DOKUZ EYLÜL UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

SECURE COMMUNICATION VIA PARTIAL SYNCHRONIZATION OF NONLINEAR SYSTEMS

by

Zekeriya SARI

July, 2016

İZMİR

# SECURE COMMUNICATION VIA PARTIAL SYNCHRONIZATION OF NONLINEAR SYSTEMS

A Thesis Submitted to the
Graduate School of Natural And Applied Sciences of Dokuz Eylül University
In Partial Fulfillment of the Requirements for the Degree of Master of Science in
Electrical and Electronics Engineering Program

by

Zekeriya SARI

July, 2016

İZMİR

We have read the thesis entitled "**SECURE COMMUNICATION VIA PARTIAL SYNCHRONIZATION OF NONLINEAR SYSTEMS** " completed by **ZEKERİYA SARI** under supervision of **ASST. PROF. DR. SERKAN GÜNEL** and we certify that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.
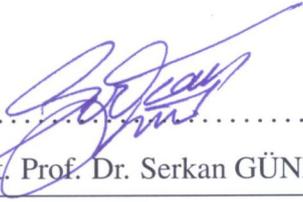
Asst. Prof. Dr. Serkan GÜNEL

Supervisor

Asst. Prof. Dr. M. Emre ÇEK

Jury Member

Doç. Dr. Cem Civelek

Jury Member

Director
Graduate School of Natural and Applied Sciences

ACKNOWLEDGEMENTS

SECURE COMMUNICATION VIA PARTIAL SYNCHRONIZATION OF NONLINEAR SYSTEMS

ABSTRACT

It is well known that due to their sensitive dependence on initial conditions, the chaotic systems are capable of producing unpredictable outputs, characteristically, with a widely spread power spectrum. The idea of using them in secure data transmission have been studied extensively over the past decades and various chaotic communication schemes have been proposed. However, their performance in data transmission have been marginally superior at best compared to the conventional approaches.

In this study, a novel method to design a secure communication system based on the cluster synchronization in networks of chaotic oscillators has been proposed. Cluster synchronization is observed when the nodes of the network synchronize in groups but there is no synchronization in between the groups. In the proposed system, one or more controllable parameters allow the cluster synchronization of different node groups. The symbols to be transmitted are represented by the cluster synchronization modes. The system is divided into two as transmitter and receiver, the change of cluster synchronization mode also changes the dynamics in the receiver side and hence the presence or the absence of the symbols are signified by the synchronization mode in the corresponding cluster. The basic concept and functioning of the proposed system have been illustrated through numerical simulations.

Keywords: Cluster synchronization, secure communication

DOĞRUSAL OLMAYAN SİSTEMLERİN KISMİ SENKRONİZASYONU İLE GÜVENLİ HABERLEŞME

ÖZ

Kaotik sistemlerin, karakteristik olarak, birbirleriyle ilintisiz, geniş frekans bandına sahip, başlangıç koşullarına hassas bağımlılıkları sebebiyle uzun süreli tahmin edilemez çıkışlar ürettikleri bilinmektedir. Bu sistemlerin güvenli veri iletişiminde kullanılması fikri geçmiş on yıllar içerisinde kapsamlı bir şekilde çalışılmıştır ve farklı kaotik iletişim şemaları önerilmiştir. Ancak, bu sistemlerin veri iletişimindeki performansı klasik yöntemlerin üzerine çıkamamıştır.

Bu çalışmada, kaotik sistemlerin öbek senkronizasyonuna dayanan yeni bir güvenli haberleşme sistemi tasarım yöntemi önerilmiştir. Öbek senkronizasyonu, ağdaki düğümlerin kümeler halinde senkronize olduğu ancak kümeler arasında senkronizasyon olmadığı durumda gözlemlenir. Önerilen yöntemde farklı düğüm gruplarının öbek senkronizasyonu bir ya da birden fazla kontrol edilebilir parametre ile sağlanmaktadır. İletilmek istenen semboller öbek senkronizasyon modları ile temsil edilmektedir. Sistem alıcı ve verici olarak ikiye ayrılmıştır, öbek senkronizasyon modunun değişmesi alıcı taraftaki dinamiği de değiştireceğinden sembollerin varlığı veya yokluğu ilgili öbekteki senkronizasyon modu ile belirtilmektedir. Önerilen yöntemin temel kavramı ve işleyişi sayısal benzetimler ile gösterilmiştir.

Anahtar kelimeler: Güvenli haberleşme, öbek senkronizasyonu

CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER ONE
INTRODUCTION

Over the past decades, there has been a significant interest in the study of behavior of the coupled dynamical systems with a special emphasis on the synchronization phenomena. The synchronization means the adjustment of the time scales of the oscillations due to the interaction between the oscillating processes. In this context, frequency synchronization and phase synchronization has been observed in the limit cycle systems (Balanov et al., 2009; Pikovsky et al., 2003). Frequency synchronization means that oscillators adjust their frequencies so as to assure a common frequency ratio while phase synchronization is observed when the phases of the oscillators are locked to some value.

For a long time, the synchronization phenomena have been restricted to the case of periodic and quasi-periodic oscillations. However, with the observation of chaotic behavior, the synchronization family has been enriched. Chaotic systems are nonlinear deterministic systems exhibiting random-like, aperiodic, long-term unpredictable behavior due to their sensitive dependence on initial conditions. The discovery of synchronization of chaotic systems without changing their dynamical characteristics (strange attractors peculiar to chaotic systems, sensitivity to initial conditions) and direct observation of this phenomenon in natural physical and biological systems have led to carefully investigation of synchronization of chaotic systems (Pecora & Carroll, 1990; Fujisaka & Yamada, 1983). In addition to the classical types of synchronization observed in limit cycle systems, numerous other types of synchronization have been reported including complete synchronization, lag synchronization, generalized synchronization (Pecora & Carroll, 1990; Rosenblum et al., 1996, 1997; Yang & Duan, 1998). In complete synchronization, the temporal behavior of coupled dynamical systems are identical. When a delay is allowed between the states of the coupled systems, the synchronization is called lag synchronization. Generalized synchronization is observed when the trajectories of the oscillators are related functionally.

Having studied the synchronization phenomena for small number of oscillators, the study of synchronization has been headed for the study of synchronization in larger, more complex networks of oscillators. The problems of what the possible modes of synchronization in large networks of oscillators are, and under what conditions these interacting dynamical systems are able to synchronize have become an important research area of dynamical systems. These problems have much more variety of results than expected at a first glance (Pecora & Carroll, 1998; Belykh et al., 2000, 2001, 2002, 2004, 2006).

Apart from complete desynchronization, the simplest mode of spatiotemporal behavior in networks of oscillators is the full synchronization. Typically, in the networks of continuous time oscillators, full synchronization is possible, if the coupling strength between the oscillators exceeds a certain threshold (Pecora & Carroll, 1990, 1998; Belykh et al., 2004, 2006). Methods developed to establish bounds for this threshold are based on the calculation of the eigenvalues of the connectivity matrix and a term depending on the individual oscillator dynamics or of the maximum Lyapunov exponent for the least stable transversal mode of the synchronization manifold and the eigenvalues of the connectivity matrix (Pecora & Carroll, 1998). However, it is difficult to satisfy necessary and sufficient conditions for time varying coupling strengths and the stability conditions. This has restricted the use of these methods to regular networks such as ring, star or globally-coupled networks with time invariant coupling strengths. Connection graph based stability method in which Lyapunov function approach is combined with the graph theoretical reasoning has been proposed in (Belykh et al., 2004). In this method, a path is chosen for any pair of nodes in the network and the coupling strength on an edge depends on the sum of all path lengths passing through the edge and a term depending on the individual oscillator dynamics. Since calculation of the eigenvalues of the connectivity matrix and Lyapunov exponents are avoided, the connection graph based stability method is applicable to complex networks such as small-world networks and scale-free networks with possibly time varying coupling strengths. The coupling strengths on the nodes may also be different from each other (Belykh et al., 2004).

Cluster synchronization is possible in the networks of oscillators in which the oscillators in the network synchronize in groups, but there is no synchronization among the groups (Belykh et al., 2000, 2001, 2002, 2003b; Ma et al., 2006; Belykh et al., 2008; Liu et al., 2011). This type of synchronization has also particular importance in biological sciences where the spatiotemporal behavior of coupled cells or functional units each exhibiting complicated nonlinear behavior. As in the case of full synchronization, cluster synchronization is directly related to the existence of stable linear invariant manifolds. Recently, existence of a family of stable linear invariant manifolds in an array of diffusively coupled identical continuous time oscillators with zero flux or periodic boundary conditions have been discovered (Belykh et al., 2000). Depending on the number of oscillators in the network and the boundary conditions, these invariant cluster synchronization manifolds have an embedding and exhibits a certain hierarchy. The study of existence and stability of cluster modes for one dimensional array of diffusively coupled identical continuous time oscillators has been extended to the two and three dimensional lattices of diffusively coupled continuous time identical oscillators (Belykh et al., 2002, 2003b). It has also been shown that these stable cluster modes are preserved up to %10 -%15 parameter mismatch when the delta-synchronization is considered which means δ neighborhood of the corresponding cluster synchronization manifold is globally stable (Belykh et al., 2003a). Apart from the investigation of the existence of the possible cluster modes for a given network, a couple of methods have also been developed to realize the arbitrarily selected cluster modes in a network of oscillators (Ma et al., 2006; Liu et al., 2011). In (Ma et al., 2006) a method has been proposed in which a sparse coupling matrix with cooperative and competitive weight couplings is constructed to stabilize the arbitrarily selected cluster mode. By the constructed coupling matrix the authors derive a sufficient condition for the global stability of the arbitrarily selected cluster mode which depends on the number of nodes in the smallest cluster as well as the dynamics of the individual nodes and the way the oscillators are coupled. Liu et al. (2011) extends these studies to a general class of more general couplings, reveals the positive and negative effects of a given coupling scheme for cluster synchronization and a method has been developed to adapt the

given coupling scheme to achieve cluster synchronization.

It is well known that due to the sensitive dependence on initial conditions, the chaotic systems are capable of producing unpredictable outputs, characteristically. The idea of using them in secure data transmission has been studied extensively for the past decades (Parlitz et al., 1992; Cuomo & Oppenheim, 1993; Kennedy & Hasler, 1993; Strogatz & Oppenheim, 1993). Chaos based secure communication systems can mainly be divided into two as analog chaos based communication systems which rely on chaos synchronization and digital chaos based ciphers employing completely different principles.

Since the chaotic systems are employed as transmitter and receiver in the analog chaos based communication systems, three different types of coupling is possible i.e. drive-response coupling, mutual coupling and external driving. In drive-response coupling, also called as master-slave coupling, one of the chaotic system drives the other resulting in bidirectional interaction, while in mutual coupling the chaotic systems influence each other equally resulting in bidirectional interaction. In the case of external coupling, an external force drives the chaotic systems resulting in directional interaction. Drive-response coupling is the one by far the most used in analog chaos based communication systems among all.

Chaotic masking, chaotic switching and chaotic modulation constitutes the basic methods exploited in the analog chaos based communication systems (Abel & Schwarz, 2002; Li et al., 2007). In chaotic masking, the message signal is added to the chaotic carrier signal to form the driving signal. In the receiver side, an estimation of the chaotic carrier signal is generated via the chaos synchronization and hence the message signal can be extracted. In order not to obstruct the chaotic synchronization, the power of the information signal must be lower than that of the chaotic carrier signal. The message signal cannot be extracted exactly, since it disturbs the synchronization. Hence, the bit error rate of the communication system employing chaotic masking is not satisfactory for low signal-to-noise ratios.

Two or more chaotic systems in the transmitter side and one chaotic systems in the

receiver side is used in the chaotic switching method. As the name implies, chaotic systems in the transmitter side is switched depending on the message signal. The message signal is recovered using the chaotic synchronization in the receiver side. The symbol transmission time must be long enough to ensure chaotic transmission and hence the transmission rate of the chaotic switching method is lower than that of the chaotic masking method.

The dynamics of the chaotic systems in the previous methods are not effected during the symbol transmission. This is not the case in the chaotic modulation method. In chaotic modulation method, the message is injected continuously to the chaotic system in the transmitter side. In the receiver side, the message is extracted by applying inverse of the system that are in the transmitter side. The change of dynamics can either be in the form of parameter modulation in which one or more system parameters are modulated by the information signal or in the form of direct modulation in which the message signal is injected into one or more states of the chaotic systems in the transmitter side. The main disadvantage of the chaotic modulation systems is that the convergence issues that needs additional consideration.

Numerous cryptoanalysis work showed that most of the analog chaos based communication systems are not secure in cryptological sense (Li et al., 2007). Although new methods have been proposed to overcome these, not much progress have been achieved.

In this study, a novel method to design a secure communication system based on the cluster synchronization in networks of chaotic oscillators has been proposed. In the proposed system, one or more controllable parameters allows the cluster synchronization of different node groups (Figure 1.1). The symbols to be transmitted are represented by the cluster synchronization modes. The system is divided into two as transmitter and receiver, the change of cluster synchronization mode also changes the dynamics in the receiver side and hence the presence or the absence of the symbols are signified by the synchronization mode in the corresponding cluster. Coupling strengths are determined so that cluster mode corresponding to the symbol

to be transmitted is enforced. All the nodes are in their chaotic regime and the nodes connecting the transmitter side and the receiver side are not in the same cluster. Therefore, by construction, the signals transmitted from the transmitter to the receiver are always chaotic. The transmitted signal is not directly modulated by the message signal to be sent and when obtained by third party, it cannot be resolved without the knowledge of the transmitter and the receiver internal topologies.

This thesis is organized as follows: The necessary and sufficient conditions to realize and globally asymptotically stabilize arbitrarily-selected cluster mode in a network of identical chaotic oscillators is studied in Chapter II. The requirements of a typical communication system and summary of the chaotic communication schemes in the literature along with their performance comparison to the classical communication schemes are given in Chapter III. Chapter IV presents the methodology of using cluster synchronization in networks of chaotic systems. Simulation results of the proposed system are given in Chapter V.
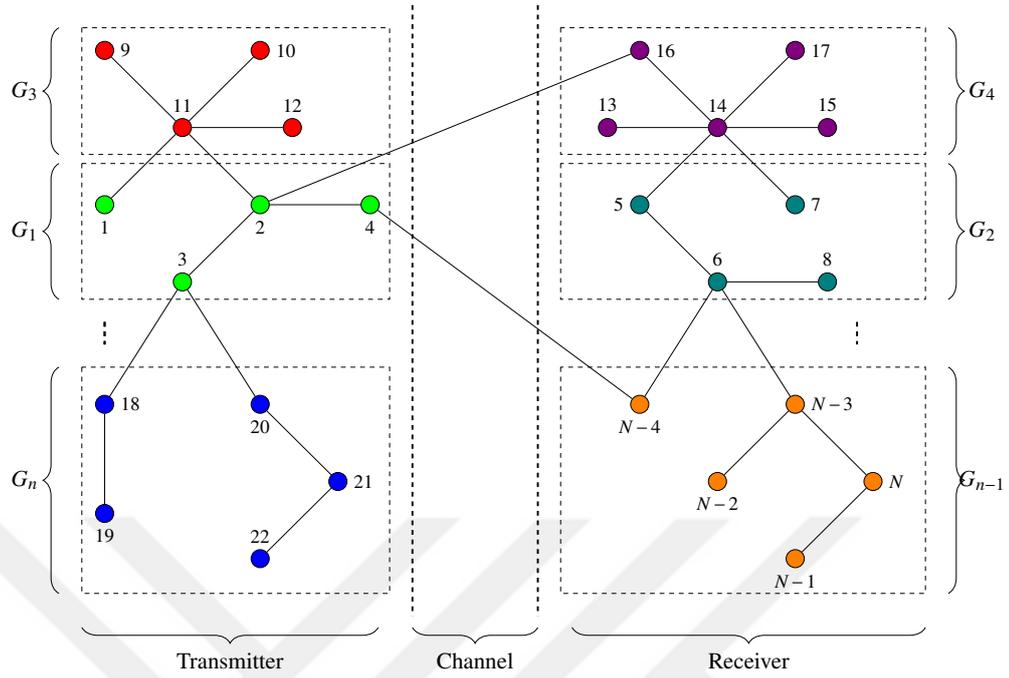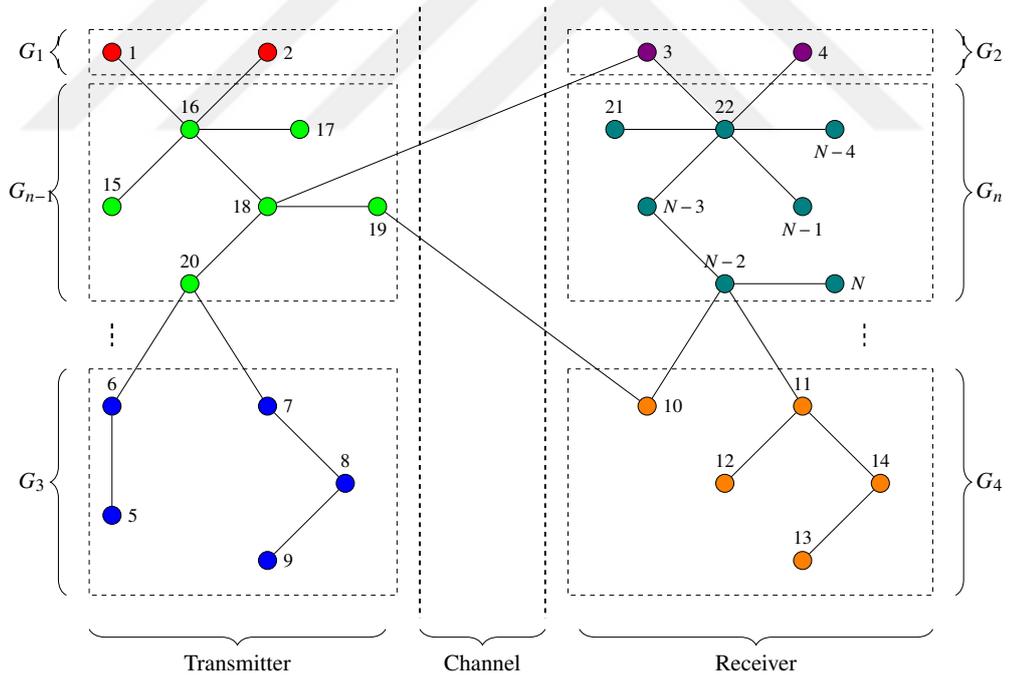
Figure 1.1 An arbitrary network of identical chaotic oscillators. The oscillators are illustrated by circles and the oscillators with the same gray level are in the same cluster. (a) The cluster mode for symbol s_j. (b) The cluster mode for symbol s_k.

CHAPTER TWO

ARBITRARY CLUSTERS OF NETWORKS OF CHAOTIC SYSTEMS

2.1 Preliminary Definitions

We start with necessary definitions to be used in the sequel.

Definition 2.1.1. Consider a network of N nodes, labeled with integers $i = 1, 2, \ldots, N$. Consider a symmetric matrix $C = [c_{ij}] \in \mathbb{R}^{N \times N}$. The coupling between the node i and the node j is called as cooperative if $c_{ij} > 0$ and competitive if $c_{ij} < 0$.

Definition 2.1.2. A symmetric matrix $C = [c_{ij}] \in \mathbb{R}^{N \times N}$ with zero row sums, i.e.

$$\sum_{j=1}^{N} c_{ij} = 0, \quad i = 1, \ldots, N \tag{2.1}$$

is called as diffusively coupled matrix, denoted as $C \in \mathbb{C}_1$, where $\mathbb{C}_1$ is the set of all diffusively coupled matrices.

Definition 2.1.3. A symmetric matrix $C = [c_{ij}] \in \mathbb{C}_1$ with $c_{ij} \geq 0$, $i \neq j$ is called non-negative diffusively coupled matrix, denoted as $C \in \mathbb{C}_2$, where $\mathbb{C}_2$ is the set of all non-negative diffusively coupled matrices.

Definition 2.1.4. A symmetric matrix $C = [c_{ij}] \in \mathbb{C}_1$ with $c_{ij} = 1$, $i \neq j$ is called globally non-negative diffusively coupled matrix, denoted as $C \in \mathbb{C}_3$, where $\mathbb{C}_3$ is the set of all globally non-negative diffusively coupled matrices.

Definition 2.1.5. A k-dimensional manifold M in d-dimensional space can be thought of the solution of the vector equation,

$$h(\boldsymbol{x}(t)) = 0, \quad \boldsymbol{x}(t) \in \mathbb{R}^d, \quad h : \mathbb{R}^d \mapsto \mathbb{R}^{d-k} \tag{2.2}$$

Definition 2.1.6. A manifold M is an invariant manifold of,

$$\dot{\boldsymbol{x}}(t) = f(\boldsymbol{x}(t)), \quad \boldsymbol{x}(t) \in \mathbb{R}^d, \quad f : \mathbb{R}^d \mapsto \mathbb{R}^d \tag{2.3}$$

if the flow generated by (2.3) is tangent to the manifold M which implies,

$$\nabla h \cdot f \Big|_{h(\boldsymbol{x}(t))=0} \equiv 0 \tag{2.4}$$

Definition 2.1.7. An invariant manifold M of (2.3) is globally asymptotically stable, if it attracts all its outside trajectories as time goes to infinity, i.e. let $\boldsymbol{x}(t, \boldsymbol{x}_0, t_0)$ be the solution at time t with an initial condition $\boldsymbol{x}_0$ at time t_0, then,

$$\lim_{t \to \infty} \boldsymbol{x}(t, \boldsymbol{x}_0, t_0) \in M \tag{2.5}$$

Definition 2.1.8. The system in (2.3) is eventually dissipative, if there exist a compact set

$$B = \{\boldsymbol{x} \mid \|\boldsymbol{x}\| \le b_1, \quad \boldsymbol{x} \in \mathbb{R}^d\} \tag{2.6}$$

and a Lyapunov function $V = \boldsymbol{x}^T \boldsymbol{Q} \boldsymbol{x}$, where $\boldsymbol{Q}$ is a positive definite matrix, whose time derivative along the trajectories of (2.3) is negative outside of this set B, i.e.,

$$\dot{V} = \boldsymbol{x}^T \boldsymbol{Q} f(\boldsymbol{x}) < 0, \quad \boldsymbol{x} \in \mathbb{R}^d, \quad \boldsymbol{x} \notin B \tag{2.7}$$

Definition 2.1.9. The dynamical system in (2.3) is called topologically transitive if for every open subsets $\mathbb{U}$ and $\mathbb{V}$ of $\mathbb{X}$ there exists $k \in \mathbb{N}$ such that $s^{(k)}(t, t_0, \mathbb{U}) \cap \mathbb{V} \ne \emptyset$ where $s(t, t_0, \boldsymbol{x}_0)$ is the state transition function of (2.3) (Li & Ye, 2016).

Definition 2.1.10. The dynamical system in (2.3) has sensitive dependence on initial conditions if there exists $\delta > 0$ such that for each $\boldsymbol{x} \in \mathbb{X}$ and each $\epsilon > 0$ there is $\boldsymbol{y} \in \mathbb{X}$ with $d(\boldsymbol{x}, \boldsymbol{y}) < \epsilon$ and $k \in \mathbb{N}$ such that $d(s^{(k)}(t, t_0, \boldsymbol{x}), s^{(k)}(t, t_0, \boldsymbol{y})) > \delta$, where d is any metric in $\mathbb{X}$ and $s(t, t_0, \boldsymbol{x}_0)$ is the state transition function of (2.3) (Li & Ye, 2016).

2.2 Arbitrary Clusters of Networks of Chaotic Systems

Although the literature has different definitions for chaotic systems suggested by Li & Yorke, Block & Coppel (Aulbach & Kieninger, 2001) and Wiggins (Wiggins, 2003), we adopt the definition introduced by Devaney. A chaotic system with the dynamics in (2.3) is called Devaney chaotic if it satisfies the following properties (Li & Ye, 2016):

1. (2.3) is topologically transitive,

2. (2.3) has sensitive dependence on initial conditions,

3. the set of periodic orbits of (2.3) is dense[1]

Consider a network consisting of identical chaotic oscillators given as,

$$\dot{x}_i = f(x_i) + \sum_{j=1}^{N} \epsilon_{ij}(t) P x_j, \quad i = 1, 2, \dots, N \tag{2.9}$$

where $x_i \in \mathbb{R}^d$ is the state vector of the ith node, $f : \mathbb{R}^d \mapsto \mathbb{R}^d$ is the vector function defining the individual node dynamics, $\epsilon_{ij}(t) \in \mathbb{R}$ is the coupling strength between the ith and j^{th} nodes, N is the number of nodes. The diagonal matrix $P = diag(p_1, p_2, \dots, p_d) \in \mathbb{R}^{d \times d}$, where $p_k > 0$ for $k = 1, \dots, s$ and $p_k = 0$ for $k = s + 1, \dots, d$ determines by which state variables the oscillators are coupled. The symmetric matrix with zero row sums $E(t) = [\epsilon_{ij}(t)] \in \mathbb{R}^{N \times N}$ determines the network topology, i.e. $\epsilon_{ij}(t) \neq 0$ if there exist coupling between the ith and j^{th} node and $\epsilon_{ij}(t) = 0$, otherwise. We consider the networks whose coupling matrix $E(t)$ can be decomposed into a time variant part $U(t) = [u_{ij}(t)] \in \mathbb{R}^{N \times N}$ and a time invariant part $C = [c_{ij}] \in \mathbb{R}^{N \times N}$ i.e., $E(t) = U(t) \circ C$, where $\circ$ denotes the element-wise product[2] of matrices.

Denoting $X = [x_1^T, \dots, x_N^T]^T$, and $F(X) = [f^T(x_1), \dots, f^T(x_N)]^T$, the network in (2.9) can be written more compactly as,

$$\dot{X} = F(X) + \big(E(t) \otimes P\big) X = F(X) + D(t) X \tag{2.10}$$

where $\otimes$ is Kronecker delta product and $D(t) = E(t) \otimes P$.

Following the formalism in (Ma et al., 2006), assume that the oscillators are labeled with integers, $\{1, 2, \dots, N\}$ and the network is divided into n clusters as $G_1 = \{1, \dots, m_1\}$, $\dots$ $G_n = \{\sum_{i=1}^{n-1} m_i + 1, \dots, \sum_{i=1}^{n} m_i = N\}$, where m_j is the number of nodes in the jth cluster. We can assume without loss of generality $m_1 \leq \dots \leq m_n$. The

---

[1]A subset $\mathbb{U}$ of a topological space $\mathbb{X}$ is called dense in $\mathbb{X}$ if,

$$x \in \mathbb{U} \text{ or } x \in \mathbb{U}', \quad \forall x \in \mathbb{X} \tag{2.8}$$

where $\mathbb{U}'$ denotes the set of all limit points of $\mathbb{U}$ (Steen et al., 1978).

[2]Element-wise product of matrices is also called as Hadamard product and denoted by various symbols such as $\bullet$, $\cdot$, $\odot$ in the literature.

notation "$i \sim j$" denotes that the ith and j^{th} nodes are in the same cluster. $\overline{G}_{\tilde{k}}$ is the number of nodes that are in the same cluster with the kth node. Associated with these clusters, the network in (2.10) can be decomposed as,

$$\dot{X}_i = F(X_i) + \sum_{j=1}^{n} D_{ij}(t)X_j, \quad i = 1,\ldots,n \tag{2.11}$$

The cluster synchronization is observed when the nodes forming the same cluster are synchronized i.e. for $k = 1,\ldots,n$ there exist l,m with $\sum_{i=1}^{k-1} m_i + 1 \leq l,m \leq \sum_{i=1}^{n} m_i$ such that $\|x_l(t) - x_m(t)\| \mapsto 0$ as $t \mapsto 0$. The invariant manifold M corresponding to the cluster synchronization is given by $M = \{x_1 = \ldots = x_{m_1},\ldots,x_{m_1+\ldots+m_{n-1}+1} = \ldots = x_N\}$.

Considering the time invariant coupling strength i.e., $u_{ij}(t) = \epsilon_1$, $i,j = 1,\ldots,N$, $\forall t$, the realization of arbitrary clusters and assurance of the stability of them require solution of two problems consequently; constructing the coupling matrix and adjusting the coupling strength between the nodes. In (Ma et al., 2006), this problem has been solved by following two steps; i.e. construction of the coupling matrix to realize the selected cluster synchronization manifold and derivation of a sufficient condition about the global asymptotic stability of the cluster synchronization invariant manifold.

The construction of the coupling matrix to realize the selected cluster synchronization invariant manifold is based on the following lemma.

Lemma 2.2.1. *If a matrix C has the form,*

$$C = \begin{bmatrix} 3C_{11} & C_{12} & 0 & 0 & \ldots & 0 & 0 \\ C_{11} & 5C_{12} & C_{23} & 0 & \ldots & 0 & 0 \\ 0 & C_{32} & 5C_{33} & \ddots & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \ldots & 5C_{n-1,n-1} & C_{n-1,n} \\ 0 & 0 & 0 & 0 & \ldots & C_{n,n-1} & 3C_{n,n} \end{bmatrix} \tag{2.12}$$

where

$$C_{ii} \in \mathbb{R}^{m_i \times m_i}$$

$$C_{ii} \in \mathbb{C}_3$$

$$C_{i,i+1} \in \mathbb{R}^{m_i \times m_{i+1}} \tag{2.13}$$

$$C_{i+1,i}^T = C_{i,i+1} = (C_{ii}, \mathbf{0}) \; if \; m_i < m_{i+1}$$

$$C_{i+1,i}^T = C_{i,i+1} = C_{ii} \; if \; m_i = m_{i+1}$$

then, the eigenvalues of C satisfy,

i. $\lambda_i = 0$ *for* $i = 1, \ldots, n$ *associated with eigenvectors* $\zeta_i = [\eta_{1i}, \ldots, \eta_{ni}]$ *where* $\eta_{ki} \in \mathbb{R}^{m_k}$, $\eta_{ki} = [1, 1, \ldots, 1]^T$ *if* $k = i$ *and* $\eta_{ki} = [0, 0, \ldots, 0]^T$ *if* $k \neq i$.

ii. $\lambda_i < 0$ *for* $i = n + 1, \ldots, N$.

Proof. See Ma et al. (2006). □

If the coupling matrix C in (2.9) is constructed in the form given in (2.12), then 0 is an eigenvalue of C with multiplicity n associated with n linearly independent eigenvectors, and hence, the manifold M is an invariant manifold of (2.9).

The global asymptotic stability of the cluster synchronization manifold M is investigated by considering the error dynamics in the clusters. Let us denote the error between i^{th} node and j^{th} node that are in the same cluster as,

$$e_{ij} = \boldsymbol{x}_j - \boldsymbol{x}_i, \quad i, j = 1, \ldots, N, \; i \sim j \tag{2.14}$$

Since C is a zero-row-sum matrix, using $\sum_{k=1}^{N} c_{ik} \boldsymbol{P} \boldsymbol{x}_i = 0$, $i = 1, \ldots, N$ and (2.9), the error dynamics is governed by,

$$\dot{e}_{ij} = f(\boldsymbol{x}_j) - f(\boldsymbol{x}_i) + \epsilon_1 \sum_{k=1}^{N} \left(c_{jk} \boldsymbol{P} e_{jk} - c_{ik} \boldsymbol{P} e_{ik} \right), \quad i, j = 1, \ldots, N, \; i \sim j \tag{2.15}$$

Let Df denote the Jacobian of f, then (2.15) can be written as,

$$\dot{e}_{ij} = \left[\int_0^1 Df(\beta \boldsymbol{x}_j + (1 - \beta) \boldsymbol{x}_i) d\beta \right] e_{ij} + \epsilon_1 \sum_{k=1}^{N} \left(c_{jk} \boldsymbol{P} e_{jk} - c_{ik} \boldsymbol{P} e_{ik} \right), \quad i, j = 1, \ldots, N, \; i \sim j \tag{2.16}$$

Adding and subtracting the term Ae_{ij} to (2.16) to suppress the positive eigenvalues of Df, where $A = diag(a_1,\ldots,a_d)$, $a_k > 0$ for $k = 1,\ldots,s$ and $a_k = 0$ for $k = s+1,\ldots,d$ (recall that s is the number of nonzero elements in diagonal matrix P), we have,

$$\dot{e}_{ij} = \left[\int_0^1 Df(\beta x_j + (1-\beta)x_i)d\beta - A\right]e_{ij} +$$
$$Ae_{ij} + \epsilon_1 \sum_{k=1}^N \left(c_{jk}Pe_{jk} - c_{ik}Pe_{ik}\right), \quad i,j = 1,\ldots,N, \; i \sim j \quad (2.17)$$

The asymptotic global stability of the origin of the (2.17) implies the asymptotic global stability of M. Before going any further in the stability analysis we need some assumptions.

We assume that individual systems $\dot{x}_i = f(x_i)$ are eventually dissipative, then it can be shown that the coupled network (2.9) is eventually dissipative (Ma et al., 2006).

Considering the auxiliary system,

$$\dot{e}_{ij} = \left[\int_0^1 Df(\beta x_j + (1-\beta)x_i)d\beta - A\right]e_{ij}, \quad i,j = 1,\ldots,N, \; i \sim j \quad (2.18)$$

we assume Lyapunov functions of the form,

$$W_{ij} = \frac{1}{2}e_{ij}^T Q e_{ij}, \quad i,j = 1,\ldots,N, \; i \sim j \quad (2.19)$$

where $Q = diag(q_1,\ldots,q_s,Q_1)$, $q_1 > 0,\ldots,q_s > 0$ and $Q_1 \in \mathbb{R}^{(d-s)\times(d-s)}$ is a positive definite matrix, whose time derivative along the trajectories of (2.18) is negative, i.e.,

$$\dot{W}_{ij} = e_{ij}^T Q \left[Df(\beta x_j + (1-\beta)x_i)d\beta - A\right]e_{ij} < 0, \quad i,j = 1,\ldots,N, \; i \sim j \quad (2.20)$$

The following theorem gives the sufficient condition for the global asymptotic stability of the cluster synchronization manifold.

Theorem 2.2.2. *Under the eventual dissipativeness of (2.9) and assumption (2.20) and with the coupling matrix taken in the form given in (2.12), invariant manifold M of (2.9) is globally asymptotically stable, if the following inequality holds:*

$$\epsilon_1 \sum_{i=1}^N \sum_{j\sim i} \overline{G}_{\tilde{j}} e_{ji}^T Q P e_{ji} \geq \sum_{i=1}^N \sum_{j\sim i} e_{ji}^T Q A e_{ji} \quad (2.21)$$

Proof. See Ma et al. (2006). □

Corollary 2.2.3. *Since $\overline{G}_{\tilde{1}} = \ldots = \overline{G}_{\tilde{m}_1} = m_1 \leq \ldots \leq \overline{G}_N = m_n$, we have,*

$$\epsilon_1 \sum_{i=1}^{N} \sum_{j \sim i} \overline{G}_{\tilde{j}} e_{ji}^T QP e_{ji} \geq \epsilon_1 \sum_{i=1}^{N} \sum_{j \sim i} m_1 e_{ji}^T QP e_{ji} \qquad (2.22)$$

Then, if

$$\epsilon_1 \sum_{i=1}^{N} \sum_{j \sim i} m_1 e_{ji}^T QP e_{ji} \geq \sum_{i=1}^{N} \sum_{j \sim i} e_{ji}^T QA e_{ji} \qquad (2.23)$$

holds, the Theorem 2.2.2 is satisfied.

Remark 2.2.4. Since $P = diag(p_1, p_2, \ldots, p_d) \in \mathbb{R}^{d \times d}$, where $p_k > 0$ for $k = 1, \ldots, s$ and $p_k = 0$ for $k = s+1, \ldots, d$ and $A = diag(a_1, \ldots, a_d)$, $a_k > 0$ for $k = 1, \ldots, s$ and $a_k = 0$ for $k = s+1, \ldots, d$, (2.23) is satisfied if,

$$\epsilon_1 \geq \frac{1}{m_1} \max_{1 \leq k \leq s} \frac{a_k}{p_k} \qquad (2.24)$$

holds.

Note from Corollary 2.2.3 that the synchronization threshold to globally asymptotically stabilize the selected cluster synchronization manifold depends on the number of nodes in the smallest cluster (m_1), a term depending on the individual node dynamics (a_h) and the way the oscillators are coupled (p_h).

2.3 Cluster Synchronization of Lorenz Systems

The Lorenz system defined by,

$$\begin{aligned}
\dot{x}^{(1)} &= \sigma(x^{(2)} - x^{(1)}) \\
\dot{x}^{(2)} &= x^{(1)}(r - x^{(3)}) - x^{(2)} \\
\dot{x}^{(3)} &= x^{(1)}x^{(2)} - bx^{(3)}
\end{aligned} \qquad (2.25)$$

is chaotic for the parameter values $\sigma = 10.0$, $b = 8.0/3.0$, $r = 28.0$ (Lorenz, 1963). Figure 2.1 shows the time waveform of $x^{(1)}$ state and the chaotic attractor for the given parameter values.
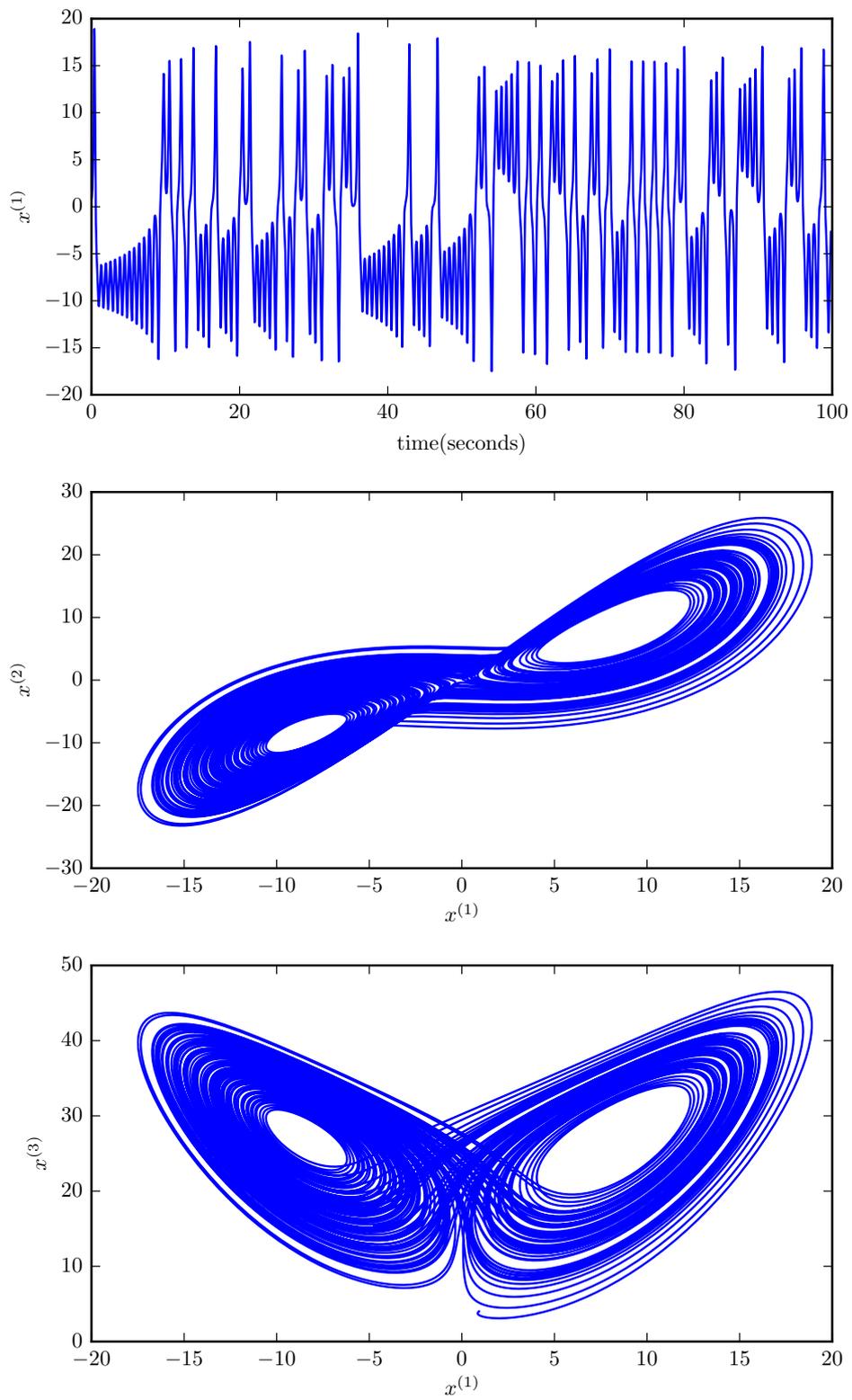
Figure 2.1 Time waveform and projections of three dimensional attractor of the Lorenz system. The parameter values are $\sigma = 10.0$, $b = 8.0/3.0$, $r = 28.0$. Upper plot shows $x^{(1)}$ state, middle plot shows the projection of the attractor on $x^{(1)} - x^{(2)}$ plane, lower plot shows the projection of the attractor on $x^{(1)} - x^{(3)}$ plane.

15
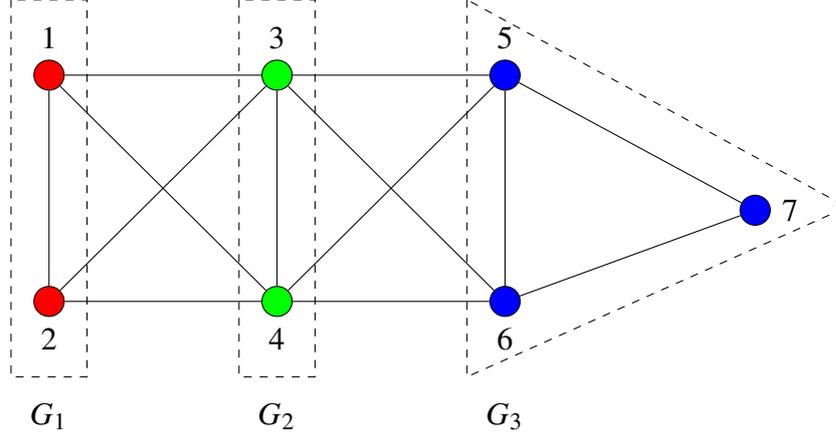
Figure 2.2 A network of 7 identical Lorenz oscillators. Oscillators are represented by circles and the oscillators with the same gray level are in the same cluster.

Consider a network of 7 identical oscillators with the dynamics in (2.9) that are coupled by their $x^{(1)}$ states i.e. $P = diag(1,0,0)$ with equal time invariant coupling strength i.e. $\epsilon_{ij}(t) = \epsilon_1$, $\forall t \geq 0$. Then, we have,

$$
\begin{aligned}
\dot{x}_i^{(1)} &= \sigma(x_i^{(1)} - x_i^{(2)}) + \epsilon_1 \sum_{j=1}^{N} c_{ij} \\
\dot{x}_i^{(2)} &= r x_i^{(1)} - x_i^{(2)} - x_i^{(1)} x_i^{(3)} \\
\dot{x}_i^{(3)} &= -b x_i^{(3)} + x_i^{(1)} x_i^{(2)}, \quad i = 1,2,\ldots,7
\end{aligned}
\tag{2.26}
$$

Assume that the clusters $G_1 = \{1,2\}$, $G_2 = \{3,4\}$, $G_3 = \{5,6,7\}$ are desired to be realized as shown in Figure 2.2. The individual Lorenz system is eventually dissipative with an absorbing domain,

$$
B_i = \left\{ \left(x_i^{(1)}\right)^2 + \left(x_i^{(2)}\right)^2 + \left(x_i^{(3)} - r - \sigma\right)^2 < \frac{b^2(r+\sigma)^2}{4(b+1)} \right\}, \quad i = 1,\ldots,7
\tag{2.27}
$$

and the assumption (2.20) corresponding to the auxiliary system of (2.26) is satisfied with $H = I$ and $A = diag(a,0,0)$, where $a = \dfrac{b(b+1)(r+\sigma)^2}{16(b-1)} - \sigma$ (Belykh et al., 2004).

According to Theorem 2.2.2, the clusters $G_1 = \{1,2\}$, $G_2 = \{3,4\}$, $G_3 = \{5,6,7\}$ are

realized if the coupling matrix is constructed as follows,

$$C = \begin{bmatrix} -3 & 3 & -1 & 1 & 0 & 0 & 0 \\ 3 & -3 & 1 & -1 & 0 & 0 & 0 \\ -1 & 1 & -5 & 5 & -1 & 1 & 0 \\ 1 & -1 & 5 & -5 & 1 & -1 & 0 \\ 0 & 0 & -1 & 1 & -6 & 3 & 3 \\ 0 & 0 & 1 & -1 & 3 & -6 & 3 \\ 0 & 0 & 0 & 0 & 3 & 3 & -6 \end{bmatrix} \tag{2.28}$$

and the coupling strength satisfies the following inequality,

$$\epsilon_1 \geq \frac{1}{m_1} \max_{1 \leq h \leq s} \frac{a_h}{p_h} = \frac{1}{2}a = \frac{1}{32} \frac{b(b+1)(r+\sigma)^2}{(b-1)} - \frac{1}{2}\sigma \tag{2.29}$$

The system in (2.26) has been numerically integrated with Runga-Kutta method for 100 seconds with a step size of 0.01 seconds. Figure 2.3 depicts that $e_{ij} \mapsto 0$ as $t \mapsto \infty$, if i and j are in the same cluster and Figure 2.4 shows that $e_{ij} \nrightarrow 0$ as $t \mapsto \infty$ if i and j are not in the same cluster. Similar results in tabular format are given in Figure 2.5 where the straight lines and squiggles in the grids imply presence and absence of the synchronization of the corresponding oscillator pairs, respectively. Hence the cluster synchronization invariant manifold $M = \{x_1 = x_2, x_3 = x_4, x_5 = x_6 = x_7\}$ corresponding to clusters $G_1 = \{1,2\}$, $G_2 = \{3,4\}$, $G_3 = \{5,6,7\}$ is globally asymptotically stable.

17
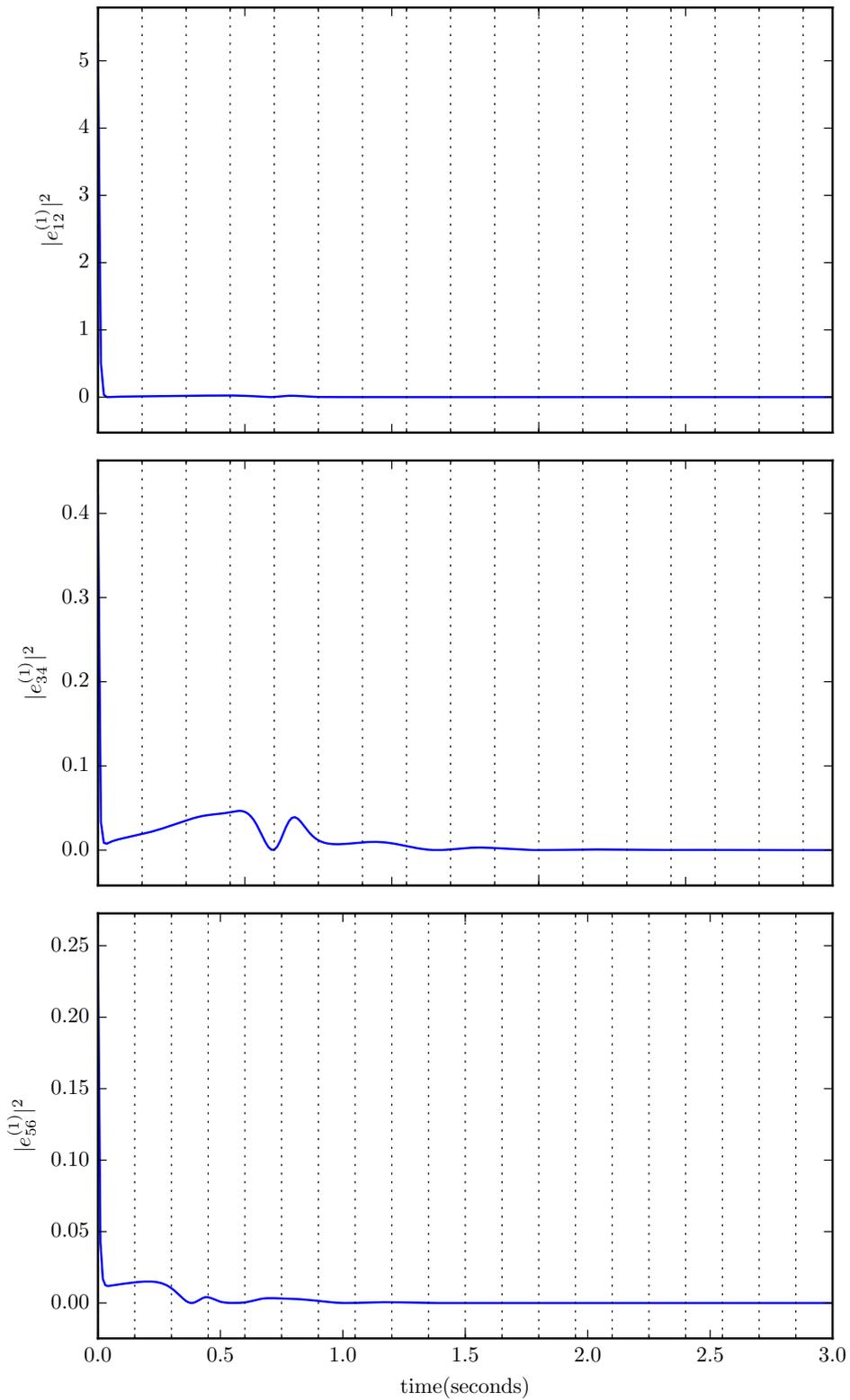
Figure 2.3 Time waveforms of errors between the oscillators that are in the same cluster. The plots share the time axis. It is seen that as $t \mapsto \infty$, $\|x_i - x_j\| \mapsto 0$ if i and j are in the same cluster.
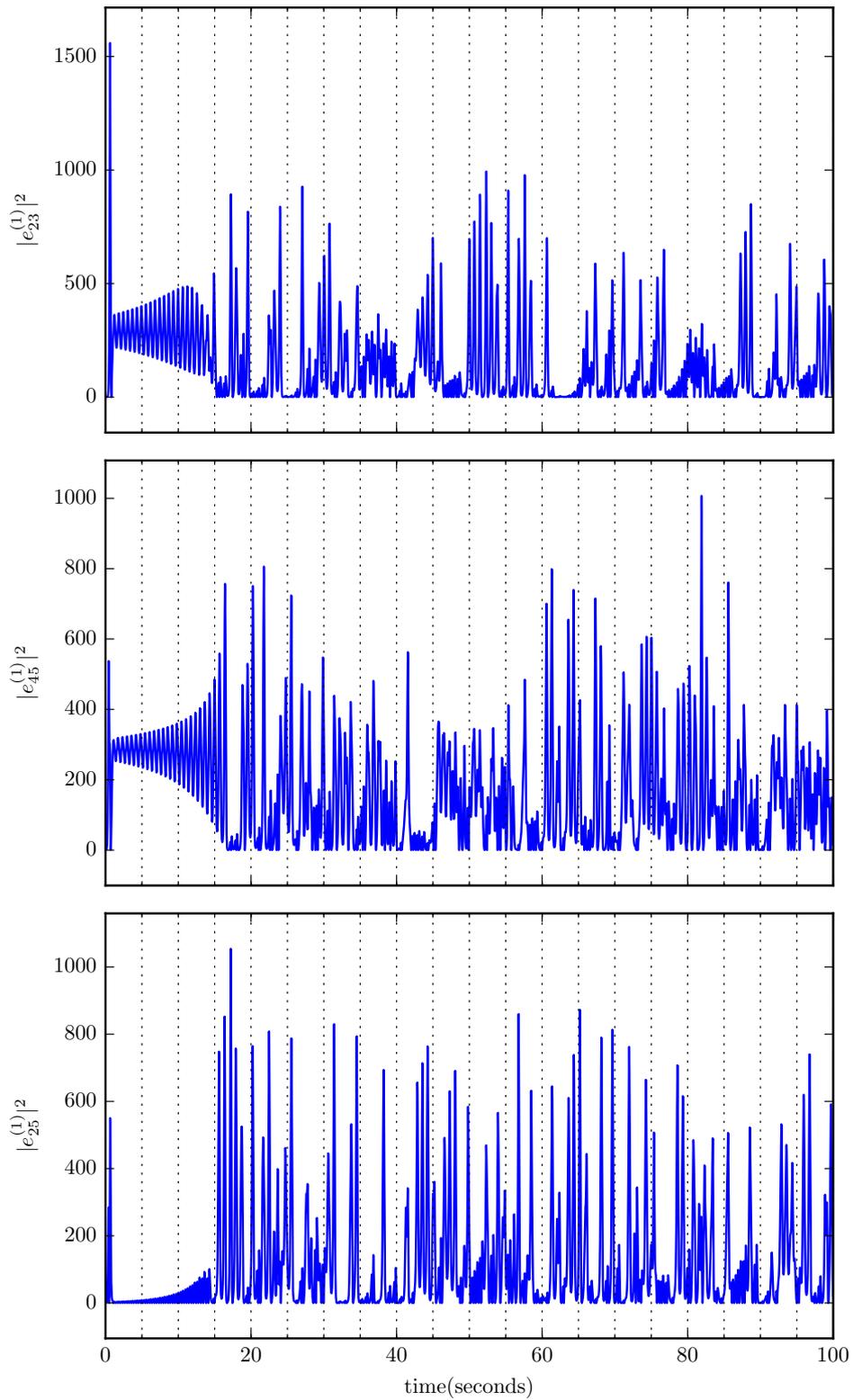
Figure 2.4 Time waveforms of errors between the oscillators that are not in the same cluster. The plots share the time axis. It is seen that as $t \mapsto \infty$, $\|x_i - x_j\| \nrightarrow 0$ if i and j are not in the same cluster.

19
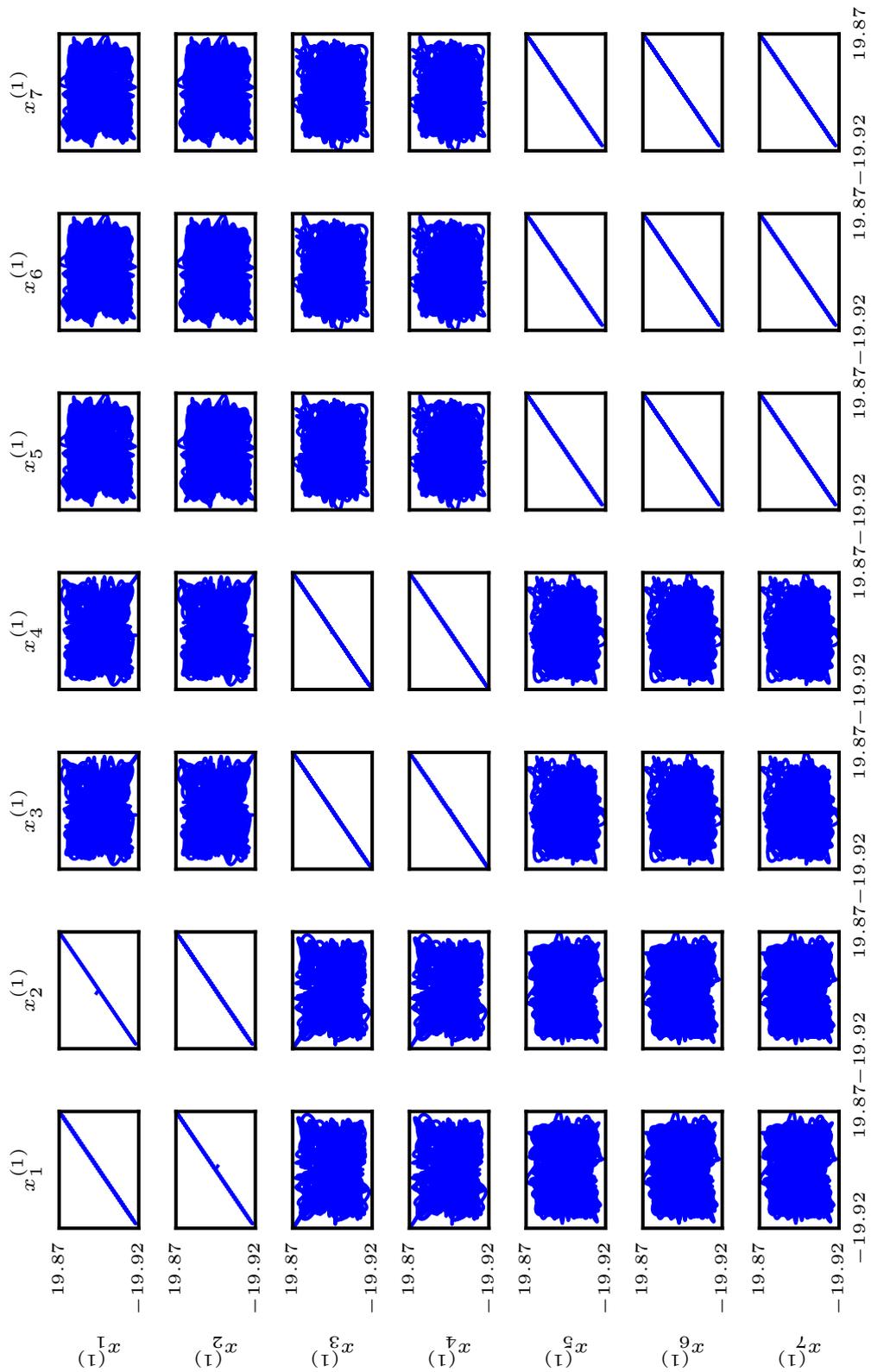
Figure 2.5 $x_i^{(1)}$ versus $x_j^{(1)}$ for $i,j = 0,\ldots,6$ for the system in (2.26). The grids in the figure show $x_i^{(1)}$ versus $x_j^{(1)}$ for $i,j = 1,\ldots,7$. The figures in the grids share their x-axis and y-axis. The straight lines and squiggles in the grids imply presence and absence of the synchronization of the corresponding oscillators pairs, respectively. The formation of the clusters $G_1 = \{1,2\}$, $G_2 = \{3,4\}$ and $G_3 = \{5,6,7\}$ is apparent from the figures

.

CHAPTER THREE
CHAOS IN COMMUNICATION SYSTEMS

Communication systems are designed to transmit information between a sender a recipient that are considered to be remotely located. There are some basic requirements such as efficiency, security and robustness that should be satisfied by a modern communication system.

Direct transmission of the message is not efficient since some parts of the information content is redundant. For an efficient transmission, these unnecessary content should be removed before transmission. This removal of unnecessary message content is achieved by source encoding which is applicable to digital signals. Digitized transmission of information makes it possible to use effective source encoding techniques.

The message to be sent is transmitted through a physical medium called as channel which is generally publicly accessible. If the message to be sent is secret, secure transmission of the message is required in the sense that the message content should not be resolved by any unwanted third party. Encryption techniques from cryptology are exploited to meet the security requirements of a communication system.

The message signal may not be suitable for the channel through which the transmission is performed. For example, an audio signal with a bandwidth of kHz range is not suitable for a direct transmission through a wireless channel with a bandwidth of MHz range. Process of message signals to meet the requirements of the channel is called modulation. By means of modulation, message signal is buried on a carrier signal suitable for the requirements of the channel. Although modulation is performed, the received signal is not exact copy of the transmitted signal. Noise and interference by ambient signals on the channel as well as filtering effect of the channel, distort the transmitted signal. Since one wishes an undistorted transmission, robustness of the transmission to these distortion effects should be considered which can partly be solved by the use of channel encoding techniques.
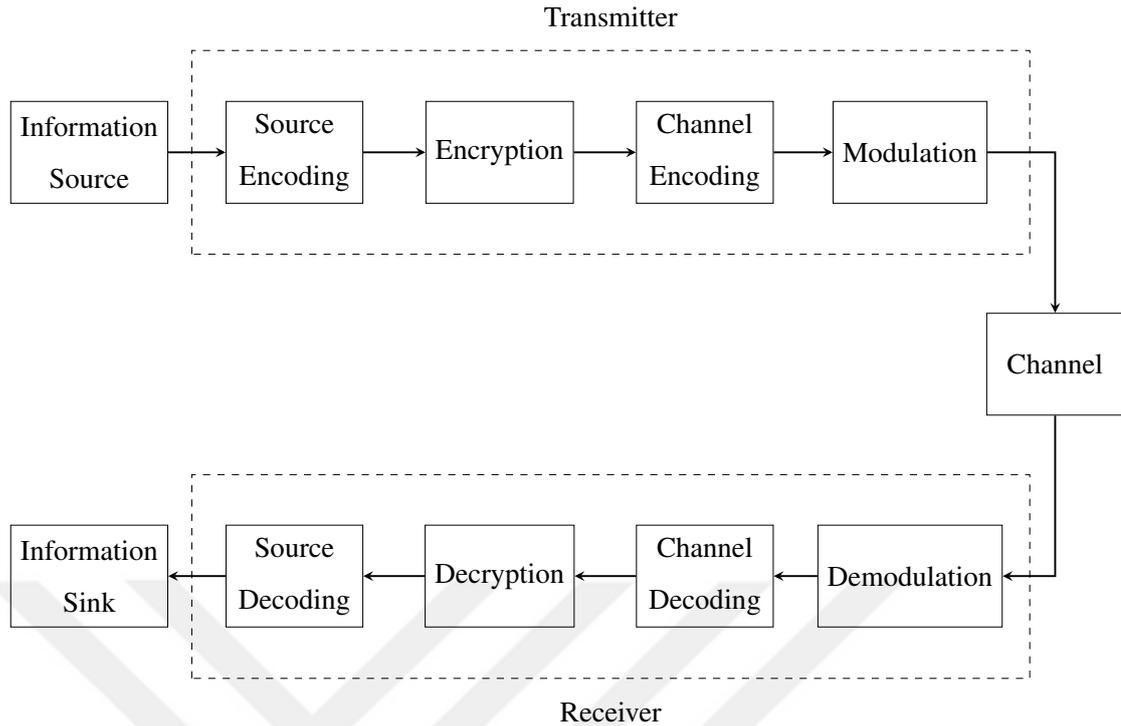
Figure 3.1 Block diagram of a typical communication system.

Considering aforementioned requirements, a typical communication system can be represented by a block diagram given in Figure 3.1. Note that each of the signal processing operation performed in the transmitter side has a corresponding reverse operation in the receiver side to obtain the message signal properly.

In addition to requirements such as efficiency, security and robustness, sharing of resources in a communication system is essential. To accomplish resource sharing, multiplexing techniques based on the use of orthogonal signals are employed (Figure 3.1 requires additional blocks for multiplexing if case the multiplexing is employed.). Orthogonality of the signals can be achieved by use of time-disjoint signals leading to time division multiple access techniques or by use of the frequency-disjoint signals leading to frequency division multiple access techniques. Orthogonality can also be achieved by the use of uncorrelated signals that are neither time-disjoint nor frequency-disjoint.

The chaotic signals have some inherent properties that are desired in different fields of communication systems. They have a widely spread power spectrum which

makes them a good match for spread-spectrum communication. The long-term unpredictability of the chaotic signals leads one to consider the use of chaotic signals in secure communication. Chaotic signals are uncorrelated signals and this makes them useful for a multiuser communication systems. All these ideas have led to the proposal of various chaotic communication schemes in the literature reviewed in the sequel.

3.1 Chaotic Communication Schemes

In most of the chaotic communication schemes, a message signal (possibly source encoded and encrypted) is mapped into a chaotic transmission signal suitable for the requirements of the physical channel. Hence, the proposed methods merge channel encoding and modulation in a single operation.

It is possible to classify communication schemes with respect to the approaches used to design their transmitter and receiver structures (Abel & Schwarz, 2002). The transmitter structures are classified according to their encoding/modulation methods. If the encoding/modulation is performed independent of the message, it is called static encoding/modulation. If the encoding/modulation is performed depending on the past values of the message, it is called dynamic encoding/modulation and this dependency can be obtained by either feeding a separate dynamical system with the message signal and the carrier signal or by feeding the carrier dynamical system with the message signal. The receiver structures are classified according to the way they extract the message. Using a reference signal, analysis of the statistics of the received signal and inverse system techniques are the methods used in the receiver structures. A reference signal synchronized to the carrier signal can be either generated locally in the receiver resulting in storage reference (SR) methods or can be transmitted from the transmitter resulting in transmitted reference (TR) methods. Analysis of the statistics (eg. average power) of the received signal is performed, if a statistical characteristics of the received signal reveals a correspondence to the transmitted symbols. In inverse system techniques, exact inverse of the operations performed in

the transmitter side is performed in the receiver side to extract the message.

3.1.1 Chaotic Masking

Figure 3.2 shows the block diagram of chaotic masking scheme. In this scheme the message signal $m(t)$ is added to a chaotic carrier $x(t)$ resulting in a transmission signal $y(t)$, i.e.

$$y(t) = x(t) + m(t) \tag{3.1}$$

In the receiver side a approximate copy of the chaotic carrier signal $\hat{x}(t)$ is generated by means of the drive-response synchronization of transmitter and receiver chaotic systems. The message signal is extracted by subtracting the generated chaotic signal $\hat{x}(t)$ from the received signal $\hat{y}(t) = y(t) + \eta(t)$, where $\eta(t)$ is the noise in the channel, followed by low pass filtering and thresholding. Note that chaotic masking is classified as static encoding/modulation and SR scheme with respect to its transmitter and receiver structures, respectively and use reference signals to extract the message.

In order not to obstruct the chaotic synchronization, the power of the message signal should be lower than that of the carrier signal. The message signal cannot be extracted exactly, since it disturbs the synchronization. Hence, the bit rate of chaotic masking scheme is not satisfactory for low signal-to-noise (SNR) ratios.

3.1.2 Chaos Shift Keying

In chaos shift keying scheme, one of the chaotic signals is transmitted corresponding to the message symbol $m(t)$, i.e. considering M-ary communication, the transmission signal $y(t)$ is given by,

$$y(t) = \begin{cases} x_1(t) & m(t) = m_0 \\ x_2(t) & m(t) = m_1 \\ \vdots & \vdots \\ x_{M-1}(t) & m(t) = m_{M-1} \end{cases} \tag{3.2}$$

Threshold

Low
Pass
Filter

$\hat{m}(t)$

$+$

$-$

$\hat{x}(t)$

Chaos
Generator
Subsystem1

Chaos
Generator
Subsystem2

Response System

$\hat{y}(t)$

$\eta(t)$

$+$

$m(t)$

$+$

$y(t)$

$x(t)$

Chaos
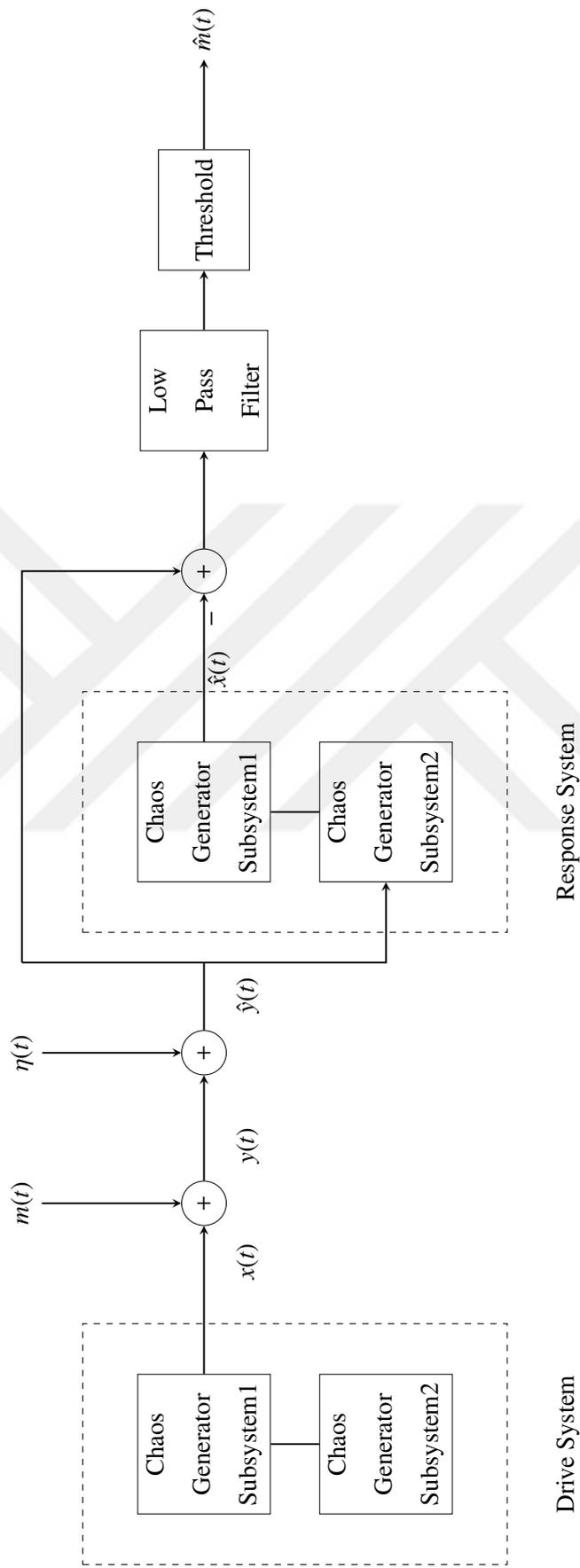Generator
Subsystem1

Chaos
Generator
Subsystem2

Drive System

Figure 3.2 Chaotic masking scheme.

Figure 3.3 shows the block diagram of the chaos shift keying scheme for the binary case, i.e. M = 2. During each symbol transmission, one of the chaotic systems in the receiver side synchronize with the corresponding chaotic system in the transmitter side and produce highly correlated outputs with the received signal $\hat{y}(t) = y(t) + \eta(t)$, where $\eta(t)$ is the noise in the channel, compared to those of the other unsynchronized chaotic systems in the receiver. The message signal is extracted by comparing low pass filtered correlator outputs followed by thresholding. Like chaotic masking scheme, chaos shift keying scheme is classified as static encoding/modulation and SR scheme with respect to its transmitter structure and receiver structure, respectively, and use reference signals to extract the message.

In chaos shift keying scheme, the symbol transmission time must be long enough to ensure chaotic synchronization causing the transmission rate of chaos shift keying scheme be lower than that of the chaotic masking scheme.

3.1.3 Differential Chaos Shift Keying

Differential chaos shift keying differs from chaos shift keying in that the reference signal is not generated but received. Therefore, differential chaos shift keying is TR scheme.

Figure 3.4 shows the block diagram of the binary differential chaos shift keying scheme. Reference carrier signal is transmitted during half of the symbol transmission time followed by the modulated carrier signal, i.e., the transmitted signal is given by,

$$y(t) = \begin{cases} x(t) & kT_b \leq t \leq (2k+1)\dfrac{T_b}{2} \\ x(t - \dfrac{T_b}{2}) & (2k+1)\dfrac{T_b}{2} \leq t \leq (k+1)T_b \quad m(t) = m_0 \quad k \in \mathbb{Z} \\ -x(t - \dfrac{T_b}{2}) & (2k+1)\dfrac{T_b}{2} \leq t \leq (k+1)T_b \quad m(t) = m_1 \end{cases} \quad (3.3)$$

In the receiver side, the message signal is extracted by correlating the received signal $\hat{y}(t) = y(t) + \eta(t)$, where $\eta(t)$ is the noise in the channel, with its delayed version followed by low pass filtering and thresholding. Differential chaos shift keying
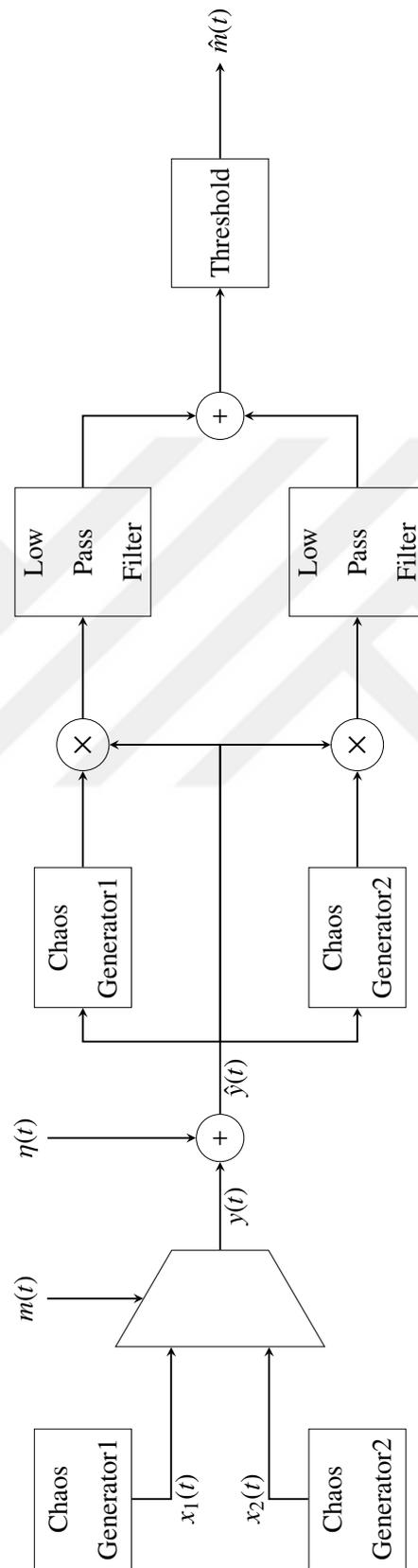
Figure 3.3 Chaos shift keying scheme.

scheme is classified as static encoding/modulation and TR scheme with respect to its transmitter structure and receiver structure, respectively, and use reference signals to extract the message. Since the reference signal is transmitted during half of the symbol transmission time, the bit rate of the differential chaos shift keying scheme is half of the chaos shift keying scheme with same resources, which is a common drawback of TR methods against SR methods.

3.1.4 Chaotic Modulation

In this scheme, the message signal $m(t)$ is fed to the dynamical system of the chaotic carrier and it modulates one or more system parameters of the carrier dynamical system whose dynamics is governed by,

$$\dot{\boldsymbol{x}}(t) = g(\boldsymbol{x}(t), m(t))$$
$$\boldsymbol{y}(t) = h(\boldsymbol{x}(t), m(t))$$

(3.4)

Figure 3.5 shows the block diagram of the chaotic modulation scheme. In the receiver side, the message is extracted by performing exact reverse of operations performed in the transmitter side. The chaotic modulation scheme is classified as dynamic encoding/modulation and SR scheme with respect to its transmitter and receiver structure, respectively, and use inverse system technique to extract the message.

Table 3.1 shows the comparison of the chaotic communication schemes explained in this chapter in terms of their transmitter and receiver structures.
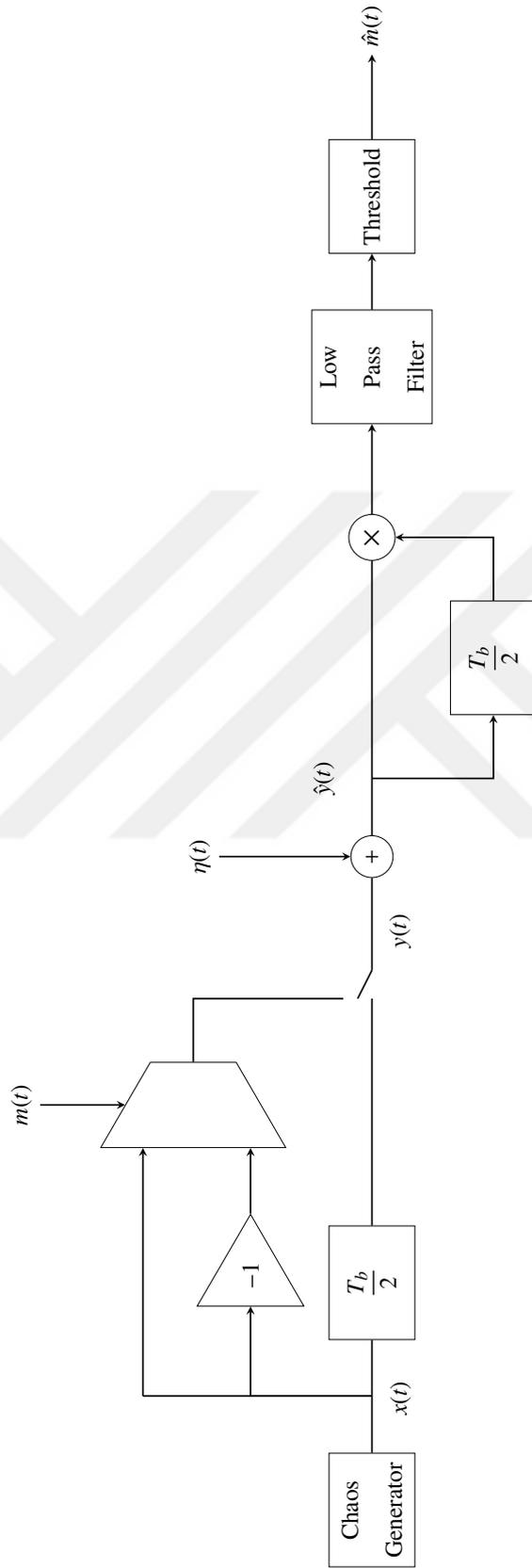
Figure 3.4 Differential chaos shift keying scheme.
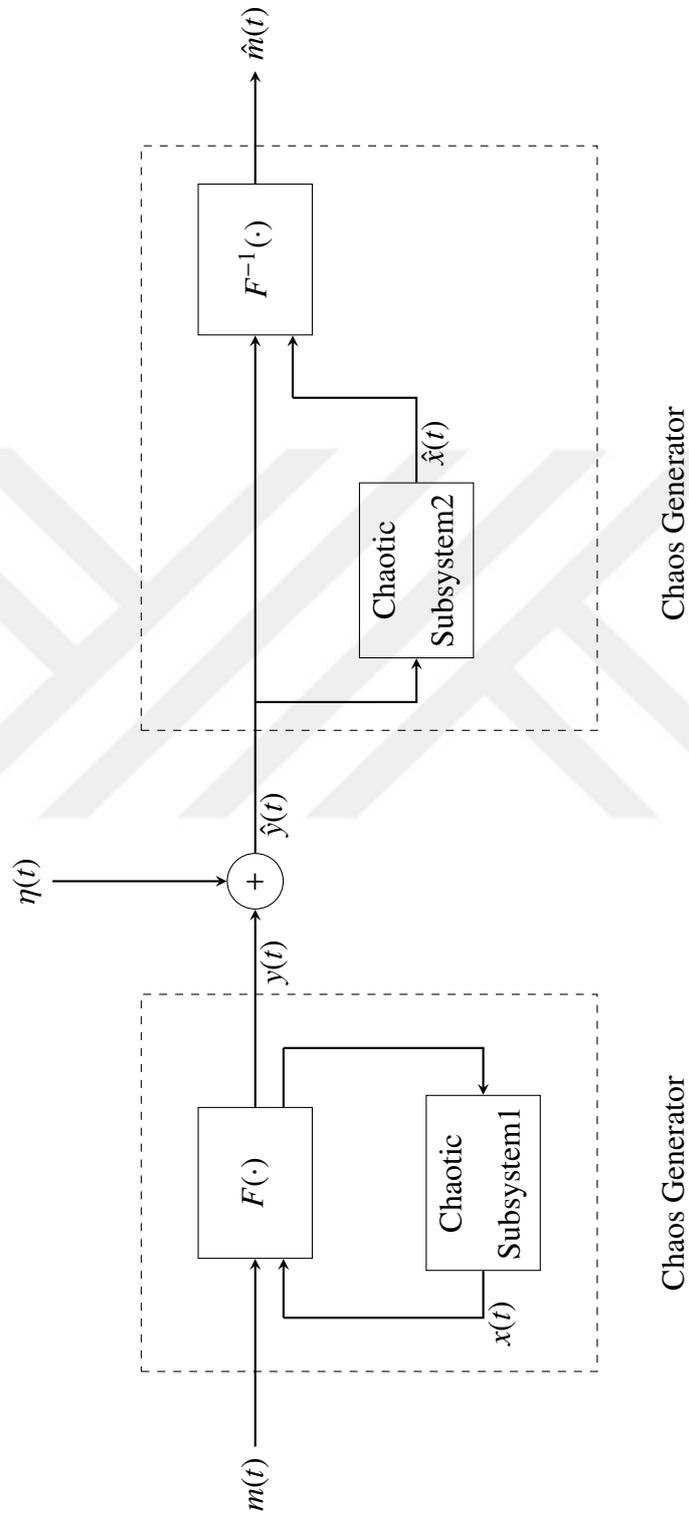
Figure 3.5 Chaotic modulation scheme.

Table 3.1 Comparison of the proposed system with the chaos communication schemes.

	Transmitter Structure		Receiver Structure	
	Static Encoding / Modulation	Dynamic Encoding / Modulation	SR Scheme	TR Scheme
Chaotic Masking	√		√	
Chaos Shift Keying	√		√	
Differential Chaos Shift Keying	√			√
Chaotic Modulation		√	√	
Proposed Scheme		√	√	

CHAPTER FOUR

SECURE COMMUNICATION VIA CLUSTER SYNCHRONIZATION OF NETWORKS OF CHAOTIC SYSTEMS

In an attempt to use cluster synchronization in networks of chaotic systems in which the information to be sent is encoded into symbols s_i, $i = 0,\ldots,M-1$, consider an arbitrary network of N identical chaotic oscillators shown in Figure 4.1. All the nodes are in their chaotic regime and the network evolves with the dynamics given in (2.10).
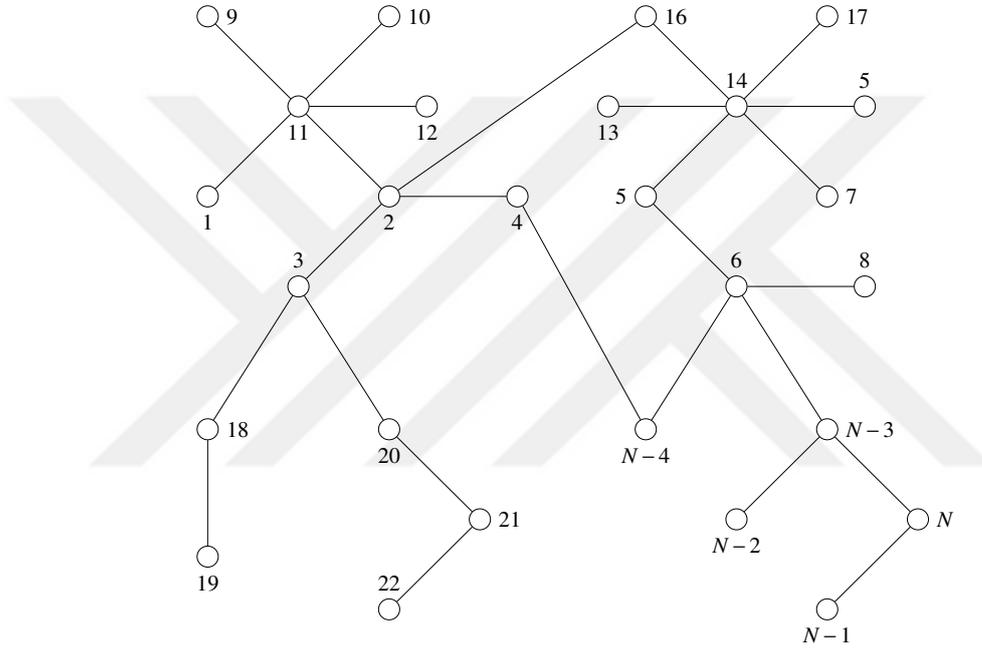

Figure 4.1 An arbitrary network of N identical chaotic oscillators.

Assume that the network can be partitioned into n clusters $G_1 = \{1,\ldots,m_1\},\ldots,G_n = \{\sum_{i=1}^{n-1} m_i + 1,\ldots,\sum_{i=1}^{n} m_i = N\}$ as shown in Figure 4.2, where $n \leq M$ and m_j is the number of nodes in the cluster G_j.

Associated with the clustering, (2.10) can be decomposed as,

$$\dot{X}_i(t) = F(X_i(t)) + \sum_{j=1}^{n} D_{ij}(t)X_j(t), \quad i = 1,\ldots,n \tag{4.1}$$

In the proposed system, the network in Figure 4.2 is divided into two to be used in the transmitter side and the receiver side of the communication system. This division
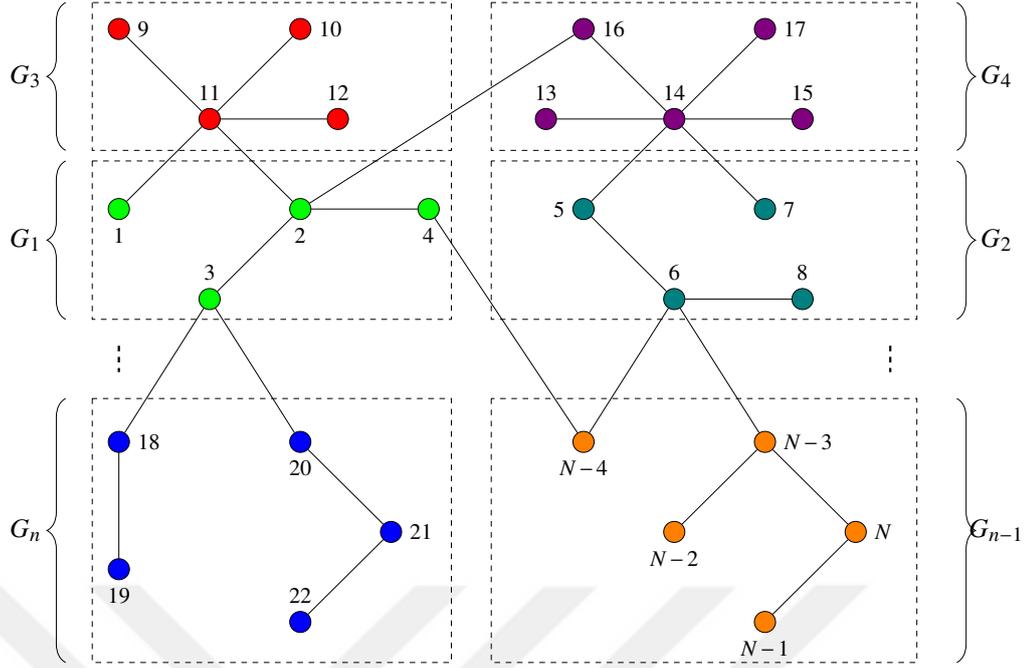
Figure 4.2 Realization of *n* clusters in the network in Figure 4.1. The oscillators are represented by the circles and the oscillators with the same color are in the same cluster.

is performed in such a way that the nodes connecting the transmitter side and the receiver side are not in the same cluster. Since change of cluster mode in the transmitter side also changes the dynamics in the receiver side, the symbols to be transmitted are represented by the absence and the presence of the cluster synchronization of the corresponding node groups. In this context, the modulation is performed by injecting the message signal $m(t)$ into the transmitter side of the network to adjust the coupling strengths in order to enforce the cluster mode corresponding to the symbol s_j, $j = 0, \ldots, M-1$ to be transmitted. Note, M different cluster modes, denoted by $\mathscr{C}_j$ $j = 0, \ldots, M-1$, are required to represent M symbols. Figure 4.3a shows cluster mode $\mathscr{C}_j$ when the symbol s_j is to be transmitted. Figure 4.3b shows the cluster mode $\mathscr{C}_k$ when the coupling strengths in the transmitter side are adjusted so that another symbol s_k is to be transmitted. Note, the spatiotemporal behavior of the whole network changes when different symbols are to be transmitted.

Identification of the cluster mode of the nodes in the receiver side is the essential step for detection of the received symbol. Identification of the cluster mode of the nodes in the receiver side requires first determination of the synchronization of

desynchronization of the each pair of nodes in the receiver side. In this context, since the error signal $e_{ij}^{(1)}(t) = x_j^{(1)}(t) - x_i^{(1)}(t)$ goes asymptotically to zero if i^{th} and j^{th} nodes are in the same cluster, the error signals $e_{ij}^{(1)}(t)$ are obtained for each pair of nodes in the receiver side. Then, zero-mean instantaneous powers (which may be thought as detrended instantaneous powers)

$$p_{ij}(t) = \left(e_{ij}^{(1)}(t)\right)^2 - \left(\overline{e_{ij}^{(1)}(t)}\right)^2 \tag{4.2}$$

are calculated. Then, envelope of the zero-mean instantaneous powers $\tilde{p}_{ij}(t)$ are obtained through low pass filtering and fed to a decompression amplifier. Synchronization and desynchronization of the nodes are determined by applying a threshold, i.e. if the decompressed envelopes are lower than a certain threshold, the ith and j^{th} nodes are synchronous, and they are not synchronous otherwise. Decompression amplifier is used to reduce the spikes at the output of the threshold. Thresholded output is sampled with a sampling period of a bit transmission time resulting in the cluster mode, say $\hat{\mathscr{C}}_j$ which is then fed to a cluster mode encoder to encode the received symbol $\hat{s}_j$.

All the nodes are in their chaotic regime, and the nodes connecting the transmitter side and the receiver side are not in the same cluster. By construction, the signals transmitted through the channel are always chaotic and cannot be resolved, directly when obtained by a third party without the knowledge of the transmitter and the receiver internal topologies.

Table 3.1 shows the comparison of the proposed scheme to the ones explained in the previous chapter in terms of its transmitter and receiver structure. In the proposed scheme can be classified as dynamic encoding/modulation with respect to its transmitter structure since the message signal is injected directly into the network in the transmitter side, and hence encoding/modulation depends on the past values of the message message signal. Since there is no reference signal transmission through the channel, but instead chaotic synchronization is used to extract the message, the proposed system can be classified as an SR scheme.
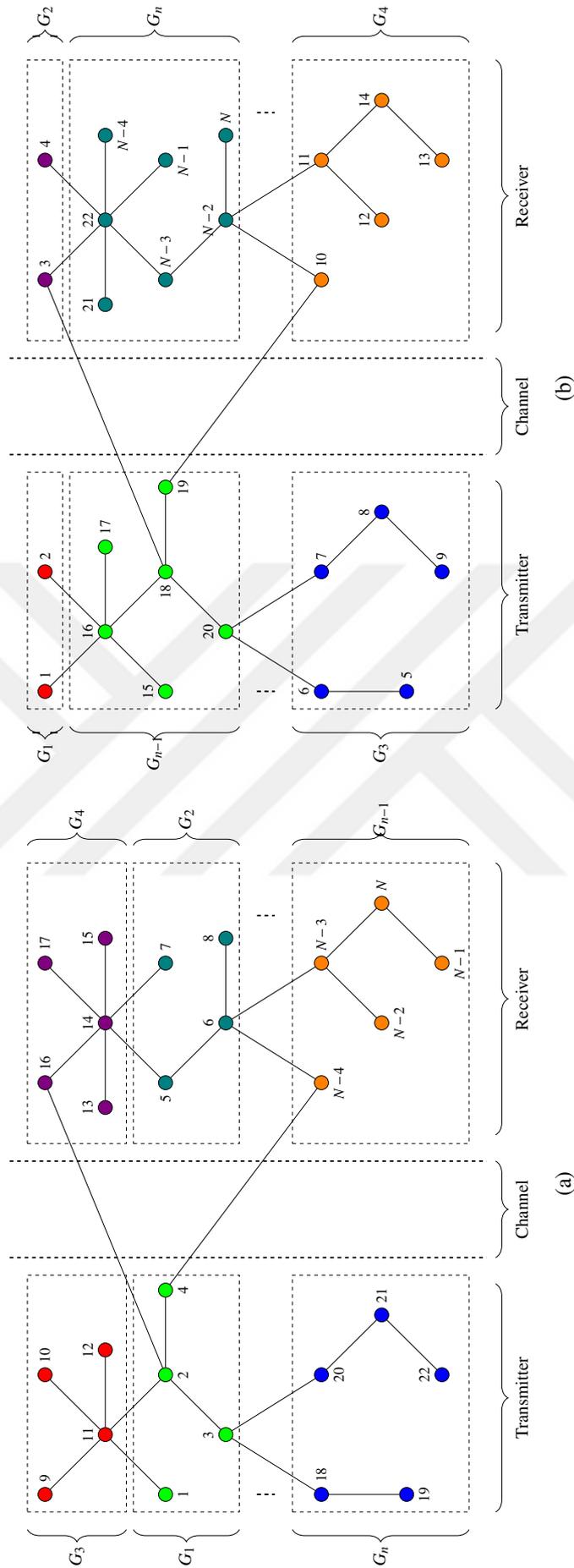
Figure 4.3 The network is divided into two as a transmitter and a receiver. (a) Cluster mode for the transmission of the symbol, say, s_k. (b) Cluster mode for the transmission of the symbol, say, s_j.
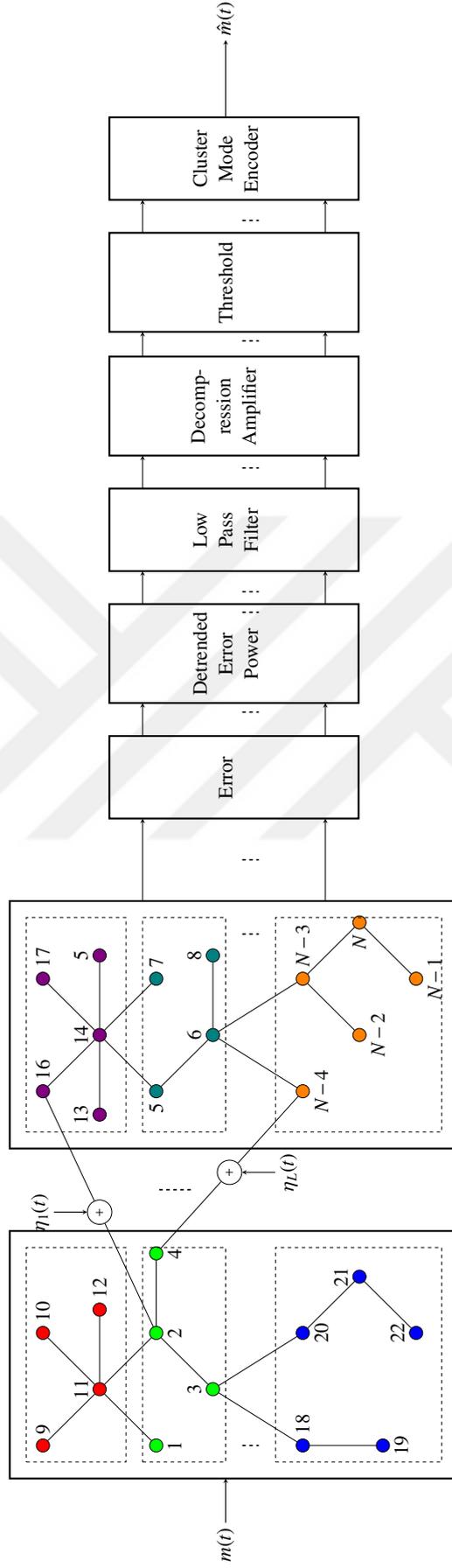
35

Figure 4.4 Block diagram of the proposed communication system. The colored circles represent the chaotic oscillators and the oscillators with the same color are in the same cluster. The network of N identical oscillators is divided into two to be used in the transmitter and the receiver side of the communication system. The transmitter side and the receiver side are coupled through L links. The message signal $m(t)$ is encoded in to the symbols m_j, $0, \ldots, M-1$. The symbols are represented by the cluster modes $\mathscr{C}_0, \ldots, \mathscr{C}_{M-1}$ of the corresponding node groups.

CHAPTER FIVE
SIMULATION RESULTS

This chapter is devoted to the numerical simulations carried out to investigate the proposed system in terms of performance and security requirements of a typical communication system.

As explained in the previous chapter, the symbols to be transmitted are signified by the presence or the absence of the cluster synchronization of different node groups. Therefore, the coupling strengths in the network are time-variant and the time it takes for the oscillators to synchronize and desynchronize are important parameters which determine the bit rate of the communication system.

The transmitted signals through the channel are not directly modulated by the message signal to be sent and when obtained by third party, it cannot be resolved without the knowledge of the transmitter and the receiver internal topologies. For this purpose, time-frequency properties of the signals transmitted through the channel have been investigated.

5.1   Time Variant Coupling

The type of coupling in the proposed system is the mutual coupling in which the coupled systems influence one another equally resulting in bidirectional interaction. For the case of electronic chaos oscillators, the mutual interaction of two chaotic oscillators can be achieved by coupling the oscillators with a resistor. In this context, consider the Lorenz-based chaotic circuit in Figure 5.1.
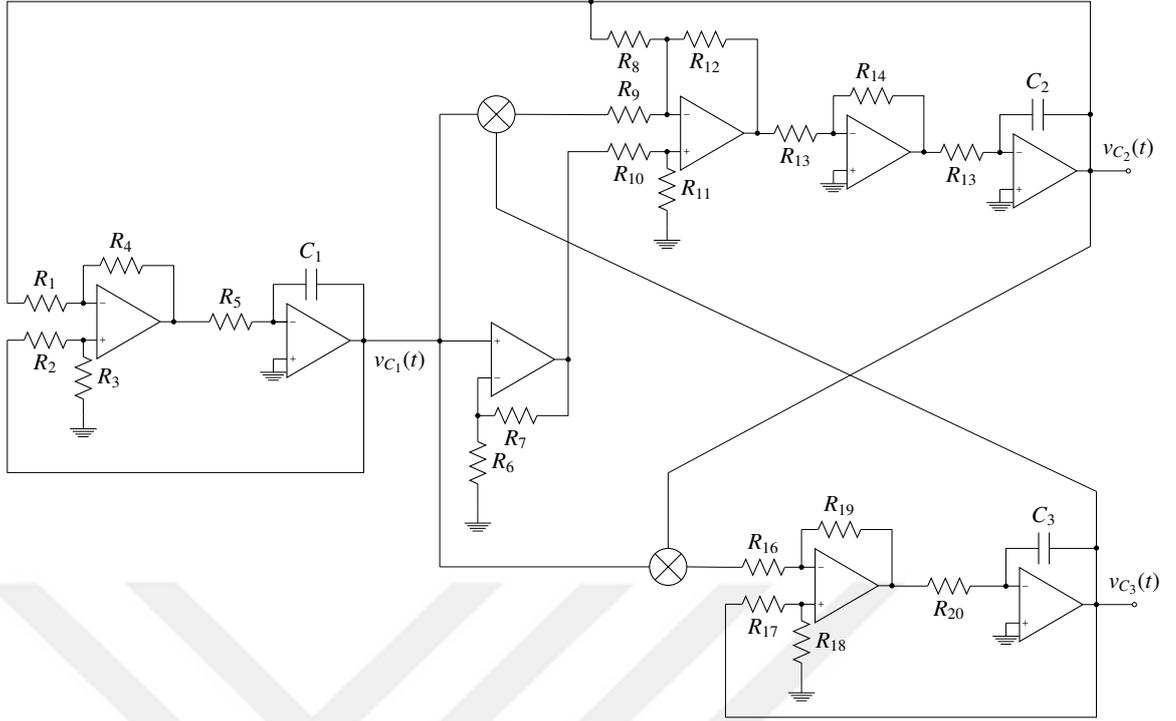
Figure 5.1 Lorenz-based chaotic circuit.

The dynamics of the circuit is governed by,

$$\dot{v}_{C_1}(t) = \frac{1}{R_1 C_1}\left[\frac{R_4}{R_1}v_{C_1}(t) - \frac{R_3}{R_2+R_3}\left(1+\frac{R_4}{R_1}\right)v_{C_1}(t)\right]$$

$$\dot{v}_{C_2}(t) = \frac{1}{R_{15}C_2}\left[\frac{R_{11}}{R_{10}+R_{11}}\left(1+\frac{R_{12}}{R_8}+\frac{R_{12}}{R_9}\right)\left(1+\frac{R_7}{R_6}\right)v_{C_1}(t) - \frac{R_{12}}{R_8}v_{C_2}(t) - \frac{R_{12}}{R_9}v_{C_1}(t)v_{C_3}(t)\right]$$

$$\dot{v}_{C_3}(t) = \frac{1}{R_{20}C_3}\left[\frac{R_{19}}{R_{16}}v_{C_1}(t)v_{C_2}(t) - \frac{R_{18}}{R_{17}+R_{18}}\left(1+\frac{R_{19}}{R_{16}}\right)v_{C_3}(t)\right]$$

$$(5.1)$$

Denoting $[v_{C_1}(t), v_{C_2}(t), v_{C_3}(t)]^T = \boldsymbol{x} = [x^{(1)}, x^{(2)}, x^{(3)}]^T$ the system (5.1) can be written as,

$$
\begin{aligned}
\dot{x}^{(1)} &= \sigma(x^{(1)} - x^{(2)}) \\
\dot{x}^{(2)} &= rx^{(1)} - x^{(2)} - x^{(1)}x^{(3)} \\
\dot{x}^{(3)} &= -bx^{(3)} + x^{(1)}x^{(2)}
\end{aligned}
\qquad (5.2)
$$

where σ, b, r are the system parameters depending on the resistors and capacitors in the circuit. The system is chaotic with parameter values $\sigma = 10.0$, $b = 8.0/3.0$, $r = 28.0$ (Lorenz, 1963).

38

Time variant coupling of the two identical systems in (5.2) can be achieved by connecting the systems through their $x^{(1)}$ states with a time variant resistor $R_c(t)$. Figure 5.2 shows the case.

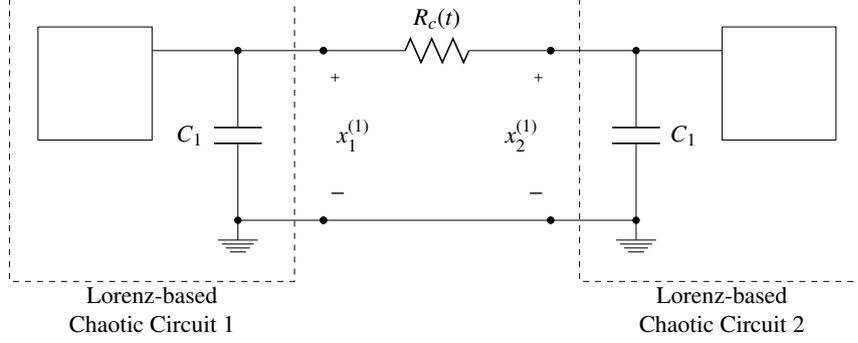
Figure 5.2 Time variant mutual coupling of two identical Lorenz-based circuits with a time variant resistor $R_c(t)$.

The dynamics of the coupled system is governed by,

$$
\begin{aligned}
\dot{x}_1^{(1)} &= \sigma(x_1^{(1)} - x_1^{(2)}) + \epsilon(t)(x_2^{(1)} - x_1^{(1)}) \\
\dot{x}_1^{(2)} &= rx_1^{(1)} - x_1^{(2)} + x_1^{(1)}x_1^{(3)} \\
\dot{x}_1^{(3)} &= -bx_1^{(3)} + x_1^{(1)}x_1^{(2)} \\
\dot{x}_2^{(1)} &= \sigma(x_2^{(1)} - x_2^{(2)}) + \epsilon(t)(x_1^{(1)} - x_2^{(1)}) \\
\dot{x}_2^{(2)} &= rx_2^{(1)} - x_2^{(2)} - x_2^{(1)}x_2^{(3)} \\
\dot{x}_2^{(3)} &= -bx_2^{(3)} + x_2^{(1)}x_2^{(2)}
\end{aligned}
\tag{5.3}
$$

where $\boldsymbol{x}_1 = [x_1^{(1)}, x_1^{(2)}, x_1^{(2)}]^T$, $\boldsymbol{x}_2 = [x_2^{(1)}, x_2^{(2)}, x_2^{(2)}]^T$ are the state vector of the first and second system, respectively, and $\epsilon(t) = \dfrac{1}{R_c(t)C_1}$. Denoting $\boldsymbol{X} = [\boldsymbol{x}_1, \boldsymbol{x}_2]$ the coupled system dynamics in (5.3) can be written more compactly as,

$$
\dot{\boldsymbol{X}} = F(\boldsymbol{X}) + \Big(\boldsymbol{E}(t) \otimes \boldsymbol{P}\Big)\boldsymbol{X}
\tag{5.4}
$$

where,

$$
\boldsymbol{E}(t) = \begin{bmatrix} -\epsilon(t) & \epsilon(t) \\ \epsilon(t) & -\epsilon(t) \end{bmatrix} \qquad \boldsymbol{P} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}
\tag{5.5}
$$

Let ϵ_0 and ϵ_1 denote the low level and high level of coupling strength for which the oscillators are able to and not able to synchronize, respectively. Consider a binary

message signal $m(t)$ represented by the symbols $s_0 = 0$, $s_1 = 1$ modulates the coupling strength as,

$$u(t) = \epsilon_0 + m(t)(\epsilon_1 - \epsilon_0) \tag{5.6}$$

Then, the dynamics of the coupled system is given by (5.4) with,

$$E(t) = \begin{bmatrix} -\epsilon(t) & \epsilon(t) \\ \epsilon(t) & -\epsilon(t) \end{bmatrix} = U(t) \circ C = \begin{bmatrix} u(t) & u(t) \\ u(t) & u(t) \end{bmatrix} \circ \begin{bmatrix} -1 & 1 \\ 1 & -1 \end{bmatrix} \tag{5.7}$$

Since (5.4) is a nonlinear ordinary differential equation system in the form of,

$$\dot{X} = \tilde{F}(X, t) \tag{5.8}$$

where $X \in \mathbb{R}^d$, $\tilde{F} : \mathbb{R}^d \times \mathbb{R} \mapsto \mathbb{R}^d$, it can be numerically integrated by a fourth order Runga-Kutta method over time interval $[0, T]$ with a step size of T_s by applying the iteration,

$$\begin{aligned} X_{n+1}^{(k)} &= X_n^{(k)} + \frac{T_s}{6}\left(k_1 + 2k_2 + 2k_3 + k_4\right) \\ t_{n+1} &= t_n + T_s \end{aligned}, \quad k = 1, \ldots, d, \quad n = 0, \ldots, M \tag{5.9}$$

where $M = T/T_s$ and

$$\begin{aligned} k_1 &= \tilde{F}(t_n, \ X_n) \\ k_2 &= \tilde{F}(t_n + \frac{T_s}{2}, \ X_n + \frac{T_s}{2}k_1) \\ k_3 &= \tilde{F}(t_n + \frac{T_s}{2}, \ X_n + \frac{T_s}{2}k_2) \\ k_2 &= \tilde{F}(t_n + T_s, \ X_n + T_s k_3) \end{aligned}$$

Figures 5.3 - 5.6 show the results when the system in (5.4) has been numerically integrated using fourth order Runga Kutta method with a step size $T_s = 0.01$ seconds for $T = 100$ seconds, $\epsilon_0 = 0.01$ and $\epsilon_1 = 10.0$ for different symbol transmission times. The results show that once the oscillators synchronize within a few seconds with a coupling strength being equal to ϵ_1, they do not desynchronize for a long time when the coupling strength is reduced to ϵ_0. This is misleading in the sense that the ambient noise is always present which drives the oscillators out of synchronization very fast. Hence, for a more realistic simulation the ambient noise should be considered.
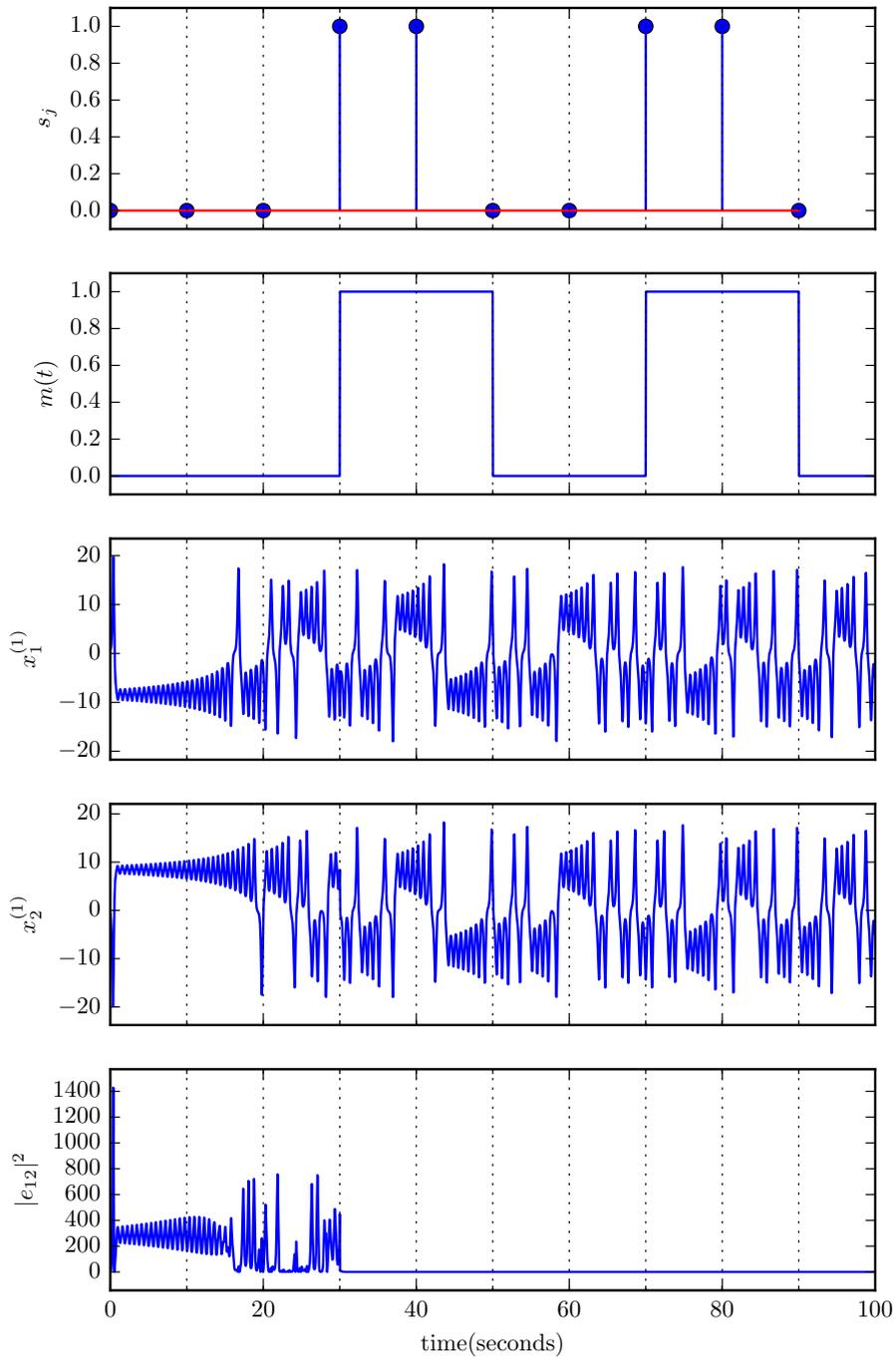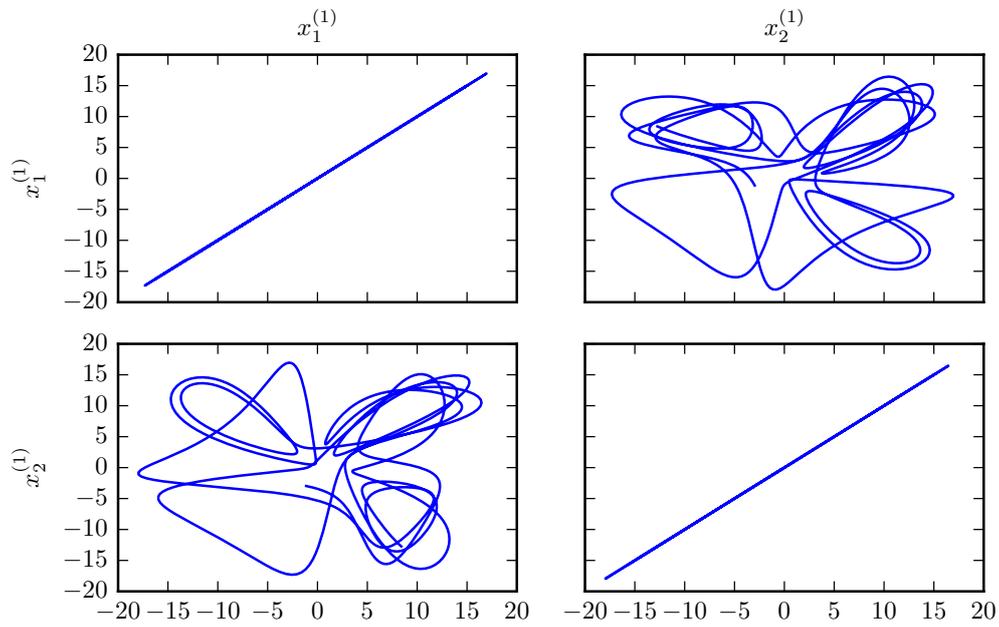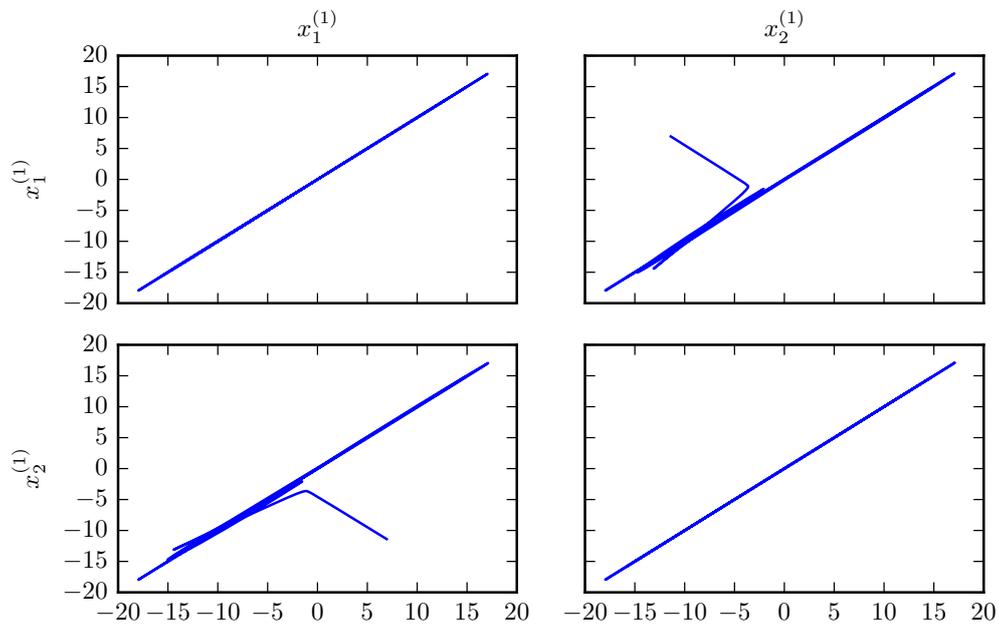
Figure 5.3 Numerical integration results of (5.4) with fourth order Runga Kutta method for a time step $T_s = 0.01$ seconds and symbol transmission time $T_b = 10$ seconds. The plots share the time axis. Note that once the oscillators synchronize after $t = 30$ seconds with coupling strength $u(t) = \epsilon_1$, they do not desynchronize even if the coupling strength is lowered to $u(t) = \epsilon_0$.

Figure 5.4 Numerical integration results of (5.4) with fourth order Runga Kutta method for a step size $T_s = 0.01$ seconds and symbol transmission time $T_b = 10$ seconds. (a) for $20 \le t \le 30$, (b) for $30 \le t \le 40$. Note that once the oscillators synchronize after $t = 30$ seconds with coupling strength $u(t) = \epsilon_1$, they do not desynchronize even if the coupling strength is lowered to $u(t) = \epsilon_0$.
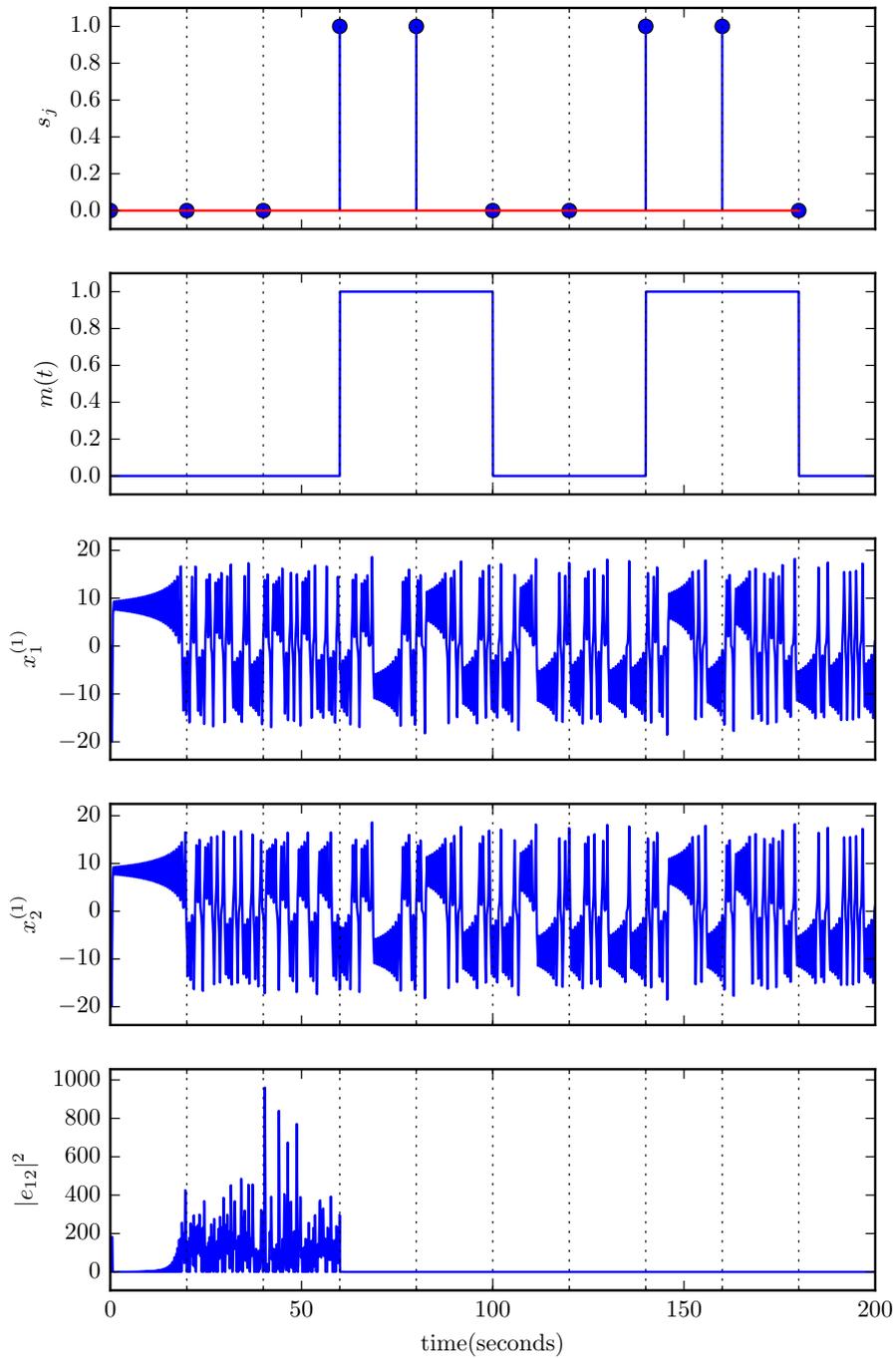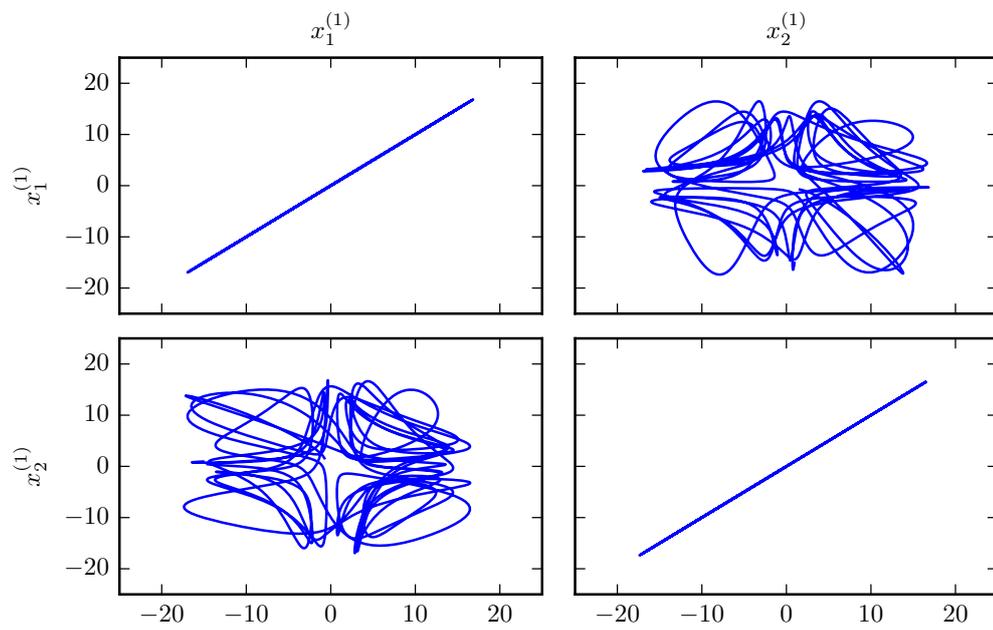
Figure 5.5 Numerical integration results of (5.4) with fourth order Runga Kutta method for a time step $T_s = 0.01$ seconds and symbol transmission time $T_b = 20$ seconds. The plots share the time axis. Note that once the oscillators synchronize after $t = 60$ seconds with coupling strength $u(t) = \epsilon_1$, they do not desynchronize even if the coupling strength is lowered to $u(t) = \epsilon_0$.
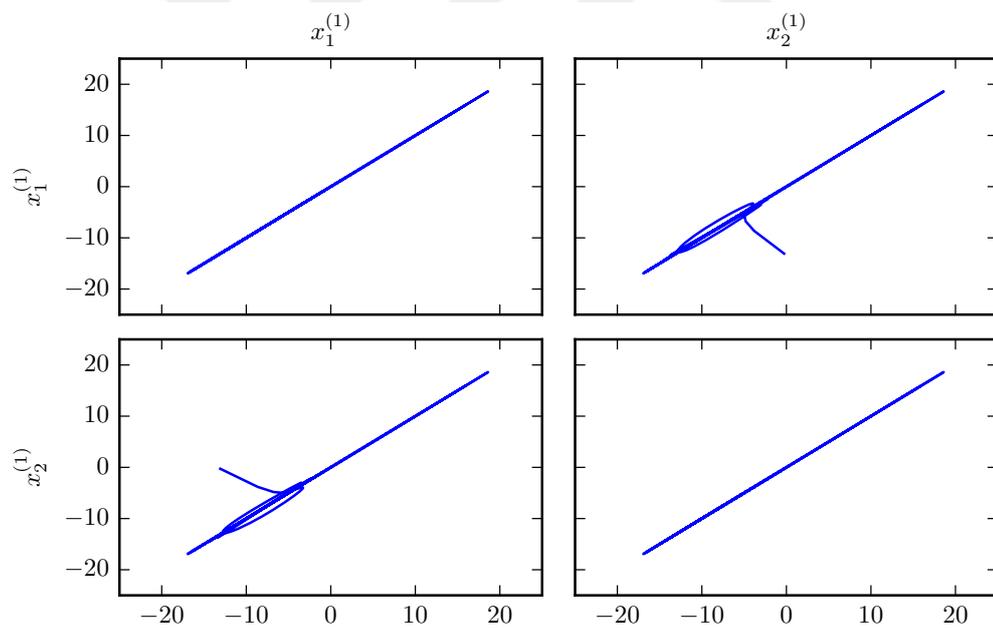
Figure 5.6 Numerical integration results of (5.4) with fourth order Runga Kutta method for a step size $T_s = 0.01$ seconds and symbol transmission time $T_b = 20$ seconds. (a) for $40 \leq t \leq 60$, (b) for $60 \leq t \leq 80$. Note that once the oscillators synchronize after $t = 60$ seconds with coupling strength $u(t) = \epsilon_1$, they do not desynchronize even if the coupling strength is lowered to $u(t) = \epsilon_0$.

5.2 Modeling of Noise

Considering the case of chaotic electronic circuits, the natural way of thinking the ambient noise is to model it with an independent voltage source $v_{noise} = \xi\hat{\eta}(t)$ as shown in Figure 5.7, where $\hat{\eta}(t)$ is the white Gaussian noise and $\xi \geq 0$ controls the amplitude of the voltage source $\hat{\eta}(t)$.
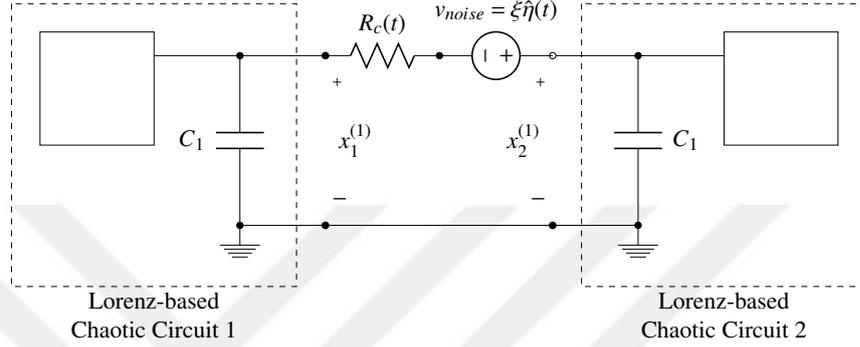

Figure 5.7 Time variant mutual coupling of two identical Lorenz-based circuits with a time variant resistor in the presence of noise modeled by the independent voltage source $v_{noise} = \xi\hat{\eta}(t)$.

Then, the coupled system is governed by,

$$
\begin{aligned}
\dot{x}_1^{(1)} &= \sigma(x_1^{(1)} - x_1^{(2)}) + \epsilon(t)(x_2^{(1)} - x_1^{(1)}) + \xi\eta(t) \\
\dot{x}_1^{(2)} &= rx_1^{(1)} - x_1^{(2)} - x_1^{(1)}x_1^{(3)} \\
\dot{x}_1^{(3)} &= -bx_1^{(3)} + x_1^{(1)}x_1^{(2)} \\
\dot{x}_2^{(1)} &= \sigma(x_2^{(1)} - x_2^{(2)}) + \epsilon(t)(x_1^{(1)} - x_2^{(1)}) - \xi\eta(t) \\
\dot{x}_2^{(2)} &= rx_2^{(1)} - x_2^{(2)} - x_2^{(1)}x_2^{(3)} \\
\dot{x}_2^{(3)} &= -bx_2^{(3)} + x_2^{(1)}x_2^{(2)}
\end{aligned}
\tag{5.10}
$$

where $\epsilon(t) = \dfrac{1}{R_c(t)C_1}$ and $\eta(t) = \dfrac{\hat{\eta}(t)}{R_c(t)C_1}$. The presence of the stochastic process $\eta(t)$ on the right hand side leads to a stochastic model of the system instead of the deterministic

one. The stochastic model of the system corresponding to (5.10) is given by,

$$dx_1^{(1)} = \left(\sigma(x_1^{(1)} - x_1^{(2)}) + \epsilon(t)(x_2^{(1)} - x_1^{(1)})\right)dt + \xi dW$$
$$dx_1^{(2)} = \left(rx_1^{(1)} - x_1^{(2)} - x_1^{(1)}x_1^{(3)}\right)dt$$
$$dx_1^{(3)} = \left(-bx_1^{(3)} + x_1^{(1)}x_1^{(2)}\right)dt$$
$$dx_2^{(1)} = \left(\sigma(x_2^{(1)} - x_2^{(2)}) + \epsilon(t)(x_1^{(1)} - x_2^{(1)})\right)dt - \xi dW \quad (5.11)$$
$$dx_2^{(2)} = \left(rx_2^{(1)} - x_2^{(2)} - x_2^{(1)}x_2^{(3)}\right)dt$$
$$dx_2^{(3)} = \left(-bx_2^{(3)} + x_2^{(1)}x_2^{(2)}\right)dt$$

where W is the standard Wiener process characterized by the following properties.

1. $W(0) = 0$

2. For each t, the random variable $W(t)$ is normally distributed with mean 0 and variance t.

3. For each $t_1 \leq t_2$, the random variable $W(t_2) - W(t_1)$ is an independent random variable of all the random variables $W(t)$, $0 \leq t \leq t_1$.

4. $W(t)$ is continuous in t, which implies $W(t)$ has continuous sample paths. Figure 5.8 shows some of the sample paths of the Wiener process.
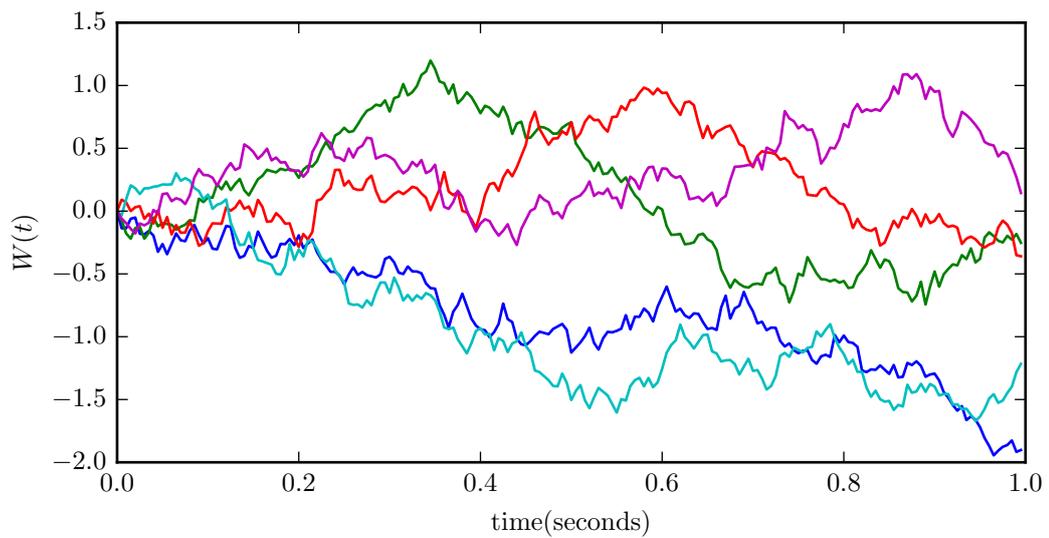

Figure 5.8 Typical sample paths of the Wiener process.

46

The system in (5.11) can be written more compactly as,

$$dX = \Big(F(X) + (E(t) \otimes P)X\Big)dt + GdW \tag{5.12}$$

where $x_1 = [x_1^{(1)}, x_1^{(2)}, x_1^{(3)}]$, $x_2 = [x_2^{(1)}, x_2^{(2)}, x_2^{(3)}]$, $X = [x_1, x_2]$, $G = [H \vdots -H]^T$, $H = [\xi, 0, 0]^T$. The system in (5.12) is a nonlinear stochastic differential equation system in the form of,

$$dX = \tilde{F}(X, t)dt + \tilde{G}(X, t)dW \tag{5.13}$$

where $X \in \mathbb{R}^d$, $\tilde{F} : \mathbb{R}^d \times \mathbb{R} \mapsto \mathbb{R}^d$, $\tilde{G} : \mathbb{R}^{d \times m} \times \mathbb{R} \mapsto \mathbb{R}^d$, $W \in \mathbb{R}^m$, which can be numerically integrated by Euler-Maruyama method over a time interval of $[0, T]$ with a step size T_s by applying the iteration,

$$X_{n+1}^{(k)} = X_n^{(k)} + \tilde{F}^{(k)}(X_n^{(k)}, nT_s)T_s + \sum_{j=1}^{m} \tilde{G}^{(k,j)}\Big(W^{(j)}((n+1)T_s) - W^{(j)}(nT_s)\Big),$$

$$k = 0, \ldots, d, \quad n = 0, \ldots, M \tag{5.14}$$

where $M = T/T_s$.

To simulate the system in (5.12) for different SNR (signal-to-noise ratio) values, the value of the parameter ξ controlling the noise strength needs to be determined according to the SNR value. SNR is defined as the ratio of the signal power $\mathcal{S}$ to the noise power $\mathcal{N}$. It is generally given in dB, i.e.,

$$SNR = 10\log_{10}\frac{\mathcal{S}}{\mathcal{N}}dB \tag{5.15}$$

where $\mathcal{S}$ and $\mathcal{N}$ are in the units of watts, hence SNR given in (5.15) is dimensionless. Throughout the simulations in the sequel, the signal power is calculated as the average power of the pure chaotic signal transmitted through the channel, say, $x_i^{(1)}$,

$$\mathcal{S} = \frac{1}{T}\int_0^T \Big(x_i^{(1)}(t)\Big)^2 dt \tag{5.16}$$

where T is the total simulation time. $\mathcal{N}$ is determined according to (5.15). Since the power $\mathcal{N}$ of a white Gaussian process $N(\hat{\mu}, \hat{\sigma})$ is its variance $\hat{\sigma}^2$, the parameter ξ in (5.12) is calculated by,

$$\xi = \sqrt{\frac{\mathcal{S}}{10^{\frac{SNR}{10}}}} \tag{5.17}$$

Figures 5.9 - 5.16 show the results when the system in (5.12) has been numerically integrated using Euler-Maruyama method with a step size $T_s = 0.01$ seconds, $\epsilon_0 = 0.01$ and $\epsilon_1 = 10.0$ for different SNR and symbol transmission times. From the results, its clear that there is no complete synchronization when the noise is present since it disturbs the synchronization and the amount of distortion is proportional to the noise power. It is also apparent that when the coupling strength between the oscillators is decreased to its low level ϵ_0, the oscillators desynchronize within seconds since the noise drives the oscillators out of synchronization.
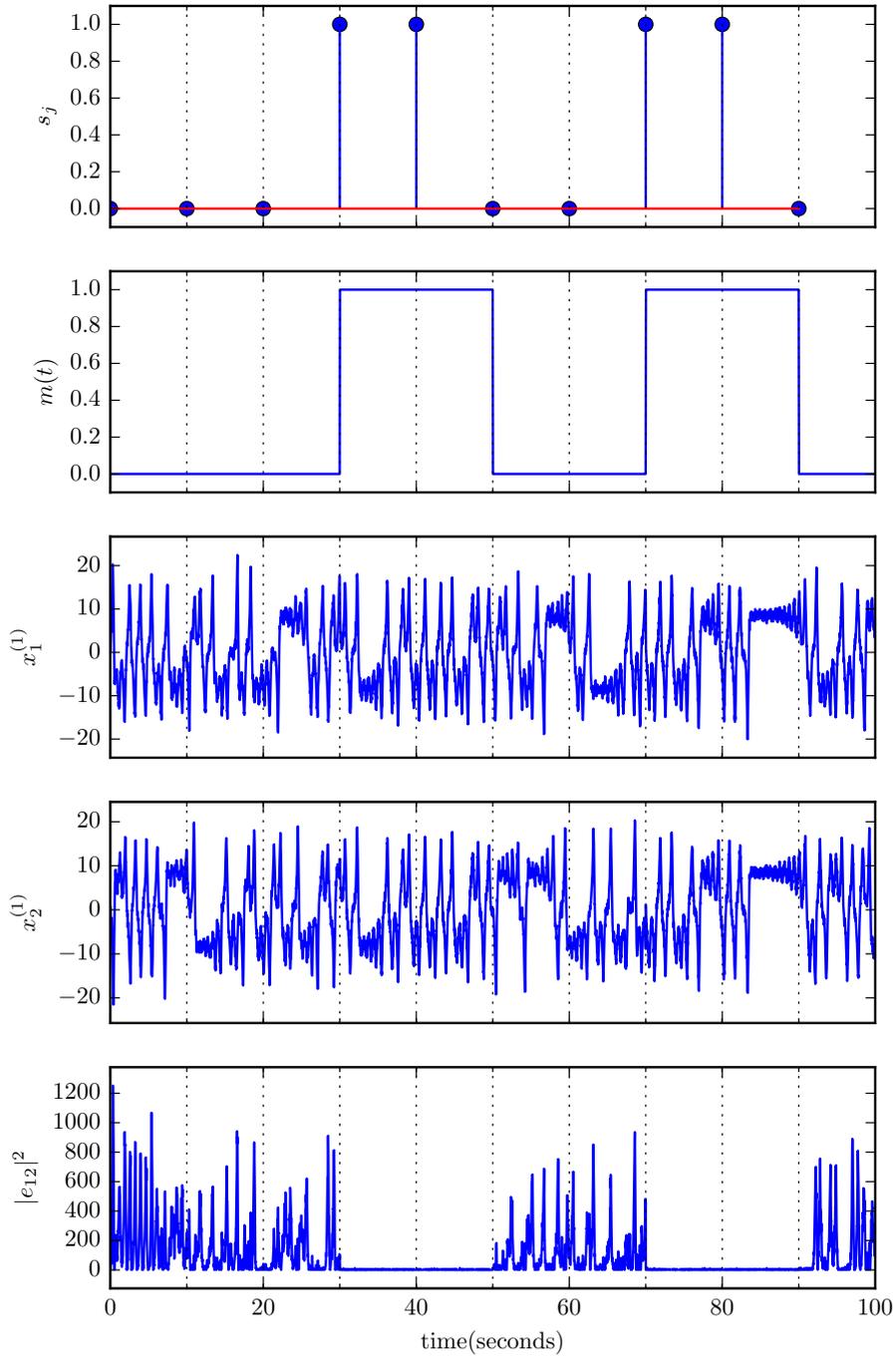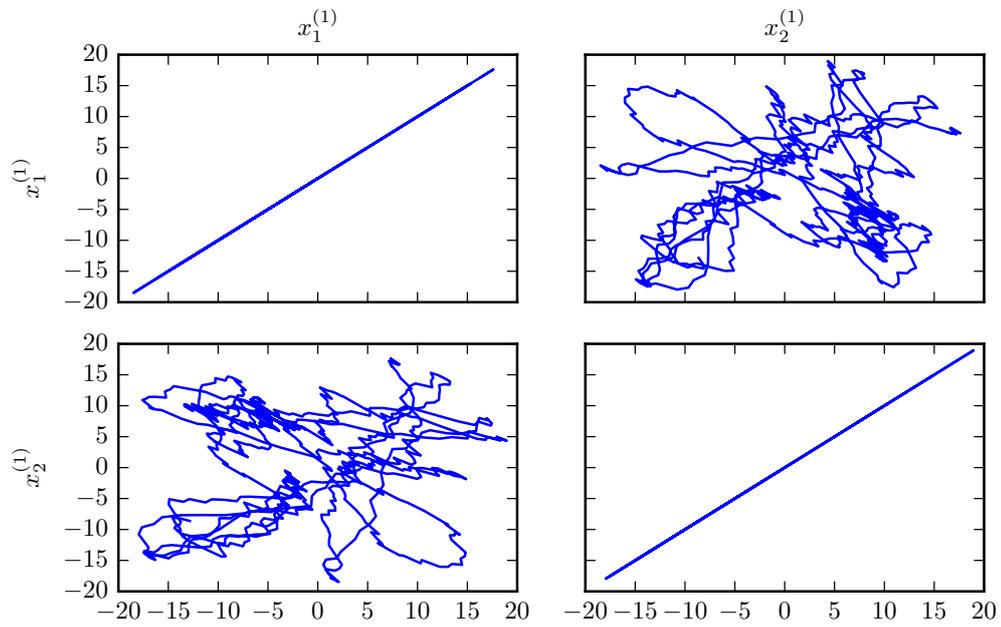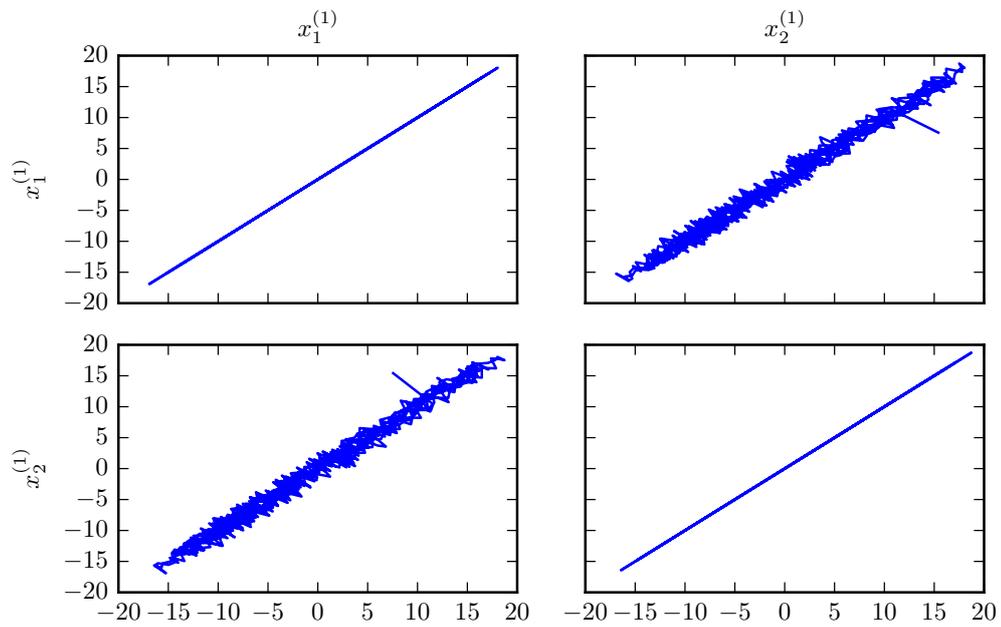
Figure 5.9 Numerical integration results of (5.12) with Euler-Maruyama method for a step size $T_s = 0.01$ seconds, symbol transmission time $T_b = 10$ seconds and SNR = 10 dB. The plots share the time axis. Note that the ambient noise drives the oscillators out of synchronization when the coupling strength is lowered to ϵ_0.

Figure 5.10 Numerical integration results of (5.12) with Euler-Maruyama method for a step size $T_s = 0.01$ seconds, symbol transmission time $T_b = 10$ seconds and SNR=10 dB. (a) for $20 \leq t \leq 30$, (b) for $30 \leq t \leq 40$. Note that the ambient noise drives the oscillators out of synchronization when the coupling strength is lowered to ϵ_0. Note also that the noise disturbs the chaotic synchronization.
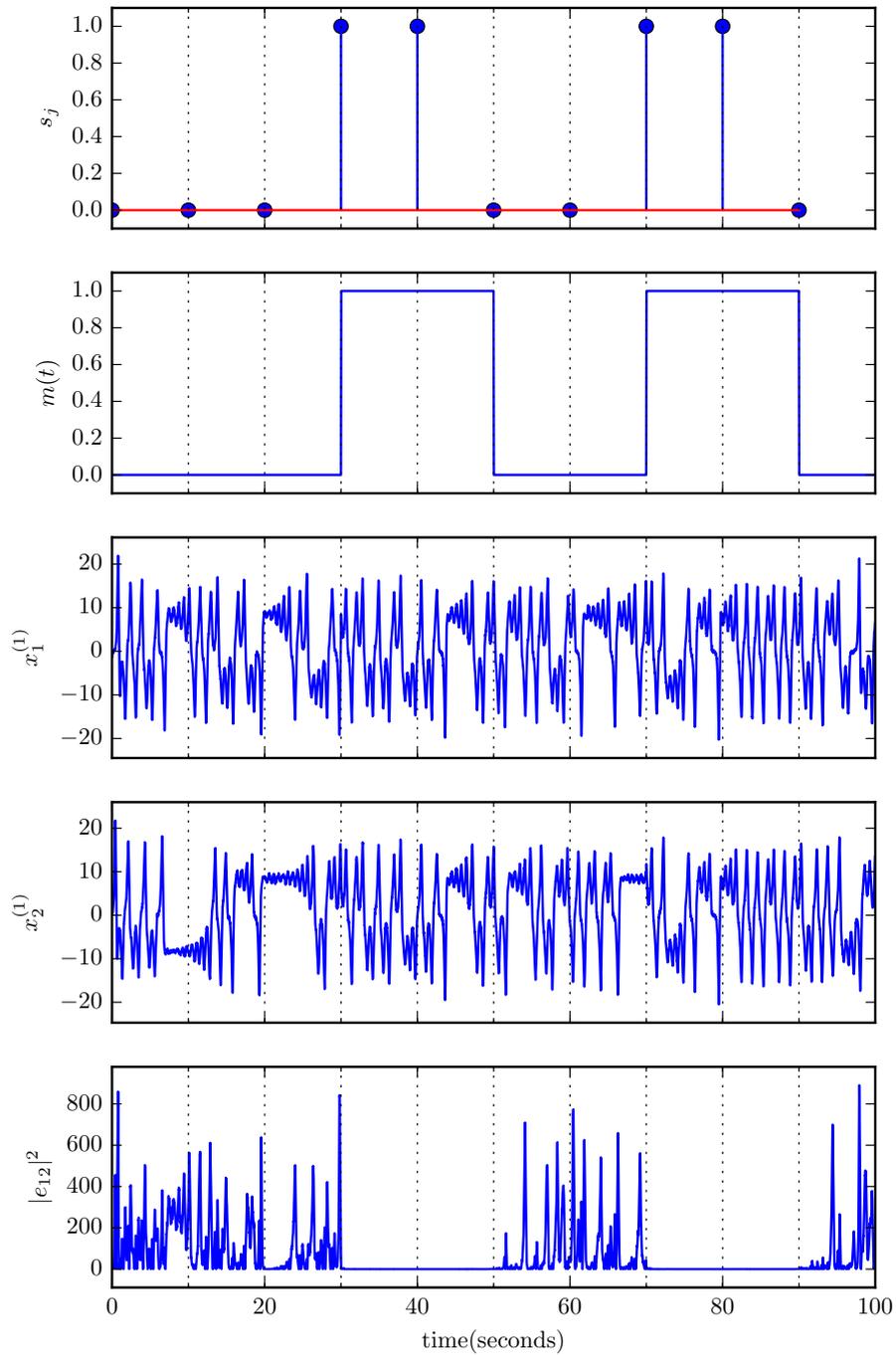
Figure 5.11 Numerical integration results of (5.12) with Euler-Maruyama method for a step size $T_s = 0.01$ seconds, symbol transmission time $T_b = 10$ seconds and SNR=20 dB. The plots share the time axis. Note that the ambient noise drives the oscillators out of synchronization when the coupling strength is lowered to ϵ_0.

Figure 5.12 Numerical integration results of (5.12) with Euler-Maruyama method for a step size $T_s =$ 0.01 seconds, symbol transmission time $T_b = 10$ seconds and SNR=20 dB. (a) for $20 \leq t \leq 30$, (b) for $30 \leq t \leq 40$. Note that the ambient noise drives the oscillators out of synchronization when the coupling strength is lowered to ϵ_0. Note also that the noise disturbs the chaotic synchronization.
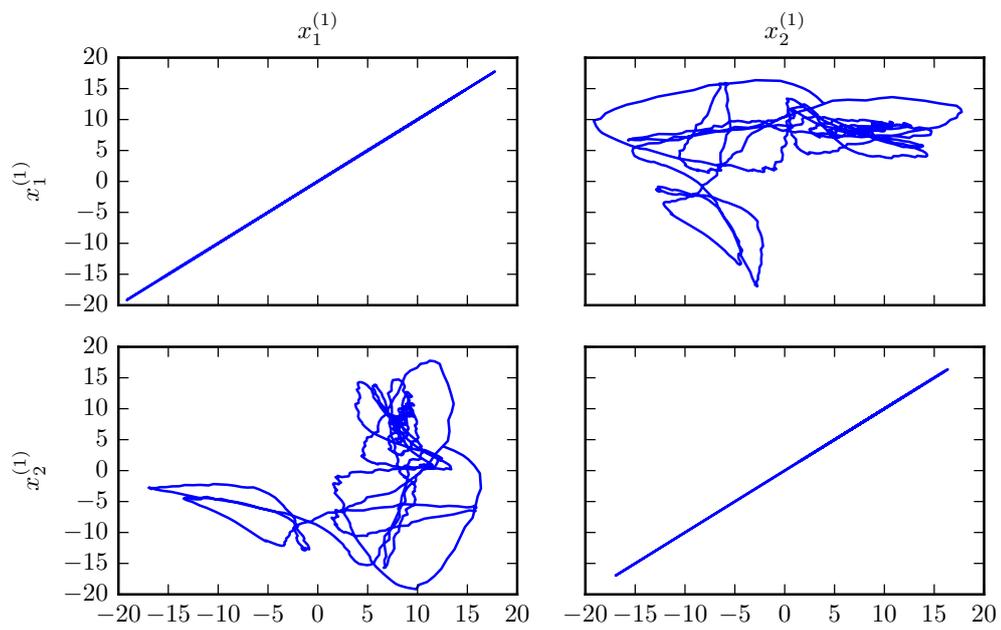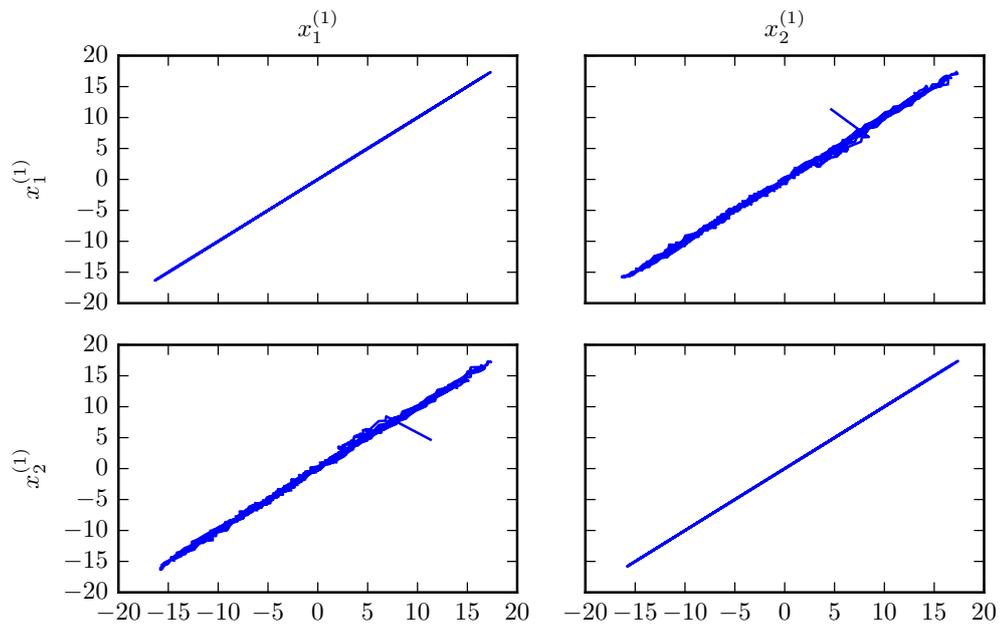
Figure 5.13 Numerical integration results of (5.12) with Euler-Maruyama method for a step size $T_s =$ 0.01 seconds, symbol transmission time $T_b = 20$ seconds and SNR=10 dB. The plots share the time axis. Note that the ambient noise drives the oscillators out of synchronization when the coupling strength is lowered to ϵ_0.

(a)

(b)

Figure 5.14 Numerical integration results of (5.12) with Euler-Maruyama method for a step size $T_s =$ 0.01 seconds, symbol transmission time $T_b = 20$ seconds and SNR=10 dB. (a) for $40 \leq t \leq 60$, (b) for $60 \leq t \leq 80$. Note that the ambient noise drives the oscillators out of synchronization when the coupling strength is lowered to ϵ_0. Note also that the noise disturbs the chaotic synchronization.
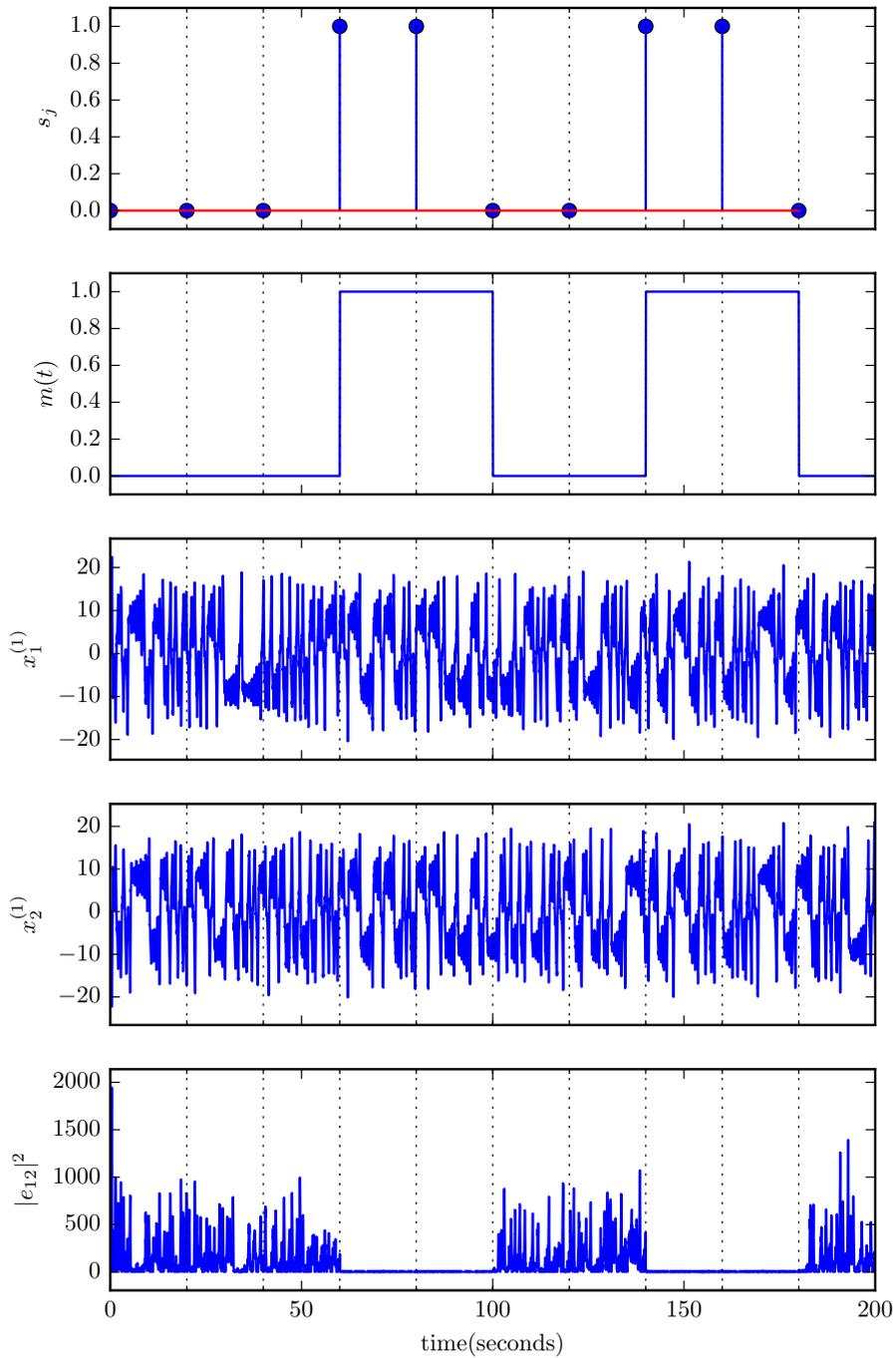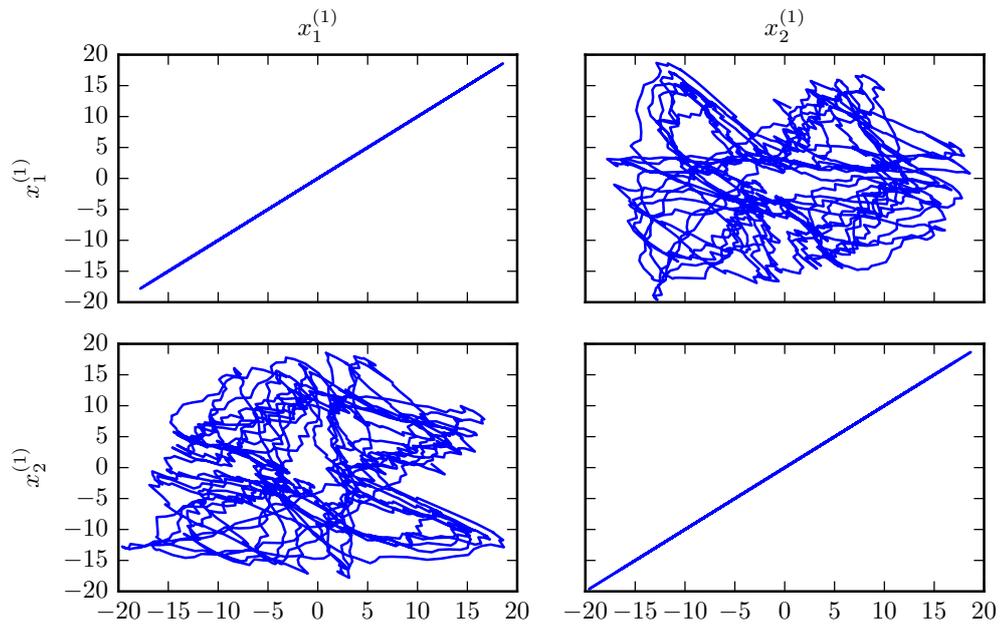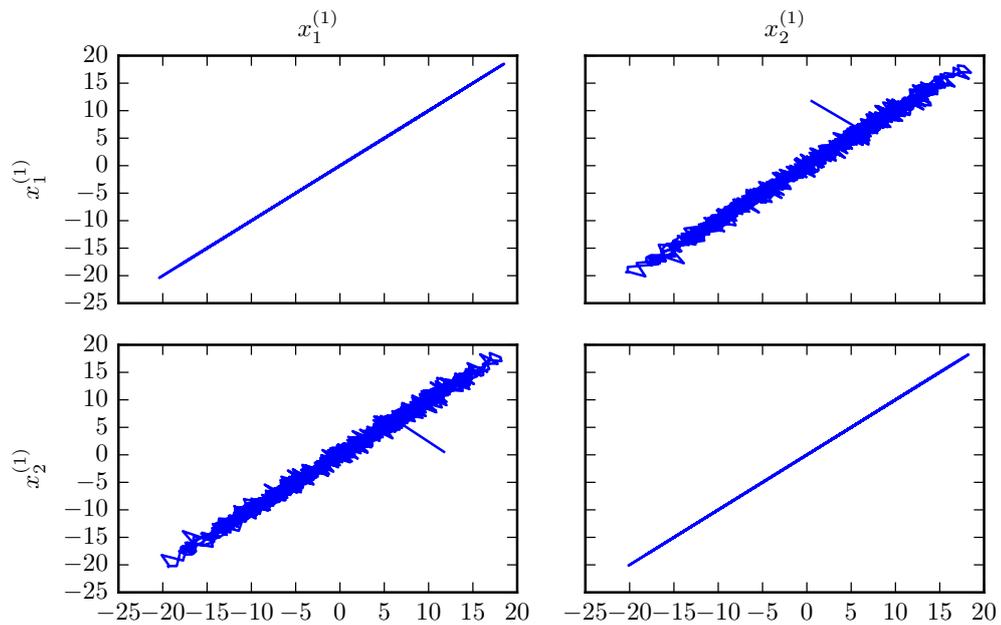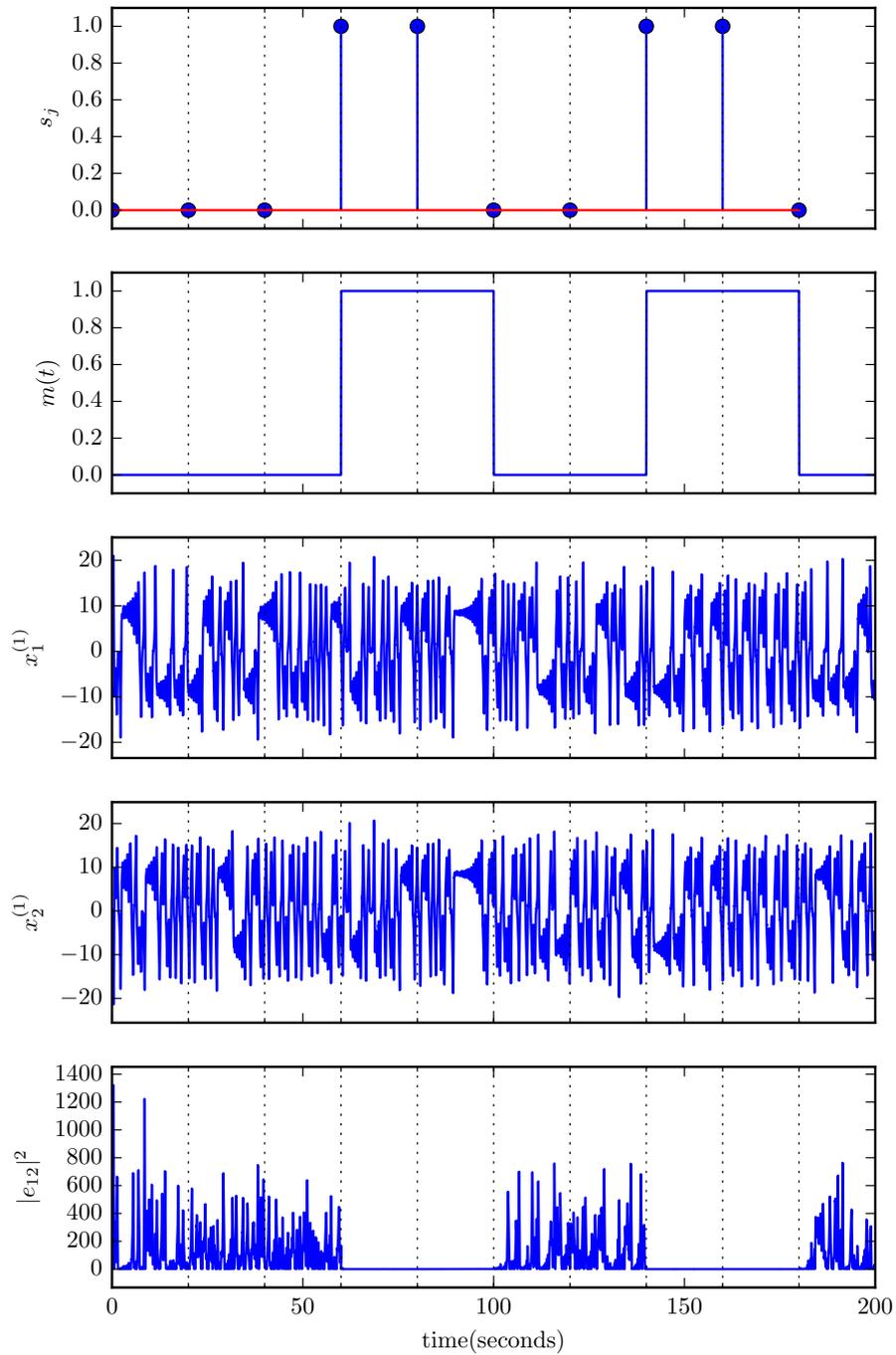
Figure 5.15 Numerical integration results of (5.12) with Euler-Maruama method for a step size $T_s = 0.01$ seconds, symbol transmission time of $T_b = 20$ seconds and SNR=20 dB. The plots share the time axis. Note that the ambient noise drives the oscillators out of synchronization when the coupling strength is lowered to ϵ_0.

Figure 5.16 Numerical integration results of (5.12) with Euler-Maruyama method for a step size $T_s = 0.01$ seconds, symbol transmission time of $T_b = 20$ seconds and SNR=20 dB. (a) for $40 \le t \le 60$, (b) for $60 \le t \le 80$. Note that the ambient noise drives the oscillators out of synchronization when the coupling strength is lowered to ϵ_0. Note also that the noise disturbs the chaotic synchronization.
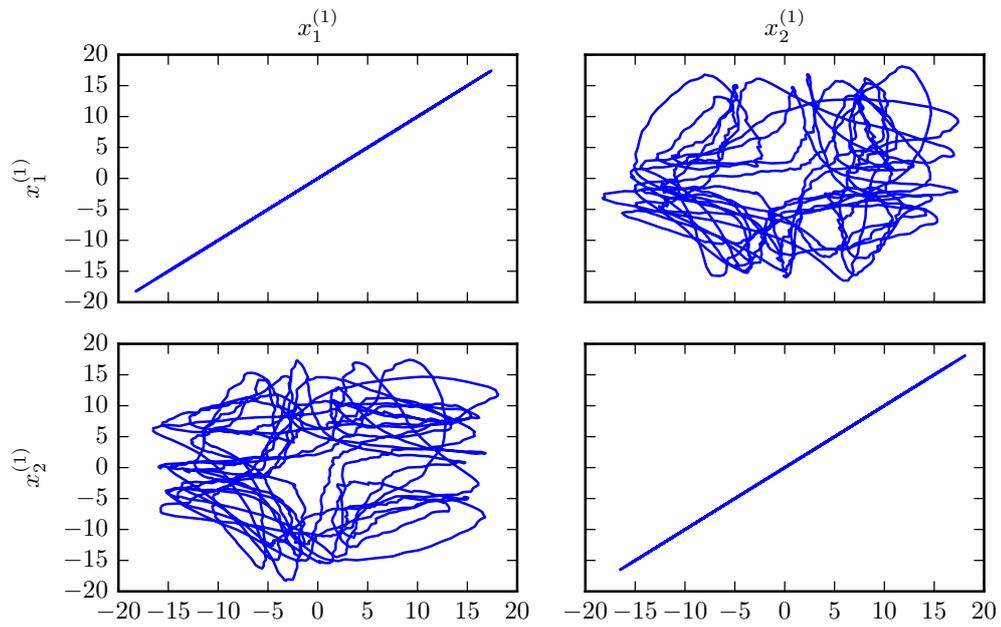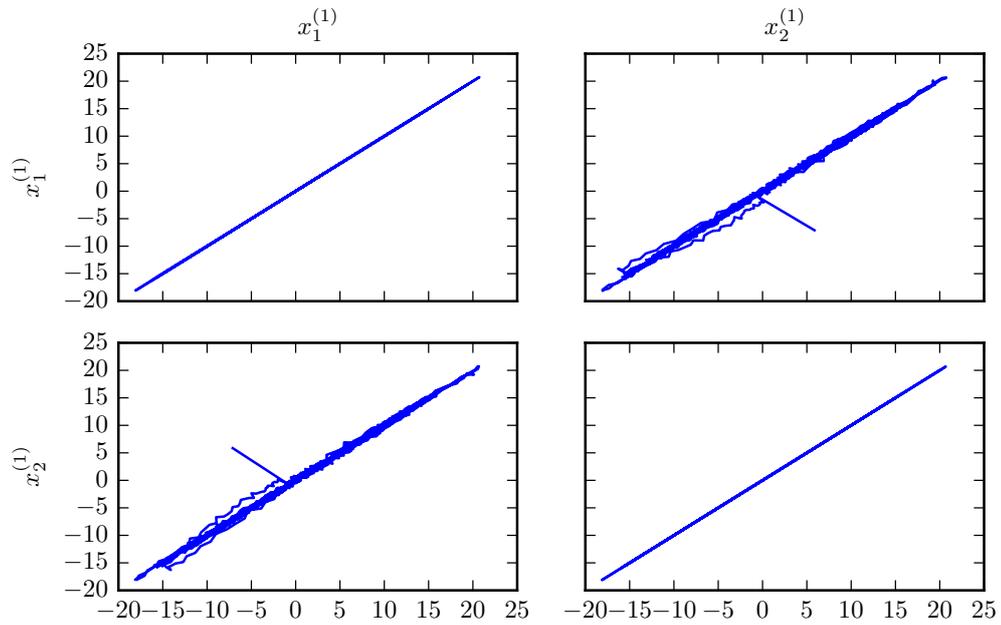
5.3 Illustrative Example

To illustrate the basic concept, consider the network of identical Lorenz oscillators given in Figure 5.17 with the network dynamics in (2.10). The Lorenz system defined by (5.2) is chaotic for the parameter values $\sigma = 10.0$, $b = 8.0/3.0$, $r = 28.0$ (Lorenz, 1963). All the oscillators in the network are coupled to each other through their $\boldsymbol{x}^{(1)}$ states, i.e. $\boldsymbol{P} = diag(1, 0, 0)$.
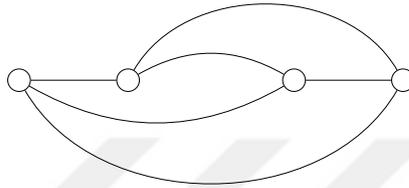

Figure 5.17 A network of identical Lorenz oscillators.

Consider that the network is to be used in a binary communication system in which the information to be sent is encoded into the symbols $s_0 = 0, s_1 = 1$. Assume that the symbol s_0 and s_1 are signified by the cluster mode $\mathscr{C}_0$ and $\mathscr{C}_1$, given in Figure 5.18a and Figure 5.18b, respectively.

Transmitter	Channel	Receiver

(a)

Transmitter	Channel	Receiver

(b)
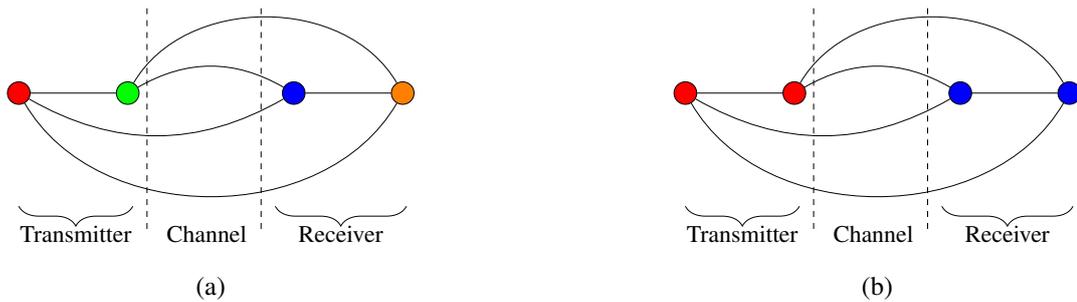
Figure 5.18 (a) Cluster mode $\mathscr{C}_0$ for symbol s_0. (b) Cluster mode $\mathscr{C}_1$ for symbol s_1. Note that when the symbol s_0 is to be transmitted all the oscillators are out of synchrony while when the symbol s_1 is to be transmitted $G_1 = \{1,2\}, G_2 = \{3,4\}$ clusters are formed.

Note that for s_1 transmission, the clusters $G_1 = \{1,2\}$ and $G_2 = \{3,4\}$ are formed while for s_0 transmission all the oscillators are out of synchrony. The message signal $m(t)$ modulates the coupling strength $u(t)$ between the node 1 and the node 2 according to (5.6). Considering Lemma 2.2.1 together with this modulation, the time varying

coupling matrix of the system takes the form,

$$E(t) = U(t) \circ C = \begin{bmatrix} u(t) & u(t) & \epsilon_1 & \epsilon_1 \\ u(t) & u(t) & \epsilon_1 & \epsilon_1 \\ \epsilon_1 & \epsilon_1 & \epsilon_1 & \epsilon_1 \\ \epsilon_1 & \epsilon_1 & \epsilon_1 & \epsilon_1 \end{bmatrix} \circ \begin{bmatrix} -3 & 3 & -1 & 1 \\ 3 & -3 & 1 & -1 \\ -1 & 1 & -3 & 3 \\ 1 & -1 & -3 & 3 \end{bmatrix} \qquad (5.18)$$

Note that during s_1 transmission $u(t) = \epsilon_1$ and Theorem 2.2.2 must be satisfied for the predefined clusters. During s_0 transmission, $u(t) = \epsilon_0$ and must be a nonzero value such that the oscillators in the network are not synchronous.

Assuming that the transmitted signals through the channel are disturbed by independent additive white Gaussian noise requires the stochastic model for the system. Since there exist $L = 4$ links through the channel and the noise on each link is assumed to be independent additive white Gaussian noise, the stochastic model corresponding to the system is given by,

$$dX = \Big(F(X) + (E(t) \otimes P) X \Big) dt + G dW \qquad (5.19)$$

where $W \in \mathbb{R}^4$ with independent column vectors and

$$G = \begin{bmatrix} H & H & 0 & 0 \\ 0 & 0 & H & H \\ -H & 0 & -H & 0 \\ 0 & -H & 0 & -H \end{bmatrix} \qquad (5.20)$$

where $H = [\xi, 0, 0]^T$.

Figures 5.19 - 5.27 show the results when the system in (5.19) has been numerically integrated with Euler-Maruyama method for $\epsilon_0 = 0.01$ and $\epsilon_1 = 10$ for different SNR and symbol transmission times. The receiver side of the system has been designed with a sixth order Butterworth low pass filter with a cut off frequency of 0.1 Hz as the low pass filter and an exponential amplifier as the decompression amplifier. Threshold value has been chosen to 0.2.

The results shows the existence of $G_1 = \{1, 2\}$, $G_2 = \{3, 4\}$ clusters, representing the

Figure 5.19 Signal flow obbtained by numerical integration of (5.19) with Euler-Maruyama method for a step size $T_s = 0.01$ seconds, symbol transmission time $T_b = 10$ seconds and SNR=10 dB. The plots share the time axis. The transmitted symbol s_j are successfully detected as $\hat{s}_j$. The decompression amplifier output is plotted on a logarithmic scale and the bottom plot shows $s_j \oplus \hat{s}_j$, where $\oplus$ is the logical exlusive-or operation.

(a)

(b)

Figure 5.20 Numerical integration results of (5.19) with Euler Maruyama method for a step size $T_s = 0.01$ seconds, symbol transmission time of $T_b = 10$ seconds and SNR=10 dB. (a) for $1020 \leq t \leq 1030$, (b) for $1030 \leq t \leq 1040$.

Figure 5.21 Numerical integration results of (5.19) with Euler-Maruyama method for a step size $T_s = 0.01$ seconds, symbol transmission time $T_b = 10$ seconds and SNR=10 dB. The plots share the time axis. Note that there is no apparent correlation between time frequency properties of the channel signal $e_{23}^{(1)}(t)$ and message signal $m(t)$.
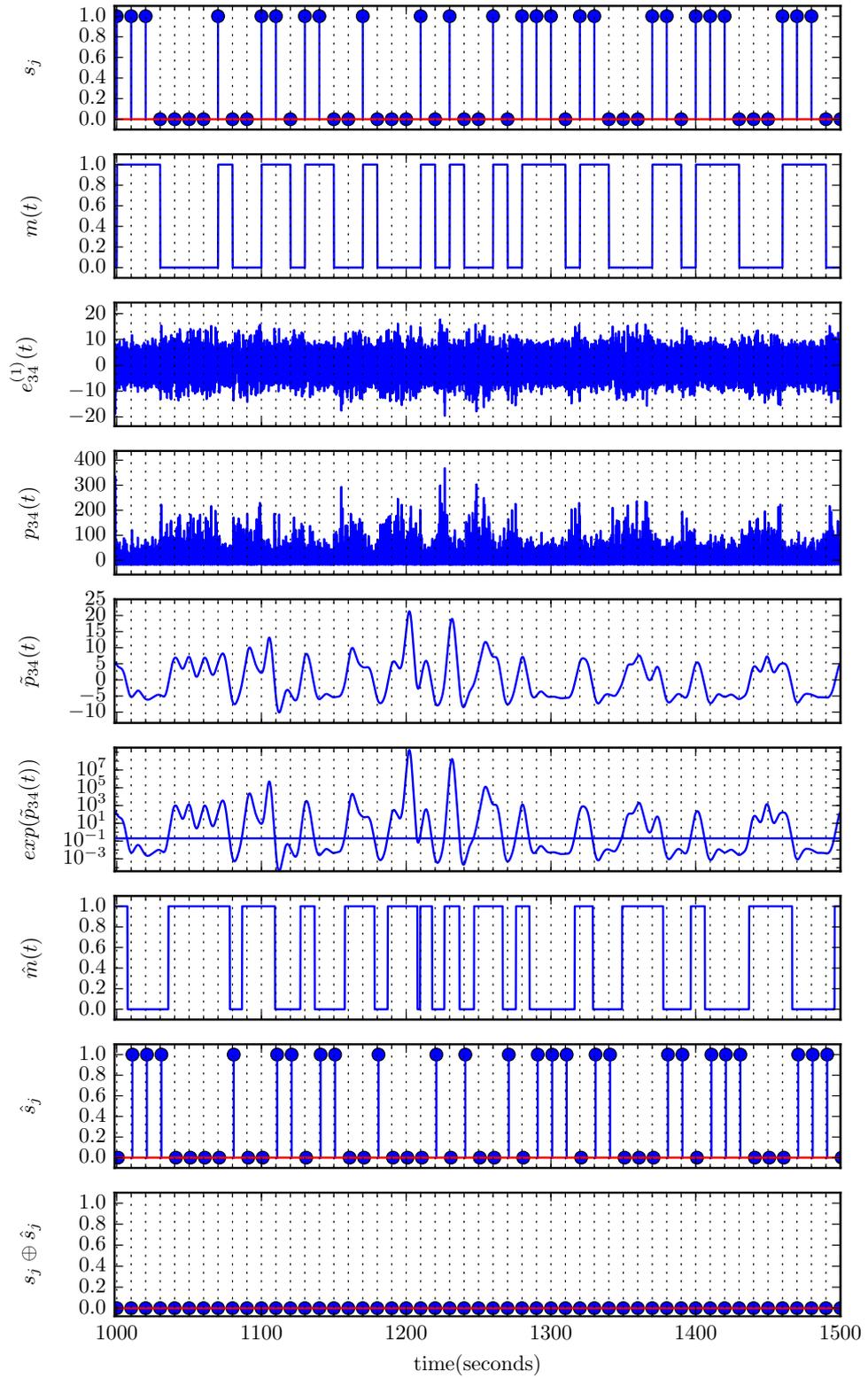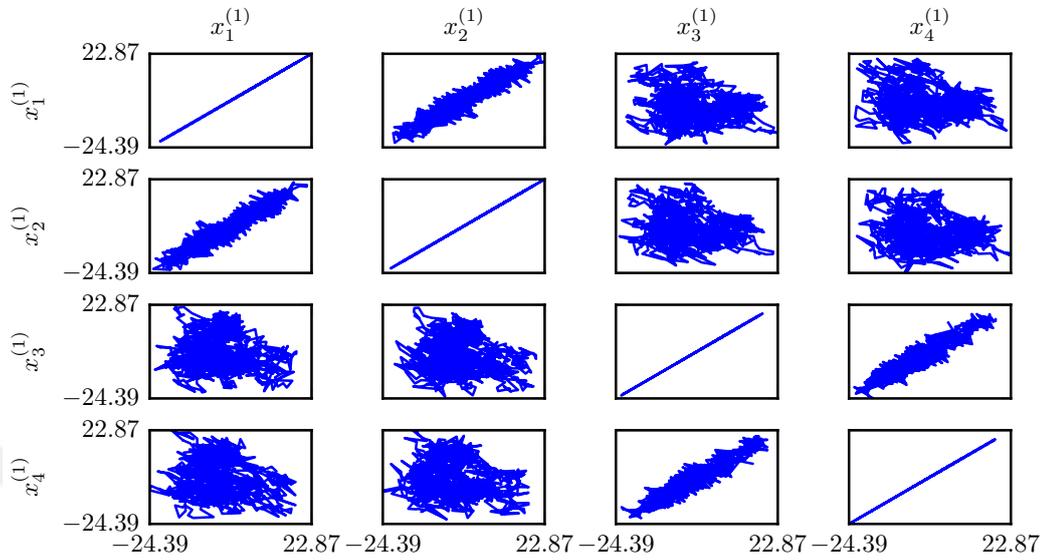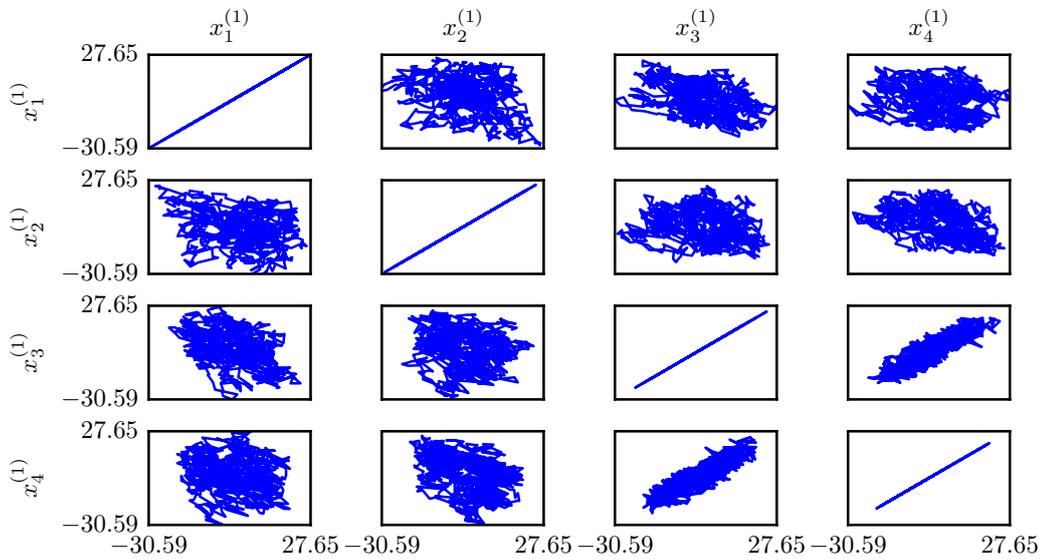
Figure 5.22 Signal flow obbtained by numerical integration of (5.19) with Euler-Maruyama method for a step size $T_s = 0.01$ seconds, symbol transmission time $T_b = 10$ seconds and SNR=15 dB. The plots share the time axis. The transmitted symbol s_j are successfully detected as $\hat{s}_j$. The decompression amplifier output is plotted on a logarithmic scale and the bottom plot shows $s_j \oplus \hat{s}_j$, where $\oplus$ is the logical exlusive-or operation.

(a)
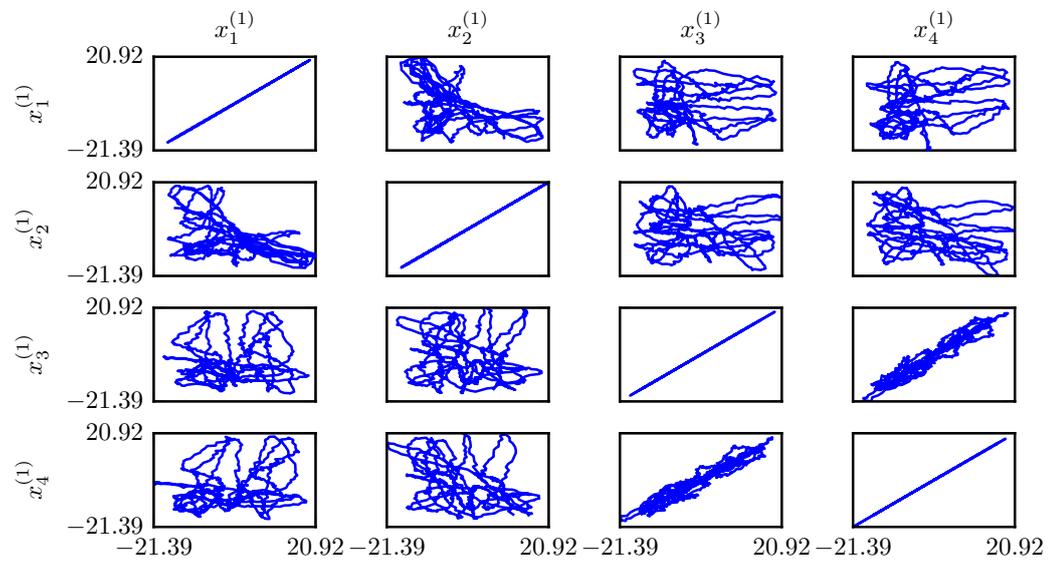
(b)

Figure 5.23 Numerical integration results of (5.19) with Euler Maruyama method for a step size $T_s = 0.01$ seconds, symbol transmission time of $T_b = 10$ seconds and SNR=15 dB. (a) for $1020 \leq t \leq 1030$, (b) for $1030 \leq t \leq 1040$.
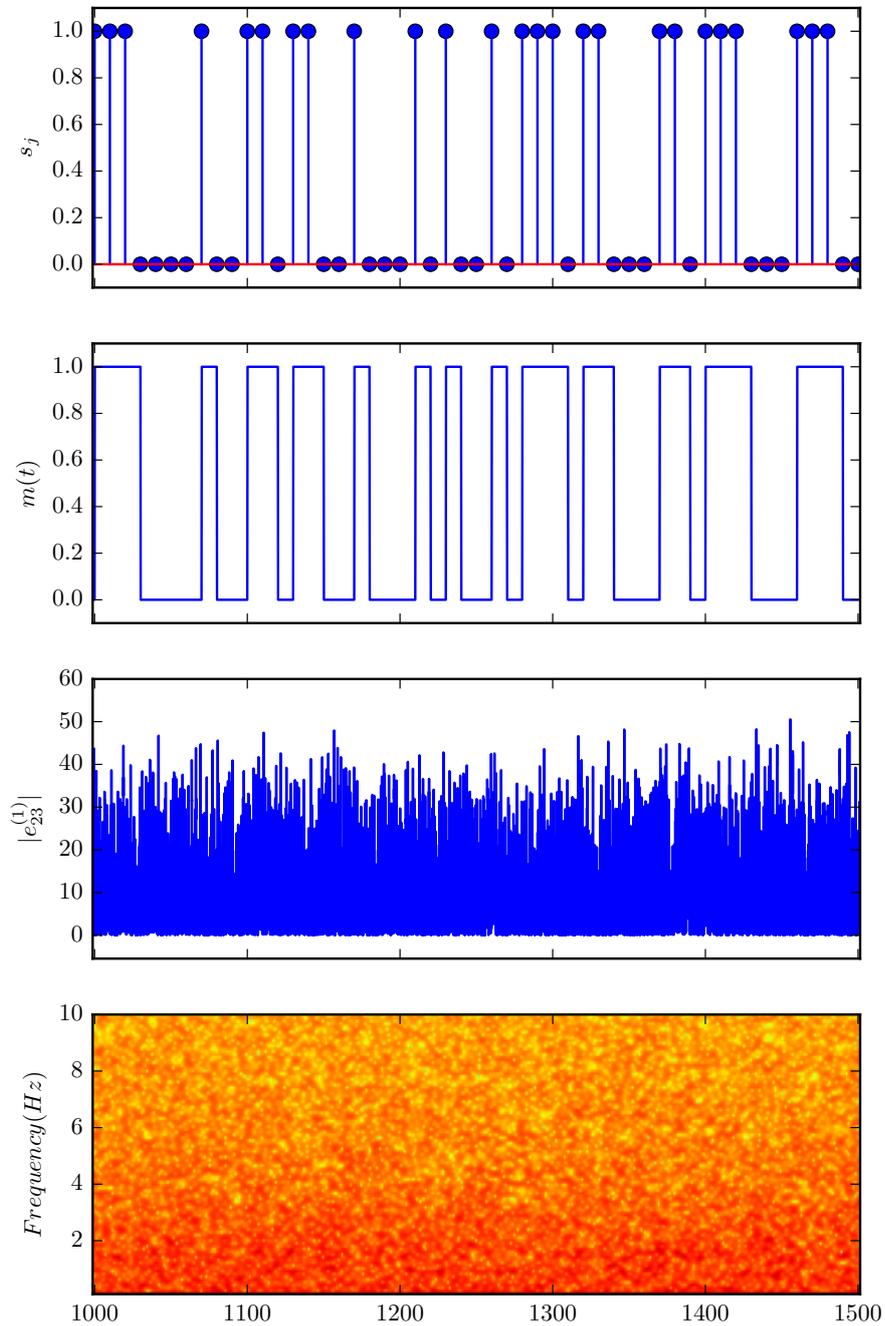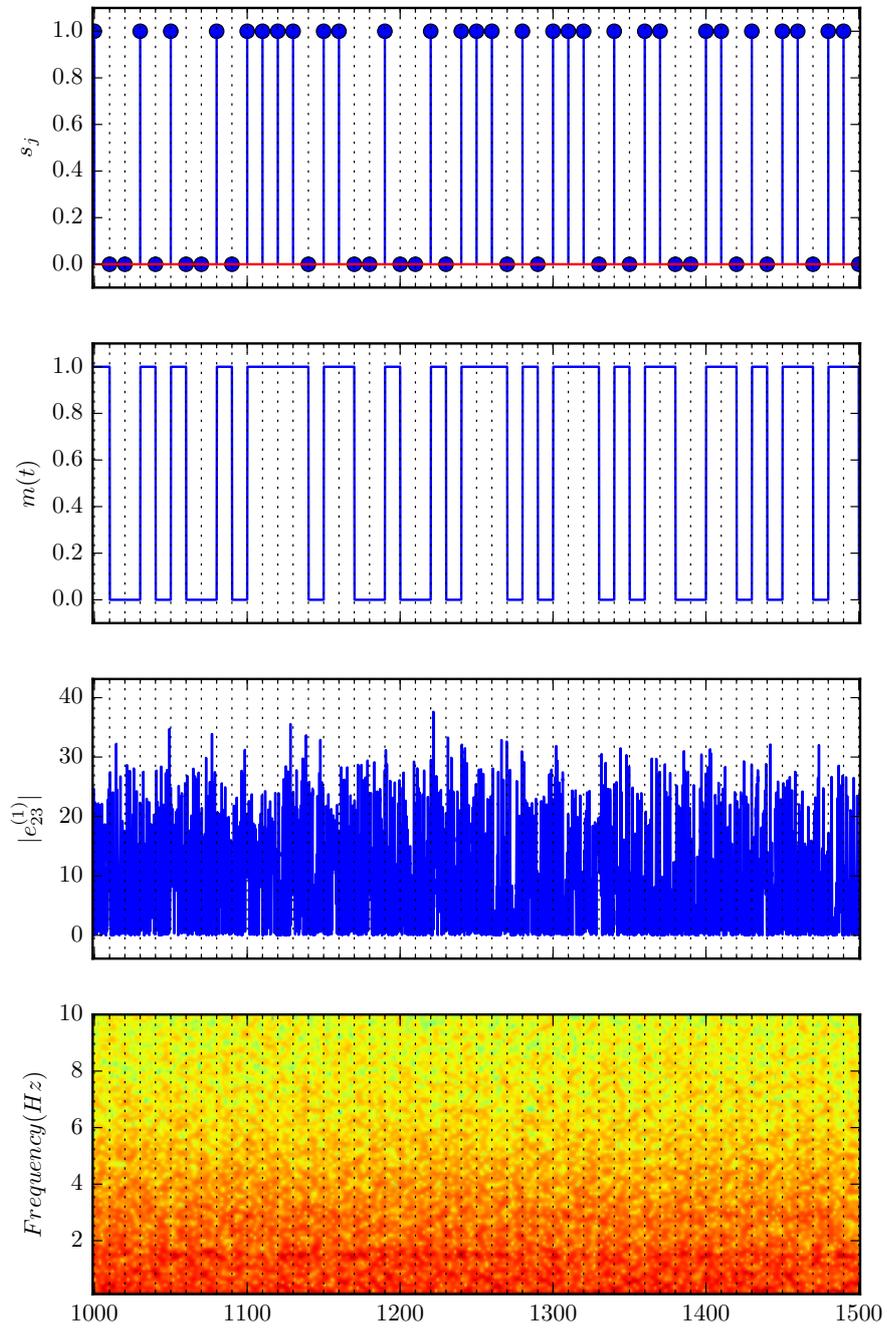
Figure 5.24 Numerical integration results of (5.19) with Euler-Maruyama method for a step size $T_s = 0.01$ seconds, symbol transmission time $T_b = 10$ seconds and SNR=15 dB. The plots share the time axis. Note that there is no apparent correlation between time frequency properties of the channel signal $e_{23}^{(1)}(t)$ and message signal $m(t)$.
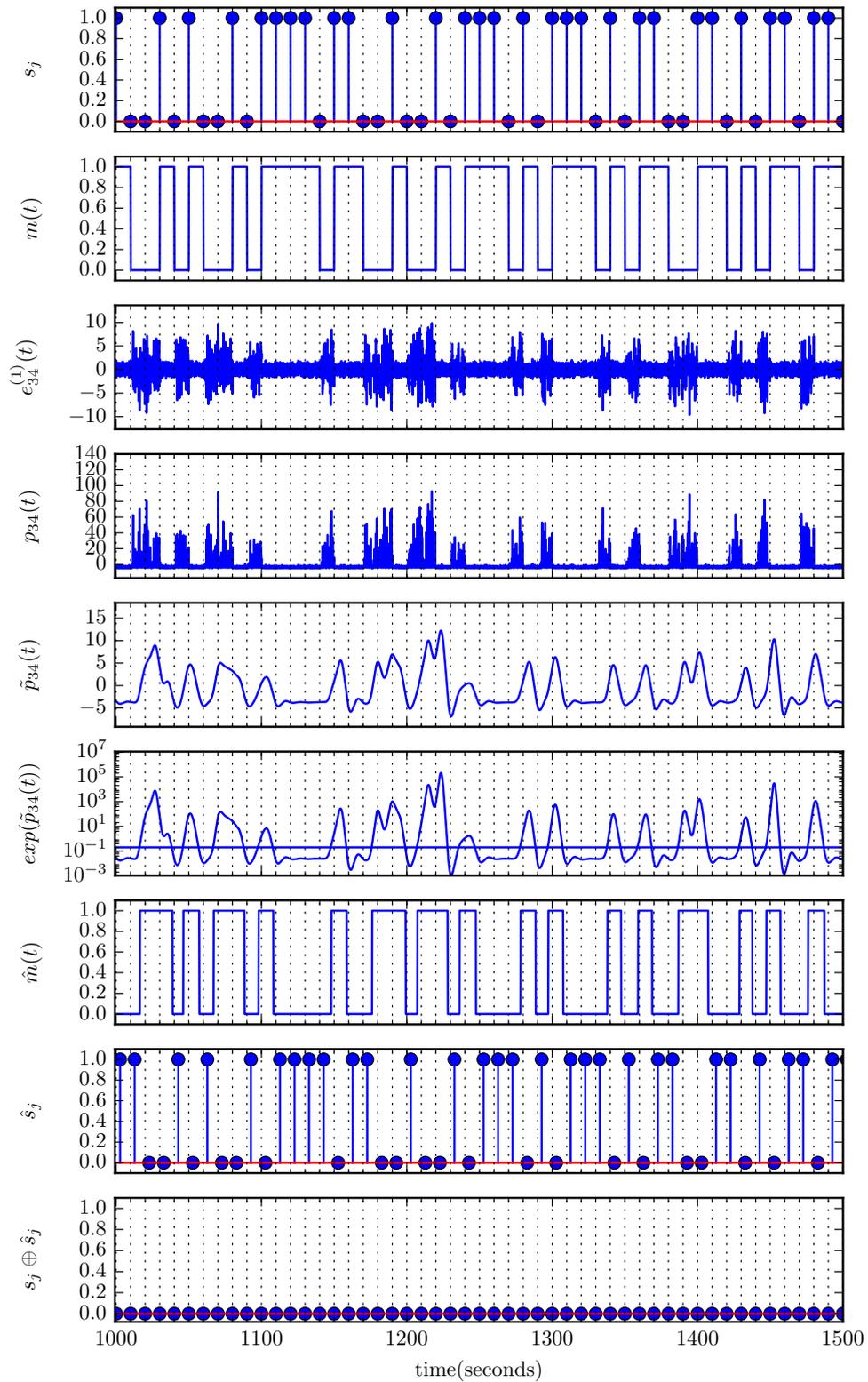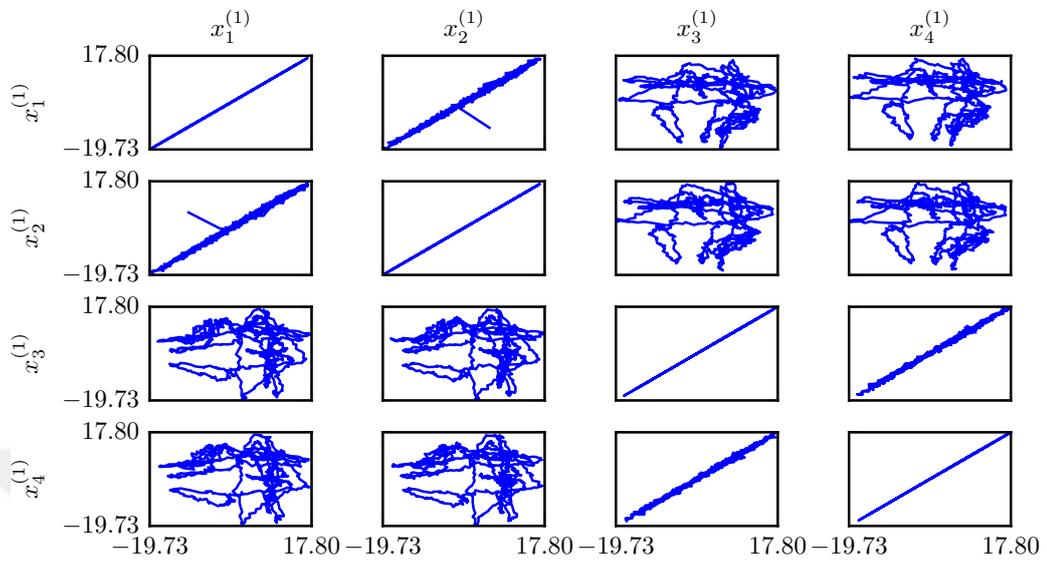
64
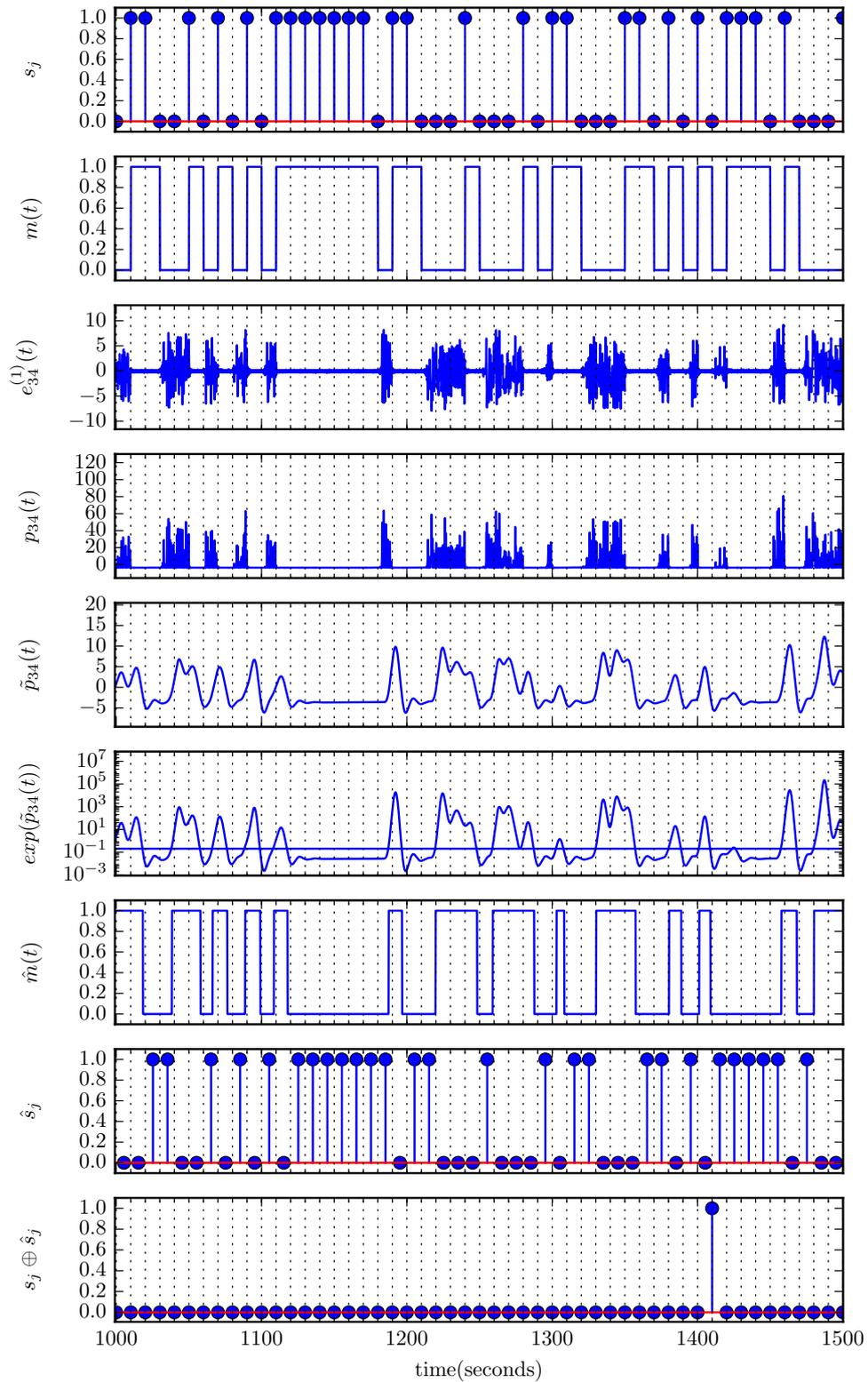
Figure 5.25 Signal flow obbtained by numerical integration of (5.19) with Euler-Maruyama method for a step size $T_s = 0.01$ seconds, symbol transmission time $T_b = 10$ seconds and SNR=30 dB. The plots share the time axis. The transmitted symbol s_j are successfully detected as $\hat{s}_j$. The decompression amplifier output is plotted on a logarithmic scale and the bottom plot shows $s_j \oplus \hat{s}_j$, where $\oplus$ is the logical exlusive-or operation..
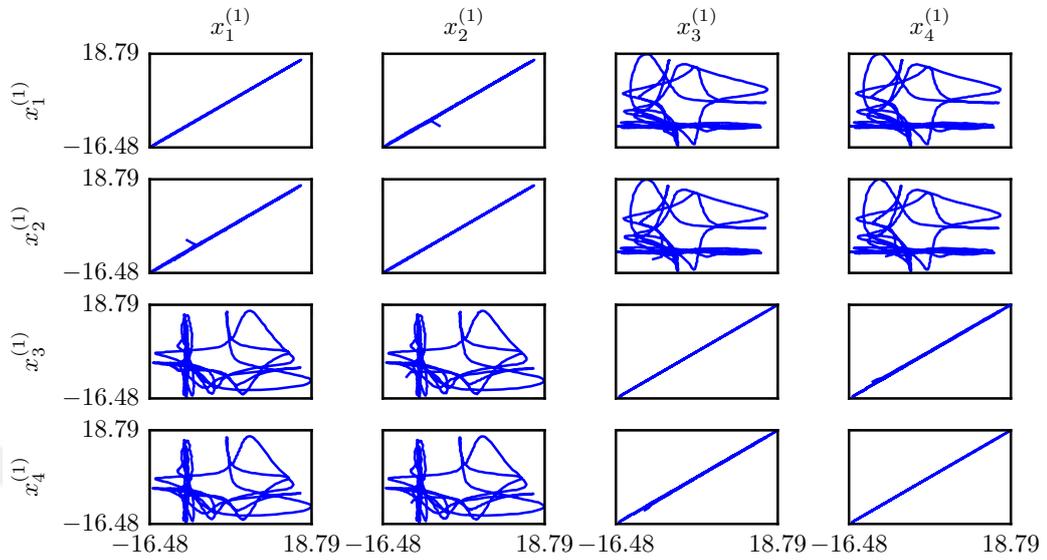
(a)
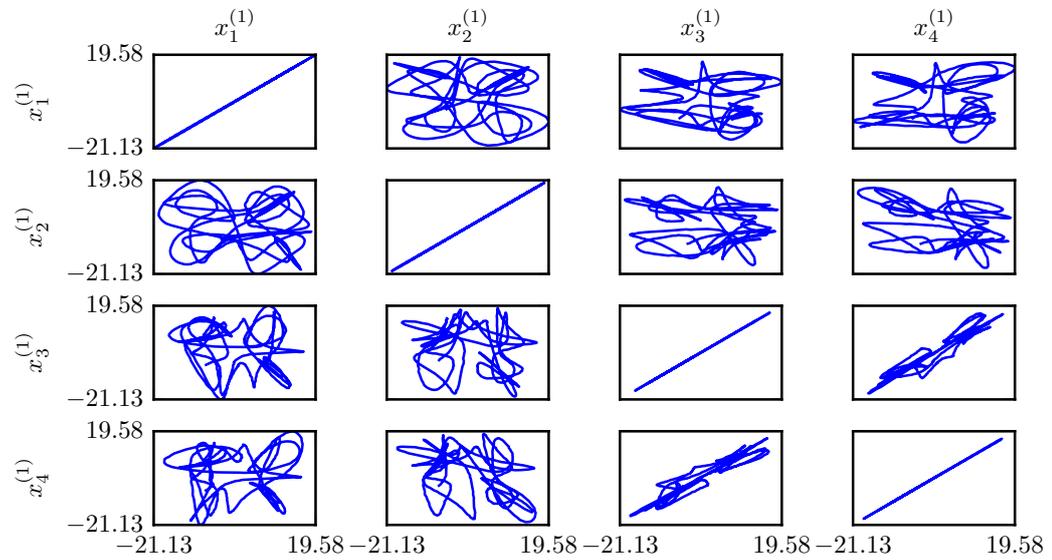
(b)

Figure 5.26 Numerical integration results of (5.19) with Euler Maruyama method for a step size $T_s = 0.001$ seconds, symbol transmission time of $T_b = 10$ seconds and SNR=30 dB. (a) for $1020 \le t \le 1030$, (b) for $1030 \le t \le 1040$.

Figure 5.27 Numerical integration results of (5.19) with Euler-Maruyama method for a step size $T_s = 0.01$ seconds, symbol transmission time $T_b = 10$ seconds and SNR=30 dB. The plots share the time axis. Note that there is no apparent correlation between time frequency properties of the channel signal $e_{23}^{(1)}(t)$ and message signal $m(t)$.
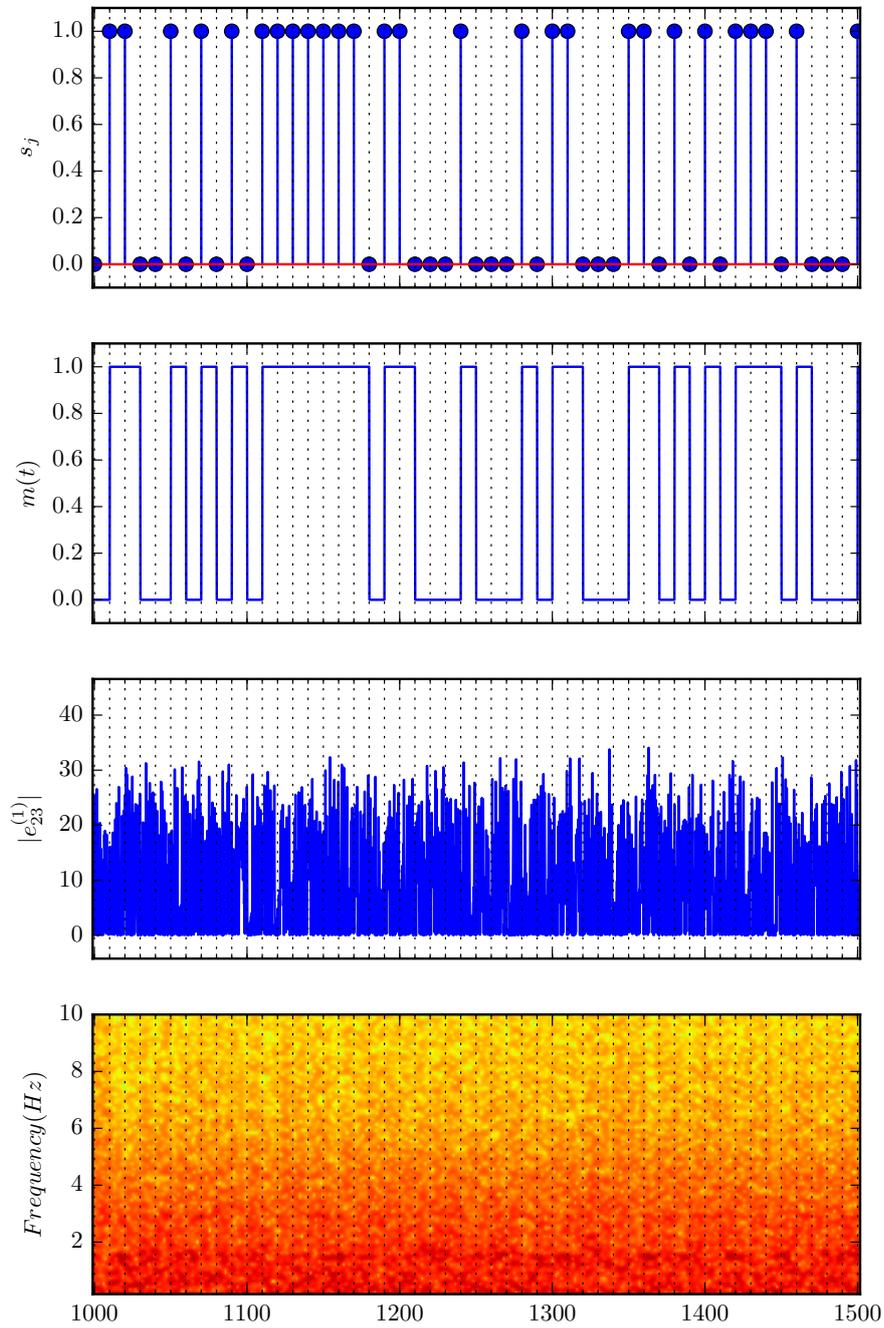
cluster mode $\mathscr{C}_1$ during s_1 transmission and their disappearance during s_0 transmission. This implies that the proposed system achieves symbol transmission.

The symbol detection, hence the cluster mode detection is performed as explained in Chapter 3. From signal flows shown in the results, a delay is apparent between the message signal $m(t)$ and the extracted message signal $\hat{m}(t)$. This delay is mainly caused by the low pass filter, and is directly related to the order of the filter. The extracted message signal $\hat{m}(t)$ is sampled with a sampling period of one symbol transmission time. The amount of delay should be considered while taking samples from the extracted message since it directly effects the symbol detection. The clock signals adjusting the bit duration in the transmitter and the receiver sides may not be exactly synchronous to each other. In order to overcome the clock signals synchronization and delay problem in the sampling process, before starting to transmit the message signal, a predetermined start sequence pulse with one edge transition is first transmitted. In the receiver side sampling of the extracted error message signal $\hat{m}(t)$ is started once edge transition of the start sequence is detected and continued by taking samples in the middle of the symbol transmission time. The results show the transmitted symbols s_j are successfully detected in the receiver side with a certain delay for a low or moderate SNR levels. However, false symbol detection may occur for high SNR levels. This is caused by the amount of noise which is modeled by just a white a Gaussian noise in the channel are not able to desynchronize the oscillators especially there is a high frequency symbol transitions in the message signal. This is again a misleading result caused by numerical simulation. In the physical realm, there is always noise internal to each oscillator which drives the oscillators out of synchrony .

The threshold level is another parameter that effects the performance of the symbol detection and should be optimized to certain level in order not to have pulse or pulses during a symbol transmission time. The start sequence can also be used to determine the optimal threshold level.

The channel signals are one of the vulnerable parts of typical communication system

since they are generally publicly accessible. For a secure communication system no message content should be obtained from the channel signals. For this purpose, the error signal $e_{23}^{(1)}(t) = x_3^{(1)}(t) - x_2^{(1)}(t)$, which is one of the error signals in the channel, has been investigated. Since node 2 and node 3 are not in the same cluster, it seen from the results that there is no change in the temporal behavior of $|e_{23}^{(1)}(t)|$ during any symbol transmission and it is always chaotic having the complexity of a typical chaotic signal. Also from the spectrogram of the $e_{23}^{(1)}(t)$, it can be seen there is no apparent correlation between the time frequency properties of $e_{23}^{(1)}(t)$ and the message signal to be transmitted, which implies no information can be extracted from the time frequency properties of the signals transmitted through the channel by a third party, directly.

CHAPTER SIX
CONCLUSION

In this study, a novel method to design a secure communication system based on the cluster synchronization in networks of chaotic oscillators has been proposed. In the proposed system, one or more controllable parameters allows the cluster synchronization of different node groups. The symbols to be transmitted are represented by the cluster synchronization modes. The system is divided into two as transmitter and receiver, the change of cluster synchronization mode also changes the dynamics in the receiver side and hence the presence or the absence of the symbols are signified by the synchronization mode in the corresponding cluster. Coupling strengths are determined so that cluster mode corresponding to the symbol to be transmitted is enforced. All the nodes are in their chaotic regime and the nodes connecting the transmitter and the receiver sides are not in the same cluster. Therefore, by construction, the signals transmitted from the transmitter to the receiver is always chaotic. The transmitted signal is not directly modulated by the message signal to be sent and when obtained by third party, it cannot be resolved without the knowledge of the transmitter and the receiver internal topologies.

To illustrate the basic concepts in the methodology of the proposed system, a time variant stochastic model of the system has been obtained corresponding to its deterministic counterpart. Signal processing blocks to detect the received symbols has been designed and functioning of the proposed system under different noise levels has been illustrated by numerical analysis. Security aspect of the proposed system has been investigated through time frequency properties of the signals transmitted through the channel.

Simulation results have shown that the proposed system achieves the desired symbol transmission and no information can be extracted from the time frequency properties of the signals transmitted through the channel, directly. It has also been realized that, in addition to the effects of noise in the channel, simulation environment should be modified to include the effects of inherent internal noise of the oscillators in order to

70

increase the detection performance of the system for high SNR levels.

In its proposed form, several coupling signals must be transmitted through the channel. Therefore, additional bandwidth is required in exchange of additional security. The chosen coupling scheme enforces several connections between transmitter and receiver, resulting in additional bandwidth usage. On the other hand, stability analysis of clustered networks proposes many other possibilities for choice of coupling scheme, possibly with single connection between the transmitter and receiver. Hence, coupling scheme shall be optimized as a future study. Current method does not specifically enforce desynchronization of clustered groups, and network modes consist of coexisting chaotic regimes only. These restrictions are to be elevated, by further studies.

This study can be improved further by using higher order stochastic numeric integration schemes. Use of the basic Euler-Maruyama method in integration is somewhat limiting because of its slowness and convergence issues. Because of these limitations, large networks could not be investigated, limiting M-ary communication possibilities.

Application of higher order stochastic integration methods can also open the possibility to simulate the stochastic effects in the chaotic oscillators for more reliable simulation of the proposed system.

The question of detection synchronization and desynchronization reliably is also an open one. This study relied on the fact that synchronization error tends to zero. But due to the chaotic nature of the network dynamics, the states of interest are eventually close enough to mimic that, even though they are not synchronized dynamically, causing bit errors. The synchronization detection method must be revised to take dynamical invariants of error dynamics into account for more reliable detection of transmitted symbols.

Currently, assessment of security of the system had not been tested enough. The system must be checked against known attacks, toughly.

Finally, the work on communication with cluster synchronization will not complete without a fair comparison of its performance with secure communication methods.

REFERENCES

Abel, A., & Schwarz, W. (2002). Chaos communications-principles, schemes, and system analysis. *Proceedings of the IEEE*, *90*(5), 691–710.

Aulbach, B., & Kieninger, B. (2001). On three definitions of chaos. *Nonlinear Dynamics and Systems Theory*, *1*(1), 23–37.

Balanov, A., Janson, N., Postnov, D., & Sosnovtseva, O. (2009). *Synchronization: from simple to complex*. Germany: Springer.

Belykh, I., Belykh, V., & Hasler, M. (2006). Generalized connection graph method for synchronization in asymmetrical networks. *Physica D: Nonlinear Phenomena*, *224*(1-2), 42–51.

Belykh, I., Belykh, V., Nevidin, K., & Hasler, M. (2003a). Persistent clusters in lattices of coupled nonidentical chaotic systems. *Chaos*, *13*(1), 165–178.

Belykh, V., Belykh, I., & Hasler, M. (2000). Hierarchy and stability of partially synchronous oscillations of diffusively coupled dynamical systems. *Physical Review E*, *62*(5), 6332–6345.

Belykh, V., Belykh, I., & Mosekilde, E. (2001). Cluster synchronization modes in an ensemble of coupled chaotic oscillators. *Physical Review E*, *63*(3), 036216.

Belykh, V. N., Belykh, I. V., & Hasler, M. (2004). Connection graph stability method for synchronized coupled chaotic systems. *Physica D: Nonlinear Phenomena*, *195*(1-2), 159–187.

Belykh, V. N., Belykh, I. V., Hasler, M., & Nevidin, K. V. (2003b). Cluster synchronization in three-dimensional lattices of diffusively coupled oscillators. *International Journal of Bifurcation and Chaos*, *13*(04), 755–779.

Belykh, V. N., Belykh, I. V., & Nelvidin, K. V. (2002). Spatiotemporal synchronization in lattices of locally coupled chaotic oscillators. *Mathematics and Computers in Simulation*, *58*(4-6), 477–492.

Belykh, V. N., Osipov, G. V., Petrov, V. S., Suykens, J. A. K., & Vandewalle, J. (2008). Cluster synchronization in oscillatory networks. *Chaos*, *18*(3).

Cuomo, K. M., & Oppenheim, A. V. (1993). Circuit implementation of synchronized chaos with applications to communications. *Physical Review Letters*, *71*(1), 65–68.

Fujisaka, H., & Yamada, T. (1983). Stability theory of synchronized motion in coupled-oscillator systems. *Progress of Theoretical Physics*, *69*(1), 32–47.

Kennedy, M. P., & Hasler, M. (1993). Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits. *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, *40*(10), 634–642.

Li, J., & Ye, X. D. (2016). Recent development of chaos theory in topological dynamics. *Acta Mathematica Sinica, English Series*, *32*(1), 83–114.

Li, S., Alvarez, G., Li, Z., & Halang, W. A. (2007). Analog chaos-based secure communications and cryptanalysis: a brief survey. *arXiv preprint arXiv:0710.5455*, 6. 0710.5455.

Liu, X., Chen, T., & Lu, W. (2011). Cluster synchronization for linearly coupled complex networks. *Journal of Industrial and Management Optimization*, *7*(1), 87–101.

Lorenz, E. N. (1963). Deterministic nonperiodic flow. *Journal of the Atmospheric Sciences*, *20*(2), 130–141.

Ma, Z., Liu, Z., & Zhang, G. (2006). A new method to realize cluster synchronization in connected chaotic networks. *Chaos*, *16*(2).

Parlitz, U., Chua, L., Kocarev, L., Halle, K., & Shang, a. (1992). Transmission of digital signals by chaotic synchronization. *International Journal of Bifurcation and Chaos*, *02*(04), 973–977.

Pecora, L., & Carroll, T. L. (1990). Synchronization in chaotic systems. *Physical Review Letters*, *64*(8), 821–824.

Pecora, L. M., & Carroll, T. L. (1998). Master stability functions for synchronized coupled systems. *Physical Review Letters*, *80*(10), 2109–2112. 0811.0649.

Pikovsky, A., Rosenblum, M., & Kurths, J. (2003). *Synchronization: a universal concept in nonlinear sciences*. Cambridge: Cambridge University Press.

Rosenblum, M. G., Pikovsky, A. S., & Kurths, J. (1996). Phase synchronization of chaotic oscillators. *Physical Review Letters*, *76*(11), 1804.

Rosenblum, M. G., Pikovsky, A. S., & Kurths, J. (1997). From phase to lag synchronization in coupled chaotic oscillators. *Physical Review Letters*, *78*(22), 4193.

Steen, L. A., Seebach, J. A., & Steen, L. A. (1978). *Counterexamples in topology*. New York: Dover Publications.

Strogatz, S. H., & Oppenheim, A. V. (1993). Synchronization of Lorenz-based chaotic circuits with applications to communications. *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, *40*(10), 626–633.

Wiggins, S. (2003). *Introduction to applied nonlinear dynamical systems and chaos*. Germany: Springer.

Yang, S., & Duan, C. (1998). Generalized synchronization in chaotic systems. *Chaos, Solitons & Fractals*, *9*(10), 1703–1707.