SYNTHESIS OF THE OPTIMAL ESTIMATOR

In this brief, we shall use a receiver that minimizes the probability of a misdetected symbol: the optimal estimator \cite{13}. Given a received word \( y \in Y \) it returns the most likely transmitted symbol \( \sigma \), that is, the \( \sigma \in \Sigma \) which maximizes
\[
\begin{align*}
P(\Sigma = \sigma | Y = y).
\end{align*}
\] (7)
It is straightforward to show \cite{13} that this is equivalent to finding the \( \sigma \) that maximizes the probability density function (pdf) of \( Y | \Sigma = \sigma, f_\sigma(y) \), so
\[
\begin{align*}
\phi(y) &= \sigma \in \Sigma : f_\sigma(y) > f_{\sigma'}(y) \quad \forall \sigma' \neq \sigma.
\end{align*}
\] (8)
In the case of a two-symbol transmitter with \( \Sigma = \{0, 1\} \), for example, the optimal estimator reduces to
\[
\begin{align*}
\phi(y) = \begin{cases} 1, & \text{if } f_1(y) > f_0(y) \\ 0, & \text{if } f_1(y) < f_0(y). \end{cases}
\end{align*}
\] (9)
Now we find the received probability density functions \( f_\sigma \) in terms of known distributions. Firstly \cite{16}
\[
\begin{align*}
f_\sigma(y) &= \int f_{X_1, Y | \Sigma = \sigma}(x_1, y | x_1) dx_1
\end{align*}
\] (10)
where \( f_{X_1, Y | \Sigma = \sigma} \) is the joint distribution function of \( X_1, Y | \Sigma = \sigma \). Since for general random variables \( X, Y \) and \( U = U(X, Y), V = V(X, Y) \)
\[
\begin{align*}
f_{X, Y}(x, y) &= f_{U, V}(u(x, y), v(x, y)) \frac{\partial(x, y)}{\partial(u, v)}
\end{align*}
\] (11)
we have that for additive noise
\[
\begin{align*}
f_{X_1, Y | \Sigma = \sigma}(x_1, y) &= f_{X_1, W | \Sigma = \sigma}(x_1, y - x) \\
&= f_{X_1 | \Sigma = \sigma}(x_1) f_W(y - x) \\
&= \rho_\sigma(x_1) f_W(y - x)
\end{align*}
\] (12)
(13)
(14)
because the signal and noise are independent. Combining (10) and (14) gives \( f_\sigma \) in terms of known density functions: the invariant density \( \rho_\sigma \) and the channel noise \( f_W \)
\[
\begin{align*}
f_\sigma(y) &= \int \rho_\sigma(x_1) f_W(y - x) dx_1.
\end{align*}
\] (15)
Alternatively, if the noise is multiplicative, we have that
\[
\begin{align*}
y_i &= w_i x_i = w_i G_i^{[i-1]}(x_1)
\end{align*}
\] (16)
so
\[
\begin{align*}
w_i &= \frac{y_i}{G_i^{[i-1]}(x_1)}
\end{align*}
\] (17)
and hence, the joint density function is given by
\[
\begin{align*}
f_{X_1, Y | \Sigma = \sigma}(x_1, y) &= f_{X_1, W | \Sigma = \sigma}(x_1, y) \\
&= f_{X_1 | \Sigma = \sigma}(x_1) f_W(y | x_1) \\
&= \rho_\sigma(x_1) f_W(y | x_1) \\
&= \rho_\sigma(x_1) f_W(y | x_1) [\prod_{i=1}^N G_i^{[i-1]}(x_1)]^{-1}
\end{align*}
\] (18)
(19)
(20)
where the vector \( y/x \) is defined to be
\[
\begin{align*}
y/x &= \left( \frac{y_1}{x_1}, \frac{y_2}{G_2(x_1)}, \ldots, \frac{y_N}{G_N^{[N-1]}(x_1)} \right)^T.
\end{align*}
\] (21)
Therefore, in the case of multiplicative noise
\[
\begin{align*}
f_\sigma(y) &= \int \rho_\sigma(x_1) f_W(y | x_1) dx_1.
\end{align*}
\] (22)

In this brief, we shall follow the common assumption that the channel distortion is additive white Gaussian noise, with zero mean and variance \( \xi^2 \) \cite{17}, in which case the pdf \( f_\sigma \) is given by
\[
\begin{align*}
f_\sigma(y) &= \frac{1}{(2\pi \xi^2)^{N/2}} \exp \left\{ -\frac{1}{2\xi^2} \sum_{i=1}^N \left[ y_i - G_i^{[i-1]}(x_1) \right]^2 \right\} dx_1
\end{align*}
\] (23)
(24)
where \( y_i \) is the \( i \)th component of \( y \). However, the general methods we discover are not restricted to this choice.

IV. CHOICE OF TRANSMITTER MAP

Having described the properties of the receiver, we now consider the choice of the maps \( G_\sigma \) used to generate the transmitted iterates. These maps are generally chosen from a limited range of candidates: tent maps or shift maps, for example, which have favorable stochastic properties, such as an analytical expression for the invariant measure.

In this brief, we choose the transmitter map to be the piecewise-linear map
\[
\begin{align*}
x_{k+1} &= G(x_k) = \begin{cases} ax + \mu, & x \geq 0 \\ bx - \mu, & x \leq 0, \end{cases}
\end{align*}
\] (25)
Piecewise smooth maps have shown to have several advantages for use in a chaotic communication scheme \cite{18}. Chaotic os-
As the noise spectral density increases through zero, however, the stable fixed point bifurcates directly to a chaotic attractor as shown in Fig. 2(b). In the nonshaded regions, the stable fixed point bifurcates directly to a chaotic attractor as shown in Fig. 2(b). More importantly, the piecewise-smooth systems are generally robust to changes of parameters [19]. The structure of the dynamics in parameter space is summarized in Fig. 1, with sample bifurcation diagrams shown in Fig. 2 for parameter values in the shaded regions of Fig. 1, the single stable fixed point bifurcates directly to a stable periodic point with period 2 in region 2, period 3 in region 3, etc. [as shown in Fig. 2(b)]. In the nonshaded regions, the stable fixed point bifurcates directly to a chaotic attractor as \( \mu \) increases through 0 [as shown in Fig. 2(a) and 2(c)]. The structure of the chaotic attractor varies too: it may be made up of any number of disjoint bands [as in Fig. 2(c)], or may fill a single contiguous interval [as in Fig. 2(a)]. Most significantly of all, the boundaries between all of these regions are known in analytic closed form [20].

Knowing exactly the boundaries of the chaotic regions in \((\alpha, \beta)\) space allows us with complete confidence to choose parameters at which the map is chaotic. There is no question, as in many smooth dynamical systems, that we may accidentally find a periodic window within a chaotic attractor, as the chaos produced by the piecewise-linear map is robust. In the next section, we show how varying the parameter values of the piecewise-linear map (25) within the chaotic regions, produces a significant variation in the performance of the communication scheme.

\[ \text{V. BER PERFORMANCE} \]

The standard performance measure for communication schemes is the BER or probability of a misdetected symbol, computed as a function of \( E_b/N_0 \). \( E_b \) is the symbol energy, defined by

\[ E_b = \langle |x|^2 \rangle \]  

which may be rewritten as

\[ E_b = \frac{1}{M} \sum_{\sigma \in \Sigma} E \left( \sum_{i=1}^{N} G_{\sigma}^{i-1}(X_1)^2 \right) \]

\[ = \frac{1}{M} \sum_{\sigma \in \Sigma} \int_{I_2} \left[ \sum_{i=1}^{N} G_{\sigma}^{i-1}(x_1)^2 \right] \rho_\sigma(x_1) dx_1 \]  

using the assumption that the \( M \) symbols are distributed uniformly in the transmitted message. \( N_0 \) is the noise spectral density; in the case of additive white Gaussian noise with zero mean and variance \( \xi^2 \)

\[ N_0 = \xi^2. \]  

Fig. 3 shows BER plots for a 2-symbol 2-iterate optimal estimator scheme, for various values of the symbol parameters \((\alpha_0, \beta_0)\) and \((\alpha_1, \beta_1)\), as reported in Table I. To produce
this graph, we vary the channel noise variance $\sigma^2$ (and hence $E_b/N_0$), and observe the number of mis-detected symbols by direct simulation. These results may also be computed by evaluation of an explicit expression for the BER

$$\text{BER} = 1 - \frac{1}{M} \int \cdots \int_{\mathbb{R}^N} \max \{ f_{\sigma_1}(y), \ldots, f_{\sigma_M}(y) \} \, dy$$  \hspace{1cm} (30)$$
derived in [21]; it is not restricted to any particular choice of transmitter maps or distribution of noise in the channel. For comparison, Fig. 3 also shows the BER performance achieved by using skew tent maps to generated the transmitted iterates [13].

The most important conclusion from Fig. 3 is that there is a large variation in performance of the communication scheme as the parameters $\alpha$ and $\beta$ are varied. It is also clear that using the piecewise-linear map gives a better BER performance than the skew tent map.

While the BER performance of the optimal estimator scheme is far from the result obtained from a conventional communication scheme, such as BPSK, we are only using two iterates of the chaotic maps to characterize each transmitted symbol (i.e., $N = 2$). For larger $N$, the BER improves substantially as $E_b/N_0$ decreases. The BER curves for 2-iterate, 8-iterate, and 16-iterate, 2-symbol optimal estimator schemes (so $N = 2$, 8, 16 and $M = 2$) for the piecewise-linear map are shown in Fig. 4.

We do not, however, note an optimal $N$ value in our simulations.

Using an optimization algorithm (Matlab routine fmincon), we can find parameter values which minimize the BER (for fixed $E_b/N_0$). These values are

$$(\alpha_0, \beta_0) = (0.477155341621, -2.119987626299)$$

$$(\alpha_1, \beta_1) = (0.480139990491, -5.796804300865)$$

(labeled 1 in Table I), and they give a BER considerably lower than tent maps, as shown in Fig. 3. This computational optimization is only possible because we have a complete understanding of the dynamics of the transmitter maps: we can prescribe the boundaries of the chaotic regions in parameter space analytically, we know that there will be no windows of periodicity within the chaotic zones, and can even prescribe the type of chaotic attractor. The parameter values found were the result of constraining the optimization routine to the regions labeled $2^f$ and $3^f$ in Fig. 1. Several other regions were chosen for subsequent executions of the optimization routine, but no points with lower BER were found.

We now wish to understand why these parameter values minimize the BER, and why there is such a large variation in the performance of the communication scheme. We have investigated simple quantities such as the Lyapunov exponents of the transmitter map (25) in the neighborhood of the optimal parameter values, and found no obvious connection between the minimum of BER and the Lyapunov exponents. We now show how the BER performance is, in fact, controlled by the attractor and invariant measure of the transmitter map.

VI. EXPLANATION OF THE VARIATION IN BER

The variation in BER, observed by the numerical explorations above, may be explained by considering the expression for the BER of an optimal estimator scheme

$$\text{BER} = 1 - \frac{1}{M} \int \cdots \int_{\mathbb{R}^N} \max \{ f_{\sigma_1}(y), \ldots, f_{\sigma_M}(y) \} \, dy$$  \hspace{1cm} (33)$$
as derived in [21].

To reduce the BER for fixed $M$ we must increase

$$I = \int \cdots \int_{\mathbb{R}^N} \max \{ f_{\sigma_1}(y), \ldots, f_{\sigma_M}(y) \} \, dy$$  \hspace{1cm} (34)$$
by manipulating $f_{\sigma}$. Fig. 5 shows the effect of changing density functions (in the case $N = 1$ and $M = 3$) in an idealized scenario. The maximum value of $I$ is equal to $M$.
density functions are disjoint, as shown. As the density functions begin
decreases, since the parts of the
between the two attractors shown in Fig. 6(a) will be
given by (15) in the case of additive noise. In the
where
, then the intersection
is the Dirac delta function), and hence
and only if all the \( M \) density functions are disjoint, as shown
in Fig. 5(a) (where \( BER = 0 \)). As the density functions begin
to overlap, the value of \( I \) decreases, since the parts of the
density functions that are not a maximum do not contribute
to the integral. The amount by which \( I \) decreases is exactly
the integral over the non-maximum portions of the density
functions, shown shaded in Fig. 5. So to minimize BER, we
must minimize this residue integral over the non-maximum
portions of the \( f_\sigma \).

So in order to explain the variation in BER, we must investigate
\( f_\sigma(y) \); given by (15) in the case of additive noise. In
the limit of zero additive noise, we have \( f_{W(w)} \rightarrow \delta(0) \) (where \( \delta \)
is the Dirac delta function), and hence

\[
\begin{align*}
\left( y_2 - G_\sigma(y_1), \ldots, y_N - G_\sigma^{[N-1]}(y_1) \right) = \\
\rho_\sigma(y_1) \delta (y_2 - G_\sigma(y_1), \ldots, y_N - G_\sigma^{[N-1]}(y_1)).
\end{align*}
\]

(35)

Thus in the case of zero noise, the received density function is
just the transmitted attractor, weighted by the invariant measure.
For very small noise, these density functions become blurred,
but essentially look very similar to in the noise free case; the
structure of the attractors is not destroyed. Therefore, to reduce
the BER we must move the attractors further apart, or reduce
the invariant measure where they are close together.

We can now explain the large variation in BER, as the param-
eters of the chaotic transmitter maps change. Fig. 6 shows plots
of the transmitted attractors in the case of the piecewise-linear
map (at the optimal parameter values identified above) and skew
tent maps, and the corresponding invariant densities. They show
that, in the noise free case, the piecewise-linear density func-
tions intersect once, while the tent maps intersect twice. Thus,
in the noise free case, the piecewise-linear maps will provide su-
perior performance to skew tent maps. As noise is introduced,
the attractors will become diffused. This diffusion will cause an
increase in the BER, but since there will be more overlap in the
skew tent map case than for the piecewise-linear map, the latter
will give rise to superior BER performance.

It is also clear from this argument how to improve the BER
performance still further. If, for example, we modify the trans-
mitter map for symbol 0 to be \( G_0(1 - x) \), then the intersection
at \( (0,1) \) between the two attractors shown in Fig. 6(a) will be
removed, and so the residue integral should decrease, and the
BER reduced further.

Heuristically, the further apart the portions of transmitted at-
tractor with high measure, the lower BER. This is an attractive
conclusion, in that it is similar in spirit to ideas in conventional
communication theory, where to maximize discrimination be-
tween transmitted symbols, poles in a constellation diagram are
moved as far apart as possible.

VII. CONCLUSION

In this brief, we have considered the effect of changing the
chaotic transmitter of a chaotic communication scheme. We
use a receiver that explicitly includes the effect of channel
disturbance in its design. To generate the transmitted iterates
we choose a class of piecewise-linear maps whose dynamics
are completely understood.

We have shown that the choice of chaotic attractor is crucial in
determining BER performance. Furthermore, we have proposed
a simple mechanism for the observed variation of BER, in terms
of the transmitted attractors and invariant measure of the trans-
mitter system: the further apart portions of transmitted attractor
with high measure, the lower the BER. Our conclusion is not
restricted to any particular distribution of noise in the channel.

There are many possible areas for further work. Real com-
unication systems work in continuous, not discrete, time, and
it is important to ensure that these ideas are still applicable in
such a setting. The general idea of the optimal estimator should
remain the same; the received data will be in the form of a con-
tinuous function instead of a discrete vector, but this should not
present any problem to the method. Moreover, for a real-world
scheme, we must understand how the performance varies with
other, more realistic channels, perhaps tailoring the statistics of
the transmitted signal to the properties of the channel, leading
to a trade-off in performance versus efficiency. It is also impor-
tant to understand whether our improvement in BER is at the
expense of some other measure of performance such as band-
width efficiency, and how such quantities vary as the chaotic
system is changed.
REFERENCES


