Chaos Communications—Principles, Schemes, and System Analysis

ANDREAS ABEL AND WOLFGANG SCHWARZ, MEMBER, IEEE

Invited Paper

This paper provides a comprehensive overview of chaotic communication methods and schemes with emphasis on digital schemes. Starting from general demands for communications, the general communication system structure is introduced. From this basic viewpoint, different classical and chaotic modulation and demodulation methods are treated and classified. For the performance analysis and comparison, a discrete-time statistical calculus is developed and applied to chaotic signal processing schemes. Discrete-time baseband models are developed, which are suitable for a statistical performance analysis. Analysis results for various example systems are provided and compared. New decoder structures are proposed and included in the comparative studies.

Keywords*—*AWGN performance, chaos communications, cumulant equations, Frobenius–Perron operator, multipath performance, statistical analysis.

I. INTRODUCTION

Chaos communication is a rather new field in the communications research. It evolved from the study of chaotic dynamical systems, not only in mathematics, but also in physics or electrical engineering. In particular engineers and physicists working on such a subject are often asked: "What is this useful for?" One of the ideas, which sparked somewhere at the beginning of the 1990s, was *chaos communications*. There was a straightforward reasoning: chaotic behavior is complex, but nevertheless can be observed in fairly simple dynamical systems. Chaotic signals are irregular, aperiodic, uncorrelated, broad band, and impossible to predict over longer times. These are properties that coincide with requirements for signals applied in communication systems, in particular for spread-spectrum communications, multiuser communications, and secure communications (cryptography). In all the areas, there can be observed an ongoing and growing research interest.

After an idea has developed, it has to be evaluated, its performance has to be quantified, and a comparison with the competitors in the field, i.e., the existing classical solutions to the studied communications problem, has to be made. This will evaluate the applicability, the competitiveness, and the benefits of a chaos-based solution to a communications problem. At its start, the research in chaos communications was mainly concerned about the possibility to map an information signal into a chaotic signal and being able to retrieve it again. The discussions were held primarily from a dynamical system point of view and in the majority dealt with synchronization issues. Since the middle of the 1990s, researchers in chaos communications more and more have adopted the classical communications framework in the choice of methods and measures. The performance analysis of their schemes based on these approaches opened the possibility for a comparison of the new ideas with the classical solutions.

In this paper, we will focus on spread-spectrum communication systems using chaotic signals. The key idea for the exploitation of spread-spectrum signals in communications is to increase the robustness against disturbances affecting narrow frequency ranges. This might be filtering effects introduced by multipath propagations or interfering signals restricted to a narrow frequency range (e.g., periodic signals). Another aspect of spreading the signal power over a wide frequency range is the possibility to transmit signals below the average noise floor. This can be of interest if the transmission power or the power spectral density (psd) in the used frequency band is limited, as, e.g., in unlicensed radio applications. Spectral spreading is also useful, if several users operate in the same frequency range. Of course, a transmission below the noise floor does also provide some kind of secrecy.

Our paper consists of three main parts.

1) Section II introduces the problems faced in communications and motivates the exploitation of chaos for

Manuscript received June 21, 2001; revised November 28, 2001.

The authors are with the Institute for Fundamentals of Electrical Engineering and Electronics, Dresden University of Technology, D-01062 Dresden, Germany (e-mail: abel@iee1.et.tu-dresden.de; schwarz@iee1.et.tu-dresden.de).

Publisher Item Identifier S 0018-9219(02)05248-9.

their solution. The most common chaos communication methods are classified from the point of view of transmitter and receiver design and related to the classical communication methods.

2) Section III provides the theory and the tools for a statistical description and analysis of chaotic systems and chaos communication schemes.
3) Section IV demonstrates the application of these tools to a statistical analysis of example communication schemes under different channel conditions—in particular, additive noise and multipath propagation. Analytical performance figures are derived, which allow a comparison to the classical solutions.

The statistical analysis in Sections III and IV is performed exclusively in discrete time due to the following reasons.

1) There is a well developed statistical calculus for a large class of discrete-time dynamical systems, which allows to perform an in-depth analysis of statistical properties of the generated chaotic signals.
2) For some examples, the methods presented in the paper allow a complete analytical estimation of performance figures based on discrete-time models of the communication scheme.
3) Discrete-time models of communication schemes, which involve the processing of random signals, are much easier to analyze and to simulate. To the knowledge of the authors the vast majority of the continuous-time chaotic systems cannot be analyzed analytically with respect to the statistical properties of the generated signals. For the simulative analysis of continuous-time chaos communication schemes, which has to deal with continuous-time random processes (e.g., channel noise), a special calculus for the treatment of the resulting stochastic differential equations is required (Ito–Stratonovich calculus—a very good example for the application of the calculus to a simulative analysis of a continuous-time chaos communications scheme was given in [1]).

Finally, it has to be noted that the demonstrated methods have their limitations and are not *ad hoc* applicable to all chaos communication schemes. So simulation-based performance evaluations continue to play an important role in the analysis of chaos communication schemes. Nevertheless, an analytical approach should be used whenever possible (at least in parts of the analysis procedure), since the results obtained are far more general and simulations in many cases, such as situations where the bit error rate (BER) of the scheme becomes very low, become extremely time-consuming.

All material in this paper is presented in an overview and tutorial style in order to open the subject to the nonexpert reader. Consequently, not every detail in the sometimes very complicated derivations is given and the reader is referred to the corresponding literature. On the other hand, many points, which are well known from chaotic dynamics and communications, are included for the benefit of readers not very familiar with these topics. In the given limited space, it is virtually impossible to discuss every aspect of chaos in communication schemes, so some topics had to be skipped in favor of a detailed treatment of others. Whenever possible, we tried to at least mention these topics in conjunction with references pointing to relevant material.

II. Communication Fundamentals and Schemes

A. Communication Requirements and Resources

1) Requirements: Communication schemes are technical systems, which transport a message (and, hence, information) from a sender (information source) to a recipient (information sink). Sender and recipient are situated in different locations. A physical media (the channel) in between is used to transport the message. This transport has to be achieved in an *efficient, secure, and robust* manner. These three requirements are implemented in different blocks of a communication scheme.

1) *Efficiency:* The signals susceptible to human beings (sound, pictures, video signals) are analog signals, which show a high amount of redundancy. The same holds for uncompressed digitally stored information such as text, sound, or images. The redundancy implies that a certain percentage of the transmitted message is unnecessary content. Its removal before the transmission, i.e., the formation of an (almost) redundancy-free message, is achieved by a process called *source encoding* [2]. Since the encoding is a digital procedure, it is applicable to digital data and is not present in purely analog schemes.
2) *Security:* The physical media, through which the message is supposed to reach the recipient, is usually public, i.e., accessible to many. If the message is secret or private, one has to prevent unwanted listeners from receiving the message. The solution to the problem is found in cryptography. The message is *encrypted* before the transmission, making an unwanted deciphering impossible or at least hard to achieve [3].
3) *Robustness:* The physical media, through which the transmission has to be achieved, usually will not be able to transmit the given message directly (e.g., a radio channel in the megahertz range cannot directly carry a speech signal with frequencies in the kilohertz region). So, the message is mapped to signals, which can pass the given physical channel. This process is called *modulation*. Further, the channel usually does not provide a one-to-one mapping between the transmitted signal and the signal at the receiver side. Instead, one will observe filtering, nonlinear distortions, and interfering signals (noise, signals from other transmissions), which corrupt the received signal. Consequently, one has to transmit a signal, which is robust against the channel distortions. On one hand, this is achieved by selecting a proper modulation scheme. On the other hand, redundancy can be added to the transmitted message in a controlled way. This controlled redundancy increase is called *channel encoding* and applies to digital communication methods.

All operations performed at the transmitter—source encoding, encryption, channel encoding, and modula-

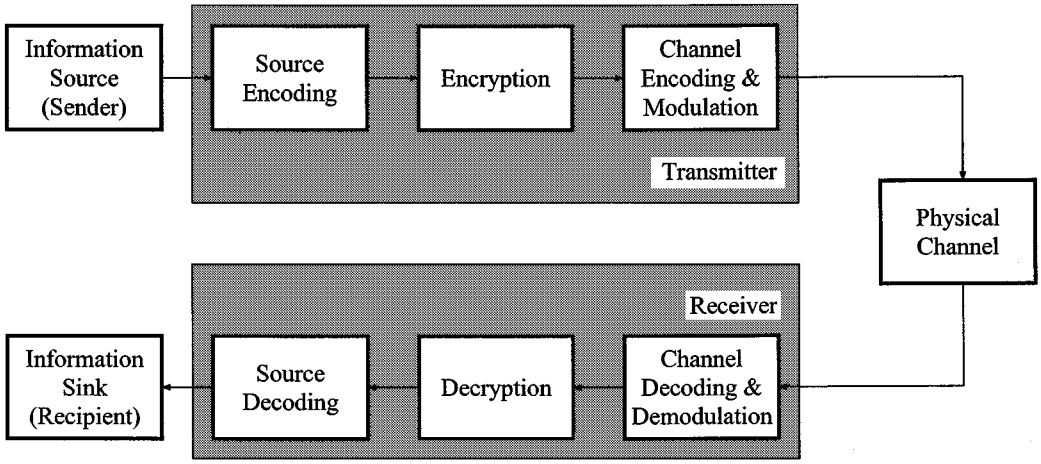

Fig. 1. General structure of a communication scheme.

tion—have to be inverted at the receiver in order to restore the original message. The resulting general structure of communication schemes is shown in Fig. 1.

2) Resource Sharing: Any given physical channel imposes several limitations to signal transmission.

1) *Bandwidth Limitation:* The channel physically provides a limited bandwidth. Further, the bandwidth may be restricted due to technical constraints (capabilities of the used systems) or administrative constraints (bandwidth assignments).
2) *Imperfections:* Channels return a distorted version of the input signal at their output due to linear or nonlinear filtering (attenuations, multipath propagation, delays), noise (from natural and technical sources), and interferences (other signals entering the channel).
3) *Publicity:* Many physical channels are publically accessible, anyone can transmit or receive signals on them.

So, a physical channel has a limited capacity to transmit messages. The sharing of the limited resources is an essential part of the communication system design. The sharing is achieved by means of *orthogonal* signals assigned to each user of a physical channel. The orthogonality ensures the separability of the signals belonging to different users. Two signals $\mathbf{x}_1$ and $\mathbf{x}_2$ are said to be orthogonal, if

$$\int_{-\infty}^{\infty} x_1(t)x_2^*(t)\,dt = 0 \tag{1}$$

where $*$ denotes complex conjugation. Equation (1) implies a vanishing crosscorrelation of $\mathbf{x}_1$ and $\mathbf{x}_2$. The signals have a Fourier representation

$$X_i(\omega) = \int_{-\infty}^{\infty} x_i(t)\exp(j\omega t)\,dt. \tag{2}$$

Due to Parseval's theorem [4]

$$\int_{-\infty}^{\infty} x_1(t)x_2^*(t)\,dt = \frac{1}{2\pi}\int_{-\infty}^{\infty} X_1(\omega)X_2^*(\omega)\,d\omega. \tag{3}$$

So, orthogonality in the time domain implies orthogonality in the frequency domain.

Orthogonality in a multiuser environment can be achieved in different ways.

1) *Signals Disjoint in Time:* If at any time either $x_1(t)$ or $x_2(t)$ becomes zero, (1) holds trivially. This method is termed time division multiple access.
2) *Signals Disjoint in Frequency:* If at any frequency either $X_1(\omega)$ or $X_2(\omega)$ vanishes, the frequency integral in (3) becomes zero. This is termed frequency division multiple access.
3) *Uncorrelated Signals:* Equation (1) can hold even if the signals are neither disjoint in time nor in frequency. This is exploited in code division multiple access (CDMA).

The three methods may be applied in parallel in one communication system (e.g., multiple frequencies with multiple time slots).

B. Potential of Chaos in Communications

The idea to exploit chaos in communication applications has sparked when research in nonlinear dynamical systems had lead to a deeper understanding of the phenomenon and scientists and engineers were looking for practical applications. One can classify three potential application fields, which follow from three different behavioral aspects of chaos.

1) Broad-Band Aspect: Chaotic signals are inherently nonperiodic and as such possess a continuous spectrum. Often, the spectrum shows significant strength over a wide range of frequencies, i.e., the signals are broad band. A design of chaotic signals according to spectral properties is possible [5].

In communications, broad-band signals are used to fight channel imperfections, in particular, narrow-band effects such as frequency-selective fading or narrowband disturbances. So, chaotic signals became candidates for spread-spectrum communications [6].

2) Complexity Aspect: Chaotic signals have a complex structure and are very irregular. One chaos generator will produce a totally different trajectory if it is slightly disturbed in its initial conditions. This makes it difficult to guess the structure of the generator and to predict the signals over longer time intervals.

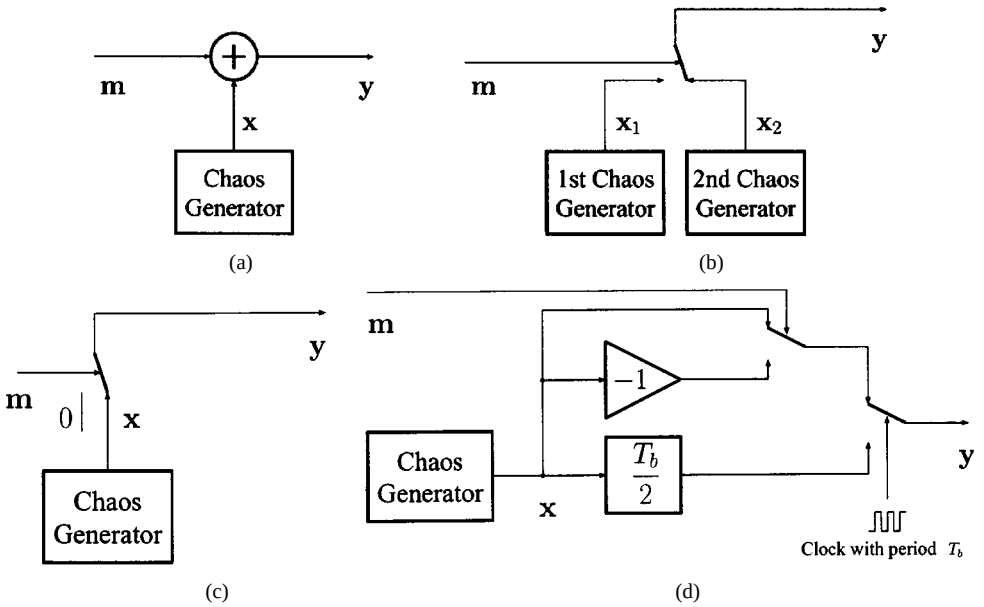

Fig. 2. Chaos communication methods with static encoding/modulation. (a) Masking. (b) CSK (binary). (c) COOK. (d) DCSK.

Highly complex and hard-to-predict signals are classically used in *cryptographic applications*, which opens another potential application field of chaos [7]–[10].

3) Orthogonality Aspect: Chaotic signals are aperiodic and, thus, have a (usually very quickly) vanishing autocorrelation function. Signals generated by different generators or by the same generator with different initial conditions can be assumed to be uncorrelated (orthogonal).

The orthogonality can be exploited in *multiuser communication applications*, which is the third potential application field for chaos. In particular, the generation of spreading codes by chaos generators for conventional CDMA systems has turned out to be a very successful application field, where the chaos-based solution can outperform classical approaches. Since the resulting schemes are classical, we do not treat this topic here. The interested reader is referred to the corresponding literature [11]–[14].

In our paper, we will concentrate on the broad-band aspect and the application of chaos in spread-spectrum systems.

C. Chaotic and Classic Communication Methods

In this section, we will give an overview and classification of the most common chaos communication methods found in the literature. Since different approaches for the design of transmitters and receivers can be combined to a certain extend, we will classify transmitters and receivers separately. This follows the classical approach [15].

1) Transmitter Structures: The application of chaos to spread-spectrum communications considers chaos in the context of channel encoding and modulation. The chaotic methods proposed so far are mainly modulation schemes. Only some ideas concern the application of chaos in channel encoding. As a consequence, we will consider channel encoding and modulation as *one* operation, which maps a message signal (which may be source-encoded and encrypted) to a transmission signal suitable for the given physical channel.

Nevertheless, the classification methods for classical encoding and modulation procedures do also apply. With respect to channel encoding, we find [2]: 1) block encoders (static) and 2) convolutional encoders (dynamic). Block encoders are memoryless with respect to subsequent message blocks, i.e., the current encoding does not depend on previous ones. The encoding is *static with respect to the message*. Convolutional encoders memorize previous message symbols and thus *encode the message dynamically*. There is a similar subdivision for modulation schemes [2]: 1) memoryless modulation methods and 2) modulation methods with memory. Here, memory is meant with respect to the message, too. The two approaches also can be called *static* or *dynamic*.

Merging channel encoding and modulation into one operation, we find: 1) static encoding/modulation schemes and 2) dynamic encoding/modulation schemes. This classification is useful for the statistical analysis of communication schemes discussed in Section III.

a) Static encoding/modulation methods: In static encoding/modulation, the message carrier is provided by a signal source, which is independent of the message. The source may be a deterministic generator with simple dynamics (e.g., periodic), a deterministic generator with complex dynamics (chaos, pseudonoise sequences), or even a random process (noise) generator.

Classical static schemes are the standard modulation methods: amplitude modulation (AM), frequency modulation (FM), and phase modulation (PM).

One of the very first proposals to use chaos in communications is chaotic masking [16], which is applicable to analog and digital messages. Here, the chaotic signal $\mathbf{x}$ is added to the message signal $\mathbf{m}$, forming the transmitted signal $\mathbf{y}$ [see, for example, Fig. 2(a)]

$$y(t) = x(t) + m(t). \tag{4}$$

On its own, this method is not an encoding/modulation, since it does not provide a signal suitable for a given physical channel but is bound to the bandwidth of $\mathbf{m}$. So, $\mathbf{y}$ has to be sent to a modulator before transmission.

Another type of chaotic encoding/modulation is chaos shift keying (CSK) [17]. CSK is a digital modulation method. Depending on the current value of the N-ary message symbol, the signal $x_i(t)$ ($i = 1, \ldots, N$) from one of N chaos generators with different characteristics is transmitted [see, for example, Fig. 2(b)]

$$y(t) = \begin{cases} x_1(t), & \text{if } m(t) = m_1 \\ x_2(t), & \text{if } m(t) = m_2 \\ \cdots & \\ x_N(t), & \text{if } m(t) = m_N \end{cases}. \tag{5}$$

A special case of CSK is the chaotic on–off keying (COOK) [18]. It uses one chaos generator, which is switched on or off according to a binary message symbol to be transmitted [see, for example, Fig. 2(c)]

$$y(t) = \begin{cases} 0, & \text{if } m(t) = m_1 \\ x(t), & \text{if } m(t) = m_2 \end{cases}. \tag{6}$$

A method found in classical communications as well as in chaos communications is the transmitted reference (TR) approach. It was designed to be used with a correlation receiver, but the method applies to any system requiring a reference in the receiver. The reference is transmitted on a separate channel (different wire, frequency band, or time slot) and, thus, does not need to be reproduced in the receiver. Compared to the so-called stored reference (SR) methods, where the reference is locally stored or generated at the receiver, half of the transmission capacity (the reference transmission) is not exploited for information transmission. So, SR schemes [e.g., phase shift keying (PSK) methods] achieve twice the bit rate using the same resources.

The TR scheme can be applied if the message carrier is a complicated signal, which cannot be recreated easily. In the early days of spread-spectrum communications, TR methods were studied with natural noise sources as signal generators [19]. In chaos communications, the principle is exploited in differential CSK (DCSK) [20]. In DCSK, the two channels are formed by time division. For every message symbol, first the reference signal is transmitted, followed by the modulated reference carrying the message symbol. For a binary message stream with symbol duration T_b, the transmitted signal becomes [see, for example, Fig. 2(d)]

$$y(t) = \begin{cases} x(t), & \text{if } kT_b \le t < \dfrac{2k+1}{2} T_b \\ x\left(t - \dfrac{T_b}{2}\right), & \text{if } \dfrac{2k+1}{2} T_b \le t < (k+1)T_b \\ & \text{and } m(t) = m_1 \\ -x\left(t - \dfrac{T_b}{2}\right), & \text{if } \dfrac{2k+1}{2} T_b \le t < (k+1)T_b \\ & \text{and } m(t) = m_2 \end{cases}. \tag{7}$$

for any $k \in \mathbb{Z}$.

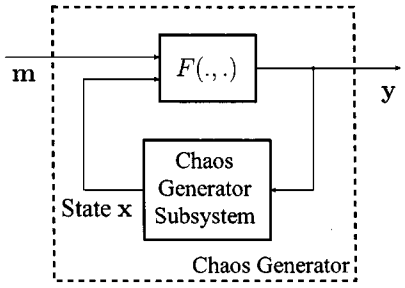

Fig. 3. Example structure for a CM scheme.

In digital communications, signal space concepts play an important role in the performance analysis [2], [4]. Statically encoding/modulating schemes map every message symbol to a different waveform. Depending on the relationship of the waveforms in signal space, there are *antipodal* and *orthogonal* schemes. These are very well studied in general [4]. Chaotic schemes can be designed such that they are antipodal or orthogonal, too. The classical knowledge can be used to establish lower bounds on the performance of the schemes [21], [22], but, since the chaotic schemes use more complex signals, a further analysis is required to obtain exact performance figures (see Section IV).

b) Dynamic encoding/modulation methods: In dynamic encoding/modulation methods, the mapping of the message to its carrier depends on past message symbols. This dependence is created by:

1) feeding the message and the message carrier into a dynamical system, which memorizes the prehistory of the message;
2) feeding the message into the carrier generator such that the generator itself memorizes the prehistory of the message.

The first approach becomes a special case of the second, if the dynamical system is considered as part of the message carrier generator.

Classical examples are schemes using convolutional channel encoders [2], [23] and differential modulation methods such as differential PSK (DPSK).

A chaotic example for the second approach is chaotic modulation (CM) [24], where the message modulates some parameter of a chaos generator. For a continuous-time transmitter, the state equations are

$$\dot{x}(t) = g(x(t), m(t)) \tag{8a}$$
$$y(t) = h(x(t), m(t)) \tag{8b}$$

where $\dot{x}(t)$ is the time derivative of $x(t)$. If $\mathbf{m}$ is discrete-valued (e.g., binary), the method is called chaotic switching (CS) [25]. Fig. 3 shows an example, where the state feedback in a chaos generator is modulated.

Another method encodes the message into the symbolic dynamics of a chaos generator [26]. Symbolic dynamics are obtained if the state space of the generator is completely partitioned into disjoint subsets, which are assigned with symbols. The sequence of symbols corresponding to a trajectory in the state space is the symbolic dynamics of that trajectory. Methods of chaos control allow a chaos generator

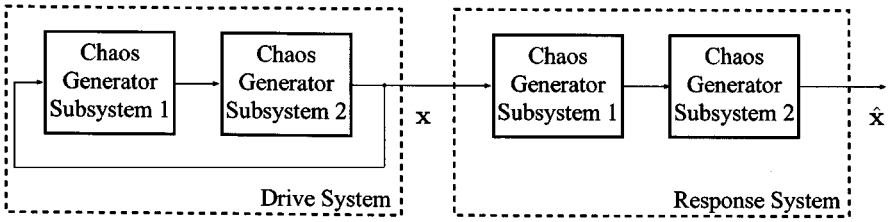

Fig. 4. Drive-response synchronization principle.

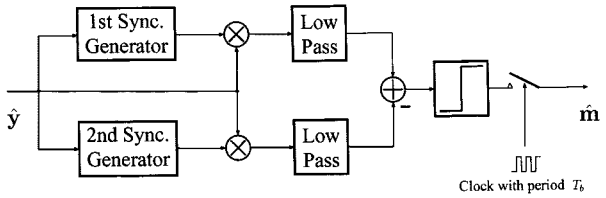

Fig. 5. Correlation-based CSK receiver.

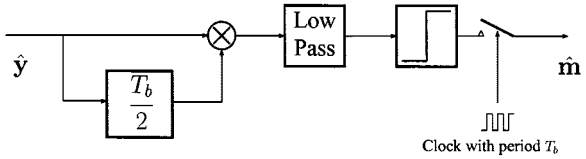

Fig. 6. DCSK receiver.

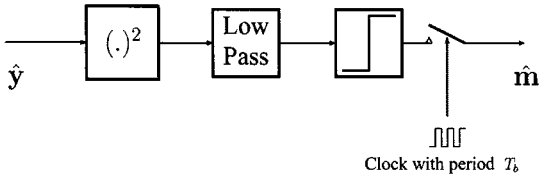

Fig. 7. COOK receiver.

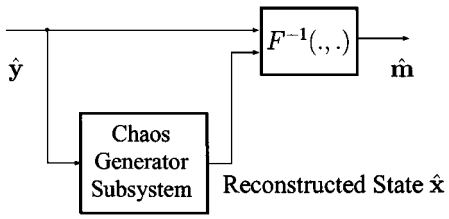

Fig. 8. Inverse structure for Fig. 3.

to be forced to a particular symbolic sequence. This can be exploited, if it happens in accordance with the message sequence.

2) Receiver Structures: For the reception of a message, in particular in chaos communications, there exist three possible methods:

1) using a reference signal;
2) analysis of the statistics of the received signal;
3) inverse system techniques.

A reference signal is used in correlation receivers and in chaotic masking for subtraction.

References can be provided by a local generator in the receiver (synchronized to the generator in the transmitter) or by a matched filter impulse response (only feasible for periodic signals). These techniques are termed SR methods. Otherwise, the reference has to be transmitted in addition to the actual message-carrying signal (TR methods).

Local references for a chaotic signal can be obtained in different ways. One method is the drive-response synchronization principle [27]. It applies to chaos generators decomposable into two subsystems, which are feedback-coupled to each other. Opening the feedback loop allows to reproduce the chaotic signal from a distorted input via the cascade of subsystems (see Fig. 4).

Another tool for obtaining a reference is provided by chaos control methods [28], [29]. Here, a copy of the transmitter's chaos generator is guided toward the received chaotic signal by a control signal derived from the error between the received and the locally generated signal.

Detection via a reference can be applied in receivers for CSK, DCSK, CS, and chaotic masking. Fig. 5 shows an example for a CSK correlation receiver. In the receiver, two synchronizable systems match the chaotic systems in the transmitter. If one of them is excited by its own signal $\mathbf{x}_i$, it synchronizes and reproduces a correlated copy $\hat{\mathbf{x}}_i$. The other does not synchronize and emits a less correlated signal. The larger of the two correlation values identifies the transmitted message symbol.

In Fig. 6, the correlation receiver of a DCSK scheme is shown. The reference is obtained by delaying the received signal by T_b.

An analysis of the statistics is possible, if statistical characteristics of the received signal show a one-to-one dependence on the transmitted message. Such a receiver contains an estimator for the particular characteristic. An application example is the COOK scheme, where the on–off keying is visible in the change in the average power of the received signal (see Fig. 7). So, the received power is estimated in the receiver. The decision is biased, since the noise power shifts the optimum decision level. The analysis of statistics is also applicable to CSK and CS, if there are significant changes in a characteristic.

Finally, inverse systems [30] provide a reception method for CM. In an inverse system, the flow of the message through the dynamical system in the transmitter is reversed. Obeying certain stability conditions this provides the inverse of the modulation operation. An example structure is shown in Fig. 8. A convergence of $\hat{\mathbf{x}}$ toward $\mathbf{x}$ is required for the system to operate.

The described receiver structures are the most commonly used and described ones. There exist further methods, which design optimum receivers and do not necessarily fit into the framework described here. They require considerably more complex structures and computational effort, but usually lead

to a better performance. This optimum receiver design is extensively treated in another paper in this issue [31].

3) Implementation Examples: By now, some chaos communication schemes have already been implemented and tested under nonideal channel conditions in order to show the applicability of chaos to communication problems:

1) inverse-system-based chaotic encryption scheme with indoor radio transmission (experimental demonstration) [9];
2) inverse-system-based communication scheme (wire link, digital-signal processor implementation) [32];
3) chaotic pulse position modulation scheme (indoor radio transmission) [33];
4) CDMA system using chaotically generated codes (wire link, multiuser) [34];
5) COOK scheme (indoor radio transmission) [35];
6) frequency-modulated DCSK (radio link via channel simulator) [36].

III. Statistical Analysis—Methods and Tools

In this paper, we want to evaluate the performance of chaos communication schemes based on statistical analysis. Thus, all signals (message, message carrier, interfering signals) have to be modeled by random processes. The signal processing, i.e., the system composed of transmitter, channel, and receiver, is assumed to be deterministic. The analysis requires three tasks to be performed:

1) stochastic modeling of all involved signals, in particular, the chaotic ones;
2) analysis of the transformation of random signals through nonlinear deterministic systems;
3) estimation of performance figures (e.g., BER) from stochastic characteristics.

The tools for Tasks 1 and 2 are provided in this section; Task 3 is discussed in Section IV.

Task 1 is solved using the Frobenius–Perron operator (FPO) theory. The FPO is a valuable tool for the estimation of statistical properties of chaotic signals. Its properties and applications are introduced in Section III-B.

Task 2 is solved using methods, which describe the transformation of statistical characteristics, in particular, moments and cumulants, by nonlinear dynamical systems. The key tool to be introduced are the so-called cumulant equations (see Section III-C).

Let us start with some statistical preliminaries.

A. Fundamentals

Assume a set of continuous-valued random variables (i.e., a random vector) $\mathbf{X} = (X_1, \ldots, X_n)$. They are described by a joint probability density function (pdf) $f_{\mathbf{X}}(\mathbf{x}) = f_{\mathbf{X}}(x_1, \ldots, x_n)$. The moments of $\mathbf{X}$ of order $\mathbf{q} = (q_1, \ldots, q_n)$, $q_i \geq 0$ are the expectation values

$$\begin{aligned}\alpha_{\mathbf{X}}^{\mathbf{q}} &= E[X_1^{q_1} \cdots X_n^{q_n}] \\ &= \int_{\mathbf{x}\in\mathbb{M}} x_1^{q_1} \cdots x_n^{q_n} f_{\mathbf{X}}(\mathbf{x})\, d\mathbf{x} \end{aligned} \tag{9}$$

where $\mathbb{M}$ is the domain of the random vector $\mathbf{X}$, usually $\mathbb{R}^n$ or $\mathbb{C}^n$. The characteristic function [37], [38]

$$\begin{aligned}&\Phi_{\mathbf{X}}(\omega_1, \ldots, \omega_n) \\ &\quad = E[\exp(j\omega_1 X_1 + \cdots + j\omega_n X_n)] \\ &\quad = \int_{\mathbf{x}\in\mathbb{M}} \exp(j\omega_1 x_1 + \cdots + j\omega_n x_n) f_{\mathbf{X}}(\mathbf{x})\, d\mathbf{x} \end{aligned} \tag{10}$$

is a Fourier transform representation of $f_{\mathbf{X}}$. The moments (9) follow from $\Phi_{\mathbf{X}}$ as the coefficients of an n-dimensional Taylor series expansion in the $j\omega_i$ around the origin [38]

$$\Phi_{\mathbf{X}}(\omega_1, \ldots, \omega_n) = \sum_{\mathbf{q}} \frac{\alpha_{\mathbf{X}}^{\mathbf{q}}}{q_1! \cdots q_n!} (j\omega_1)^{q_1} \cdots (j\omega_n)^{q_n} \tag{11}$$

where $\alpha_{X_1, \ldots, X_n}^{0, \ldots, 0} = 1$. So, $\Phi_{\mathbf{X}}$ is also called the moment-generating function.

The cumulants $\varkappa_{\mathbf{X}}^{\mathbf{q}}$ of $\mathbf{X}$ follow similarly to (11) from the cumulant-generating function $\Psi_{\mathbf{X}} = \ln(\Phi_{\mathbf{X}})$ [38]

$$\Psi_{\mathbf{X}}(\omega_1, \ldots, \omega_n) = \sum_{\mathbf{q}} \frac{\varkappa_{\mathbf{X}}^{\mathbf{q}}}{q_1! \cdots q_n!} (j\omega_1)^{q_1} \cdots (j\omega_n)^{q_n} \tag{12}$$

where $\varkappa_{X_1, \ldots, X_n}^{0, \ldots, 0} = 0$. Cumulants are in particular useful due to their special properties.

1) Addition of a constant to a random variable keeps all but the first cumulant unchanged.
2) Gaussian pdfs have cumulants of first and second order (mean values, autocovariances, and crosscovariances) only, i.e., the pdf is fully described by a limited set of cumulants.
3) Joint cumulants of independent variables vanish (e.g., $\varkappa_{X_1, X_2}^{q_1, q_2} = 0$ for independent X_1, X_2).
4) The cumulant of a sum of independent variables is the sum of the respective cumulants of the variables (e.g., $\varkappa_{X_1+X_2}^{q} = \varkappa_{X_1}^{q} + \varkappa_{X_2}^{q}$).
5) Cumulants are transformed separately by linear systems (i.e., the nth order input cumulant affects the nth order output cumulant only).

These properties are of interest, since in communication systems the message, message carrier, and noise signals usually can be assumed to be statistically independent. Also, Gaussian noise is a widely used model for the noise influences on the channel.

There exists a close relationship between moments and cumulants—a moment of order $\mathbf{q}$ depends on cumulants of order up to $\mathbf{q}$ and vice versa [38]. The most convenient way to calculate one from the other are recursive relationships [39], since the explicit expressions get complicated very quickly.

Having a description of random vectors via moments and cumulants, the extension to random processes (and, thus, random signals) is straightforward. Random processes are infinite-dimensional random vectors indexed by the time variable. Many well known signal characteristics are nothing else but moment or cumulant functions of a random process:

1) mean $\alpha_{X(t)}^{1} = \varkappa_{X(t)}^{1}$;
2) autocorrelation function $\alpha_{X(t_1), X(t_2)}^{1,1}$;

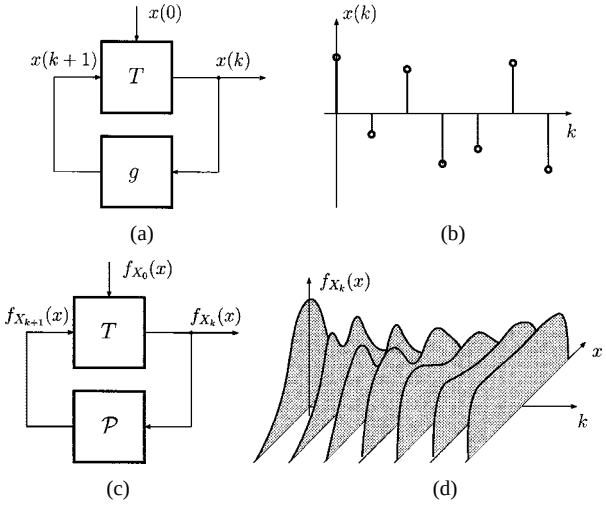

Fig. 9. State-space and density-space models of a dynamical system. (a) State-space model. (b) State-space trajectory (sequence of values). (c) Density space model. (d) Density space trajectory (sequence of pdf's).

3) cross-correlation function $\alpha^{1,1}_{X_1(t_1),\,X_2(t_2)}$;
4) autocovariance $\varkappa^{1,1}_{X(t_1),\,X(t_2)}$;
5) cross covariance $\varkappa^{1,1}_{X_1(t_1),\,X_2(t_2)}$.

B. Statistical Analysis of Chaotic Systems and Signals

Now, we construct a stochastic model of the chaotic signals involved in the chaos communication schemes. Chaotic signals are deterministic, but many of their properties make them already look like realizations of random processes (e.g., lack of long-term predictability, continuous spectrum, etc.). In order to get a proper model, we randomize the initial condition x_0 of the chaos generator and assign it with a pdf $f_{X_0}(x_0)$. Now, assume a discrete-time chaotic generator (for the continuous-time counterpart the derivation is equivalent)

$$x(k+1) = g(x(k)), \qquad x(0) = x_0. \tag{13}$$

If every of the initial conditions with pdf f_{X_0} undergoes one iteration of g, we obtain a new set of values $x_1 = x(1)$, which have a pdf $f_{X_1}(x_1)$. The possible x_1 are now realizations of a random variable X_1. The sequence $X_0, X_1, \ldots, X_n, \ldots$ of random variables generated this way is a random process.

Instead of the state-space model (13), we can equivalently use a model in the space of pdfs, since the deterministic map g implies a relationship between the subsequent pdfs

$$f_{X_{k+1}}(x) = \mathcal{P}(f_{X_k}(x)), \qquad \text{initial pdf } f_{X_0}(x). \tag{14}$$

The operator $\mathcal{P}$ iterating the pdf is called the FPO [40]. Its action is illustrated in Fig. 9. Introducing the distribution function F, which is the integral over f, the FPO can be linked to the map g

$$\begin{aligned} f_{X_{k+1}}(x) &= \frac{d}{dx} F_{X_{k+1}}(x) \\ &= \frac{d}{dx} P\{X_{k+1} < x\} = \frac{d}{dx} P\{g(X_k) < x\} \\ &= \frac{d}{dx} \int_{g(x')<x} f_{X_k}(x')\, dx' = \mathcal{P}(f_{X_k}(x)). \end{aligned} \tag{15}$$

The FPO is a linear operator. It has an integral representation

$$\begin{aligned} &f_{X_{k+1}}(x) \\ &\quad = \int_{\mathbb{M}} f_{X_{k+1}|X_k}(x|x') f_{X_k}(x')\, dx' \\ &\int_{\mathbb{M}} \delta(x - g(x')) f_{X_k}(x')\, dx' \\ &\quad = \mathcal{P}(f_{X_k}(x)) \end{aligned} \tag{16}$$

where $\mathbb{M}$ is the domain of x and δ is the delta function. δ appears because g is deterministic, i.e., knowing a particular x at time $k+1$, all the preimages under g are determined.

The FPO has some fundamental properties.

1) *Linearity:* The superposition principle holds.
2) *Invariance on Densities:* The application of $\mathcal{P}$ to a pdf again results in a pdf.
3) *Eigensystems:* As a linear operator $\mathcal{P}$ can be represented in terms of eigenfunctions and corresponding eigenvalues.

Knowing the FPO, statistical properties of the chaotic sequence generated by g can be derived. If the FPO has a fixed point, then this is an invariant density of the map g. If there is only a single and stable fixed point, the process is ergodic and mixing [40]. This property holds for almost all initial conditions. This means that averages calculated from f_{X_k} are the same as averages calculated from a single time series.

The FPO is well studied for quite a few classes of maps. For the communication system examples discussed later on, we will focus on one particular type of maps—one-dimensional (1-D) piecewise-linear fully stretching maps. These are maps g with the following properties.

1) The map is an onto map of an interval $I = [x_{\min}, x_{\max}]$.
2) There exists a partition (set of n disjoint intervals I_i, $n > 1$) such that the union of the I_i is I and the map g maps every I_k onto the whole I.
3) At each interval, the map is described by an affine function $g_i(x) = a_i x + b_i$.

We start from the FPO (15) applied to an arbitrary function h defined on I [I coincides with $\mathbb{M}$ in (16)]

$$\begin{aligned} \mathcal{P}(h(x)) &= \frac{d}{dx} \int_{g(x')<x} h(x')\, dx' \\ &= \frac{d}{dx} \sum_{i=1}^{n} \int_{g_i^{-1}([x_{\min},\, x))} h(x')\, dx' \end{aligned} \tag{17}$$

where $g_i^{-1}([x_{\min}, x))$ denotes the preimage of the interval $[x_{\min}, x)$ under g_i. Applying some straightforward transformations, the FPO can be described in terms of the parameters a_i and b_i

$$\mathcal{P}(h(x)) = \sum_{i=1}^{n} \frac{1}{|a_i|}\, h\left(\frac{x}{a_i} - \frac{b_k}{a_i}\right). \tag{18}$$

The FPO has the uniform density on I as its only stable fixed point. So, the sequences generated from almost all initial conditions are also uniformly distributed on I and ergodic. If h is an mth order polynomial, $\mathcal{P}(h)$ also will be an mth order

polynomial. So, the FPO is invariant on spaces of polynomials of order m.

The Koopman operator (KO) is the adjoint operator of the FPO. It will be introduced in the sequel [40]. Assume a random process $\mathbf{X}$ generated by the map g with the initial pdf f_{X_0}. The expectation of a function h of X_k (i.e., of the process at time instant k) is

$$E[h(X_k)] = \int_{\mathbb{M}} h(x) f_{X_k}(x)\, dx = \langle h,\, f_{X_k} \rangle. \tag{19}$$

where f_{X_k} can be expressed via the FPO and the initial pdf as $\mathcal{P}^k(f_{X_0})$. Equivalently, knowing that the generating map is g, we can express the expectation as

$$E[h(X_k)] = \int_{\mathbb{M}} h(g^k(x)) f_{X_0}(x)\, dx = \langle h \circ g^k,\, f_{X_0} \rangle. \tag{20}$$

The application of h to the k-fold iteration ($k = 1, 2, \ldots$) of g defines the KO

$$\mathcal{U}^k(h) = h \circ g^k. \tag{21}$$

The adjoint operators FPO and KO are related by

$$\langle \mathcal{U}^k(h),\, f \rangle = \langle h,\, P^k(f) \rangle. \tag{22}$$

It can be seen from (21) that the k-fold application of $\mathcal{U}$ achieves a time shift of the process $\mathbf{X}$. With respect to products of functions, the KO possesses a shift property

$$\begin{aligned} \mathcal{U}^{k_1}(h_1)\mathcal{U}^{k_2}(h_2) &= (h_1 \circ g^{k_1})(h_1 \circ g^{k_1}) \\ &= (h_1 \circ g^{k_1})(h_1 \circ g^{k_1} \circ g^{k_2-k_1}) \\ &= \mathcal{U}^{k_1}(h_1 \mathcal{U}^{k_2-k_1}(h_2)) \end{aligned} \tag{23}$$

with $k_2 \geq k_1 \geq 0$. Their properties allow the use of KO and FPO for the estimation of correlation functions of the stochastic process $\mathbf{X}$ associated with a chaotic map g. For example, the second-order correlation function calculates as

$$\begin{aligned} E[X_0 X_{k_1} X_{k_2}] &= \alpha^{1,1,1}_{X_0, X_{k_1}, X_{k_2}} \\ &= \langle x g^{k_1}(x) g^{k_2}(x),\, f_{X_0}(x) \rangle \\ &= \langle \mathcal{U}^{k_1}(x) \mathcal{U}^{k_2}(x),\, x f_{X_0}(x) \rangle \\ &= \langle \mathcal{U}^{k_1}(x U^{k_2-k_1}(x)),\, x f_{X_0}(x) \rangle \\ &= \langle x U^{k_2-k_1}(x),\, \mathcal{P}^{k_1}(x f_{X_0}(x)) \rangle \\ &= \langle x,\, \mathcal{P}^{k_2-k_1}(x \mathcal{P}^{k_1}(x f_{X_0}(x))) \rangle \end{aligned} \tag{24}$$

in terms of the FPO. It is determined from the knowledge of f_{X_0} and the FPO. A further example will be shown in Section IV-C1.

C. Processing of Chaotic and Random Signals

The second set of tools needed for the analysis of chaos communication schemes are those that describe the processing of random signals in deterministic systems. This problem is solved for the class of linear time-invariant systems [38]. However, transmitters and receivers in chaos communication schemes are usually nonlinear.

1) Moment Transformation on Polynomial Nonlinearities: If the output of the processing scheme calculates as a polynomial of several input values (values of the input signals at different time instants), the operator rules of the expectation value operator can be applied.

Take as an example the following system description:

$$y_k = x_{k-1} x_{k-2} + x_k + \eta_k \tag{25}$$

where $\mathbf{x}$ and η are realizations of random processes. Consequently, $\mathbf{y}$ is also a random process realization. Obviously

$$\begin{aligned} \alpha^1_{Y_k} &= E[Y_k] = E[X_{k-1} X_{k-2}] + E[X_k] + E[\eta_k] \\ &= \alpha^{1,1}_{X_{k-1}, X_{k-2}} + \alpha^1_{X_k} + \alpha^1_{\eta_k} \end{aligned} \tag{26}$$

$$\begin{aligned} \alpha^2_{Y_k} &= E[Y_k^2] \\ &= \alpha^{2,2}_{X_{k-1}, X_{k-2}} + \alpha^2_{X_k} + \alpha^2_{\eta_k} \\ &\quad + 2(\alpha^{1,1,1}_{X_{k-1}, X_{k-2}, X_k} + \alpha^{1,1,1}_{X_{k-1}, X_{k-2}, \eta_k} + \alpha^{1,1}_{X_k, \eta_k}). \\ &\quad \ldots \end{aligned} \tag{27}$$

These relations can be simplified by taking into account the properties of $\mathbf{X}$ and η. For instance, η might be zero-mean ($\alpha^1_{\eta_k} = 0$), η and $\mathbf{X}$ might be independent ($\alpha^{1,1,1}_{X_{k-1}, X_{k-2}, \eta_k} = \alpha^{1,1}_{X_{k-1}, X_{k-2}} \alpha^1_{\eta_k} = 0$), etc. Using the appropriate relationships, from the moment relations, the cumulant relations and the mixed moment-cumulant relations can be obtained. This method is limited to polynomial dependencies. In order to obtain a certain moment, one first has to expand the polynomial term into a sum, which addends then can be rewritten in terms of moments. After this, the properties of the involved signals (such as vanishing moments, independence, stationarity, etc.) can be taken into account in order to simplify the obtained expressions. Albeit the resulting expressions may turn out to be fairly simple, the first step of the moment expansion may lead to very complicated expressions for higher order moments. This is a disadvantage of the approach.

2) Cumulant Equations: An approach, which is not limited to polynomial dependencies, are cumulant equations [37]. They allow to calculate partial derivatives of output moments of a system by cumulants of the input variables. These partial derivatives form the coefficients of a Taylor series expansion of the output moments in terms of the input cumulants and thus (under certain prerequisites) allow to calculate output moments as functions of input cumulants.

Let us start with the simple example of a nonlinear function $Y = h(X)$, where X and Y are real-valued random variables. X and Y can be understood as the input and output of the static nonlinearity h. The expectation of Y calculates as

$$E[h(X)] = \int_{-\infty}^{\infty} h(x) f_X(x)\, dx \tag{28}$$

which, using the characteristic function $\Phi_X(\omega) = \exp(\Psi_X(\omega))$ (i.e., the Fourier transform of f_X), becomes

$$E[h(X)] = \int_{-\infty}^{\infty} h(x) \frac{1}{2\pi} \int_{-\infty}^{\infty} \exp(-j\omega x) \cdot \exp(\Psi_X(\omega))\, d\omega\, dx. \tag{29}$$

Now, we determine the dependence of $E[h(X)]$ on particular cumulants of X, i.e., we calculate the partial derivatives

$\partial^k E[h(X)]/\partial(\varkappa_X^q)^k$. Based on (12) (1-D case) it is easy to show that

$$\begin{aligned}\frac{\partial^k \exp(-j\omega x+\Psi_X(\omega))}{\partial(\varkappa_X^q)^k}&=\left(\frac{(j\omega)^q}{q!}\right)^k \exp(-j\omega x+\Psi_X(\omega))\\&=\frac{(-1)^{kq}}{(q!)^k}\frac{\partial^{kq}\exp(-j\omega x+\Psi_X(\omega))}{\partial x^{kq}}.\end{aligned}\tag{30}$$

Introducing this result into (29), after a few transformations, one obtains

$$\frac{\partial^k E[h(X)]}{\partial(\varkappa_X^q)^k}=\frac{(-1)^{kq}}{(q!)^k}\int_{-\infty}^{\infty}h(x)\frac{\partial^{kq}f_X(x)}{\partial x^{kq}}\,dx.\tag{31}$$

Using the rules for partial integration and keeping in mind that all derivatives of f_X vanish at infinity since f_X is a pdf, after kq partial integration steps, we obtain

$$\frac{\partial^k\alpha_Y^1}{\partial(\varkappa_X^q)^k}=\frac{\partial^k E[h(X)]}{\partial(\varkappa_X^q)^k}=\frac{1}{(q!)^k}E\left[\frac{d^{kq}h(X)}{dX^{kq}}\right].\tag{32}$$

This is the so-called cumulant equation for the 1-D case. It relates the partial derivatives of the output moment α_Y^1 by the input cumulant $\varkappa_X^q$ to expectations of derivatives of the nonlinearity h. The joint derivatives with respect to several cumulants are derived in the same manner. These expressions represent the coefficients of a Taylor series expansion of $\alpha_Y^1=E[h(X)]$ in the cumulants of X. The most suitable expansion point is the one where all cumulants are zero ($\varkappa_X^q=0$ for all q). This expansion point in the space of cumulants corresponds to a pdf $f_X(x)=\delta(x)$. The expectation on the right-hand side in (32) has to be calculated according to this particular pdf. This is straightforward—one simply has to calculate the expression in the square brackets at $x=0$.

In exactly the same manner, one derives cumulant equations for systems with multiple inputs and consequently multivariate pdfs of the input signals

$$\begin{aligned}\frac{\partial^{k_1+\cdots+k_N}\alpha_Y^r}{(\partial\varkappa_{\mathbf{X}}^{\mathbf{q}_1})^{k_1}\cdots(\partial\varkappa_{\mathbf{X}}^{\mathbf{q}_N})^{k_N}}&=\frac{1}{(\mathbf{q}_1!)^{k_1}\cdots(\mathbf{q}_N!)^{k_N}}\\&\cdot E\left[\frac{\partial^{(q_{11}+\cdots+q_{1n})k_1+\cdots+(q_{N1}+\cdots+q_{Nn})k_N}h^r(\mathbf{X})}{\partial X_1^{q_{11}k_1+\cdots+q_{N1}k_N}\ldots\partial X_n^{q_{1n}k_1+\cdots+q_{Nn}k_N}}\right]\end{aligned}\tag{33}$$

where $\mathbf{X}=(X_1,\ldots,X_n)$, $\mathbf{q}_i=(q_{i1},\ldots,q_{in})$, and $\mathbf{q}_i!=q_{i1}!\ldots q_{in}!$.

As almost all calculations involving random variables, the derivation of output moments via cumulant equations is a tedious task. Nevertheless, the special properties of the cumulants help to reduce the effort considerably.

1) We do not have to care about cumulants which are zero (i.e., cumulants of order >2 of Gaussian variables, joint cumulants of independent variables).
2) The structure of h may further reduce the required effort. Only nonzero derivatives of h at $\mathbf{X}=\mathbf{0}$ on the right-hand side of a cumulant equation have to be taken into account. Zero derivatives cancel the influence of the corresponding cumulant.
3) If h is a polynomial in the X_i, derivatives in X_i vanish from a certain order upwards. Only a finite number of derivatives has to be calculated and the expression for the moments of Y will be a finite Taylor series, i.e., expectations of powers of Y are exactly representable. This property conceptually coincides with the moment property in Section III-C1.

Let us now consider a simple example, which was given in [7]

$$Y=h(X_1,X_2,X_3)=X_1^3+aX_2^2X_3.\tag{34}$$

Assume we are interested in the first moment $\alpha_Y^1=E[h(X_1,X_2,X_3)]$. Without knowledge about the cumulants of X_1, X_2, and X_3, a Taylor series expansion would have to be calculated in *all* cumulants of the inputs, which is virtually impossible. However, from the properties above, we know that only nonzero derivatives of h at $\mathbf{X}=\mathbf{0}$ result in a nonzero partial derivative of α_Y^1 by cumulants of the inputs. All other partial derivatives can be neglected in the calculations.

There are seven nonvanishing partial derivatives of h at $(X_1,X_2,X_3)=(0,0,0)$. The first one leads $\partial^3\alpha_Y^1/\partial(\varkappa_{X_1}^1)^3$ according to (33)

$$\frac{\partial^3\alpha_Y^1}{\partial(\varkappa_{X_1}^1)^3}=\frac{1}{(1!)^3}\cdot E\left[\frac{\partial^3 h(X_1,X_2,X_3)}{\partial X_1^3}\right]=6\tag{35}$$

the other partial derivatives are calculated equivalently as

$$\begin{aligned}\frac{\partial^2\alpha_Y^1}{\partial\varkappa_{X_1}^1\,\partial\varkappa_{X_1}^2}&=3 & \frac{\partial\alpha_Y^1}{\partial\varkappa_{X_1}^3}&=1\\\frac{\partial^3\alpha_Y^1}{\partial(\varkappa_{X_2}^1)^2\,\partial\varkappa_{X_3}^1}&=2a & \frac{\partial^2\alpha_Y^1}{\partial\varkappa_{X_2}^2\,\partial\varkappa_{X_3}^1}&=a\\\frac{\partial^2\alpha_Y^1}{\partial\varkappa_{X_2,X_3}^{1,1}\,\partial\varkappa_{X_2}^1}&=2a & \frac{\partial\alpha_Y^1}{\partial\varkappa_{X_2,X_3}^{2,1}}&=a.\end{aligned}\tag{36}$$

The corresponding Taylor series reads as (nonvanishing terms only)

$$\begin{aligned}\alpha_Y^1&=\frac{1}{3!}\frac{\partial^3\alpha_Y^1}{\partial(\varkappa_{X_1}^1)^3}+\frac{\partial^2\alpha_Y^1}{\partial\varkappa_{X_1}^1\,\partial\varkappa_{X_1}^2}\\&\quad+\frac{\partial\alpha_Y^1}{\partial\varkappa_{X_1}^3}+\frac{1}{2!}\frac{\partial^3\alpha_Y^1}{\partial(\varkappa_{X_2}^1)^2\,\partial\varkappa_{X_3}^1}\\&\quad+\frac{\partial^2\alpha_Y^1}{\partial\varkappa_{X_2}^2\,\partial\varkappa_{X_3}^1}+\frac{\partial^2\alpha_Y^1}{\partial\varkappa_{X_2,X_3}^{1,1}\,\partial\varkappa_{X_2}^1}+\frac{\partial\alpha_Y^1}{\partial\varkappa_{X_2,X_3}^{2,1}}\\&=\varkappa_{x_1}^1{}^3+3\varkappa_{x_1}^1\varkappa_{x_1}^2+\varkappa_{x_1}^3\\&\quad+a(\varkappa_{x_2}^1{}^2\varkappa_{x_3}^1+\varkappa_{x_2}^2\varkappa_{x_3}^1+2\varkappa_{x_2,x_3}^{1,1}\varkappa_{x_2}^1+\varkappa_{x_2,x_3}^{2,1}).\end{aligned}\tag{37}$$

All the described tools require a considerable effort in their application to existing chaos communication schemes. Nevertheless, the application is possible and leads to a deep insight into the behavior and potentials of chaos communication methods. This will be demonstrated in the Section IV.

Apart from their usefulness, the described methods have a limitation, which restricts the classes of systems, to which they can be applied: *There must be an explicit relationship between the input signals and the output signal(s).* So, the

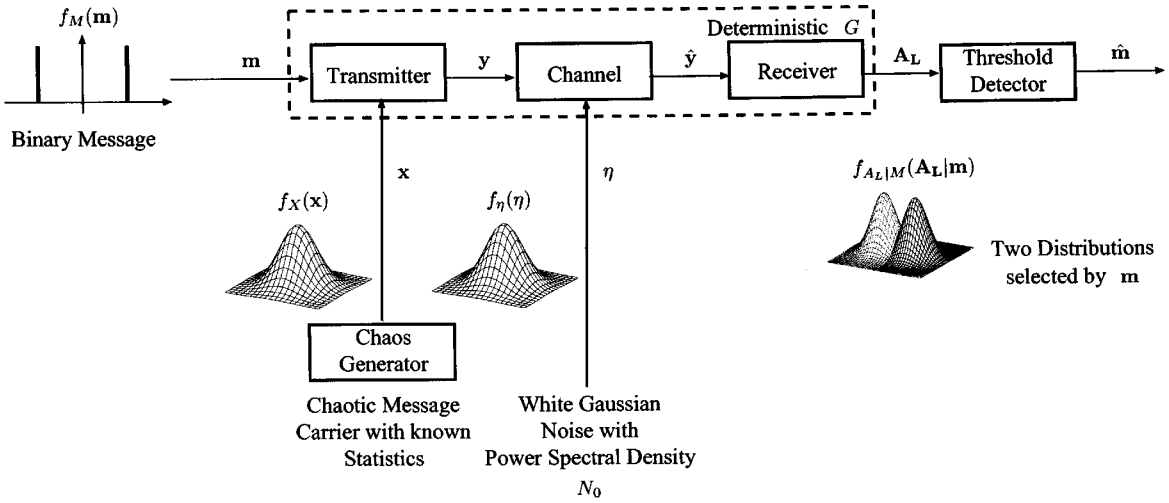

Fig. 10. General structure to be studied in chaos communication problems (AWGN channel).

analyzed system can be dynamical (i.e., containing delay elements), but it may not have feedback components in its structure. Unlike for linear systems, there does not exist a closed-form solution for the general case. Thus, communication systems, which contain feedback components (which is very likely for schemes with chaotically synchronizing receivers), cannot be directly analyzed this way. A solution might be the derivation of explicit input-output relations, e.g., by Volterra series. However, this restricts the dynamics severely, so the results will probably hold for particular cases only (e.g., in the synchronized state). No research has been performed for these problems yet.

IV. Performance of Digital Chaos Communication Schemes in Additive White Gaussian Noise

Initially, the research on chaos communications was concerned about the functioning of the proposed methods and few attention was paid to the working environment of a scheme. The channel was assumed to be ideal, with no noise and infinite bandwidth. By now, it is recognized that a scheme must also operate under real channel conditions.

Chaos communication proposes new methods and approaches. However, there are also solutions from the classical communications research—the main competitor. So, chaos communications have to be compared with and evaluated against the achievements in the rapidly developing field of classical communications.

The classical methods are well studied and established methods exist on how to obtain comparable performance figures for communication schemes under prescribed channel conditions. In order to discuss the feasibility of chaos communication methods, they have to be compared with classical schemes using the standard evaluation methods. These two goals—evaluation and comparison—are the aim of the performance analysis of chaotic communication schemes.

We will provide methods and results for the performance analysis of chaos communication schemes in the presence of white Gaussian noise (WGN) on the channel. Two examples, one for static and one for dynamic encoding/modulation, are studied. The results will provide an insight in the properties of chaos communication schemes.

A. Performance Evaluation of Communication Schemes

The analysis of a digital communication system tries to answer the question: How well does a scheme perform its main task—the transmission of a message? Transmission quality can be rated by the number of errors relative to the number of transmitted symbols, or more precisely in terms of the BER. Assume that a scheme (static encoding/modulation) transmits the symbol m_0 correctly with a probability $P_{00} = P\{\hat{m}(k) = 0 | m(k) = 0\}$ and the symbol m_1 with $P_{11} = P\{\hat{m}(k) = 1 | m(k) = 1\}$. m_0 is erroneously received as m_1 with $P_{01} = 1 - P_{00} = P\{\hat{m}(k) = 1 | m(k) = 0\}$ and m_1 as m_0 with $P_{10} = 1 - P_{11} = P\{\hat{m}(k) = 0 | m(k) = 1\}$. This setup is called a discrete memoryless channel. If the symbols appear with probabilities P_0 and P_1, the BER calculates as

$$\mathrm{BER} = P\{m(k) \neq \hat{m}(k)\} = P_{01}P_0 + P_{10}P_1. \qquad (38)$$

P_{01} and P_{10} depend on the parameters of the underlying communication scheme (modulation principle, encoding, channel distortions, noise, etc.).

A common model for the channel noise is a zero-mean white random process with a Gaussian pdf. Often, the noise appears to be additive on the channel. This is called an additive WGN (AWGN) channel. Such a noise has a constant psd N_0 (or $\mathrm{N}_0/2$ if a two-sided psd is considered) [15].

The general structure to be analyzed is given in Fig. 10. It is described by a deterministic functional G applied to random inputs $\mathbf{m}$, $\mathbf{x}$, and η and resulting in the input $\mathbf{A_L}$ of a threshold detector

$$\mathbf{A_L} = G(\mathbf{m}, \mathbf{x}, \eta). \qquad (39)$$

The threshold detector has to be designed according to the pdf of $\mathbf{A_L}$. A maximum likelihood approach [41] places the decision threshold optimally. From the knowledge of the statistical properties of $\mathbf{A_L}$, the BER can be calculated. G transforms the statistics of the inputs $\mathbf{m}$, $\mathbf{x}$, and η into the statis-

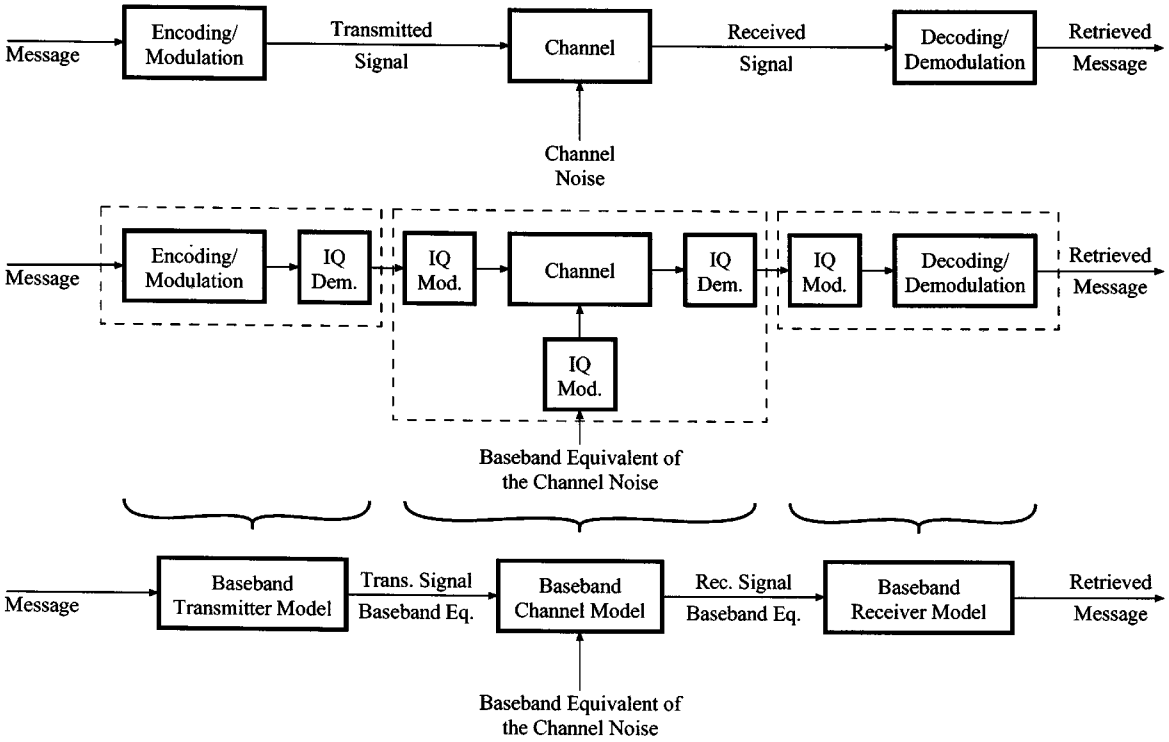

Fig. 11. Baseband modeling procedure for a communication scheme.

tics of $\mathbf{A_L}$. This transformation in general is nonlinear and depends on the properties of G.

Assume η to be a WGN and assume $\mathbf{m}$ to be a sequence of independent and equally probable binary symbols of duration T_b (this is well justified for most communication schemes). Then, the BER is a function h of $\mathrm{N_0}$ and the statistics of $\mathbf{x}$, which will be symbolically denoted by the cumulants $\varkappa_X$

$$\mathrm{BER} = h(\varkappa_X, \mathrm{N_0}, T_b). \tag{40}$$

To derive or to approximate the function h is the goal of our analysis. For the classical schemes, this problem is solved and the results are found in the literature. For the majority of the chaotic communication schemes, there are no analytical results so far.

A well-known classical example is the binary PSK (BPSK), where a zero-mean signal $\mathbf{x}$ (periodic with period T_b) is multiplied by ± 1 according to the symbol to be transmitted. The optimum receiver for the AWGN channel is a correlator, correlating the received noisy signal with a stored copy of one period of $\mathbf{x}$. The resulting A_L is Gaussian, with two mean values corresponding to the two message symbols. The signal-to-noise ratio (SNR) of A_L is [4]

$$\mathrm{SNR}_{A_L} = \frac{2\mathrm{E_b}}{\mathrm{N_0}} = \frac{2P_X T_b}{\mathrm{N_0}}. \tag{41}$$

$\mathrm{E_b}$ is the transmitted energy per bit, i.e., the average power P_X of $\mathbf{x}$ multiplied by the bit duration T_b.

With the optimum threshold detector [15]

$$\mathrm{BER} = \frac{1}{2}\mathrm{erfc}\left(\sqrt{\frac{\mathrm{E_b}}{\mathrm{N_0}}}\right) = \frac{1}{2}\mathrm{erfc}\left(\sqrt{\frac{\mathrm{SNR}_{A_L}}{2}}\right) = h\left(\frac{\mathrm{E_b}}{\mathrm{N_0}}\right). \tag{42}$$

Obviously, only $\mathrm{E_b}/\mathrm{N_0}$, the bit-energy-to-noise ratio, determines the BER of the scheme. This property is shared by many classical approaches. So, it is common to depict the BER as a function of $\mathrm{E_b}/\mathrm{N_0}$ in order to describe the performance of a scheme. This has the following implications.

1) Signal power can be traded for bit duration. A low-power low-bit-rate transmission achieves the same BER as a high-power high-bit-rate transmission for constant $\mathrm{N_0}$ and $\mathrm{E_b}$.
2) A noise power increase is compensated by a proportional bit energy increase.
3) A transmission below the noise floor is possible.

We will call this property noise robustness. Noise robustness is essential in applications with high ambient noise, such as CDMA, unlicensed radio with power limitations, or transmissions below the noise floor.

B. Baseband Modeling of Communication Schemes

The efficient and fast analysis and simulation of a communication scheme is obstructed by two problems.

1) The systems act on several time scales, which may be separated by several orders of magnitude. The message signal is located in the so-called baseband, the transmitted signal at the much higher radio frequencies (RFs). We are interested in the low-frequency input–output behavior of the communication system only. However, analysis and simulation are dominated by the fast RF part.
2) Digital messages are discrete-time signals, whereas the physical channel is continuous-time. We are only interested in the discrete-time part, but have to look at everything in continuous time.

The solution is the derivation of discrete-time baseband models, a well-known procedure from classical communication system analysis [2], [42]. In the modeling procedure, the bandpass signals on the channel are transformed into complex-valued low-pass signals by means of an inphase/quadrature modulation/demodulation. Virtually, this is a spectral shift of the power density spectrum at positive frequencies toward zero frequency. The modeling procedure is schematically depicted in Fig. 11. The transmitter and receiver devices are transformed into systems acting in the complex domain on the complex-valued low-pass equivalents of the channel input and output signals. If the low-pass signals are limited to a bandwidth $< f_s$, the system can be represented by a discrete-time equivalent obtained by sampling with f_s.

Statistical characteristics of the RF signals are transformed into properties of the baseband equivalents as follows [2], [42].

Real system	Discrete-time model
Time intervals:	
Δt	$\Delta k = f_s \Delta t$
Signal power:	
P	$P_d = 2P$
Signal energy:	
E	$E_d = 2 f_s E$
AWGN:	
$\eta;\ P_\eta = f_s \mathrm{N}_0$	$\eta_d = \eta_r + j\eta_i,$ $P_{\eta_d} = 2 f_s \mathrm{N}_0 = 2P_{\eta_r} = 2P_{\eta_i},$ η_r, η_i are independent, white, and Gaussian
Bit energy to noise ratio:	
$\mathrm{E_b/N_0}$	$E_{b_d}/\varkappa_{\eta_d, \eta_d^*}$

The derivation of baseband models is fairly simple for the standard modulation methods with harmonic carriers, such as AM, PM, or FM [43]. It becomes complicated, if a chaos generator operating at RF is to be transferred into the baseband. However, the task can be solved if the RF generator can be represented by a baseband generator with an added classical modulation method (this is the case, e.g., in frequency-modulated DCSK [44]) or if the scheme operates with an arbitrary chaos generator (COOK, DCSK, TR). Based on their discrete-time baseband models, two example schemes—a CSK scheme and DCSK—are analyzed in the sequel. Further details on the derivation of low-pass equivalent models of chaos communication schemes are found in [45]–[47].

1) Example I—Chaos Shift Keying: Let us assume the following CSK scheme [48]. The transmitter consists of two discrete-time chaos generators

$$x_1(k+1) = \mathrm{modf}(2\, x_1(k)) \tag{43a}$$
$$x_2(k+1) = \mathrm{modf}(2\, x_2(k) + 1) \tag{43b}$$

where

$$\mathrm{modf}(x) = \mathrm{rem}(x+1,\, 2) - 1 \tag{44}$$

is the overflow nonlinearity on the interval $[-1,\, 1)$. $\mathrm{rem}(x,\, y)$ denotes the remainder of the division of x by y and takes values from the interval $[0,\, y) \subset \mathbb{R}$. Depending on the message symbol (m_1 or m_2), the signal from generator (43a) or (43b) is transmitted. The resulting discrete-time baseband signal shall be transformed to the RF by PM

$$y(t) = \begin{cases} \cos(\omega_0 t + \pi x_1(k)) & m(k) = m_1 \\ \cos(\omega_0 t + \pi x_2(k)) & m(k) = m_2. \end{cases} \tag{45}$$

In the discrete-time baseband model for the PM, the modulating signal is mapped to the unit circle of the complex plane

$$y(k) = \begin{cases} \exp(j\pi x_1(k)) & m(k) = m_1 \\ \exp(j\pi x_2(k)) & m(k) = m_2. \end{cases} \tag{46}$$

Reformulating (43) in terms of values on the unit circle, one obtains equivalent complex-valued chaos generators (with initial conditions on the unit circle)

$$x_1(k+1) = f_1(x_1(k)) = (x_1(k))^2 \tag{47a}$$
$$x_2(k+1) = f_2(x_2(k)) = -(x_2(k))^2 \tag{47b}$$
$$y(k) = x_i(k) \qquad \text{if } m(k) = m_i. \tag{47c}$$

Note that the above maps are derived for modeling purposes. The unit circle is an unstable limit set of the maps, i.e., the dynamics have to be restricted to this set in order to model the behavior correctly. The transmitter structure can be simplified further without a change in the main properties of the scheme. One observes that sequences emitted by the first complex-valued generator (f_1) after a multiplication by -1 become sequences, which can be emitted by the second generator (f_2). So

$$x(k+1) = f_1(x_1(k)) = (x_1(k))^2 \tag{48a}$$
$$y(k) = m(k)\, x(k) \tag{48b}$$

where ($m(k) \in \{-1,\, 1\}$) is a simpler realization. Another possibility, which also uses only one generator, is a CS scheme. The transmitter consists of a chaos generator with one state variable. The map iterating the state is switched according to the message symbol to be transmitted

$$x(k+1) = f_i(x(k)) \quad \text{if} \quad m(k) = m_i \tag{49a}$$
$$y(k) = x(k). \tag{49b}$$

Apart from a dynamical dependence of the chaotic sequences belonging to unequal subsequent message symbols, the simplified structures produce signals, which are virtually equivalent to signals from (47). As will be shown later (see Section IV-F), this mutual dependence can be exploited in receiver design.

The straightforward receiver implementation is a correlation receiver, correlating the received signal with versions created by the drive-response synchronization method for the two generators. As in the transmitter, the structure can be simplified to one synchronizing system. The synchronization becomes a prediction of the next value to be received from the previously received symbol $\hat{y}(k-1)$ by the square map f_1

$$\hat{x}(k) = f_1(\hat{y}(k-1)). \tag{50}$$

The stability concerns for the map mentioned above are not relevant here, since only a simple feedforward structure is used. A correlation of $\hat{y}$ and $\hat{x}$

$$A_L(k) = \sum_{i=0}^{L-2} \hat{y}^*(k-i)\hat{x}(k-i) \tag{51}$$

results in 1 or -1 (ideal noise-free case) and, thus, allows to retrieve $\hat{m}$ via threshold detection. L is the discrete-time equivalent of the bit duration T_b—the number of samples of $\mathbf{y}$ carrying one message symbol. Note that only $L-1$ samples are correlated under the assumption of two independent generators in the transmitter. Otherwise, in the time instant of message detection, $\hat{x}(K-L+1)$ would be predicted from $\hat{x}(K-L)$, which belongs to the previously transmitted bit. If only one chaos generator is used in the transmitter, the correlation can include L samples.

2) Example II—Differential Chaos Shift Keying: DCSK can be implemented with virtually any message carrier signal $\mathbf{x}$. So, the derivation of a baseband model does not face difficulties, unless a particular RF chaos generator is to be used, which does not transform easily into the baseband. The structures of transmitter and receiver remain virtually unchanged, apart from acting now in discrete time and in the complex domain. The receiver correlates L samples (half the bit duration) of the received signal $\hat{\mathbf{y}}$ with an L-sample delayed copy of $\hat{\mathbf{y}}$ [7]

$$A_L(k) = \sum_{i=0}^{L-1} \hat{y}(k-i)\hat{y}^*(k-i-L). \tag{52}$$

In the sequel, we will show how to analyze the performance of the example schemes using the methods presented in Section III.

C. Statistical Analysis of Discrete-Time Baseband Models in AWGN

In this section, we will consider the AWGN channel [15]. It is given by

$$\hat{\mathbf{y}} = \mathbf{y} + \eta \tag{53}$$

in both the real scheme and the discrete-time baseband model.

1) Analysis of Example I Using the FPO: The aim of the FPO in communication system analysis is the calculation of statistics of the involved chaotic signals. For this calculation, one has to know the FPO for the used chaos generator (see Section III-B). This is the case for piecewise-linear maps as in (43). So, we reformulate (48) with the piecewise-linear generator separated

$$x(k+1) = g(x(k)) = \operatorname{modf}(2x(k)+1) \tag{54a}$$

$$y(k) = m(k)\exp(j\pi x(k)). \tag{54b}$$

The FPO of (54a) follows from (18) as

$$\mathcal{P}(h(z)) = \frac{1}{2}\left(h\left(\frac{z-1}{2}\right) + h\left(\frac{z+1}{2}\right)\right). \tag{55}$$

The FPO has a fixed point, which is the invariant pdf of the chaotic sequence $x(k)$ [48], [49]

$$f_X(x) = \tfrac{1}{2}\,\mathbf{1}(x) \tag{56}$$

with

$$\mathbf{1}(x) = \begin{cases} 1, & x \in [-1,\, 1) \\ 0, & \text{elsewhere.} \end{cases} \tag{57}$$

The mean of $\exp(j\pi x(k))$ is zero. Using the FPO's adjoint operator—the KO—one is able to calculate the autocorrelation function of $\exp(j\pi x(k))$

$$\begin{aligned} &E[\exp(j\pi X(k))\exp(-j\pi X(k+\tau))] \\ &\quad = E[\exp(j\pi X)\mathcal{U}^\tau(\exp(-j\pi X))] \\ &\quad = \tfrac{1}{2}\langle \exp(j\pi x)\mathcal{U}^\tau(\exp(-j\pi x)),\, \mathbf{1}(x)\rangle. \end{aligned} \tag{58}$$

Since KO and FPO are adjoint operators, we get

$$\begin{aligned} &E[\exp(j\pi X)\mathcal{U}^\tau \exp(-j\pi X)] \\ &\qquad = \langle \exp(-j\pi x),\, \mathcal{P}^\tau(\exp(j\pi x)\mathbf{1}(x))\rangle. \end{aligned} \tag{59}$$

Using (55), one calculates the first value of the autocorrelation function ($\tau = 1$) to be zero.

Iterations of the map f create again maps of the same type, which are analyzed in a similar fashion [48]. In the result, the correlation values for $\tau > 1$ are zero too. So, finally

$$E[\exp(j\pi X)\mathcal{U}^\tau \exp(-j\pi X)] = \delta(\tau) = \begin{cases} 1, & \tau = 0 \\ 0, & \text{elsewhere} \end{cases}. \tag{60}$$

In the example, the knowledge of mean and autocorrelation function (or variance) of the chaos generator on the complex unit circle is sufficient to calculate the mean and the variance of A_L using a suitable method (moment expansion over sums, cumulant equations). In AWGN, A_L is given as

$$\begin{aligned} A_L = \sum_{i=0}^{L-1} &(m\exp(j\pi x(k-i)) + \eta(k-i))^* \\ &\cdot(m\exp(j\pi x(k-i-1)) + \eta(k-i-1))^2. \end{aligned} \tag{61}$$

Mean and variance are calculated as [47], [48]

$$\varkappa^1_{A_L} = m = \frac{m}{L}\,E_b \tag{62a}$$

$$\varkappa^{1,1}_{A_L, A_L^*} = \frac{5\varkappa^{1,1}_{\eta,\eta^*} + 6(\varkappa^{1,1}_{\eta,\eta^*})^2 + 2(\varkappa^{1,1}_{\eta,\eta^*})^3}{L}. \tag{62b}$$

Being an average, A_L is approximately Gaussian for larger L, which implies the cumulants of order greater than two to be nonzero, but vanishing with increasing L. As in (42), one

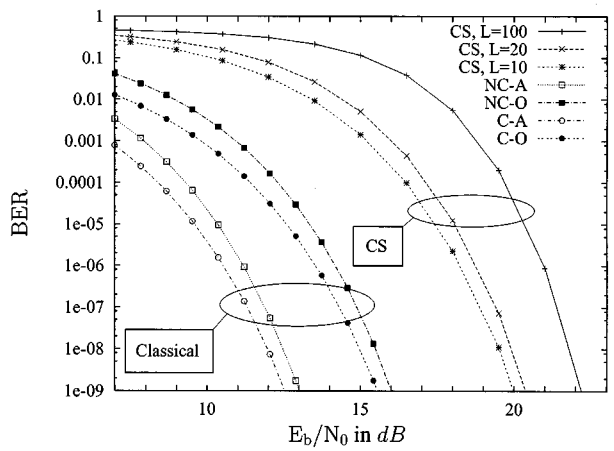

Fig. 12. AWGN performance of a CS (CSK) example (Gaussian Approximation for A_L) in comparison to classical modulation schemes.

obtains the BER from $\mathrm{SNR}_{A_L} = (\varkappa^1_{A_L})^2/\varkappa^{1,1}_{A_L,A_L^*}$ [48] [the SNR_{A_L} in the complex-valued model is half the SNR_{A_L} of the real system in (42) due to the imaginary part in A_L]

$$\mathrm{BER} = \frac{1}{2}\,\mathrm{erfc}\left(\sqrt{\frac{1}{5\frac{\mathrm{N_0}}{\mathrm{E_b}} + 6L\left(\frac{\mathrm{N_0}}{\mathrm{E_b}}\right)^2 + 2L^2\left(\frac{\mathrm{N_0}}{\mathrm{E_b}}\right)^3}}\right) \tag{63}$$

where $\mathrm{E_b/N_0} = L/\varkappa^{1,1}_{\eta,\eta^*}$. This result is depicted in Fig. 12 in comparison with the performance of classical communication schemes [15] ("C-A": coherent antipodal, such as BPSK; "C-O": coherent orthogonal, such as coherent binary FSK; "NC-A": noncoherent antipodal, such as DPSK; "NC-O": noncoherent orthogonal, such as noncoherent binary FSK). The results for the CS scheme also agree well with simulations for the $L = 20$ and $L = 100$ cases [48]. For smaller L, larger deviations are observed due to the non-Gaussian pdf of A_L.

Comparing the curves for the classical schemes and CS, one observes that CS requires 4–10 dB better $\mathrm{E_b/N_0}$ in order to achieve the same BER, which is a fairly high gap and a clear disadvantage of the scheme. Moreover, in the recent literature [50], it was shown that the analyzed receiver is optimum for the given modulation scheme. The only possible improvement is achieved by a decrease of L, which implies an increase of the channel SNR and, hence, of the transmission power.

The analyzed CS example shows a typical case, where the analysis approach described in this paper is applicable. The dependence between the input and output signals of the scheme does not contain feedback structures and is a polynomial in each of the inputs. Thus, moments and cumulants can be obtained in a closed form. The fact that a correlator is used allows one to derive a BER formula from the first- and second-order cumulants of A_L due to the assumption of approximate Gaussianity.

2) Analysis of Example II Using Cumulant Equations: Cumulant equations suit DCSK very well as an analysis tool, since the scheme operates with arbitrary signals and in the cumulant equations the cumulants of $\mathbf{X}$ remain as free parameters. Thus, not only performance figures for one particular case, but for larger classes of implementations are obtained. Also, an optimization with respect to the exploited signal becomes possible.

Consider the baseband model of a DCSK communication scheme in AWGN. The threshold detector input at the time instant of message symbol detection can be formulated as

$$A_L = \frac{1}{L}\sum_{i=0}^{L-1}(mx(i)+\eta(i+L))(x(i)+\eta(i))^* \tag{64}$$

with $m \in \{m_1, m_2\} = \{-1, 1\}$. The optimum decision threshold is the imaginary axis due to the symmetry of the setup.

As in Example I, we can assume the distribution of A_L to be approximately Gaussian, in particular for large values of L. Performing a cumulant analysis (for more details see [51], [7]) and taking into account: 1) the zero-mean AWGN $\Longrightarrow$ cumulants of second order only and δ-like cumulant functions; 2) the independence of η and $\mathbf{X} \Longrightarrow$ no joint cumulants; and 3) the stationarity of η and $\mathbf{X} \Longrightarrow$ time-invariance of the statistics, one obtains [7], [51]

$$\varkappa^1_{A_L} = m\varkappa^1_P = \frac{m}{2L}E_b \tag{65a}$$

$$\varkappa^{1,1}_{A_L,A_L^*} = \sum_{k=-L+1}^{L-1}\frac{L-|k|}{L}\,\varkappa^{1,1}_{P(0),P(k)} + \frac{2\varkappa^1_P\varkappa^{1,1}_{\eta,\eta^*}}{L} + \frac{(\varkappa^{1,1}_{\eta,\eta^*})^2}{L}, \tag{65b}$$

where $P(k) = x(k)x^*(k)$ is the transmission power. With $\mathrm{SNR}_{A_L} = (\varkappa^1_{A_L})^2/\varkappa^{1,1}_{A_L,A_L^*}$ follows an approximative formula for the BER as in (42). As in Example I, the SNR_{A_L} of the complex-valued model is half the SNR_{A_L} in the real system. An optimization of the transmitted signal requires the minimization of SNR_{A_L} or the maximization of $\varkappa^{1,1}_{A_L,A_L^*}$ for a fixed $\varkappa^1_{A_L}$. The tunable parameter is $\varkappa^{1,1}_{P(0),P(k)}$—the autocovariance function of the signal power. It controls the sum term in (65b) and, as such, the variance $\varkappa^{1,1}_{A_L,A_L^*}$ in the noise-free case ($\varkappa^{1,1}_{\eta,\eta^*} = 0$). The minimum is reached, if the sum term equals zero. This is trivially guaranteed, if $\varkappa^{1,1}_{P(0),P(k)} = 0$ for any k, i.e., if the power of $\mathbf{x}$ is constant in the baseband model. This implies a restriction of the exploited chaotic signal to a circle in the complex plane (the unit circle without loss of generality), which is the case, e.g., for generators as given in (47).

For the optimized case, we obtain an approximate expression for the BER in terms of $\mathrm{E_b/N_0} = 2L\varkappa^1_P/\varkappa^{1,1}_{\eta,\eta^*}$ [47]

$$\mathrm{BER} = \tfrac{1}{2}\,\mathrm{erfc}\left(\sqrt{\frac{1}{4\frac{\mathrm{N_0}}{\mathrm{E_b}} + 4L\left(\frac{\mathrm{N_0}}{\mathrm{E_b}}\right)^2}}\right). \tag{66}$$

It is depicted in Fig. 13 in comparison with the performance of classical communication schemes [15] ("C-A": coherent antipodal, such as BPSK; "C-O": coherent orthogonal, such as coherent binary FSK; "NC-A": noncoherent antipodal,

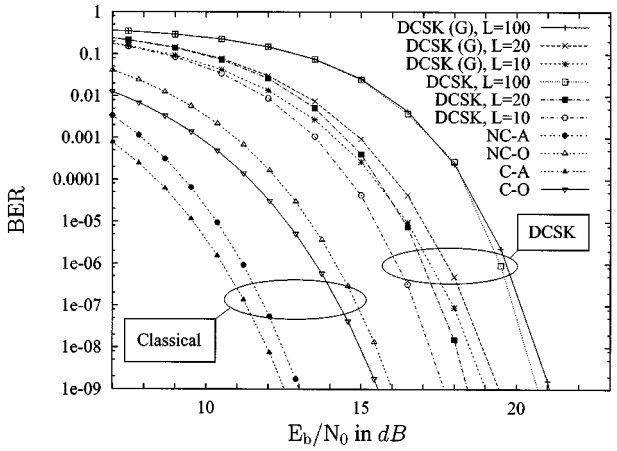

Fig. 13. AWGN performance of DCSK ("G": Gaussian approximation for A_L) in comparison to classical modulation schemes.

such as DPSK; "NC-O": noncoherent orthogonal, such as noncoherent binary FSK).

Under the assumption of the optimized signals the analysis can be continued to higher-order cumulants. The first aim of this procedure is to calculate the statistical parameters *skewness* and *kurtosis* [38]

$$\gamma_3 = \frac{\varkappa^3_{\Re\{A_L\}}}{\left(\varkappa^2_{\Re\{A_L\}}\right)^{3/2}}, \qquad \gamma_4 = \frac{\varkappa^4_{\Re\{A_L\}}}{\left(\varkappa^2_{\Re\{A_L\}}\right)^{2}} \tag{67}$$

($\Re$—real part), which measure the deviation of a pdf from a Gaussian one. They show that the approximation only holds for large L or, if L is small, for small $\mathrm{SNR} = \varkappa^1_P/\varkappa^{1,1}_{\eta,\eta^*}$ on the channel [51].

Continuing the cumulant analysis, general expressions may be found (for the real part of A_L, which only is relevant, since the decision threshold is the imaginary axis). Normalized to $\varkappa^1_{\Re\{A_L\}}$ they read [51]

$$\varkappa^q_{\Re\{A_{L_n}\}} = m^q \left(q! \left(\frac{\varkappa^{1,1}_{\eta,\eta^*}}{2PL} \right)^{q-1} + (1+(-1)^q) L (q-1)! \left(\frac{\varkappa^{1,1}_{\eta,\eta^*}}{2PL} \right)^{q} \right). \tag{68}$$

This allows one to calculate the characteristic function and to derive an explicit expression for the BER of DCSK under the assumption of constant transmission power or constant bit energy, respectively, [21], [51]

$$\mathrm{BER} = \frac{1}{2^L} e^{-(\mathrm{E_b}/2\mathrm{N_0})} \sum_{i=0}^{L-1} \frac{\left(\frac{\mathrm{E_b}}{2\mathrm{N_0}}\right)^i}{i!} \sum_{j=i}^{L-1} \frac{1}{2^j} \binom{j+L-1}{j-i}. \tag{69}$$

Here, the analysis is completed, giving the full knowledge of the DCSK performance in AWGN. Equation (69) is a complicated expression, so where appropriate, the much simpler (66) should be used.

The result also is depicted in Fig. 13. Again, there is a large gap between the classical modulation schemes and DCSK. However, for the limit case $L = 1$, DCSK reaches the performance of noncoherent orthogonal modulation.

Simulations verifying the BER formulas are found in various publications studying DCSK [21], [47]. They all agree with the calculations.

D. Noise Robustness Problems

From the performance figures for the chaotic schemes (63) and (66), an interesting observation is made. To the contrary of many classical methods, the diagram of the BER over $\mathrm{E_b/N_0}$ shows not only a single curve, but a set of curves depending on a system parameter (L in this case). So, the schemes are *not* noise robust in the sense described in Section IV-A. The performance curves are seen to shift to the right with growing L in all analyzed cases. The performance depends on how the energy per bit is transmitted. A high-power high-bit-rate transmission gives a lower BER than a low-power low-bit-rate transmission for the same $\mathrm{E_b/N_0}$. This effect is in particular observable for a channel SNR below 0 dB, i.e., if the interference power is larger than the transmission power [47], [51]. This is a typical situation in CDMA environments or situations with high ambient noise.

There are some classical approaches, which share this property—in particular, the TR schemes [52], where the effect was observed first [19]. It is also known to appear in suboptimum DPSK systems [21], [53], where the same receiver as in DCSK (see Fig. 6) is applied to a differentially modulated signal. With this receiver, DPSK becomes a transmitted-reference scheme.

Lacking noise robustness is a disadvantage of the chaotic schemes, since it limits their range of applicability. However, AWGN channels are only one facet of the application fields of chaos communications. There are other aspects such as multipath channels (and linear filtering in general) and nonlinear distortions, which have to be studied and where only very few results exist by now.

E. Multipath Channels

Once the performance for the AWGN channel is known, one can proceed to more complex channel models, covering further imperfections of a communication channel. A particular effect appearing in channels for mobile as well as indoor communications is multipath propagation. So, a receiver picks from the channel a superposition of copies of the transmitted signal, which have different propagation times, attenuations, and phase shifts. An AWGN is still present. In the discrete-time baseband model, such a channel with two paths is described as follows [54]:

$$\hat{y}(k) = \alpha y(k) + \beta y(k-M) + \eta(k) \tag{70}$$

where $\hat{\mathbf{y}}$ is the channel output, $\mathbf{y}$ is the channel input (DCSK signal), and η is an AWGN. The filter taps α and β are complex numbers, representing the attenuations and phase shifts on the two propagation paths. M is the delay on the second path relative to the first.

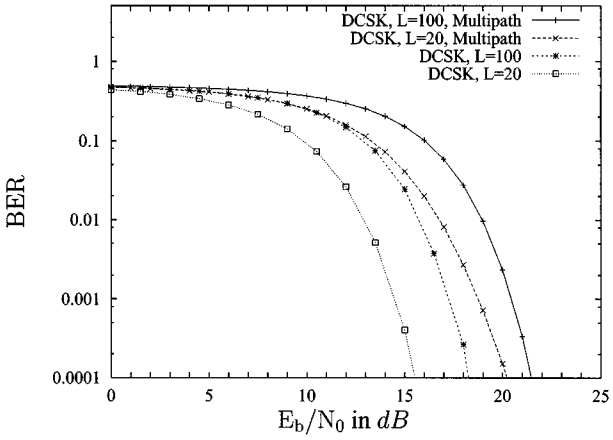

Fig. 14. Performance of DCSK in a two-ray channel with AWGN (compared to the plain AWGN case).

This channel model has to be incorporated in the formulation of A_L for the scheme to be analyzed. Then, the tools described in Section III can be applied. For the DCSK scheme, the following formula is calculated (assuming A_L to be Gaussian) [54]

$$\mathrm{BER} = \frac{1}{2}\mathrm{erfc}\left(\frac{a^2+b^2\frac{L-M}{L}}{\sqrt{\frac{b^4M}{L^2}+2\frac{a^2b^2}{L}+4(b^2+a^2)\frac{N_0}{E_b}+4L\frac{{N_0}^2}{{E_b}^2}}}\right) \tag{71}$$

where $a = |\alpha|$ and $b = |\beta|$. For $a = b = 0.5$ and $M = 2$, the performance graphs are shown in Fig. 14. The multipath channel leads to a remarkable drop in the overall system performance, which, however, decreases with increasing L. The lack in noise robustness remains also visible. The analysis results are confirmed by simulations [54]. The Gaussian assumption is better justified than in the plain AWGN case, since more terms (L from each propagation path) are averaged in the receiver. Still, L has to be large enough ($L > 10$) to obtain satisfactory results.

In the case of multipath propagation, the broad-band nature of chaotic signals can make chaotic schemes superior to narrowband classical methods, which can be shown to fail catastrophically in some cases due to the filtering in the channel. This was shown for the DCSK scheme in [55]. Compared to broad-band classical schemes, this advantage does not exist. Hence, the situation here is similar to the plain AWGN channel, as it was shown in [54] for DCSK in comparison to a broad-band implementation of DPSK. The performance curves of the broad-band DPSK were located about 5–6 dB left of the DCSK performance curves on the same multipath channel ($L = 20$ and $L = 100$ for DCSK). Comparable multipath performance figures can be reached for high SNR on the channel only. With lower SNR, the lack of noise robustness causes the chaotic scheme again to fall behind the classical ones.

F. Alternative Receiver Structure for Example I

The CS implementation (47) of Example I describes a dynamic encoding/modulation scheme. It can be decoded with a method from classical communications—the *Viterbi decoder* [15], [56], which was designed for receivers of dynamically encoded/modulated signals. The Viterbi decoder was developed for digital communications, i.e., it operates in discrete time and with discrete values. It exploits the interdependence between transmitted symbols, which is introduced by the dynamic encoding/modulation, and uses an effective search procedure to perform a maximum likelihood decision about the transmitted sequence.

The Viterbi-decoding technique cannot be applied directly to the chaotic schemes, since they always act on a continuous-valued state space. However, it can be applied to the *symbolic dynamics*. As stated in Section II-C1b, symbolic dynamics create sequences arising when partitioning the state space in disjoint sets, which are assigned with different symbols. Not every symbol may be mapped to every other symbol by the generator, which forms the symbol interdependence exploitable by a Viterbi decoder.

From the point of view of symbolic dynamics, the transmitter can be seen as the shift register structure shown in Fig. 15 ($L = 1$, 2^3 states). Based on this, a Viterbi decoder can be designed for the receiver.

Knowing that a Viterbi decoder is used in the receiver, the transmission can be limited to the symbolic dynamics instead of the continuous-valued chaotic sequence. In Fig. 16, the performance of such a scheme is shown for Viterbi decoders with different numbers of states (or symbols of the symbolic dynamics) and continuous-valued transmission or symbolic dynamics transmission. In the latter case, the scheme reaches the performance of classical coherent orthogonal modulation. Since the decoding algorithm is very complex and cannot be described by a dynamical system structure suitable for the statistical analysis methods discussed in this paper, computer simulations were used in order to obtain the results in Fig. 16.

The details of the design, analysis, and simulation of this scheme can be found in [57].

G. Chaotic Schemes in Comparison to Classical Schemes

The analysis methods and results presented above allow to perform a comparison of the presented chaotic and classical schemes. This comparison can be based on analytical results for the situations and schemes discussed.

The performance of classical methods can be reached for limit cases, in particular, for $L = 1$ in the CM scheme (equivalent to a classical coherent orthogonal scheme [4], [57]) and in the DCSK scheme (equivalent to a noncoherent orthogonal scheme [4], [21]). However, there is the lack in noise robustness, which causes the performance to drop with decreasing SNR on the channel and, thus, fall behind the classical approaches.

The situation remains the same on multipath channels. For the DCSK example, it was shown that it has an advantage over narrowband solutions due to the broad-band nature of the signal. However, classical broad-band solutions can perform better than DCSK on multipath channels.

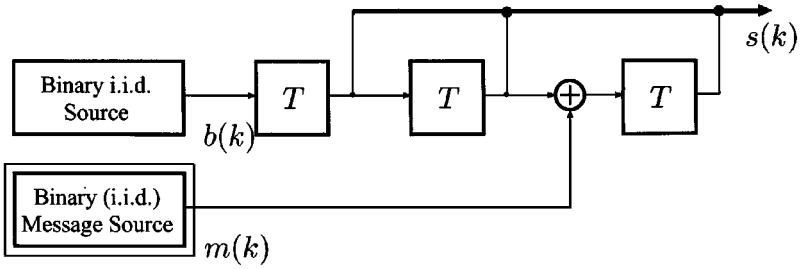

Fig. 15. Shift register representation of the CS transmitter—$m(k)$ message sequence, $b(k)$ bits generated by the map iteration, $s(k)$ symbolic sequence (3 bits).

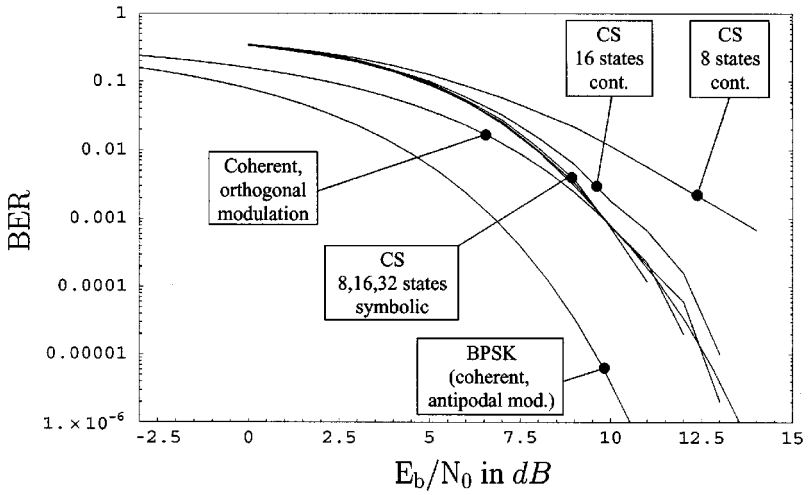

Fig. 16. Performance of CM with Viterbi decoder in AWGN.

The only known potential advantage of the chaos communication schemes lies in the simplicity of the generator structures and of some of the receivers (e.g., DCSK).

As mentioned above, there is only one communication problem known so far where the application of chaos is beneficial: the generation of spreading codes for classical CDMA systems.

V. Summary and Conclusions

In this paper, we tried to give an overview over the most common chaos communication methods found in the literature. Of course, there are many ideas and a discussion of all of them cannot be provided within just one journal article, but we hope to have covered the majority of methods in our classification.

The standard approach to a classical communication scheme is a statistical one, since many of the involved signals are random and thus best described by stochastic models. The analysis of chaos communication methods should follow this track, not only because it would be useful for a comparison with the classics, but because chaotic signals resemble random signals. We presented a set of tools that opens the possibility for a statistical approach to the performance of chaos communication schemes. The methods are not universal, but they allow to analyze a part of the chaos communication schemes and their application provided analytical solutions for the first time.

Analytical solutions are more general than simulation-based results. Hence, one can draw conclusions, which hold for at least wide parameter ranges of a chaos communication scheme. As a rule, they are a convenient base for system design. The primary observation following from the analysis is the performance drop in low SNR conditions, which is often observed in chaos communication schemes. The analysis cannot provide a final answer, whether this effect is avoidable or not, but one can search for possible reasons for such a behavior. Chaotic signals contain more information in the information-theoretical sense (chaos generators permanently produce information) than the classical message carriers, which are periodic and, thus, do not introduce additional information. The receiver relies on the additional information contained in the chaos in order to derive a reference signal or to synchronize [58]. This means that there is further information beside the message to be transmitted, which increases the total amount of information and grows with increasing bit duration due to the longer chaotic sequences exploited. The link between the performance drop and the rate of information generation in a chaos generator remains to be studied.

The research in chaos communications is progressing steadily, but the field in which chaos communications definitely outperform classical solutions remains to be clearly identified.

ACKNOWLEDGMENT

The authors would like to thank the reviewers and Guest Editor Prof. M. Hasler for detailed and helpful comments and suggestions.

REFERENCES

[1] C. C. Chen and K. Yao, "Stochastic-calculus-based numerical evaluation and performance analysis of chaotic communication systems," *IEEE Trans. Circuits Syst. I*, vol. 47, pp. 1663–1672, Dec. 2000.

[2] J. G. Proakis, *Digital Communications*, 3rd ed. New York: McGraw-Hill, 1995.

[3] D. R. Stinson, *Cryptography—Theory and Practice*. Boca Raton, FL: CRC Press, 1995.

[4] J. M. Wozencraft and I. M. Jacobs, *Principles of Communication Engineering*. New York: Wiley, 1965.

[5] A. L. Baranovski, W. Schwarz, and A. Mögel, "Statistical analysis and design of chaotic switched dynamical systems," in *Proc. Int. Symp. Circuits and Sytems*, vol. V, Orlando, FL, May/June 1999, pp. 467–470.

[6] M. P. Kennedy, G. Kolumbán, and Z. Jákó, "Chaotic modulation schemes," in *Applications of Chaotic Electronics to Telecommunications*, M. P. Kennedy, R. Rovatti, and G. Setti, Eds. Boca Raton, FL: CRC Press, 2000, ch. 6, pp. 151–183.

[7] W. Schwarz, M. Götz, K. Kelber, A. Abel, T. Falk, and F. Dachselt, "Statistical analysis and design of chaotic systems," in *Applications of Chaotic Electronics to Telecommunications*, M. P. Kennedy, R. Rovatti, and G. Setti, Eds. Boca Raton, FL: CRC Press, 2000, ch. 9, pp. 253–305.

[8] M. Götz, K. Kelber, and W. Schwarz, "Discrete-time chaotic encryption systems. Part I: Statistical design approach," *IEEE Trans. Circuits Syst. I*, vol. 44, pp. 963–970, Oct. 1997.

[9] K. Kelber, T. Falk, M. Götz, W. Schwarz, and T. Kilias, "Discrete-time chaotic encryption systems. Part II: Continuous- and discrete-value realization," in *Proc. Int. Workshop Nonlinear Dynamics in Electronic Systems*, Seville, Spain, June 1996, pp. 27–32.

[10] F. Dachselt, K. Kelber, and W. Schwarz, "Discrete-time chaotic encryption systems. Part III: Cryptographical analysis," *IEEE Trans. Circuits Syst. I*, vol. 45, pp. 883–888, Sept. 1998.

[11] G. Mazzini, R. Rovatti, and G. Setti, "Interference minimization by auto-correlation shaping in asynchronous DS-CDMA systems: Chaos-based spreading is nearly optimal," *Electron. Lett.*, vol. 35, no. 13, pp. 1054–1055, June 1999.

[12] L. Cong and L. Shaoqian, "Chaotic spreading sequences with multiple access performance better than random sequences," *IEEE Trans. Circuits Syst. I*, vol. 47, pp. 394–397, Mar. 2000.

[13] G. Mazzini, R. Rovatti, and G. Setti, "Chaos-based asynchronous DS-CDMA systems," in *Applications of Chaotic Electronics to Telecommunications*, M. P. Kennedy, R. Rovatti, and G. Setti, Eds. Boca Raton, FL: CRC Press, 2000, ch. 4, pp. 33–79.

[14] C. C. Chen and K. Yao, "Design of spread spectrum sequences using chaotic dynamical systems and ergodic theory," *IEEE Trans. Circuits Syst. I*, vol. 48, pp. 1110–1114, Sept. 2001.

[15] S. S. Haykin, *Communication Systems*, 3 ed. New York: Wiley, 1994.

[16] Lj. 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, no. 3, pp. 709–713, 1992.

[17] M. P. Kennedy and H. Dedieu, "Experimental demonstration of binary chaos-shift-keying using self-synchronising Chua's circuits," in *Proceedings of the International Workshop Nonlinear Dynamics in Electronic Systems*. Singapore: World Scientific, 1994, pp. 262–275.

[18] G. Kolumbán, M. P. Kennedy, and G. Kis, "Performance improvement of chaotic communications systems," in *Proc. Eur. Conf. Circuit Theory and Design*, vol. 1, Budapest, Hungary, Aug./Sept. 1997, pp. 284–289.

[19] B. L. Basore, "Noise-like signals and their detection by correlation," Ph.D. dissertation, MIT, Cambridge, MA, 1952.

[20] G. Kolumbán, B. Vizvari, W. Schwarz, and A. Abel, "Differential chaos shift keying: A robust coding for chaos communication," in *Proc. Int. Workshop Nonlinear Dynamics in Electronic Systems*, Seville, Spain, June 1996, pp. 87–92.

[21] G. Kolumbán, "Theoretical noise performance of correlator-based chaotic communications schemes," *IEEE Trans. Circuits Syst. I I*, vol. 47, no. 12, pp. 1692–1701, December 2000.

[22] R. Rovatti, G. Setti, G. Mazzini, and S. Callegari, "Performance upper-bound for full-$\mathcal{E}_b$ bilinear FM-DCSK receivers," in *Proc. Int. Workshop Nonlinear Dynamics in Electronic Systems*, Catania, Italy, 2000, pp. 170–173.

[23] C. Lee, *Convolutional Coding: Fundamentals and Applications*. Norwood, MA: Artech House, 1997.

[24] K. S. Halle, C.-W. Wu, M. Itoh, and L. O. Chua, "Spread spectrum communication through modulation of chaos," *Int. J. Bifurcation Chaos*, vol. 3, no. 2, pp. 469–477, 1993.

[25] U. Parlitz, L. O. Chua, Lj. Kocarev, K. S. Halle, and A. Shang, "Transmission of digital signals by chaotic synchronization," *Int. J. Bifurcation Chaos*, vol. 2, no. 4, pp. 973–977, 1992.

[26] T. Schimming and J. Schweizer, "Chaos communication from a maximum likelihood perspective," in *Proc. Int. Symp. Nonlinear Theory and Applications*, vol. 1, Crans Montana, Switzerland, Sept. 1998, pp. 77–80.

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

[28] E. Ott, C. Grebogi, and J. A. Yorke, "Controlling chaos," *Phys. Rev. Letters*, vol. 64, pp. 1196–1199, 1990.

[29] H. D. I. Abarbanel, L. Korzinov, A. I. Mees, and I. M. Starobinets, "Optimal control of nonlinear systems to given orbits," *Syst. Control Lett.*, vol. 31, no. 5, pp. 263–276, 1997.

[30] U. Feldmann, M. Hasler, and W. Schwarz, "Communication by chaotic signals: The inverse system approach," *Int. J. Circuit Theory Appl.*, vol. 24, no. 5, pp. 551–579, 1996.

[31] M. Hasler and T. Schimming, "Optimal and suboptimal chaos receivers," *Proc. IEEE*, vol. 90, pp. 733–746, May 2002.

[32] A. Dmitriev, S. Starkov, and S. Yemetz, "Chaotic communication using digital signal processors," in *Proc. Int. Symp. Nonlinear Theory and Applications*, vol. 3, Crans Montana, Switzerland, Sept. 1998, pp. 1093–1096.

[33] M. Sushchik, N. Rulkov, L. Larson, L. Tsimring, H. Abarbanel, K. Yao, and A. Volkovskii, "Chaotic pulse position modulation: A robust method of communicating with chaos," *IEEE Commun. Lett.*, vol. 4, pp. 128–130, Apr. 2000.

[34] F. Agnelli, G. Mazzini, R. Rovatti, and G. Setti, "A first experimental verification of optimum MAI reduction in chaos-based DS-CDMA systems," in *Proc. Int. Symp. Circuits and Systems*, vol. III, Sydney, Australia, 2001, pp. 137–140.

[35] A. Dmitriev, B. Kyarginsky, A. Panas, and S. Starkov, "Direct chaotic communication system. Experiments," in *Proc. Int. Workshop Nonlinear Dynamics in Electronic Systems*, Delft, The Netherlands, June 2001, pp. 157–160.

[36] K. Król, L. Azzinnari, E. Korpela, A. Mozsàry, M. Talonen, and V. Porra, "An experimental FM-DCSK chaos radio system," in *Proc. Eur. Conf. Circuit Theory and Design*, vol. III, Espoo, Finland, Aug. 2001, pp. 17–20.

[37] A. N. Malakhov, "Cumulant analysis of random non-Gaussian processes and their transformations" (in Russian), in *Sovetskoe Radio*, Moscow, Russia, 1978.

[38] C. L. Nikias and A. P. Petropulu, *Higher-Order Spectra Analysis*. Englewood Cliffs, NJ: Prentice-Hall, 1993.

[39] P. J. Smith, "A recursive formulation of the old problem of obtaining moments from cumulants and vice versa," *Amer. Statistician*, vol. 49, no. 2, pp. 217–218, May 1995.

[40] A. Lasota and M. C. Mackey, "Chaos, fractals, and noise," in *Applied Mathematical Sciences 97*. New York: Springer-Verlag, 1994.

[41] H. V. Poor, *An Introduction to Signal Detection and Estimation*. Berlin, Germany: Springer-Verlag, 1994.

[42] M. Schwartz, W. R. Bennett, and S. Stein, *Communication Systems and Techniques*. New York: McGraw-Hill, 1966.

[43] L. W. Couch, II, *Digital and Analog Communication Systems*, 5th ed. London, U.K.: Prentice-Hall, 1997.

[44] G. Kolumbán, G. Kis, M. P. Kennedy, and Z. Jákó, "FM-DCSK: A new and robust solution for chaotic communications," in *Proc. Int. Symp. Nonlinear Theory and Applications*, vol. 1, Nov./Dec. 1997, pp. 117–120.

[45] M. Hasler, "Chaotic communications over a noisy channel (Tutorial talk)," in *Proc. Eur. Conf. Circuit Theory and Design*, Streza, Italy, Aug./Sept. 1999, p. 256.

[46] G. Kolumbán, "Performance evaluation of chaotic communications systems: Determination of low-pass equivalent model," in *Proc. Int. Workshop Nonlinear Dynamics in Electronic Systems*, Budapest, Hungary, July 1998, pp. 41–51.

[47] A. Abel, M. Götz, and W. Schwarz, "Statistical analysis of chaotic communication schemes," in *Proc. Int. Symp. Circuits and Sytems*, vol. 4, Monterey, USA, 1998, pp. IV-465–IV-468.
[48] M. Götz, A. Abel, and W. Schwarz, "What is the use of the Frobenius–Perron operator for chaotic signal processing?," in *Proc. Int. Workshop Nonlinear Dynamics in Electronic Systems*, Moscow, Russia, 1996, pp. 8–13.
[49] M. Götz and A. Abel, "Design of infinite chaotic polyphase sequences with perfect correlation properties," in *Proc. Int. Symp. Circuits and Sytems*, vol. 3, Monterey, USA, 1998, pp. III-279–III-282.
[50] T. Schimming and B. J. Zouhair, "Phase modulated ergodic chaos shift keying," in *Proc. Int. Symp. Nonlinear Theory and Applications*, Miyagi, Japan, 2001, pp. 549–552.
[51] A. Abel, W. Schwarz, and M. Götz, "Noise performance of chaotic communication systems," *IEEE Trans. Circuits Syst. I*, vol. 47, pp. 1726–1732, Dec. 2000.
[52] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook*. New York: McGraw-Hill, 1994.
[53] Yu. Okunev, *Phase and Phase-Difference Modulation in Digital Communications*. Norwood, MA: Artech House, 1997.
[54] A. Abel and W. Schwarz, "DCSK and DPSK—A comparative analysis in multipath environments," in *Proc. Int. Symp. Nonlinear Theory and Applications*, Miyagi, Japan, Nov. 2001, pp. 549–552.
[55] M. P. Kennedy, G. Kolumbán, G. Kis, and Z. Jákó, "Performance evaluation of FM-DCSK modulation in multipath environments," *IEEE Trans. Circuits Syst. I*, vol. 47, pp. 1702–1711, Dec. 2000.
[56] A. J. Viterbi, "Error bounds for convolutional codes and an asymptotically optimum decoding algorithm," *IEEE Trans. Inform. Theory*, vol. IT-13, pp. 260–269, Apr. 1967.
[57] A. Abel and W. Schwarz, "Maximum likelihood detection of symbolic dynamics in communication systems with chaos shift keying," in *Proc. Int. Workshop Nonlinear Dynamics in Electronic Systems*, Catania, Italy, May 2000, pp. 174–178.
[58] T. Stojanovski, L. Kocarev, and R. Harris, "Application of symbolic dynamics in chaos synchronization," *IEEE Trans. Circuits Syst. I*, vol. 44, pp. 1014–1018, Oct. 1997.

Andreas Abel received the Dipl.-Ing. degree in electrical engineering from the Dresden University of Technology (TU Dresden), Dresden, Germany, in 1996. He is currently working toward the Ph.D. degree at the Institute for Fundamentals of Electrical Engineering and Electronics at TU Dresden.

He was a Visiting Researcher at the Communications Laboratory of the Helsinki University of Technology, Helsinki, Finland, in 1997 and the Laboratory of Nonlinear Systems at the Swiss Federal Institute of Technology Lausanne, Switzerland, in 2000. His current research interests include the application of chaos in communications, the statistical analysis of nonlinear dynamical systems and chaos, and nonlinear signal processing.

Mr. Abel was a Member of the organizing committees of the 7th International Workshop on Nonlinear Dynamics in Electronic Systems, Rønne, Bornholm, Denmark, in 1999 and the International Symposium on Nonlinear Theory and its Applications, Dresden, Germany, in 2000.

Wolfgang Schwarz (Member, IEEE) received the Dipl.-Ing., the Dr.-Ing., and the Dr.-Ing. habil. degrees from the Dresden University of Technology, Dresden, Germany in 1965, 1969, and 1976 respectively.

From 1969 to 1974, he was an Assistant Professor with the Engineering College Mittweida, Germany, where he taught lectures in control engineering and conducted research on robot control systems. From 1974 to 1977, he was a Member of the Research and Design Staff with Starkstromanlagenbau Chemnitz, Germany, where he worked in the development of CNCs for machine tools. From 1977 to 1983, he was a Professor of Information Engineering Head of the Department of Information Electronics with the Engineering College Mittweida, Germany. In 1974 and 1977, he was an Invited Professor at the Moscow Telecommunication Institute, where he lectured on stochastic signals and dynamical systems. From 1983 to 1992, he was a Professor of Electronic Circuits and, since 1992, he has been a Full Professor of Fundamentals of Electrical Engineering and Electronics with the Technical University of Dresden, where he was also a founding Chairman of the Institute of Fundamentals of Electrical Engineering and Electronics from 1990 to 1993. In 1992, he was an Invited Researcher at the University of California, Berkeley. His current research interests are in the fields of nonlinear dynamic systems and circuits.

Dr. Schwarz cofounded the International Workshop on Nonlinear Dynamic Electronic Systems (NDES) in 1993. He was the local organizer of the V. EUROCHIP Workshop on VLSI Design Training, Dresden, Germany, the Technical Chair of NDES in 1999, the General Co-Chair and Local Arrangements Chair of the International Symposium on Nonlinear Theory and Applications in 2000.