PERFORMANCE ANALYSIS OF FILTERING BASED CHAOTIC SYNCHRONIZATION AND DEVELOPMENT OF CHAOTIC DIGITAL COMMUNICATION SCHEMES

AJEESH P. KURIAN

(*B.Tech, University of Calicut, India*)

A THESIS SUBMITTED

FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

NATIONAL UNIVERSITY OF SINGAPORE

2006

To my Teachers

Acknowledgements

I would like to thank:

- My advisor Dr. Sadasivan Puthusserypady for his prompt guidance. Above all for teaching me the importance of perfection.
- My teachers for showing me how beautiful this world is if I have the quest to learn and explore; especially Mrs. Santhakumari, Mr. Sathyavan, Prof. N. O. Inasu, Prof. V. P. Mohandas, Dr. N. Rajanbabu and Dr. S. Sreenadhan.
- My thesis committee members, Prof. C. S. Ng and Dr. George Mathew and thesis examination panel, Prof. Chor Eng Fong, Prof. Kam Pooi Yuen and Prof. Xu Jian-Xin for for their valuable comments and suggestions.
- Examiners of this thesis for their insightful comments.
- My parents for allowing me to pursue this study when the circumstances were not in their favor.
- My friends for helping me to recover from many setbacks; especially Mr. Jayachandran for teaching me the importance of going the extra mile and Mr. Saravanan for all the helps and motivations.

Papers Originated from this Work

Published/Accepted

1. Ajeesh P. Kurian, Sadasivan Puthusserypady, and Su Myat Htut, "Performance enhancement of DS/CDMA system using chaotic complex spreading sequences," *IEEE Trans. Wireless Commun.*, vol. 4, pp. 984–989, 2005.

2. Ajeesh P. Kurian and Sadasivan Puthusserypady, "Performance analysis of nonlinear predictive filter based chaotic synchronization," *IEEE Trans. Circuits Sys. –II*, vol. 9, pp. 886–890, 2006.

3. Ajeesh P. Kurian and Sadasivan Puthusserypady, "Chaotic synchronization: A nonlinear predictive filtering approach," *Chaos*, vol. 16, 2006.

4. Ajeesh P. Kurian and Sadasivan Puthusserypady, "Secure digital communication using chaotic symbolic dynamics," *Invited paper, ELEKTRIK: Turkish J. of Elec. Eng. & Comp. Sci.,* (Special issue on Electrical and Computer Engineering Education in the 21^{st} Century: Issues, Perspectives and Challenges), vol. 14, pp. 195–207, 2006.

5. Ajeesh P. Kurian and Sadasivan Puthusserypady, "Unscented Kalman Filter and Particle Filter for Chaotic Synchronization", *IEEE Asia Pacific Conference on*

Circuits and Systems (APCCAS2006), Grand Copthorne Waterfront, Singapore, December 4–7, 2006

6. Su Myat Htut, Ajeesh P. Kurian, and Sadasivan Puthusserypady, "A novel DS/SS system with complex chaotic spreading sequence," *Proceedings of the* 57^{th} *IEEE Vehicular Technology Conference 2003*, Jeju, Korea, April 22−25, 2003, pp. 2090–2094.

7. Bhaskar T N, Ajeesh P Kurian, and Sadasivan Puthusserypady, "Synchronization of chaotic maps using predictive filtering techniques," *Proceedings of the International Conference on Cybernetics and Information Technology, Systems and Applications*, Orlando, USA, July 14–17, 2004.

Submitted/In Preparation

1. Ajeesh P. Kurian and Sadasivan Puthusserypady, "Self synchronizing chaotic stream ciphers," *IEEE Trans. Circuits Sys. –I: Regular Papers* (Submitted).

2. Ajeesh P. Kurian and Sadasivan Puthusserypady, "Synchronization of chaotic systems using unscented Kalman filter and particle filter," *IEEE Trans. Circuits Sys. –I: Regular Papers* (Submitted).

List of Abbreviations

AWGN	Additive White Gaussian Noise
BER	Bit Error Rate
BPSK	Binary Phase Shift Keying
CA	Chaotic Attractor
CC	Computational Complexity
cdf	Cumulative Density Function
CM	Chaotic Masking
CDMA	Code Division Multiple Access
COOK	Chaotic On Off Keying
CSK	Chaotic Shift Keying
CSP	Constant Summation Property
DCSK	Differential Chaotic Shift Keying
DS/SS	Direct Sequence Spread Spectrum
EDP	Equi-Distributive Property
EKF	Extended Kalman Filter
FM-DCSK	Frequency Modulated Differential Chaotic Shift Keying
HT	Hyperbolic Tangencies
i.i.d	Independent and Identically Distributed

IM	Ikeda Map
LFSR	Linear Feedback Shift Register
LLE	Local Lyapunov Exponent
MAI	Multiple Access Interference
MC	Monte−Carlo
MG	Mackey−Glass
MMSE	Minimum Mean Square Error
NCA	Non-hyperbolic Chaotic Attractor
NISE	Normalized Instantaneous Square Error
NMSE	Normalized Mean Square Error
NPF	Nonlinear Predictive Filter
pdf	Probability Density Function
PDMA	Parameter Division Multiple Access
PF	Particle Filter
PHT	Primary Homoclinic Tangencies
PN	Pseudo Noise
PWLAM	Piece-Wise Linear Affine Map
SD	Symbolic Dynamics
SIS	Sequential Importance Sampling
SNR	Signal to Noise Ratio
SS	Spread Spectrum
SUT	Scaled Unscented Transform
TMSE	Total Mean Square Error
TNMSE	Total Normalized Mean Square Error
UKF	Unscented Kalman Filter
UPF	Unscented Particle Filter
UT	Unscented Transform

List of Frequently used Symbols

$\mathbf{f}(.)$	Smooth nonlinear function (Process function)
$\mathbf{h}(.)$	Output function (Measurement function)
$\mathbb{E}[.]$	Expectation operation
$p(x)$	Probability density function
$p(x\|y)$	Conditional probability density function of x given y
$\frac{\partial x}{\partial y}$	Partial derivative of x with respect to y
$Q(.)$	Q–function
$\bigoplus$	Exclusive OR (XOR)
$J(.)$	Cost function
$diag[.]$	Diagonal matrix
$col[.]$	Column matrix
$\Re\{.\}$	Real part of a complex variable
$\Im\{.\}$	Imaginary part of a complex variable

Summary

The property of sensitive dependence of chaotic systems/maps on its initial conditions is being exploited in developing chaotic communication systems. Because of this property, any change in control parameters or the initial conditions of the chaotic systems/maps leads to an entirely different and uncorrelated trajectory. Chaotic communication systems are developed with the aim of improved security.

In chaotic communication schemes, synchronization of transmitter and receiver chaotic systems/maps has prime importance. Following the drive−response synchronization scheme developed by Pecora and Carrol, researchers from different disciplines have suggested several methods to achieve faster and accurate synchronization. One of the widely studied method for chaotic synchronization is the coupled synchronization. It is shown that the drive−response system is a special case of the coupled synchronization. Another interesting aspect of the coupled synchronization is its similarity with the observer design problems encountered in nonlinear control systems. In recent literature, many observer design techniques are successfully applied for chaotic synchronization.

Extended Kalman filter (EKF) is a widely studied nonlinear observer for the synchronization of chaotic systems/maps. In the presence of the channel noise, its performance is found to be similar or better than the optimal coupled synchronization. However, it is observed that the trajectories tend to diverge when EKF is applied to synchronize

chaotic maps with non−hyperbolic chaotic attractors (NCA). In Chapter 2, all plausible divergence behaviours of the EKF based scheme when it is applied to synchronize Ikeda maps (IM) are analyzed in detail. A better understanding of this behaviour is obtained through the study of homoclinc tangencies, dynamics of the posterior error covariance matrix and the local Lyapunov exponents (LLEs) of the receiver IM. The normalized mean square error (NMSE), total normalized mean square error (TNMSE), and normalized instantaneous square error (NISE) are used for performance evaluation, and are presented in Chapters 2, 3 and 4. The first two performance indices give an idea about the synchronization error while the latter gives an idea about the speed of synchronization.

To overcome the divergence of the trajectories encountered in the EKF based synchronization, other nonlinear filtering methods such as unscented Kalman filter (UKF), particle filter (PF) and nonlinear predictive filter (NPF) are proposed and studied. UKF and PF are sequential Monte−Carlo methods. Using carefully sampled points from the prior probability, the posterior density is approximated. UKF assumes that the prior density is Gaussian and uses unscented transform (UT) to approximate the posterior density. Unlike UKF, the PF does not use the Gaussianity of the prior density. PF can deal with any probability density and it allows complete representation of the posterior probability density of the states. Using the PF, any statistical quantities (such as mean, modes, kurtosis, and variance) can be computed. In Chapter 3, the performance of the UKF and PF based methods in synchronizing IM, Lorenz and Mackey−Glass (MG) systems are discussed in detail. Performance of the EKF based scheme is used for comparison.

NPF uses a very simple predictor corrector model for synchronization. The advantages of the NPF are: (*i*) the model error is assumed unknown and is estimated as a part of the solution, (*ii*) for a continuous system, it uses a continuous model to estimate the states and hence avoids discrete state jumps, and (*iii*) there is no need to make any assumptions on the prior density. In Chapter 4, the performance of the proposed NPF based scheme is compared to the EKF based scheme. IM, Lorenz and MG systems are used for the numerical evaluation. The condition for stability and an approximate expression for the total normalized mean square error (TNMSE) are also derived.

Symbolic dynamics (SD) is a coarse−grain representation of the dynamics of chaotic systems/maps. SD based method are shown to be capable of providing high quality synchronization. In Chapter 5, using the SD based synchronization of 1−D chaotic maps, a novel dynamic encoding system is proposed for secure communication. This scheme is secure and has the self synchronizing properties. A theoretical expression for the upper bound of the bit error rate (BER) is derived for the new scheme. BER performances of the new scheme is comparable to that of the binary phase shift keying (BPSK) system at moderate signal to noise ratios (SNRs). The security aspect of the new system is also analyzed in detail.

Time series generated from chaotic maps can be used as spreading codes (sequences) for the direct sequence/spread spectrum (DS/SS) communication applications. It is an inexpensive alternative to the linear feedback shift register (LFSR) sequences such as m-sequences and Gold sequences. In Chapter 6, a novel DS/SS communication system which exploits the complex nature of the IM is proposed. With this double spreading DS/SS system, the effect of multiple access interference (MAI) is mitigated by choosing spreading sequences with appropriate cross−correlation properties. The performance of the system is assessed and demonstrated in multiuser environments by means of computer simulation with additive white Gaussian noise (AWGN), Rayleigh fading, and selective fading channel conditions. The proposed system significantly outperforms the Gold code DS/SS BPSK system in synchronous channel conditions. In asynchronous case, the improvement is substantial for low SNR values.

Contents

List of Tables

List of Figures

Chapter 1

Motivation and Literature Survey

1.1 Introduction

Chaotic systems/maps are nonlinear systems which exhibit complex behaviour. In chaotic systems, the state variables move in a bounded, non−periodic, random−like fashion. A distinct property of chaotic dynamics is its long-term unpredictability. In systems which exhibit chaotic dynamics, initial states which are very close to each other produce markedly different trajectories[1]. This is referred to as sensitive dependence on initial conditions [1]-[3]. In chaotic systems/maps, due to the sensitive dependence on initial conditions, when nearby points are iterated the error is amplified in each iteration resulting in uncorrelated trajectories.

1.2 Characteristics of Chaotic Dynamics

A dynamic system exhibits either one of the following characteristics when it is excited by an external stimulus: (*i*) the system dissipates all its energy and settles down to a stable point, (*ii*) it travels through a periodic orbit with time, or (*iii*) it diverges from its initial point and becomes unstable eventually. A fourth class is the chaotic behaviour where the dynamics exhibit a deterministic yet random−like behavior [4]. In chaotic systems, the dynamics travel through a non−periodic orbit called a strange attractor.

[1]The points through which the system states travel in the state space are called the trajectories.

These systems are characterized by three essential properties: (i) sensitivity to its initial conditions, (ii) mixing, and (iii) dense unstable periodic points [1]. When nearby trajectories evolve to result in uncorrelated trajectories, while forming the same attractor, the dynamical system is said to possess sensitive dependance to initial conditions. Mixing is the property of the states of a dynamic system to move from one point to another in state space with non−zero measure (i.e. each point in state space is visited with a non−zero probability) [1]. Every chaotic attractor is formed by a skeleton of unstable periodic points with different periods. The trajectories generated from chaotic systems have wide−band characteristics and noise−like appearance [3]. Chaotic dynamics have found numerous applications in communication, digital water marking etc. [5]. In this thesis, chaotic systems/maps are studied for their applications in communications.

1.3 Communication using Chaos

Chaotic time series, with their inherent wide−band and random−looking characteristics, naturally qualify for secure communication applications. A communication scheme is chaotic if a chaotic signal generator is used in the system to encode, spread or carry the information signal [6][7]. These systems exploit the properties of chaotic dynamics in one way or the other. There are many applications in which chaos can be used in communication systems. Most widely studied methods are as follows.

i. **Chaotic Masking:** This scheme uses chaotic time series as wide-band carrier so that coding and modulation can be accomplished together. In chaotic masking (CM) [8], the weak information signal is added to a strong chaotic carrier. With a synchronized chaotic system at the receiver, a local copy of the carrier signal is generated and it is subtracted from the received signal to retrieve the information. Here, the random−looking behavior is used to introduce security.

ii. **Chaotic Modulation:** In chaotic modulation, parameters of the chaotic system/map at the transmitter are changed according to the information signal and the resulting chaotic waveform is transmitted. At the receiver, these parameter changes are tracked using appropriate methods and the information is retrieved [9].

iii. **Chaotic Shift Keying:** In coherent schemes such as chaotic shift keying (CSK) and chaotic on–off keying (COOK) [10]-[13], digital information is transmitted using carrier signals generated by two different chaotic systems/maps. In CSK, output from two chaotic systems/maps are switched according to the transmitted bit ('0' or '1'). In COOK, only one chaotic system is used to convey the information bits; chaotic system/map is turned on or turned off according to the information bits. In both cases, synchronized chaotic systems/maps at the receiver is used to retrieve the information bits.

iv. **Non−coherent Chaotic Shift Keying:** To avoid the need of chaotic synchronization, many non−coherent chaotic communication systems have been developed (e.g. differential chaotic shift keying (DCSK) [14], frequency modulated DCSK (FM−DCSK) [15], etc.). Since these schemes are non−coherent, only a portion of the transmitted signal is used for carrying the information and rest are used to retrieve the information. Hence, this class of communication schemes does not need a synchronized chaotic system at the receiver.

v. **Symbolic Dynamics:** Symbolic representations of controlled chaotic orbits/ trajectories produced can be used for developing communication schemes. By manipulating the symbolic dynamics (SD) of chaotic systems[2]/maps in an intelligent way, the system produces trajectories in which digital information is embedded in the corresponding SD [16][17]. Using appropriate synchronization techniques at the receiver, the message can be retrieved.

vi. **Direct Sequence Spread Spectrum:** Another way of using chaotic systems/maps in communication systems is to generate spreading codes from chaotic systems/maps. Since chaotic signals are wide−band, non−periodic and noise−like, chaotic systems offer an ample choice of spreading codes [18]-[20].

[2]For chaotic systems, the SD is obtained through the Poincare return map [16].

1.4 Chaotic Synchronization

It is clear from the above discussion that in most of the chaotic communication schemes, synchronization of the transmitter and the receiver chaotic systems/maps is essential for reliable/accurate retrieval of information. Indeed, the use of synchronizing chaotic circuits for communication applications has evolved into an active area of research. Related works of synchronization dates back to the research carried out by Fujisaka and Yamada [21] in 1983. Pecora and Carroll [22] showed that chaotic systems can be synchronized using the drive−response scheme. They showed that, by splitting the chaotic system into drive and response systems, chaotic synchronization can be established if all the transversal Lyapunov exponents of the response system are negative. Following this seminal work, numerous methods have been proposed to synchronize chaotic systems/maps. A detailed review of the present state of synchronization of chaotic systems/maps is available in [23].

Among the various methods reported, coupled synchronization has attracted the most interest [24]. If proper coupling is introduced between the transmitter and receiver systems, reliable synchronization can be established. Synchronization behaviours (speed and accuracy) depend on the coupling strength. Coupling strength is selected such that the local and global transversal Lyapunov exponents of the receiver systems become negative in noisy and noiseless situations, respectively [25]. Due to the similarity of coupled synchronization scheme with the nonlinear observer design problem, there has been lot of interest in applying nonlinear observer design schemes for the synchronization of chaotic systems/maps [26]-[29].

Research results show that intervals of desynchronization bursts can appear in coupled synchronization when noise is present in the system [27]. In [30], this behavior is explained with the help of the existence of unstable periodic orbits of chaotic systems. In such situations, an adaptive estimation of coupling strengths would be optimal. In fact, this idea led to the application of stochastic estimation techniques for synchronization of chaotic systems. In [31], stochastic control methods are applied for the synchronization of chaotic systems.

Extended Kalman filter (EKF) is one of the widely used stochastic estimation schemes in nonlinear state estimation and tracking applications [32, Chapter 5]. In EKF, Kalman filtering [32, Chapter 4] [33][34, Chapter 6] is applied to the linearized[3] nonlinear function. The use of EKF in synchronizing Lorenz systems is reported in [35]. Sobiski and Thorp [36] used the EKF to develop parameter division multiple access (PDMA) communication scheme. Application of EKF to synchronize chaotic maps is studied in [37]. Analytical results for 1D and 2D chaotic maps are derived in [38]. However, a major disadvantage of EKF is the error in function approximation. For highly nonlinear systems, this error causes the divergence of trajectories leading to the burst of desynchronization behaviour [39]-[42].

1.4.1 Divergence of EKF in Non−hyperbolic Chaotic Maps

Noise−induced escape from a chaotic attractor (CA) to another co−existing CA or a stable fixed point is observed in many non−hyperbolic chaotic attractors (NCAs) [43]. In such systems, small perturbations get amplified near the primary homoclinic tangencies (PHTs) and it may eventually take the system states from one CA to another CA or to a fixed point. Homoclinic tangencies (HTs) are points where the stable and unstable manifolds of an unstable periodic orbit meet tangentially. At these points, the perturbations may get amplified by a factor of 100 to 1000 [43]. The most probable exit path (i.e. the most probable set of points through which trajectories travel from one basin of attractor to the other) and the mean exit time of such chaotic systems/maps give a measure of the system's stability against weak noise perturbations. In Chapter 2, divergence behaviour of the EKF based scheme applied to the synchronization of IM is analyzed in detail. It is found that the trajectories originating from the CA is taken to a stable fixed point. Since the EKF uses the first order Taylor series for approximating the nonlinearities, large errors are introduced to systems with higher order nonlinearities. A possible solution to overcome such difficulties is to apply filtering methods which introduce less approximation errors. Accordingly, in this thesis, three nonlinear filtering algorithms are proposed and applied for the synchronization of the chaotic systems/maps, namely, (i)

[3]Linearization is done using the first order Taylor series.

the unscented Kalman filter (UKF), (*ii*) the particle filter (PF), and (*iii*) the nonlinear predictive filter (NPF).

1.4.2 The Unscented Kalman Filter

Many alternatives to the EKF have been suggested to overcome the problems associated with the approximation errors. If the noise is Gaussian, instead of approximating the nonlinear function, one can approximate the posterior density itself [39]. UKF follows this approach by using an unscented transform (UT). For this, with the knowledge of the mean and covariance of the prior density, a set of points (called the sigma points) are selected. Each sigma point is associated with a scalar weight. These points are propagated through the nonlinearity and the resultant points are used to obtain the approximate estimate the of mean and covariance of the posterior density [39][40]. If the prior density is Gaussian, these filters can correctly estimate the mean and covariance of the signal up to the third order compared to the first order approximation in the EKF [40]. In [44][45], uses of UKF for the synchronization of chaotic systems in direct sequence spread spectrum (DS/SS) applications are reported. Application of UKF to synchronize polynomial systems is discussed in [46]. Noise reduction in chaotic signals using UKF is reported in [47]. An expectation maximization based unscented Kalman smoother to simultaneously estimate parameters of system along with the equalized chaotic signal is reported in [48].

1.4.3 The Particle Filter

UKF relies on the Gaussianity of the prior density. This might be a very stringent assumption for many nonlinear filtering problems. Particle filters (PFs) are a class of nonlinear filters that do not require any assumption on the underlaying noise. It is based on the sequential Monte−Carlo (MC) simulation method; a set of weighted samples (particles) approximate the posterior distribution [49]. In Chapter 3, the UKF and PF are applied for the synchronization of chaotic systems/maps. The EKF is used as a reference for comparing the performance of the proposed algorithms. Synchronization behaviours of Lorenz and Mackey−Glass (MG) systems and IM are studied.

1.4.4 The Nonlinear Predictive Filter

NPF is based on a predictive tracking scheme first introduced by Lu [50]. In the NPF based scheme, though the model error is unknown, it is estimated as part of the solution. It uses a continuous model to determine the states and hence avoids any discrete state jumps. A major advantage of NPF is that it does not assume Gaussianity of the posterior probability unlike in EKF. In Chapter 4, the application of NPF to the synchronization of various chaotic systems/maps is studied in detail. The performance of the proposed scheme is compared with the EKF method. The well known Lorenz and MG systems as well as IM are used for numerical evaluation of the performance.

1.5 Symbolic Dynamics

SD is defined as the coarse−grain description of the chaotic dynamics and has been used for the analysis of chaotic systems [51]. It is the representation of the orbits (trajectories) of dynamical systems by symbols selected from a finite alphabet. The state−space of the system/map is partitioned and specific symbols are assigned for each of the partitions; thus making the representation coarse−grain. Recently, SD is being used for secure communication applications. In [16], chaotic communication by the feedback of SD is proposed. Application of SD for differential chaotic shift keying (DCSK) is discussed in [52]. SD based noise reduction and coding are proposed in [53], [54]. When the transmitter and the receiver synchronizes with a synchronization error below certain threshold, it is said to have high quality synchronization [55]. This is ideal for setting up reliable secure communication. In [56], a high quality synchronization is achieved using SD. The synchronization using SD is reformulated from an information theoretic point of view in [57]. In Chapter 5, a novel secure digital communication scheme using the chaotic SD is proposed. This scheme is similar to the self synchronizing stream ciphers. The newly suggested system has well behaved bit error rates (BER) in additive white Gaussian noise (AWGN) and multi−path channels. Moreover, existing coding and modulation methods can be used to enhance the BER performance, if needed. In this scheme, the synchronization information is sent periodically. Hence, dynamic degradation, where

the finite precision computation makes the chaotic trajectories to become periodic after certain iterations, is not observed.

1.6 Chaos based DS/SS Communication System

In DS/SS communication systems, each user is given a unique signal (spreading sequence) having a bandwidth which is much higher than that of the information signal [58]. Hence, the transmitted signal, after spreading, has less power spectral density and high bandwidth relative to the original information signal. At the receiver, with the same (synchronized) sequence, a correlation operation is performed on the received signal to retrieve the information. These spreading sequences should possess minimal cross-correlation to reduce the multiple access interference (MAI) as well as excellent auto−correlation for synchronization and multi-path performance [59].

Many authors have shown that chaotic spreading sequences can be used as an inexpensive alternative to the linear feedback shift register (LFSR) sequences such as m-sequences and Gold sequences. In [18]-[20], the possibility of generating infinite number of spreading sequences for a DS/SS communication system by means of 1D chaotic maps is claimed. Simulation based comparisons between Gold sequences and the sequences generated with coupled map lattice chaotic time series are also reported in [60] for a synchronous DS/SS system. Analytical results for the applicability of chaotic sequences for DS/SS systems are available in the literature for chaotic time series based communication systems [61]-[64]. Kohda and Tsuneda [65] reported that there exists a wide class of ergodic maps with the equi−distributivity property (EDP) and their associated binary functions with constant summation property (CSP). They have shown that independent and identically distributed (i.i.d) binary spreading codes can be generated from these maps which are optimal for quasi–synchronous communication channels [65]-[67]. The generation and optimization of spreading sequences from piece-wise linear affine map (PWLAM) have been analyzed by many researchers [5][68][69]. They have shown that these systems can accommodate 15 to 20 % more users than the conventional systems based on the pseudo noise (PN) sequences in asynchronous channel. In Chapter 6, a novel

double spreading communication system which exploits the complex nature of the IM sequence is proposed. The idea is to select the spreading codes such that the interference in quadrature phase is negated by the interference in the in−phase.

1.7 Major Contributions and Organization of this Thesis

From the above discussions, three key areas that can be identified in chaotic communication systems are: (*i*) synchronization of chaotic systems, (*ii*) application of SD to secure communications, and (*iii*) application of chaotic time series to generate spreading sequences for SS communication systems.

- For coherent chaotic communication schemes, synchronization of chaotic systems/maps (at the transmitter and receiver) is the most important step. Hence, synchronization of chaotic systems/maps is explored. Since filtering based synchronization schemes come as handy tools, such methods are explored in detail.

- One of the main drawbacks of the existing chaotic communication systems is their inability to perform in multi−path channel conditions. Using the SD of 1D chaotic map, a novel secure chaotic communication scheme (which has similar properties as of a chaotic stream ciphers) is proposed.

- In DS/SS communication systems, the MAI due to the correlation between the spreading sequence (of the users) reduces the capacity. Complex nature of the IM sequence is exploited to develop a novel DS/SS communication system.

The major contributions and organization of the thesis are as follows.

1. When the EKF based synchronization method is applied to chaotic systems/maps with NCAs, large number of trajectories are found to be diverging. Reasons for this divergence behaviour is attributed to two facts: (*i*) in NCAs with fractional basin boundaries, small perturbations can get amplified and take the system states to a co−existing point (or another chaotic) attractor and (*ii*) convergence of the Kalman gain is different in different regions of the state space. This behaviour of

the EKF based scheme, when it is applied to synchronize IM, is analyzed in detail in Chapter 2. More insight into the behaviour is obtained by analyzing the local Lyapunov exponents (LLEs) of the receiver system.

2. The main problem associated with the EKF based synchronization scheme is the error introduced by the first order Taylor series state approximation and the divergence behaviour observed in the NCAs. Other nonlinear filtering algorithms (with lower approximation error capabilities) such as the UKF and the PF are proposed and applied for the chaotic synchronization. A detailed study of these two filtering based synchronization schemes is presented in Chapter 3.

3. The application of NPF to the synchronization of chaotic systems/maps is presented in Chapter 4. The performance of the proposed scheme is compared with the EKF method. Analytical results for the system stability are also derived.

4. In Chapter 5, a secure digital communication scheme using the SD is developed. The BER characteristics are analyzed both numerically and theoretically. Unlike other chaotic communication systems such as the CSK or DCSK, the proposed scheme is bandwidth efficient. This scheme has self synchronization properties. Moreover, the BER characteristics of the new system converges asymptotically to that of the BPSK system at high SNRs. Security aspects the new scheme are also discussed.

5. Chaotic maps have long been considered as a potential source of spreading codes for SS communications. In Chapter 6, a new DS/SS communication scheme is developed which exploits the 2D complex chaotic IM as the new spreading sequence. By selecting the in−phase and quadrature phase components appropriately, the proposed system reduces the MAI effectively. The BER performance of the proposed scheme is compared with that of the conventional Gold sequence BPSK schemes with the help of computer simulations.

Chapter 2

Extended Kalman Filter for Chaotic Synchronization: Analysis of Divergence Behavior

2.1 Introduction

Extended Kalman filter (EKF) has been shown to be successful in synchronizing chaotic systems/maps in stochastic environments. This ability of the EKF initiated a significant research interest [35][28]. The EKF based scheme can be considered as a coupled synchronization scheme which is capable of estimating the coupling strengths adaptively. Chaotic systems with non−hyperbolic chaotic attractors (NCA) displays noise induced escape from a chaotic attractor (CA) to another CA or a fixed point. In this chapter, synchronization of Ikeda map (IM) which has NCA is analyzed.

This chapter is organized as follows. In Section 2.2, the chaotic synchronization as a state estimation problem is discussed. The EKF is introduced in Section 2.3 from a Bayesian point of view. In Section 2.5, the NCAs and noise induced escape found in such systems are explained. Detailed discussion of different types of divergence behaviour is given in Section 2.6. In Section 2.7, the numerical evaluation of the EKF based synchronization of IM is presented. Concluding remarks are provided in Section 2.8.

2.2 Synchronization of Chaotic Systems as a State Estimation Problem

In a chaotic communication scheme, there are at least two chaotic systems/maps which constitute the transmitter and the receiver systems. Chaotic signals are used as carrier waveforms to transmit information from the transmitter to the receiver. To retrieve this information effectively at the receiver, these two systems must be synchronized. Here, synchronization referrers to the application of suitable mechanisms to establish a relationship between the trajectories of the two systems. Because of the sensitive dependence on the initial conditions, synchronization of chaotic systems, also known as the chaotic synchronization is considered to be a difficult task.

Consider two chaotic systems given by the following set of equations:

$$\dot{\mathbf{x}}(t) = \mathbf{f}(\mathbf{x}(t)) \tag{2.1a}$$

$$\dot{\hat{\mathbf{x}}}(t) = \mathbf{f}(\hat{\mathbf{x}}(t)) \tag{2.1b}$$

where $\mathbf{x}(t) = [x^1(t), \ldots, x^n(t)]^T$ and $\hat{\mathbf{x}}(t) = [\hat{x}^1(t), \ldots, \hat{x}^n(t)]^T$ are the $n-$dimensional state vectors of the transmitter and the receiver systems, respectively. $\dot{\mathbf{x}}(t)$ and $\dot{\hat{\mathbf{x}}}(t)$ are the derivatives of $\mathbf{x}(t)$ and $\hat{\mathbf{x}}(t)$ with respect to time, t, respectively. In the above equation, $\mathbf{f} = [f_1(.), \ldots, f_n(.)]^T$ is a smooth nonlinear vector$-$valued function. These two systems are said to be synchronized if

$$\lim_{t\to\infty} ||\mathbf{x}(t) - \hat{\mathbf{x}}(t)|| = 0. \tag{2.2}$$

From the transmitter only few (typically one) state variables are transmitted. These signals are generally corrupted by the channel noise, $\mathbf{v}(t)$. The received signal is given by

$$\mathbf{y}(t) = \mathbf{h}(\mathbf{x}(t)) + \mathbf{v}(t), \tag{2.3}$$

where $\mathbf{h}(.) = [h_1(.), \ldots, h_m(.)]^T$ is a $m-$dimensional linear/nonlinear output function.

Similarly, an iterated chaotic map (discrete time chaotic system) based transmitter

system can be modeled as

$$\mathbf{x}_{k+1} = \mathbf{f}(\mathbf{x}_k) \tag{2.4a}$$

$$\mathbf{y}_k = \mathbf{h}(\mathbf{x}_k) + \mathbf{v}_k, \tag{2.4b}$$

where the transmitter state at the k^{th} time instant is $\mathbf{x}_k = [x_k^1, \ldots, x_k^n]^T$ and the corresponding output is, $\mathbf{y}_k = [y_k^1, \ldots, y_k^m]^T$.

2.2.1 Coupled Synchronization

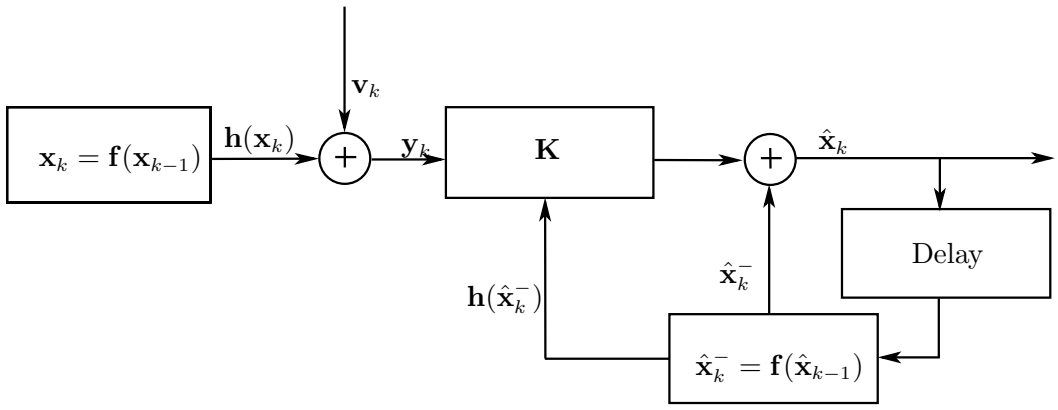


Figure 2.1: Schematic of the coupled synchronization method.

Figure 2.1 shows the schematic of the coupled synchronization method. $\hat{\mathbf{x}}_k^-$ represent the predicted value to which the correction $\mathbf{K}(\mathbf{y}_k - \hat{\mathbf{y}}_k)$ is added. This results in the receiver dynamics

$$\hat{\mathbf{x}}_k = \mathbf{f}(\hat{\mathbf{x}}_{k-1}) + \mathbf{K}(\mathbf{y}_k - \hat{\mathbf{y}}_k), \tag{2.5}$$

where $\hat{\mathbf{y}}_k = \mathbf{h}(\mathbf{f}(\hat{\mathbf{x}}_{k-1}))$. Another way to look at Eq.(2.5) is as a predictor corrector filter. In general, a predictive filter predicts the subsequent states and corrects it with additional information available from the observation. In conventional coupled synchronization, if there is no channel noise $\mathbf{v}_k$, $\mathbf{K}$ is selected such that the global transversal Lyapunov exponents [1] are negative. This enables the receiver to synchronize with the

[1]The Lyapunov exponents of a dynamic system are the quantities that characterize the rate of divergence of the trajectories generated by infinitesimally close initial conditions under the dynamics [2, Chapter 2].

transmitter asymptotically. On the other hand if the channel is noisy, $\mathbf{K}$ is selected such that the local transversal Lyapunov exponents are negative [27]. It is a good idea to employ stochastic techniques for synchronization. Instead of keeping $\mathbf{K}$ constant, if it is determined adaptively, the coupled synchronization will have a similarity with the predictive filtering techniques such as the EKF. In the next section, the basic idea of the stochastic estimation method, from which the EKF is developed, is discussed.

2.3 Stochastic Estimation of States

In stochastic state estimation methods, one would like to estimate the state variable $\mathbf{x}_k$ based on the set of all available (noisy) measurement $\mathbf{y}_{1:k} = \{\mathbf{y}_1, \ldots, \mathbf{y}_k\}$ with certain degree of confidence. This is done by constructing the conditional probability density function (pdf), $p(\mathbf{x}_k|\mathbf{y}_{1:k})$ (i.e. the probability of $\mathbf{x}_k$ given the observations $\mathbf{y}_{1:k}$) known as the posterior probability. It is assumed that $p(\mathbf{x}_0|\mathbf{y}_0)$ is available. In predictor corrector filtering methods, $p(\mathbf{x}_k|\mathbf{y}_{1:k})$ is obtained recursively by a prediction step which is estimated without the knowledge of current measurement, $\mathbf{y}_k$ followed by a correction step where the knowledge of $\mathbf{y}_k$ is used to make the correction to the predicted values.

In the recursive computation of $p(\mathbf{x}_k|\mathbf{y}_{1:k})$, it is assumed that at time $k-1$, $p(\mathbf{x}_{k-1}|\mathbf{y}_{1:k-1})$ is available. Using the Chapman−Kolmogorov equation [70], the prediction is estimated as

$$p(\mathbf{x}_k|\mathbf{y}_{1:k-1}) = \int p(\mathbf{x}_k|\mathbf{x}_{k-1})p(\mathbf{x}_{k-1}|\mathbf{y}_{1:k-1})d\mathbf{x}_{k-1}, \tag{2.6}$$

where the state transition is assumed to be a Markov process of order one and $p(\mathbf{x}_k|\mathbf{x}_{k-1}, \mathbf{y}_{1:k-1}) = p(\mathbf{x}_k|\mathbf{x}_{k-1})$. To make the correction, one needs to make use of the information available in the current observation, $\mathbf{y}_k$. Using Bayes' rule

$$p(\mathbf{x}_k|\mathbf{y}_{1:k}) = \frac{p(\mathbf{x}_k|\mathbf{y}_{1:k-1})p(\mathbf{y}_k|\mathbf{x}_k)}{p(\mathbf{y}_k|\mathbf{y}_{1:k-1})} \tag{2.7}$$

where the normalizing constant

$$p(\mathbf{y}_k|\mathbf{y}_{1:k-1}) = \int p(\mathbf{y}_k|\mathbf{x}_k)p(\mathbf{x}_k|\mathbf{y}_{1:k-1})d\mathbf{x}_k \tag{2.8}$$

Though closed form solutions of the above equations exist for a linear system with Gaussian noise (e.g. Kalman filter [32, Chapter 5]), in general, for a nonlinear system,

they are not available. However, one of the suboptimal filtering methods, the EKF is found to be useful in many nonlinear filtering applications.

2.3.1 Extended Kalman Filter

The Kalman filter is an optimal recursive estimation algorithm for linear systems with Gaussian noise [33]. A distinctive feature of this filter is that its mathematical formulation is described in terms of the state−space concepts. One of the key features of the Kalman filter is its applicability to both stationary and nonstationary environments. The EKF is an extension of the Kalman filtering algorithm to nonlinear systems [32, Chapter 5]. The system is linearized using first order Taylor series approximation. To this approximated system, the Kalman filter is applied to obtain the state estimates. Consider a generic dynamic system governed by

$$\mathbf{x}_k = \mathbf{f}(\mathbf{x}_{k-1}, \mathbf{w}_k) \tag{2.9a}$$

$$\mathbf{y}_k = \mathbf{h}(\mathbf{x}_k, \mathbf{v}_k) \tag{2.9b}$$

where the process noise, $\mathbf{w}_k$, and observation (measurement) noise, $\mathbf{v}_k$, are zero mean Gaussian processes with covariance matrices $\mathbf{Q}_k$ and $\mathbf{R}_k$, respectively. This model becomes the system described in Eq.(2.1), if $\mathbf{w}_k$ is zero and $\mathbf{v}_k$ is additive such that $\mathbf{h}(\mathbf{x}_k, \mathbf{v}_k)$ becomes $\mathbf{h}(\mathbf{x}_k) + \mathbf{v}_k$.

In minimum mean square estimation (MMSE) the receiver computes $\hat{\mathbf{x}}_k$, which is an estimate of $\mathbf{x}_k$, from the available observations $\mathbf{y}_{1:k} = [\mathbf{y}_1, \ldots, \mathbf{y}_k]$ such that the mean square error (MSE), $\mathbb{E}\left[\mathbf{e}_k^T \mathbf{e}_k\right]$ (where $\mathbf{e}_k = \mathbf{x}_k - \hat{\mathbf{x}}_k$), is minimized. The EKF algorithm for the state estimation is given by [32, Chapter 5]

$$\hat{\mathbf{x}}_{k|k-1} = \mathbf{f}(\hat{\mathbf{x}}_{k-1}, 0), \tag{2.10a}$$

$$\mathbf{P}_{k|k-1} = \mathbf{F}_{k-1}\mathbf{P}_{k-1}\mathbf{F}_{k-1}^T + \mathbf{W}_k\mathbf{Q}_k\mathbf{W}_k^T. \tag{2.10b}$$

In the above equations, the notation $k|k-1$ denotes an operation performed at time instant, k, using the information available till $k-1$. At k, $\hat{\mathbf{x}}_{k|k-1}$ is the *a priori* estimate of the state vector $\mathbf{x}_k$, $\mathbf{P}_{k|k-1}$ is the *a priori* error covariance matrix, $\mathbf{F}_{k-1}$ is the Jacobian of $\mathbf{f}(.)$ with respect to the state vector $\mathbf{x}_{k-1}$ and $\mathbf{W}_k$ is the Jacobian of $\mathbf{f}(.)$ with respect

to the noise vector $\mathbf{w}_k$. The EKF update equations are:

$$\mathbf{K}_k = \mathbf{P}_{k|k-1}\mathbf{H}_k^T \left\{\mathbf{H}_k\mathbf{P}_{k|k-1}\mathbf{H}_k^T + \mathbf{V}_k\mathbf{R}_k\mathbf{V}_k^T\right\}^{-1} \tag{2.11a}$$

$$\hat{\mathbf{x}}_k = \hat{\mathbf{x}}_{k|k-1} + \mathbf{K}_k\big(\mathbf{y}_k - \hat{\mathbf{y}}_k\big) \tag{2.11b}$$

$$\mathbf{P}_k = (\mathbf{I} - \mathbf{K}_k\mathbf{H}_k)\mathbf{P}_{k|k-1} \tag{2.11c}$$

where $\mathbf{K}_k$ is the Kalman gain, $\mathbf{H}_k$ is the Jacobian of $\mathbf{h}(.)$ with respect to $\hat{\mathbf{x}}_{k|k-1}$, $\hat{\mathbf{x}}_k$ is the *a posteriori* estimate of the state vector, $\mathbf{V}_k$ is the Jacobian of $\mathbf{h}(.)$ with respect to the noise vector $\mathbf{v}_k$, and $\mathbf{P}_k$ is the *a posterior* error covariance matrix. When EKF is used for synchronization of chaotic maps, $\mathbf{K}_k$ acts as the coupling strength which is updated iteratively (Figure 2.2).

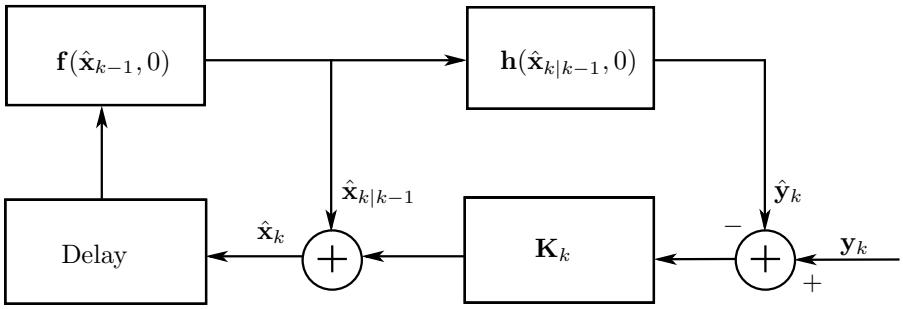


Figure 2.2: Schematic of extended Kalman filter

Convergence Analysis of EKF

Convergence analysis of $\mathbf{K}_k$ can be carried out by studying the convergence of $\mathbf{P}_{k|k-1}$. At any time instant k, according to the *matrix fraction propagation* of $\mathbf{P}_{k|k-1}$, it can be shown that [32, Chapter 4]

$$\mathbf{P}_{k|k-1} = \mathbf{A}_k\mathbf{B}_k^{-1}, \tag{2.12}$$

where $\mathbf{A}_k$ and $\mathbf{B}_k^{-1}$ are factors of $\mathbf{P}_{k|k-1}$. If $\mathbf{F}_k$ is nonsingular (i.e. the map is invertible), $\mathbf{A}_{k+1}$ and $\mathbf{B}_{k+1}$ are given by the recursive equation as

$$\begin{bmatrix} \mathbf{A}_{k+1} \\ \mathbf{B}_{k+1} \end{bmatrix} = \begin{bmatrix} \mathbf{F}_k + \mathbf{W}_k\mathbf{F}_k^{-T}\mathbf{H}_k^T\mathbf{R}_k^{-1}\mathbf{H}_k & \mathbf{W}_k\mathbf{F}_k^{-T} \\ \mathbf{F}_k^{-T}\mathbf{H}_k^T\mathbf{R}_k^{-1}\mathbf{H}_k & \mathbf{F}_k^{-T} \end{bmatrix} \begin{bmatrix} \mathbf{A}_k \\ \mathbf{B}_k \end{bmatrix}. \tag{2.13}$$

From the above expression, it can be shown that, when there is no process noise (i.e. $\mathbf{W}_k = \mathbf{0}$) and $\mathbf{F}_k$ is *contractive* (i.e. the magnitudes of its eigenvalues are less than one), $\mathbf{P}_{k|k-1}$ will converge in time. However, inside the CA, the behaviour of $\mathbf{P}_{k|k-1}$ is aperiodic [77]. When the EKF is used for the synchronization of NCAs with fractal basin boundaries (for example the IM), these properties play a key role in deciding the dynamics of the receiver system.

2.4 Terminology

2.4.1 Source, Sink and Saddle Fixed Points [2, Chapter 2]

There are different types of behaviors in dynamics. Among them, the most basic ones are fixed points. As the name implies, the fixed points do not change under dynamics. There are basically three types of fixed points namely, stable fixed points, unstable fixed points and saddle points. A fixed point is a *sink* (also known as stable fixed point) if the points near it are moved even closer to the fixed point under the dynamis. On the other hand, with *source* fixed point (also known as unstable), nearby points repel from the *source* under the dynamics. A third behaviour is called the *saddle*. Here, some nearby points will be attracted while others are repelled from the fixed point under each iterations.

2.4.2 Stable and Unstable Manifolds [2, Chapter 2] and Homoclinic Tangencies [43]

In simple terms, the set of points that converges to a saddle point is called a stable manifold while the set of points that diverges from it is called an unstable manifold. An n–Dimensional manifold is a set that locally resembles Euclidean space $\mathbb{R}^n$. Homoclinic tangencies (HTs) are points on the attractor where the stable and unstable manifolds of a periodic orbit is tangent to each other. Primary homoclinic tangency (PHT) is a HT where the perturbations are amplified both in forward and reverse iterations. In Figure 2.3, stable and unstable manifolds and corresponding HTs of a saddle point $\mathbf{p}$ are shown. Non hyperbolic chaotic systems/maps are systems with HTs. A hyperbolic CA is an attractor with all the points are hyperbolic (i.e. the map has no eigenvalues with

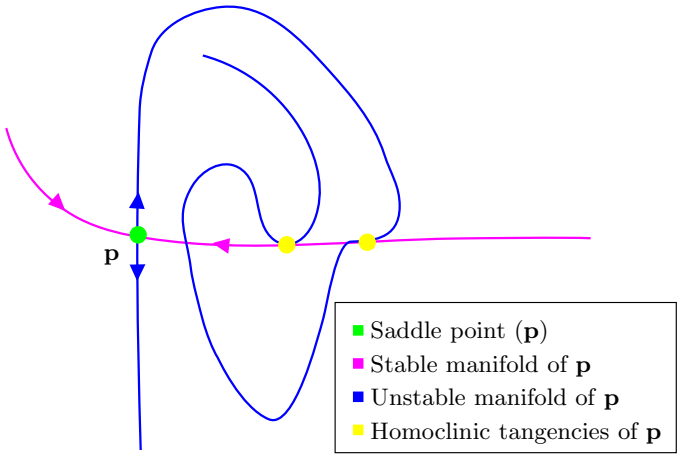


Figure 2.3: Stable and unstable manifolds and HT of a fixed point

absolute value one at any point in the CA) whereas NCA is a chaotic attractor with HTs.

2.5 Noise Induced Escape from Non−Hyperbolic Chaotic Systems/Maps

Noise−induced escape from a CA to another co−existing CA or a stable fixed point is observed in many NCAs [43][71]-[73]. In such systems, small perturbations get amplified near the PHTs and it may eventually take the system states from a CA to another CA or to a fixed point. The most probable exit path and the mean exit time of such chaotic systems give a measure of the system's stability to weak noise perturbations.

In our studies, when the EKF algorithm is used to synchronize two IMs, three different types of behaviours are observed. Firstly, when the initial estimate of the receiver states fall in the basin of attraction of the stable fixed point of the IM, the subsequent iterations take the states to the stable fixed point. Secondly, the receiver initially synchronizes with the transmitter and after a few iterations, the receiver states move to the basin of attraction of the stable fixed point. As before, further iterations take the system to the stable fixed point. Thirdly, the receiver synchronizes with the transmitter. However, intermittent bursts of desynchronization are observed. In other words, the attractor

formed by the receiver dynamics is a smeared version of the transmitter attractor.

2.5.1 Primary Homoclinic Tangencies of Ikeda Map

The IM arises from the analysis of the passage of a pumped laser beam around a lossy ring cavity [74]-[76]:

$$z_{k+1} = p + Bz_k exp\left[\sqrt{-1}\left(\phi - \frac{\omega}{1+|z_k|^2}\right)\right], \tag{2.14}$$

where z_k is a complex−valued state variable with $z_k = x_k^R + \sqrt{-1}x_k^I$. Here, x_k^R is $\Re\{z_k\}$ and x_k^I is $\Im\{z_k\}$. $\Re\{.\}$ and $\Im\{.\}$ give the real and imaginary parts of a complex variable, respectively. For the set of parameters $p = 0.92$, $B = 0.9$, $\phi = 0.4$ and $\omega = 6$, this map (shown in Figure 2.4) has a NCA, two unstable fixed points ($P2$ and $P3$) and a stable fixed point ($P1$) [76]. Basins of attractions of CA and $P1$ are also shown in Figure 2.4. The green area is the basin of attraction of the stable fixed point $P1$ whereas the white area is the basin of attraction of CA. The HTs (yellow) and the most probable exit path (red +) are shown in Figure 2.5.

2.6 Discussion

Three different divergence behaviours of the EKF algorithm, when it is used for the synchronization of IMs, are discussed here. Experiments are carried out at a signal–to–noise ratio (SNR) of 40dB. The SNR is defined by

$$\text{SNR} = \frac{\frac{1}{N}\sum_{i=1}^{N} x_i^2}{\sigma^2}, \tag{2.15}$$

where σ^2 is the variance of the noise and N is the total number of samples used for evaluation. For each of the observations, the transmitter (blue) and the receiver (magenta) CAs are plotted.

2.6.1 Case-I: Convergence to a Stable Fixed Point

This type of divergence is shown in Figure 2.6. In this case, the initial estimate of the receiver states fall within the basin of attraction of the stable fixed point $P1$. For the two

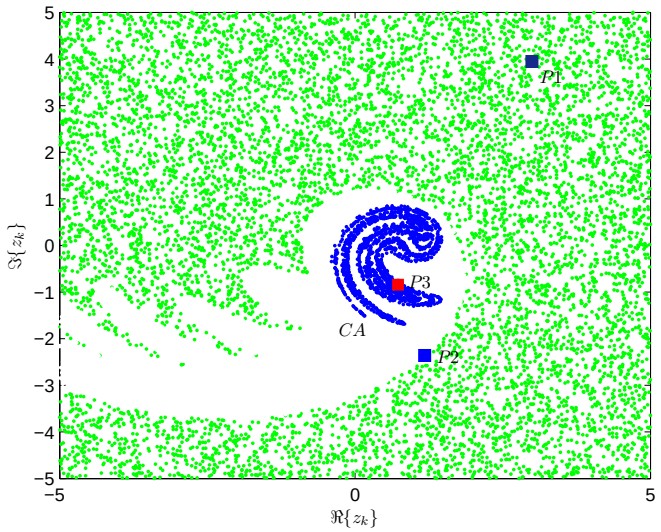


Figure 2.4: The stable fixed point and CA (blue) of the IM. Basin of attraction for CA (white) and $P1$ (green) are also shown.

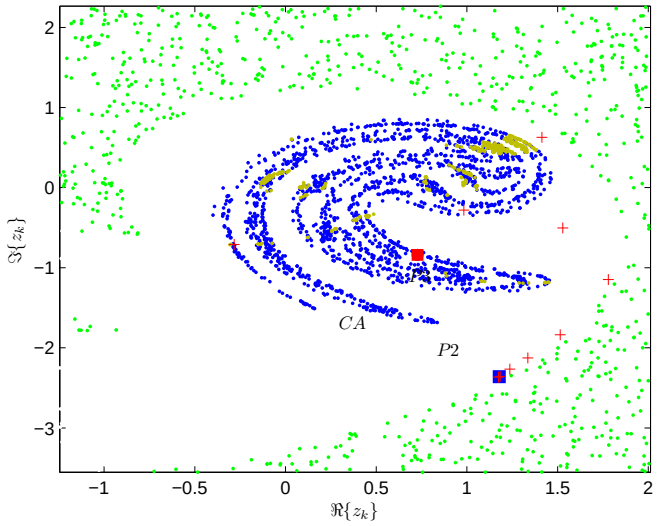


Figure 2.5: PHTs (yellow) and the most probable exit path (red+).

different basins of attractions (of CA and $P1$), the system behaves differently. An initial estimate can be a point in the basin of attraction of $P1$ depending on the choice of $\mathbf{P}_0$ (i.e. the initial *a posterior* error covariance matrix), the transmitter and receiver states and the channel noise. In the simulation studies, it is found that when $\mathbf{P}_0$ is changed, a diverging trajectory may be brought back to the CA. However, there is no specific

pattern observed for the choice of $\mathbf{P}_0$. If the receiver state happens to be in the basin of attraction of $P1$ for a sufficiently long duration of time, $\mathbf{P}_{k|k-1}$ contracts according to Eqs. (2.12) and (2.13) and hence, $\mathbf{K}_k$ converges to zero. This affects the correction added to the current receiver states by the EKF algorithm. If the contraction rate is high as compared to the correction added, the receiver state finds its trajectory along the stable manifold of $P1$ to the fixed point $P1$. If the initial computation of the receiver state leads to a point that lies in the basin of attraction of $P1$, there is a high possibility that the receiver states reach the stable fixed point eventually.

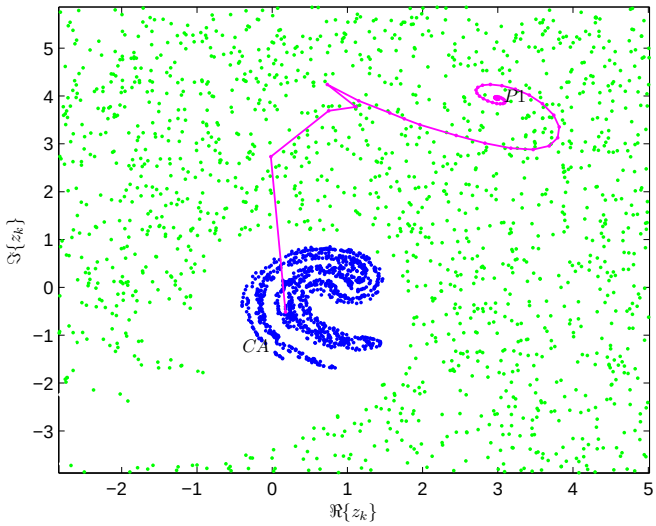


Figure 2.6: Transmitter and receiver CAs (Case-I).

2.6.2 Case-II: Synchronization with Divergence to a Stable Fixed Point

Figure 2.7 shows another type of divergence. Here, the receiver states follow the transmitter states for few iterations in the beginning. After that, the states are taken to the basin of attraction of $P1$. Initial state estimates of the EKF based scheme are very close to the actual transmitter states. At some points, the error between the transmitter and receiver states is amplified such that the receiver states find a path out of the basin of attraction of CA. Since the IM has a NCA, the approximation errors, channel noise and numerical errors can get amplified at the PHTs. If these errors are sufficiently high and if $\mathbf{K}_k$ is relatively small, the EKF will not get enough time to push the system back to

the CA. In hyperbolic attractors, as a result of the Shadowing Lemma [43], small perturbations do not cause the system to leave the attractor. Once the system states reach the basin of attraction of $P1$, $\mathbf{P}_{k|k-1}$ begins to contract. Hence, the state updates get less importance and the system states follow the stable manifold of $P1$. In this case, it is less likely that the receiver states will return to the CA. As discussed in [77], because of the ergodic nature of the CA, $\mathbf{P}_{k|k-1}$ and hence $\mathbf{K}_k$ vary aperiodically. When the receiver states are in the CA, the state updates act as weak perturbations that cause the divergence as shown in Figure 2.7.

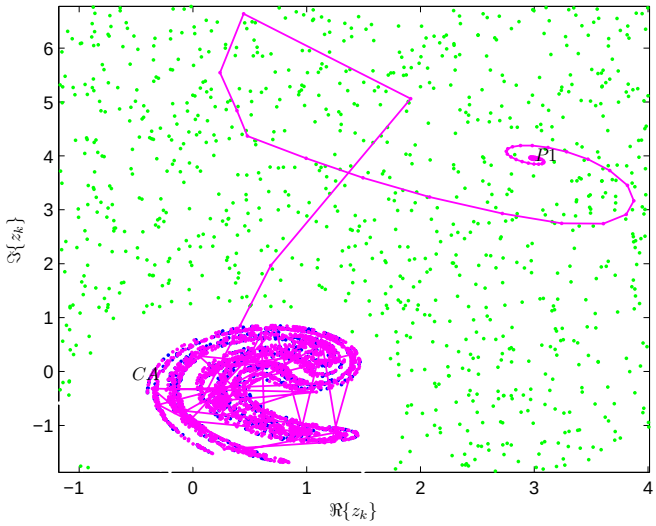


Figure 2.7: Transmitter and receiver CAs (Case-II).

2.6.3 Case-III: Synchronization with Intermittent Burst of Desynchronization

A third situation (Figure 2.8) is where the receiver states follow the transmitter states for most of the iterations. Since the receiver states are in the CA, $\mathbf{P}_{k|k-1}$ and hence $\mathbf{K}_k$ vary aperiodically. Again, the corrections made to the receiver states by the EKF can get amplified at the PHTs. However, these perturbations take the system states to points which are outside the CA, yet inside the basin of attractor of the CA. Moreover, some of the transmitter states are not visited by the receiver. Since the receiver states are inside the basin of attraction of the CA, the EKF brings the receiver states back to

the transmitter states. As it can be observed from Figure 2.8, the CA formed by the receiver is a smeared version of the transmitter CA. Many points are seen to be scattered around the transmitter CA.

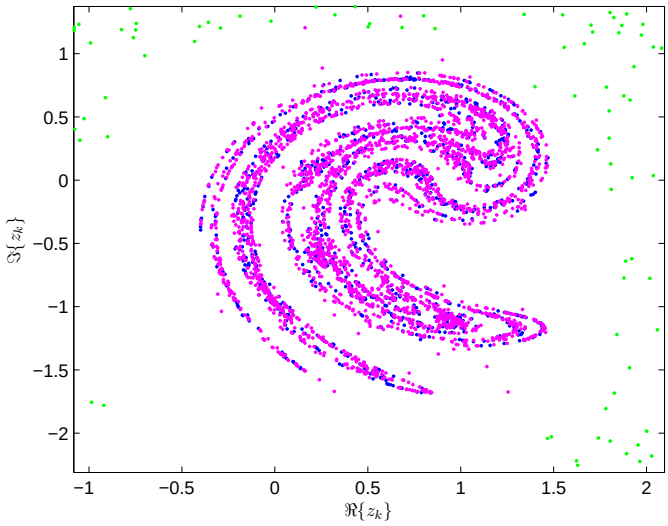


Figure 2.8: Transmitter and receiver CAs (Case-III).

To study the speed of synchronization, the normalized instantaneous square error (NISE(k)), defined by

$$\text{NISE}(k) = \frac{1}{N}\sum_{i=1}^{n}(x_k^i - \hat{x}_k^i)^2 \tag{2.16}$$

is computed and plotted. Here, N is the total number of iterations and x_k^i is the value of i^{th} state variable at the k^{th} time instant. For NISE(k), the index k is dropped (while plotting). The results are plotted on a log−log scale (Figure 2.9) to emphasize the relevant regions of the graph, especially the initial iterations. From Figure 2.9, three distinctive regions can be identified. Initially the NISE is very high. After few iterations, the receiver states start following the transmitter states. This results in very small instantaneous square error values. However, the receiver states are intermittently taken out of the CA and bursts of desynchronization occurs. Accordingly, in the NISE curve, intermitted bursts of increasing NISE values are observed in the third region.

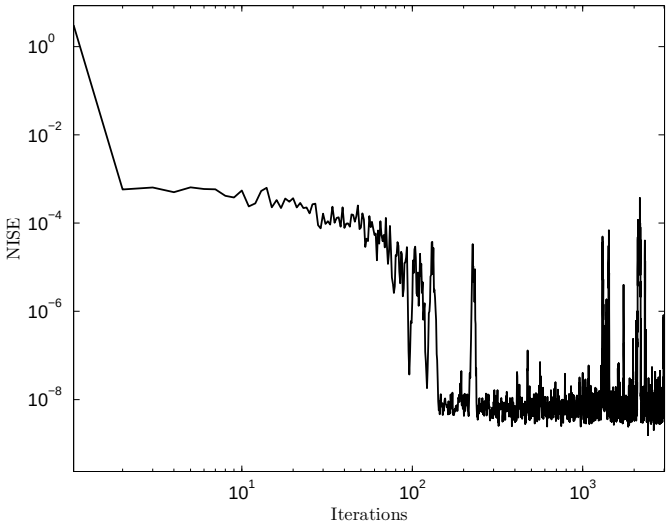


Figure 2.9: NISE performance of EKF based synchronization of IMs.

2.6.4 Behaviour of Local Lyapunov Exponents

Local Lyapunov exponents (LLEs) give us the information about how rapidly the perturbations grow or shrink locally [75]. The variation of LLEs is significant when the value of L is small. Thus, these exponents can be used for the analysis of local behaviour of the chaotic systems/maps. The behaviour of the LLE of the trajectories at the receiver for the three divergence behaviours discussed above are presented in Figure 2.10. As expected, when the states are in the CA, the sum of the LLEs has fluctuating positive and negative values. When the trajectory moves to the basin of attraction of the stable point $P1$, the sum of the LLEs takes on negative values and it finally settles down to a constant (negative) value. When examining Case-I (Figure 2.10 (a)), it is clear that the sum of the LLEs are quickly becoming negative, implying that the receiver states are moving towards the stable fixed point. In Case-II (Figure 2.10 (b)), the receiver states are in the CA for a long period of time and therefore, the LLEs have positive and negative values. However, this behaviour is changed suddenly when the system states move to the fixed point (this happens at about 2800 iterations). In Case-III (Figure 2.10 (c)), on the other hand, the receiver states are not escaping from the basin of attraction of the CA and hence, the behaviour of the LLEs is the same as that of the initial portion of

Case-II. These observations clearly substantiate the claims made in this chapter. Figure 2.11 shows the transmitter and receiver states after synchronization (after 500 iterations). The straight line portion of the figure shows the synchronized regions of the trajectories, whereas the scattered points show the desynchronized portion.

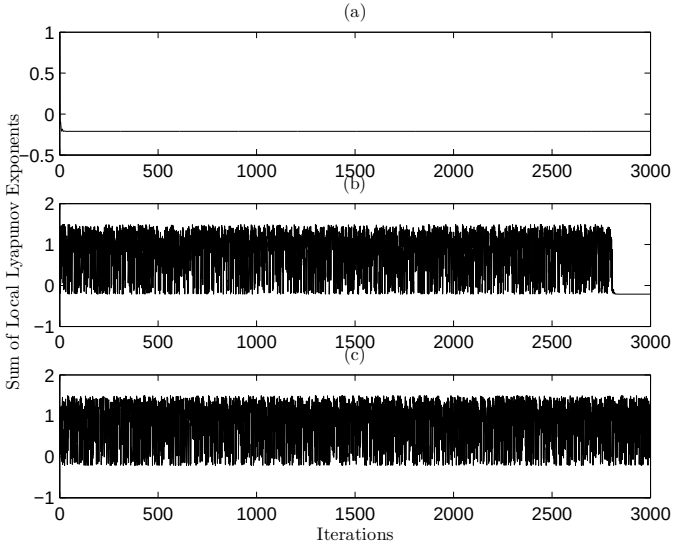


Figure 2.10: Local Lyapunov exponents: (a) Case-I, (b) Case-II and (c) Case-III.

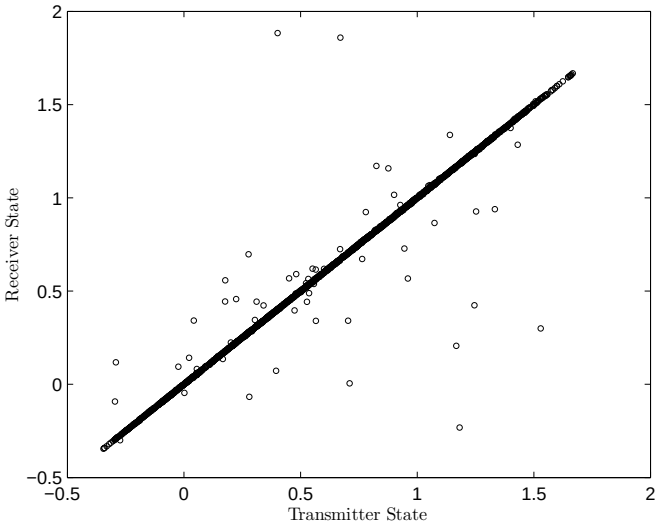


Figure 2.11: Transmitter *vs* receiver states (x^R and $\hat{x}^R$) after synchronization for EKF based scheme.

2.7 Synchronization Characteristics of IM

Two performance indices namely, NMSE and total NMSE (TNMSE) are used to study the noise dependency of synchronization. The NMSE^i between transmitter state (x^i) and receiver state ($\hat{x}^i$) is defined as

$$\text{NMSE}^i = \frac{\sum_{k=1}^{N}(x_k^i - \hat{x}_k^i)^2}{\sum_{k=1}^{N}(x_k^i)^2}, \tag{2.17}$$

where N is the number of iterations and the superscript i represents the index of the state variable (i.e. the i^{th} state variable). The total NMSE (TNMSE) is defined as the sum of all the NMSEs corresponding to individual states

$$\text{TNMSE} = \sum_{i=1}^{n} \text{NMSE}^i. \tag{2.18}$$

To avoid the effect of initial transients, few hundred initial samples are discarded while computing the NMSEs. At each SNR value, the experiment is repeated 50 times and the average of the NMSEs and the TNMSEs are computed. These values are plotted in Figure 2.12 on a semi−log scale.

To study the effect of noise on synchronization, NMSE and TNMSEs are plotted against the SNR. SNR is changed from 35 to 60dB. This is because, for SNRs below 35dB, most of the trajectories are found to be diverging. At higher SNRs, although there are diverging trajectories, they are relatively low. Hence, to avoid misleading results, trajectories which are diverging are excluded from the computation of NMSE and TNMSE. The NMSE and TNMSE values are given in Figures 2.12 and 2.13, respectively. It can be seen that both NMSE and TNMSE values are noise dependent.

2.8 Conclusion

In this chapter, synchronization behaviours of IM using EKF are studied in detail. For the EKF based synchronization, many of the receiver trajectories diverge at all SNRs. This is explained with the fractal basin boundaries of IM where an NCA coexist with

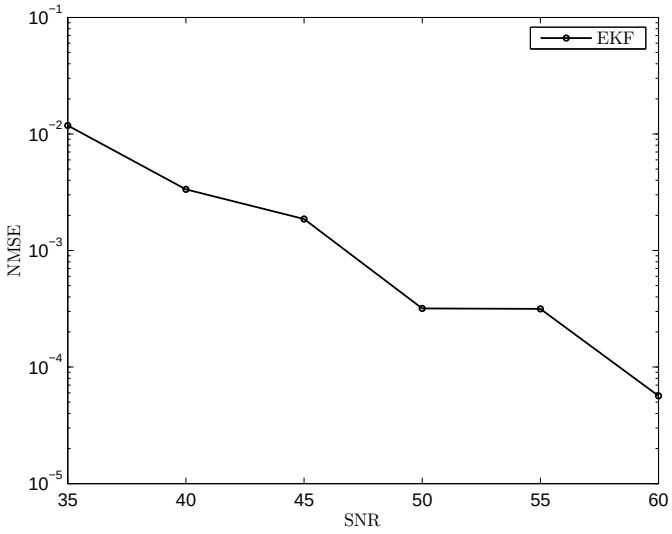


Figure 2.12: NMSE performance of EKF based scheme.

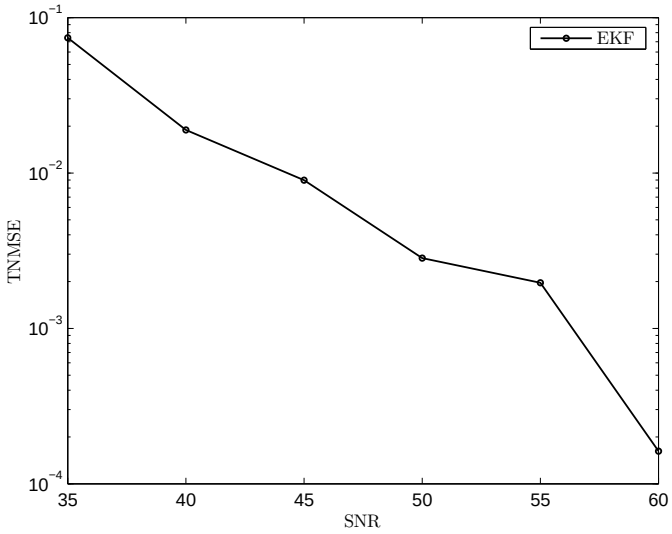


Figure 2.13: TNMSE performance of EKF based scheme.

a stable fixed point. In addition, the EKF algorithm behaves differently in different basins of attractions (basin of attractor of NCA and stable fixed point). As a result of the converging nature of Kalman gain in the basin of attraction of the stable fixed point and the presence of approximation errors and channel noise, it is observed that the EKF based scheme is incapable of guaranteeing stable synchronization. At low SNRs the number of diverging trajectories are large. At high SNRs, on the other hand, this

number is significantly reduced and even in no noise case (infinite SNR), few diverging trajectories are observed.

The synchronizing properties of the EKF based scheme are analyzed using the performance indices such as the NISE, NMSE and TNMSE. The NISE converges after few tens of iterations implying the receiver trajectory close to the transmitter trajectory. However, desynchronizing bursts are observed even after trajectories are synchronized. NMSE and TNMSE of the EKF are found to be noise dependent: with an increase in SNR, these performance indices are found to be decreasing.

Chapter 3

Unscented Kalman Filter and Particle Filter for Chaotic Synchronization

3.1 Introduction

From Chapter 2, it is found that the EKF exhibits divergence behaviour when it is applied for the synchronization of chaotic maps with NCAs. The approximation error introduced by the EKF together with the expansions of this error at the HTs makes the system unstable and diverging trajectories are generated at the receiver. One way to mitigate this problem is to use nonlinear filters with better approximation capabilities. Unscented Kalman filter (UKF) and particle filter (PF), which result in lower approximation errors, are proposed as alternatives to the extended Kalman filter (EKF). In this chapter, both the filtering algorithms are applied to the synchronization of Lorenz and Mackey−Glass (MG) systems and Ikeda map (IM) and the performance is analyzed numerically. One can expect a better synchronization performance in terms of divergence behaviour and synchronization errors (compared to that of the EKF based scheme). In order to gauge the performance, normalized mean square error (NMSE), total normalized mean square error (TNMSE), and normalized instantaneous square error (NISE) are used as performance indices.

This chapter is organized as follows. In Section 3.2, the UKF algorithm is presented in detail. Details of the PF algorithm is provided in Section 3.3. Results of the simulation

studies are detailed in Section 3.4 followed by some concluding remarks in Section 3.5.

3.2 The Unscented Kalman Filter

The UKF algorithm was first introduced by Julier and Uhlmann in 1997 [39]-[41]. It is essentially an approximation method to solve Eq.(2.7). UKF works based on the principle of unscented transform (UT)[42].

3.2.1 Unscented Transform

In Figure 3.1, the UT of a random variable, $\mathbf{u}$, which undergoes a nonlinear transformation ($\mathbf{f}(\mathbf{u})$) to result in another random variable, $\mathbf{v}$ is shown. To calculate the statistics of $\mathbf{v}$, the ideal solution is to get posterior density, $p(\mathbf{v})$, analytically from the prior density $p(\mathbf{u})$. The mean and covariance of $\mathbf{v}$ can also be computed analytically. However, this is highly impractical in most of the situations because of the nonlinearity. UT is a method for approximating the statistics of a random variable which undergoes a nonlinear transformation. It uses carefully selected vectors ($\mathcal{U}_i$), known as *sigma points*, to approximate the statistics of the posterior density. Each sigma point is associated with a weight W_i. The number of sigma points is $2n+1$ where n is the dimension of the state vector. With the knowledge of the mean ($\hat{\mathbf{u}}$) and covariance ($\mathbf{P_u}$) of the prior density, these sigma points are constructed as

$$(\mathcal{U}_0, W_0) = \left(\hat{\mathbf{u}}, \frac{\kappa}{n+\kappa}\right); \qquad i = 0 \tag{3.1a}$$

$$(\mathcal{U}_i, W_i) = \left(\hat{\mathbf{u}} + \left(\sqrt{(n+\kappa)\mathbf{P_u}}\right)_i, \frac{1}{2(n+\kappa)}\right); \quad i = 1, \ldots, n \tag{3.1b}$$

$$(\mathcal{U}_i, W_i) = \left(\hat{\mathbf{u}} - \left(\sqrt{(n+\kappa)\mathbf{P_u}}\right)_i, \frac{1}{2(n+\kappa)}\right); \quad i = n+1, \ldots, 2n \tag{3.1c}$$

where κ is a scaling parameter and $\left(\sqrt{(n+\kappa)\mathbf{P_u}}\right)_i$ is the i^{th} row or column of the square root of the matrix, $(n+\kappa)\mathbf{P_u}$. These sigma points are propagated through the nonlinearity $\mathbf{f}(.)$ to obtain

$$\mathcal{V}_i = \mathbf{f}(\mathcal{U}_i) \quad \text{for } i = 0, 1, \ldots, 2n. \tag{3.2}$$

Using the set of $\mathcal{V}_i$, the mean ($\hat{\mathbf{v}}$) and covariance ($\mathbf{P_v}$) of the posterior density is estimated as

$$\hat{\mathbf{v}} = \sum_{i=0}^{2n} W_i \mathcal{V}_i \tag{3.3a}$$

$$\mathbf{P_v} = \sum_{i=0}^{2n} W_i \left(\mathcal{V}_i - \hat{\mathbf{v}}\right)\left(\mathcal{V}_i - \hat{\mathbf{v}}\right)^T . \tag{3.3b}$$

It is shown that the UKF based approximation is equivalent to a third order Taylor series approximation if the Gaussian prior is assumed [40]. Another advantage of UT is that it does not require the calculation of the Jacobian or Hessian.

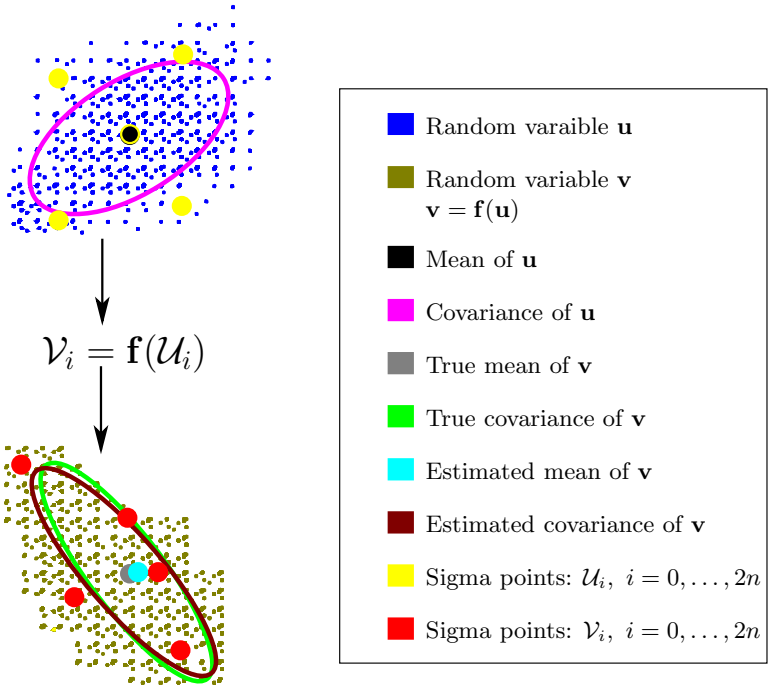


Figure 3.1: Unscented transform.

3.2.2 Scaled UT

The SUT (SUT) is a generalization of the UT. It is a method that scales an arbitrary set of sigma points but yet capture the mean and covariance correctly. The new transform is given by

$$\mathcal{U}_i^{'} = \mathcal{U}_0 + \alpha\left(\mathcal{U}_i - \mathcal{U}_0\right) \quad \text{for} \quad i = 0, \ldots, 2n \tag{3.4}$$

where α is a positive scaling parameter. By this the distribution of the sigma points can be controlled without affecting the positive definitive nature of the matrix, $(n+\kappa)\mathbf{P_u}$. A set of sigma points, $\{\mathbf{U} = [\mathcal{U}_0, \ldots, \mathcal{U}_{2n}], \mathbf{W} = [W_0, \ldots, W_{2n}]\}$, is first calculated using Eq.(3.1) and then transformed into scaled sigma points, $\left\{\mathbf{U}' = \left[\mathcal{U}_0', \ldots, \mathcal{U}_{2n}'\right], \mathbf{W}' = \left[W_0', \ldots, W_{2n}'\right]\right\}$, by

$$\mathcal{U}_i' = \mathcal{U}_0 + \alpha\left(\mathcal{U}_i - \mathcal{U}_0\right) \quad \text{for} \quad i = 0, 1, \ldots, 2n \tag{3.5a}$$

$$W_i' = \begin{cases} \frac{W_0}{\alpha^2} + \left(1 - \frac{1}{\alpha^2}\right) & i = 0 \\ \frac{W_i}{\alpha^2} & i \neq 0 \end{cases}. \tag{3.5b}$$

The sigma point selection and scaling can be combined to a single step by setting [41]

$$\lambda = \alpha^2(n+\kappa) - n \tag{3.6}$$

and setting

$$\mathcal{U}_0' = \hat{\mathbf{u}}$$

$$\mathcal{U}_i' = \hat{\mathbf{u}} + \left(\sqrt{(n+\lambda)\mathbf{P_u}}\right)_i \quad i = 1, \ldots, n \tag{3.7a}$$

$$\mathcal{U}_i' = \hat{\mathbf{u}} - \left(\sqrt{(n+\lambda)\mathbf{P_u}}\right)_i \quad i = n+1, \ldots, 2n \tag{3.7b}$$

$$W_0^{(m)} = \frac{\lambda}{n+\lambda} \tag{3.7c}$$

$$W_0^{(c)} = \frac{\lambda}{(n+\lambda)} + (1 - \alpha^2 + \beta) \tag{3.7d}$$

$$W_i^{(m)} = W_i^{(c)} = \frac{1}{2(\lambda+n)} \quad \text{for} \quad i = 1, 2, \ldots, 2n. \tag{3.7e}$$

Parameter β is another control parameter which affects the weighting of the zeroth sigma point for the calculation of the covariance. Using SUT, the mean and the covariance can be estimated as

$$\hat{\mathbf{v}} = \sum_{i=0}^{2n} W_i^{(m)} \mathcal{V}_i' \tag{3.8a}$$

$$\mathbf{P_v} = \sum_{i=0}^{2n} W_i^{(c)} \left(\mathcal{V}_i' - \hat{\mathbf{v}}\right)\left(\mathcal{V}_i' - \hat{\mathbf{v}}\right)^T \tag{3.8b}$$

where $\mathcal{V}_i' = \mathbf{f}(\mathcal{U}_i')$.

Guidelines on Selecting α, β and κ [41]

Selection of κ should be such that it should result in positive semidefiniteness of the covariance matrix. Choosing $\kappa \geq 0$ guarantees this and a good choice is $\kappa = 0$. Choose $0 \leq \alpha \leq 1$ and $\beta \geq 0$. For Gaussian prior density, $\beta = 2$ is an optimal choice. Since α controls the spread of the sigma points, it is selected such that it should not capture the non−local effects when nonlinearities are strong.

3.2.3 Unscented Kalman Filter

UKF is an application of the SUT. It implements the minimum mean square estimates as follows. The objective is to estimate the states $\mathbf{x}_k$, given the observations, $\mathbf{y}_{1:k}$. For this the state random variable is redefined as the concatenation of the original state and noise variables (i.e. $\mathbf{x}_k^a = \begin{bmatrix}\mathbf{x}_k^T & \mathbf{w}_k^T & \mathbf{v}_k^T\end{bmatrix}^T$ with dimension n_a). The steps involved in UKF are listed below.

Algorithm 1: Unscented Kalman Filter

- Initialization

$$\begin{aligned}
\hat{\mathbf{x}}_0 &= \mathbb{E}[\mathbf{x}_0] \\
\mathbf{P}_0 &= \mathbb{E}[(\mathbf{x}_0 - \hat{\mathbf{x}}_0)(\mathbf{x}_0 - \hat{\mathbf{x}}_0)^T] \\
\hat{\mathbf{x}}_0^a &= \begin{bmatrix}\hat{\mathbf{x}}_0^T & \mathbf{0} & \mathbf{0}\end{bmatrix}^T \\
\mathbf{P}_0^a &= \begin{bmatrix} \mathbf{P}_0 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{Q} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{R} \end{bmatrix}
\end{aligned}$$

- For $k = 1, 2, \ldots$
  - Calculate the sigma points:

$$\mathcal{X}_{k-1}^a = \begin{bmatrix}\hat{\mathbf{x}}_{k-1}^a & \hat{\mathbf{x}}_{k-1}^a \pm \sqrt{(n_a + \lambda)\mathbf{P}_{k-1}^a}\end{bmatrix}$$

– Time update:

$$\begin{aligned}
\mathcal{X}_{k|k-1} &= \mathbf{f}\left(\mathcal{X}^x_{k-1}, \mathcal{X}^w_{k-1}\right) \\
\hat{\mathbf{x}}_{k|k-1} &= \sum_{i=0}^{2n_a} W_i^{(m)} \mathcal{X}^x_{i,k|k-1} \\
\mathbf{P}_{k|k-1} &= \sum_{i=0}^{2n_a} W_i^{(c)} \left[\mathcal{X}^x_{i,k|k-1} - \hat{\mathbf{x}}_{k|k-1}\right] \left[\mathcal{X}^x_{i,k|k-1} - \hat{\mathbf{x}}_{k|k-1}\right]^T \\
\mathcal{Y}_{k|k-1} &= \mathbf{h}\left(\mathcal{X}^x_{k|k-1}, \mathcal{X}^v_{k|k-1}\right) \\
\hat{\mathbf{y}}_{k|k-1} &= \sum_{i=0}^{2n_a} W_i^{(m)} \mathcal{Y}_{i,k|k-1}
\end{aligned}$$

– Measurement update:

$$\begin{aligned}
\mathbf{P}_{\hat{\mathbf{y}}_k\hat{\mathbf{y}}_k} &= \sum_{i=0}^{2n_a} W_i^{(c)} \left[\mathcal{Y}_{i,k|k-1} - \hat{\mathbf{y}}_{k|k-1}\right] \left[\mathcal{Y}_{i,k|k-1} - \hat{\mathbf{y}}_{k|k-1}\right]^T \\
\mathbf{P}_{\hat{\mathbf{x}}_k\hat{\mathbf{y}}_k} &= \sum_{i=0}^{2n_a} W_i^{(c)} \left[\mathcal{X}_{i,k|k-1} - \hat{\mathbf{x}}_{k|k-1}\right] \left[\mathcal{Y}_{i,k|k-1} - \hat{\mathbf{y}}_{k|k-1}\right]^T \\
\mathbf{K}_k &= \mathbf{P}_{\hat{\mathbf{x}}_k\hat{\mathbf{y}}_k} \mathbf{P}^{-1}_{\hat{\mathbf{y}}_k\hat{\mathbf{y}}_k} \\
\hat{\mathbf{x}}_k &= \hat{\mathbf{x}}_{k|k-1} + \mathbf{K}_k\left(\mathbf{y}_k - \hat{\mathbf{y}}_{k|k-1}\right) \\
\mathbf{P}_k &= \mathbf{P}_{k|k-1} - \mathbf{K}_k \mathbf{P}_{\hat{\mathbf{y}}_k\hat{\mathbf{y}}_k} \mathbf{K}_k^T.
\end{aligned}$$

†††

It is shown in [40] that the approximation introduced by the UKF has more number of Taylor series terms. The effect of the approximation errors is different for different nonlinear systems. In some cases, if the nonlinearity is quadratic, approximation error will not have any strong influence. However, as discussed in Chapter 2, when they are chaotic maps with NCAs, it leads to the divergence of trajectories.

3.3 Particle Filters

Particle filters are sequential Monte−Carlo (MC) methods for nonlinear analysis. It is a method to implement recursive Bayesian filter by MC simulations. This class of filters can deal with any probability distributions and allows complete representation of the posterior probability distribution of the states [49][78]. Hence, any statistical

estimates such as mean, modes, kurtosis and covariance can be estimated numerically. The key idea is to represent the required posterior density function by a set of random samples with associated weights. As the number of samples become very large, this MC characterization become close to the actual density [78].

3.3.1 Perfect Monte−Carlo Simulation

In MC simulation, the integral is mapped to a discrete sum by a set of weighted samples. More precisely, the posterior density is approximated as

$$\hat{p}(\mathbf{x}_{0:k}|\mathbf{y}_{1:k}) = \frac{1}{N}\sum_{i=1}^{N}\delta(\mathbf{x}_{0:k} - \mathbf{x}_{0:k}^{i}) \tag{3.9}$$

where N is the number of particles, $\delta(.)$ is the Dirac delta function and $\{\mathbf{x}_{0:k}^{i}, i = 1,\ldots,N\}$ are the samples drawn from the posterior distribution. Hence any expectation of the form

$$I(f_k) \quad = \quad \int f_k(\mathbf{x}_{0:k})p(\mathbf{x}_{0:k}|\mathbf{y}_{1:k})d(\mathbf{x}_k) \tag{3.10}$$

can be approximated as

$$\hat{I}(f_k) = \sum_{i=1}^{N} f_k(\mathbf{x}_{0:k}^{i}) \tag{3.11}$$

The law of large numbers guarantees that $\hat{I}(f_k) \rightarrow I(f_k)$ when N is sufficiently large. One key requirement here is the need for sampling from the posterior density. However, in most cases, this density may not be directly computable. Then one needs to resort to importance sampling [78].

3.3.2 Importance Sampling

In PF, the key idea is to use the principle of importance sampling. In other words, sample particles from a known distribution called the proposal distribution. It is achieved by choosing an importance function, $\pi(\mathbf{x}_{0:k}|\mathbf{y}_{1:k})$, from which samples can be easily drawn.

Let the expectation of a function f_k be given as

$$\begin{aligned} I(f_k) &= \int f_k(\mathbf{x}_{0:k}) \frac{p(\mathbf{x}_{0:k}|\mathbf{y}_{1:k})}{\pi(\mathbf{x}_{0:k}|\mathbf{y}_{1:k})} \pi(\mathbf{x}_{0:k}|\mathbf{y}_{1:k}) d(\mathbf{x}_{0:k}) \\ &= \int f_k(\mathbf{x}_{0:k}) \frac{p(\mathbf{y}_{1:k}|\mathbf{x}_{0:k}) p(\mathbf{x}_{0:k})}{p(\mathbf{y}_{1:k}) \pi(\mathbf{x}_{0:k}|\mathbf{y}_{1:k})} \pi(\mathbf{x}_{0:k}|\mathbf{y}_{1:k}) d(\mathbf{x}_{0:k}) \\ &= \int f_k(\mathbf{x}_{0:k}) \frac{w_k(\mathbf{x}_{0:k})}{p(\mathbf{y}_{1:k})} \pi(\mathbf{x}_{0:k}|\mathbf{y}_{1:k}) d(\mathbf{x}_{0:k}). \end{aligned} \tag{3.12}$$

where

$$w_k(\mathbf{x}_{0:k}) = \frac{p(\mathbf{y}_{1:k}|\mathbf{x}_{0:k}) p(\mathbf{x}_{0:k})}{\pi(\mathbf{x}_{0:k}|\mathbf{y}_{1:k})}. \tag{3.13}$$

By drawing N samples from $\pi(\mathbf{x}_{0:k}|\mathbf{y}_{1:k})$, Eq.(3.12) can be approximated as

$$\begin{aligned} \hat{I}(f_k) &= \frac{\frac{1}{N} \sum_{i=1}^{n} f_k(\mathbf{x}^i_{0:k}) w_k(\mathbf{x}^i_{0:k})}{\frac{1}{N} \sum_{i=1}^{N} w_k(\mathbf{x}^i_{0:k})} \\ &= \sum_{i=1}^{N} f_k(\mathbf{x}^i_{0:k}) \tilde{w}_k(\mathbf{x}^i_{0:k}), \end{aligned} \tag{3.14}$$

where the unknown normalizing function $p(\mathbf{y}_{1:k})$ is avoided by normalizing the weights as follows [79]

$$\tilde{w}_k(\mathbf{x}^i_{0:k}) = \frac{w_k(\mathbf{x}^i_{0:k})}{\sum_{j=1}^{N} w_j(\mathbf{x}^j_{0:k})}. \tag{3.15}$$

If $\pi(\mathbf{x}_k|\mathbf{x}_{0:k-1}, \mathbf{y}_{0:k}) = \pi(\mathbf{x}_k|\mathbf{x}_{k-1}, \mathbf{y}_k)$, the importance density depends only on $\mathbf{x}_{k-1}$ and $\mathbf{y}_k$. In order to compute a sequential estimate of the posterior distribution at time k, following recursive formula for the proposal distribution can be used

$$\pi(\mathbf{x}_k|\mathbf{y}_k) = \pi(\mathbf{x}_{k-1}|\mathbf{y}_{k-1}) \pi(\mathbf{x}_k|\mathbf{x}_{k-1}, \mathbf{y}_k). \tag{3.16}$$

Hence the computation of $\tilde{w}_k(\mathbf{x}^i_k)$ can be recursively done as

$$\begin{aligned} \tilde{w}_k(\mathbf{x}^i_k) &= \frac{p(\mathbf{y}_k|\mathbf{x}^i_k) p(\mathbf{x}^i_k)}{\pi(\mathbf{x}^i_{k-1}|\mathbf{y}_{k-1}) \pi(\mathbf{x}^i_k|\mathbf{x}^i_{k-1}, \mathbf{y}_k)} \\ &= \tilde{w}_{k-1} \frac{p(\mathbf{y}_k|\mathbf{x}^i_k) p(\mathbf{x}^i_k|\mathbf{x}^i_{k-1})}{\pi(\mathbf{x}^i_k|\mathbf{x}^i_{k-1}, \mathbf{y}_k)}. \end{aligned} \tag{3.17}$$

Above equation [Eq.(3.17)] is the essence of the PF. Using the N samples drawn from $\pi(\mathbf{x}^i_k|\mathbf{x}^i_{k-1}, \mathbf{y}_k)$, the posterior density can be approximated numerically.

Degeneracy of Sequential Importance Sampling

The sequential importance sampling (SIS) has a serious limitation. The variance of all but one importance weights become zero after few iterations. This degeneracy implies that the a large computational effort is devoted to updating particles whose contribution to the approximation of $p(\mathbf{x}_k|\mathbf{y}_{1:k})$ is negligible. To avoid the degeneracy of the SIS algorithm, re−sampling techniques are applied. The measure of degeneracy in PF is done with the effective sample size N_{eff} which is given by

$$N_{eff} = \frac{1}{1 + \mathrm{Var}(\tilde{w}_k(\mathbf{x}_k^i))}, \tag{3.18}$$

where Var(.) denotes the variance. Re−sampling involves mapping the Dirac random measure $\{\mathbf{x}_k^i, \tilde{w}_k(\mathbf{x}_k^i)\}$ into an equally weighted random measure $\{\mathbf{x}_k^j, \frac{1}{N}\}$. This is done by sampling the particles uniformly from the discrete set $\{\mathbf{x}_k^i, i = 1, \ldots, N\}$ with probabilities $\{\tilde{w}(\mathbf{x}_k^i), i = 1, \ldots, N\}$ [80]. The re−sampling process is shown in Figure 3.2. First, the cumulative density function (cdf) of $\{\mathbf{x}_k^i, \tilde{w}_k(\mathbf{x}_k^i)\}$ is constructed. $p(i)$ is the pdf of a uniform random variable. Sampling index i drawn from $p(i)$ is projected onto the distribution range and then onto the distribution domain. The intersection with the domain constitutes the new sample index, j. In other words $\mathbf{x}_k^j$, is accepted as a new sample. This is performed for N times to get a set of particles $\hat{\mathbf{x}}_k^i$ and corresponding weights, $\frac{1}{N}$. Since index i is selected uniformly, there is a higher probability to select the same j if the weight associated with j^{th} index is large compared to others. The objective of the overall process is to avoid particles with low importance weights and multiply (i.e. make more copies) the particles with higher importance weights.

3.3.3 Choice of Proposal Distribution

Choice of the importance function (proposal distribution) plays a crucial role in the design of PF. The importance function should be selected such that it minimizes the variance of the importance weights [78]. One way to accomplish this is to use UKF to construct the importance function. In this framework, the UKF approximates the optimal minimum mean square estimate (MMSE) estimator of the system state by calculating the conditional mean of the state, given all of the observations. This is done recursively

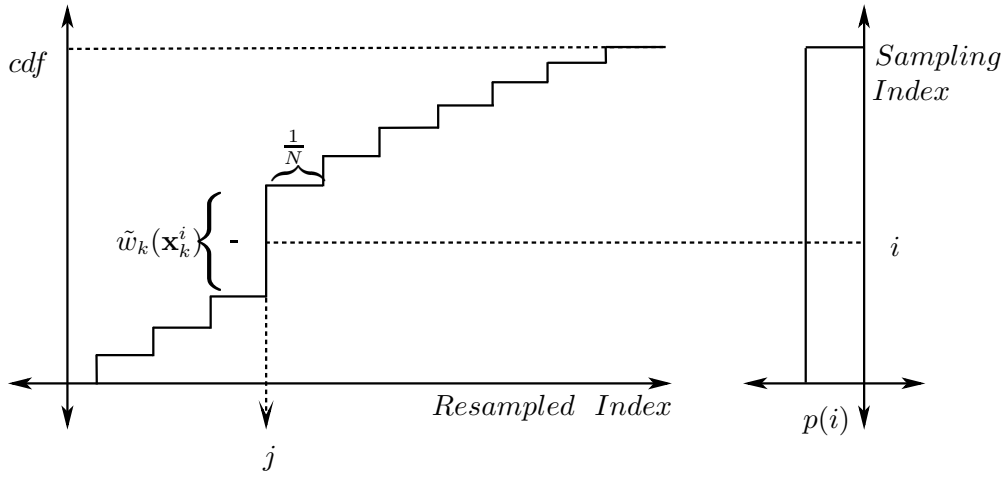


Figure 3.2: Re−sampling process.

by propagating the Gaussian approximation of the posterior distribution through time, combining it at each time step with the new observation. Within the PF framework, a separate UKF is used to generate and propagate a Gaussian proposal distribution for each particle (i.e. $\pi(\mathbf{x}_k^i|\mathbf{x}_{k-1}^i, \mathbf{y}_k) = \mathcal{N}(\bar{\mathbf{x}}_k^i, \bar{\mathbf{P}}_k^i)$. Here, $\mathcal{N}(\mu, \sigma^2)$ represents a normalized Gaussian density with mean μ and variance σ^2. $\bar{\mathbf{x}}_k^i$ and $\bar{\mathbf{P}}_k^i$ are the approximate estimate of the mean and covariance obtained by the intermediate UKF step). The UKF is used here because it has a better approximation capabilities and wider span. This method is called unscented particle filter (UPF) [79]. In this chapter, UPF is used for the synchronization of chaotic systems/maps. Steps involved in UPF are briefed next.

Algorithm 2: Unscented Particle Filter

1. Initialize: $k = 0$

   - For $i = 1, \ldots, N$, draw particles $\mathbf{x}_k^i$ from the prior $p(\mathbf{x}_0)$
   - Set

$$\begin{aligned} \hat{\mathbf{x}}_0^i &= \mathbb{E}[\mathbf{x}_0^i] \\ \mathbf{P}_0^i &= \mathbb{E}\left[\left(\mathbf{x}_0^i - \hat{\mathbf{x}}_0^i\right)\left(\mathbf{x}_0^i - \hat{\mathbf{x}}_0^i\right)^T\right] \\ \hat{\mathbf{x}}_0^{(i,a)} &= \mathbb{E}[\mathbf{x}_0^{(i,a)}] = \left[\hat{\mathbf{x}}_0^i \; \mathbf{0} \; \mathbf{0}\right] \end{aligned}$$

$$\mathbf{P}_0^{(i,a)} = \mathbb{E}\left[\left(\mathbf{x}_0^{(i,a)} - \hat{\mathbf{x}}_0^{(i,a)}\right)\left(\mathbf{x}_0^{(i,a)} - \hat{\mathbf{x}}_0^{(i,a)}\right)^T\right] = \begin{bmatrix} \mathbf{P}_0^i & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{Q} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{R} \end{bmatrix}$$

2. For $k = 1, 2, \ldots$

- Importance sampling step
  - For $i = 1, \ldots, N$:
    - Update the particle filter with the UKF
      - Calculate sigma Points:

$$\mathcal{X}_{k-1}^{(i,a)} = \left[\hat{\mathbf{x}}_{k-1}^{(i,a)} \quad \hat{\mathbf{x}}_{k-1}^{(i,a)} \pm \sqrt{(n_a + \lambda)\mathbf{P}_{k-1}^{(i,a)}}\right]$$

      - Time update:

$$\begin{aligned}
\mathcal{X}_{k|k-1} &= \mathbf{f}\left(\mathcal{X}_{k-1}^{(i,x)}, \mathcal{X}_{k-1}^{(i,w)}\right) \\
\hat{\mathbf{x}}_{k|k-1}^i &= \sum_{j=0}^{2n_a} W_j^{(m)} \mathcal{X}_{j,k|k-1}^{(i,x)} \\
\mathbf{P}_{k|k-1}^i &= \sum_{j=0}^{2n_a} W_j^{(c)} \left[\mathcal{X}_{j,k|k-1}^{(i,x)} - \hat{\mathbf{x}}_{k|k-1}^i\right]\left[\mathcal{X}_{j,k|k-1}^{(i,x)} - \hat{\mathbf{x}}_{k|k-1}^i\right]^T \\
\mathcal{Y}_{k|k-1}^i &= \mathbf{h}\left(\mathcal{X}_{k|k-1}^{(i,x)}, \mathcal{X}_{k|k-1}^{(i,v)}\right) \\
\hat{\mathbf{y}}_{k|k-1}^i &= \sum_{j=0}^{2n_a} W_j^{(m)} \mathcal{Y}_{j,k|k-1}^i
\end{aligned}$$

      - Measurement update:

$$\begin{aligned}
\mathbf{P}_{\hat{\mathbf{y}}_k\hat{\mathbf{y}}_k} &= \sum_{j=0}^{2n_a} W_j^{(c)} \left[\mathcal{Y}_{j,k|k-1}^i - \hat{\mathbf{y}}_{k|k-1}^i\right]\left[\mathcal{Y}_{j,k|k-1}^i - \hat{\mathbf{y}}_{k|k-1}^i\right]^T \\
\mathbf{P}_{\hat{\mathbf{x}}_k\hat{\mathbf{y}}_k} &= \sum_{j=0}^{2n_a} W_j^{(c)} \left[\mathcal{X}_{j,k|k-1}^i - \hat{\mathbf{x}}_{k|k-1}^i\right]\left[\mathcal{Y}_{j,k|k-1}^i - \hat{\mathbf{y}}_{k|k-1}^i\right]^T \\
\mathbf{K}_k &= \mathbf{P}_{\hat{\mathbf{x}}_k\hat{\mathbf{y}}_k}\mathbf{P}_{\hat{\mathbf{y}}_k\hat{\mathbf{y}}_k}^{-1} \\
\bar{\mathbf{x}}_k^i &= \hat{\mathbf{x}}_{k|k-1}^i + \mathbf{K}_k\left(\mathbf{y}_k - \hat{\mathbf{y}}_{k|k-1}^i\right) \\
\bar{\mathbf{P}}_k^i &= \mathbf{P}_{k|k-1}^i - \mathbf{K}_k\mathbf{P}_{\hat{\mathbf{y}}_k\hat{\mathbf{y}}_k}\mathbf{K}_k^T
\end{aligned}$$

    - Sample $\mathbf{x}_k^i$ from the importance density, $\mathcal{N}\left(\bar{\mathbf{x}}_k^i, \mathbf{P}_k^i\right)$
  - Evaluate the importance weights to get $\left\{\mathbf{x}_k^i, w_k^i(\mathbf{x}_k^i)\right\}$

– Normalize the importance weights to get $\left\{\mathbf{x}_k^i, \tilde{w}_k^i(\mathbf{x}_k^i)\right\}$

- Re−sample to get $\left\{\hat{\mathbf{x}}_k^i, \frac{1}{N}\right\}$ (and corresponding set of $\mathbf{P}_k^i$)
- Approximate the density with $\left\{\hat{\mathbf{x}}_k^i, \frac{1}{N}\right\}$

†††

A schematic of the steps involved in PF is given in Figure 3.3. Assume that at time k, there are $N = 12$ particles $(\mathbf{x}_k^i)$ with associated importance weights, N^{-1}. This is the result of the intermediate UKF computations and sampling from $\mathcal{N}(\bar{\mathbf{x}}_k^i, \bar{\mathbf{P}}_k^i)$. Now, for each particle, the importance weights are computed recursively using Eq.(3.17) and these weights are normalized. This results in weighted measure, $\{\mathbf{x}_k^i, \tilde{w}_k(\mathbf{x}_k^i)\}$. In this figure, the size of the circle represents the weight associated with each particle. To avoid the degeneracy, re-sampling is performed so that samples with small values of $\tilde{w}_k(\mathbf{x}_k^i)$ are discarded while samples with large values of $\tilde{w}_k(\mathbf{x}_k^i)$ are multiplied. This forms a new set of particles $\{\hat{\mathbf{x}}_k^i, N^{-1}\}$, which is an approximation of $p(\mathbf{x}_k|\mathbf{y}_{1:k})$. This is iteratively done for each time step, k.

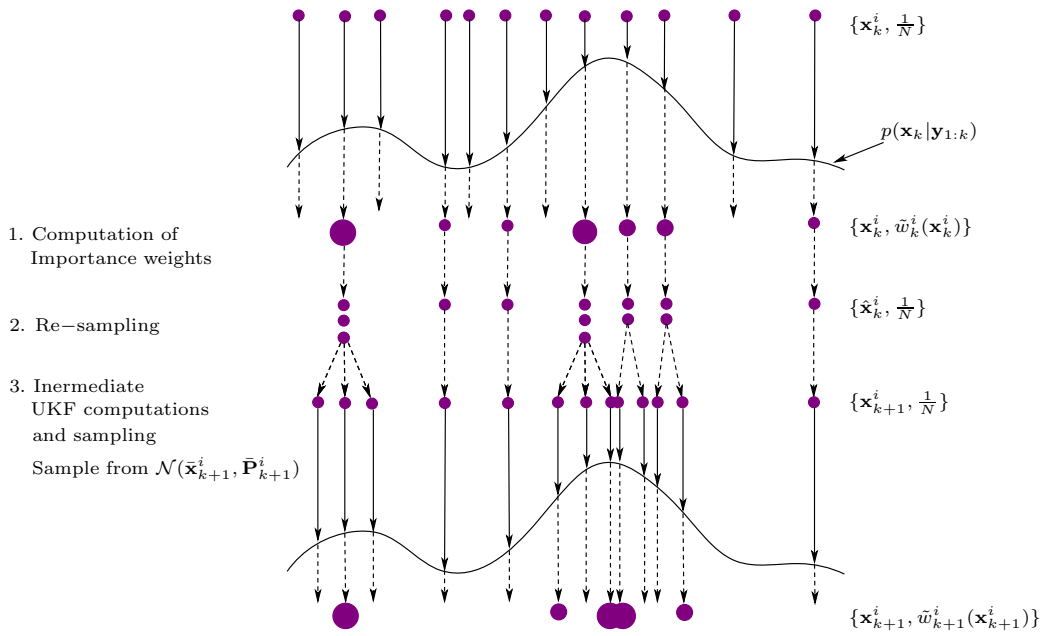


Figure 3.3: Schematic of PF.

3.4 Results and Discussion

To assess the performance of the UKF and PF based synchronization schemes, simulation studies are carried out on three different chaotic systems/maps: (*i*) IM, (*ii*) Lorenz system, and (*iii*) Mackey−Glass (MG) system. These systems are chosen because of the following reasons. The IM is chosen because it has non−negligible higher order terms in its Taylor series approximation. The Lorenz system is one of the archetypical chaotic systems commonly studied for chaotic synchronization, while, the complexity of the chaotic attractor (in terms of the correlation dimension[1]) for the MG system can be controlled by simply adjusting one of its parameters. Extensive computer simulations are carried out and the results are discussed in detail in this section. In all the computer simulations, the SNR is varied from -5dB to 50dB for the Lorenz and MG systems and in the case of IM, it is varied from 35dB to 60dB. For these simulations, no specific communication scheme is assumed. Also, for chaotic systems, it is assumed that analog signals are transmitted and this signal is appropriately sampled at the receiver.

3.4.1 Case–I: IM

IM is already introduced in Section 2.5.1. The states of the IM are randomly initialized and generated iteratively. From Eq.(2.14), it can be easily verified that the map has non-negligible higher order terms in the Taylor series approximation due to the presence of *sine* and *cosine* terms.

State x^R is transmitted from the transmitter. Noise is added to this signal to produce the received signal y at different SNRs. At the receiver, the transmitter states are estimated using this information. Figure 3.4 shows the transmitter state (x^R) *vs* the estimated receiver state ($\hat{x}^R$) when the UKF and PF (using 20 particles) algorithms are used for synchronization (here the SNR is set to 50dB and the first 100 samples are omitted while generating this plot). For the PF and UKF schemes, this plot is a straight line implying perfect synchronization (or synchronization with negligible error) of the

[1]Correlation dimension of an attractor is a is a measure of the dimensionality of the space occupied by a set of random points [75, Chapter 5]

transmitter and the receiver systems.

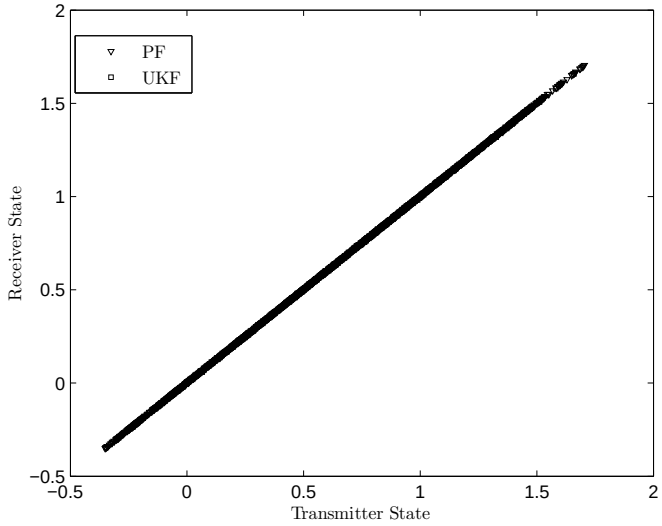


Figure 3.4: Transmitter *vs* receiver states (x^R and $\hat{x}^R$) after synchronization for PF and UKF based schemes (IM).

The synchronization speed of both algorithms are compared by computing the NISE [Eq.(2.16)] and are illustrated in Figure 3.5. In 20 iterations the PF based scheme achieves synchronization while the UKF based scheme needed almost 50 iterations to achieve it. A faster synchronization means less overhead is needed for communication purposes. In the case of the PF based synchronization scheme, the NISE settles down to a value of the order 10^{-7}. For the UKF based scheme on the other hand, this value is slightly higher. The range of the NISE values provides an insight to the instantaneous deviation from the synchronized trajectory. Here, the UKF based scheme has a larger spread of the NISE values implying frequent departure from the synchronized trajectory, whereas as in the case of the PF, the NISE curve is well behaved implying no intermittent burst of desynchronization.

To compare the synchronization performance of the algorithms for different SNRs, NMSEs and TNMSEs are computed and plotted on a semi−log scale (Figures 3.6 and 3.7). The performance of the EKF based scheme is used for comparison. The SNR is restricted from 35dB to 60dB, since majority of the trajectories of the EKF based scheme diverge for SNR values below 35dB. For the UKF based scheme, there are few trajectories

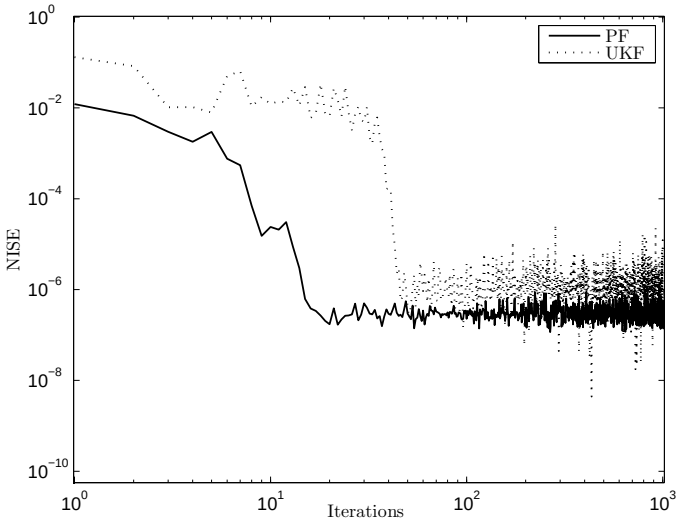


Figure 3.5: Error dynamics of IM for the PF and UKF based schemes.

which are diverging even in the range of 35dB to 60dB. For the PF based scheme, no trajectories are found to diverge in this range. However, a large number of trajectories are found to be diverging at SNRs below 20dB. To avoid misleading results, only the synchronized trajectories are considered for the calculation of NMSE, TNMSE and NISE. The NMSE (Figure 3.6) of the UKF and PF based schemes are almost identical while TNMSE (Figure 3.7) of the PF is slightly better than that of the UKF based scheme. This implies that the estimation of the imaginary part of the state variable (x_k^I) is more accurate with PF compared to the UKF and EKF. In Table 3.1, the actual values of the NMSEs are provided. For all the SNR values, the NMSEs of the UKF and PF based schemes are almost similar. Considering the TNMSE performances and the fact that no diverging trajectories are observed in the case of PF based synchronization, it makes an appropriate choice for the synchronization of IM.

Table 3.1: NMSE of IM

SNR	UKF	PF
35	1.83e-04	1.85e-04
45	1.64e-05	1.69e-05
55	1.71e-06	1.62e-06

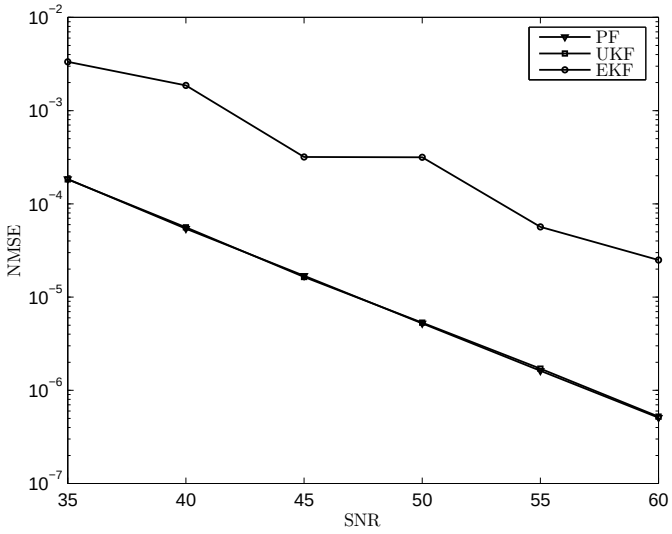


Figure 3.6: NMSE of IM for the PF, UKF and EKF based schemes.

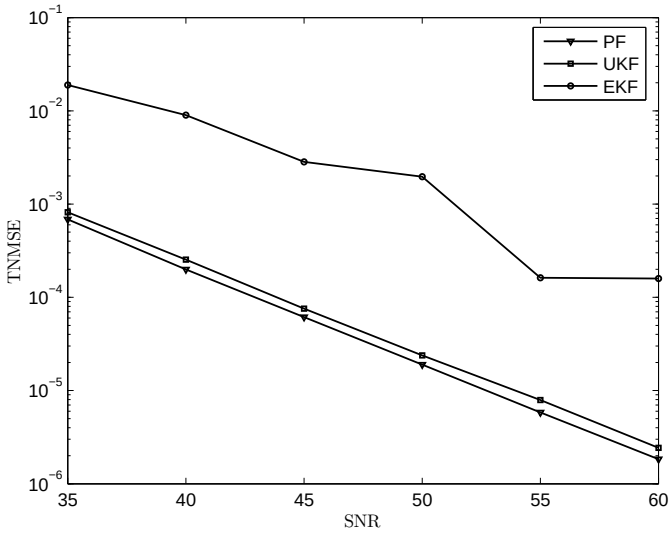


Figure 3.7: TNMSE of IM for the PF, UKF and EKF based schemes.

3.4.2 Case–II: Lorenz System

The Lorenz system is a three dimensional vector field, $\phi(x, y, z) : R^3 \rightarrow R^3$, representing the interrelation of temperature variation and convective motion [81]. The set of coupled

differential equations representing the Lorenz system is given by

$$\begin{aligned} \dot{x}(t) &= \sigma(y(t) - x(t)), \\ \dot{y}(t) &= -x(t)z(t) + rx(t) - y(t), \\ \dot{z}(t) &= x(t)y(t) - cz(t), \end{aligned} \tag{3.19}$$

where $\sigma = 10$, $r = 28$ and $c = \frac{8}{3}$ are used to obtain the Lorenz attractor. The three states (x, y and z) are randomly initialized and with the use of fourth order Runge−Kutta method, the states are iteratively generated. The Lorenz attractor is shown in Figure 3.8.

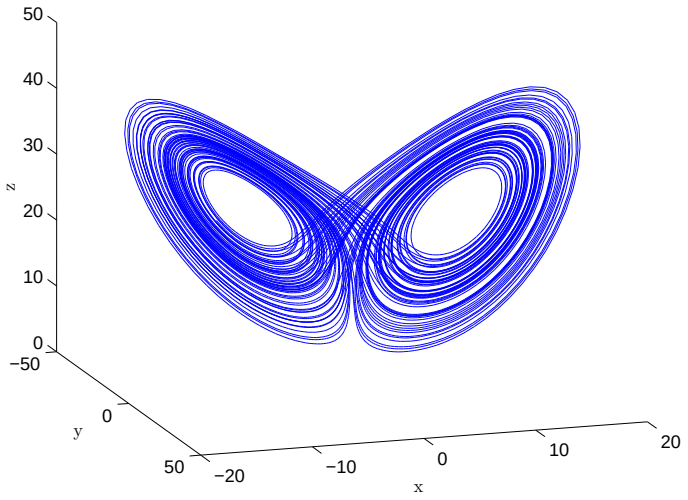


Figure 3.8: Lorenz attractor ($\sigma = 10$, $r = 28$ and $c = \frac{8}{3}$).

For Lorenz system, the state x alone is transmitted and at the receiver all the three states, x, y and z, are estimated. Figure 3.9 shows the graph of the state x of the transmitter plotted against the state $\hat{x}$ of the receiver for the UKF and the PF based synchronization schemes. The linear relationship of the states for both the schemes shows perfect synchronization of the transmitter and the receiver states.

The NISE for the PF and UKF based schemes is presented in Figure 3.10. For the UKF based scheme, fast convergence is observed which takes about 10 iterations whereas for the PF scheme, it takes almost 100 iterations to reach small NISE values. The steady state convergence error is also relatively higher for the PF. A comparison with Figure

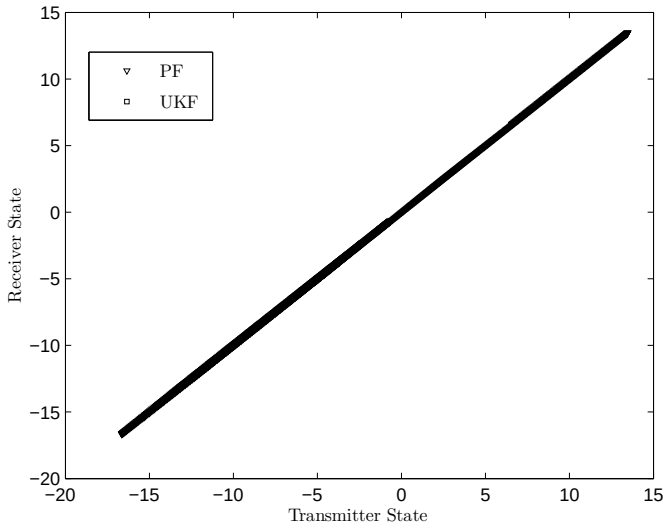


Figure 3.9: Transmitter *vs* receiver states (x and $\hat{x}$) after synchronization for the PF and UKF based schemes (Lorenz system).

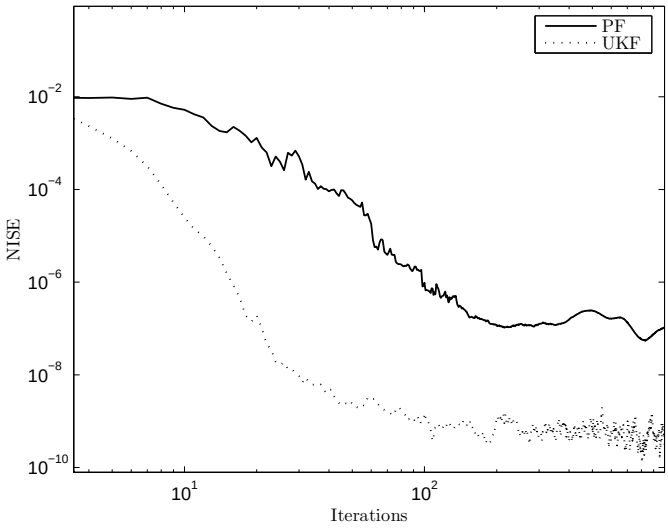


Figure 3.10: Error dynamics of Lorenz system for UKF and PF based schemes.

4.8 reveals that both of these schemes converge faster than the EKF based scheme which takes almost 1500 iterations. In Figure 3.11, NMSEs of the state x for the PF, UKF and EKF based schemes are provided. Numerical values of the NMSE can be obtained from Table 3.2. The corresponding TNMSE variation is illustrated in Figure 3.12. From Figures 3.11 and 3.12 , it can be observed that while the NMSE and TNMSE of UKF and

EKF have decreasing values of with increase in SNRs, these values of the PF saturate to constant values at high SNRs. One possible explanation for this behaviour is the numerical computations involved in determining the particles. Near the solution, the elements of the covariance matrix $\hat{\mathbf{P}}_k^i$ will become small in values. This is because the error variance become small near the solution. Moreover, the trajectories are locally correlated. Hence the sigma points generated using these matrices will not be diverse enough to capture the dynamics. This lack of diversity causes the error floor.

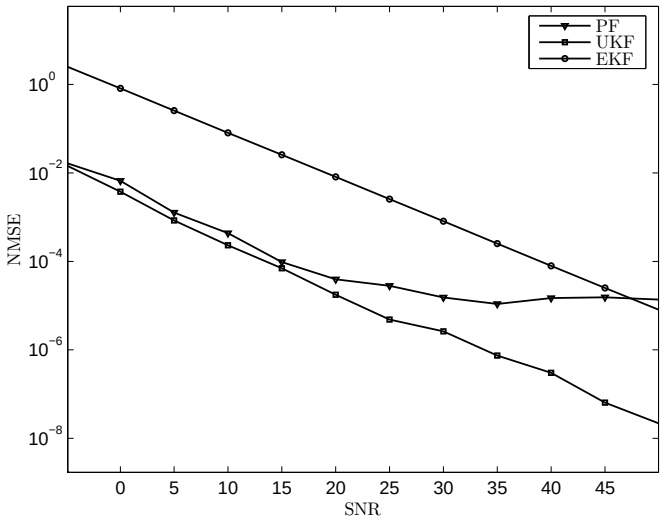


Figure 3.11: NMSE of state x (Lorenz) for the PF, UKF and EKF based schemes.

Table 3.2: NMSE of the Lorenz system

SNR	UKF	PF
0	1.48e-02	1.68e-02
25	4.85e-06	2.81e-05
50	2.18e-08	1.39e-05

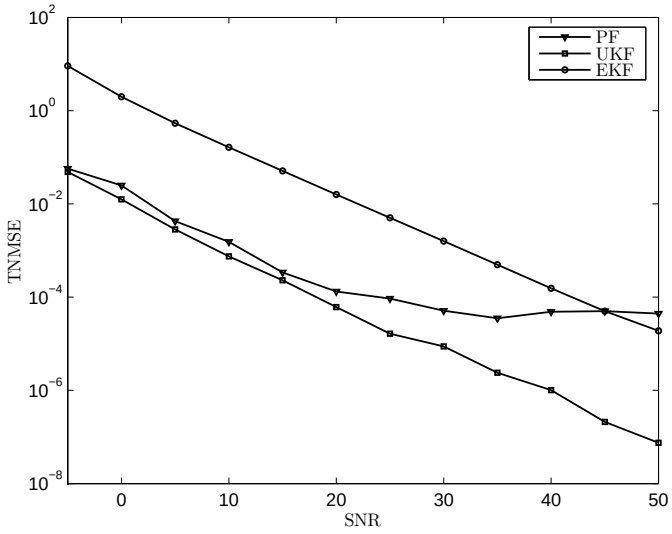


Figure 3.12: TNMSE of Lorenz system for the PF, UKF and EKF based schemes.

3.4.3 Case–III: MG System

The MG system was originally proposed as a first order nonlinear delay differential equation to describe physiological control systems [82]. It is given by

$$\dot{x}(t) \quad = \quad -ax(t) + \frac{bx(t-\tau)}{1+x(t-\tau)^{10}}. \tag{3.20}$$

This system is chaotic for values of $b = 0.2$, $a = 0.1$ and $\tau \geq 17$. An interesting feature of this system is that its complexity (i.e. the correlation dimension) increases as τ increases. For the generation of MG system, a delay differential equation solver is used [84, Chapter 4]. Figure 3.13 shows the MG attractor.

The MG system has only one state (x) which is transmitted through a noisy channel and the received signal is used for synchronization. For this system, the simulations are carried out for two different τ values (17 and 50). The transmitter *vs* the receiver states after synchronization ($\tau = 17$) is plotted in Figure 3.14 for both the schemes. A straight line relationship shows the perfect synchronization of the transmitter and the receiver states. However, for the EKF based scheme (see Figure 4.12), the graph is spread over the entire area showing its inability to synchronize the trajectories. Figure 3.15 presents the NISE characteristics of the PF and UKF based synchronization schemes. One can easily see that the PF based scheme is able to provide quick synchronization. For the

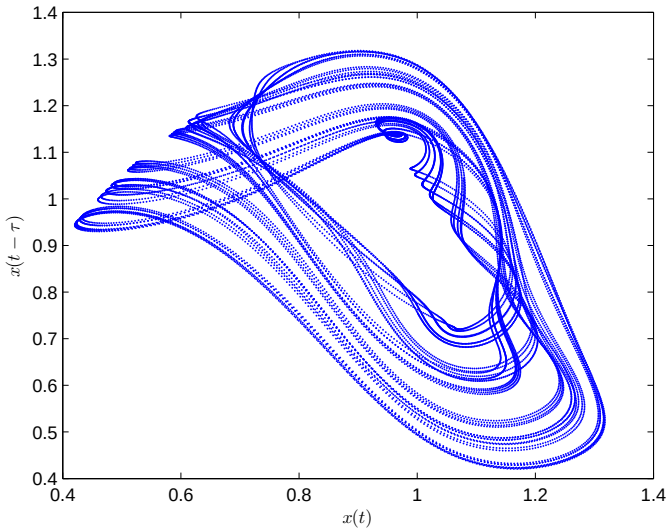


Figure 3.13: MG attractor ($b = 0.2$, $a = 0.1$ and $\tau = 17$).

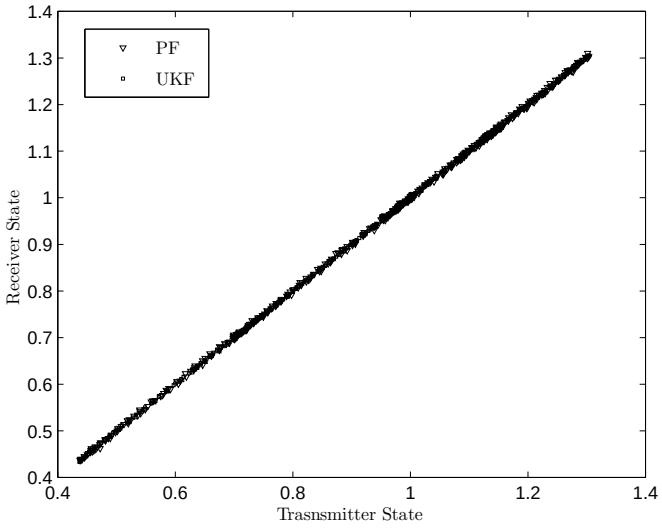


Figure 3.14: Transmitter *vs* receiver states (x and $\hat{x}$) after synchronization for EKF based scheme (MG system).

UKF based scheme, although the initial values are very close, a complete synchronization of the transmitter and the receiver trajectories happens only after about 100 iterations. The value to which NISE settles down are different for the PF and UKF schemes.

The SNR *vs* NMSE for the PF, UKF and EKF based schemes for $\tau = 17$ and 50 are illustrated in Figure 3.16. Table 3.3 provides the values of the NMSEs. It can be seen

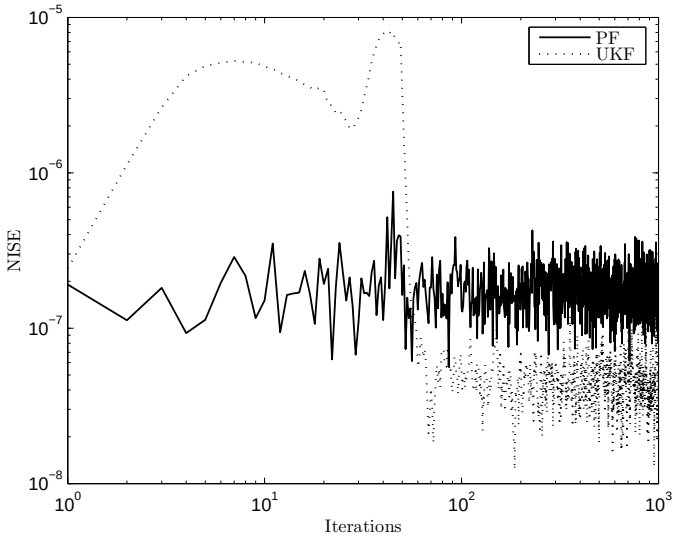


Figure 3.15: Error dynamics of MG system for the PF and UKF based schemes.

that the PF based scheme is relatively insensitive to the increase in the complexity (in other words, increase in the τ values) at higher SNR values. For instance, when $\tau = 17$ and 50, the NMSEs of PF based scheme are almost the same. On the other hand, for the UKF and EKF based schemes, noticeable differences in the NMSE values are observed for different values of τ: when $\tau = 50$, the NMSE is higher compared to when $\tau = 17$. Here again, the NMSE of the PF is higher than that of the UKF and it is clearly noticeable at high SNRs and low values of τ. For low values of τ, the trajectories of MG system are locally correlated. One needs more diverse samples for proper functioning of PF. However, this is not the case with higher values of τ. The trajectories have less local correlation causing the Frobenius norm of each covariance matrix (corresponding to each sample) to shrink fast resulting in less diversity.

Table 3.3: NMSE of the MG system

SNR	UKF ($\tau = 17$)	PF ($\tau = 17$)	UKF ($\tau = 50$)	PF ($\tau = 50$)
0	9.48e-02	3.75e-02	1.54e-01	1.41e-01
25	1.12e-04	3.39e-04	1.74e-03	3.23e-04
50	3.35e-06	7.07e-06	1.45e-05	7.07e-06

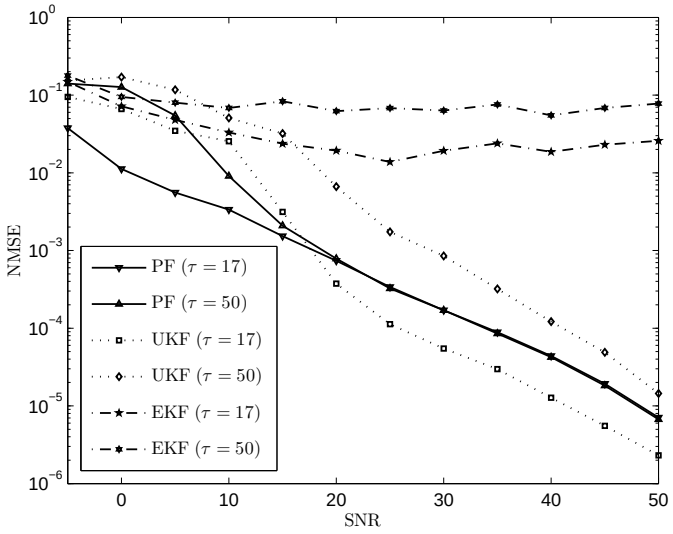


Figure 3.16: NMSE MG system for UKF, PF and EKF based schemes.

3.5 Conclusion

The EKF is one of the most widely investigated stochastic filtering methods for chaotic synchronization. However, for highly nonlinear systems, it introduces approximation errors causing unacceptable degradation in the synchronization performance. In this chapter, two nonlinear filtering algorithms (PF and UKF) are proposed for the synchronization of the chaotic systems/maps. The objectives here are twofold: (*i*) to get faster synchronization and (*ii*) low synchronization errors. Both the PF and UKF based schemes are able to meet these two requirements compared to the EKF based scheme. These two algorithms are tested on two chaotic systems (Lorenz and MC systems) and one chaotic map (IM). The main conclusions drawn from this study are as follows.

- For all the chaotic systems/maps studied, PF and UKF are able to give a fast and accurate synchronization.
- Comparing the NISE, NMSE and TNMSE of the IM, PF has performed better compared to the UKF and EKF.
- For the IM, the PF based scheme has additional advantage that no diverging trajectories are observed, whereas for the EKF and UKF based schemes, diverging

trajectories are observed.

- For proper operation of the PF based scheme, the particles should be diverse (sampled from all areas of the state space). However, this fails when the PF is applied to the synchronization of the Lorenz and MG systems causing the synchronization error to be slightly higher compared to UKF.

Chapter 4

Nonlinear Predictive Filter for Chaotic Synchronization

4.1 Introduction

Many alternatives to the EKF have been proposed for nonlinear estimation and tracking. A simple and efficient method is the nonlinear predictive filter (NPF). It is widely used in nonlinear control applications. The NPF algorithm is based on a predictive tracking scheme first introduced by Lu [50]. Crassidis and Markley [85] modified the algorithm for filtering applications. The NPF has several advantages over the EKF: (*i*) it uses a continuous time model to estimate the states and hence avoids discrete state jumps, (*ii*) no explicit assumption about the model error is required, and (*iii*) unlike EKF, it does not assume Gaussianity of the posterior probability. In this chapter, NPF based scheme for chaotic synchronization is proposed and analyzed in detail.

In the next section, the NPF scheme is discussed briefly. In Section 4.3, condition for the stability of the NPF based scheme is derived. Theoretical upper bound for the TNMSE is also derived. The numerical results are discussed in detail in the following section (Section 4.4) and some concluding remarks are provided in Section 4.5.

4.2 Nonlinear Predictive Filter

NPF is a predictive corrective filtering algorithm. With the current state information at time t, the NPF predicts the output at a future instant, $t + \Delta t$. The time step, Δt, is assumed to be sufficiently small. The error between this predicted value and the actual value is calculated. Using this error, the NPF generates a control signal, which is added to the current state as a correction, such that the prediction error is minimized. It is assumed that the state and the output estimates are given by a preliminary model and a to-be-determined model error vector ($\mathbf{d}(t)$). The receiver model is given by

$$\dot{\hat{\mathbf{x}}}(t) = \mathbf{f}(\hat{\mathbf{x}}(t)) + \mathbf{G}(\hat{\mathbf{x}}(t))\mathbf{d}(t), \tag{4.1a}$$

$$\hat{\mathbf{y}}(t) = \mathbf{h}(\hat{\mathbf{x}}(t)) \tag{4.1b}$$

where $\mathbf{G}(\hat{\mathbf{x}}(t))$ is the error distribution matrix. Using Taylor series, at time t, the model output can be expanded as

$$\hat{\mathbf{y}}(t + \Delta t) = \hat{\mathbf{y}}(t) + \Xi(\hat{\mathbf{x}}(t)) + \Lambda \mathbf{s}\left(\hat{\mathbf{x}}(t)\right)\mathbf{d}(t) \tag{4.2}$$

where

$$\Xi(\hat{\mathbf{x}}(t)) = col\Big[\sum_{j=1}^{p_i} \frac{\Delta t^j}{j!} L_f^k(h_i)\Big] \tag{4.3a}$$

$$\Lambda = diag\Big[\frac{\Delta t^{p_i}}{p_i!}\Big] \tag{4.3b}$$

$$\mathbf{s}\left(\hat{\mathbf{x}}(t)\right) = col\Big[L_{g_i}[L_f^{p_i-1}(h_i)]\Big]. \tag{4.3c}$$

Here, $i = 1, \ldots, m$, operators $diag[.]$ and $col[.]$ denote diagonal and column matrices, respectively. p_i is the order of the derivatives such that $\mathbf{d}(t)$ is explicitly available in the expansion, $L_f^j(h_i)$ is the j^{th} order Lie derivative [50] given by

$$L_f^0(h_i) = h_i, \tag{4.4a}$$

$$L_f^j(h_i) = \frac{\partial L_f^{j-1}(h_i)}{\partial \hat{\mathbf{x}}^T(t)}\mathbf{f}(\hat{\mathbf{x}}(t)), \quad j \geq 1, \tag{4.4b}$$

and the Lie derivative within Eq.(4.3c) is given by

$$L_{g_i}[L_f^{p_i-1}(h_i)] = \frac{\partial L_f^{p_i-1}(h_i)}{\partial \hat{\mathbf{x}}_j^T}\mathbf{G}(\hat{\mathbf{x}}_j). \tag{4.5}$$

The objective here is to find $\mathbf{d}(t)$ such that the following cost function[1] is minimized:

$$J(\mathbf{d}(t)) = \frac{1}{2}[\mathbf{y}(t+\Delta t) - \hat{\mathbf{y}}(t+\Delta t)]^T \mathbf{R}^{-1}[\mathbf{y}(t+\Delta t) - \hat{\mathbf{y}}(t+\Delta)] + \frac{1}{2}\mathbf{d}(t)^T \mathbf{W}\mathbf{d}(t). \quad (4.6)$$

In the above equation, $\mathbf{W}$ and $\mathbf{R}$ are positive semi−definite weighting matrices. The conditions for the selection of $\mathbf{W}$ and $\mathbf{R}$ are discussed in Section 4.3. When $J(\mathbf{d}(t))$ is minimized, the control signal, $\mathbf{d}(t)$, is obtained as

$$\begin{aligned} \mathbf{d}(t) = \quad - \quad & \left\{[\Lambda \mathbf{s}(\hat{\mathbf{x}}(t))]^T \mathbf{R}^{-1} \Lambda \mathbf{s}(\hat{\mathbf{x}}(t)) + \mathbf{W}\right\}^{-1} \\ & [\Lambda \mathbf{s}(\hat{\mathbf{x}}(t))]^T \mathbf{R}^{-1}[\Xi(\hat{\mathbf{x}}(t)) - \mathbf{y}(t+\Delta t) + \hat{\mathbf{y}}(t)]. \end{aligned} \quad (4.7)$$

The block diagram of the NPF is depicted in Figure 4.1.

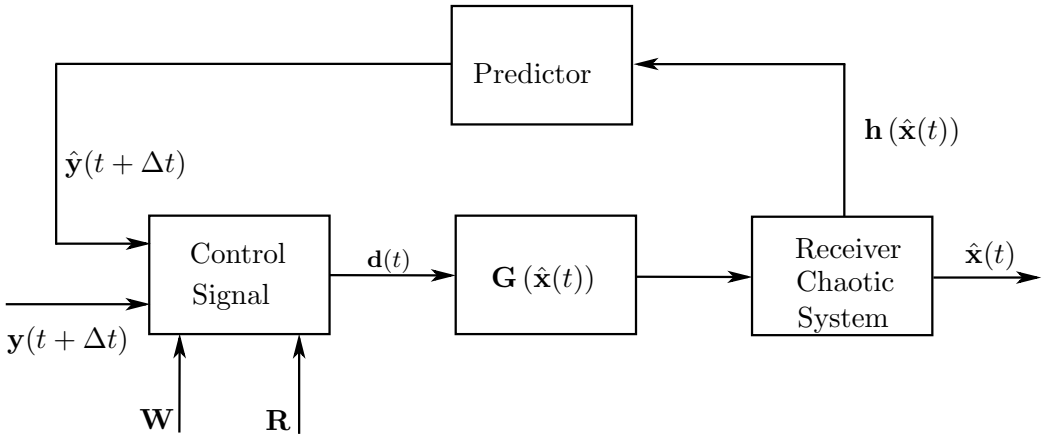


Figure 4.1: Schematic of the NPF.

4.3 Stability Analysis

In chaotic communication schemes, typically, one state out of the n states of the chaotic systems/maps are transmitted. Assume, $\mathbf{G}(\mathbf{x}(t))$ is independent of the states $\mathbf{x}(t)$. Also assume $\mathbf{h}(.)$ is a vector $\bar{\mathbf{h}} = [h_1, \ldots, h_m]$. Here, h_i, corresponding to the i^{th} entry of $\bar{\mathbf{h}}$ takes the value 1 if the i^{th} state variable is transmitted and 0 otherwise. This makes $\mathbf{y}(t)$ and $\hat{\mathbf{y}}(t)$ to be a scalar quantity, $y(t)$ and $\hat{y}(t)$, respectively. In this case, $\mathbf{G}(\hat{\mathbf{x}}(t))$ is a

[1]For chaotic maps, the objective function is written as $J(\mathbf{d}_k) = \frac{1}{2}[\mathbf{y}_{k+1} - \hat{\mathbf{y}}_{k+1}]^T \mathbf{R}^{-1}[\mathbf{y}_{k+1} - \hat{\mathbf{y}}_{k+1}] + \frac{1}{2}\mathbf{d}_k^T \mathbf{W}\mathbf{d}_k$.

vector $\mathbf{g} = [g_1, \ldots, g_n]^T$. Hence the control signal also becomes scalar given by

$$d(t) \quad = \quad -\Delta t c w^{-1} \mathbf{g}^T \bar{\mathbf{h}}^T r^{-1} \Big\{ \hat{y}(t) - \bar{y}(t + \Delta t) + \Delta t \bar{\mathbf{h}} \mathbf{f}(\hat{\mathbf{x}}(t)) \Big\}, \tag{4.8}$$

where the quantity c is equal to $1 - w^{-1}\mathbf{g}^T\bar{\mathbf{h}}^T \left[\bar{\mathbf{h}}\mathbf{g}w^{-1}\mathbf{g}^T\bar{\mathbf{h}}^T + \Delta t^{-2} r\right]^{-1} \bar{\mathbf{h}}\mathbf{g}$. w and r are the weights used in Eq.(4.7). If one keeps w, r, and Δt constants for a specific SNR then, $\Delta t c w^{-1} \mathbf{g}^T \bar{\mathbf{h}}^T r^{-1}$ in the above equation will be a scalar constant, say M. It is assumed that the noise, $v(t)$, is additive and bandlimited with a variance σ^2. Using these assumptions, stability of the NPF based scheme is analyzed in this section. An approximate expression for the total mean square error (TMSE) is also derived. Please note that TMSE and TNMSE differs in a normalizing constant.

At time t, let the error between the transmitter and receiver system states be

$$\mathbf{e}(t) = \mathbf{x}(t) - \hat{\mathbf{x}}(t). \tag{4.9}$$

The receiver output at any time, t, be $\hat{y}(t) = \bar{\mathbf{h}}\hat{\mathbf{x}}(t)$. Expanding $\hat{y}(t + \Delta t)$ at $\hat{y}(t)$, the control signal, $d(t)$, can be approximated as

$$d(t) \quad = \quad -M\bar{\mathbf{h}}\Big(\hat{\mathbf{x}}(t) - \big(\mathbf{x}(t) + \Delta t \mathbf{f}(\mathbf{x}(t))\big) + \Delta t \mathbf{f}(\hat{\mathbf{x}}(t))\Big) + Mv(t). \tag{4.10}$$

The error dynamics, $(\dot{\mathbf{e}}(t))$, is given by

$$\dot{\mathbf{e}}(t) \quad = \quad \dot{\mathbf{x}}(t) - \dot{\hat{\mathbf{x}}}(t) = \mathbf{f}(\mathbf{x}(t)) - \mathbf{f}(\hat{\mathbf{x}}(t)) - \mathbf{g}d(t) \tag{4.11}$$

When the channel noise is small and the synchronization error is small (i.e. $\hat{\mathbf{x}}(t)$ is close to $\mathbf{x}(t)$), linearizing at the transmitter trajectories $\mathbf{x}(t)$, $\mathbf{e}(t)$ can be given by

$$\mathbf{e}(t) = \mathbf{A}\mathbf{e}(t) + \mathbf{K}(t)\mathbf{e}(t) - M\mathbf{g}v(t) \tag{4.12}$$

where $\mathbf{A} = -M\mathbf{g}\bar{\mathbf{h}}$ and $\mathbf{K}(t) = \big(\mathbf{I} - \Delta t M \mathbf{g}\bar{\mathbf{h}}\big)\frac{\partial \mathbf{f}(\mathbf{x}(t))}{\partial \mathbf{x}}$. The solution $(\mathbf{e}(t))$ of the above stochastic differential equation is given by

$$\mathbf{e}(t) = \exp\left(\int_{t_0}^{t} (\mathbf{A} + \mathbf{K}(\tau))\, d\tau\right) \mathbf{e}(t_0) - \int_{t_0}^{t} \exp\left(\int_{\tau}^{t} (\mathbf{A} + \mathbf{K}(s))\, ds\right) M\mathbf{g}v(\tau) d\tau. \tag{4.13}$$

Taking the expectation over the channel noise $v(t)$, we get

$$\begin{aligned}\mathbb{E}\left[\mathbf{e}^T(t)\mathbf{e}(t)\right] &= \mathbf{e}^T(t_0)\left[\exp\left(\int_{t_0}^{t}\mathbf{A}d\tau+\frac{t-t_0}{t-t_0}\int_{t_0}^{t}\mathbf{K}(\tau)d\tau\right)\right]^T \\ &\exp\left(\int_{t_0}^{t}\mathbf{A}d\tau+\frac{t-t_0}{t-t_0}\int_{t_0}^{t}\mathbf{K}(\tau)d\tau\right)\mathbf{e}(t_0)+ \\ &\sigma^2\int_{t_0}^{t}M\mathbf{g}^T\left[\exp\left(\int_{\tau}^{t}\mathbf{A}ds+\frac{t-\tau}{t-\tau}\int_{\tau}^{t}\mathbf{K}(s)ds\right)\right]^T \\ &\exp\left(\int_{\tau}^{t}\mathbf{A}ds+\frac{t-\tau}{t-\tau}\int_{\tau}^{t}\mathbf{K}(s)ds\right)M\mathbf{g}d\tau. \qquad (4.14)\end{aligned}$$

For $t\to\infty$, $\frac{t-t_0}{t-t_0}\int_{t_0}^{t}\mathbf{K}(\tau)d\tau=(t-t_0)\mathcal{K}$, where $\mathcal{K}=<\mathbf{K}(\tau)>$ is the average taken over the Sinai-Bowen-Ruelle (SBR) measure [83]. If the real part of the eigenvalues of the matrix $\left[(\mathbf{A}+\mathcal{K})^T+(\mathbf{A}+\mathcal{K})\right]$ are all negative, the first term becomes zero as $t\to\infty$. This is the necessary condition for the asymptotic stability of the NPF based synchronization scheme. By replacing $\frac{1}{t-\tau}\int_{\tau}^{t}\mathbf{K}(s)ds$ with $\mathcal{K}$, we get

$$\begin{aligned}\mathbb{E}\left[\mathbf{e}^T(t)\mathbf{e}(t)\right] &= \mathbf{e}^T(t_0)\exp\left[\Big((\mathbf{A}+\mathcal{K})^T+(\mathbf{A}+\mathcal{K})\Big)(t-t_0)\right]\mathbf{e}(t_0)+ \\ &\sigma^2\left\{\int_{t_0}^{t}M\mathbf{g}^T\exp\left[\Big((\mathbf{A}+\mathcal{K})^T+(\mathbf{A}+\mathcal{K})\Big)(t-\tau)\right]M\mathbf{g}d\tau\right\} \qquad (4.15)\end{aligned}$$

As $\lim_{t\to\infty}$, the asymptotic error is given by

$$\lim_{t\to\infty}\mathbb{E}\left[\mathbf{e}^T(t)\mathbf{e}(t)\right] \approx -(M\sigma)^2\mathbf{g}^T\left[(\mathbf{A}+\mathcal{K})^T+(\mathbf{A}+\mathcal{K})\right]^{-1}\mathbf{g}. \qquad (4.16)$$

Trace of $\lim_{t\to\infty}\mathbb{E}\left[\mathbf{e}^T(t)\mathbf{e}(t)\right]$ gives an indication of the total mean square error (TMSE). It depends on the channel noise, M (which in turns depends on $\mathbf{g}$, $\bar{\mathbf{h}}$, Δt, w and r), and chaotic systems/maps (through $\mathcal{K}$).

The TNMSE dynamics of the NPF based scheme is presented in Figure 4.2. Numerical integration of the Eq.(4.13) is used to obtain this. The MC simulation results for 50 different initial conditions are averaged and presented in this graph. It can be seen that the NPF is able to provide a low TNMSE for an arbitrarily large initial state error. After almost 2000 iterations, the TNMSE is settling down to a very small value of the order of 10^{-7}. This observation ascertains the above argument that, if all the eigenvalues of the matrix $\left[(\mathbf{A}+\mathcal{K})^T+(\mathbf{A}+\mathcal{K})\right]$ are negative, the TNMSE becomes independent of the initial states. This condition is satisfied by following steps.

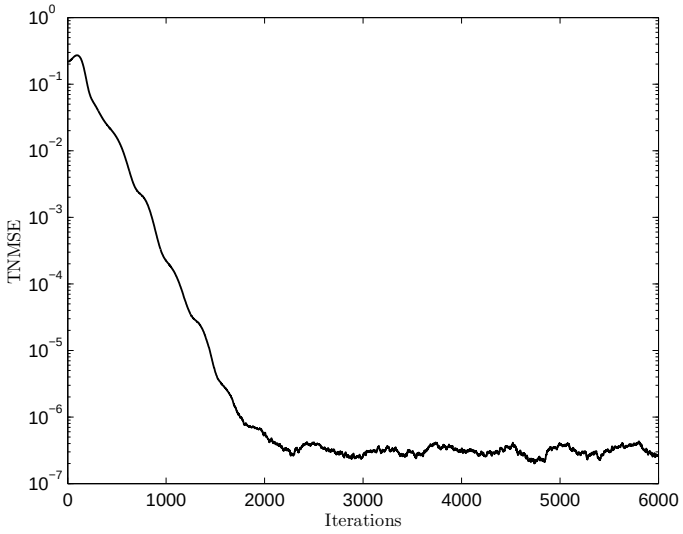


Figure 4.2: TMSE for NPF based scheme (Lorenz system: using numerical integration of Eq.(4.13)).

1. Select the prediction step, Δt. This is selected such that the numerical integration of the differential equation of the chaotic system is possible.
2. Set $r = \sigma^2$.
3. Compute $\mathcal{K}$ numerically.
4. Select $\mathbf{g}$ and w so that the eigenvalues of the matrix, $\left[(\mathbf{A}+\mathcal{K})^T + (\mathbf{A}+\mathcal{K})\right]$, will have negative real parts.

In all the simulations carried out in this chapter, stability of the NPF is guaranteed by following first two steps listed above. Instead of computing the matrix $\left[(\mathbf{A}+\mathcal{K})^T + (\mathbf{A}+\mathcal{K})\right]$ and finding its eigenvalues, $\mathbf{g}$ is selected arbitrarily with positive values and then w is adjusted such that the NPF converges eventually.

4.4 Results and Discussion

4.4.1 Case–I: IM

From the transmitter, the state x^R is transmitted. Noise is added to this signal to produce the received signal y at different SNRs. At the receiver, the transmitter states

are estimated using this information. The performance of the NPF based scheme is compared to that of the EKF based scheme. Figure 4.3 shows the transmitter state (x^R) *vs* the estimated receiver state ($\hat{x}^R$) when the NPF and EKF algorithms are used for synchronization[2]. It can be seen that the relationship between the transmitter and the receiver states is linear for the NPF based scheme which implies perfect synchronization of the transmitter and the receiver. The corresponding picture for the EKF based scheme is also shown in the same figure. Although a linear region is present in this figure, some of the points are scattered around. This is due to the intermittent burst of desynchronization experienced when the EKF is used[3].

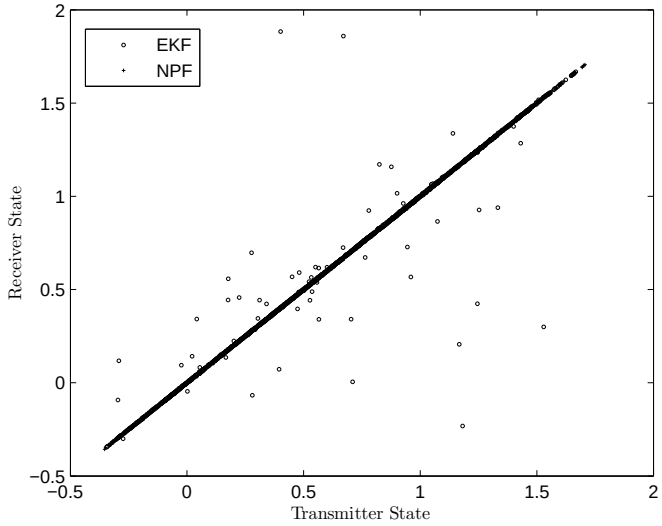


Figure 4.3: Transmitter *vs* receiver states (x^R and $\hat{x}^R$) after synchronization for NPF based scheme (IM).

The synchronization speed of both the algorithms are compared by computing the NISE [Eq.(2.16)] and are illustrated in Figure 4.4. It can be seen that, compared to the EKF, the NPF based scheme achieves faster synchronization. When it is used, the NISE converges to a very small value of the order of 10^{-7} and remains more or less the same from thereon after about 40 iterations. In the case of the EKF, it takes more iterations (few hundreds) to settle down to a smaller NMSE value (of the order of 10^{-8}). However,

[2]Here the SNR is set to 50dB and the first 500 samples are discarded while generating this plot.

[3]Please refer the discussion in Section 2.6.3

it can be observed that the EKF suffers from intermittent bursts of desynchronization. One reason for this behavior can be attributed to the presence of hyperbolic tangencies [43] as discussed in Section 2.6.3. This picture clearly shows that the NPF based scheme synchronizes much faster and remains synchronized thereon.

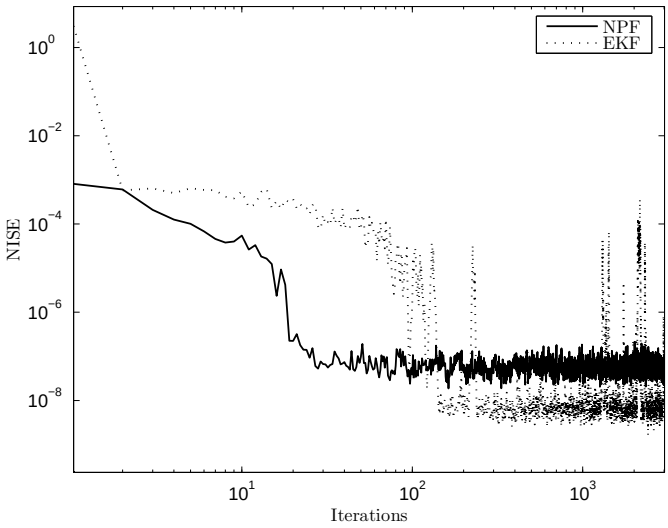


Figure 4.4: Error dynamics of IM for NPF and EKF based schemes.

To compare the performance of both the algorithms for different SNRs, NMSEs and TNMSEs are computed and plotted on a semi−log scale (Figures 4.5 and 4.6). Here the SNR is restricted from 35dB to 60dB. During the simulation studies, it is observed that for the given set of parameters, the EKF is unable to synchronize certain trajectories (outliers), whereas the NPF always synchronizes. It is also observed that at low SNRs (below 35dB), the number of outliers are very high; in some cases, none of the trajectories synchronize. Hence in this case the SNR values are restricted to 35dB and above. In this range also divergence of trajectories is observed, however, they are only very few. Hence to avoid misleading results, only the synchronized trajectories are considered for the calculation of NMSE, TNMSE and NISE. From these figures, it can be seen that the NPF based scheme has better performance than that of the EKF based scheme in terms of both NMSE (Figure 4.5) and TNMSE (Figure 4.6). The NMSE and TNMSE performances of the EKF based scheme are also shown in these figures. These values are much higher than that of the NPF based scheme. A possible reason for this behaviour

could be the intermittent bursts of desynchronization, which can be attributed to the channel noise and the approximation errors. In Table 4.1, the NMSEs at different SNRs are provided for both the schemes. From this table, it is clear that NPF has much better NMSE performance compared to EKF.

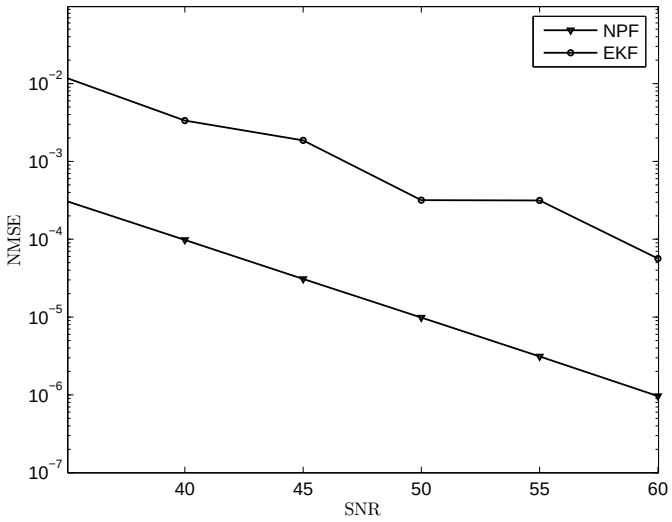


Figure 4.5: NMSE of state x^R (IM) for NPF and EKF based schemes.

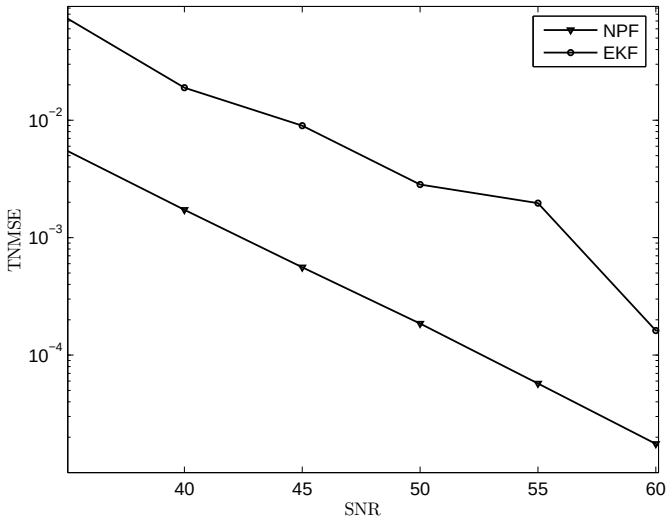


Figure 4.6: TNMSE of IM for NPF and EKF based schemes.

Table 4.1: NMSE of IM

SNR	EKF	NPF
35	1.20e-02	3.08e-04
45	1.86e-03	3.08e-05
55	3.16e-04	3.12e-06

4.4.2 Case–II: Lorenz System

For Lorenz system, the state x alone is transmitted and at the receiver all the three states (x, y and z) are estimated. From Eq.(3.19), it can be verified that the Lorenz system has a quadratic nonlinearity and hence the linear approximation error should be minimum. Hence, one could expect the performance of the NPF and EKF to be comparable. Figure 4.7 shows the graph of the state x of the transmitter plotted against the state $\hat{x}$ of the receiver of the NPF and the EKF based synchronization schemes. The linear relationship of the states for both the schemes show perfect synchronization.

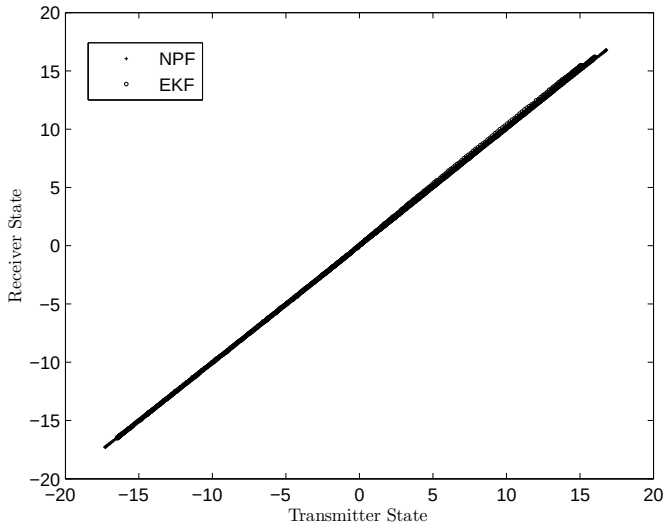


Figure 4.7: Transmitter *vs* receiver states (x and $\hat{x}$) after synchronization for NPF and EKF based schemes (Lorenz system).

The NISE curves of both the synchronization schemes are presented in Figure 4.8. From this figure, it can be seen that NPF converges faster (in about 1000 iterations)

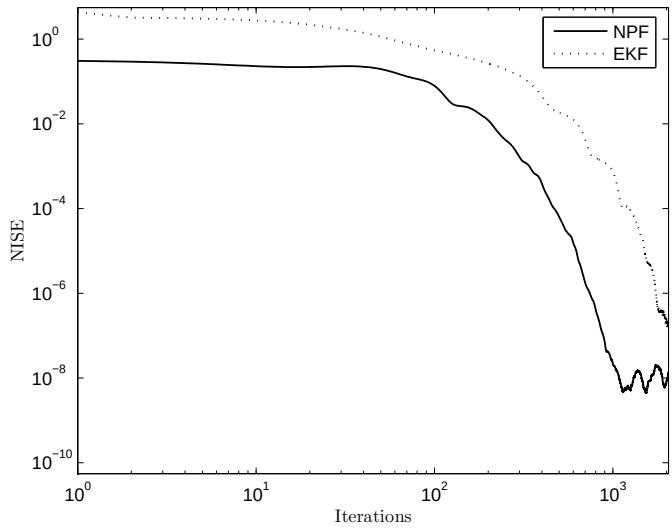


Figure 4.8: Error dynamics of Lorenz system for NPF and EKF based schemes.

compared to EKF which take almost 1500 iterations to converge. This implies that the NPF based scheme synchronizes faster than the EKF based scheme. This figure also shows that both the NPF and EKF based schemes have similar error dynamics. In Figure 4.9, NMSEs of state x for both the schemes are presented. The corresponding TNMSE variation is illustrated in Figure 4.10. From both of these graphs, it can be observed that the NPF always outperforms the EKF in synchronizing Lorenz systems (as the NMSE and TNMSE values for the NPF based scheme are always smaller than that for the EKF based scheme). Table 4.2 provides a closer look at the values of NMSE at different SNRs. For all the SNRs considered, the NMSE of NPF is lower than that of EKF at least by a factor of 10. This study shows that in the case of Lorenz systems also the NPF based scheme has better synchronization properties compared to EKF.

Table 4.2: NMSE of Lorenz system

SNR	EKF	NPF
0	8.12e-01	4.89e-02
25	2.56e-03	1.55e-04
50	8.53e-06	5.55e-07

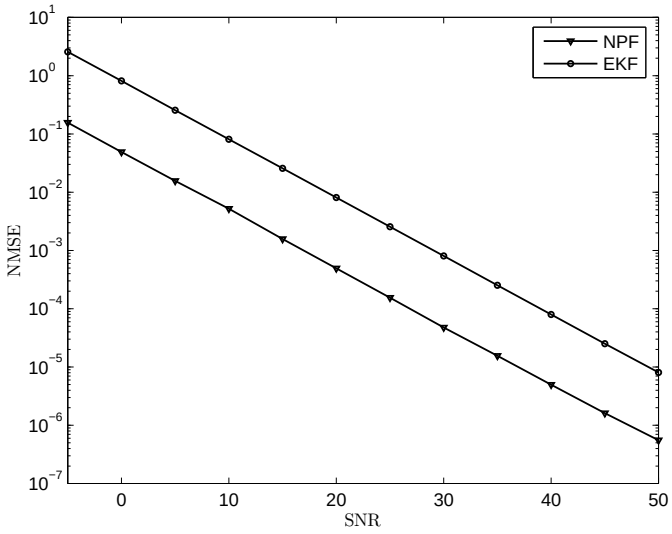


Figure 4.9: NMSE of state x (Lorenz) for NPF and EKF based schemes.

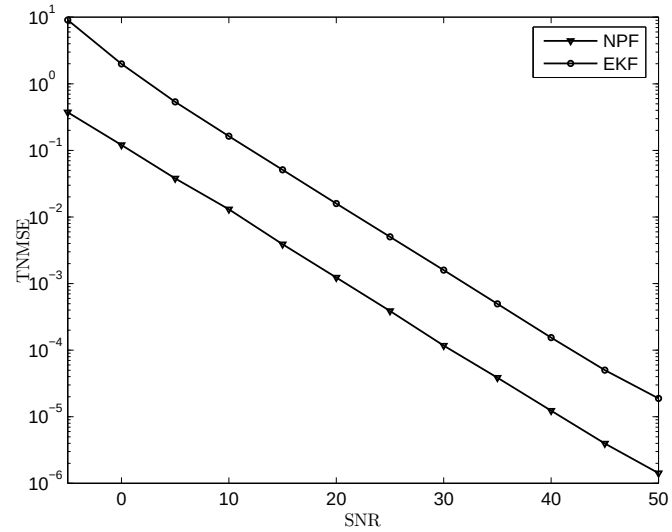


Figure 4.10: TNMSE of Lorenz system for NPF and EKF based schemes.

4.4.3 Case–III: MG System

The MG system has only one state (x) which is transmitted through a noisy channel and the received signal is used for synchronization. For this system, the simulations are carried out for two different τ values (17 and 100). The transmitter *vs* the receiver states after synchronization ($\tau = 17$) is plotted in Figure 4.11 for the NPF and the EKF based schemes. From this figure, a linear relationship can be observed in the case of NPF which

implies perfect synchronization of the transmitter and the receiver states. However, for the EKF based scheme, the graph is spread over the entire area. Figure 4.12 presents the NISE characteristics of both the synchronization schemes. For the NPF based scheme, the NISE settles down to a very small value in few iterations (< 100). A short−lived divergence (of the order of 10^{-5}) is observed in the error dynamics. However, it quickly settles down to a very small value. In the case of the EKF based scheme, even though the NISE reduces after a few iterations, the reduction is only of the order of 10^{-1} and it remains more or less at this level for the remaining iterations.

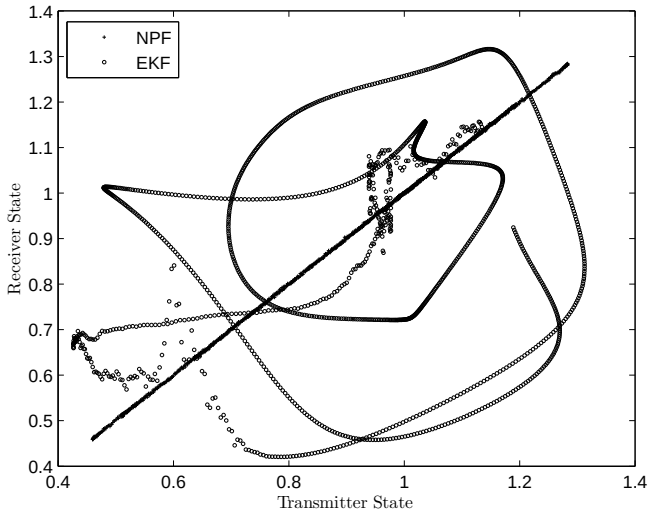


Figure 4.11: Transmitter *vs* receiver states (x and $\hat{x}$) after synchronization for NPF and EKF based schemes (MG system).

The SNR *vs* NMSE for the NPF and EKF based schemes for $\tau = 17$ and 100 are illustrated in Figure 4.13. It can be seen that the performance of the NPF based scheme is consistently much better than that of the EKF based scheme for SNR values above 15dB. Another observation is that the NPF based scheme is relatively insensitive to the increase in the complexity (in other words, increase in the τ values). For instance, when $\tau = 17$ and 100, the NMSEs of NPF based scheme are almost the same. For the EKF based scheme, on the other hand, a noticeable change in the NMSE values is observed for different values of τ (17 and 100): when $\tau = 100$, the NMSE is higher compared to when $\tau = 17$. It is also observed that the NMSE of EKF is insensitive to the SNR values while NPF shows steadily declining NMSE values. The exact NMSE values for MG system for

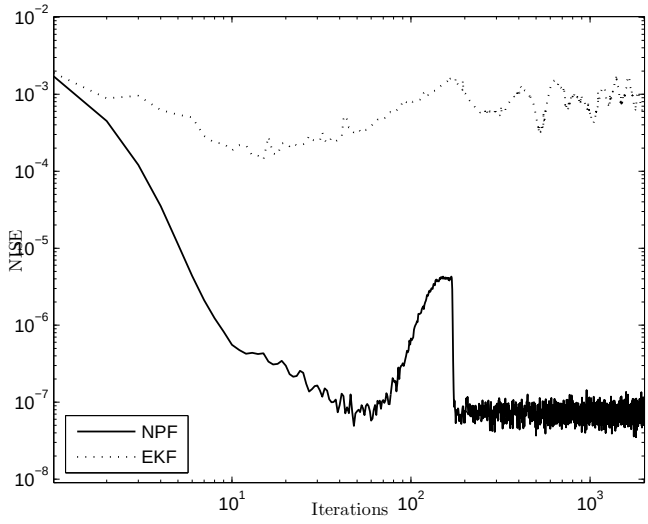


Figure 4.12: Error dynamics of MG system for the NPF and EKF based schemes.

different values of τ can be seen from Table 4.3.

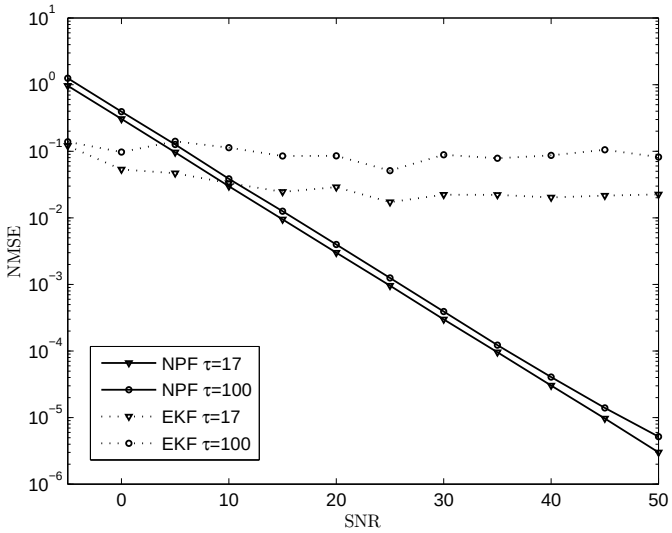


Figure 4.13: NMSE of state x (MG system) for NPF and EKF based schemes.

4.4.4 Parameter Mismatch

Since the NPF assumes modeling errors as a part of the state estimation, effect of parameter mismatch at the transmitter and receiver is studied in this section. In MG system, this study is possible because its complexity can be controlled by the τ values. Here

Table 4.3: NMSE of MG system for different values of τ (17 and 100)

SNR	EKF (τ=17)	NPF (τ=17)	EKF (τ=100)	NPF (τ=100)
0	5.34e-02	3.06e-01	9.75e-02	3.94e-01
25	1.72e-02	9.58e-04	5.10e-02	1.25e-03
50	2.25e-02	3.00e-06	8.18e-02	5.18e-06

complexity refers the complexity of the attractor which changes with τ. In this experiment, the transmitter τ value is set to 50 while the corresponding value at the receiver is set to 17. The NMSEs for the NPF and the EKF based synchronization schemes are computed and are plotted in Figure 4.14. The NMSEs of the two schemes for the same values of τ are also provided in the same graph for comparison. It can be seen that for the NPF based scheme, the NMSEs for both cases (identical τs and different τs) are almost similar, implying the insensitiveness of the scheme to the parameter change. In the case of the EKF based scheme however, the parameter variation causes an increase in the NMSE. Thus, these studies clearly show the superiority of the NPF based synchronization method, even in the case of parameter mismatch between the transmitter and the receiver.

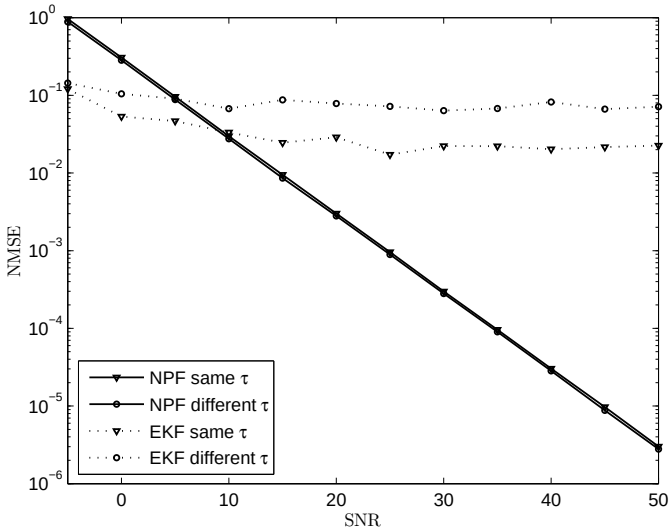


Figure 4.14: NMSE of MG system for different values of τ at transmitter for EKF and NPF based schemes.

4.4.5 Performance Comparison of EKF, UKF, PF and NPF

Table 4.4: Performance comparison for IM

Performance Indices	EKF	UKF	PF	NPF
Outliers	Yes	Yes	No	No
CC	M	M	VH	L
TS	150	80	11	30
NMSE	3.16e-04	1.71e-06	1.62e-06	3.12e-06
TNMSE	1.20e-03	7.90e-06	5.81e-06	5.72e-05

Table 4.5: Performance comparison for Lorenz system

Performance Indices	EKF	UKF	PF	NPF
Outliers	No	No	No	No
CC	M	M	VH	L
TS	1500	11	100	1000
NMSE	8.53e-06	2.18e-08	1.38e-05	5.55e-07
TNMSE	1.87e-05	7.47e-07	4.42e-05	1.45e-06

Table 4.6: Performance comparison for MG system ($\tau = 17$)

Performance Indices	EKF	UKF	PF	NPF
Outliers	No	No	No	No
CC	M	H	VH	L
TS	>1000	18	1	21
NMSE	2.25e-02	3.35e-06	7.07e-06	3.00e-06

In this section a comparison of the performances of EKF, UKF, PF and the NPF algorithms are provided. Tables[4] 4.4 to 4.6 provide the comparison of all the filtering based synchronization schemes studied in this thesis. Different aspects of synchronization such as speed, mean square error, divergence behaviour (outliers) and computational

[4]Legend: *Computational Complexity* (CC), *Low* (L), *Medium* (M), *Very High* (VH) and *Time to synchronize* (TS).

complexity are compared. When EKF and UKF are applied for synchronization of IM, outliers (i.e. diverging trajectories) are observed. Comparing the computational complexity, for all the chaotic systems/maps considered, NPF has the lowest and PF has the most. EKF and UKF have moderate computational requirements. From the tables, comparing the time each scheme has taken for synchronization, it can be seen that the PF has the fastest convergence for the IM and MG system but for Lorenz system, UKF has the fastest convergence. NMSE and TNMSE studies of the IM reveals that these values for the PF based scheme is the smallest among the four algorithms. For Lorenz system, the NMSE and TNMSE performances of the UKF are found to be the lowest compared to other methods. In the case of MG, the NMSE and TNMSE performances of the UKF and PF are superior to the NPF based scheme at low SNRs. However, at high SNRs, performance of the NPF based scheme is slightly superior to the other schemes. In general, PF is found to be an appropriate method for the synchronization of the chaotic systems/maps despite its computational complexity. NPF is a very simple algorithm which can give performance close to the UKF and PF based schemes.

4.5 Conclusion

In this chapter, the NPF is proposed for synchronization of chaotic systems. There are many advantages with the NPF. It does not require the computation of the Jacobian. Other features of the NPF are: (*i*) the model error is assumed unknown and is estimated as a part of the solution, (*ii*) it uses a continuous model to determine the state estimates and hence avoids discrete state jumps, and (*iii*) there is no need to make Gaussianity assumption of the *a posterior* error. The performance of the proposed scheme is compared to the EKF, UKF and PF based schemes. The well known Lorenz and MG systems as well as IM are used for numerical evaluation. Performance measures such as NMSE, TNMSE and NISE are used for comparison. The main conclusions drawn from this study are as follows

- It is observed that for all the systems, the NPF based scheme has better synchronization properties over the EKF based scheme in terms of NMSE, TNMSE and

NISE.

- For the IM based communication scheme, due to the presence of hyperbolic tangencies, frequent divergence behaviour is observed when EKF is used for synchronization, especially in the low SNR cases. No such anomaly is observed in the case of NPF based scheme.

- When EKF and NPF are used to synchronize IM with different parameters at the transmitter and receiver, it is observed that the NPF is able to give much lower NMSE. For MG systems, when transmitter and the receiver have two different τ values, the NPF based scheme provides a very small NMSE which is dependent on the SNR, whereas the EKF based scheme fails to synchronize.

- Comparing the performance of NPF with the other filtering based schemes such as the UKF and PF, it has less computational complexity. While the synchronization time is comparatively higher for the NPF, the NMSE and TNMSE are on par with that of the UKF and PF.

Chapter 5

Dynamical Encoding using Symbolic Dynamics

5.1 Introduction

The sensitivity of chaotic systems/maps on its initial conditions and the parameters is used to introduce the security where the latter being used as the secret key. However, the applicability of conventional chaotic systems/maps in communication channels with significant noise and multi−path is limited. Symbolic dynamics (SD) is defined as the coarse−grain description of the chaotic dynamics and has been used for the analysis of chaotic systems [51]. SD based methods are shown to provide high quality synchronization.

Dynamical degradation[1] is one of the main concerns when a stream cipher is implemented on the digital computer [86]. In this chapter, a new self−synchronizing chaotic stream ciphers is proposed using the symbolic dynamics based synchronization. In the proposed system, the synchronization information is provided periodically. The theoretical and numerical BER performances for the new system is obtained. These results are compared with that of the binary phase shift keying (BPSK) and the CSK systems. Statistical tests are conducted to asses the security aspects of the proposed system. These

[1]When chaotic maps are implemented in digital computers, eventually all the trajectories become periodic due to the finite precision computations.

test results show that the proposed system has good statistical properties to qualify as a random bit generator which in turn emphasizes the system security. The system's sensitivity to the changes in parameters is also studied.

This chapter is organized as follows. In Section 5.2, the CSK scheme is introduced. A brief overview of SD and synchronization of chaotic maps using SD is given in Section 5.3. In Section 5.4, the proposed secure communication scheme is explained in detail. A theoretical expression for the upper bound of the BER is derived and is also presented in this section. Numerical results are discussed in Section 5.5 and this chapter is concluded with some remarks in Section 5.6.

5.2 Chaotic Shift Keying

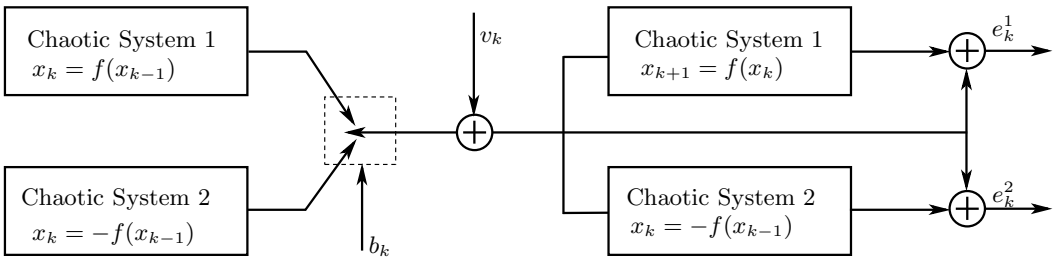


Figure 5.1: Chaotic shift keying scheme.

Figure 5.1 shows a CSK scheme. It is one of the earliest chaotic communication methods [87]. Most widely studied CSK system is the binary CSK in which two identical chaotic systems/maps are used at the transmitter and the receiver. Depending on the information bit ($b_k = \pm 1$), one of these chaotic systems is selected and the state variable corresponding to that system is transmitted. This state is corrupted by the channel noise, v_k, and is available at the receiver. The classical CSK receiver works on the assumption that chaotic systems can typically synchronize an identically driven version of themselves through a suitable coupling. In that case, the synchronized system results in a lower mean square error with the received signal. But due to the inability of the other system to synchronize with the driving system, the mean square error will be large. Hence, it is

easy to decode the information by simply looking at the magnitude of the mean square error. From Figure 5.1, if $f(x_k)$ is selected (say bit $+1$ is transmitted) the mean square error $\mathbb{E}[(e_k^1)^2]$ should be less than $\mathbb{E}[(e_k^2)^2]$ to decode the message correctly[2]. Otherwise, the bit is detected incorrectly.

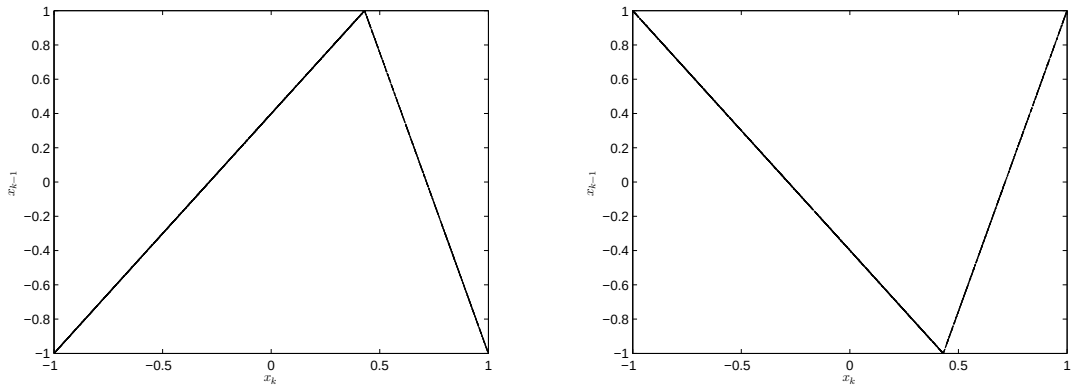
A *skewed tent map* and an *inverted skewed tent map* are used to obtain the two chaotic systems at the transmitter [88]. The skewed tent map is given by

$$x_{k+1} = f(x_k) = \begin{cases} \frac{2x_k+1-a}{a+1} & \text{for} \quad -1 \leq x_k \leq a \\ \frac{2x_k-1+a}{a-1} & \text{for} \quad a \leq x_k \leq 1 \end{cases}. \tag{5.1}$$

The inverted skewed tent map is given by

$$x_{k+1} = -f(x_k) = \begin{cases} \frac{a-2x_k-1}{a+1} & \text{for} \quad -1 \leq x_k \leq a \\ \frac{1-2x_k-a}{a-1} & \text{for} \quad a \leq x_k \leq 1 \end{cases}. \tag{5.2}$$

These maps are defined in the interval $[-1, +1]$. The state spaces of the above two maps



(a) (b)

Figure 5.2: Sate spaces of the skewed tent maps ($a = 0.43$): (a) skewed tent map and (b) inverted skewed tent map.

are shown in Figure 5.2. Exact copies of these maps are used at the receiver. However, the initial conditions are uncertain. To keep the phase continuity, at the transmitter, the last state of the map currently selected is used as the initial condition for the next bit duration.

[2]Here ergodicity of the chaotic dynamics is assumed.

5.3 Symbolic Dynamics

Symbolic dynamics is a coarse−grain description of the actual system dynamics [51]. It is being widely applied for the analysis of chaotic systems/maps. By partitioning a chaotic state−space into arbitrary regions, and labeling each region with a specific symbol, the trajectories can be converted to a sequence of symbols. This coarse−grain formulation of the system makes the deterministic nature of the dynamical system into a stochastic one. Hence, such systems can be treated as Markov systems, which have finite topological entropies.

Let the state−space ($\mathcal{S}$) of the iterated chaotic map[3] be partitioned into m disjoint regions, $\beta = \{\mathcal{C}\}_{i=1}^{m}$, such that $\mathcal{C}_i \cap \mathcal{C}_j = \emptyset$ for $i \neq j$ and $\cup_{i=1}^{m} \mathcal{C}_i = \mathcal{S}$. If one can assign m alphabets ($\mathbf{X} = [X_1, \ldots, X_m]$), one each to each of the disjoint regions, the dynamics of the system can be represented by a sequence of finite alphabet $\mathbf{X}$. This sequence is called the SD of the system/map. The entropy of the new information source is given by

$$H_n^{\beta} = -\sum_{\mathbf{Y}_n^i} P(\mathbf{Y}_n^i) \log P(\mathbf{Y}_n^i), \tag{5.3}$$

where $P(\mathbf{Y}_n^i)$ is the probability to find a code word $\mathbf{Y}_n^i$ of length n. The superscript i in Eq.(5.3) represents a specific combination of symbolic sequence. The summation is taken over all such possible sequences. The source entropy of a dynamical system is

$$h^{\beta} = \lim_{n\to\infty} h_n^{\beta} = \lim_{n\to\infty} \frac{1}{n} H_n^{\beta}. \tag{5.4}$$

The Kolmogorov−Sinai entropy of the system is defined as [89, Chapter 4]

$$h_{KS} = \sup_{\beta} h^{\beta}. \tag{5.5}$$

From the above discussions, it is clear that an iterated chaotic map is an information source with entropy h_{KS}.

[3]For a chaotic system, corresponding discrete−time map can be obtained by the Poincare return map.

5.3.1 SD of the Logistic Map

The *logistic map* [1] is one of the widely studied 1D maps; the dynamics of which is governed by

$$x_{k+1} = \mu x_k(1 - x_k), \tag{5.6}$$

where μ is a constant. For a range of values of μ, the logistic map has chaotic dynamics. In this study $\mu = 4$ is chosen for generating the map. The dynamics of logistic map is defined in $(0, 1)$. The state space representation and the partition to generate symbolic dynamics are shown in Figure 5.3. If $0 < x_k \leq 0.5$ symbol 0 is assigned and 1 is assigned if $0.5 < x_k < 1$.

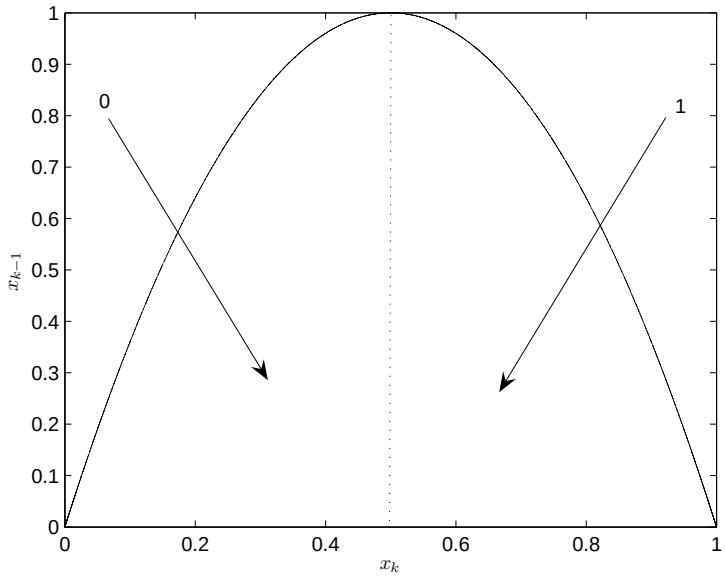


Figure 5.3: Generating partition of the logistic map.

5.3.2 Synchronization using SD

Using the tent map with binary partition, the SD−based synchronization can be explained [57]. Consider the chaotic map described by Eq.(5.1). Assume that there is no message transmitted and there is no channel noise. For an initial condition x_0, let $\mathcal{X} = [x_0, \ldots, x_{m-1}]$ be the fiducial trajectory generated by Eq.(5.1). Here a finite length trajectory is considered for simplicity. Let the corresponding binary trajectory be $\mathcal{X}_b$

of the same length (i.e. m) which is transmitted from the transmitter to the receiver. At the receiver, an exact copy of the same map is available; but the initial condition is unknown. The task is then to estimate the initial condition, x_0, using $\mathcal{X}_b$. Consider a sit-

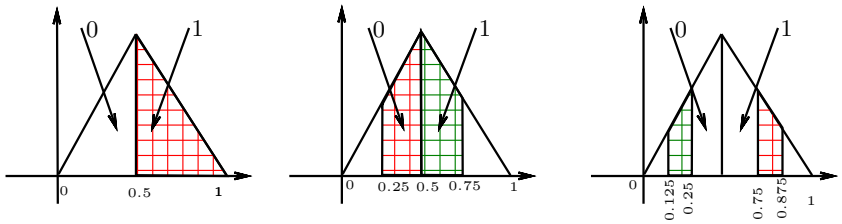


Figure 5.4: Synchronization using SD.

uation where only three bits are transmitted. From these three bits the initial condition x_0 needs to be estimated. Figure 5.4 shows this situation. A tent map with $A = 0.5$ is used for this illustration. The state space is partitioned into two. If x_k is between 0 and 0, then symbol 0 is assigned and symbol 1 is assigned otherwise. In this figure, shaded regions are the areas in which x_k may lie. Let $\mathcal{X}_b(0) = 1, \mathcal{X}_b(1) = 0$ and $\mathcal{X}_b(2) = 1$. If one has the knowledge only about $\mathcal{X}_b(2)$, he can conclude that x_2 lies in between 0.5 and 1. In Figure 5.4(b), the shaded area represents the pre-image of the interval $[0.5, 1)$ under the tent map[4]. Considering $\mathcal{X}_b(2)$ and $\mathcal{X}_b(1)$, a more accurate estimate about x_1 can be obtained, because if $\mathcal{X}_b(2) = 1$, x_1 should be either between 0.25 and 0.5 or between 0.5 and 1. However, $\mathcal{X}_b(1) = 0$ indicates that x_1 should be between 0 and 0.5. Taking this into account one can conclude that x_1 lies between 0.25 and 0.5. Here the estimation error reduced by half the amount from the previous step (Note that in the previous step, the variable of interest was x_2). Since three bits are available to estimate x_0, a more accurate estimate can be obtained using similar construction (Figure 5.4(c)). This implies, if m consecutive bits are considered for estimation, x_0 can be estimated with an estimation error less than $\frac{1}{2^m}$.

[4]Pre image of a set X for a particular iterative map is the set of points, Y, which are mapped to X when the map is applied on Y.

5.4 Dynamic Encoding

The schematic of the baseband representation of the proposed scheme is shown in Figure 5.5. The system has identical chaotic maps at the transmitter and the receiver. At the transmitter, using the initial condition x_0, the chaotic time series of length N is generated. This is then converted to corresponding symbolic sequences, $\mathcal{X}_b$. The filter block filters out the first m bits for representing the initial condition. The remaining $N-m$ bits are used to code the binary information signal $\mathcal{B}$ of length $N-m$. Using the cryptographic terminology, let $\mathcal{B}(k)$ be the plain text (the information that the transmitter wants to send), $\mathcal{X}_b(m+k)$ be the key (sequence generated from the chaotic map) and the $\mathcal{Y}_{msg}(k)$ (subscript msg means it contains the message) be the cypher text. The encryption can be done using the following operations.

$$\mathcal{Y}_{msg}(k) = \quad \mathcal{B}(k) \oplus \mathcal{X}_b(m+k), \quad \text{for } k = 0, \ldots, N-1-m. \tag{5.7}$$

where $\oplus$ is the XOR operation. The purpose of the shuffler block is to hide the bits conveying the initial condition $\mathcal{Y}_{init} = [\mathcal{X}_b(0), \ldots, \mathcal{X}_b(m-1)]$. The output is a binary sequence $\mathcal{Y}$ of length N. The format of the transmitted sequence is shown in Figure 5.6. The resultant sequence can be transmitted using conventional digital communication techniques such as the BPSK or quadrature phase shift keying (QPSK).

At the receiver, signal corrupted by AWGN (v_k) is available. Using conventional matched filter receiver, the transmitted sequence can be estimated as $\hat{\mathcal{Y}}$. The filter block at the receiver uses the knowledge about the way $\mathcal{Y}_{msg}$ is hidden to separate $\hat{\mathcal{Y}}_{msg}$ and $\hat{\mathcal{Y}}_{init}$ from the output of the matched filter. Using the synchronization method described in subsection 5.3.2, the synchronizer estimates the initial conditions $\hat{x}_0$. These initial conditions are used to reconstruct the symbolic sequence $\hat{\mathcal{X}}_b$. The information signal is then retrieved using the following equation:

$$\hat{\mathcal{B}}(k) = \quad \hat{\mathcal{Y}}_{msg}(k) \oplus \hat{\mathcal{X}}_b(m+k), \quad \text{for } k = 0, \ldots, N-1-m. \tag{5.8}$$

In order to decode these signals, the receiver should know three things– the chaotic map employed, the initial condition and the control parameter of the chaotic map. By selecting a new initial condition for each block transmission, large number of codes for

encryption can be derived. It is worth noting that chaotic maps are capable of generating i.i.d binary sequences [66] and hence the output sequence from the transmitter posses randomness.

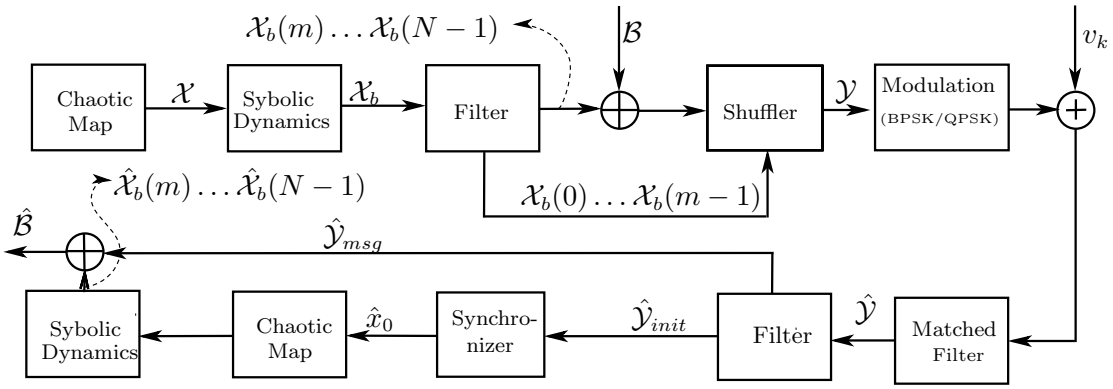


Figure 5.5: Proposed communication system.

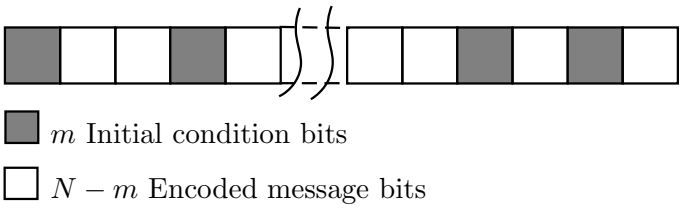


Figure 5.6: Format of the transmission sequence with interleaved initial condition.

5.4.1 Theoretical Upper Bound of the BER

It is clear from Figure 5.6 that there are two possibilities for the bit error to occur: (i) the decoding information may be wrong which causes a wrong estimation of the initial condition, and (ii) the detection of the message itself is wrong due to the noise.

To decode the message completely, all the m bits should be detected correctly. Let the BER of the BPSK system, p_b, be

$$p_b = Q\left(\sqrt{\frac{2E_b}{N_0}}\right), \tag{5.9}$$

where N_0 is the noise power and E_b is the bit energy. Hence, the probability of wrongly

detecting the sequence, p_s, is

$$p_s = 1 - (1 - p_b)^m. \tag{5.10}$$

Here, it is assumed that the symbolic alphabets are equiprobable. If a sequence is wrongly detected, then the probability of wrong decision about the transmitted message, p_d, which is given by

$$p_d = 0.5(1 - p_b). \tag{5.11}$$

The probability of error when the decoding information is wrong is given by

$$p_1 = p_d p_s = (1 - (1 - p_b)^m)\, p_d. \tag{5.12}$$

Considering the second situation, where the first m bits are decoded correctly and the message decoding is incorrect, the bit error probability is given by

$$p_2 = (1 - p_s)p_b. \tag{5.13}$$

Hence the total probability of error (BER) is given by

$$\begin{aligned} p &= p_1 + p_2 = (1 - (1 - p_b)^m)\, p_d + (1 - p_s)p_b \\ &= (1 - (1 - p_b)^m)\, 0.5(1 - p_b) + (1 - p_b)^m p_b \\ &= 0.5(1 - p_b) + (1 - p_b)^m (1.5p_b - 0.5). \end{aligned} \tag{5.14}$$

When the SNR is high, p_b is close to zero and hence $(1-p_b)^m \approx 1$. Then from Eq.(5.14), it can be clearly seen that the proposed system has a BER performance similar to that of the BPSK communication system.

5.5 Results and Discussion

5.5.1 BER Analysis

Extensive numerical simulations are carried out to assess the performance of the proposed secure communication system. Tent map, skewed tent map and logistic map are used for the generation of chaotic sequences. 10^5 bits are transmitted for each SNR values and

the corresponding BER is calculated. The experiments are carried out for simple AWGN and frequency selective channels.

The BER performance of the proposed system for the AWGN channel is presented in Figure 5.7. This performance is compared to that of the CSK and conventional BPSK schemes. As expected, at lower SNRs (here, SNR is defined as E_b/N_0), the BER of the proposed scheme is relatively high. For instance, at an SNR value of 4dB, the proposed method has a BER of 0.31 while CSK has a BER of 0.2 and BPSK has BER of 0.06. In order to estimate the initial condition accurately, all the m symbols should be detected correctly which is very unlikely in lower SNR values. However, when the BPSK achieves a BER of 10^{-3}, the BER performance of the proposed system starts following that of the BPSK. For example, at 12dB SNR, the proposed system has a BER of 4×10^{-4}. The corresponding BER values of BPSK and CSK systems are 10^{-4} and 8.2×10^{-3}, respectively. This trend is observed for all the maps used for the simulation. It is also interesting to note that even though the CSK based communication scheme has a slight performance advantage over the proposed system in low SNR regions, at high SNR values CSK is unable to provide fast BER decay. To see the asymptotic BER performances, the upper bound of BER [derived in Eq.(5.14)] is plotted in Figure 5.8 along with that of the BPSK system. It can be seen that when the SNR increases, the BER performance of the proposed method closely follows that of the BPSK system. Although, such high SNRs are possible only in theory, we can infer that the upper bound of BER of the proposed system can be brought to an arbitrarily small value by appropriate coding schemes.

To test the applicability of the proposed algorithm to other maps, the experiment is carried out for the skewed tent map and the logistic map. A similar behaviour is observed here also. For low SNR cases, the BER is relatively high. As the SNR increases, the BER curve of the proposed system closely follows that of the BPSK system. Some observations are in order. As the inverse of the logistic map requires a square root, finite precision algorithms can introduce approximation errors. In this experiment, initial conditions have less precision compared to the computer and hence after computing the estimate of the initial condition at the receiver, the high precision digits are discarded.

Most of the communication channels encountered in practice are band−limited and

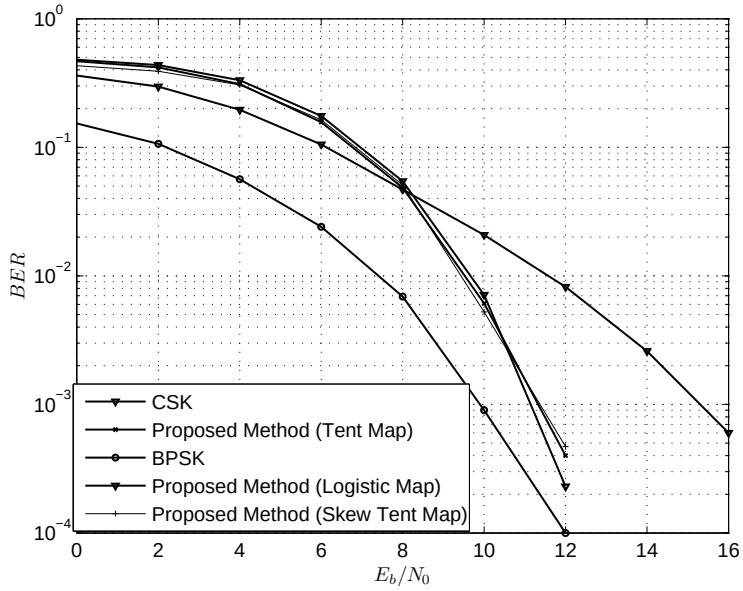


Figure 5.7: BER performance for AWGN channel.

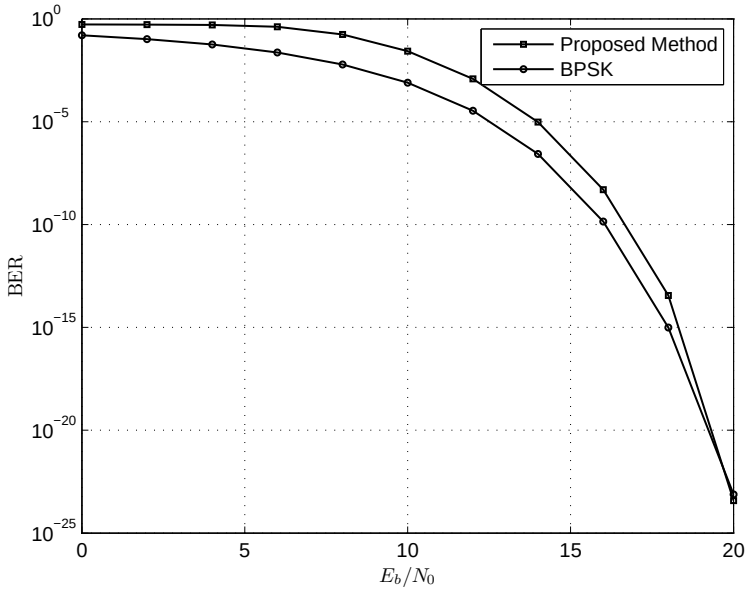


Figure 5.8: Theoretical BER curves of BPSK and the proposed method (AWGN channel).

frequency selective. To study the performance of the proposed system in such channels, another set of simulations is carried out. Two different channel models discussed in [90, Chapter 10] are considered. The first channel is a three−ray channel model with tap weights $[0.474, 0.815, 0.474]$ and the second channel is a five−ray channel with tap weights

$[0.227, 0.460, 0.688, 0.460, 0.227]$. At the receiver end, the maximum likelihood sequence estimation method (Viterbi Algoritm) is used to remove the inter symbol interference caused by the channel. Simulation results are presented in Figures 5.9 and 5.10. The proposed system behaves exactly as in the previous situation; at low SNRs it exhibit a high BER and as the SNR increases the BER closely follows the BER curve of the BPSK system. In the second channel condition as well, the proposed system has a fast BER decay which can be observed from Figure 5.10. In all the simulations, irrespective of the map used, BER curves have shown similar characteristics.

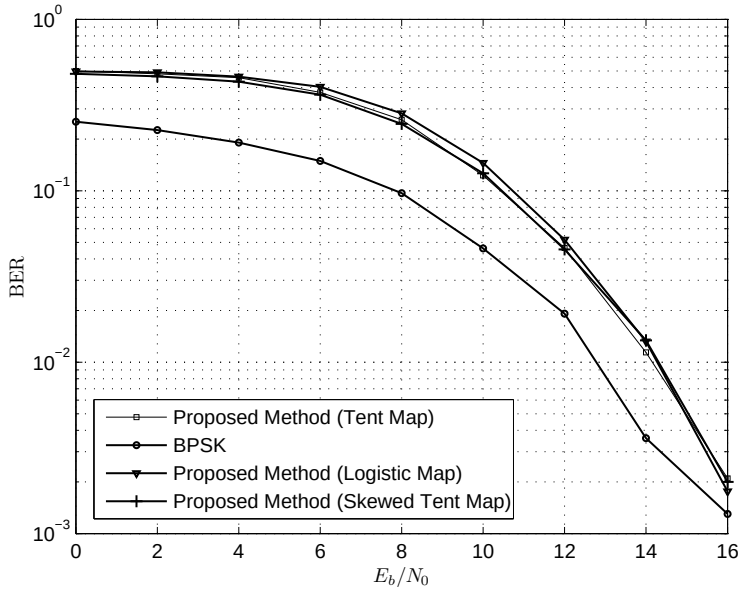


Figure 5.9: BER performance for band−limited channel (Channel model-I).

5.5.2 Security Analysis

There are three ways by which security can be introduced in the system. Here, the transmitter is first verified as source of the random bit sequence. Then, possible way to hide the initial condition is discussed. To study the security of the proposed scheme, the sensitivity of it to the control parameter variations is analyzed.

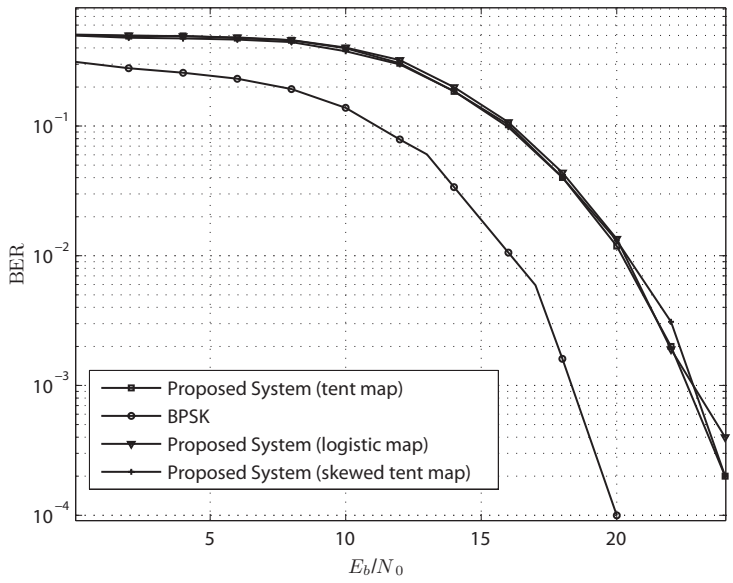


Figure 5.10: BER performance for band−limited channel (Channel model-II).

Randomness of the Output Generated by the Transmitter

For this method to work, the message should not posses any specific pattern. In other words, it should act like a random sequence. Statistical tests are conducted to asses the randomness of such an encryption method using the statistical testing suite developed in [91]. The results of the tests and the corresponding degrees of confidence are provided in Table I. It can be seen that the proposed system passes all the statistical tests[5] implying that the output of this system has good randomness property.

Diffusion of the bits carrying initial conditions

It is clear from the above discussions that the initial condition of the chaotic map should be available at the receiver in order to decode the message. One way to increase the security is to diffuse information about the initial condition in a random fashion which is known to the receiver *a priori*. This random pattern can be conveyed to the receiver *a priori* or can be transmitted through a dedicated (secure) channel. For example this pattern may be based on a linear feedback shift register (LFSR) where the initial state

[5]Test 12 has many P_{values} and hence it is omitted.

Table 5.1: Statistical Test Results

No	Test	P_{value}	Result
1	Frequency Test	0.042162	SUCCESS
2	Block Frequency Test	0.150647	SUCCESS
3	Run Test	0.455884	SUCCESS
4	Cumulative Sum Test	0.081931	SUCCESS
5	Fast Fourier Transform Test	0.602015	SUCCESS
6	Approximate Entropy Test	0.315695	SUCCESS
7	Linear Complexity Test	0.511244	SUCCESS
8	Longest Run of Ones Test	0.320249	SUCCESS
9	Overlapping Template Test	0.679082	SUCCESS
10	Rank Test	0.504374	SUCCESS
11	Universal Statistical Test	0.916838	SUCCESS
12	Non−periodic Template Test	–	SUCCESS
13	Serial Test	0.336143	SUCCESS

and the feedback connection can be conveyed to the receiver in a highly secure connection.

Precision

Other important parameter that can be used as the security feature is the precision at which the chaotic generators are operating. It also include the length of the number of bits (m) used to convey the initial conditions. In simulation studies, using proper software codes, it is possible to adjust the precision to any value up to the maximum value supported by the machine. If there is a slight error, the resulting trajectory would become completely uncorrelated and produce an entirely different sequence [1]. This prohibits the intruder to decode the message.

Knowledge of the chaotic map

Assume that the intruder somehow managed to extract the bits representing initial conditions and the precision at the initial condition is specified. Now the question that needs

to be answered is whether the intruder can decode the message. In order to decode the message, the knowledge of the chaotic map is essential. It is also very important that the communication system should be very sensitive to the changes in system parameters. Figure 5.11, the parameter *vs* the BER performance is plotted. Clearly, if the difference in parameter of the transmitter and receiver system is greater than 10^{-16}, the BER is high. If the parameter mismatch is below 10^{-16}, it can be seen that the intruder can decode the information easily as the BER is close to zero.

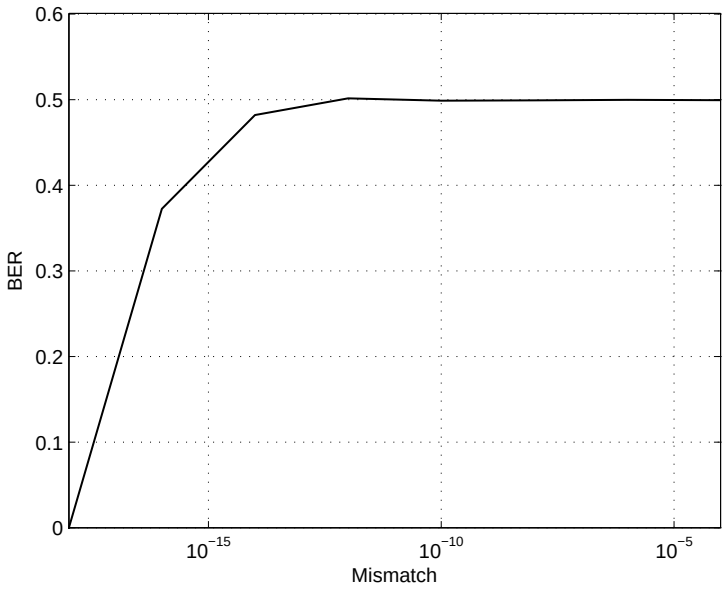


Figure 5.11: Parameter mismatch *vs* BER.

Figure 5.12 shows the performance of the proposed scheme under parameter mismatch. The parameter, A, of the transmitter tent map is set to 0.8. Assuming that the receiver guessed this value approximately (say, $A = 0.8 + 10^{-16}$), it is desirable to know if the intruder is able to decode the message. This slight parameter mismatch makes the receiver incapable of reconstructing the chaotic trajectory used generated at the transmitter causing the receiver BER to remain at a high value. For a visual demonstration of this effect, a picture[6](shown in Figure5.13(a)) is transmitted from the transmitter after encryption. Figure 5.13 (b) is the decrypted signal when the receiver has the correct

[6]This particular portrait of Sir Isaac Newton is taken from http://en.wikipedia.org/wiki/Isaac_Newton. This image is in the *public domain*.

knowledge of the parameter. Figure 5.13 (c) is the decrypted message corresponding to the use of wrongly guessed encryption key. It is clearly seen that the slight parameter mismatch makes the receiver incapable of decoding the information correctly.

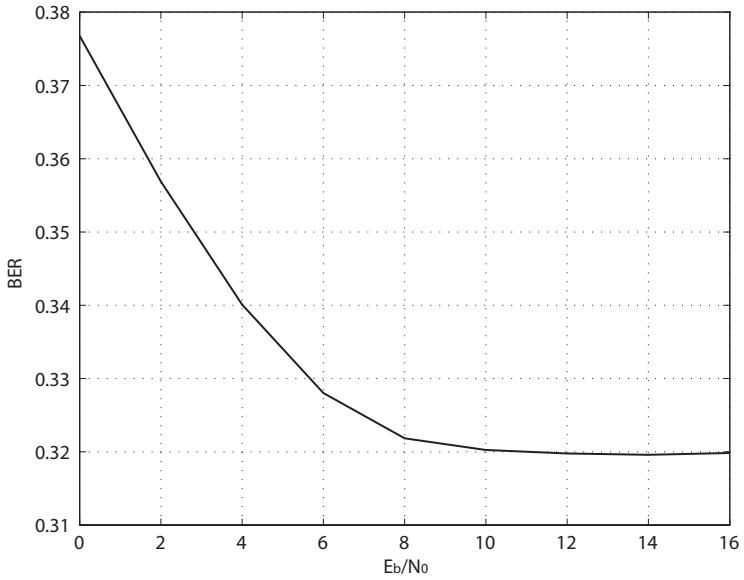


Figure 5.12: BER performance under parameter mismatch.

Figure 5.13: (a) Original image (b) Receiver uses $A = 0.8$ (c) Receiver uses $A = 0.8 + 10^{-16}$.

If one try to break the proposed system with brute force attack (i.e. trying each parameter) he has to explore only 10^{16} values. This in fact can lead to a low security. To improve the security, the method suggested in [92] can be used. Here, multiple chaotic systems are used for the generation of the sequence used for encryption. Transmitter

and the receiver schematic of the new system is shown in Figure 5.15(a) and Figure 5.15(b), respectively. At the transmitter there are L number of chaotic maps. Each of them are initialized with $x_0^1, \ldots, x_0^L$ and has control parameter $A^1, \ldots, A^L$. Initial conditions $x_0^2, \ldots, x_0^L$ holds some deterministic relationships with x_0^1. After converting to its corresponding symbolic sequences, first m bits of each sequence is discarded. A bit–wise XOR is done on the resultant sequence to produce a single stream of length $N - m$. Shuffler mixes first m bit generated by the first chaotic map to get $\mathcal{Y}$. Since there is a relationship between x_0^1 and the other initial conditions, the other values can be computed at the receiver.

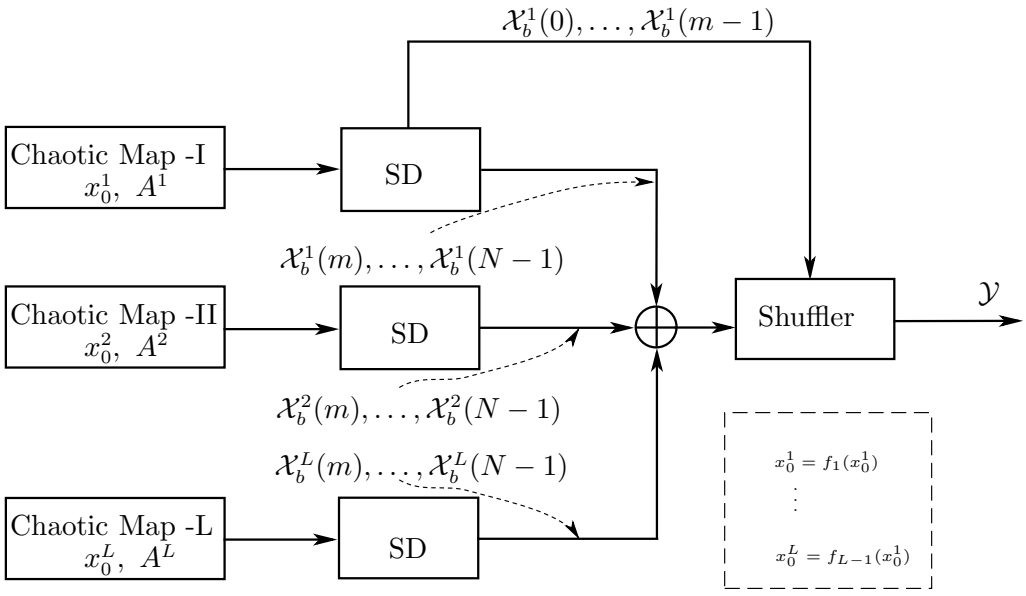


Figure 5.14: Schematic of the modified transmitter.

Since the current key space is $[A^1, \ldots, A^L]$, to do a brute force attack the intruder has to search for 10^{16L} values. By adjusting the L a balance can be achieved between the required computational complexity and the security. Note that, the synchronizer need to estimate only one initial condition and hence, the computational burden does not increase significantly at the receiver when L become larger. In addition to this, the relationship between the initial conditions also can be used as a secret to improve the security.

From the above discussion it is clear that the proposed system assures certain level

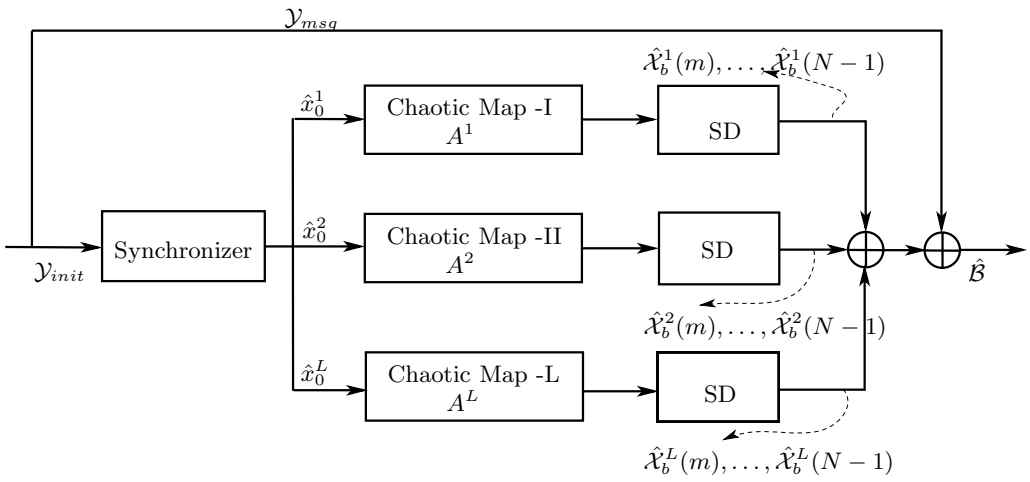


Figure 5.15: Schematic of the modified receiver.

of security which is ideal for places where moderate security is needed. This system can be used in applications such as remote keyless entry system, video phone, and wireless telephone etc. [93].

5.6 Conclusion

Synchronization of chaotic systems is an important step in implementing chaotic communication schemes. Especially in noisy environment, the application of SD to synchronize chaotic systems is proved to be a good choice. In this work, using SD of the chaotic maps, a new chaotic communication scheme is proposed. The information is dynamically encoded using 1D iterated chaotic maps. The proposed method is tested for different maps like tent map, skewed tent map and logistic maps. BER performance of the proposed scheme is analyzed analytically and numerically. It is found that the BER of the proposed communication scheme is comparable to that of the BPSK at moderately high SNR. Overhead needed for the proposed communication scheme is very minimal. Statistical tests reveal that the proposed system qualifies as random binary source. The sensitivity of the proposed system is also analyzed. This in effect emphasizes the security of the proposed communication system.

Chapter 6

Spread Spectrum Communication System using Ikeda Map

6.1 Introduction

In the last several years, increasing efforts have been devoted to study the possibility of using chaotic dynamics to enhance the features of communication systems [10]-[11]. Chaos-based communication systems qualify as broadband systems in which the natural spectrum of the information signal is spread over a very large bandwidth. This class of systems are called spread spectrum (SS) communication systems since they make use of a much higher bandwidth than that of the data bandwidth to transmit the information. Among many SS communication schemes, investigations on wireless personal and computer networks have recently addressed SS systems with direct sequence (DS) approach, where users are multiplexed by orthogonal (or nearly orthogonal) spreading sequences [94].

In this chapter, a new DS/SS communication scheme is proposed. Time series obtained from 2D IM is used to generate the spreading sequences. The BER performance of the proposed scheme is compared with that of the conventional Gold sequence BPSK schemes with the help of computer simulations. Results show that the proposed system has a noticeable improvement in BER performance in low signal to noise ratios (SNRs).

In Section 6.2 the transmitter and the receiver structure of the proposed system is

detailed. Spreading code generation from the IM is described in Section 6.3. Performance of the proposed system under different channel conditions are analyzed in Section 6.4. Some concluding remarks are provided in Section 6.5.

6.2 System Model

In this section, the system model of the proposed (double spreading DS/SS) system is described in detail.

6.2.1 Transmitter

Consider a CDMA system with N number of active users. The transmitter model for the proposed chaotic communication system of the n^{th} user is illustrated in Figure 6.1. The block diagram of the transmitter in pass band is given in Figure 6.1(a) and the complex spreading operation is shown in Figure 6.1(b). The data is double spread and it is transmitted using quadrature modulation system. Here, double spreading means the information signal is spread using two separatespreading sequence and transmitted using the inphase and quadrature phase components of the QPSK system. For the above coded binary double spreading DS/SS scheme, the transmitted signal of the n^{th} user is given by

$$s^n(t) = A^n b^n(t) c^n(t) \cos(\omega_c t + \theta^n) \tag{6.1}$$

where A^n is the amplitude of the transmitted signal for the n^{th} user, $b^n(t)$ is the phase encoded information signal, $c^n(t)$ is the complex spreading waveform derived from the IM ω_c is the carrier frequency, and θ^n is the carrier phase. Further, $\Re[c^n(t)]$ and $\Im[c^n(t)]$ in Figure 6.1(b) are the real and imaginary parts, respectively, of the complex spreading signal $c^n(t)$, which is given by

$$c^n(t) = \sum_{k=-\infty}^{\infty} c_k^n p_{T_c}(t - kT_c), \tag{6.2}$$

where $\{c_k^n\} \in \{\pm 1, \pm\sqrt{-1}\}$ is the chip of complex spreading sequence $\mathbf{c}^n$ of length N_s (processing gain). $p_{T_c}(t)$ is the rectangular pulse shaping function given by

$$p_{T_c}(t) = \begin{cases} 1, & 0 < t < T_c \\ 0, & \text{otherwise} \end{cases}, \tag{6.3}$$

and T_c is the chip duration. We assume that each code symbol is spread with N_s chips, i.e. $T_b = N_s T_c$, where T_b is the bit duration. The encoded information signal can be expressed as

$$b^n(t) = \sum_{k=-\infty}^{\infty} b_k^n p_{T_b}(t - kT_b), \tag{6.4}$$

where $\{b_k^n\} \in \{\pm 1\}$ is the information symbol sequence generated by the encoder, and $p_{T_b}(t)$ is the rectangular pulse shaping function similar to $p_{T_c}(t)$.

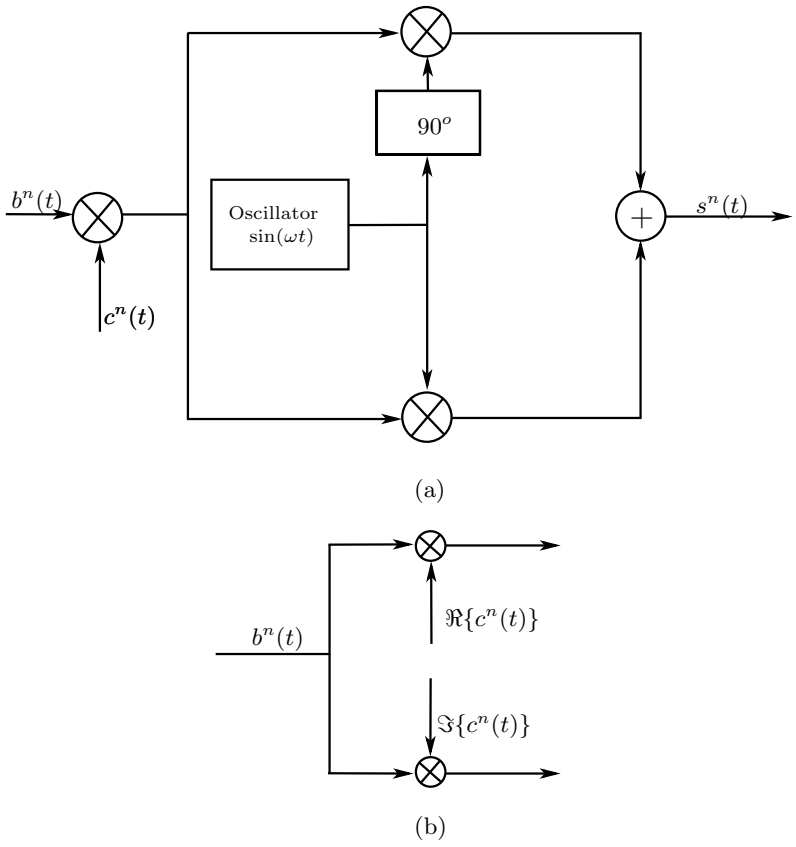


Figure 6.1: Transmitter model for the n^{th} user in the proposed chaotic communication system: (a) passband transmitter model, (b) complex spreading.

6.2.2 Receiver

In general, the received signal $r(t)$ can be expressed as

$$r(t) = \sum_{n=1}^{N} s^n(t - \tau^n) + \nu'(t) \tag{6.5}$$

where τ^n is the sequence delay for each user and $\nu'(t)$ is the complex AWGN. In a synchronous system, τ^n can be set to zero without loss of generality. For asynchronous system, τ^n can take any value between 0 and $T_c N_s$. The receiver model for the proposed

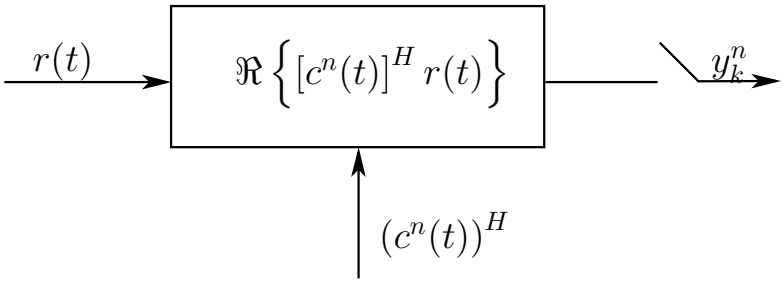


Figure 6.2: Receiver model for the n^{th} user in the proposed chaotic communication system.

chaotic communication system (for n^{th} user) is illustrated in Figure 6.2. At the receiver end, the de–spreading is performed by taking the dot product of the received signal with $(c^n(t))$ of the spreading sequence. The resultant signal is given by

$$\begin{aligned}
\hat{y}(t) &= [c^n(t)]^H r(t) \\
&= \left[\Re\{c^n(t)\}^T - \sqrt{-1}\Im\{c^n(t)\}^T\right]\left[\Re\{r(t)\} + \sqrt{-1}\Im\{r(t)\}\right] \\
&= \Re\{c^n(t)\}^T \Re\{r(t)\} + \Im\{c^n(t)\}^T \Im\{r(t)\} + \\
&\quad \sqrt{-1}\left[\Re\{c^n(t)\}^T \Im\{r(t)\} - \Im\{c^n(t)\}^T \Re\{r(t)\}\right]
\end{aligned} \tag{6.6}$$

The cross correlation between the real and imaginary part of the spreading code is close to zero, the imaginary part does not contain much bit energy. Hence only real part alone is considered for the detection purpose. After sampling at an interval T, the received signal, y_k^n, for n^{th} user can be written as

$$y_k^n = 2A^n b_k^n + \sum_{l=1, l\neq n}^{N} A^l(\rho^{R,l} + \rho^{I,l}) b_k^l + \nu_k, \tag{6.7}$$

where ν_k is the noise term due to the de–spreading. A synchronous channel with perfect sequence acquisition for the desired user is assumed for the analysis.

From Eq.(6.7), it can be seen that the multiple access interference (MAI) term has two cross–correlation terms $\rho^{R,l}$ and $\rho^{I,l}$ corresponding to the real and imaginary part of the spreading sequence. If these terms are opposite in sign, the sum, $\rho^{R,l} + \rho^{I,l}$, can be made smaller than the individual values. This property of the cross–correlation terms is utilized for the MAI cancelation. Since the spreading sequences are generated using the chaotic IM, with different initial conditions, a large number of sequences with the above mentioned property can be identified and used.

6.3 Spreading Sequence Generation

The performance of DS/SS system depends primarily on the code properties and hence there has been increasing effort to obtain spreading sequences with good cross-correlation and auto−correlation properties [59, 94]. There are two broad class of spreading sequences which can be found in the current literature. They are: (i) PN sequence generated from linear shift registers (LFSR) such as m–sequences and Gold sequences, and (ii) sequence generated from ergodic maps.

6.3.1 m- Sequences and Gold Sequences

Conventional DS/SS systems are based on the PN sequences such as m-sequences (maximum length sequences) and Gold sequences. The m- sequences can be generated from LFSRs using the modulo-2 arithmetic [94]. A primitive polynomial of degree r is used to get the maximum length sequence of period $2^r - 1$. If a pair of m-sequences called $preferred\ pair$, is selected and modulo-2 addition of these two sequences and their phase shifts are performed, it will result in a new set of sequences which are called Gold sequences [95]. Other sequences like Walsh sequences, Kasami sequences *etc.* are also in use [59].

6.3.2 Design of Spreading Sequence with Iterated Chaotic Maps

In this section, details of the generation of binary spreading sequences from iterated chaotic maps are described. IM [Eq.(2.14)] is such a chaotic map and is used in generating complex−valued spreading sequences in the proposed communication system.

6.3.3 Spreading Codes from IM

To construct chaotic spreading sequences for the proposed communication system, Eq.(2.14) is used with initial conditions x_0^R and x_0^I. Repeated application of the map generates two sequences x_k^R and x_k^I. The real and imaginary parts of the chaotic spreading sequences $\Re[\mathbf{c}^n]$ and $\Im[\mathbf{c}^n]$ of length N_s for the n^{th} user can be obtained from the values of x_k^R and x_k^I in the following way:

$$\Re[\mathbf{c}^n] = sgn\{\mathbf{x}^{R,n} - \bar{\mathbf{x}}^{R,n}\} \text{ and } \Im[\mathbf{c}^n] = sgn\{\mathbf{x}^{I,n} - \bar{\mathbf{x}}^{I,n}\}, \tag{6.8}$$

where $\mathbf{x}^{R,n}$ and $\mathbf{x}^{I,n}$ are vectors (formed from x_k^R and x_k^I) of length N_s, and $\bar{\mathbf{x}}^{R,n}$ and $\bar{\mathbf{x}}^{I,n}$ are the average of these spreading sequences, respectively. The complex spreading sequence is then constructed as $\mathbf{c}^n = \mathbf{c}^{R,n} + \sqrt{-1}\mathbf{c}^{I,n}$.

6.3.4 Optimum Selection of IM based Spreading Sequences

In this section, a detailed description of the method adopted for doing optimal selection of spreading sequences from a large number of sequences generated using Eqs.(2.14) and (6.8) is given. From a large group of sequences, a set of sequences (of length $N_s = 31$) with better correlation properties are selected. Since a synchronous model with single user correlator detector is analyzed, only the periodic cross–correlation properties of the spreading sequences are considered [96]. The normalized periodic discrete cross-correlation at a shift (τ) between the real part of n^{th} and m^{th} users' spreading sequences is defined as

$$\rho_\tau^{n,m} = \frac{1}{N_s - \tau} \sum_{k=0}^{N_s-\tau} c_k^{R,n} c_{k+\tau}^{R,m}. \tag{6.9}$$

The cross-correlation for the imaginary part of the spreading sequence can be defined in a similar way.

Pursley [96] showed that it is possible to express the average SNR at the receiver output of a DS/SS system for the n^{th} user as a function of the cross–correlation parameter $\rho^{n,m}$ and the power of AWGN present in the channel (N_0); where n is the desired user, and the other user are $m = 1, \ldots, N, m \neq n$. Hence, we use the cross–correlation parameter $\rho^{n,m}$ ($i.e.$value of $\rho_\tau^{n,m}$ at $\tau = 0$) as the criteria in choosing the desired number (N) of spreading sequences from a large pool of sequences.

From a large pool of quadrature phase and in−phase sequences, two sequences are selected randomly which forms the first in−phase and quadrature phase spreading sequences. Cross-correlation between these sequences and rest of the sequences are calculated. Sequences with negative and positive correlation values are grouped and then sorted. The sequences with lowest cross-correlation values from each group are selected as the next pair of complex sequence. These steps are repeated until the required number of sequences are obtained.

6.4 Results and Discussion

Computer simulations are carried out to evaluate the performance of a 31 chip IM based double spreading scheme under different channel conditions. The BER performance of the new system is compared with the 31 chip as well as the 63 chip Gold sequence based BPSK systems. Since the proposed scheme uses the same amount of bandwidth as the 63 chip Gold sequence based BPSK system, comparison between the 31 chip IM based double spreading system and 63 chip Gold sequence based BPSK system is justified. A DS/SS communication system with 9 active users is considered for the simulation. Four samples per chip and no perfect power control at the transmitter is assumed. The SNR is varied from 0 to 14 dB for plotting the BER curves. For each SNR, individual BER of each user is averaged in order to get the performance figure. The simulations are conducted for synchronous (AWGN), asynchronous (AWGN), asynchronous fading, and selective fading channel conditions.

6.4.1 Synchronous System

Figure 6.3 shows the BER performance of the proposed synchronous DS/SS system with IM spreading sequences (31 chip) and the conventional system with the Gold sequence (31 and 63 chip) under AWGN. From this figure, it is very clear that the proposed scheme significantly outperforms the conventional Gold sequence systems. The 63 chip Gold sequence system requires a SNR of 10dB to achieve a BER of 10^{-3}, while the proposed system needs only 8dB. This merit figure is dominant in all SNR values and especially at low SNRs (Here also SNR is defined as E_b/N_0, where E_b is the bit energy and N_0 is the variance of the additive noise).

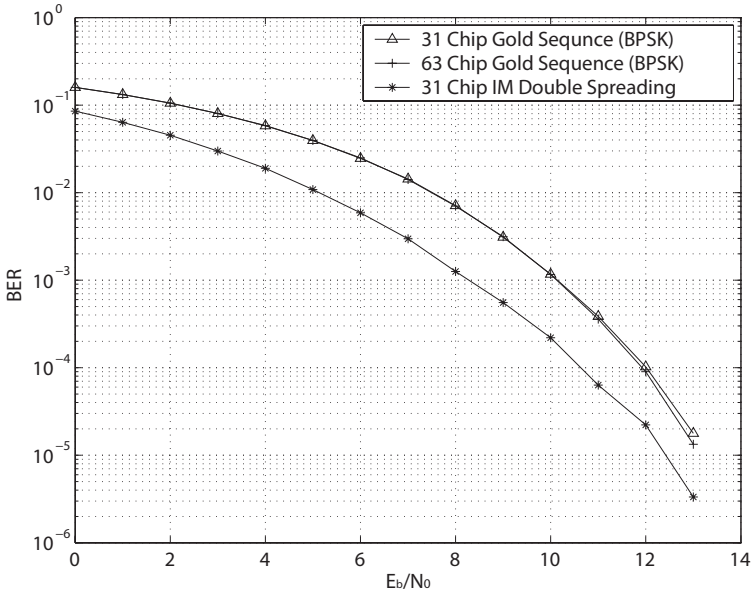


Figure 6.3: BER curves under AWGN channel (Synchronous).

6.4.2 Asynchronous System

It is known that the uplink of a wireless communication system is essentially asynchronous. Hence, the performances of the proposed system have to be evaluated under asynchronous channel conditions. In this section, the BER performance of the proposed system is compared with the other two systems in asynchronous channel, Rayleigh fading channel and selective fading channel conditions. The delay, τ^n, of each user except the desired user is made to vary uniformly between 0 to $4 \times N_s$. The simulation is carried

out and the results are presented in Figs. 6.4, 6.5 and 6.6, respectively for asynchronous case, Rayleigh fading channel, and selective fading channels.

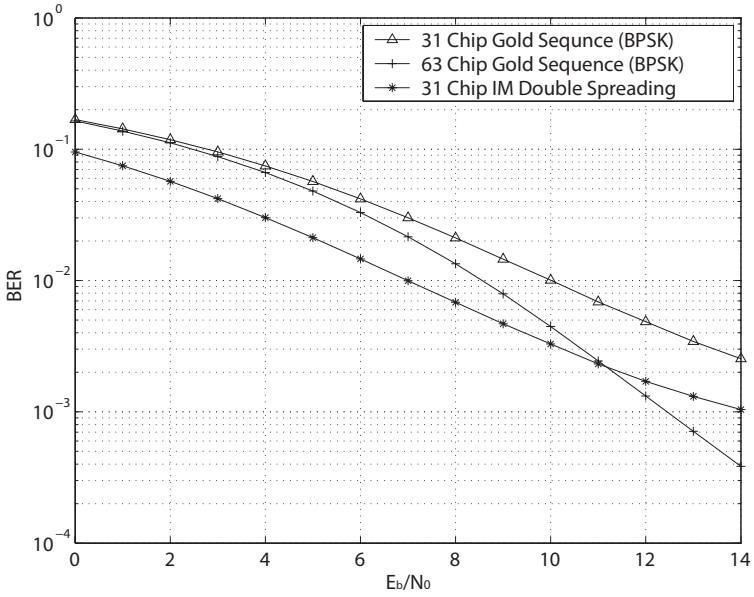


Figure 6.4: BER curves under AWGN channel (Asynchronous).

The BER performance of the proposed system is compared with the other two systems where all the parameters are kept unchanged as in the first experiment. However, the users except the desired user are delayed by τ^n (uniformly between 0 to $4 \times N_s$) amount. From Figure 6.4, it can be seen that, the proposed scheme achieves better BER performance in low SNR with almost 2dB improvement. We also observe a crossing of the BER curves of the new scheme with the 63 chip Gold code scheme at 11dB. Although the performance of 63 chip Gold sequence BPSK system is better than the proposed system at SNR greater than 11dB, the performance of the proposed scheme is noticeable in low SNRs. A comparison with 31 chip Gold sequence based BPSK system reveals that the new scheme is superior for all SNR values.

Asynchronous fading case is considered in this particular simulation. Rayleigh fading occurs in a wireless transmission system where there is no direct signal component due to line of sight. To determine the system performance under Rayleigh fading channel, it is assumed that the transmitted signal propagates through Rayleigh faded radio channel with unity power [97]. Transmission is asynchronous and each user is undergoing

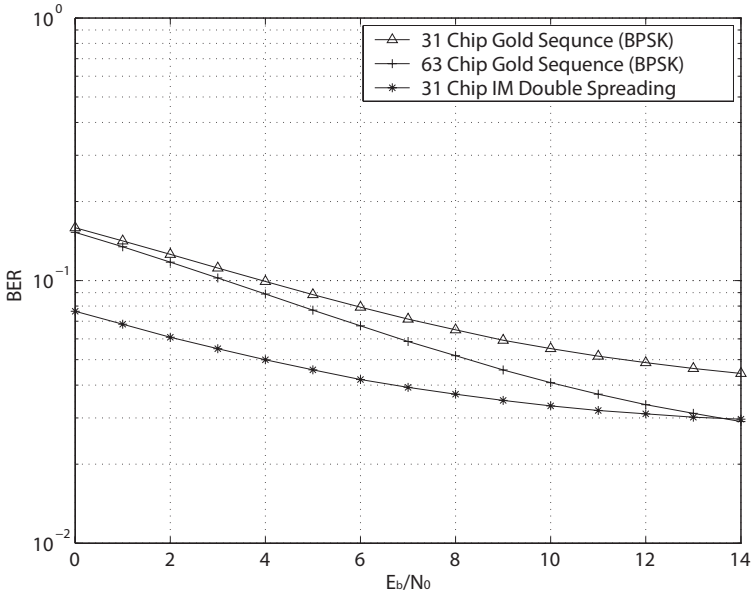


Figure 6.5: BER curves under Rayleigh fading channel (Asynchronous).

independent fading. Results are shown in Figure 6.5. Here also it can be observed that the new scheme outperform the conventional schemes at low SNR. The improvement is almost 5dB around 0dB SNR. It can be observed that the proposed scheme is superior to the 31 chip BPSK system almost everywhere.

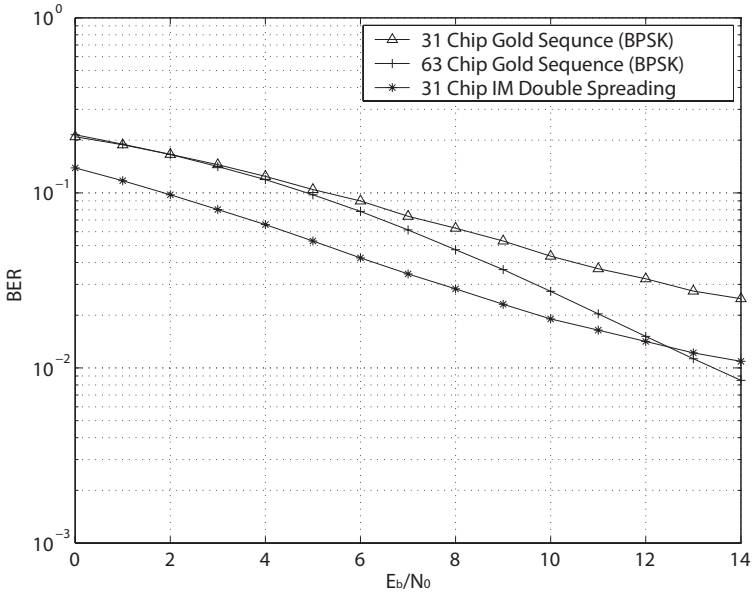


Figure 6.6: BER curves under selective fading channel (Asynchronous).

Next, performance of the new scheme in multi-path channel conditions are evaluated next. It is known that a RAKE receiver can be used in multi-path situations to improve the performance of DS/SS system [98]. Three ray channel with exponential delay profile was considered. Again the users are asynchronous and Rayleigh fading is assumed in all the individual paths. The BER performance curve for the proposed system and other conventional systems are presented in Figure 6.6. It can be seen that in low SNRs, the proposed scheme outperforms the conventional schemes. When we compare 31 chip Gold sequence and the proposed system, a huge difference in performance can be observed. As in the previous figures there is a crossing of BER curves of proposed schemes and that of 63 chip Gold code scheme at 13dB.

From all these simulation results, it can be seen that the proposed system performance is much better than the conventional Gold sequence system, in general. In asynchronous case, the performance improvement is very good in low SNR situations while in synchronous case, proposed system considerably outperforms the conventional systems for all SNR values. In synchronous case, the low bit error rate is attributed to the opposite sign of MAI generated by the in phase and quadrature components. But in all the other cases, it can be easily shown that the proposed system sends the same information through two nearly uncorrelated channels. At the receiver, the output of these two channels are combined and then the decision is made. This is in deed similar to the diversity combining popularly used in digital communication systems [90, Chapter 14]. The improved BER performances of the new scheme is attributed to the diversity combining gain.

6.5 Conclusion

In this chapter, a novel DS/SS communication system is proposed. This scheme exploits the 2-D complex valued chaotic IM as the spreading sequences. The performance analysis of the proposed scheme is evaluated numerically. The property of having opposite sign in the cross–correlation values of the real and imaginary components of the complex spreading sequence is utilized for the MAI cancelation. Such sequences are selected optimally from a large set of complex sequences. A detailed description of the systematic procedure

that is adopted to generate the IM based spreading sequences is presented. From the simulation results, it is observed that the performance of the proposed system is superior to that of the conventional system (with Gold sequence) under different channel conditions. Specifically in synchronous case, better performance can be observed everywhere while in all asynchronous situations, a noticeable improvement is achieved at relatively low SNRs.

Chapter 7

Conclusion

Perhaps the most important lesson to be drawn from the study of nonlinear dynamical systems over the past few decades is that even simple dynamical systems can give rise to complex behavior (chaos) which is statistically indistinguishable from that produced by a complex random process. Sensitive dependence on initial conditions is the most defining characteristic of such chaotic systems. A distinct property of a chaotic process is its long-term unpredictability. In mathematical terms, this property is referred to as the sensitive dependence on initial conditions. A simple way to demonstrate this property is to operate 2−D chaotic processes from slightly different initial conditions. Although the two systems retain the same attractor pattern and chaotic invariants, they soon diverge from each other.

Recently, the concept of communications using chaos has been widely explored. Chaotic waveforms and sequences have many characteristics that are of interest in communications, namely, *wide-band power spectra, noise-like appearance, high complexity* and *low cross−correlation*. Recent research in chaos has caught the attention of communication system designers and developers as it promises to provide significant improvements over the current systems in the all aspects mentioned above. The primary aim of implementing chaos in communication systems is to increase the security of the transmitted message. Unless the receivers have the keys (exact initial conditions and the parameters), it would be almost impossible to intercept or decode the messages.

In this thesis, application of chaotic systems/maps for communications is explored.

The objectives of this study are: (*i*) to analyze the divergence behavior of the EKF based synchronization scheme when it is applied to the IM, (*ii*) to develop stable synchronization methods such as the UKF, PF and NPF, (*iii*) to apply SD to develop new chaotic digital communication systems which is multi−path resistant, and (*iv*) to generate spreading codes from complex chaotic systems such as the IM and analyze the performance of such codes for different chaotic modulation schemes.

7.1 Chaotic Synchronization

Chaotic systems/maps have potential applications in secure communications due to their wide−band nature. There are many forms of chaotic communication systems. The main difficulty in implementing chaotic communication systems is the synchronization of the transmitter and the receiver systems. This task will be even more formidable when the channel and the measurement noises are present in the system. Stochastic methods are applied to synchronize such systems. Nonlinear filters come as a handy tool in chaotic synchronization due to their similarity with coupled synchronization. In this thesis, first, the EKF based synchronization is analyzed in detail for the synchronization of chaotic maps with NCAs such as IM. It is found that, in simple AWGN channels, the system fails to synchronize due to the presence of such tangencies. In order to mitigate this issue as well as to get better synchronization error characteristics, other nonlinear filtering methods such as the UKF, PF and NPF are analyzed. The well known chaotic systems such as Lorenz and MG systems as well as IM are used for performance evaluation.

7.1.1 Performance of the UKF and PF

The EKF is one of the most widely investigated stochastic filtering methods for chaotic synchronization. However, for highly nonlinear systems, the EKF introduces approximation errors causing unacceptable degradation in the system performance. UKF has the advantage that it has better approximation capabilities than EKF. Instead of approximating the nonlinear function, it tries to approximate the *posterior* density itself using a UT of the random variable. PF are nonlinear filters capable of approximating any kind

of *posterior* density. It uses the MC simulations for approximating the density. Since there are no Gaussianity assumption about the *posterior* density, these filters are capable of evaluating any densities. To get a faster and accurate synchronization, UKF and PF based schemes are proposed and analyzed. Performance indices such as NISE, NMSE and TNMSE are used to evaluate the performance of the proposed algorithm. The main conclusions drawn from this study are as follows

- For all the chaotic systems/maps studied, PF and UKF are able to give a fast and accurate synchronization.
- For IM, the PF based scheme has additional advantage that no diverging trajectories are observed.
- For proper operation of the PF based scheme, the particles should be diverse (sampled from all the parts of the state space). However, this fails when the PF is applied to the synchronization of the Lorenz and MG systems. Hence, the synchronization error is relatively higher.

7.1.2 Performance of NPF

One of the widely studied nonlinear filtering method which does not need the Gaussianity assumption of the noise is the NPF. One of the main advantages of NPF is its simplicity when it is used for synchronization of chaotic systems. If properly designed, for NPF, the approximation of chaotic nonlinearity is not required. Secondly, this method does not need the computation of the Jacobian. Other advantages of the NPF are: (*i*) the model error is assumed to be unknown and is estimated as a part of the solution, (*ii*) it uses a continuous model to determine the state estimates and hence avoids discrete state jumps, and (*iii*) there is no need to make Gaussianity assumption of the *a posterior* error. The following conclusions can be drawn from the study.

- In all the simulations, the NPF based scheme gives a better error characteristics (low values of NMSE and TNMSE).
- It also has faster convergence compared to the EKF based scheme.

- Moreover, unlike in the EKF, no diverging trajectories are observed when NPF is applied to the IM.

- Comparing the performance of NPF with the other filtering based schemes such as the UKF and PF, it has lesser computational complexity. While NISE is comparatively higher for the NPF, the NMSE and TNMSE are on par with that of the UKF and PF.

From these extensive studies, it can be concluded that the NPF is an ideal candidate for synchronization of chaotic systems/maps with low computational requirement and comparable mean square error performance (with UKF and PF). If faster synchronization is needed, one can advice the use of either UKF or PF though their computational complexity is higher compared to the NPF.

7.2 Application of SD to Communications

Synchronization of chaotic systems by the application of SD has the advantage that it provides a high quality synchronization. Using SD of the chaotic maps, a new scheme for secure communication is proposed in this thesis. The information is dynamically encoded using 1D iterated chaotic maps. BER performance of the proposed scheme is analyzed analytically and numerically. It is found that, at moderate SNRs, the proposed system has BER performance that is similar to that of the conventional BPSK system and is superior to that offered by the CSK communication scheme. Unlike CSK, the proposed system demonstrated a better multi−path resistance. Statistical tests also reveal that the proposed system qualifies as a random binary source. This in effect emphasizes the security of the proposed communication system.

7.3 IM based DS/SS Communication System

An important quality of chaotic systems is its ability to generate information. This led the researchers to apply chaotic time series for spread spectrum communication applications. In this thesis, a novel DS/SS communication system is proposed. This scheme exploits

the 2D complex valued chaotic IM as the spreading sequences. The performance analysis of the proposed scheme is evaluated numerically. The property of having opposite sign in the cross–correlation values of the real and imaginary components of the complex spreading sequence is utilized for achieving MAI cancelation. The new system has very low BER compared to the Gold code system with same bandwidth in synchronous AWGN multiuser case. In the case of asynchronous and fading cases, at low SNRs, the proposed system has a superior performance compared to the conventional system with Gold code as the spreading sequence.

7.4 Future Directions

1. So far all the synchronization aspects are studied in a point to point communication systems. It would be of great practical use to see how this synchronization methods perform in multiuser environment.

2. In all the synchronization schemes discussed in this thesis, only one state of the chaotic systems/maps is used for the synchronization. However, Taken's embedding theorem states that one can reconstruct the entire state space with a proper delay embedding. A future work would be to use this theorem to develop synchronization schemes and analyze their performance.

3. In this thesis, SD of $1-$D maps are explored for secure digital communication applications. However, as a future work, one could investigate the possibilities of using the SD of higher dimensional maps to develop better secure communication schemes.

4. Recent developments have highlighted that a statistical approach may greatly benefit the study of correlation properties of discrete$-$time chaotic systems (maps). In order to fully exploit the potential of chaotic systems in the field of communication, it is required to evaluate the statistical properties of chaotic sequences. This will lead to a systematic approach for the selection of code sequences instead of the brute$-$force method used currently.

Bibliography

[1] R. L. Devaney, *An introduction to chaotic dynamical system*, The Benjamin/Cummings Publishing Company Inc., 1985.

[2] K. T. Alligood, T. D. Sauer, and J. A. Yorke, *Chaos, an introduction to dynamical systems*, Springer Verlag, 1997.

[3] R. C Hilborn, *Chaos and nonlinear dynamics, an introduction for scientists and engineers* , 2^{nd} Ed. Oxford University Press, 2000.

[4] S. H. Strogatz, *Nonlinear dynamics and chaos: with applications to physics, biology, chemistry, and engineering,* Perseus Books, Cambridge MA, 2001.

[5] G. Setti, G. Mazzini, R. Rovatti, and S. Callegari, "Statistical modeling of discrete -time chaotic process – Basic finite dimensional tools and applications," *Proc. IEEE*, vol. 90, No. 5, pp. 662–690, 2002.

[6] M. P. Kennedy, R. Rovatti, and G. Setti, *Chaotic electronics in telecommunications*, CRC Press, 2000.

[7] F. C. M. Lau and C. K. Tse, *Chaos–based digital communication systems*, Springer Verlag, 2003.

[8] K. Cuomo and A. V. Oppenheim, "Circuit implementation of synchronized chaos with application to communication," *Phys. Rev. Lett.*, vol. 71, pp. 65–68, 1993.

[9] M. Itoh and H. Murakami, "New communication system via chaotic synchronization and modulations," *IEICE Trans. Fund. Electron. Commun. and Comput. Sci.*, vol E78-A, pp. 285-290, 1995.

[10] A. Abel and W. Schwarz,"Chaos communications –principles, schemes, and system analysis," *Proc. IEEE,* vol. 90, No. 5, pp. 691–710, 2002.

[11] M. P. Kennedy and G. Kolumban, "Digital communications using chaos," *Signal Processing,* vol. 80, pp. 1307–1320, 2000.

[12] H. Dedieu, M. P. Kennedy, and M. Haseler,"Chaotic shift keying: Modulation and demodulation of chaotic carrier using self synchronized Chua's circuit," *IEEE Trans. Circuits Sys.–II*, vol. 40, pp. 634–642, 1993.

[13] G. Kolumban and M. P. Kennedy, "The role of synchronization in digital communication using chaos– Part-III: Performance bounds," *IEEE Trans. Circuits Syst.–I*, vol. 47, pp. 1673–1683, 2000.

[14] G. Kolumban, B. Vizvari, W. Schwarz, and G. Kis, "Performance evaluation of differential chaotic shift keying: A coding for chaotic communications," *Proceedings International Workshop on Nonlinear Dynamics in Electronic Systems*, Seville, Spain, pp. 87-92, 1996

[15] G. Kolumban, G. Kis, Z. Jk, and M. P. Kennedy, "FM-DCSK: A robust modulation scheme for chaotic communications," *IEICE Trans. Fund. Electron. Commun. and Comput. Sci.*, vol. E81-A, pp. 1798-1802, 1998.

[16] E. R. Bollt, "Review of chaos communication by feedback control of symbolic dynamics," *Intl. J. Bifurc. and Chaos*, vol. 13, pp. 269–285, 2003.

[17] Y. C. Lai and E. Bollt and C. Grebogi, "Communicating with chaos using two-dimensional symbolic dynamics," *Phys. Lett. A*, vol. 255, No. 1-2, pp. 75–81, 1999.

[18] G. Heidari-Bateni, "A chaotic direct-sequence spread-spectrum communication system," *IEEE Trans. Commun.*, vol.42, pp. 1524–1527, 1994.

[19] G. Heidari-Bateni, "Chaotic sequences for spread spectrum: an alternative to PN-sequences," *IEEE International Conference on Selected Topics in Wireless Communication*, Vancouver, B.C., Canada, pp. 437–440, 1992.

[20] Q. Zhang and J. Zheng, "Choice of chaotic spreading sequences for asynchronous DS-CDMA communication," *Proceedings of IEEE Asia-Pacific Conference on Circuits and Systems.*, pp. 642–645, 2000.

[21] H. Fujisaka and T. Yamada, "Stability theory of synchronized motion in coupled-oscillator systems," *Prog. Theor. Phys.*, vol. 69, No. 1, pp. 32–47, 1983.

[22] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.*, vol. 64, pp. 821–824, 1990.

[23] L. M. Pecora, T. L. Carroll, G. A. Johnson, D. J. Mar, and J. F. Heagy, "Fundamentals of synchronization in chaotic systems, concepts, and applications," *Chaos*, vol. 7, pp. 520–543, 1997.

[24] M. J. Ogorzalek, "Taming chaos–Part I: Synchronization," *IEEE Trans. Circuits Sys.–I*, vol. 40, No. 10, pp. 693–699, 1993.

[25] M. M. Sushchik, N. F. Rulkov, and H. D. I. Abarbanel, "Robustness and stability of synchronized chaos: An illustrative model," *IEEE Trans. Circuits Syst.–I*, vol. 44, pp. 867–873, 1997.

[26] H. Nijmeijer and I. M. Y. Mareels, "An observer looks at synchronization," *IEEE Trans. Circuits Sys.–I*, vol. 44, No. 10, pp. 882–890, 1997.

[27] R. Brown, N. F. Rulkov, and N. F. Tufillaro, "Synchronization of chaotic systems: the effect of additive noise and drift in the dynamics of the driving," *Phys. Rev. E*, vol. 50, pp. 4488–4511, 1994.

[28] H. Leung and Z. Zhu, "Time varying synchronization of chaotic systems in the presence of system mismatch," *Phys. Rev. E*, vol. 69, pp. 026201(1–5), 2004.

[29] N. F. Rulkov, M. M. Sushchik, L. S. Tsimring, and H. D. I. Abarbanel, "Generalized synchronization of chaos in directionally coupled chaotic systems," *Phys. Rev. E*, vol. 51, pp.980-994, 1995.

[30] J. F. Heagy, T. L. Carroll, and L. M. Pecora, "Desynchronization by periodic orbits," *Phys. Rev. E*, vol. 52, pp. R1253-R1256, 1995.

[31] T. B. Flower, "Application of stochastic control techniques to chaotic nonlinear systems," *IEEE Trans. Autom. Control*, vol. 34, No. 2, pp. 201–205, 1989.

[32] M. S. Grewal and A. P. Andrews, *Kalman filtering: Theory and practice using MATLAB*, 2^{nd} Ed., John Wiley & Sons, 2001.

[33] R. E. Kalman, "A new approach to linear filtering and prediction problems," *Trans. ASME J. Basic Eng.*, pp. 35-45, 1960

[34] T. Soderstrom, *Discrete time stochastic systems: estimation and control,* 2^{nd} Ed., Springer-Verlag, 2002.

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

[36] D. J. Sobiski and J. S. Thorp, "PDMA–1: Chaotic communication via the extended Kalman filter," *IEEE Trans. Circuits Sys.–I*, vol. 45, No. 2, pp. 194–197, 1998.

[37] C. Cruz and H. Nijmeijer, "Synchronization through filtering," *Intl. J. of Bifurc. and Chaos*, vol. 10, No. 4, pp. 763–775, 2000.

[38] H. Leung and Z. Zhu, "Performance evaluation of EKF based chaotic synchronization," *IEEE Trans. Circuits Syst.–I*, vol. 48, 9, pp. 1118–1125, 2001.

[39] S. J. Julier and J. K. Uhlmann, "A new extension of the Kalman filter to nonlinear systems," *Proc. of AeroSense: The 11th International Symposium on Aerospace/Defense Sensing, Simulation and Control,"* 1997.

[40] S. J. Julier and J. K Uhlman, "Unscented Kalman filtering and nonlinear estimation," *Proc. IEEE,* vol. 92, pp. 401–421, 2004.

[41] S. J. Julier, J. Uhlman, and H. F. Durrant-Whyte, "A new method for the nonlinear transformation of means and covariance in filters and estimators," *IEEE Trans. Autom. Control,* vol. 45, No. 3, pp. 477–482, 2000.

[42] A. W. Eric and R. van der Merwe, "The unscented Kalman filter for nonlinear estimation," *Proceedings of IEEE Symposium on Adaptive Systems for Signal Processing, Communication and Control (AS-SPCC), Lake Louise, Alberta, Canada* Oct. 2000.

[43] L. Jaeger and H. Kantz,"Homoclinic tangencies and non-normal Jacobians - effects of noise in non-hyperbolic systems," *Phys. D*, vol. 105, pp. 79–96, 1997.

[44] M. B. Luca, S. Azou, G. Burel, and A. Serbanescu, "A complete receiver solution for a chaotic direct sequence spread spectrum communication system," *International Symposium on Circuits and Systems 2005*, vol.4, pp.3813-3816, 23-26 May 2005

[45] S. Azou and G. Burel, "Design of a chaos based spread spectrum communication system using dual unscented Kalman filter," *IEEE Communication Conference 2002*, Bucharent, Romania, Dec 5-7, 2002.

[46] Luca, M. B., S. Azou, G. Burel, and A. Serbanescu, "On exact Kalman filtering of polynomial system," *IEEE Trans. Circuits Syst. -I*, vol.53, pp.1329–1340, June 2006

[47] J. Feng and Xie, "A noise reduction method for noisy contaminated chaotic signal," *International Conference on Communication Circuits and Systems*, vol.2, 27–30 May 2005

[48] V. Venkatasubramanian and H. Leung, Chaos based semi-blind system identification using a EM-UKS estimation," *IEEE System Man and Cybernetics Conference*, vol.3, pp.2873–2878, Oct 2005

[49] A. Doucet, J. F. G. de Freitas, and N. J. Gordon, *Sequential Monte-Carlo methods in practice,* New York, Springer Verlag, 2001.

[50] P. Lu, "Nonlinear predictive controllers for continuous systems," *J. of Guidance, Control and Dynamics*, vol. 17, No. 3, pp. 553–560, 1994.

[51] H. Bai-lin, *Elementary symbolic dynamics and chaos in dissipative systems*, World Scientific, Singapore, 1989.

[52] G. M. Maggio and G. Galias, "Application of symbolic dynamics to differential chaotic shift keying," *IEEE Trans. Circuits Syst.–I*, vol. 49, pp. 1729–1735, 2002.

[53] J. Schweizer and T. Schimming, "Symbolic dynamics for processing chaotic signals-I: Noise reduction of chaotic sequences," *IEEE Trans. Circuits Syst.–I*, vol. 48, pp. 1269–1282, 2001.

[54] J. Schweizer and T. Schimming, "Symbolic dynamics for processing chaotic signals-II: Communication and coding," *IEEE Trans. Circuits Syst.–I*, vol. 48, pp. 1283–1295, 2001.

[55] D. J. Gauthier and J. C. Bienfang "Intermittent loss of synchronization in coupled chaotic oscillators: Towards a new criterion for high-quality synchronization," *Phys. Rev. Lett.*, vol. 77, pp.1751-1754, 1996.

[56] T. Stojanovski, L. Kocarev, and R. Harris, "Application of symbolic dynamics in chaos synchronization," *IEEE Trans. Circuits Syst.–I*, vol. 44, pp. 1014–1018, 1997.

[57] A. S. Dimitriev, G. A. Kassian and A. D. Khilinsky, "Chaotic synchronization: Information theory viewpoint," *Intl. J. Bifurc. and Chaos*, vol. 10, pp. 749–761, 2000.

[58] A. J. Viterbi, *CDMA principles of spread spectrum communication*, Addison Wesley, 1995.

[59] E. H. Dinan and B. Jabbari, "Spreading codes for direct sequence CDMA and wide−band CDMA cellular networks," *IEEE Commun. Mag.*, pp. 48–54, June 1998.

[60] H. Saigui, Z. Yong, H. Jiandong, and B. Liu, "A synchronous CDMA system using discrete coupled-chaotic sequence," *Proceedings of IEEE Southeastcon '96, Bringing Together Education Science and Technology*, vol.42, pp. 1524–1527, 1994.

[61] C. C. Chen, K. Yao, and E. Biglieri, "Design of spread-spectrum sequences using chaotic dynamical systems and ergodic theory," *IEEE Trans Circuits Syst.–I*, vol. 48, No. 9, pp. 1110-1114, 2001.

[62] R. Rovatti and G. Mazzini, "Interference in DS-CDMA systems with exponentially vanishing autocorrelations: chaos based spreading is nearly optimal," *Elec. Lett.,* vol. 34, pp. 1911-1913, 1998.

[63] G. Mazzini and R. Rovatti,"Interference minimization autocorrelation shaping in asynchronous DS-CDMA systems: chaos based spreading is nearly optimal," *Elec. Lett.,* vol. 35, pp. 1054-1055, 1999.

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

[65] T. Kohda and A. Tsuneda "Statistics of chaotic binary sequence," *IEEE Trans. Inf. Theory,* vol. 43, No. 1, pp. 104–112, Aug. 1999.

[66] T. Kohda, "Sequence of IID random variables from chaotic dynamics," *Proceedings of Sequences and Their Applications,* pp. 297–307, 1998.

[67] T. Kohda, "Information sources using chaotic dynamics," *Proc. IEEE*, vol. 90, No. 5, pp. 641–661, 2002.

[68] G. Mazzini, G. Setti, and R. Rovatti, "Chaotic complex spreading sequences for asynchronous DS–CDMA Part I: System modeling and results," *IEEE Trans. Circuits Syst.-I,* vol. 44, No.10, pp. 937–947, 1997.

[69] G. Mazzini, G. Setti, and R. Rovatti, "Chaotic complex spreading sequences for asynchronous DS–CDMA Part II: Some theoretical performance bound," *IEEE Trans. Circuits Syst.–I,* vol. 45, pp. 496–506, 1998.

[70] S. Arulampalam, S. Maskell, N. Gordon, and T. Clapp, "A tutorial on particle filters for on–line non–linear/non–Gaussian Bayesian tracking," *IEEE Trans. Signal Process.,* vol. 50, pp. 174–188, 2001.

[71] I. A Khovanov, D. G. Luchinsky, R. Mannella, P. V. E. McClintock, "Fluctuation and energy optimal control of chaos," *Phys. Rev. Lett.*, vol. 85, pp. 2100–2103, 2000.

[72] S. Kraut, C Grebogi, "Escaping from non hyperbolic chaotic attractors," *Phys. Rev. Lett.*, vol. 71, pp. 2100–2103, 2004.

[73] A. N. Silchenko, S. Beri, D. G. Luchinsky, and P. V. E. McClintock, "Fluctuational transitions across different kinds of fractal basin boundaries," *Phys. Rev. E*, Vol. 71, pp. 046203.(1-9), 2003.

[74] K. Ikeda, "Multiple-valued stationary state and its instability of transmitted light by a ring cavity system," *Opt. Comm.*, vol.30, pp. 257-261, 1979.

[75] H. D. I. Abarbanel, *Analysis of observed chaotic data*, Springer, USA, 1996.

[76] Z. Galias, "Rigorous investigation of the Ikeda map by means of interval arithmetic," *Nonlinearity,* vol. 15, pp. 1759–1779, 2002.

[77] H. Leung, Z. Zhu, and Z. Ding, "An aperiodic phenomenon of the extended Kalman filter in filtering noisy chaotic signal," *IEEE Trans. Signal Process.*, vol. 48, No. 6, pp. 1807–1810, 2000.

[78] A. Doucet, S. Godsill, and C. Andrieu, "On sequential Monte-Carlo sampling methods for Bayesian filtering," *Stat. Comput.*, vol. 10, pp. 197-208, 2000.

[79] R. van der Merwe, A. Doucet, N. de Freitas, and E. Wan, "The unscented particle filter," *Technical Report CUED/F-INFENG/TR 330, Cambridge University Engineering Department*, 2000.

[80] B. Efron, *The Bootstrap, Jacknife and other resampling plans*, SIAM, Philadelphia.

[81] E. N. Lorenz, "Deterministic non−periodic flow," *J. Atmos. Sci.*, vol. 20, pp. 130–141, 1963.

[82] M. C. Mackey and L. Glass, "Oscillation and chaos in physiological control systems," *Science*, vol. 197, pp. 287–289, 1977.

[83] R. Bowen and D.Ruelle, "Ergodic theory of axiom A flows," *Invent. Math.* vol. 29, pp. 181-201, 1975

[84] L. F. Shampine, I. Gladwell, and S. Thompson, *Solving ODEs with MATLAB*, Cambridge, 2003.

[85] J. L. Crassidis and F. L. Markley, "Predictive filtering for nonlinear systems," *J. of Guid. Control and Dynamics*, vol. 20, No. 3, pp. 566–572, 1997.

[86] D. D Wheeler, "Problems with chaotic cryptosystems," *Cryptologia,* vol. XIII, pp. 243-250, 1989.

[87] Y. L. Bel'skii, and A. S. Dimitriev,"Information transmission using deterministic chaos (in Russian)," *Radiotekh Electron*, vol. 38, pp. 1310–1215,1993.

[88] T. Schimming, "Statistical analysis and optimization of the chaos based broadband communications," PhD thesis, Ècole Polytechnique fèdèrale de Lausanne, 2002.

[89] E. Ott, *Chaos in Dynamical Systems.* New York: Cambridge University Press, 1993.

[90] J. G. Proakis, *Digital communications*, 4^{th} Ed, McGraw Hill, 2001.

[91] Statistical Test Suit- V1.8, Available for download at http://csrc.nist.gov/rng/.

[92] V. A. Protopopescu, R. T. Santoro, and J. S. Tollover. "Fast and secure encryption – decryption method based on chaotic dynamics," *US Patent No. 5479513*, 1995.

[93] O. Gonzales, G. Han, J. Gyvez, and E. Sanchez-Sinencio, "Lorenz-based chaotic cryptosystem: a monolithic implementation," *IEEE Trans. Circuits Syst. –I*, vol. 47, pp. 1243-1247, 2000.

[94] R. L Peterson, R. E Zeimer, and D. E Borth, *Introduction to spread spectrum communications,* Prentice Hall, 1995.

[95] R. Gold, "Maximal recursive sequence with 3-valued recursive cross correlation function," *IEEE Trans. Inf. Theory,* vol. 4, pp. 154–156. 1968.

[96] M. B. Pursley, "Performance evaluation for phase-coded spread-spectrum multiple-access communication-Part I: System analysis," *IEEE Trans. Commun.*, vol. 25, pp. 795–799, 1977.

[97] T. S. Rappaport, *Wireless communications principles and practice,* Prentice Hall, 1996.

[98] G. Mazzini, R. Rovatti, and G. Setti, "Chaos based asynchronous DS–CDMA systems and enhanced rake receivers: Measuring the improvements," *IEEE Trans. Circuits Syst–I,* vol. 48, pp. 1445–1453, 2001.