DESIGN OF NONLINEAR OBSERVER FOR CHAOTIC MESSAGE TRANSMISSION

A Thesis Submitted to
the Graduate School of Engineering and Sciences of
İzmir Institute of Technology
in Partial Fulfillment of the Requirement for the Degree of

MASTER OF SCIENCE

in Electronics and Communication Engineering

by
Muhammed ÇOBANLAR

January 2014
İZMİR

ACKNOWLEDGMENTS

I would like to thank, first and foremost, to my advisor Assoc. Prof. Dr. Enver TATLICIOĞLU for his support, guidance, contributions and everlasting patience during the completion of this thesis. Without his support and help, I would not have been able to finish this thesis on time.

I would like to thank to Prof. Dr. Serdar İPLİKÇİ and Assoc. Prof. Dr. Aydoğan SAVRAN for their contributions and help.

My sincere thanks to my parents, my father and my mother, for their encouragement and moral support.

Finally, my special thanks to my wife, Zehra, for her constant support and patience through my ups and downs, her ever smiling face and love.

ABSTRACT

DESIGN OF NONLINEAR OBSERVER FOR CHAOTIC MESSAGE TRANSMISSION

Chaos is an interesting nonlinear phenomena that occurs in wide variety of fields. A significant amount of research was devoted to understanding chaos and its properties. After that, researchers focused on searching for possible application areas for chaos to utilize its properties. The need to increase the security of a communication system is considered as a perfect match for chaos and its several properties, yielding chaotic communication.

In this thesis, chaotic communication is approached from a control theory perspective. Specifically, three nonlinear observers are designed to extract message encrypted in a chaotic communication signal. The design and stability analysis is presented for the first observer, and the other observers are presented as modifications to the first one.

Extensive numerical simulations are performed to demonstrate the viability of the proposed observers. Robustness of the observers to noise, additive disturbances, and parametric mismatch, and security of the observers are demonstrated numerically.

ÖZET

KAOTİK MESAJ İLETİMİ İÇİN DOĞRUSAL OLMAYAN GÖZLEMCİ TASARIMI

Kaos, çok geniş ve çeşitli alanda varlık gösterebilen, ilgi çekici lineer olmayan bir olaydır. Kaosu ve onun özelliklerini anlamak için dikkat çekici sayıda araştırma bu konuya adanmıştır. Daha sonra, araştırmacılar kaosun özelliklerinden faydalanabilecekleri muhtemel uygulama alanlarını tespit etmeye odaklanmışlardır. Haberleşme sistemlerinin güvenliğini sağlamak adına kaos üreteçlerinin kullanılması, kaosun özelliklerinin pratik hayata geçirilmesi için çok önemli bir fırsat oluşturmuştur.

Bu tezde, kaotik haberleşme konusuna kontrol teorisi açısından yaklaşılmıştır. Özellikle, kaotik sinyallerle şifrelenmiş mesajın tekrar ortaya çıkarılması için üç adet lineer olmayan gözlemci tasarlanmıştır. İlk gözlemci için tasarım ve kararlılık analizi detaylıca verilmiş, diğer gözlemciler için ise ilk gözlemci ile arasındaki değişiklikler belirtilmiştir.

Önerilen gözlemcilerin başarımlarının doğrulanması amacıyla çok sayıda simülasyon yapılmıştır. Ayrıca gözlemcilerin gürültüye, ek bozulmalara ve parametre hatalarına karşı direnci ve güvenlik analizleri ispat edilmiştir.

TABLE OF CONTENTS

LIST OF FIGURES

Figure **Page**

LIST OF TABLES

CHAPTER 1

INTRODUCTION

Security and privacy of personal information is becoming an extremely important subject day by day. Growth in using mobile communication devices and the internet for personal communications make data encryption and security indispensable [1], [2]. The main reason for this is that the information being sent from a transmitter has to be ensured to be free of listening by unwanted listeners. While classical cryptology systems are being used for security and privacy, the pioneering works by Pecora and Carroll introduced the possibility of synchronization and control of chaotic systems which resulted in using chaotic signals for secure and private communication [3], [4], [5], [6], [7], [8].

Before discussing chaotic communication, we would to like give brief information about Chaos. Chaos, which comes from Greek word *khaos* meaning “abyss, that which gapes wide open, is vast and empty”, is a very popular, universal and robust phenomenon in many nonlinear systems. The first note about the possibility of existence of chaotic behavior in mechanical systems was put into words by the great Mathematician Poincaré in 1892 [9]. After Lorenz published his paper [10], chaos came into prominence among the researchers. Misunderstanding between chaos and noise in engineering community resulted in losing about twenty years [11], and the first studies on chaos started nearly 1980s.

Chaos is commonly used in a wide variety of fields such as meteorology, aerodynamics and turbulence modeling, chemical reactions (Belousov-Zhabotinskii reaction), nonlinear electronic circuits (Van Der Pol Oscillators, Chua’s Circuit), ecology, biology and population evolution, observed time series like electrocardiogram, electroencephalogram, and financial data [12].

There are three basic fundamentals for chaotic systems;

- Dependency on the initial conditions: Chaotic systems are sensitively dependent on the initial conditions.
- Long term unpredictability: They are quite complex and it is usually impossible to predict the signal over longer times.
- Condition of not being random: In spite of impossible prediction, there is an arrangement in itself.

Besides complexity and sensitivity on the initial conditions, chaotic systems are wideband, noise-like, irregular, a-periodic, and uncorrelated (i.e. orthogonal). And despite these, chaos can be observed in rather simple dynamical systems [13].

Chaotic systems are dynamical systems which defy or resist synchronization [14]. Uncorrelation between two identical autonomous chaotic systems’ trajectories can be observed to be deviating significantly even if they start from very close initial values. That shows us that it is quite tough to set up identical and synchronized chaotic systems in laboratory [3]. The seminal works by Pecora and Carroll demonstrate that there is a way to achieve synchronization and control of the chaotic systems [3]. They achieved this by linking two chaotic systems via a common signal or signals [3].

Based on Pecora and Carrol’s works, achieving synchronization is possible for a transmitter-receiver system. As can be seen in Figure 1, a transmitter-receiver system commonly consists of two main parts where the first part is the drive system that generates the chaotic signals, and the second part is the response system which receives the transmitted signals. The usually preferred way of synchronizing two systems is achieved by generating an input signal via the drive system, and then sending signal as an input to the receiver part. To make the information crypted, the information is transformed by the drive system in such a way that is specific for this system, and the response system, which is an authorized one, converts the transmitted signal to the original message signal provided the prior knowledge of the specific transmission parameters of the drive system. The level of the difficulty encountered by the unwanted listeners, who try to decode the information signal, classifies the security of the information.

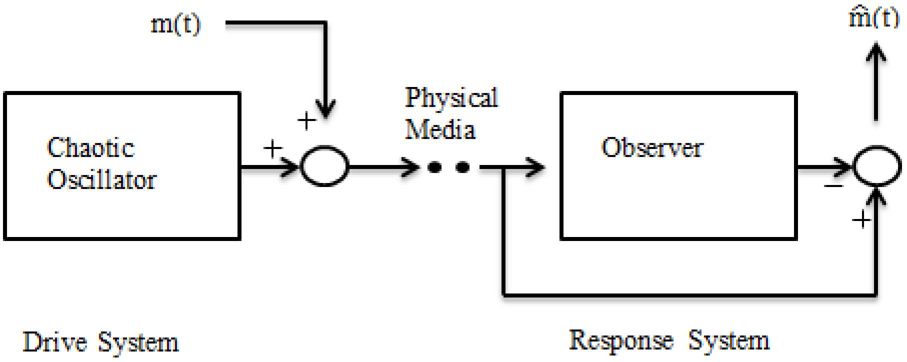


Figure 1. A general block diagram of chaotic oscillator in a secure communication system

Despite being a relatively new field, a significant amount of research was devoted to chaos communication, mostly to use it effectively in a wide variety of areas. Since chaotic based secure communication is relatively simpler in view of practicing its hardware implementation [15] and it is highly unpredictable than the conventional schemes (i.e., it has higher security), several aspects of chaotic schemes are being investigated [16]. Using chaotic signals for secure communication also increases the performance of the communication system; see [17]. There are several approaches in the literature for the security of the communication. Most of these approaches are based on conventional encryption and security schemes. However, hardware implementations of these approaches are usually very complicated for the conventional communication schemes [15], [16], [18]. In addition to ensure the privacy of a system, the integrity of the transmitted message must be ensured by secure communication.

A comparison between the Chaotic Property and Cryptographic Property is listed in the Table 1 [19]. Both chaotic systems and cryptographic systems have nonlinear transformation but though cryptographic systems have finite number of state and iterations, chaotic systems have infinite. Both systems are so sensitive to the initial conditions or secret key.

Chaotic property	Cryptographic property	Description
Chaotic system: Nonlinear transformation Infinite number of state Infinite number of iterations	Pseudo-chaotic system: Nonlinear transformation Finite number of state Finite number of iterations	
Ergodicity	Confusion	The output has the same distribution for any input
Sensitivity to initial conditions/control parameter	Diffusion with a small change in the plaintext/secret key	A small deviation in the input can cause a large change at the output
Mixing property	Diffusion with a small change in one plain-block of the whole plain text	A small deviation in the local area can cause a large change in the whole space
Structure complexity	Algorithm (attack) complexity	A simple process has a very high complexity

Table 1. Comparison between chaos and cryptography properties

Privacy of the communications is approached by using chaotic signal masking technique which was introduced in [20] and [21]. Besides the chaotic signal masking (CM) there are three more modulation schemes in the literature such as Chaos On-Off Keying (COOK), Chaos

Shift Keying (CSK) and Differential Chaos Shift Keying (DCSK). We will give brief information about these schemes later on.

Although there are numerous circuits which are developed for chaotic scenarios, the most investigated and implemented autonomous systems are Chua oscillator, Rössler Oscillator and Lorenz Chaotic System. These systems' chaotic dynamics are well known [22]. Implemented Chua circuit and also Lorenz based circuit models has the ability to transmit either analog or digital forms of the signals. Chua circuit is a commonly used circuit in the literature but if we compare the performance of Lorenz based circuit with Chua's circuit, it will be observed that Lorenz's circuit is better in performance [23].

Broadband chaotic oscillations can be produced by Lorenz Chaotic System and all the properties of chaotic systems such as being noise-like, and dependence on the initial conditions and system parameters, being difficult to estimate are obtained. As a result, we can use Lorenz System for secure communication. In this system, the synchronization is highly robust to perturbations in the drive signal as shown numerically in [24].

This thesis focuses on designing observers for message extracting from chaotic communication systems. Specifically, we propose three new nonlinear observers for chaotic communication systems and apply these ideas to the Lorenz Chaotic System. This system was proposed 40 years ago for modeling two-dimensional fluid convection by Edward Lorenz of the Massachusetts Institute of Technology, Massachusetts, MA, USA [10]. The stability analysis of the first observer is examined by Lyapunov's stability theorem (Lyapunov's Direct Method) which states if we measure the system's total energy, and if the rate of the change of the energy is decreasing, then the system's states will finally reach an equilibrium point [25]. Although it has been always tough to analyze nonlinear systems, the most flexible, intuitive, and powerful way is provided by Lyapunov based design techniques. The most important step of the analysis is to define the Lyapunov function whose time derivative will be evaluated.

This thesis is organized as follows. Chapter 1 introduces some basic knowledge about chaos and communication and relationship between chaos and cryptography. Chapter 2 gives detailed information about chaos communication and its requirements. Chapter 3 presents our proposed nonlinear observer for chaotic message transmission. Finally, the thesis is summarized in Conclusion chapter and future works are determined.

The contributions of this thesis are:

- A nonlinear observer utilizing the integral of the signum of the observer error terms is designed for message extraction in a chaotic system. According to our best knowledge, the integral of the signum of the observer error terms was not utilized for message extraction in a chaotic communication system before.
- The second observer is obtained by replacing the signum term in the first observer with hyperbolic tangent function. This observer is utilized for message extraction from a chaotic communication system for the first time in the literature.
- The third observer is designed by replacing the signum function in the first observer with saturation function. This is a novel observer.

CHAPTER 2

WHAT IS CHAOS COMMUNICATION?

Studies on chaotic dynamical systems introduced the question "How can chaos be used in different fields?" At the beginning of the 1990s, the answer was given as chaos communication. The main reason is that despite the fact that the dynamical system representations of chaotic systems are fairly simple the resulting/obtained chaotic behavior is complex. Other characteristics of chaotic signals, such as being irregular, aperiodic, noise-like, uncorrelated, broadband, and long-term predictability make them suitable for sub-fields of communication systems like spread-spectrum communications, for multi-user communications, and especially for secure communications (i.e., cryptography) [24], [26].

One of the main research problems chaotic communications is the synchronization of the transmitter and the receiver. The pioneering works of Pecora and Carroll [3], [4] which were the milestones of the synchronization problem, attracted several researchers to work on synchronization and also on control of chaotic systems in various fields.

2.1. Communication Fundamentals and Schemes

In this section, communication requirements and resources, and also potential of chaos in communication systems are discussed.

The general structure of communication scheme is demonstrated in Figure 2. Source decoding, decryption, and channel decoding, demodulation have to be performed at the receiver side to the received message to obtain the original (transmitted) message.

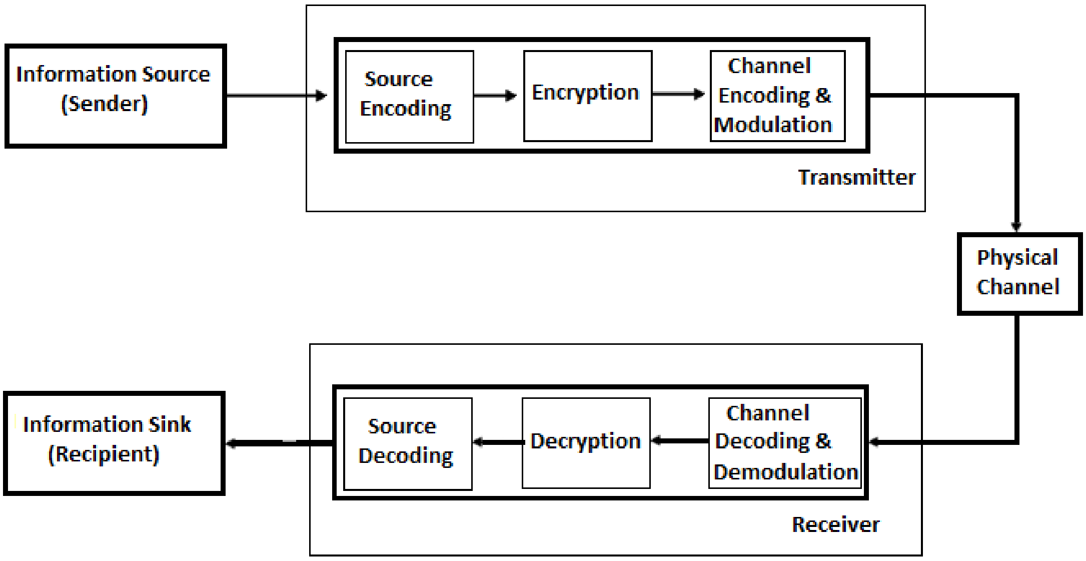


Figure 2. General Structure of a communication scheme

2.1.1. Communication Requirements and Resources

This subsection provides information about requirements of a communication channel and its limitations.

2.1.1.1. Requirements

In a communication system, there is a transmitter which transmits the message/information to a receiver or a recipient. Transmitter and receiver are usually located in different places. The message is transmitted by a physical media (i.e., the communication channel). This channel has to have the standard requirements such as being efficient, secure and robust. Different blocks of a communication scheme implement these three requirements.

2.1.1.1.1. Efficiency

Analog signals (such as sound, picture, and video signals) usually have a lot of redundancy. Uncompressed digital signals (such as text, sound or images) may be redundant as well. This redundancy can be cancelled by omitting unnecessary content from the information. Removing the unnecessary content of the signal before the transmission (i.e., forming an almost redundancy-free message) is achieved by a process called source encoding [27]. Analog schemes are not suitable for this encoding because it is a digital procedure and only digital data is suitable for this.

2.1.1.1.2. Security

The physical media, which we transmit the signal over (i.e., the communication channel), is usually public which means it is accessible by many receivers. If the sender wants to prevent the message from unwanted listeners for security or privacy reasons, cryptography will be a solution. Encryption is applied to message before the transmission so that the message is aimed to be totally protected from unwanted listeners [28].

2.1.1.1.3. Robustness

The message is usually not transmitted over the transmission channel or the physical media directly. For example, although the frequency of a speech signal is in the kilohertz region, one cannot transmit it over a radio channel which is in megahertz region. So, the message is mapped to signals which can pass the given physical channel. This process is called modulation. It has to be mentioned that in general the transmitted and the received signals are not same. Specifically, the received signal is corrupted because of filtering, nonlinear distortions, and interference from other signals in the communication medium. In conclusion, the transmission should be robust to all anticipated channel distortions. The first method to increase robustness is to choose a proper modulation scheme. Another way is to add a redundant signal to the transmitted signal in a controlled way. This second method is called channel encoding and is one of the digital communication methods [26].

2.1.1.2. Resource Sharing

There are always various limitations to signal transmission because of the restrictions of the physical channel. These are detailed below.

- *Bandwidth Limitation:* Bandwidth limitation is caused by the physical communication channel. Although the channel can provide a bandwidth physically, there may be some restrictions due to technical or administrative constraints.
- *Imperfections:* The received signal is usually distorted because of attenuations, multipath propagation and delays due to linear or nonlinear filtering, noise caused by nature or technical sources, and also interference from other received signals.
- *Publicity:* Most of the physical channels are unsecure, thus the signals transmitted over these channels can be received by unwanted listeners.

We can say that, while transmitting messages over a physical channel, there is always a limitation for capacity which means that the resources are limited. The communication system design has to provide an optimized model for these limited resources. Utilizing orthogonal signals is one way for this optimization. This is done by assigning an orthogonal signal to each user of the physical communication channel. Another advantage of utilizing orthogonal signals is that one can separate the signals that belong to different users easily. For example, consider x_1 and x_2 which are orthogonal if

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

where superscript * denotes complex conjugation. Equation (1) implies a vanishing cross-correlation of x_1 and x_2. Fourier representations of these signals are given by

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

for i=1, 2. From Parseval’s Theorem [29] , we can obtain

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

From the duality property, orthogonality in the time domain implies orthogonality in the frequency domain. There are some ways to achieve orthogonality property in multi-user environments.

- *Signals disjoint in time:* Time Division Multiple Access (TDMA) is one way when one of the signals (i.e., either x_1 or x_2) is equal to zero at any time.
- *Signals disjoint in frequency:* Frequency Division Multiple Access (FDMA) is another way to obtain orthogonality. The expression in (3) is equal to zero if any of the Fourier representations of the signals ($X_1(\omega)$ or $X_2(\omega)$) vanishes.
- *Uncorrelated signals:* Aside from TDMA and FDMA, Code Division Multiple Access (CDMA) is another way to use orthogonality. In CDMA, there is no obligation for signals to be disjoint neither in time nor in frequency.

2.2. Potential of Chaos in Communication

After significant improvements in nonlinear dynamical systems, the chaotic communication applications have been understood more precisely. These improvements motivate researchers for practical solutions and applications. There are three main potential application areas. These three areas create three different behavioral aspects of chaotic signals.

2.2.1. Broad-Band Aspect

As we mentioned before, chaotic signals are aperiodic because of their nature and they also have a continuous spectrum. Often, the spectrum shows significant strength over a wide range of frequencies, i.e., the signals are broad band. These spectral properties let us design models for chaotic signals [30].

It should be noted that, one way to deal with channel imperfections is using broadband signals in communications. So that chaotic signals are appropriate candidates for spread-spectrum communications [1].

2.2.2. Complexity Aspect

As commonly stated in the literature chaotic signals are irregular and have a complex structure. When there is a minimal change in the initial conditions of a chaos generator, its output trajectory will be totally different. It is a good feature for secure communication because, after longer time intervals, predicting the signals and guessing the structure of the generator become extremely difficult.

As a result, cryptographic applications, which classically use highly complex and hard-to-predict signals, is considered as a potential application for chaos [31], [32].

2.2.3. Orthogonality Aspect

The autocorrelation functions of chaotic signals usually vanish so fast since they are aperiodic. They can thus be assumed uncorrelated (i.e., orthogonal) when the signals are generated by different chaos generators or same generator with different initial conditions.

Due to the orthogonality property, the third potential application field for chaos is multi-user communication applications. Chaos-based solutions for conventional CDMA systems which use chaos generators for the generation of spreading codes are better in the manner of performance then classical approaches.

2.3. Chaos Modulation Schemes

As we mentioned in the Introduction, there are four different chaos modulation schemes. Although Chaotic Masking scheme is investigated in this thesis, brief information about other three schemes which are Chaos On-Off Keying, Chaos Sift Keying, and Differential Chaos Shift Keying will be given.

2.3.1. Chaotic Masking

The chaotic masking scheme is composed of two identical chaotic systems. One of them is at the receiver part and the other one is at the transmitter part. As demonstrated in Figure 3, the transmitted message c(t) is obtained by adding the chaotic mask signal to the message signal m(t). The copy of the chaotic mask signal ĉ(t) is produced by another but identical chaotic system at the receiver part. When the difference between the transmitted signal r(t) and chaotic mask signal ĉ(t) is zero, the recovered message signal m̂(t) is equal to m(t).

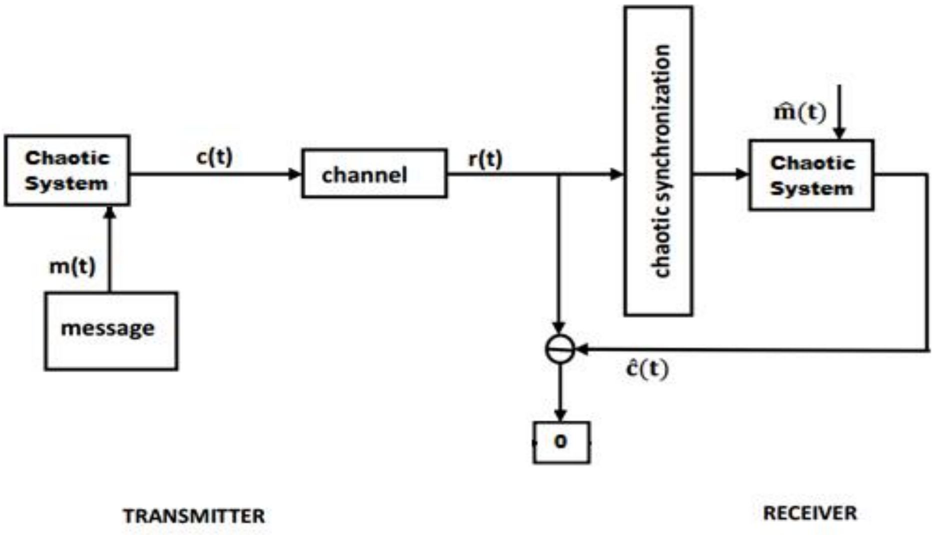


Figure 3. Chaotic Masking

If the channel is noise-free and the synchronization is perfect between the two systems then $r(t) = c(t)$. When the difference between $r(t)$ and $\hat{c}(t)$ is zero then $\hat{c}(t) = c(\mathrm{t})$. Finally, we can conclude that $\widehat{m}(t) = m(\mathrm{t})$.

2.3.2. Chaos Shift Keying

In Chaos Shift Keying (CSK) scheme, there are two statistically similar attractors at the transmitter part. These two systems with the same structure but different parameters generate two different chaotic signals which are $c_0(t)$ and $c_1(t)$, respectively. In this scheme, the message signal should be digital signal. Determination output of which chaotic signal will be sent depends on the message signal's bit which can be 0 or 1 [11], [33].

At the receiver end, correlation between the received signal and the reproduction of any of the two chaotic signals used in the transmitter is obtained. The synchronization error is used for recovering the message signal by low-pass filtering and thresholding. The block diagram model of this scheme is shown in Figure 4.

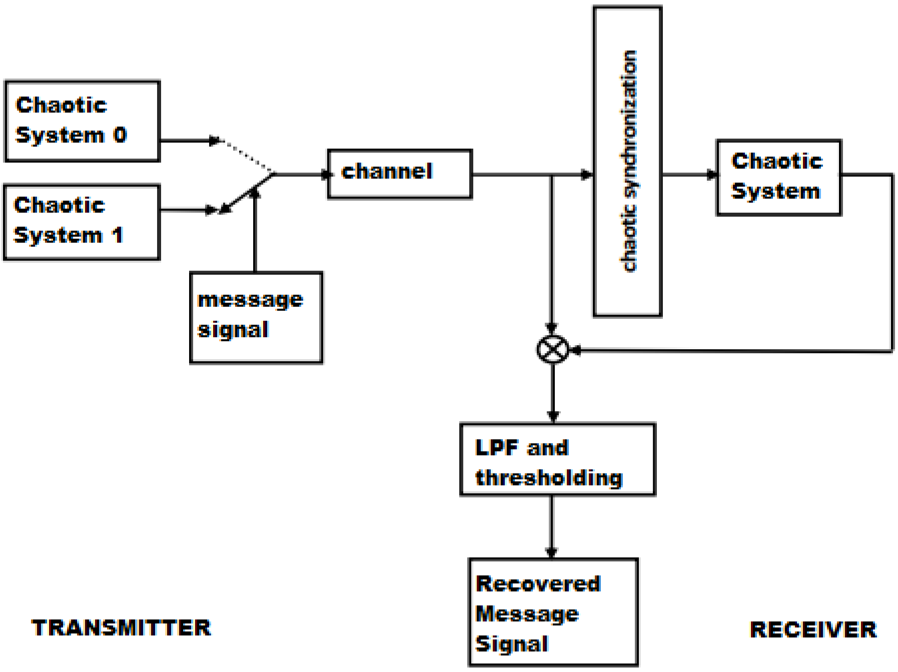


Figure 4. Chaos Shift Keying

2.3.3. Chaos On-Off Keying

Chaos On-off Keying (COOK) is another communication scheme which is very similar to CSK structurally. Difference between CSK and COOK is that COOK uses only one chaotic signal while CSK uses two different chaotic signals. In COOK, the second signal is equal to 0. If the message signal is equal to 1 then the chaotic signal is transmitted, else no signal is transmitted. Demodulation procedure is same with CSK as shown in Figure 5.

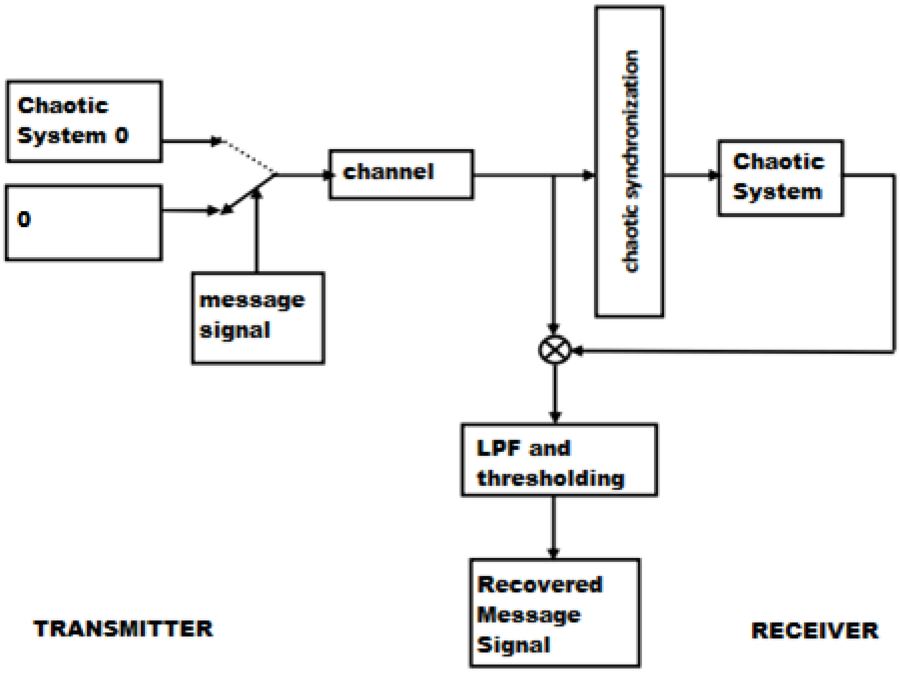


Figure 5. Chaos On-Off Keying

2.3.4. Differential Chaos Shift Keying

In this scheme, there are two sample functions which represent the bit to be transmitted. Reference signal is the first sample function and information signal is carried by the second sample function. If the reference signal is transmitted twice in successively, it means that the message bit is 1. If inverted copy of the chaotic signal is transmitted after the original chaotic signal then the message bit is 0. In the receiver, these two sample functions’ correlation is used with the help of a level comparator for decision.

As we previously discussed, there should be a synchronization signal between the receiver and the transmitter in the first three chaos modulation schemes. On the contrary Differential Chaos Shift Keying (DCSK) does not need a synchronization signal. So that we do not need a chaotic system at the receiver part. The same chaotic signal generated at the transmitter part is used for transmitting and demodulating the message signal at the receiver part which is shown in Figure 6.

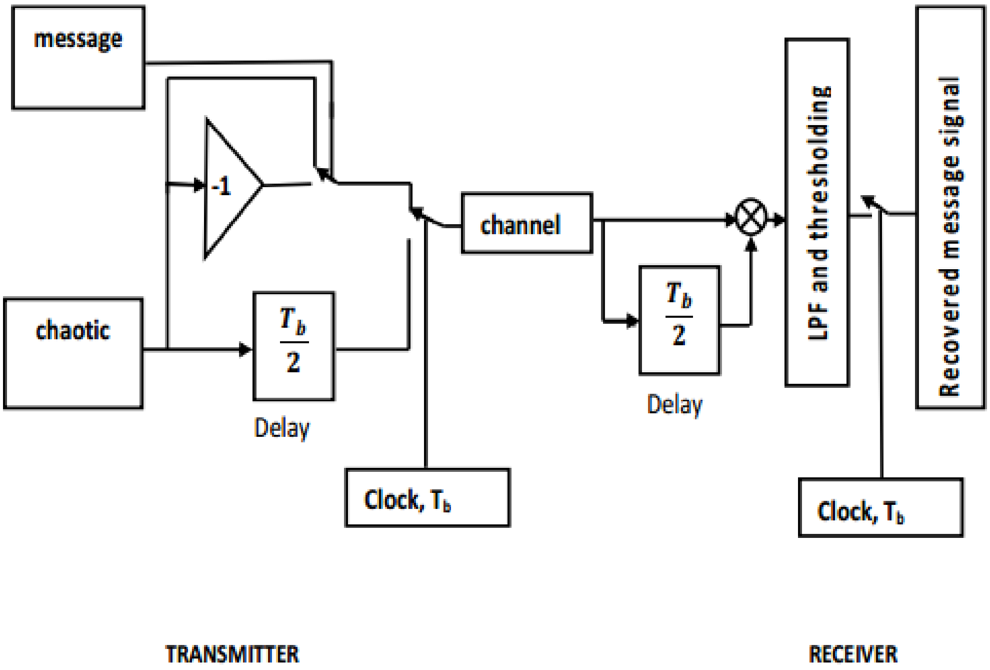


Figure 6. Differential Chaos Shift Keying

2.4. Advantages and Disadvantages of Chaos-based Encryption Schemes

In this sub-section, a comparison between the chaos based encryption schemes and traditional encryption schemes are listed. As we discussed earlier, chaos based encryption has more advantages than conventional encryption methods which are shown below [34]:

- Although there is a requirement of digitizing the message in traditional encryption schemes because of being defined over integer number field, chaos based encryption schemes can be used without this requirement since they can be defined over continuous number field. Because of being defined over continuous number field, chaos based encryption schemes can be used for encryption with more variety of functions.
- The chaos based encryption schemes can be realized directly by hardware implementation of high speed analog components but digital hardware must be used for implementation of traditional encryption schemes.

- There must be two circuits in traditional encryption scheme. The first one is for digital encryption, the second one is for broadband modulation which is obtained form an analog circuit. But in chaos based encryption scheme, a single circuit is enough for both encoding and broadband modulation.
- We need to mask a message with either non-periodic pseudo random waveforms which are generated by chaotic dynamics or pseudo-random sequences generated by traditional encryption schemes. The handicap of using pseudo-random sequences generated by traditional schemes is that they will be periodic eventually (because of being implemented using digital hardware) since the periodicity of these sequences are limited by the number of bits which are generated by the state of the pseudo number sequence generator.

The disadvantages of chaotic encryption schemes are as follows:

- Since chaotic encryption is a relatively new field of research, its security is not proven totally.
- Traditional communication schemes are better in the power efficiency, bandwidth efficiency and bit error rate performance than the chaos based efficiency.

2.5. Summary

In this chapter, a survey of communication fundamentals, potential of chaos communication, and chaos modulation schemes are presented. The requirements of a communication channel and limitations because of the physical channel are also provided.

CHAPTER 3

DESIGN OF NONLINEAR OBSERVERS FOR CHAOTIC MESSAGE TRANSMISSION

In this chapter, firstly, general Lorenz Chaotic System will be deeply investigated with some simulation results. Secondly, novel nonlinear observers will be proposed. The design and the associated stability analysis will be given in detail for the first one, while the other two of them will be presented as extensions to the first one.

3.1. General Lorenz System

General Lorenz chaotic system is defined by the following system of ordinary differential equations. Extensive numerical simulations will also be presented to demonstrate the effectiveness of proposed observers. Finally, security of our algorithm will be discussed briefly. The governing equations of the system are;

$$\dot{x}(t) = \sigma(y(t) - x(t)) \tag{4}$$

$$\dot{y}(t) = rx(t) - y(t) - x(t)z(t) \tag{5}$$

$$\dot{z}(t) = x(t)y(t) - bz(t) \tag{6}$$

where x(t), y(t) and z(t) are system states, σ, r and b are system parameters that define the Lorenz system.

Typical parameters that generates chaotic dynamics for this system are σ = 10, r = 28 and b = 8/3. In Figure 7, waveforms of the system states are given for the above parameter and initial conditions of $x(0)$ = 10, $y(0)$ = 10 and $z(0)$ = 1, and the attractors generated the signals shown in Figure 8.

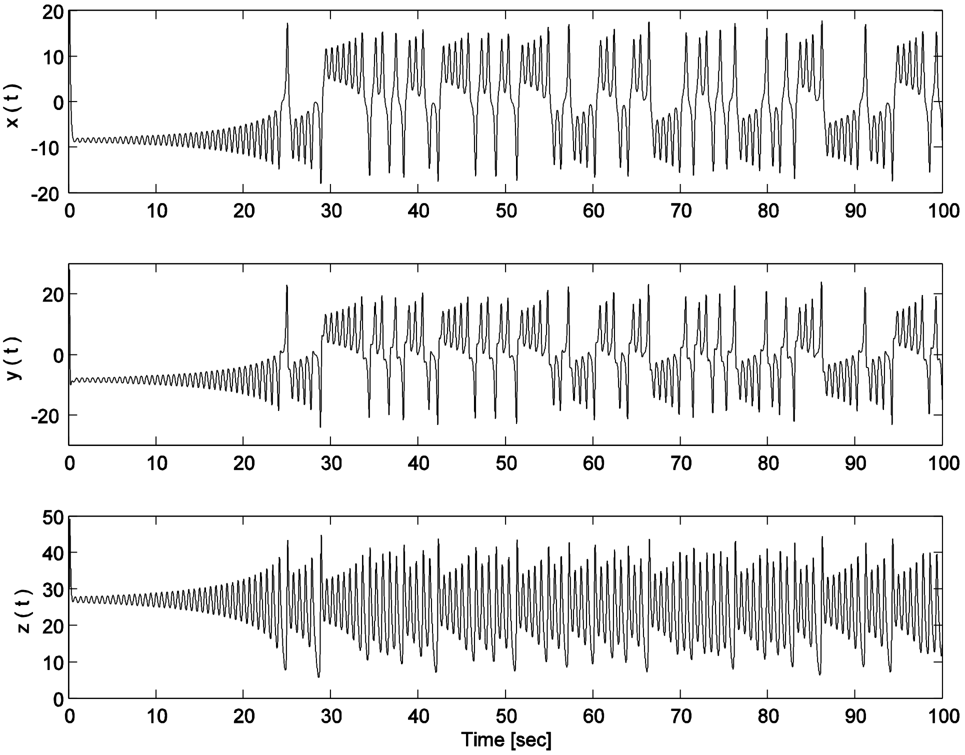
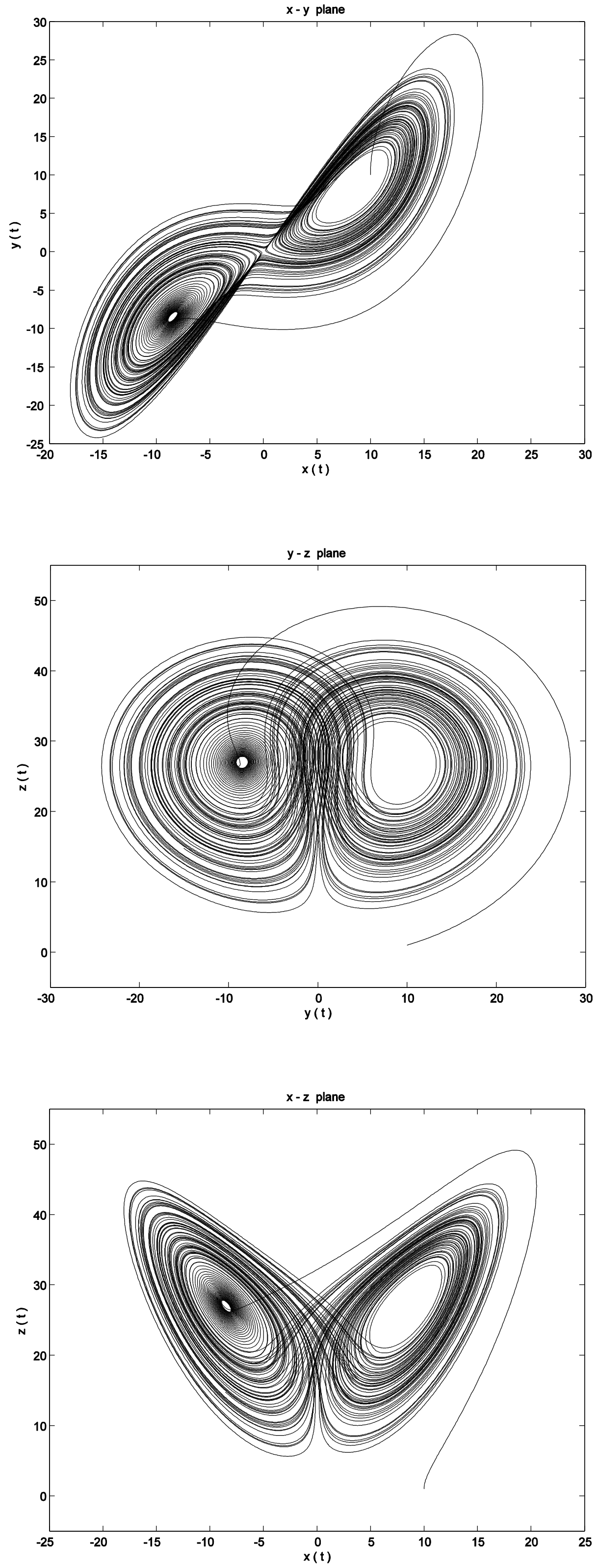


Figure 7. x(t), y(t) and z(t)



(a)

(b)

(c)

Figure 8. Chaotic attractors of Lorenz for given parameters. a) xy-plane b) yz-plane c) xz-plane

3.1.1. The Effect of the Initial Conditions

As mentioned before, chaotic systems are extremely sensitive to their initial conditions. If two identical chaotic systems start with a small difference between their initial conditions, they will diverge from each other. This special feature is simulated for the Lorenz system in (4) - (6). Initial conditions are now chosen as $x(0)$ = 10.001, $y(0)$ = 10 and $z(0)$ = 1. Since the initial value of $x(t)$ was 10 and now chosen as 10.001, it is only changed by 0.001, while keeping the initial values of $y(t)$ and $z(t)$ same. The states of $x(t)$ are demonstrated in Figure 9. It is trivial that a small difference in the initial conditions caused dramatic changes at the trajectory of $x(t)$ after the 30th second.

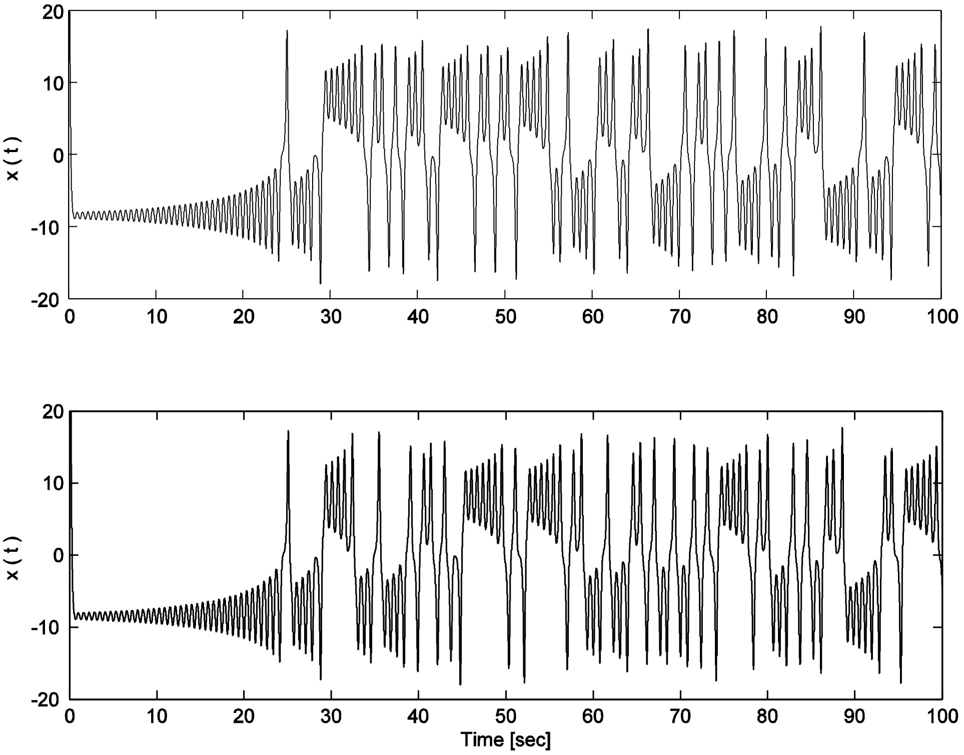


Figure 9. The above trajectory is for $x(0)$ = 10 and the below one is for $x(0)$ = 10.001.

3.1.2. The Effect of the System Parameter

There is a hypercube in the parameter space where the system is in the chaotic regime. When in the chaotic regime, systems are sensitively dependent on the system parameters. Making a change at a specific parameter can significantly affect the chaotic behavior.

In Figure 10, comparative simulation results for r = 28 and r = 35 are shown. As you can see, a change in the “r” parameter makes the chaotic behavior totally different.

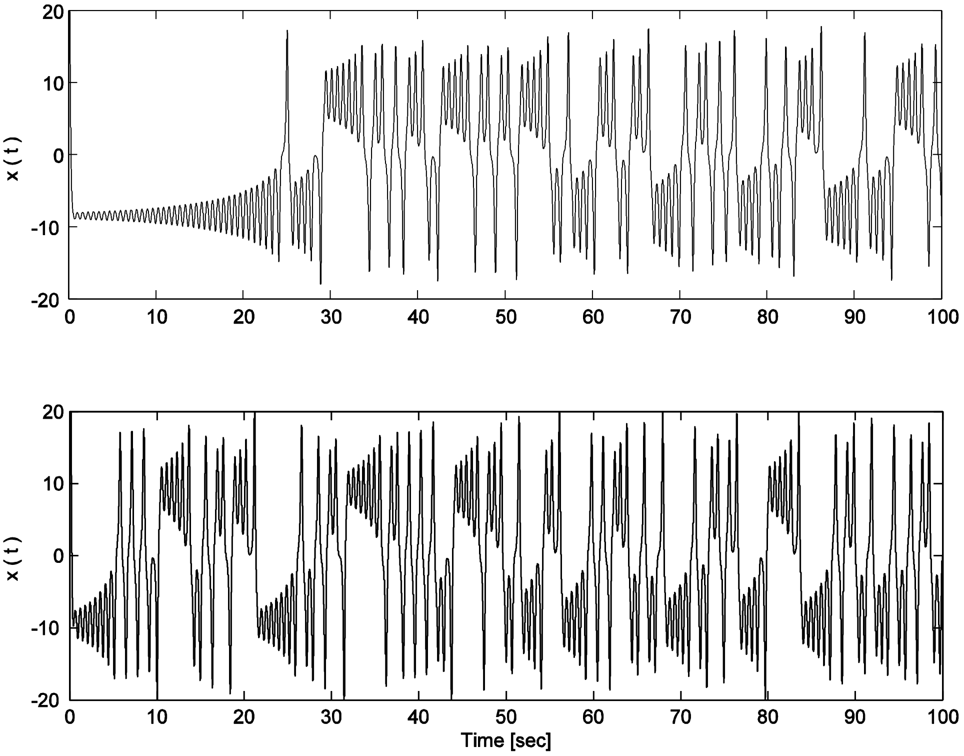


Figure 10. The Effect of the System Parameter. The above figure is for r = 28 is above and the below figure is for r = 35

3.2. Nonlinear Observer Design

In this section, firstly, the dynamic model of the Lorenz System is given, secondly, the observer design is investigated, and finally, stability analysis for this system is showed in detail. The simulation results based on these analysis are illustrated in Figures.

3.2.1. Dynamic Model of the Lorenz System

In the case of chaotic masking, the dynamic model of the chaotic Lorenz system is given by following equations

$$\dot{x}(t) = -10x(t) + 10y(t) + m(t) \tag{7}$$

$$\dot{y}(t) = 28x(t) - y(t) - x(t)z(t) \tag{8}$$

$$\dot{z}(t) = x(t)y(t) - \frac{8}{3}z(t) \tag{9}$$

where $m(t)$ is the message signal. For the Lorenz System $x(t)$ is considered as the output and it is the only signal that is available for use in the observer design. (i.e., it is the only signal that is transmitted to the receiver part.) Similar to the previous studies in the literature, we assume that we know the structure of the Lorenz system (i.e., we know all the constant parameters). In the observer design part, the initial conditions of the drive system are not known. We will design observers for x(t), y(t) and z(t). Since the message signal is hidden –crypted– in chaotic signal $x(t)$, our overall objective is to reconstruct the message signal m(t) online from $x(t)$.

3.2.2. Observer Design

Based on the subsequent stability analysis, we design the following nonlinear observer

$$\dot{\hat{x}} = -10x + 10\hat{y} + \hat{m}(t) \tag{10}$$

$$\dot{\hat{y}} = 28x - \hat{y} - x\hat{z} \tag{11}$$

$$\dot{\hat{z}} = x\hat{y} - \frac{8}{3}\hat{z} \tag{12}$$

where $\hat{x}(t)$, $\hat{y}(t)$, $\hat{z}(t)$ are the observer signals for x(t), y(t), z(t), respectively, and $\widehat{m}(t)$ is the observed signal that will be designed subsequently. It should be noticed that since x(t) is available then we used it in the designs of $\dot{\hat{x}}(t)$, $\dot{\hat{y}}(t)$ and $\dot{\hat{z}}(t)$, and did not utilize neither y(t) nor z(t) in our observer design.

To quantify the mismatch between the actual signals and the corresponding observer signals, we define observer errors

$$\tilde{x} \triangleq x - \hat{x} \tag{13}$$

$$\tilde{y} \triangleq y - \hat{y} \tag{14}$$

$$\tilde{z} \triangleq z - \hat{z}. \tag{15}$$

The observed message is designed as [35]

$$\hat{m}(t) = (k+1)\left[\tilde{x}(t) - \tilde{x}(0) + \int_0^t \tilde{x}(\sigma)d\sigma\right] + \beta\Pi(t) \tag{16}$$

where k and β are positive observer gains and $\Pi(t)$ is a filter signal updated according to

$$\dot{\Pi}(t) = sgn(\tilde{x}(t)) \text{ with } \Pi(0) = 0 \tag{17}$$

with $sgn(.)$ being the standard signum function.

3.2.3. Stability Analysis

The stability analysis is conducted in two parts. In the first part, we will prove the convergence of $\tilde{y}$ and $\tilde{z}$ to zero, and in the second part, we will prove the convergence of $\tilde{x}$ to zero and then conclude with proving the convergence of $\hat{m}(t)$ to $m(t)$ (i.e., $\hat{m}(t) \rightarrow m(t)$).

The time derivative of the observer error $\tilde{y}$ is obtained as

$$\begin{aligned}\dot{\tilde{y}} &= \dot{y} - \dot{\hat{y}} \\ &= -\tilde{y} - x\tilde{z}.\end{aligned} \tag{18}$$

where (8) and (11) were utilized. The time derivative of the observer error $\tilde{z}$ is obtained as

$$\begin{aligned}\dot{\tilde{z}} &= \dot{z} - \dot{\hat{z}} \\ &= x\tilde{y} - \tfrac{8}{3}\tilde{z}.\end{aligned} \tag{19}$$

where (9) and (12) were utilized.

We now define a Lyapunov function, denoted by $V_1(\tilde{y},\tilde{z}) \in R$, as

$$V_1(\tilde{y},\tilde{z}) \triangleq \frac{1}{2}\tilde{y}^2 + \frac{1}{2}\tilde{z}^2 \tag{20}$$

It should be noted that $V_1(\tilde{y},\tilde{z}) \geq 0 \, \forall \tilde{y},\tilde{z}$. The time derivative of V_1 is obtained as

$$\dot{V}_1 = \tilde{y}\dot{\tilde{y}} + \tilde{z}\dot{\tilde{z}} \tag{21}$$

and after substituting (18) and (19), we obtain

$$\begin{aligned} \dot{V}_1 &= -\tilde{y}^2 - \tfrac{8}{3}\tilde{z}^2 \\ &\leq -\tilde{y}^2 - \tilde{z}^2 \\ &= -2V_1 \end{aligned} \tag{22}$$

where (20) was utilized to obtain the last line.

After solving the above linear differential inequality, we can conclude that $\tilde{y}$ and $\tilde{z}$ goes to 0 exponentially fast. After utilizing the fact that x(t) is a bounded function of time, we can conclude that $\tilde{y}(t)$, $\tilde{z}(t)$, $\dot{\tilde{y}}(t)$, and $\dot{\tilde{z}}(t)$ are bounded functions of time. From (22), it is clear that $\tilde{y}(t)$ and $\tilde{z}(t)$ are square integrable functions. This concludes the first part of the proof.

We now define an auxiliary error-like signal, denoted by $r(t) \in R$, as

$$r \triangleq \dot{\tilde{x}} + \tilde{x}. \tag{23}$$

We will now obtain the dynamics of $r(t)$. If we take the time derivative of (13), we obtain

$$\dot{\tilde{x}} = \dot{x} - \dot{\hat{x}} \tag{24}$$

and after substituting (7) and (10) then we get

$$\dot{\tilde{x}} = 10\tilde{y} + m - \hat{m}. \tag{25}$$

The time derivative of the auxiliary error-like signal $r(t)$ is obtained as

$$\dot{r} = \ddot{\tilde{x}} + \dot{\tilde{x}}. \tag{26}$$

Since $\dot{\tilde{x}} = r - \tilde{x}$ and using the time derivative of $\dot{\tilde{x}}$ (i.e., $\ddot{\tilde{x}}$), we obtain the time derivative of $r(t)$ as

$$\dot{r} = 10\dot{\tilde{y}} + \dot{m} - \dot{\hat{m}} + r - \tilde{x}. \tag{27}$$

since the time derivative of the observed message is required for (27), we obtain from (16) and (17) that

$$\dot{\hat{m}} = (k+1)r + \beta sgn(\tilde{x}) \tag{28}$$

where (23) was utilized. Substituting (28) into (27) results in

$$\dot{r} = 10\dot{\tilde{y}} + \dot{m} - \mathrm{kr} - \beta sgn(\tilde{x}) - \tilde{x}. \tag{29}$$

Before starting the Lyapunov–based analysis, we introduce an auxiliary function, denoted by $\mathrm{P(t)} \in \mathrm{R}$, that will be utilized in the Lyapunov function

$$P = \gamma_p - \int_0^t r(\sigma)\left[\dot{m}(\sigma) - \beta sgn\left(\tilde{x}(\sigma)\right)\right] d\sigma. \tag{30}$$

where $\gamma_\mathrm{p} \in \mathrm{R}$ is a nonnegative constant. It can be shown that $\mathrm{P(t)} \geq 0 \; \forall t$ [36].

Consider the following Lyapunov function

$$V_2 \triangleq \frac{1}{2}\tilde{x}^2 + \frac{1}{2}r^2 + P. \tag{31}$$

Since $\mathrm{P(t)} \geq 0 \; \forall t$ then $V_2 \geq 0 \; \forall \mathrm{t}$. If we take the derivative of this function, we get

$$\begin{aligned} \dot{V}_2 &= \tilde{x}\dot{\tilde{x}} + r\dot{r} + \dot{P} \\ &= -\tilde{x}^2 - kr^2 + r10\dot{\tilde{y}} \end{aligned} \tag{32}$$

where (23), (27) and time derivative of (30) were utilized.

If we recall the equation (18)

$$\dot{\tilde{y}} = -\tilde{y} - x\tilde{z}.$$

Note that, x(t) is bounded since the original system is a modified chaotic system with m(t), $\dot{\mathrm{m}}(t)$, and $\ddot{\mathrm{m}}(t)$ being bounded. We also know that $\tilde{\mathrm{y}}(t)$ and $\tilde{\mathrm{z}}(t)$ are square integrable. These could be utilized along with the right-hand side of (32) to show that $\dot{\tilde{y}}(\mathrm{t})$ is a square integrable. Mathematically,

$$\int_0^\infty \dot{\tilde{y}}^2(\sigma)d\sigma \leq \gamma_1 < +\infty \tag{33}$$

where $\gamma_1 \in \mathrm{R}$ is a positive bounding constant.

Utilizing the fact that $2ab \leq a^2 + b^2$, we can obtain the following

$$10r\dot{\tilde{y}} \leq 5r^2 + 5\dot{\tilde{y}}^2. \tag{34}$$

If we use (34) along with (32), we get

$$\dot{V}_2 \leq -\tilde{x}^2 - kr^2 + 5\,r^2 + 5\dot{\tilde{y}}^2. \tag{35}$$

If we rearrange the above expression, we obtain

$$\tilde{x}^2 + (k-5)r^2 \leq -\dot{V}_2 + 5\dot{\tilde{y}}^2. \tag{36}$$

After integrating the above expression from 0 to t, we obtain

$$\int_0^\infty \tilde{x}^2(\sigma)d\sigma + (k-5)\int_0^\infty r^2(\sigma)d\sigma \leq -\int_0^\infty \dot{V}_2(\sigma)d\sigma + 5\int_0^\infty \dot{\tilde{y}}^2(\sigma)d\sigma \tag{37}$$

We know that $\int_0^\infty \dot{V}_2(\sigma)\mathrm{d}\sigma = \mathrm{V}_2(\infty) - \mathrm{V}_2(0)$, and after substituting this fact into (37), we obtain

$$\int_0^\infty \tilde{x}^2(\sigma)d\sigma + (k-5)\int_0^\infty r^2(\sigma)d\sigma \leq V_2(0) - V_2(t) + 5\gamma_1. \tag{38}$$

Since $\mathrm{V}_2(\mathrm{t})$ is a positive function $V_2(0) - V_2(t) \leq V_2(0)$ is always true, then

$$\int_0^\infty \tilde{x}^2(\sigma)d\sigma + (k-5)\int_0^\infty r^2(\sigma)d\sigma \leq V_2(0) + 5\gamma_1. \tag{39}$$

We can separate (39) into two parts, where the first one is

$$\int_0^\infty \tilde{x}^2(\sigma)d\sigma \leq V_2(0) + 5\gamma_1 \tag{40}$$

and the second one is

$$\int_0^{\infty} r^2(\sigma)d\sigma \leq \frac{1}{(k-5)}(V_2(0) + 5\gamma_1) \tag{41}$$

where $k > 5$ is required.

As we can see from (40) and (41) it is clear that, x̃(t) and r(t) are square integrable. Since $\tilde{x}(t)$ and $r(t)$ are bounded and then from (23), $\dot{\tilde{x}}(t)$ is bounded as well. Finally we can show that $\dot{\tilde{x}}(t), \dot{r}(t)$ are bounded. Thus, from Barbalat's Lemma [37], $\tilde{x}(t)$ and $r(t) \rightarrow 0$ as $t \rightarrow +\infty$. Given the definition of $r(t)$, we can conclude that $\dot{\tilde{x}}(t) \rightarrow 0$ as $t \rightarrow +\infty$.

Recall the definition of $\dot{\tilde{x}}(t)$ as in (25)

$$\dot{\tilde{x}} = 10\tilde{y} + m - \hat{m}$$

and since $\dot{\tilde{x}}(t)$, $\tilde{y}(t) \rightarrow 0$ then it is clear that $(m - \hat{m}) \rightarrow 0$ as $t \rightarrow +\infty$, thus reaching the objective.

3.2.4. Simulation Results

In this section, we will provide numerical simulation results. We choose the message as $\mathrm{m(t)} = \frac{1}{2} + 10\sin(\frac{2\pi t}{T})$ where T = 10 seconds. Observer gains k and β are tuned by using self-tuning the algorithm proposed in [38], [39] and found as k = 13,0868 and β = 19,5921. Here we would like to note that the simulations were run for different values of k and β, and in all those runs, satisfactory performance was obtained.

The numerical solutions were run for 4 different cases. In Case 1, perfect communication channel between the transmitter and the receiver is assumed (i.e., no distortions). In Case 2, the transmitted chaotic signal $x(t)$ is considered to be subject to additive noise with an SNR of 10 dB. In Case 3, the transmitted chaotic signal $x(t)$ is considered to be perturbed by an additive sinusoidal disturbance. Finally in Case 4, a parametric uncertainty is considered by changing one parameter of the Lorenz System at the receiver part.

Case 1: The result of this simulation is shown in Figures 11-15. The message signal m(t) is shown in Figure 11, and the chaotic signal $x(t)$ is demonstrated in Figure 12. Figure 13 shows x(t) versus y(t) and y(t) versus z(t). In Figure 14, x̃(t) is shown which goes to 0 fast. The message signal $m(t)$, recovered message signal $\hat{m}(t)$ and the difference between original message and recovered message $\tilde{m}(t)$ are shown in Figure 15. As can be seen in Figure 15(c) which is m̃, we recovered the message with reasonable accuracy. Also we can see from the result m̃ goes to 0 so fast.

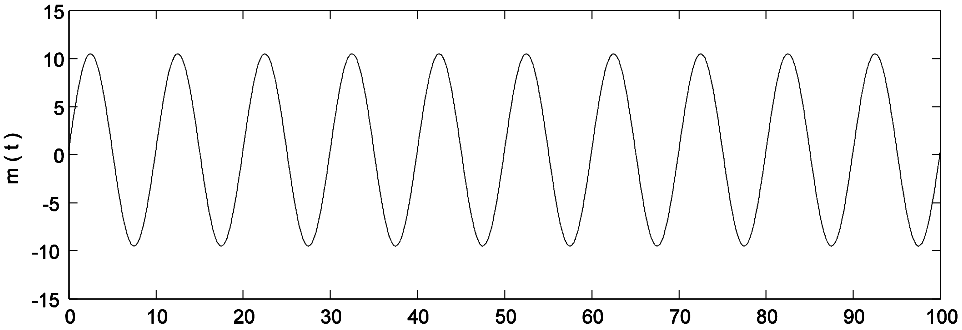


Figure 11. Case 1: The message signal m(t).

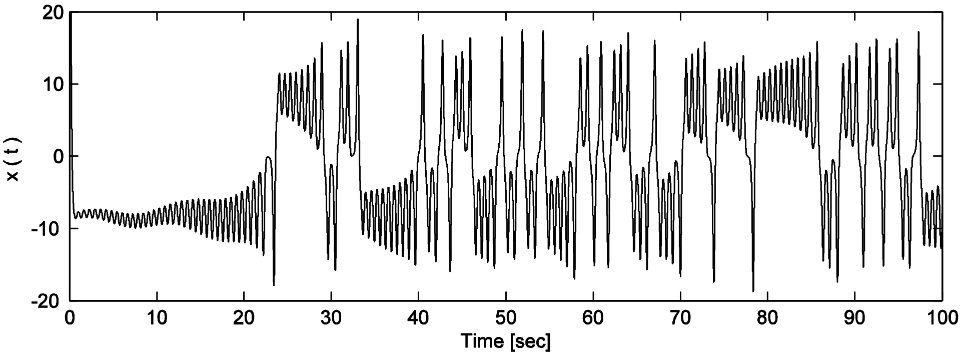


Figure 12. Case 1: x(t)

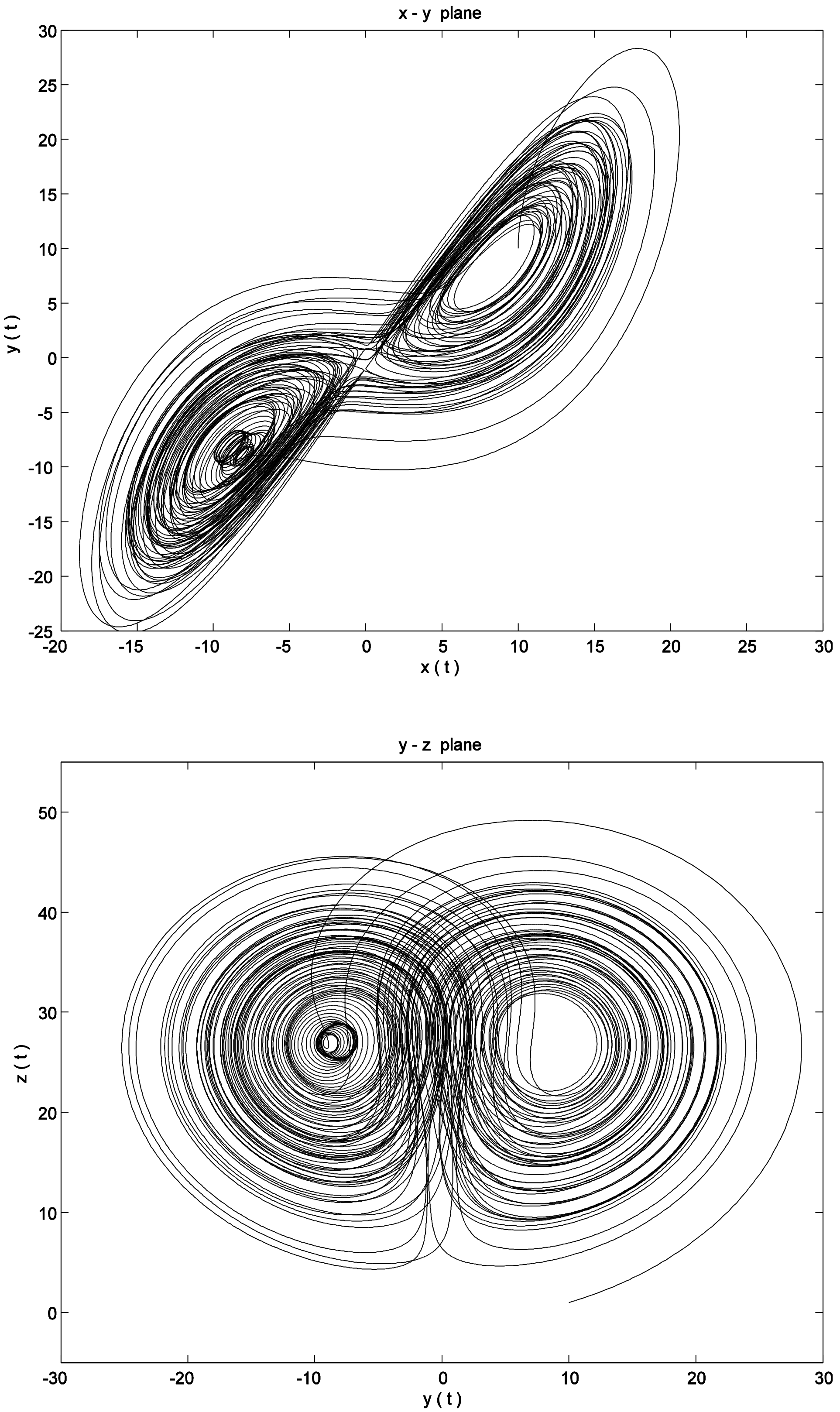


Figure 13. Case 1: Chaotic attractors of Lorenz System. The above attractor is x versus y, and the below one is y versus z.

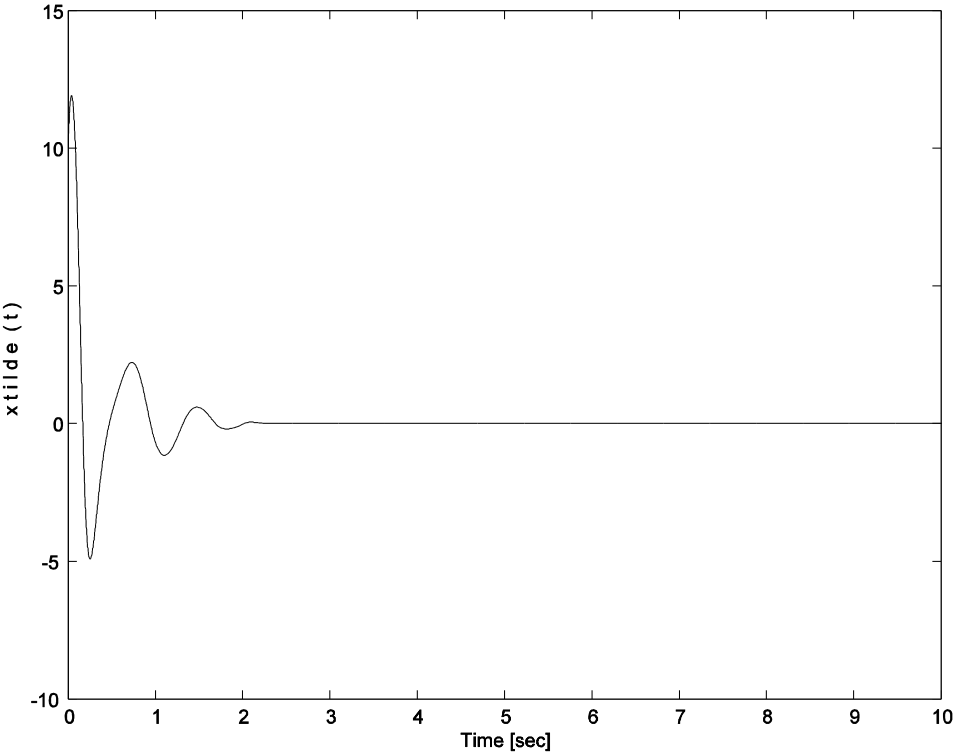


Figure 14. Case 1: $\tilde{x}(t)$

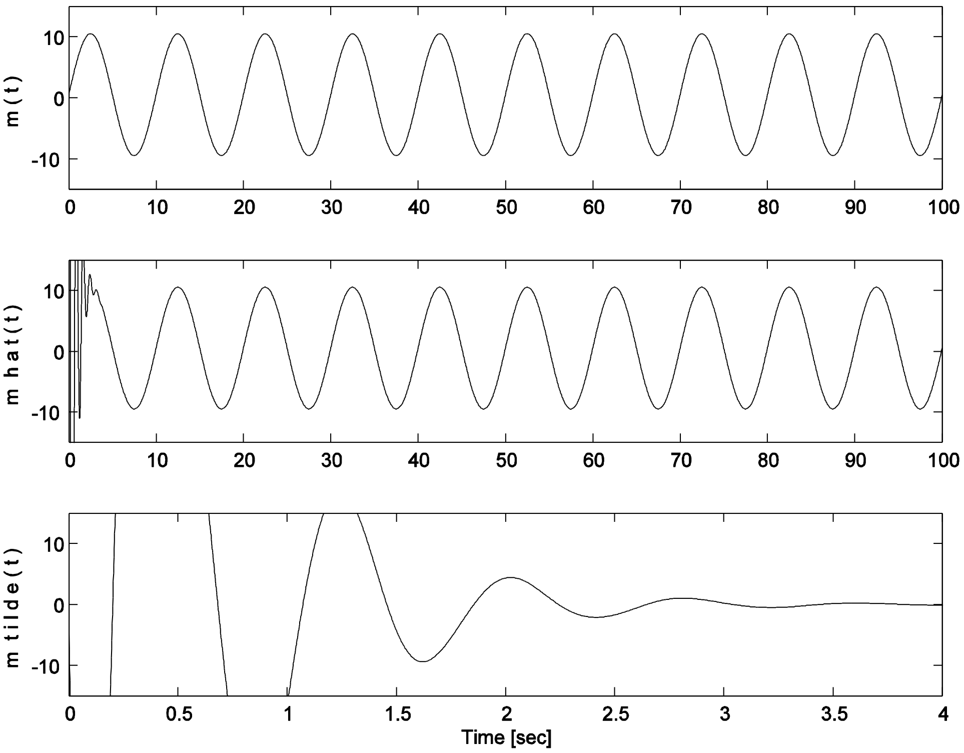


Figure 15. Case 1: m(t), $\hat{m}(t)$ and $\tilde{m}(t)$ for signum function

We simulated the system for 100 seconds. Although we showed m(t) and x(t) for 100 seconds to emphasize the a-periodicity of x(t) and also how accurate $\hat{m}(t)$ is, $\tilde{m}(t)$ is shown for 4 seconds to make it clear how fast $\tilde{m}(t)$ goes to zero.

We can show that our nonlinear observer works for high frequency sinusoidal signals. If we do the simulation for the message signal as $m(t) = \frac{1}{2} + 10\sin(\frac{20\pi t}{T})$ where T = 10 seconds. Observer gains are chosen as $k = 97{,}0341$ and $\beta = 23{,}1679$. The message signal m(t), recovered message signal $\hat{m}(t)$ and the difference between original message and recovered message $\tilde{m}(t)$ are shown in the Figure 16.

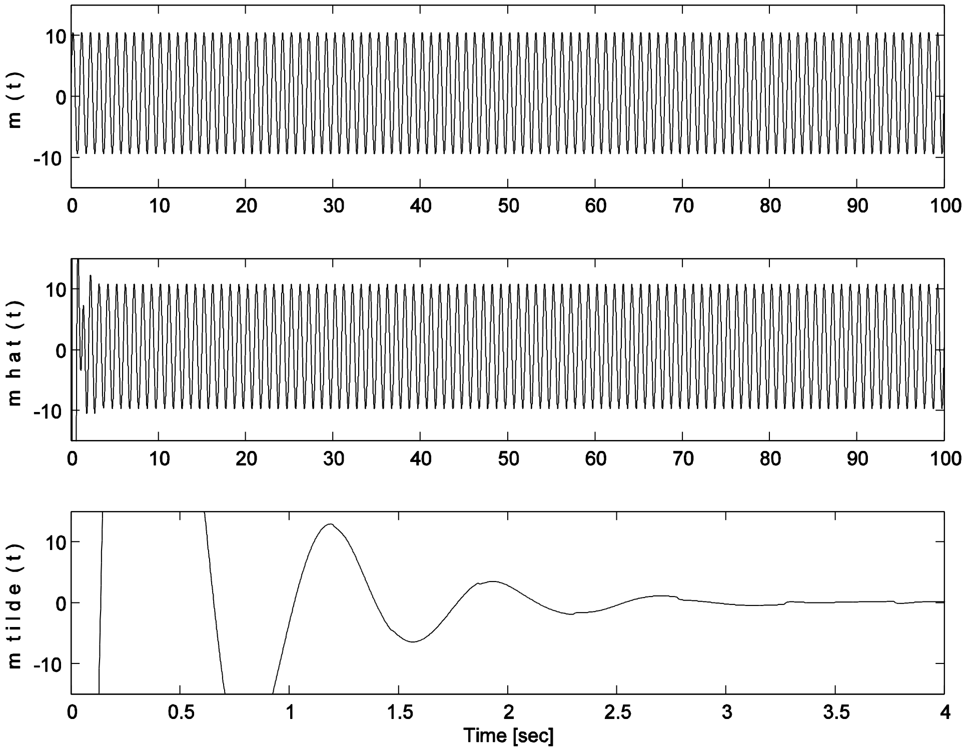


Figure 16. Case 1:m(t), $\hat{m}(t)$ and $\tilde{m}(t)$ for high frequency signum function

Case 2: It was assumed that the transmission channel was noise-free case 1. In this section, the message signal is transmitted to the receiver via a noisy channel. The channel type is Additive White Gaussian Noise (AWGN) which adds white Gaussian noise to the signal that passes through it. The relative power of noise in an AWGN channel is described by a Signal-to-Noise Ratio (SNR) value. It is assumed that

SNR value is 10 dB for this channel. The same observer gains are used for this simulation. Simulation results are shown in Figure 17 and Figure 18. In Figure 17, the observer error for x(t) (i.e., x̃(t)) and, in Figure 18, the transmitted message, the recovered message and the message observer error are given. As you can see from the Figures, while there is an increase at the error signal, the message signal is recovered within a good precision. However if SNR value increases then it would be tough to detect the message signal.

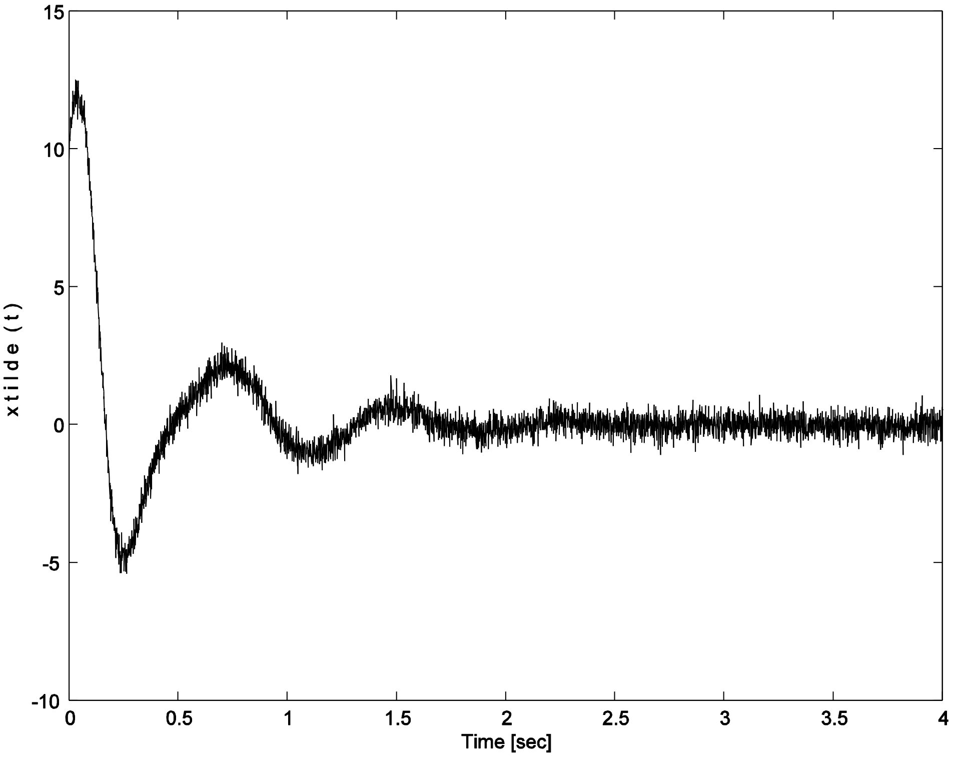


Figure 17. Case 2: x̃(t) for AWGN channel

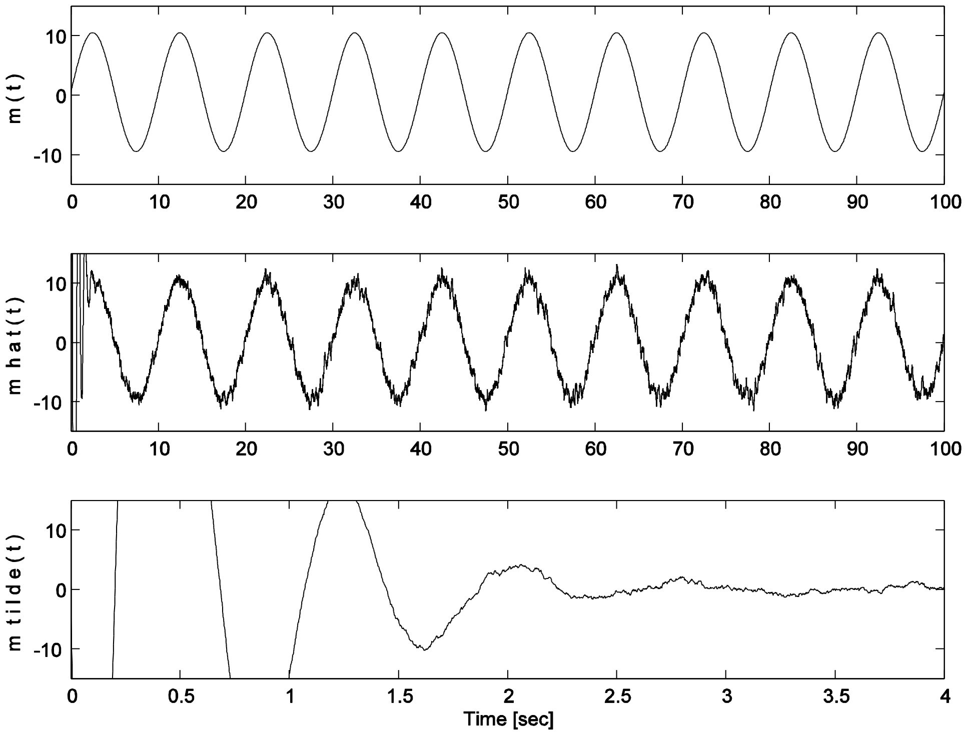


Figure 18. Case 2: m(t), $\hat{m}(t)$ and $\tilde{m}(t)$ for AWGN channel

Case 3: In this case, the transmission channel is assumed to impose an additive sinusoidal disturbance as $0.1\sin(\frac{2\pi t}{T})$ where T = 30 seconds. After the transmitted signal x(t) is sent to the receiver part, it is summed by this disturbance (i.e., x(t) obtained at the receiver part is equal to $x(t) + 0.1\sin(\frac{2\pi t}{T})$). The simulation results are shown in Figure 19 and Figure 20. In Figure 19, the observer error $\tilde{x}(t)$ and, in Figure 20, the transmitted message, the recovered message and the message observer error are given. As you can see from the Figures, while there is an increase at the error signal, the message signal is recovered within a good precision. However if the amplitude of the sinusoidal disturbance increases then it would be tough to detect the message signal.

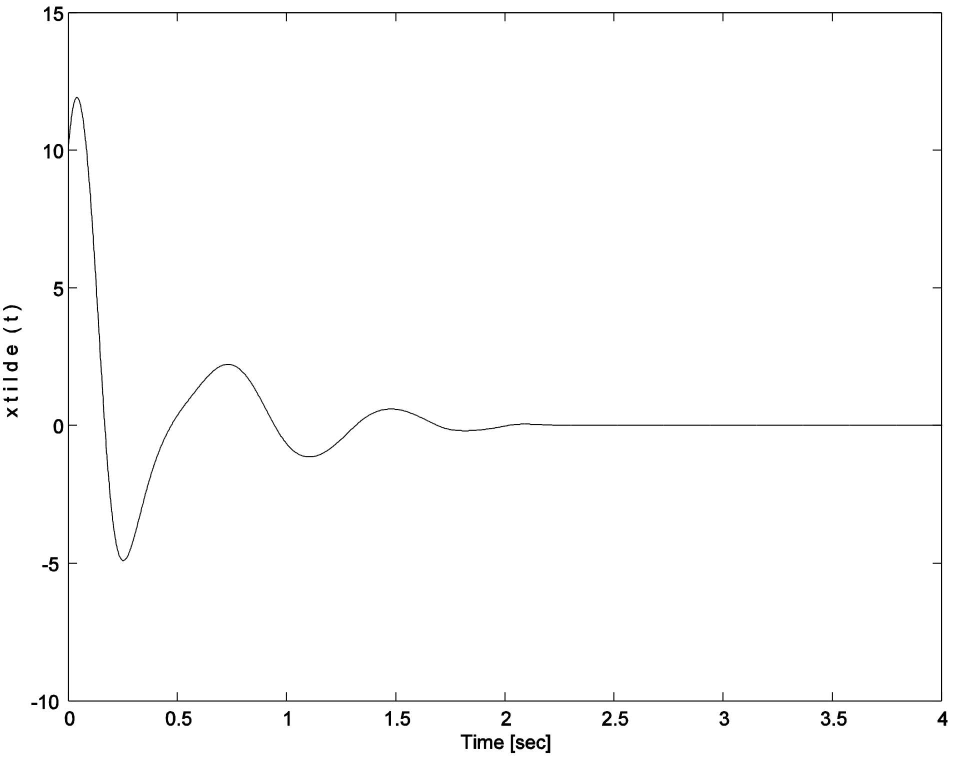


Figure 19. Case 3: x̃(t) for additive noise channel

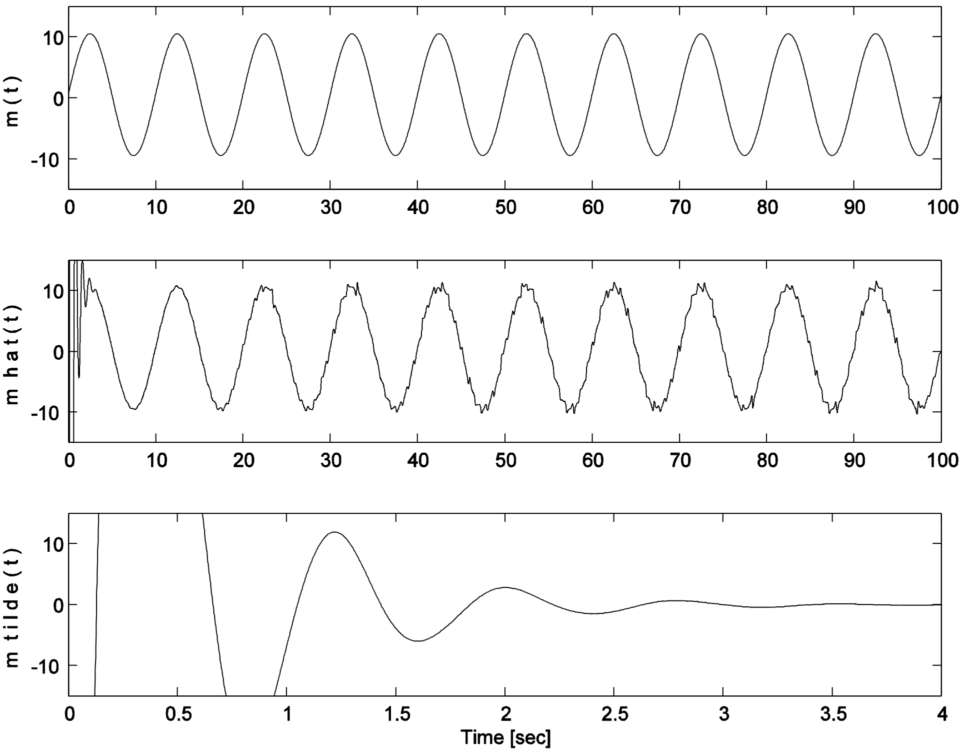


Figure 20. Case 3: m(t), m̂(t) and m̃(t) for additive noise channel

Case 4: Besides noise and additive disturbances, there can also be uncertainty at the system parameters. As mentioned before, the system parameters were chosen as σ = 10, r = 28 and b = 8/3. We now change one of the system parameters at the receiver part by choosing σ = 10.5. The simulation results for this scenario are shown in Figure 21 and Figure 22. In Figure 20, the observer error $\tilde{x}(t)$ and, in Figure 21, the transmitted message, the recovered message and the message observer error are given. As you can see from the Figures, while there is an increase at the error signal, the message signal is recovered within a good precision. However if the change at the parameters increases or all three system parameters are quite different then it would be tough to detect the message signal.

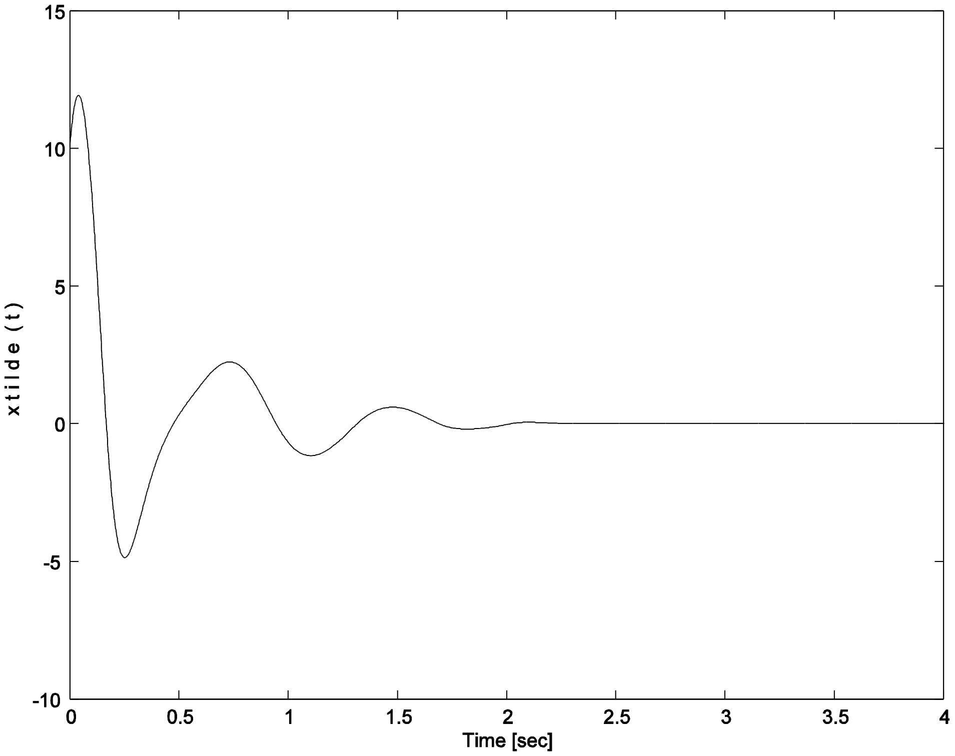


Figure 21. Case 4: $\tilde{x}(t)$ for parametric uncertainty case

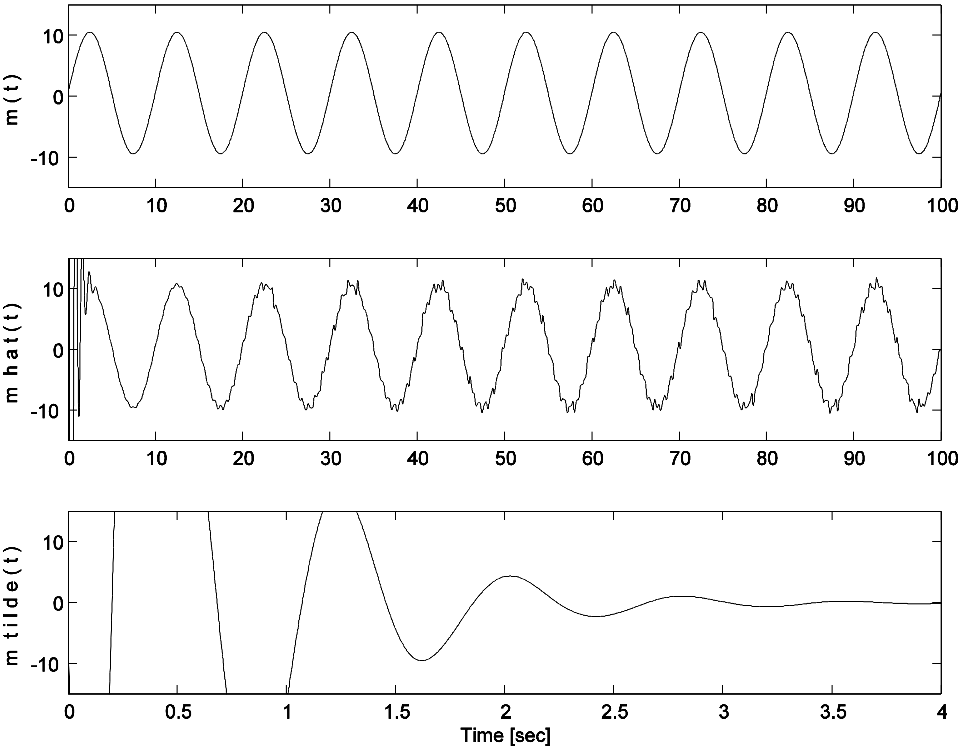
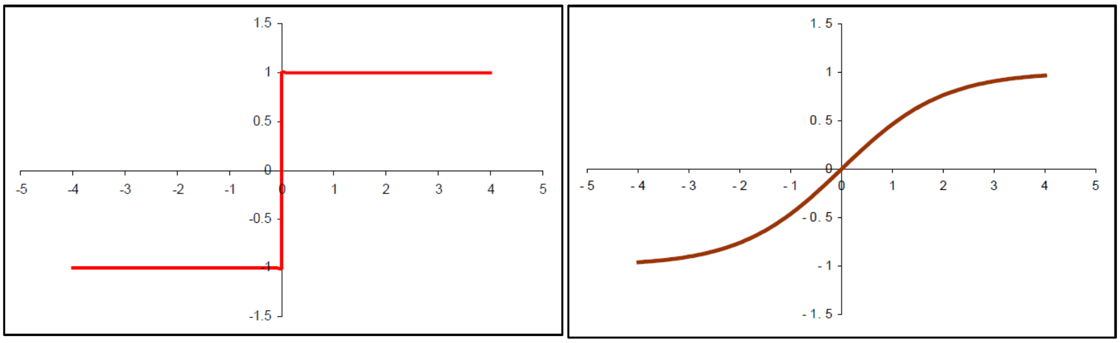


Figure 22. Case 4: m(t), $\hat{m}(t)$ and $\tilde{m}(t)$ for parametric uncertainty case

3.3. Hyperbolic Tangent Version of the Observer in Section 3.2

Recall that in the design of $\hat{m}(t)$ we used $\text{sgn}(\tilde{x})$. As extensively discussed in the literature, hyperbolic tangent function is an approximation of the signum function. See Figure 22 for signum and tangent hyperbolic functions. Mathematically, it is possible to say that, hyperbolic tangent function for large Ӄ is a smooth approximation of the signum function is in the sense that

$$sgn(\tilde{x}) \approx \tanh(\text{Ӄ}\tilde{x}). \tag{42}$$



(a) (b)

Figure 23. (a) Signum Function, (b) Tanh Function for Ꞵ=1

This motivated us to design hyperbolic tangent function version of the observer as

$$\hat{m}(t) = (k+1)\left[\tilde{x}(t) - \tilde{x}(t_0) + \int_0^t \tilde{x}(\sigma)d\sigma\right] + \beta \int_0^t tanh\,(\tilde{x}(\sigma))d\sigma \qquad (43)$$

where $\tilde{x}(t)$, $\tilde{\mathrm{y}}(t)$ and $\tilde{\mathrm{z}}(t)$ were designed the same as the signum observer (13), (14) and (15). Notice that the $\tanh(\tilde{x})$ term in our new observer is not a close approximation of the $sgn(\tilde{x})$ as the constant multiplying $\tilde{x}$ in $\tanh()$ is equal to 1. This causes the need for stability analysis to be modified for this new observer.

Specifically, we need to modify $P(t)$ in (30) as

$$P = \gamma_p - \int_0^t r(\sigma)[\dot{m}(\sigma) - \beta tanh(\tilde{x}(\sigma))]\, d\sigma \qquad (44)$$

and nonnegativeness of this term must be ensured. In [40], it was proven that, after satisfying a high gain condition by β, and when $|\tilde{x}(t)| > \epsilon_1$ for some small $\epsilon_1 \in R$, then $P(t) > 0$ and when $|\tilde{x}(t)| < \epsilon_1$ then $P(t) < 0$ is not valid anymore. As a result it is possible to drive $\tilde{\mathrm{m}}$ to a small value. A comprehensive analysis was given in [40].

The observer gains k and β are tuned by using the algorithm proposed in [41] and found as k = 13,2245 and β = 18,1966. If we simulate our system with the new observer in (43) (i.e., hyperbolic tangent function) we obtain $\tilde{x}(t)$ as in Figure 24, and m(t), $\hat{\mathrm{m}}$(t) and $\tilde{\mathrm{m}}$(t) for hyperbolic tangent function are shown in Figure 25.

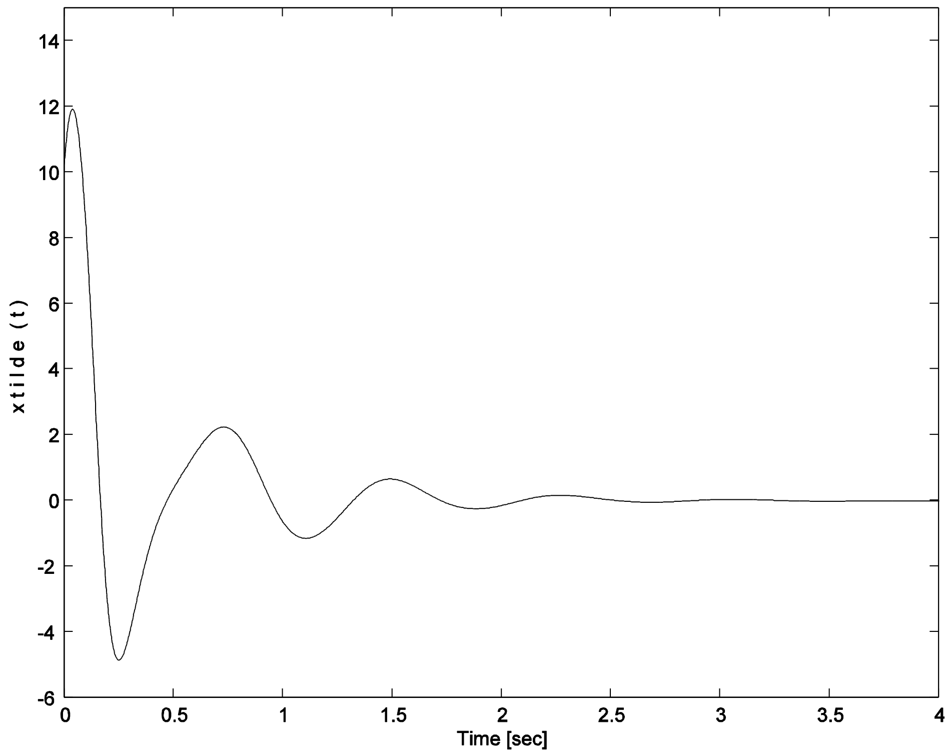


Figure 24. Tanh observer: Case 1: x̃(t)

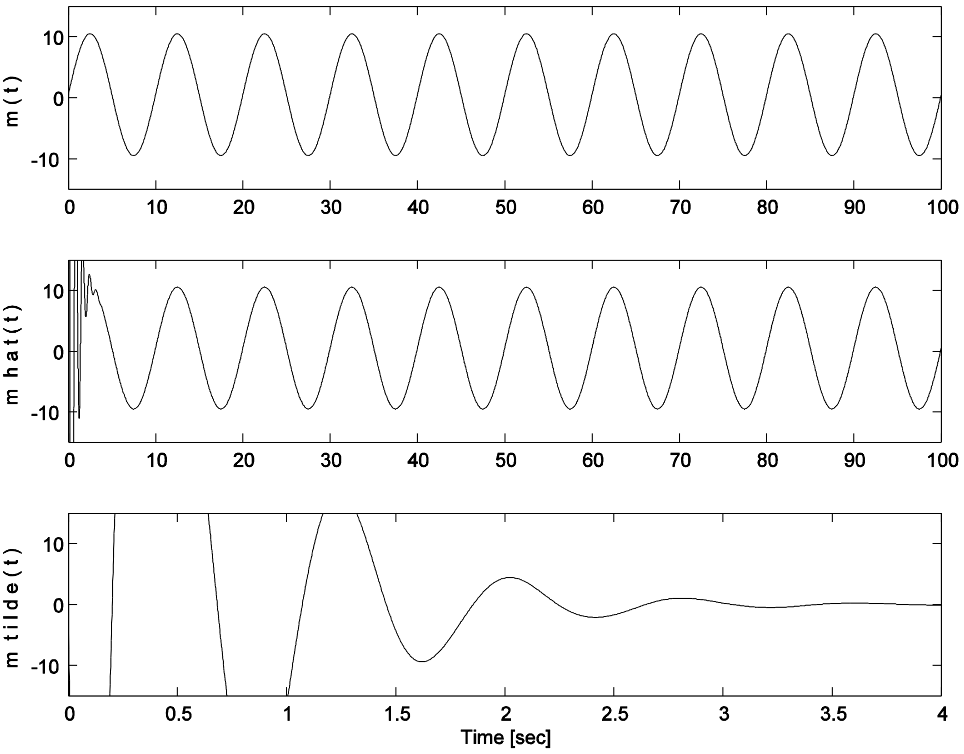


Figure 25. Tanh observer: Case 1:m(t), m̂(t) and m̃(t)

As can be seen from the Figures 24-25, changes at the observer that is done resulted in no difference at the simulation results.

Simulation results for AWGN channel, additive noise channel and parametric uncertainty cases are shown in following Figures.

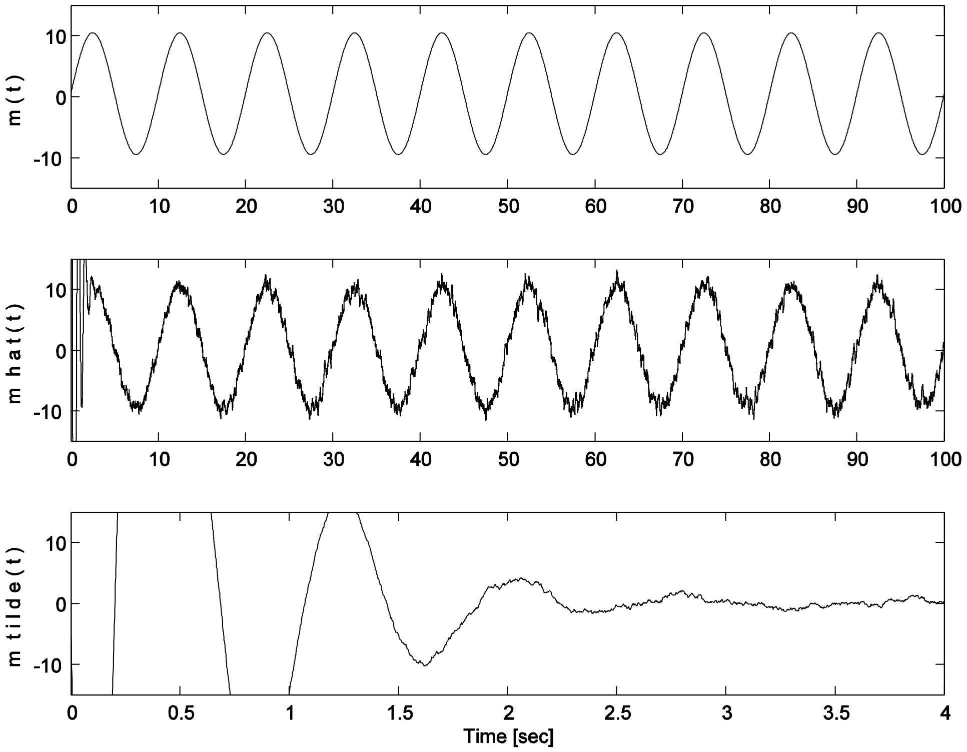


Figure 26. Tanh observer: Case 2: m(t), $\hat{m}(t)$ and $\tilde{m}(t)$

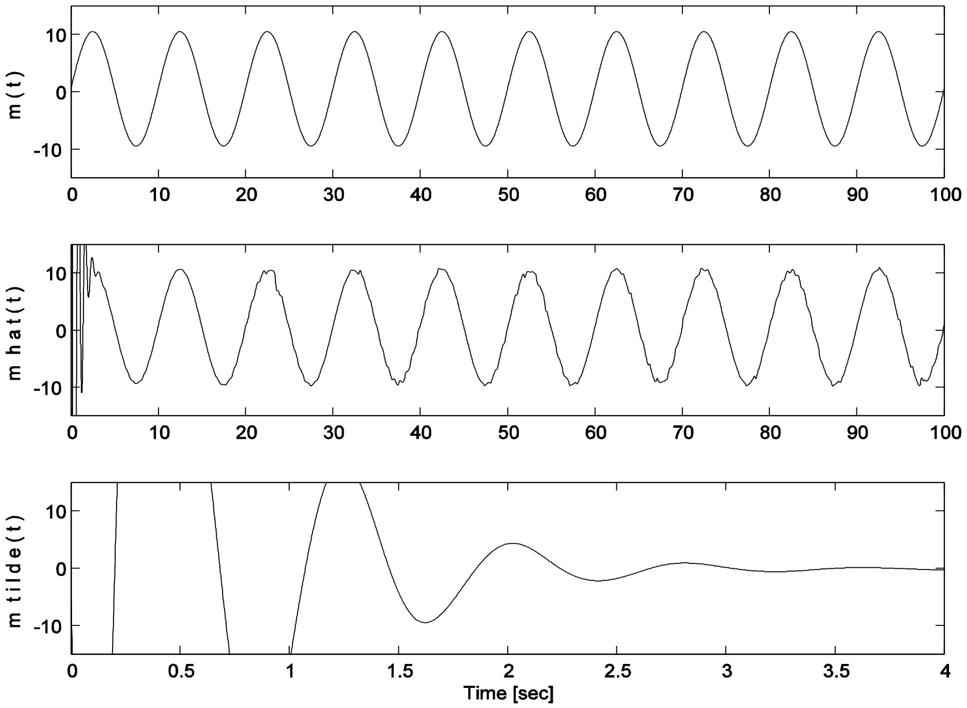


Figure 27. Tanh observer: Case 3: m(t), $\hat{m}(t)$ and $\tilde{m}(t)$

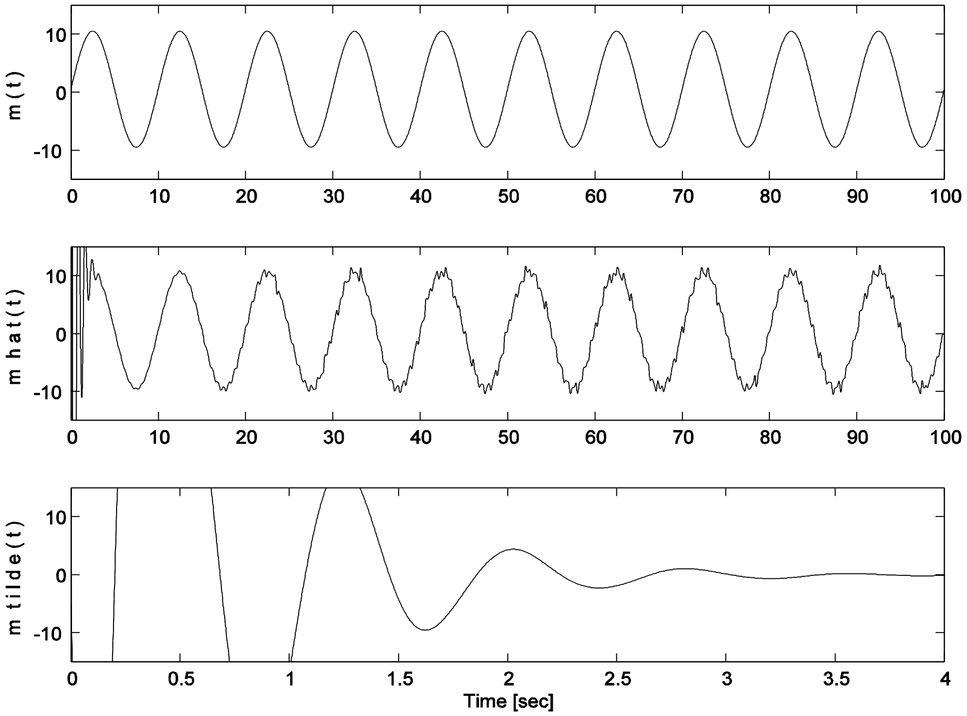


Figure 28. Tanh observer: Case 4: m(t), $\hat{m}(t)$ and $\tilde{m}(t)$

3.4. Saturation Function Version of the Observer in Section 3.2

Alternatively, $sgn(\tilde{x})$ can be approximated by the function saturation $sat(\tilde{x})$ in the design of $\hat{m}(t)$. As broadly discussed in the literature, saturation function is another approximation of the signum function. See Figure 29 for signum and saturation functions. There is a smooth approximation of the saturation function for small ∈

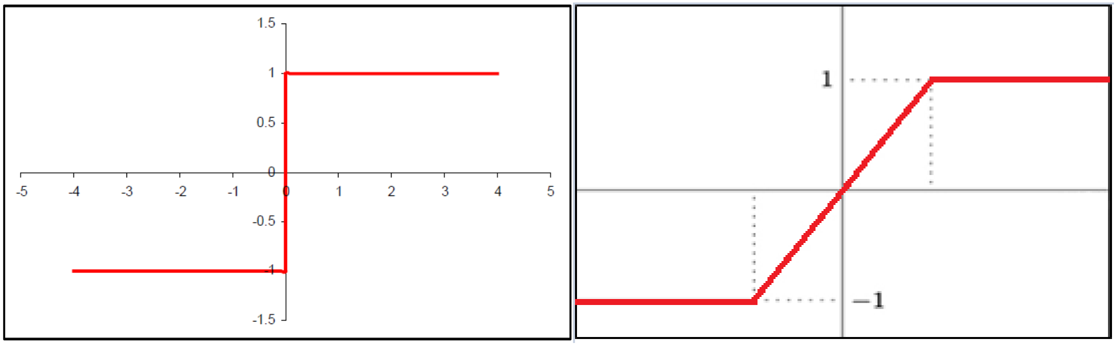
$$sgn(\tilde{x}) \approx \mathrm{sat}(\tilde{x}/\in). \tag{45}$$

The new observer design is given as

$$\hat{m}(t) = (k+1)\left[\tilde{x}(t) - \tilde{x}(t_0) + \int_0^t \tilde{x}(\sigma)d\sigma\right] + \beta\int_0^t sat(\tilde{x}(\sigma)/\in)d\sigma \tag{46}$$

where ∈ = 1, and $\tilde{x}(t)$, $\tilde{y}(t)$ and $\tilde{z}(t)$ were designed the same as (13),(14) and (15).

The observer gains k and β are tuned by using a similar algorithm to that of [41] and found as k = 13,2038 and β = 19,2507. If we simulate our system with these new observer in (46) (i.e., saturation function), we obtain x̃(t) as in Figure 30-34. Simulation results for AWGN channel, additive noise channel and parametric uncertainty cases are shown in following Figures.



(a) (b)

Figure 29. (a) Signum Function, (b) Saturation Function where ∈ = 1

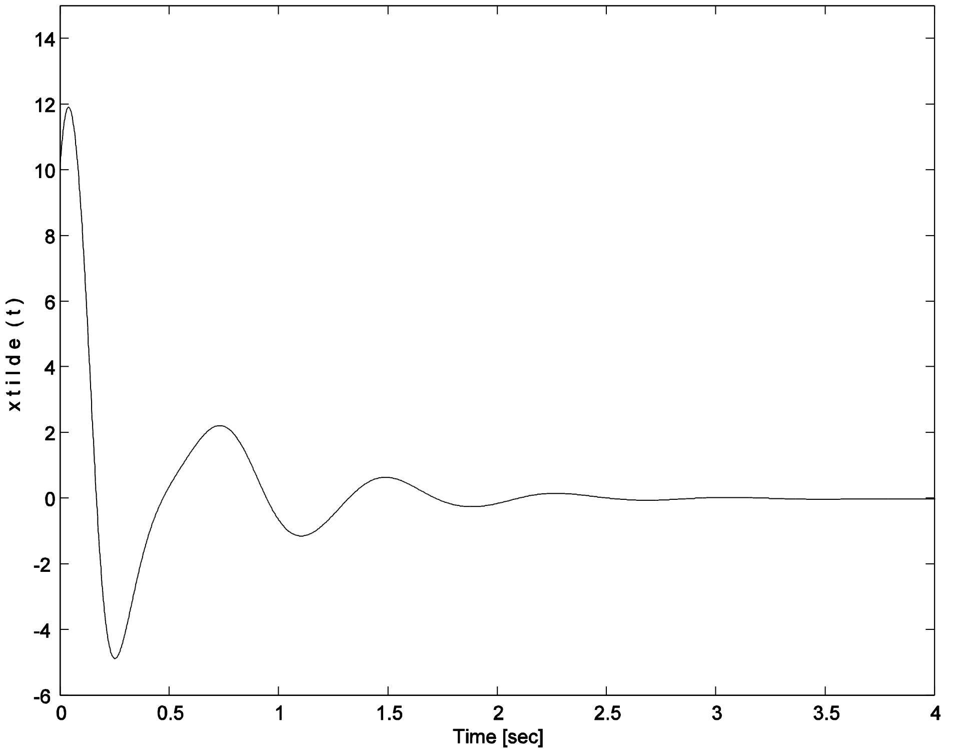


Figure 30. Sat observer: Case 1: x̃(t)

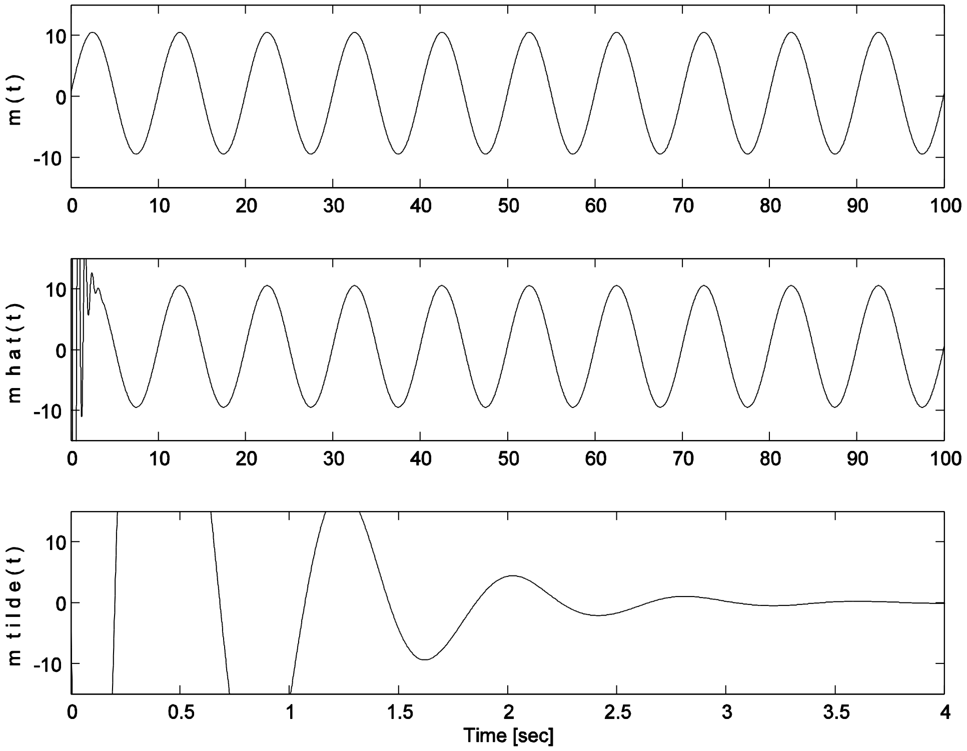


Figure 31. Sat observer: Case 1: m(t), m̂(t) and m̃(t)

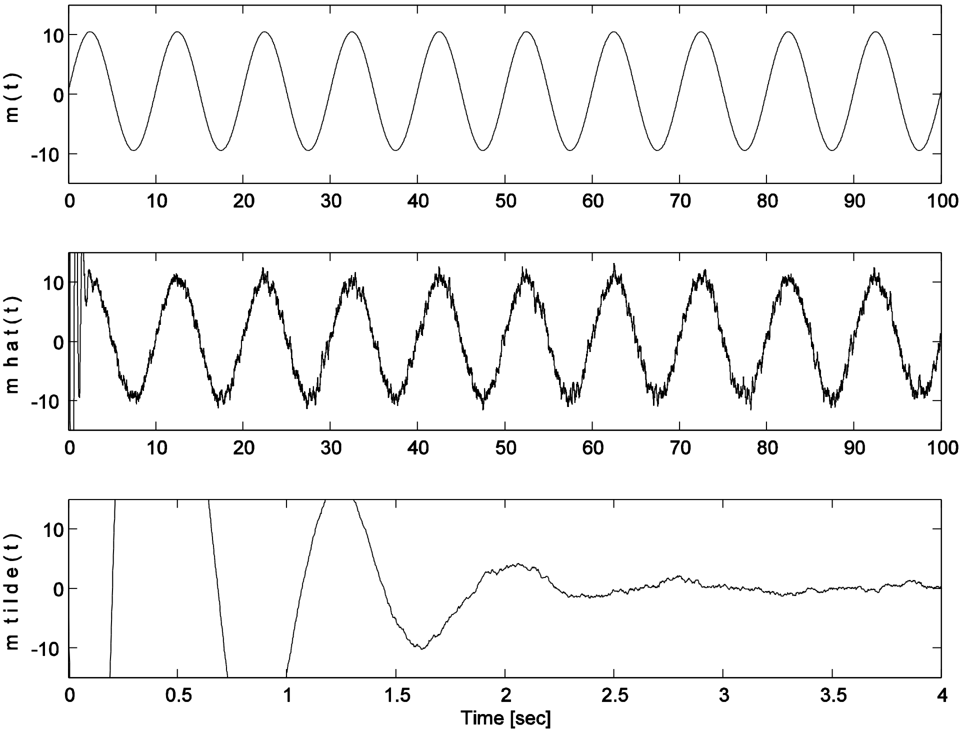


Figure 32. Sat observer: Case 2: m(t), $\hat{m}(t)$ and $\tilde{m}(t)$

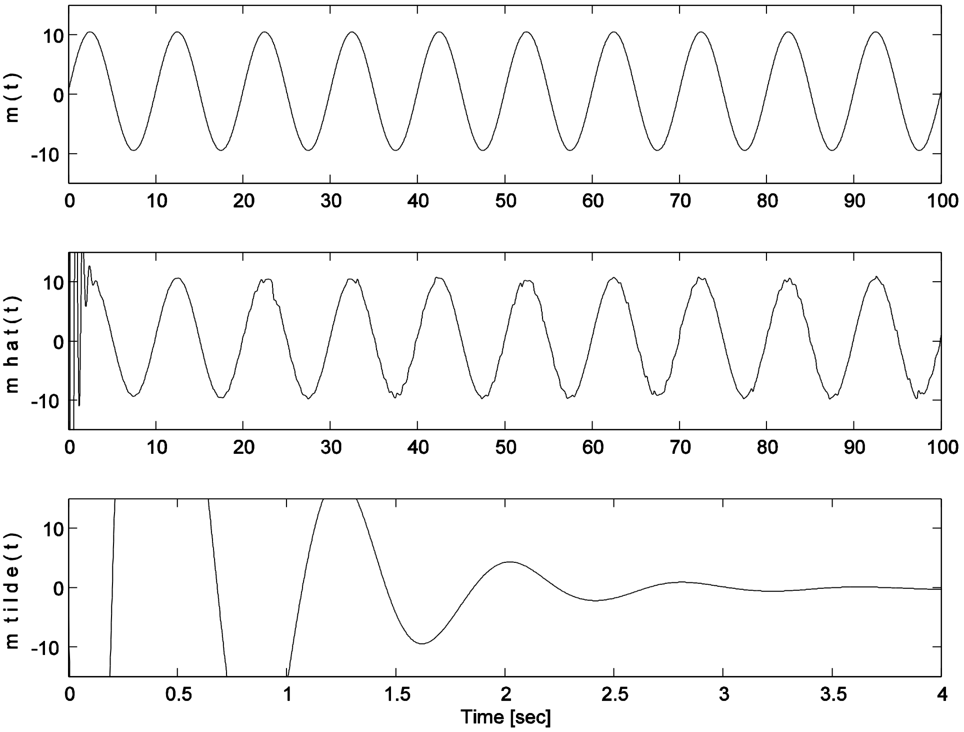


Figure 33. Sat observer: Case 3: m(t), $\hat{m}(t)$ and $\tilde{m}(t)$

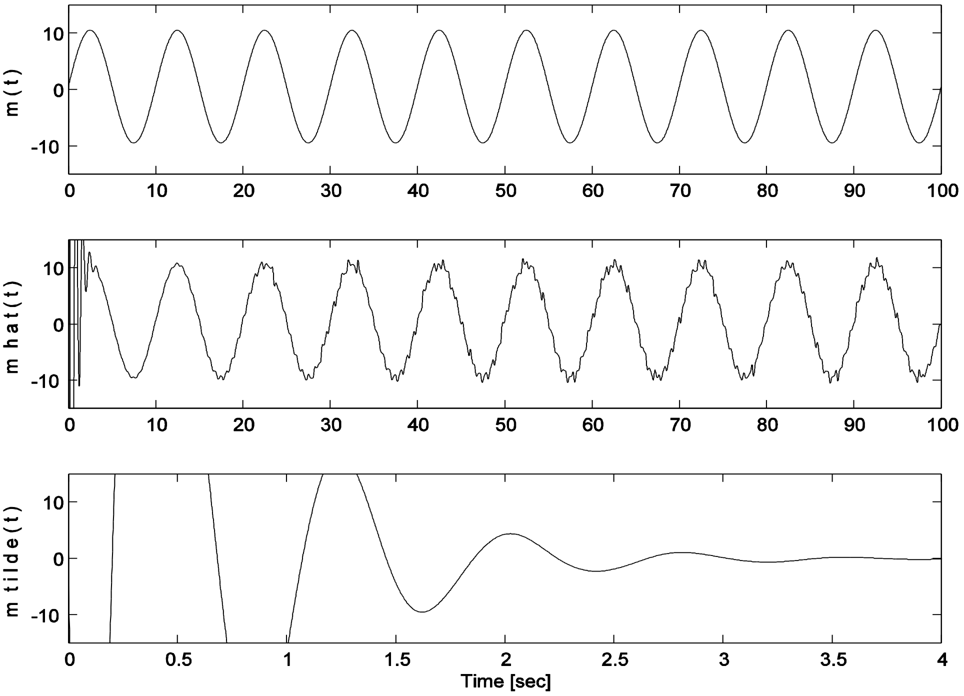


Figure 34. Sat observer: Case 4: m(t), $\widehat{\mathrm{m}}(\mathrm{t})$ and $\widetilde{\mathrm{m}}(\mathrm{t})$

Finally, we compare these three novel nonlinear observers by calculation the squared error during the simulation run via the formula;

$$\int_0^{100} \tilde{x}^2(\sigma)\, d\sigma. \tag{47}$$

The observers are compared for case 2 where the transmission channel is disturbed by AWGN with 10 dB SNR. When above expression yielded 28.1321, 28.0289, and 28.0244, for the signum function, tanh function, sat function based observers, respectively. It is clear that all three observers performed similarly.

3.5. Nuclear Simulation

In [42], it is stated that [direct quote] “Secure long-distance monitoring of plant data is becoming increasingly important for safe and efficient operation of nuclear power plants.” Instead of using a sinusoidal signal of the form $\mathrm{m(t)} = \frac{1}{2} + 10\sin(\frac{2\pi t}{T})$ as the message signal, we take a signal from the following reduced-order Boiling Water Reactor model [42] is considered as an example of MOS:

$$\begin{bmatrix} \dot{n} \\ \dot{c} \\ \dot{T} \\ \dot{\gamma} \\ \dot{v} \end{bmatrix} = \begin{bmatrix} -\beta_1/\Delta & \lambda & D/\Delta & 1/\Delta & 0 \\ \beta_1/\Delta & -\lambda & 0 & 0 & 0 \\ \alpha_1 & 0 & -\alpha_2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & -\alpha_3 & -\alpha_4 \end{bmatrix} \begin{bmatrix} n \\ c \\ T \\ \gamma \\ v \end{bmatrix} + \begin{bmatrix} (n/\Delta)(DT+\gamma) \\ 0 \\ 0 \\ 0 \\ -k_1 T \end{bmatrix} \qquad (48)$$

as the message signal. In (48), $n(t)$ is excess neutron population normalized to the steady-state neutron density and is chosen as the message signal to be encrypted. Other states are $c(t)$, $T(t)$, $\gamma(t)$ and $v(t)$. Model parameters of the reactor are given in Table 2.

Model Parameters	Values	Model Parameters	Values
α_1	25.04	D	-2.52 x 10^{-5}
α_2	0.23	Δ	0.0056
α_3	2.25	β_1	4 x 10^{-5}
α_4	6.82	λ	0.08
k_1	4.2 x 10^{-3}		

Table 2. Model Parameters for Nuclear Simulation [43]

Firstly, by utilizing the information in [43], we tried to obtain a replica of the results in [42]. As can be seen in
Figure 35, the message signal of $n(t)$ obtained in Matlab Simulink is exactly same shown as the one in [42].

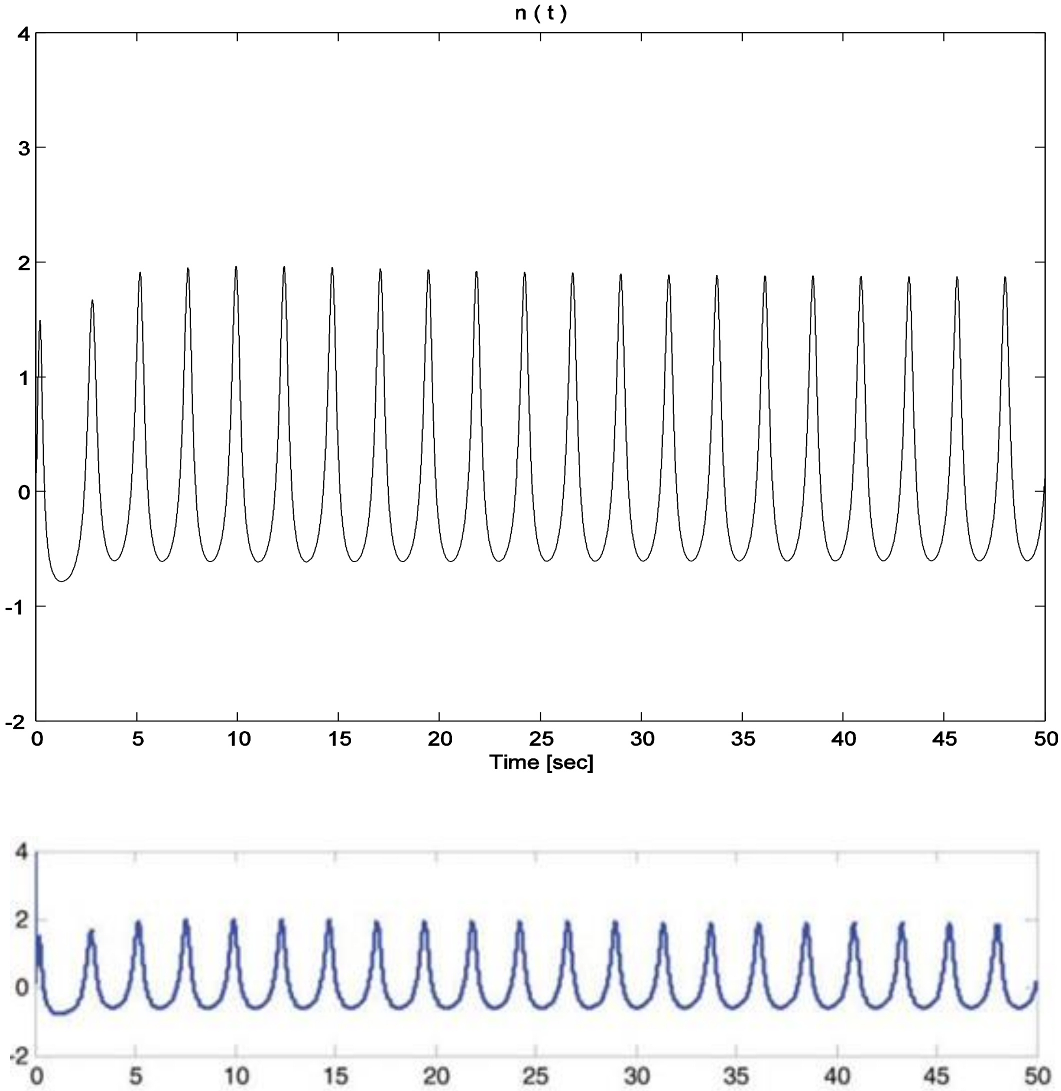


Figure 35. The message signal n(t), obtained from Matlab (top) and from [42] (bottom).

After obtaining the signal n(t), it is used as the message signal for our Lorenz Chaotic System. Simulations are run for all three observers, separately. The observer gains were same as the previous values.

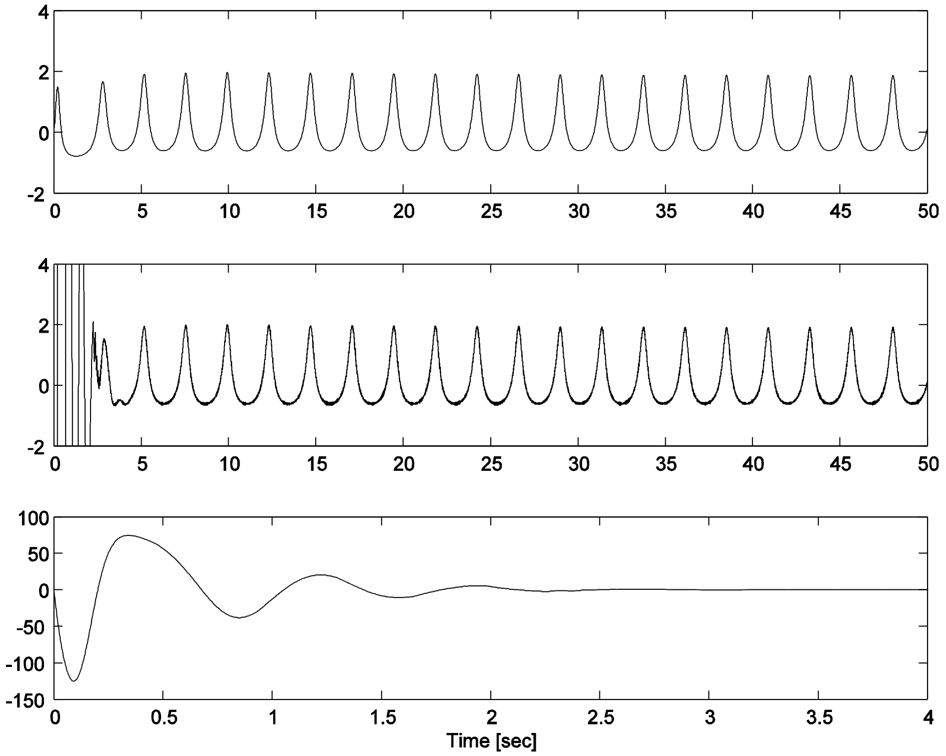


Figure 36. Nuclear simulation for the signum observer: The above figure is m(t) (where m(t) = n(t)), $\hat{m}(t)$ and the below one is $\tilde{m}(t)$ for signum function

As can be seen at the Figure 36(c) the difference between the transmitted message and the received message goes zero fast.

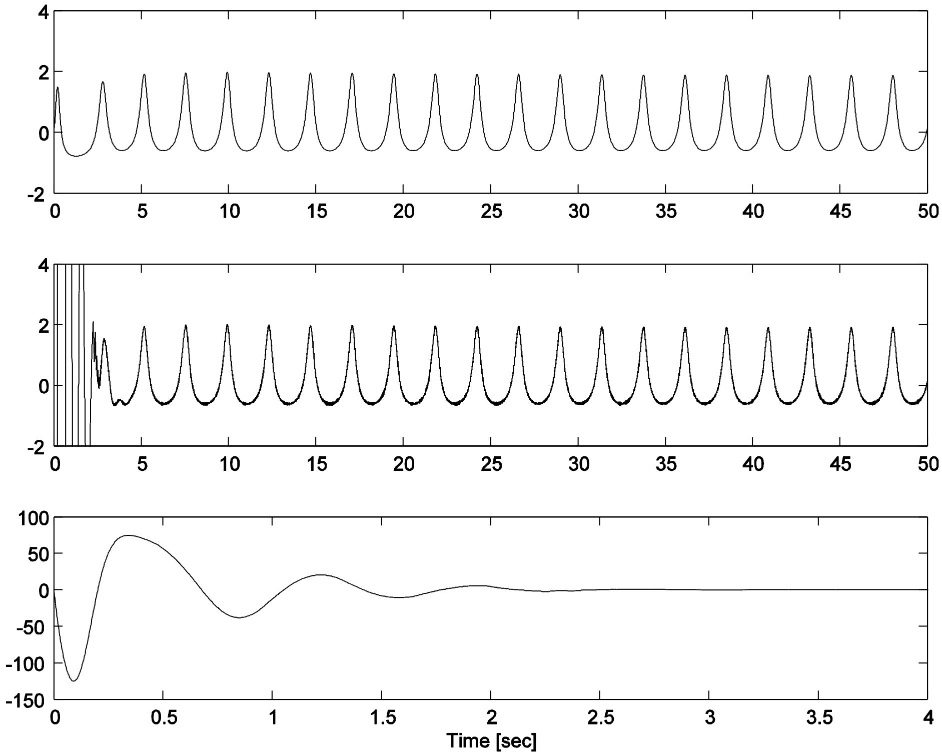


Figure 37. Nuclear simulation for the tanh observer: The above figure is m(t) (where m(t) = n(t)), $\hat{m}(t)$ and the below one is $\tilde{m}(t)$

Nuclear simulation is run with the hyperbolic tangent function version and the results are shown in Figure 37. As can be seen in Figure 37(c), $\tilde{m}(t)$ goes zero fast.

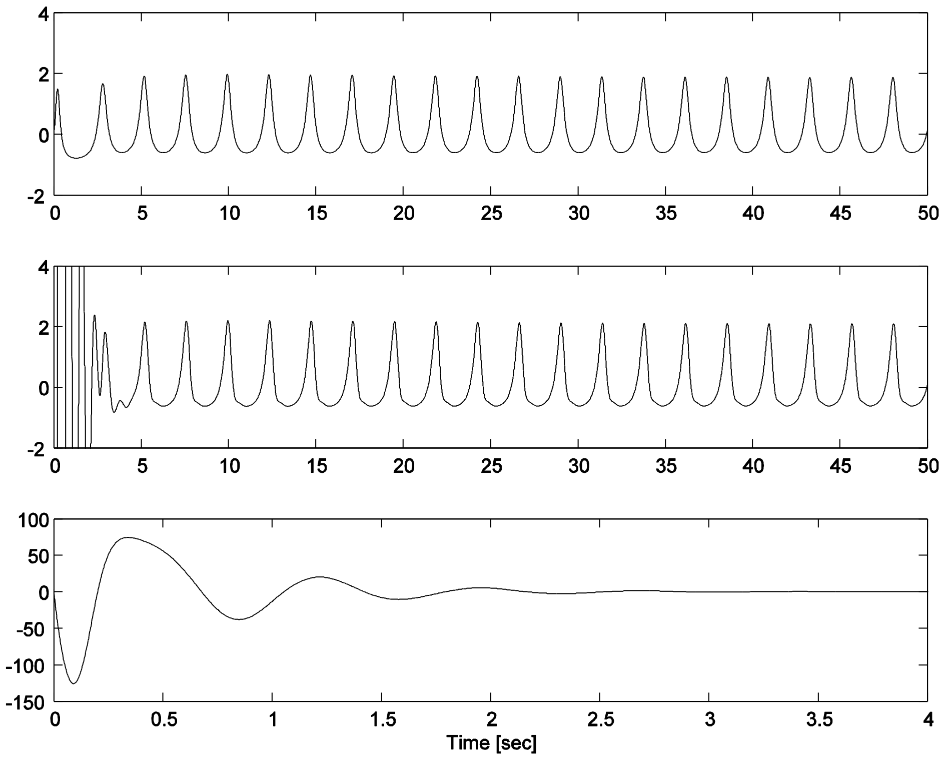


Figure 38. Nuclear simulation for saturation function. The above figure is m(t) (where m(t) = n(t)), $\hat{m}(t)$ and the below one is $\tilde{m}(t)$.

Nuclear simulation is run for the last observer which is saturation function version, and $\tilde{m}(t)$ goes zero fast for this observer, as can be seen from Figure 38(c).

3.6. Security Analysis of Our System

In his book [44], Tao-Yang defines the relationship and difference between classical cryptography and chaotic cryptography as [direct quote] “In classical cryptology, the cryptography is a systematic science with well-established analytical and synthetic principles, and the cryptanalysis is rather like an art depending heavily on intuition and experience than a science. Also, chaotic cryptography has been developed rapidly in recent years while chaotic cryptanalysis is still at its beginning with very few results littered among a huge ocean of chaotic cryptography literature.” In this point of view, the differences and the similarities between classical cryptography and chaotic cryptography, and also advantages and disadvantages between them are going to be analyzed in this section. Detailed information about cryptography can be found in [45], [46]. It is possible to find numerous papers in the literature about cryptanalysis of chaos-based communication methods [19], [47], [48], [49], [50], [51], [52], [53], [54], [55], [56].

There are mainly three possible ways to break a cryptosystem;

- Transmitted ciphertext signal is used for re-assembling the message signal.
- The message signal can be recovered by extracting the chaotic carrier signal by the difference between transmitted ciphertext signal and extracted chaotic carrier signal.
- Transmitted signal is used for estimating the key (or secret) parameters. [19]

Although chaotic communication is considered as secure, there are some ways to decode the message signal despite the lack of parameter values, keys or exact knowledge of the system that is used. Specifically, in [49], two different algorithms to break the cryptosystems using Lorenz's attractors are presented. These algorithms, namely Power Analysis Attack and Generalized Synchronization Attack, are used to examine the security our observer design.

3.6.1. Power Analysis Attack

The Lorenz System in [49] is simulated and obtained that the algorithm breaks the chaotic system as shown in Figure 39. The algorithm starts by squaring the ciphertext signal $x(t)$, then low pass-filtering of this squared ciphertext signal, and finally, binary quantization is applied to this signal. The low-pass filter is a four pole Butterfly filter with a cutoff frequency of 0.5 Hz. Smith-Trigger is then used as a quantizer with switch on point at 85 and switch off point at 5. These points are different from [49] to obtain better recovered plaintext.

As you can see in the Figure 39, the plaintext is recovered (with some shift on the time domain) without the knowledge of the kind of the system [49] that was used for encryption, and neither its parameters and nor its keys.

If we apply the same scheme to signum function observer, we get the results in Figure 40. As you can see, the recovered message signal (plaintext) is not the time shifted version of the original message. Although we change switch points, we do not get the transmitted plaintext as the recovered plaintext. This shows that the algorithm break the system in [49] does not work for our system.

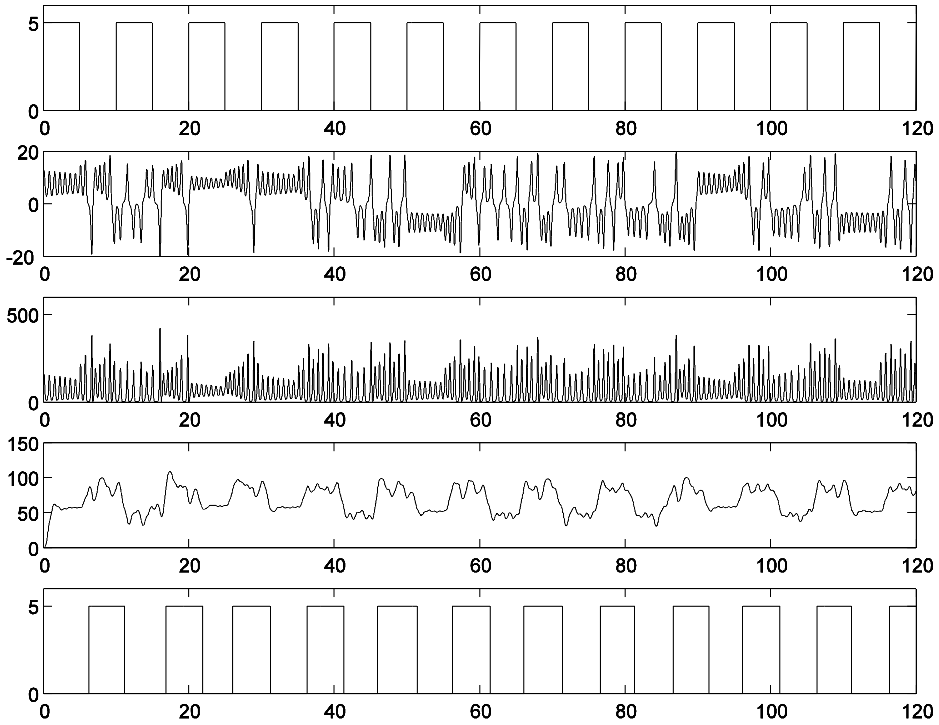


Figure 39. Message signal (plaintext), $x(t)$ (ciphertext), $x^2(t)$ (squared ciphertext signal), low-pas filtered $x^2(t)$, recovered plaintext from above to below.

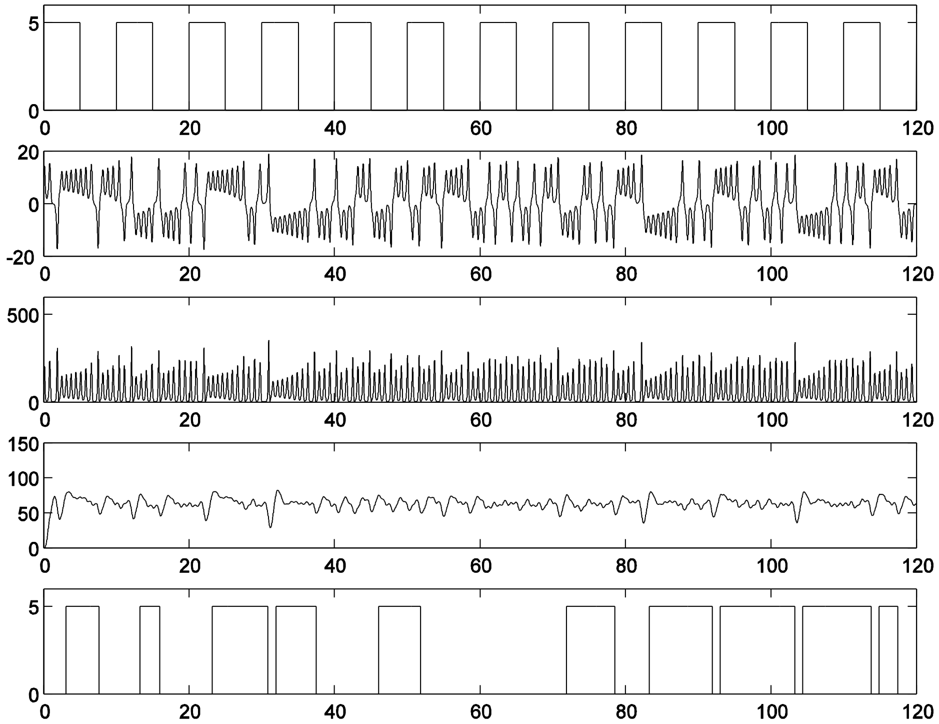


Figure 40. Power Analysis Attack applied to our signum function observer system. Message signal (plain text), x(t) (ciphertext of our system), $x^2(t)$ (squared ciphertext signal), low-pas filtered $x^2(t)$, recovered plaintext from above to below.

3.6.2. Generalized Synchronization Attack

In [49], the second way of breaking a chaotic communication system is based on the knowledge of the kind of chaotic system is used for encryption, but still lack of knowing neither its parameters nor initial condition values. This algorithm starts with calculating the difference between x(t) and $\hat{x}(t)$, second step is multiplying x(t) by $\tilde{x}(t) = \hat{x}(t) - x(t)$, then multiplied signal is low-pass filtered and, finally, a binary quantizer is used to re-generate the original message signal (plaintext). Switch on point was at 11, switch off point was at 9 for this attack. The simulation results for the given system are shown in Figure 41.

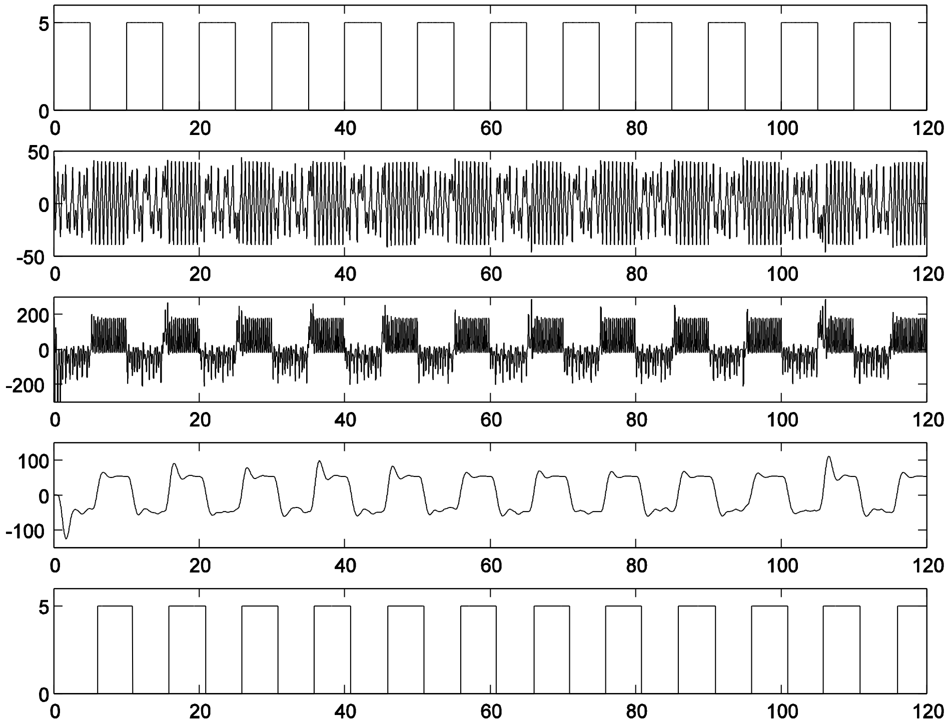


Figure 41. Message signal (plain text), x(t) (ciphertext), $x(t)$ multiplied by $\tilde{x}(t)$, low-pass filtered version of the multiplied signal, recovered plaintext from above to below.

As can be seen in Figure 41, recovered plaintext is time shifted version of the original plaintext. So the algorithm works for this system. If we apply this security algorithm to our system and make the simulations again, we get the Figure 42.

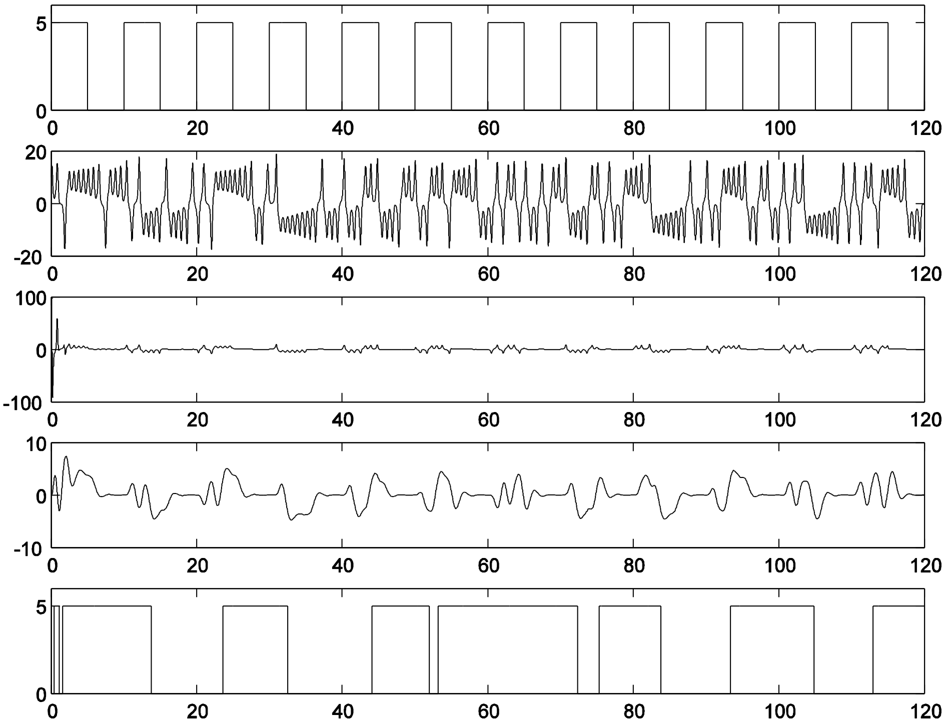


Figure 42. Generalized Synchronization Attack for our signum function observer system. Message signal (plain text), x(t) (ciphertext), x(t) multiplied by $\tilde{x}(t)$, low-pass filtered version of the multiplied signal, recovered plaintext from above to below.

As shown in Figure 42 the recovered message signal (plaintext) is not similar the original message. Although we change switch points, we do not get the transmitted plaintext as the recovered plaintext. That shows us this algorithm to break the system does not work for our system.

Although these two algorithms did not break our observer design, we believe that our system must be tested extensively by other algorithms in the literature.

3.7. Summary

In this chapter, after giving the General Lorenz System, we proposed a nonlinear observer for the Lorenz Chaotic System described in Section 3.2. Observer design and stability analysis of this system are provided and also we presented our simulation results via Matlab Simulink where robustness to the channel imperfections were also demonstrated. In Sections 3.3 and 3.4, we change our observer design by replacing the signum function with hyperbolic tangent and saturation functions, respectively. In Section 3.5, we showed that our observer works not only for a sinusoidal message signal but also a signal generated by a dynamical system (i.e., a nuclear reactor model) via simulations. In section 3.6, we applied some decryption methods from the literature to our observer and tested its security.

CHAPTER 4

CONCLUSION

In this thesis, chaotic communication was studied. An observer-based approach was followed to extract message encrypted in a chaotic signal. Specifically, a message signal was considered to be added to the dynamics of the Lorenz chaotic system which served as the transmitter. The output of the transmitter was considered as the input to the receiver which was a replica of the Lorenz chaotic system on the transmitter side. An observer was designed to obtain the states of the Lorenz chaotic system and a novel nonlinear observer was designed to estimate the message signal. Stability of the closed-loop system was investigated via Lyapunov-based arguments and convergence of the error signals to zero was proven. In addition, after modifications to the nonlinear argument in the message observer, two nonlinear observers were proposed.

To demonstrate the performance of the proposed observers, extensive numerical simulations were performed. Robustness to imperfectnesses such as additive noise, additive perturbations and parametric uncertainties were shown numerically. For a real-world scenario, we considered the dynamic model of a BWR and one of its states was treated as the message signal to be encrypted. This case was also simulated and satisfactory performance was obtained.

Finally, we investigated the security level of our observer. Two algorithms designed for a Lorenz chaotic system were considered. These algorithms were tried to break the cryptosystem in our observer. After several numerical tries our observer was not to broken.

There is much to be considered as future work. The main difference of the observer design in this thesis from the existing literature is that it is Lyapunov-based. As a result, the analysis can be fused with adaptive algorithms to enhance robustness to parametric uncertainties. Generalizing the observer in this thesis to be applicable to various other chaotic systems may also be an interesting future work.

REFERENCES

[1] M. P. Kennedy, G. Kolumbán, and Z. Jákó. *"Chaotic modulation schemes" in Applications of Chaotic Electronics to Telecommunications.*: CRC Press, 2000.

[2] W. Bender, N. Gruhi, A. Morimoto, and H. Lu. *Techniques in Data Hiding.*: IBM Systems Journal, 1996.

[3] L.Pecora, and T.Carroll. *Synchronization in Chaotic Systems.*: Physical Review Letters, 64, 821, 823, 1990.

[4] L.Pecora, and T.Carroll. *Driving systems With Chaotic Signals.*: Physical Review Letter, 44, 2374-2383., 1991.

[5] L.Kocarev, K.S.Hall, K.Eckert, L.O.Chua, and U.Parlitz. *Experimental Demonstration of Secure Communications via Chaotic Synchronization* International Journa. of Bifurcation and Chaos, 2, 709., 1992.

[6] K.M.Cuomo, and A.V.Oppenheim. *Circuit Implementation of Synchronized Chaos with applications to Communication.* : Phys. Rev. Lett., 71, 65-68., 1993.

[7] I.Pehlivan, and Y.Uyaroglu. *Rikitake Attractor and its Synchronization Application for Secure Communication Systems.* : J. of Applied Sciences, 7(2), 232-236, 2007.

[8] Y.Uyaroglu, and I.Pehlivan. *Simplified Chaotic Diffusionless Lorentz Attractor and its Application to Secure Communication Systems.*: IET Communications, 1(5), 1015-1022, 2007.

[9] H.Poincaré. *Les Methodes Nouvelles de la Mechanique Celeste.*: In English, NASA Translation TTF-450/452, 1967, 1892.

[10] E.N.Lorenz. *Deterministic Nonperiodic Flow.* : Journal of the Athmosferic Sciences, Vol. 20, 130-141, 1963.

[11] T.Yang. *A Survey of Chaotic Secure Communication Systems.* : International Journal of Computational Cognition Volume 2, Number 2, Pages 81–130, 2004.

[12] U.Gürsoy. *Kaotik Sistemlerde Lyapunov Karakteristik Üstelleri.* : İTÜ, 1996.

[13] J. N. Blakely, M. B. Eskridge, and N. J. Corron. *A Simple Lorenz Circuit and Its Radio Frequency Implementation.* : Chaos 17(2), 023112, 2007.

[14] Y. S. Tang, A. I. Mees, and L. O. Chua. *Synchronization and Chaos.* : IEEE Trans. Circuits and Systems 30, 620, 1983.

[15] M.Itoh. *Spread Spectrum Communication Via Chaos.* : Int. Jour. of Bifurc. & Chaos, vol. Vol. 9, pp. pp. 155-213, 1999.

[16] L. S. Tsimring, and R.Tenny. *Security Issues in Chaos-based Communication and Encryption.* : Proc. of Winter School on Chaotic Communication, Institute for Nonlinear Science, UCSD, 2003.

[17] G.Kolumban, M.Kennedy, and L.Chua. *The role of synchronization in digital communications using chaos.* : Fundamentals of digital communications, 44(10): 927–936, 1997.

[18] A. R. Volkovskii, L. S. Tsimring, N. F. Rulkov, and I. Langmore. *Spread Spectrum Communication System with Chaotic Frequency Modulation.* : Chaos, vol. Vol. 15, pp. pp. 1-6, 2005.

[19] G. Alvarez, and S.Li. *Some Basic Cryptographic requirements for chaos-based cryptosystems.* : International Journal of Bifurcation and Chaos, vol. 16, pp. 2129-2151, 2006.

[20]. K. M. Cuomo, A. V. Oppenheim, and S. H. Isabelle. *Spread spectrum modulation and signal masking using synchronized chaotic systems.* : MIT Res. Lab. Elecrron. TR 570, 1992.

[21] A. V. Oppenheim, G. W. Womell, S. H. Isabelle, and K. M. Cuomo. *Signal processing in the context of chaotic signals.* : Proc. IEEE ICASSP, 1992.

[22] R.Kılıç. *Karışık Modlu Yeni Bir Kaotik Devre Modeli Tasarımıve Güvenilir Haberleşme AmaçlıSistem Gerçekleştirilmesinde Kullanılması.* : Doktora Tezi, Erciyes Üniversitesi Fen Bilimleri Enstitüsü, Kayseri, 1-20, 2000.

[23] F.E.Yardim, and E.Afacan. *Lorenz-Tabanlı Diferansiyel Kaos Kaydırmalı Anahtarlama (DCSK) Modeli Kullanılarak Kaotik Bir Ha-*

berleşme Sisteminin Simülasyonu. : Gazi Üniv. Müh. Mim. Fak. Der. Cilt 25, No 1, 2009.

[24] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz. *Synchronization of Lorenz-Based Chaotic Circuits with Applications to Communications.* : IEEE Transactions on Circuits and Systems-11: Analog and Digital Signal Processing, Vol. 40, No. 10, 1993.

[25] M. S. de Queiroz, D.M. Dawson, S.P. Nagarkatti, and F. Zhang. *Lyapunov-Based Control of Mechanical Systems.* : Birkhäuser, 1999.

[26] A. Abel, and W. Schwarz. *Chaos Communications Principles, Schemes, and System Analysis.* : IEEE, VOL. 90, NO. 5, 2002.

[27] J.G.Proakis. *Digital Communications.* : Mc -GrawHill, 1995.

[28] D.R.Stinson. *Cryptography—Theory and Practice.* : CRC Press, 1995.

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

[30] A. L. Baranovski, W. Schwarz, and A. Mögel. *Statistical analysis and design of chaotic switched dynamical systems.* : Proc. Int. Symp. Circuits and Sytems, vol. V, 1999.

[31] W. Schwarz, M. Götz, K. Kelber, A. Abel, T. Falk, and F. Dachselt. *"Statistical analysis and design of chaotic systems" in Applications of Chaotic Electronics to Telecommunications.*: CRC Press, 2000.

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

[33] H. Yu, and H. Leung. *A Comparative Study of Different Chaos Based Spread Spectrum of Different Chaos Based Spread Spectrum*: Proc. IEEE Int.Symp. Cct. & Syst. (ISCAS 2001), vol. Vol. 2,pp. pp. 213-216, 2001.

[34] R.Tenny, L. S.Tsimring, H. D. I.Abarbanel, and L. E.Larson. *Security of chaos-based communication and encryption.*:Springer, In Digital Communications Using Chaos and Nonlinear Dynamics Book., 2006.

[35] E. Tatlicioglu, M. McIntyre, D. Dawson, and T. Burg. *Coordination Control for Haptic and Teleoperator Systems.* : Proceedings of the 45th IEEE Conference on Decision & Control, 2006.

[36] B. Xian, D. M. Dawson, M. S. de Queiroz, and J. Chen. *A Continuous Asymptotic Tracking Control Strategy for Uncertain Nonlinear Systems.* : IEEE Transactions on Automatic Control, Vol. 49, No. 7, 2004.

[37] Y.Mukherjee, and R.Nakamura. *Nonholonomic path planning of space robots via a bidirectional approach.* : IEEE Trans. Robot. Automat., vol.7, pp. 500–514, 1991.

[38] B. Bidikli, E. Tatlicioglu and E. Zergeroglu. *A Self Tuning RISE Controller Formulation.* : American Control Conference, 2013.

[39] B. Bidikli, E. Tatlicioglu, A. Bayrak, and E. Zergeroglu. *A New Robust 'Integral of Sign of Error' Feedback Controller with Adaptive Compensation Gain.* : Proc. of IEEE Conference on Decision and Control, 3782–3787, Florence, Italy, 2013.

[40] J. Dasdemir, and E. Zergeroglu. *A New Continuous High-Gain Controller Scheme for a Class of Uncertain Nonlinear Systems.* : International Jounal of Robust and Nonlinear Control, 2013.

[41] A. Bayrak, E. Tatlicioglu, and E. Zergeroglu. *A New Continuous Velocity Observer Formulation for a Class of Uncertain Nonlinear Mechanical Systems.* : American Control Conference, 2013.

[42] G.Ablay, C.E.Koksal, and T.Aldemir. *Chaotic Data Encryption for Long-Distance Monitoring of Nuclear Reactors.* : Nuclear Science and Engineering Vol.170, 2011.

[43] J.March-Leuba. *Nonlinear Dynamics and Chaos in Boiling Water Reactors.* : NATO Advanced Research Workshop on Noise and Nonlinear Phenomena in Nuclear Systems, 1988.

[44] T.Yang. *Chaotic communication systems.* : Nova Science, 2001.

[45] A.J.Menezes, S.A.Vanstone, and P.C.V.Oorschot. *Handbook of Applied Cryptography.* : CRC Press, 1996.

[46] C.E.Shannon. *A Mathematical Theory of Communication.* : BellSystem Technical Journal, 1948.

[47] C. Çokal, and E.Solak. *Cryptanalysis of a Chaos Based Image Encryption Algorithm.* : Phys. Lett. A, 373, 1357, 2009.

[48] G. Álvarez, S. Li, F. Montoya, G. Pastor, and M. Romera. *Breaking Projective Chaos Synchronization Secure Communication Using Filtering and Generalized Synchronization.* : Chaos, Solitons Fractals, 24, 3, 775, 2005.

[49] G. Álvarez, F. Montoya, M. Romera, and G. Pastor. *Breaking Parameter Modulated Chaotic Secure Communication System.* : Chaos, Solitons Fractals, 21, 4, 783, 2004.

[50] S. Li, G. Álvarez, and G. Chen. *Breaking a Chaos Based Secure Communication Scheme Designed by an Improved Modulation Method.* : Chaos, Solitons Fractals, 25, 1,109, 2005.

[51] C. Li, S. Li, G. Álvarez, G. Chen, and K. Lo. *Cryptanalysis of a Chaotic Block Cipher with External Key and Its Improved Version*: Chaos, Solitons Fractals,37,1, 299, 2008.

[52] M. Lei, G. Meng, and Z. Feng. *Security Analysis of Chaotic Communication Systems Based on Volterra–Wiener–Korenberg Mode.* :Chaos, Solitons Fractals,28,1, 264, 2006.

[53] G. Álvarez, F. Montoya, M. Romera, and G. Pastor. *Cryptanalyzing an Improved Security Modulated Chaotic Encryption Scheme Using Ciphertext Absolute Value.* : Chaos, Solitons Fractals, 23, 5, 1749, 2005.

[54] F. Huang, and Z.Guan. *Cryptosystem Using Chaotic Keys.* : Chaos, Solitons Fractals, 23, 3, 851, 2005.

[55] A. Ali Pacha, N. Hadj-said, B. Belmeki, and A. Belgoraf. *Chaotic Behavior for the Secret Key of Cryptographic System.* : Chaos, Solitons Fractals,23,5, 1549, 2005.

[56] M. I. Sobhy, and A. R.Shehata. *Methods of Attacking Chaotic Encryption and Countermeasures.* : Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, Vol. 2, p. 1001, 2001.