5-15-2015

Time-Delay Switch Attack on Networked Control Systems, Effects and Countermeasures

Arman Sargolzaei
asarg001@fiu.edu

DOI: 10.25148/etd.FIDC000126

Recommended Citation

Sargolzaei, Arman, "Time-Delay Switch Attack on Networked Control Systems, Effects and Countermeasures" (2015). *FIU Electronic Theses and Dissertations*. 2175.
https://digitalcommons.fiu.edu/etd/2175

FLORIDA INTERNATIONAL UNIVERSITY

Miami, Florida

TIME-DELAY SWITCH ATTACK ON NETWORKED CONTROL SYSTEMS
EFFECTS AND COUNTERMEASURES

A dissertation submitted in partial fulfillment of the

requirements for the degree of

DOCTOR OF PHILOSOPHY

in

ELECTRICAL ENGINEERING

by

Arman Sargolzaei

2015

To: Dean Amir Mirmiran
College of Engineering and Computing

This dissertation, written by Arman Sargolzaei and entitled Time-Delay Switch Attack on Networked Control Systems, Effects and Countermeasures, having been approved in respect to style and intellectual content, is referred to you for judgment.

We have read this dissertation and recommend that it be approved.

Armando Barreto

Arif I. Sarwat

Bogdan Carbunar

Abolfazl Mehbodniya

Kang K. Yen, Major Professor

Date of Defense: May 15, 2015

The dissertation of Arman Sargolzaei is approved.

Dean Amir Mirmiran
College of Engineering and Computing

Dean Lakshmi N. Reddi
University Graduate School

Florida international University, 2015

DEDICATION

To my beloved wife, parents and brother

ACKNOWLEDGMENTS

First and foremost, I would like to express my deep appreciation to my major professor, Dr. Kang K. Yen. I can hardly forget the amount of joy and motivation I experienced since I met Dr. Yen and expressed my interests in studying under his tutelage. Today, I acknowledge that I can never thank him enough for his continual support, guidance, patience and expertise.

I would also like to thank my committee members, Dr. Armando Barreto, Dr. Arif I. Sarwat, Dr. Bogdan Carbunar, and Dr. Abolfazl Mehbodniya for their valuable input and support. I wish to extend my warmest regards to Dr. Jean Andrian and Dr. Shekhar Bhansali for their kind support and guidance. Much appreciation also goes to Ms. Pat Brammer in the ECE department. I am indebted to my previous mentors and advisers, Dr. Ranu Jung, Dr. Subra Ganesan, Dr. Vahid Assadpour, and Dr. Amin Jajarmi for their support over the years.

My thanks also goes to Mr. Carlos Huerta, President of PLC International Inc., for his support on many technical issues related to expanding my understanding about industrial applications. I would also like to thank Dr. Mohammed Abdelghani, who helped me with many aspects of my dissertation. Without a doubt, he is a true inspiration to my research.

I would like to acknowledge the Department of Electrical and Computer Engineering for providing me with a graduate assistantship, a Donors of Engineering Dean's Merit, Leadership Scholarship, and SGA Graduate Scholarships, all of which facilitated the research of this dissertation.

ABSTRACT OF THE DISSERTATION

TIME-DELAY SWITCH ATTACK ON NETWORKED CONTROL SYSTEMS EFFECTS AND COUNTERMEASURES

by

Arman Sargolzaei

Florida International University, 2015

Miami, Florida

Professor Kang K. Yen, Major Professor

In recent years, the security of networked control systems (NCSs) has been an important challenge for many researchers. Although the security schemes for networked control systems have advanced in the past several years, there have been many acknowledged cyber attacks. As a result, this dissertation proposes the use of a novel time-delay switch (TDS) attack by introducing time delays into the dynamics of NCSs. Such an attack has devastating effects on NCSs if prevention techniques and countermeasures are not considered in the design of these systems. To overcome the stability issue caused by TDS attacks, this dissertation proposes a new detector to track TDS attacks in real time. This method relies on an estimator that will estimate and track time delays introduced by a hacker. Once a detector obtains the maximum tolerable time delay of a plant's optimal controller (for which the plant remains secure and stable), it issues an alarm signal and directs the system to its alarm state. In the alarm state, the plant operates under the control of an emergency controller that can be local or networked to the plant and remains in this stable mode until the networked control system state is restored.

In another effort, this dissertation evaluates different control methods to find out which one is more stable when under a TDS attack than others. Also, a novel, simple and effective controller is proposed to thwart TDS attacks on the sensing loop (SL). The modified controller controls the system under a TDS attack. Also, the time-delay estimator will track time delays introduced by a hacker using a modified model reference-based control with an indirect supervisor and a modified least mean square (LMS) minimization technique.

Furthermore, here, the demonstration proves that the cryptographic solutions are ineffective in the recovery from TDS attacks. A cryptography-free TDS recovery (CF-TDSR) communication protocol enhancement is introduced to leverage the adaptive channel redundancy techniques, along with a novel state estimator to detect and assist in the recovery of the destabilizing effects of TDS attacks. The conclusion shows how the CF-TDSR ensures the control stability of linear time invariant systems.

TABLE OF CONTENTS

CHAPTER PAGE

LIST OF TABLES

TABLE PAGE

LIST OF FIGURES

FIGURE PAGE

SYMBOLS AND ABBREVIATIONS

AC	Alternating Current
AGC	Automatic Generation Control
ARP	Address Resolution Protocol
CPU	Central Processing Unit
CSBI	Current Source Boost Inverter
CSI	Current Source Inverter
DC	Direct Current
DCS	Distributed Control System
DoS	Denial of Service
DPA	Differential Power Analysis
DSP	Digital Signal Processor
ECG	Electrocardiogram
ELC	Emotional Learning Controller
ELPIC	Emotional Learning PI controller
FDI	Fault Data Injection
FPGA	Field-Programmable Gate Array
HJB	Hamilton-Jacobi-Bellman
HPM	Homotopy Perturbation Method
HRV	Heart Rate Variability
HTTP	HyperText Transfer Protocol
ICS	Industrial Control System
LFC	Load Frequency Control

LTI	Linear Time Invariant
MAC	Media Access Control
NACK	Negative Acknowledgement
NCS	Networked Control System
NPCS	Networked Power Control System
OC	Optimal Controller
PCT	Proposed Control Technique
PID	Proportional Integral Derivative
PLC	Programmable Logic Controller
PMU	Phase Measurement Unit
PWM	Pulse Width Modulation
RHP	Right Hand Plane
SA	Sensitivity Approach
SAA	Successive Approximate Approach
SCADA	Supervisory Control and Data Acquisition
SE	Sustainable Energy
SL	Sensing Loop
SPA	Simple Power Analysis
SVPWM	Space-Vector Pulse Width Modulation
TCP	Transmission Control Protocol
TDS	Time-Delay Switch
TOC	Traditional Optimal Controller
TPBVP	Two Point Boundary Value Problem

VSI	Voltage Source Inverter
WAMS	Wide Area Measurement System

CHAPTER 1

INTRODUCTION

1.1 General Statement of Problem Area

Control systems have many applications in the industry. An innovation in control systems is the networked control system (NCS), which is used to monitor and control systems in wide areas, enabling engineers to more easily configure, monitor and control devices. In recent years, the security of networked control systems has been an important challenge for many researchers. Industrial Control Systems (ICSs) include Networked Control Systems (NCSs), Supervisory Control and Data Acquisition (SCADA), Process Control Systems (PCSs), Distributed Control Systems (DCSs), Load Frequency Control (LFC) and Programmable Logic Controllers (PLCs). Security of the abovementioned ICSs plays an important role in the successful performance of industrial and critical infrastructures. Energy and power sectors, transportation system sectors, water and wastewater system sectors, healthcare and public health sectors are examples of industries facing a high probability of attacks on their performance. Along with the development and advancement of security schemes for control systems during the past several years, there have also been many cyber attacks. This is evidence that control systems are not very secure in light of cyber attacks.

The following is a summary of several attacks that occurred in control systems in various industries:

- The energy and power industry is one of the most important industries in the world, which demands high security. Any failure in security of this industry will cause catastrophic damage to society. Many past and ongoing research efforts attempt to make this industry tech smart and globalized in terms of control and monitoring. The blackout in India in August 2012, and North American blackout in 2003 have brought serious attention the immediate needs of new schemes to prevent the occurrence of cyber attacks. [1, 2]
- Water and wastewater systems clean all of the waste and harmful microscopic viruses in our water supply sphere. In January 2000, an incident of attack on a sewage control system in Australia was reported. During a four-month period, these problems eventually led to the flooding of the grounds of a nearby hotel, a park, and a river with a million liters of sewage. [3]
- The natural gas industry has also been targeted by attackers. In 2000, the Russian Interior Ministry recorded attacks to their control systems. The hacker accessed the control system that regulates gas flow [4].
- Transportation systems are expanding quickly. Hackers can attack the control systems in this industry and make them harmful and dangerous. Currently, train tramway tracks are wireless and remote-controlled. In 2008, a teenager modified a TV remote, resulting in four derailments and many injuries [5].
- Biomedical devices usually involve control systems. The proper use of these devices is a critical necessity in the public health industry. Recently, the U.S. Department of Homeland Security underscored some threats affecting almost 300 medical devices. Wireless devices such as pacemakers are a possible target of

attack. The false data injection, denial of service, and other types of attacks pose as dangerous threats to patients.

Traditionally, control systems are designed in normal environments, with no attacks involved in the design process. In this case, any distortion, delay or attack to any part of control systems such as sensors, communication lines and others, can result in an unstable system or even failure of the system.

Currently, industries use security algorithms that were introduced by IT researchers, which stand the chance of not working efficiently or properly for the networked control systems under a TDS attack. Hence, control systems are in need of hardware and software protection protocol.

Based on the information above, security analyses of NCSs could improve our understanding of the possible effects and results of cyber attacks. Also, the design and implementation of safe, robust and secure controller and communication protocol could ensure the reliability of industries that use networked control systems. The goal of this research is to study and analyze different types of attacks, in particular, the Time-Delay Switch (TDS) attack on the NCS, as well as to drive the general model of the system under TDS attacks. This research also proposes a new robust controller for the network control systems experiencing a TDS attack. The new controller overcomes the stability issues caused by TDS attacks. Furthermore, an attack-resistant communication protocol is implemented to guarantee the stability of networked control systems experiencing a TDS attack.

1.2 Problem Statement and Research Questions

The research for the development of a robust and stable automated networked control system that will resist cyber attacks consists of the following tasks:

1. The current networked control systems were designed under normal operations, with no attacks included in the design process. It is necessary to outline a reliable and general model for a system under a TDS attack, and then design the robust controllers.

2. Investigating the effects of attacks on the stability of systems under a TDS attack is a difficult task because an attack can occur at any time interval and can be a random process.

3. Attackers can target wireless, fiber or other type of communication medium and disrupt the system. An attacker can access the communication channel and cause a denial of service, or cause a delay, as well as a data jam or an injection of fault data into the system. In this case, the controller either does not obtain sensor information or receives wrong data in the decision-making process.

4. Since an attack is a random event, determining an appropriate protocol, technique, and software package for estimating and detecting the type of attack is complicated.

5. Separating a TDS attack from a natural delay and disturbance is a difficult task.

Following is a summary of the research questions:

- Is it necessary to study the stability of networked control systems experiencing a TDS attack?

- Can TDS attacks be detected and tracked in real time for linear systems?
- Is it possible to design a secure and robust controller to overcome the effects of TDS attacks for NCSs?
- Is it possible to design a secure communication protocol between controllers and plants for a system experiencing a TDS attack?

1.3 Dissertation Roadmap

The five main research themes of this dissertation can be described as follows:

- ✓ Introducing a new type of attack on NCSs called a “TDS attack” and showing that this attack can disturb and disable a NCS.
- ✓ Detecting and tracking TDS attacks in real time, alerting the controller center, and using the emergency controller design.
- ✓ Proposing a new controller design to overcome the stability effects of TDS attacks.
- ✓ Proposing a new communication protocol to solve the stability and effects of TDS attacks on NCSs.
- ✓ Evaluation of a controller’s methods to find the best existing controller design for nonlinear NCSs experiencing TDS attacks.

Accordingly, this dissertation is structured as follows:

Chapter 2 provides a general definition of a NCS and its applications. It follows with a discussion on NCS security challenges and the different types of attacks on NCS.

Furthermore, this chapter includes a general model of attacks for NCS, along with relevant literature related to NCS security and the different type of attacks.

Chapter 3 examines the effects of natural time delays in control systems. The first section provides time-delay effects and solutions for controlling a three-phase single stage current source boost inverter. The second section discusses an optimal control problem with time delay and presents the design complexity of the controller and effects of ignoring time delays in the cost function result.

Chapter 4 introduces a new type of attack on NCS called the time-delay switch (TDS) attack. It provides a stability analysis of a NCS experiencing a TDS attack. It also shows how TDS attacks can cause stability issues on two real-world applications. One is the networked power control systems, which is the Load Frequency Control (LFC) on smart grid applications. The second one involves biomedical application. It provides simulation results of TDS attacks on wireless pacemakers by understanding the dynamic model of the system.

Chapter 5 includes a literature review about research dealing with the natural time delays of control systems. It also contains a new method that detects and tracks real-time TDS attacks on NCS. At the end of this chapter, simulation results display the power of this method on LFC applications.

Chapter 6 details a simple proposed control method to overcome stability issues of TDS attacks on linear NCS. Simulation results of a sample complex example and LFC on two interconnected power areas show that this controller can prevent stability and inefficiency effects of TDS attacks on NCS.

Chapter 7 describes the Emotional Learning Controller (ELC) in detail. It also evaluates ELC’s robustness and stability when compared with two other controllers under a TDS attack. It also introduces a local and emergency controller design for a NCS under a TDS attack.

Chapter 8 provides a new, simple communication protocol that does not need encryption techniques. This chapter proposes a protocol called “CF-TDSR” in order to address issues caused by a TDS attack on a NCS. It also includes simulation results of using the CF-TDSR protocol on an LFC system under a TDS attack.

Chapter 9 concludes this dissertation with a discussion on the findings and implications for potential future research.

CHAPTER 2

LITERATURE REVIEW AND DESIGN FUNDAMENTALS

2.1 Networked Control Systems

A Networked Control System (NCS) is a control system in which the control feedback process is closed through a real-time communication network [6]. In this case, the control system can be shared with other nodes outside the control system. Figure 2.1 shows a typical NCS. In this figure, sensors measure the output signal from the plant and transmit it through the communication channels to the controller. Then, the controller compares the signals with the reference values and injects the control signals into the plant.

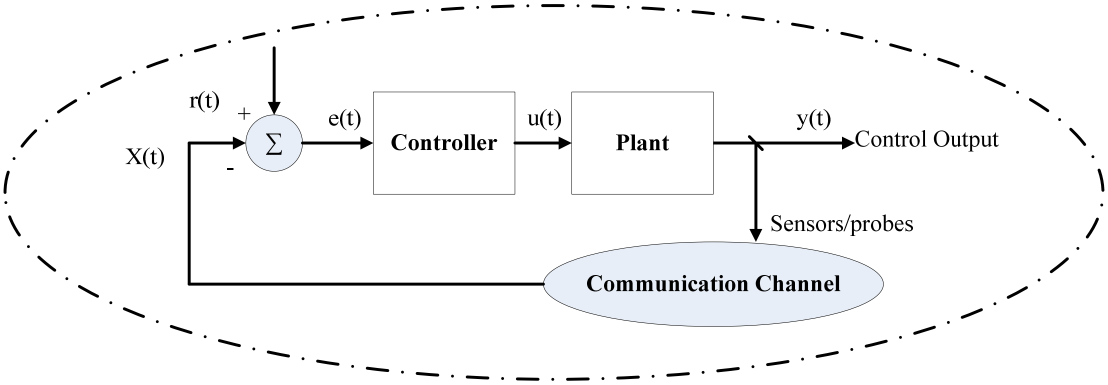


Figure 2.1: A Typical Networked Control System

NCSs are of pervasive use in the industry and are an integral part of any infrastructure. They are the information communication and control highway. NCSs are sometimes referred to as industrial control systems, industrial control networks, command and control networks, distributed control systems, or the World Wide Web, depending on the application and context. Technological advances in communication and control made it possible to monitor and control many systems over a wide geographical area. This is the essence of NCSs that makes it easier for engineers to configure, monitor, and control devices from a distance, and make it possible to coordinate the operations of a large and distributed infrastructure with ease and efficiency.

As previously stated, NCSs have many applications [6] in the industry, including the Supervisory Control and Data Acquisition (SCADA), Process Control System (PCS), Distributed Control System (DCS), Load Frequency Control (LFC), and Programmable Logic Controllers (PLC). Industrial Control Systems (ICSs) play an important role in the protection of industrial and critical infrastructures, such as the energy and power sector, transportation systems sector, water and wastewater systems sector, healthcare and public health sector, etc. Hence, the security of the controllers is very important. In the following sections, the focus will be on the security and stability of NCSs.

2.2 Challenges for Networked Control Systems

In recent years, the security and stability of NCSs has been at the center stage for researchers, engineers, and governmental entities, since exploited security risks could have potential catastrophic consequences [7, 8]. Although the security and stability schemes for NCSs have advanced in the past several years, there have been many acknowledged cyber attacks and confirmations that these control systems are not very safe and stable in the face of attacks and natural disturbances.

A survey of literature indicates that the study and improvement of the security of NCSs is necessary. The first key problem of conventional control systems is that they were designed in a normal environment with no attacks considered. In this case, any attack to any part of a control system, such as sensors and communication links, can drive the system to an unstable mode and cause inefficiency.

There are many researchers that have studied these problems. A class of False Data Injection (FDI) attacks that bypassed the bad data detection in SCADA systems was proposed by [9]. In [10], adversaries launched FDI attacks against state estimates of power systems, with only the knowledge of the perturbed model of the power system. Y. Mo et al. [9] studied FDI attacks on a control system equipped with a Kalman filter. In [11], the smallest set of hacker-controlled meters was identified as performing an unobservable attack. Recently, Amin et al. [12] considered the Denial of Service (DoS) attacks on the communication channels in the measurements telemetered in remote terminal units (RTUs) sent to the control center of power systems. They demonstrated that a hacker may make power systems unstable by properly designing DoS-attack sequences. Liu et al. [13] considered how a switched-DoS attack on a smart grid can affect the dynamic performance of its power systems. The Viking projects [14] considered cyber attacks on the Load Frequency Control (LFC), one of a few automatic control loops in SCADA power systems. They analyzed the impacts of cyber attacks on the control centers of power systems by using reachability methods. However, they only considered attacks on the control centers, which are usually harder to attack than the communication channels in the SL of a power system.

The above literature review talked about current problems and existing attacks. Also, it explained how different researchers attempt to solve them. However, in papers that described attacks to NCS, not much research has been done on the making the design of the controller more robust and optimal. In [12], a NCS under a DOS attack is modeled. They used the stochastic control theory to secure the system, but only the LTI model was studied.

Another key problem in network control systems is that there are no solid methods that prevent attackers from hacking controllers, wireless sensors, reference inputs, etc. Currently, industries use security algorithms to secure their control networks. These algorithms were introduced by IT researchers in the context of the World Wide Web, where there is no mandate for real-time data. Therefore, the security of NCSs cannot be guaranteed when using those algorithms. This problem, along with existing, relevant literature, is addressed in detail in Chapter 8.

2.3 Time-Delay Estimation

This dissertation focuses on stability issues caused by time delays on control systems. There are many studies on time-delay estimation, all of which have limitations. Tan [15] developed two different time varying time-delay estimation methods for nonlinear systems using neural networks. The first method is an indirect time-delay estimator procedure using nonlinear programming. The second one is a direct time-delay estimation scheme that uses a neural network to construct a time-delay estimator. The methods proposed by the author show that his/her method is more general and accurate than the simple linear time-delay estimation procedures [16, 17] for time-varying time-delay signals. However, the methods proposed are complex, and the estimation process takes time to obtain results. Examination of their results shows that it is obvious that the algorithm took 80 sec to estimate and learn a 4-sec time-delay value. Also, their methods were not used in the context of real-time control. Furthermore, to train the neural network, the authors used a specific pattern of input, or a combination of sinusoids, to achieve a good estimation function.

It should be noted that the time-delay calculation procedure, either by the neural network or the nonlinear programming method, is done offline before the algorithms are applied to estimate a real-time varying signal.

The method works well in estimating a slowly varying time delay (the time delay was modeled by a ramp function to force the neural network to learn it slowly), but fails when tested with switched time-delay attack (e.g. step time delay).

2.4 Different Types of Attacks on NCS

This section introduces a generalized attack model and illustrates it for the most important attacks in detail. Later in this chapter, the most common attacks on NCSs are described in detail. Let us consider a NCS (*f, g*) with controller *h* as shown in Figure 2.2.

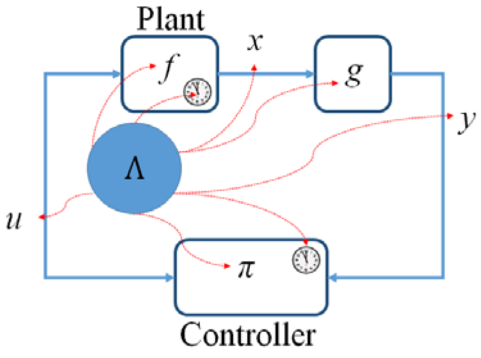


Figure 2.2: Generalized Cyber Attacks on a Typical NCS.

The system with the controller and the communication channel can be described concisely as an output feedback system having the following form:

$$\begin{aligned} \dot{x} &= f(t,x,u) \\ y &= g(x) \end{aligned} \tag{2.1}$$

where f is a function describing the plant behavior, x is the plant state vector and u is the control vector. The function, g, describes the plant output and the communication methodology used. The controller is described as:

$$u = h(y) \tag{2.2}$$

where y is the information communicated to the controller about the plant state. The function h is describing the controller.

An attack on the control system involves altering any component of the NCS. A general attack can be described as a function that alters any of the components of the system:

$$(\tilde{f},\tilde{g},\tilde{h},\tilde{x},\tilde{y},\tilde{u},\tilde{t}) = \Lambda(f,g,h,x,y,u,t) \tag{2.3}$$

where $(\tilde{f},\tilde{g},\tilde{h},\tilde{x},\tilde{y},\tilde{u},\tilde{t})$ are the corrupted functions and information as result of the attack Λ.

The following are the most possible attacks on the NCS, especially on the Networked Power Control System (NPCS):

I. Denial of Service (DoS)

This attack seeks to sabotage a NCS by overwhelming its communication and computational resources in order to prevent it from working [18]. This attack can be applied to multiple layers in a NCS. This type of attack can take place between the plant and the controller. The DoS can disconnect service or data from the plant to the controller, from the controller to the plant, or both at the same time. In the general model of attacks, this attack can be described as follows:

$$\tilde{y} = \begin{cases} y & otherwise \\ \alpha & attack \end{cases} \tag{2.4}$$

where α can be zero, or some random value.

II. Fault Analysis Attack

This class of attack injects faults into a device performing some type of computation. These faults can be anything from unusual environmental conditions (increased heat, for example), the injection of a laser beam at the appropriate frequency [19], or the injection of data packets that collide with legitimate packets [20]. The work of Yuan and Liu et al. showed that the load redistribution attack [21-23] is a false data injection attack by modifying selected information in a SCADA power system. This attack is especially dangerous due to it being able to manipulate the estimation of a system power flow. Depending on whether the attack is short-term or long-term, it can have damaging effects on the security-constrained economic dispatch (SCED) price estimation [22]. This attack can be modeled as follows:

$$\tilde{y} = \begin{cases} y & otherwise \\ z & attack \end{cases} \tag{2.5}$$

where z is an input signal designed by the attacker for the purpose of either misleading the control system, causing system inefficiencies, or sabotaging it.

III. **Physical Layer Attacks**

One only needs to connect to the communication channel rather than the actual network to launch this attack [24]. Channel jamming attacks become one of the most efficient ways that attackers use, and are one of the most dangerous for utilities and customers alike. Examples of such attacks include the continuous emission and injection of high power wave tones and FM modulated noise into the communication channel at a brute force level. A more sophisticated attack is detailed by the work of Proano and Lazos, wherein they exploit specific weaknesses in communications protocols (in their case, TCP) to perform their attacks [25]. Their selective jamming attack sees the hacker classifying packets in real time, decoding the control field at the MAC layer, and corrupting them before the end of their transmissions.

IV. **MAC Layer Attacks**

The Media Access Control (MAC) layer is responsible for two-way communication and is susceptible to attackers who wish to modify parameters, which gives the attacker better leeway in accessing the network at the cost of degrading network performance for legitimate customers on the same channel [24]. Examples include spoofing attacks, which can target both network availability and integrity. One way this attack may be realized is through sending fake Address Resolution Protocol (ARP) messages and packets into the local area network. The attacker's MAC address becomes associated with the IP address of a legitimate host, causing traffic meant for the host to go to the hacker [26].

V. **Network/Transport Layer Attack**

TCP/IP protocols are said to be the two more vulnerable standards in the network infrastructure, due to the use of email as the communication media [24, 27]. Traffic flooding and worm attacks through the internet have led to serious performance issues [24]. Buffer flooding attacks through the DNP3 protocol were examined in the literature [28, 29]. The work of East et al. saw the creation of a taxonomy of such attacks, which can range from sending fake DNP3 messages in order to reset, manipulate, or corrupt data from a substation [30].

VI. **Application Layer Attack**

Application layer attacks seek to exhaust the resources of a communication channel, focusing on transmission bandwidth in computers and routers [24]. These attacks seek to limit the bandwidths of CPU's and I/O's of connected devices. The work of Ranjan et al. saw the study and categorization of a number of such attacks. A flood attack sends requests at higher than normal frequencies, while asymmetrical attacks send high-workload requests. A one-shot attack involves the attacker spreading the workload over multiple sessions, using HTTP floods to stress the servers over time [31].

VII. **Decryption Attacks**

This attack is used to discover the encryption key of a network in order to connect to it and steal its data. An attacker may do this by accessing and obtaining the physical frames of the network, and storing enough of them so they can be decrypted by using correct algorithms [32]. Another form of attack that yields success is called the "side channel attack." This attack exploits some aspect of a physical system that employs a data encryption algorithm [32].

VIII. **Electromagnetic Attacks**

These attacks deal with discerning the encoded plaintext of a power line message through the leakage of electromagnetic radiation [19].

These attacks use special probes placed at various locations along the unit or circuit in question. The probe location depends on detecting direct or unintentional emissions. Direct emissions are intentional current flows through a line, where short currents burst with sharp rising edges, which can cause large bandwidths [33]. Unintentional emissions are those electromagnetic leakages that couple to those of other circuit components or cabling. These emissions are typically modulations of the carrier signals that are either present or have been introduced into the device. Under these definitions, direct emissions are the more difficult of the two to detect, requiring close proximity to the device in question. An attacker would likely prefer the unintentional emissions, as these provide a wide spectrum of signals to probe and through which encryption keys in the data may be found [33, 34].

Many proofs of the concept have been demonstrated in the laboratory. The work of Enev and Gupta [35] experimented on the information leakage from eight televisions connected to the same power line. It was found that the radiative interference patterns of TV power supplies yielded discernible information about the media being played. The work of Hayashi et al. [36-38] demonstrated the viability of obtaining secret keys from the radiation patterns of power and communication cables attached to FPGA boards. Their work showed that cryptographic key information may leak from a near field [36] and far field [37] radiation patterns.

IX. **Power Analysis Attacks**

Power analysis attacks are characterized by analyzing the use of the electrical power of a device while it performs an encryption algorithm [39]. They are divided into two classes, simple and differential. Simple Power Analysis (SPA) attacks observe the data visually (oscilloscope, for example), and interpret what cryptographic algorithm the signal has been encoded with. Differential Power Analysis (DPA) applies statistical error-correcting algorithms to SPA by monitoring trends in the data. DPA attacks are especially dangerous, as they can be so precise that even the switching of a transistor can give away an encryption key. All cryptographic algorithms, and devices running them, have so far been shown to be vulnerable to DPA [39].

CHAPTER 3

NATURAL TIME DELAY IN CONTROL SYSTEMS, EFFECTS AND SOLUTIONS

3.1 Time-Delay Effects on a Three-Phase Current Source Boost Inverter

Sustainable Energy (SE) is the future energy source [40]. However, in order to use SE sources efficiently, it is necessary to integrate them into a power grid. Inverters and electronic circuits are needed for this purpose [41]. These interface electronic circuits are recognized as the SE inverters. The SE inverters should convert Direct Current (DC) to Alternating Current (AC) with as little harmonic content as possible. To do so, they should be designed to harmonize their outputs with the utility grid line.

There are many different topologies for SE inverters, such as Current Source Boost Inverters (CSBIs) [42-44], Voltage Source Inverters (VSIs) [45], multi-level inverters [46, 47], and matrix converters [48, 49]. VSIs have many advantages and been used in many industrial applications [50]. However, despite other types of inverters, CSBIs can invert and boost currents in a single stage from a DC source, such as photovoltaic cells to an AC voltage [51]. This advantage recognizes CSBIs as one of the best choices for SE grid-connected conversion systems.

In this section, the switching pattern and circuit topology of the three-phase CSBI proposed in [52] are considered. The suggested CSBI offers a better robust method in terms of the control of the voltage and the injected power based on a novel switching pattern.

Despite the advantage, the proposed CSBI does not consider the time-delay effects of hardware, software and components on grid synchronization. Furthermore, results show more harmonics and less current waveform quality.

Most of the inverters can be controlled with digital signal processors (DSPs). DSPs offer high performance in feedback control, as well as user flexibility for design and implementation. However, a time delay exists in the electronic components and microprocessors. In a DSP system, there is a predictable effecting time delay in each sampling cycle [53]. This delay has a significant effect on switching control, monitoring and feedback control of the CSBI [52].

In this effort, the focus is on the time-delay effect on a grid-connected CSBI with a recent literature switching pattern. This section is organized as follows: Section 3.1.1 discusses the SVPWM-based switching pattern for a grid-connected three-phase current source inverter and circuit topology proposed by [52]. Then, the effect of time delays on DSPACE is shown and the proposed technique to overcome this issue is discussed. Section 3.1.3 will show the results using the proposed technique, which produces less harmonic and higher waveform quality, followed by the conclusion.

3.1.1 Switching Pattern and Control of CSBI

A. Switching Pattern

The Current Source Boost Inverter (CBSI) topology is illustrated in Figure 3-1, based on the modified Space-Vector PWM technique, called the "SVPWM." A detailed description of the developed switching pattern is presented in [52].

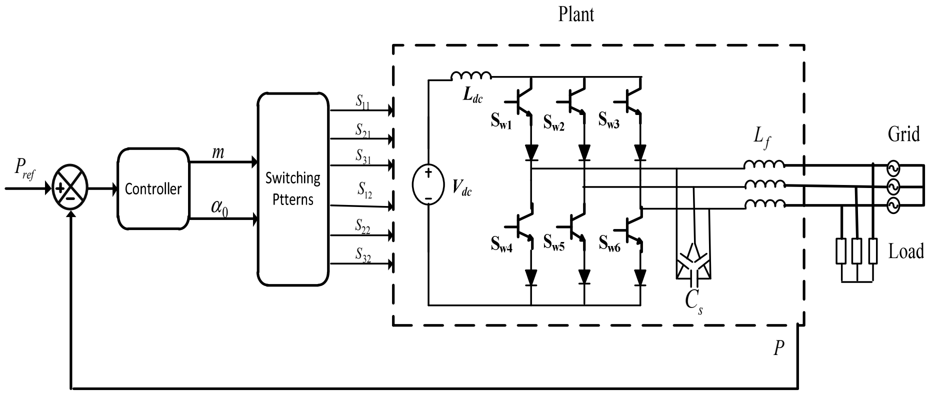


Figure 3.1: CSBI and its Controller Configuration

In [54], the capability of this technique is demonstrated specifically for controlling the active and reactive powers effectively. The main purpose of the switching pattern is to inject in-phase sinusoidal currents into the three phases of the grid, whereas the dc inductor current is kept at a constant, desired level. In terms of the SVPWM method, in order to achieve an effective operation, six sections in each grid voltage cycle are proposed in Figure 3.2.

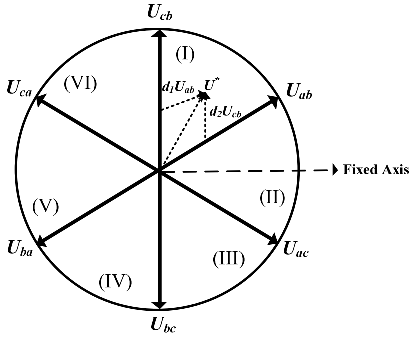
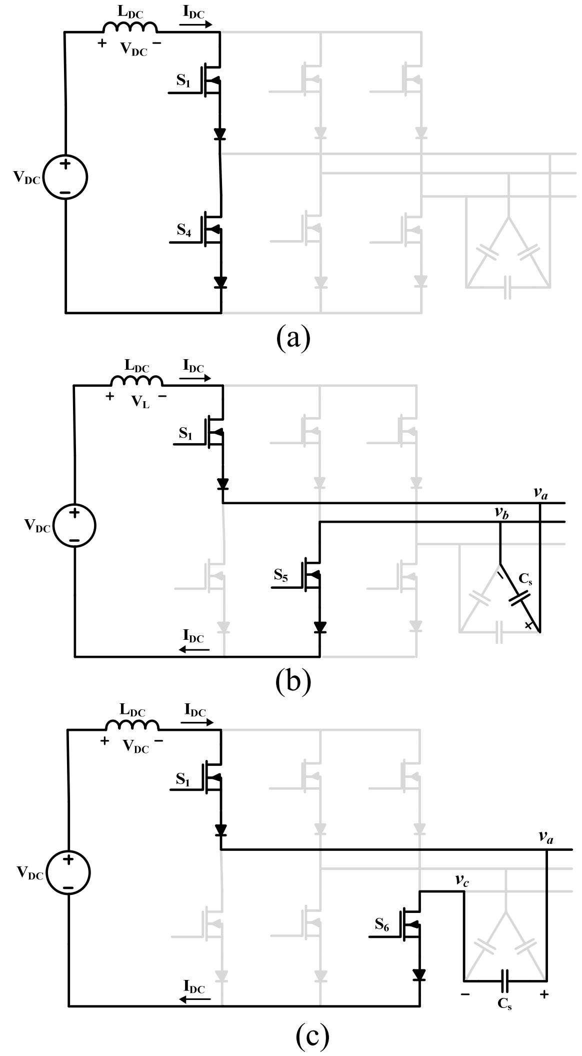


Figure 3.2: Sectors of the Proposed Switching for CSB

In each section, there is one charging stage by keeping the switches on to store energy in the dc link inductor, and two discharging stages by applying the two line-to-line voltages to the output of the inverter to inject the stored energy into the grid. The inductor current increases and output currents are supplied by *C*s. In Stages II and III shown in Figure 3.3 (b) and (c), the inductor current discharges through *C*s, in which the two line-to-line voltages V_{ab} and V_{ac} are applied to the inverter, respectively. Since phase "*a*" is common between these two stages, this phase is used for the charging stage.

The switching pattern on all sectors can be found in Figure 3.4 and Table 3.1. Here t_c is the charging time; t_{d1} and t_{d2} are the time intervals of discharging. The relationship of these time intervals yields

$$T_s = t_c + t_{d1} + t_{d2} \tag{3.1}$$



(a)

(b)

(c)

Figure 3.3: Three stages of different switching patterns for CSB (a) Stage I. (b) Stage II. (c) Stage III

These time intervals must satisfy the following objectives: (i) The inverter output current contains minimum harmonic contents, and (ii) the dc-link inductor current stays at a fixed level.

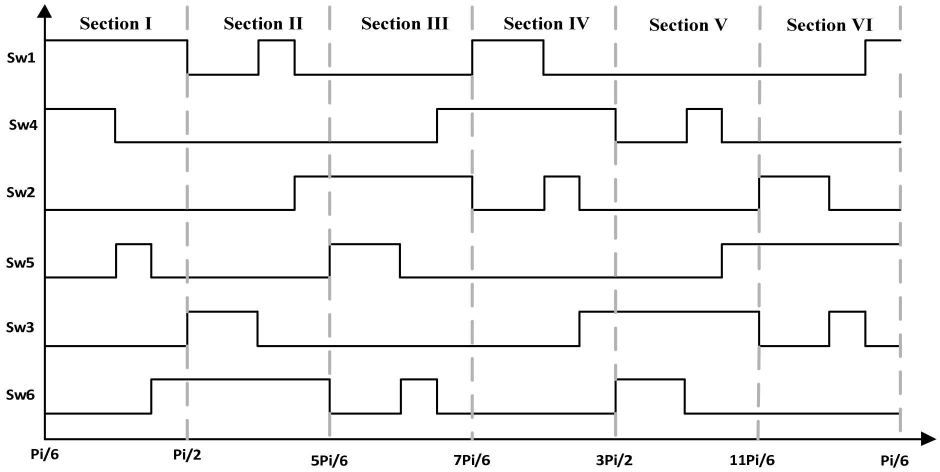


Figure 3.4: Three Stages for Different Switching

Table 3.1: The Switching Patterns

Section	**I**	**II**	**III**	**IV**	**V**	**VI**
U_1	v_{ab}	v_{ac}	v_{bc}	v_{ba}	v_{ca}	v_{cb}
U_2	v_{ac}	v_{bc}	v_{ba}	v_{ca}	v_{cb}	v_{ab}
S_{w1}	T_s	t_{d1}	0	t_c	0	t_{d2}
S_{w2}	t_c	0	t_{d2}	T_s	t_{d1}	0
S_{w3}	0	t_{d2}	T_s	t_{d1}	0	t_c
S_{w4}	t_{d1}	0	t_c	0	t_{d2}	T_s
S_{w5}	0	t_c	0	t_{d2}	T_s	t_{d1}
S_{w6}	t_{d2}	T_s	t_{d1}	0	t_c	0

As a result, if $v_{ab} = \sqrt{6}V_{rms}\cos(\omega t)$ measured as the reference signal for this method, the duty cycles of the two discharging and one charging time intervals are computed as follows:

$$d_1 = m\cos(\omega t - \alpha_0) \tag{3.2}$$

$$d_2 = m\cos(\omega t - \alpha_0 - \frac{2\pi}{3}) \tag{3.3}$$

where $d_1=t_{d1}/T_s$ and $d_2=t_{d2}/T_s$ are the two discharging duty cycle and $d_c = 1-(d_1+d_2) = t_c/T_s$ is the charging duty cycle, *m* is the modulation index and α_0 is the phase shift with respect to the line-line reference voltage, v_{ab}.

B. State-Space Averaged Modelling of CSBI

The state-space model, considered in this study, is defined as

$$\begin{aligned} \dot{x}(t) &= Ax(t) + Bu(t) \\ y(t) &= Cx(t) \end{aligned} \tag{3.4}$$

where, *x*, *u* and *y* are the states, control inputs, and outputs of the system, while *A*, *B* and *C* represent the system matrix, control matrix and output matrix, respectively. The large-signal state-space-averaged model of the grid-connected single-stage boost inverter system can be represented in the synchronous d_q-frame of reference, as shown in (3.5).

$$\frac{d}{dt}\begin{bmatrix} i_{dc} \\ v_q \\ v_d \end{bmatrix} = \begin{bmatrix} \frac{-R_{dc}}{L_{dc}} & \frac{-\sqrt{3}m\cos\varphi}{2L_{dc}} & \frac{-\sqrt{3}m\sin\varphi}{2L_{dc}} \\ \frac{\sqrt{3}m\cos\alpha}{2C} & 0 & -\omega_s \\ \frac{\sqrt{3}m\sin\varphi}{2C} & \omega_s & 0 \end{bmatrix} \begin{bmatrix} i_{dc} \\ v_q \\ v_d \end{bmatrix} + \begin{bmatrix} \frac{1}{L_f} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} v_{dc} \\ v_{qs} \\ v_{ds} \end{bmatrix} \tag{3.5}$$

The state vector *x* consists of the state variables of the system, which are the independent inductor current and capacitor voltages, i.e. $x = [i_{dc}, v_q, v_d]^T$. Also, $u = [v_{dc}, v_{qs}, v_{ds}]^T$ represents the system inputs. The modulation angle φ is constant, but modulation index *m* regulates the injected active powers to the grid.

3.1.2 Practical Control with Time Delay and Solution

A time delay can be estimated around a sampling period in most DSP-based controllers, however, a DSP board can introduce a greater time delay, and it depends on the complexity of application, parallel processors, and threats. Here, in the experimental result and setup, a dSPACE multi DSP board DS1104 was used. This board can be directly programmed by MathWorks joint with Real-Time Interface (RTI) developed by dSPACE using MATLAB/SIMULINK and is connected to a desktop computer. The board has two processors: The first one is a master DSP that operates at 250MHz, and second one is a TMS320F240 microcontroller that operates at 20MHz as a slave DSP. The master DSP generates and debugs the control algorithm and also monitors the data. The slave DSP acts as a modulator for the master DSP [53].

In practical use, a time delay exists in the controlling signal and the sensing signal. For grid-connected applications, the SE-inverters should be synchronized with grid signals. Two voltage sensors perform this task. The data from these two sensors proceeds to the Analog to Digital (A/D) Inputs/Outputs (I/O) of dSPACE, and then triggers the SVWPM algorithm to generate the switching signal. On the other hand, switching signals should be sent to the SE-CS inverter using dSPACE D/A I/O and should be modulated by the slave DSP. Both sensing and generating switching signals processes introduce time delays in the system. Estimating and finding solutions for these delays improves system performance and avoids unwanted failures. For now, let an assumption include switching the signal time delay. The time delay acquainted with the dSPACE controller can be calculated by [53]:

$$\tau = T_{exc} + 0.5T_s \tag{3.6}$$

where τ is the time delay, T_{exc} is the execution time of the master DSP and T_s is the sampling time.

In (3.6), if T_{exc} is greater than $0.5T_s$, the resulting time delay is longer than one sampling cycle. In this case, if the time delays existing in the control input (switching signals) and feedback section (grid voltage) of the system is ignored, then the dynamic performance of the system can be corrupted and even worse, become unstable and fail. Here, the focus is on the time delay existing in the sensing line.

To overcome this problem, a step function is sent to one of the dSPACE D/A I/O's and obtains its feedback from the A/D I/O's. As soon as the step function is detected, the clock stops and the results are divided by two. This provides a real-time track of the time delay for both sensing signals. If this time delay is larger than the sampling time, it should be estimated. A buffer will be used to store all data received from the grid sensors for each sampling period. As the states are periodic, one can easily predict and estimate the current phase of the grid for all three phases and send appropriate switching patterns to the system. For a time delay on the control input, a modified controller can be used, as follows.

Consider the state-space model for a SVPWM switching control (3.4). Following is the discretized state space model of the system without a time delay:

$$\begin{aligned} x(k+1) &= Gx(k) + Hu(k) \\ y(k) &= Cx(k) \end{aligned} \tag{3.7}$$

where, $H = B\int_{0}^{T_S} e^{A\lambda} d\lambda$ and $G = e^{AT_S}$. The control input signal is designed based on the state feedback algorithm [55]:

$$u(k) = K_I x_I(k) - K_P x(k) \tag{3.8}$$

where K_I and K_P are the integration and proportional gains that can be determined by the pole-placement method. Also, the new state variable x_I can be calculated from:

$$x_I(k) = x_I(k-1) + y_r(k) - y(k) \tag{3.9}$$

where y_r is the reference input. With the above definitions, the following are the new state space model results:

$$\begin{aligned} X(k+1) &= \hat{A}X(k) + \hat{B}u(k) + \hat{D}y_r(k+1) \\ y(k) &= \hat{C}X(k) \end{aligned} \tag{3.10}$$

Where $X(k) = \begin{bmatrix} x(k) & x_I(k) \end{bmatrix}^T$, $\hat{A} = \begin{bmatrix} G & 0 \\ -CG & I \end{bmatrix}$, $\hat{C} = \begin{bmatrix} C & 0 \end{bmatrix}$ $\hat{B} = \begin{bmatrix} H & -CH \end{bmatrix}^T$ and $\hat{D} = \begin{bmatrix} 0 & I \end{bmatrix}^T$.

If there is a time delay in the control section, the Equations (3.7) will be converted to:

$$\begin{aligned} \dot{x}(t) &= Ax(t) + Bu(t-\tau) \\ y(t) &= Cx(t) \end{aligned} \tag{3.11}$$

In order to solve the time-delay effect in the switching control signal (3.11), an observer controller was used based on modification of the smith predictor [52, 55]. The control input signal under the time-delay effect can be found by substituting states x by its predicted $\hat{x}$ in (3.8):

$$u(k) = K_I x_I(k) - K_P \hat{x}(k) \tag{3.12}$$

and y by $C\hat{x}$ in (3.9):

$$x_I(k) = x_I(k-1) + y_r(k) - C\hat{x}(k) \tag{3.13}$$

where $\hat{x}$ is the estimated state vector calculated by the observer that predicts the state vector x one τ ahead of time. In the case where τ is larger than sampling period T_s, the state estimate can be calculated as follows.

$$\hat{x}(k) = \hat{G}x(k) + \hat{H}_1 u(k-2) + \hat{H}_2 u(k-1) \tag{3.14}$$

where $\hat{G} = e^{A\tau}$, $\hat{H}_1 = Be^{AT_1} \int_0^{T_S} e^{A\lambda} d\lambda$, $\hat{H}_2 = B \int_0^{\tau - T_s} e^{A\lambda} d\lambda$.

3.1.3 Simulation and Experimental Results

The simulation and experimental results are presented in this section to show the effectiveness of the proposed controller based on the time delay. Figure 3.5 shows the layout of the experimental setup. The circuit parameters in this simulation were selected as: V_{dc}=30 volt, C_{s}=15 μF, L_{dc}=12 mH, L_{f}=2mH. The control section is implemented using MATLAB Simulink, in conjunction with the dSPACE 1104 control block, which is interfaced with the hardware. The PWM switching frequency is set to be 3 *k*Hz, and the line-to-line rms voltage value is 207.846 volt.

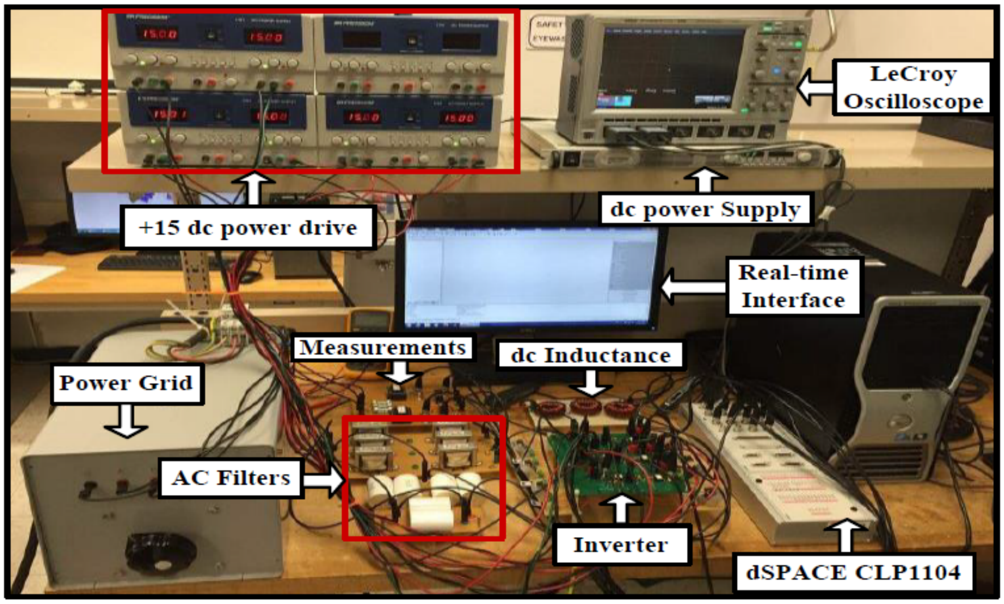
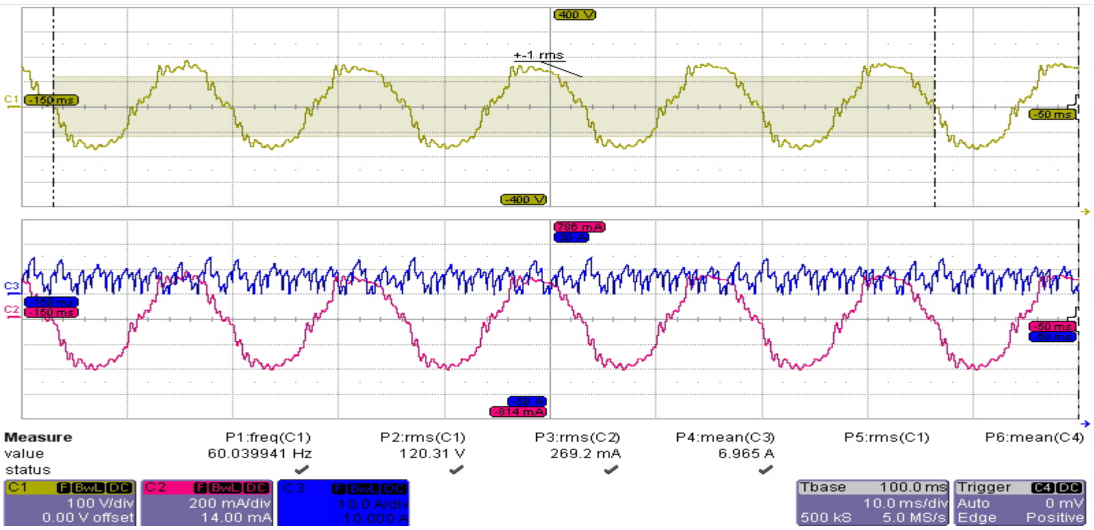


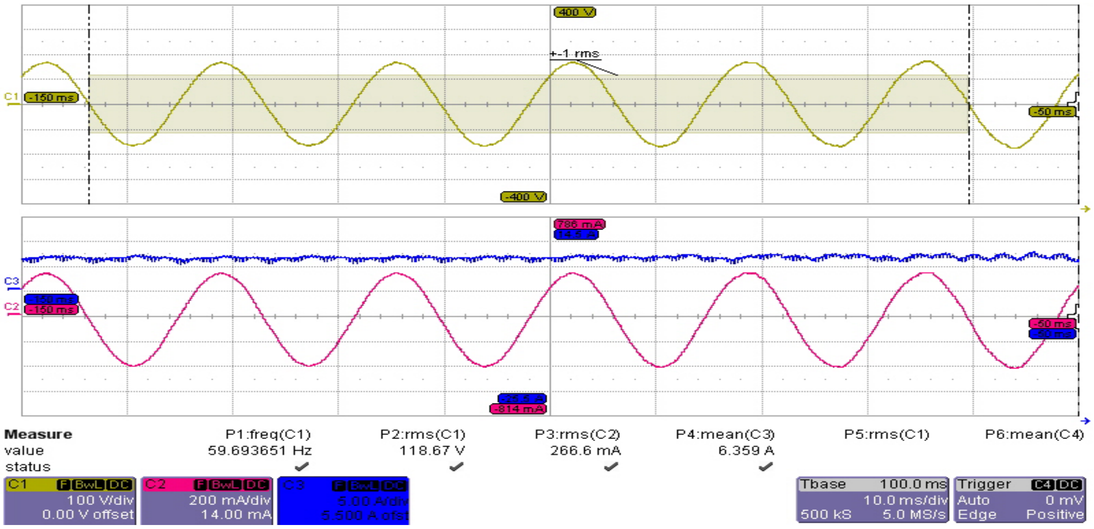
Figure 3.5: Layout of Experimental Setup

Figure 3.6 illustrates the experimental results of inverter current and output voltage when the conventional control algorithm is applied (without consideration of time delay). Since the waveforms of all the three phases are similar, only the current and the voltage of phase A are shown. It can be seen that the inverter current fluctuates effectively due to the time delay of the controller, which it is not taken into account. On the other hand, as shown in Figure 3.7, using the proposed control method, the fluctuation in the inverter current and output voltage is properly eradicated and the CSI operates properly. To evaluate the dynamics of the CSI, simulation is carried out to investigate the response of the active power of the converter output to a step change of reference power.



```
Measure   P1:freq(C1)     P2:rms(C1)  P3:rms(C2)  P4:mean(C3)  P5:rms(C1)  P6:mean(C4)
value     60.039941 Hz    120.31 V    269.2 mA    6.965 A
status    ✓               ✓           ✓           ✓
C1 BwL DC            C2 BwL DC          C3 BwL DC        Tbase 100.0 ms        Trigger C4 DC
100 V/div            200 mA/div         10.0 A/div       10.0 ms/div           Auto 0 mV
0.00 V offset        14.00 mA           10.000 A         500 kS 5.0 MS/s       Edge Positive
```

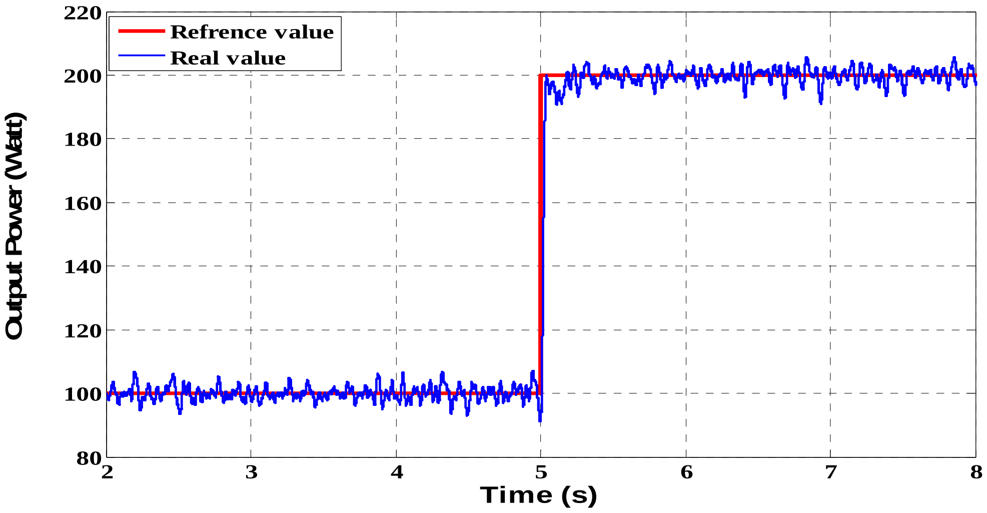
Figure 3.6: CSBI Performance with Conventional Control Method



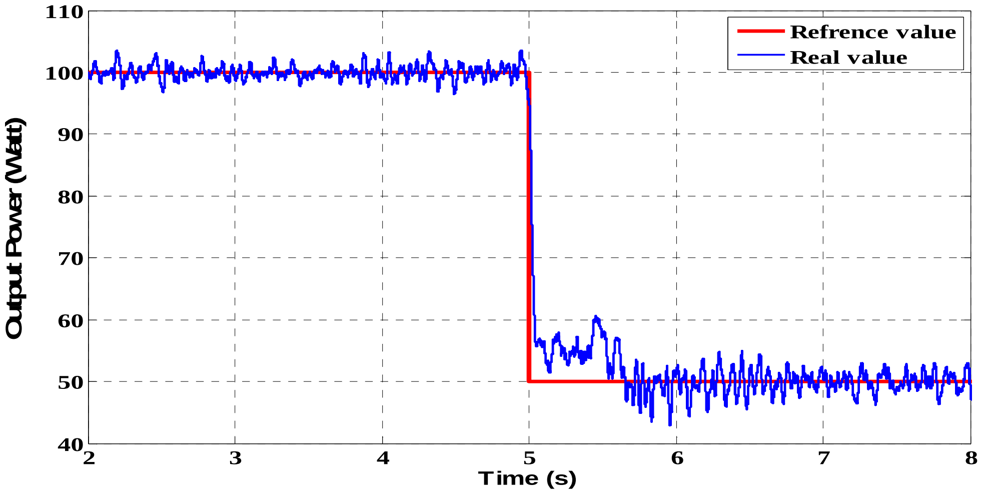
```
Measure   P1:freq(C1)     P2:rms(C1)  P3:rms(C2)  P4:mean(C3)  P5:rms(C1)  P6:mean(C4)
value     59.693651 Hz    118.67 V    266.6 mA    6.359 A
status    ✓               ✓           ✓           ✓
C1 BwL DC            C2 BwL DC          C3 BwL DC        Tbase 100.0 ms        Trigger C4 DC
100 V/div            200 mA/div         5.00 A/div       10.0 ms/div           Auto 0 mV
0.00 V offset        14.00 mA           5.500 A ofs      500 kS 5.0 MS/s       Edge Positive
```

Figure 3.7: CSBI Performance with Proposed Control Method

Figures 3.8(a) and 3.8(b) show the simulation of the converter current when the active power, P_{ref}, has instantly changed at t=5sec from 100 to 200 watts and 100 to 50, respectively. As shown, the controllers can effectively track the change of the active power references without harming the stability of the system.



(a)



(b)

Figure 3.8: Simulation Results of CSBI Response to Step Change of Active Power

3.2 Optimal Control Problem with Time-Delay

The goal of the optimal control theory is to determine control laws for a given dynamic system subjected to optimizing one or more predefined criteria. Time delays in biology, chemistry, electronics and mechanics domains [56-60] add one level of difficulty in the design phase of the control system the process. A valuable amount of studies in the control theory have been dedicated to the optimal control theory of time-delay systems.

Different approaches have been proposed, each with its own pros and cons from the accuracy and computational complexity point of view in theory and practical implementation [61-65]. The conventional techniques for solving optimal control problems can be categorized into two broad classes: (1) direct methods where the problem is being transferred into a nonlinear programming space by parameterization and discretization operators [60, 66], and (2) indirect methods that find the solution by applying a dynamic programming on Hamilton-Jacobi-Bellman (HJB) equation [61] or applying Pontryagin's maximum principle in a two-point boundary-value problem (TPBVP) [62].

Since solving a nonlinear HJB partial differential equation is complex in most cases, many researchers avoid using it. An excellent literature review on HJB is provided in [63]. On the other hand, one of the most accurate methods for solving optimal control problems is to set a series of optimal first-order necessary conditions based on Pontryagin's Maximum Principle. This method yields more accurate solutions and provides more confidence with the obtained responses than the others. However, the Pontryagin’s conditions that produce a system of nonlinear boundary-value differential equations are difficult to solve. As mentioned above, the TPBVP resulting from Pontryagin’s maximum principle does not have an analytical solution, hence, researchers are trying to find an approximate solution for these problems and have introduced the

Sensitivity Approximation Approach [64], and the Successive Approximation Approach (SAA) [65].

Here, the Homotopy Perturbation Method (HPM) is proposed and applied to solve the two-point boundary-value problem (TPBVP). The idea of HPM is to introduce a Homotopy parameter that takes its values from range [0 1]. The solution of each stage of deformation is close to that one of the previous stage. In brief, the system has the original form of equation at $p=1$, and by progressively decreasing the value of p to 0 at the final stage of deformations, the favorable solution is found. HPM provides an accurate solution in a few numbers of perturbations and therefore speeds up the convergence. The proposed approach considers a quadratic cost function as the criterion and transforms the time-delay optimal control problem into a time-delay and time-advance in the shape of a Two-Point Boundary-Value Problem (TPBVP), and then finally converts it to a set of linear time invariant TPBVP by applying the Homotopy Perturbation Method. Unlike traditional approaches [61-65], the presented technique only requires solving a sequence of linear TPBVPs that effectively reduce the required amount of computations and makes it more practical when comparing it with the approximation approaches applied in conventional platforms.

Section 3.2.1 introduces the nonlinearity and time delay in the optimal control theory, and Section 3.2.2 discusses the main idea of the Homotopy Perturbation Method (HPM). A new algorithm to find a suboptimal solution based on the HPM is presented in Section 3.2.3. Results are described in Section 3.2.4, followed by the conclusion.

3.2.1 Problem Statement

Consider a linear system with a time delay in state, as described below:

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) + B_1 x(t - t_d) \quad , \quad 0 \le t \le t_f \\ x(t) = \phi(t) \quad , \quad -t_d \le t \le 0 \\ x(0) = X_0 \end{cases} \tag{3.15}$$

with its quadratic performance index

$$J = \frac{1}{2} x^T(t_f) Q_f x(t_f) + \frac{1}{2}\int_0^{t_f} \left(x^T(t) Q x(t) + u^T(t) R u(t) \right) \tag{3.16}$$

where $x \in R^n$ and $u \in R^m$ are the state and the control functions, respectively. Matrices A, B and B_1 are constant with appropriate dimensions. Also let $\phi(t)$ be a given initial vector function, X_0 be an initial value, t_d be a time delay and a positive integer, $Q \in R^{n\times n}$ is a positive semi-definite matrix and $R \in R^{m\times m}$ is a positive definite matrix. The optimal control problem is to find the optimal control $u^*(t)$, which minimizes the performance index (3.16) and is subject to the system dynamic described in (3.15).

In accordance with the Pontryagin's maximum principle, the optimal condition is obtained as the following nonlinear TPBVP containing time-delay and time-advance terms:

$$\begin{cases} \dot{x}(t) = Ax(t) + B_1 x(t - t_d) - BR^{-1}B^T \lambda(t) \quad , \quad 0 \le t \le t_f \\ \dot{\lambda}(t) = Qx(t) + A^T \lambda(t) + \chi(t)(B_1 \lambda(t + t_d)) \ , \ 0 \le t \le t_f \\ x(t) = \phi(t) \quad , \quad -t_d \le t < 0 \\ \lambda(t_f) = Q_f x(t_f) \end{cases} \tag{3-17}$$

where

$$\chi(t) = \begin{cases} 1 & , \quad 0 \le t \le (t_f - t_d) \\ 0 & , \quad (t_f - t_d) \le t \le t_f \end{cases} \tag{3-18}$$

Hence, the optimal control law can be stated as:

$$u^*(t) = -R^{-1}B^T\lambda(t) \tag{3-19}$$

Since it is quite difficult to solve such a problem approximating solutions of the two-point boundary-valued problems (TPBVP) in (3.17) or finding a solution that will produce, a suboptimal control will be sought. Hence, the HPM will be considered the method to solve the TPBVP described in (3.17); details will follow.

3.2.2 Proposed Method

The model in (3.17) has both time-delay and time-advance terms. A new method based on HPM is introduced; it will generate a linear sequence of inhomogeneous TPBVP with no delay and advance in the state and co-state variables. To show the basic idea of this method, let us define an operator F in (3.20a) for $0 \le t \le (t_f - t_d)$, and in (3.20b) for $(t_f - t_d) \le t \le t_f$:

$$F(x(t),\lambda(t)) \overset{\Delta}{=} \begin{bmatrix} -\dot{x}(t) + Ax(t) + B_1x(t-t_d) - BR^{-1}B^T\lambda(t) \\ -\dot{\lambda}(t) + Qx(t) + A^T\lambda(t) + B_1\lambda(t+t_d) \end{bmatrix} = 0 \tag{3.20a}$$

$$F(x(t),\lambda(t)) \overset{\Delta}{=} \begin{bmatrix} -\dot{x}(t) + Ax(t) + B_1x(t-t_d) - BR^{-1}B^T\lambda(t) \\ -\dot{\lambda}(t) + Qx(t) + A^T\lambda(t) \end{bmatrix} = 0 \tag{3.20b}$$

Now let us separate the operator F into two parts:

$$F(x(t),\lambda(t)) = L(x(t),\lambda(t)) + N(x(t),\lambda(t)) \tag{3.21}$$

here, L and N represent linear and nonlinear terms, respectively.

Based on (3.21), the Homotopy technique presented in [67] can be written as the following:

$$H(x(t,p),\lambda(t,p),P) = QL(x(t,p),\lambda(t,p)) + PF(x(t,p),\lambda(t,p)) = 0 \tag{3.22}$$

which is equivalent to:

$$H(x(t,p),\lambda(t,p),P) = L(x(t,p),\lambda(t,p)) + PN(x(t,p),\lambda(t,p)) = 0 \tag{3.23}$$

where $Q = \begin{bmatrix} q & 0 \\ 0 & q \end{bmatrix}$, $q = 1-p$, $P = \begin{bmatrix} p & 0 \\ 0 & p \end{bmatrix}$ and $p \in [0\ 1]$ is an embedding parameter, which is named the Homotopy parameter. Thus, in a way that agrees with Homotopy equations in (3.23), the perturbed vectors of $x(t,p)$ and $\lambda(t,p)$ become as follows:

$$\begin{cases} x(t,p):[t_0,t_f]\times[0,1] \to R^n \\ \lambda(t,p):[t_0,t_f]\times[0,1] \to R^n \end{cases} \tag{3.24}$$

Obviously from (3.24) we have:

$$H(x(t,p),\lambda(t,p),0) = L(x(t,p),\lambda(t,p)) = 0 \tag{3.25a}$$

$$\begin{aligned} H(x(t,p),\lambda(t,p),I_{2\times2}) &= L(x(t,p),\lambda(t,p)) + N(x(t,p),\lambda(t,p)) \\ &= F(x(t,p),\lambda(t,p)) = 0 \end{aligned} \tag{3.25b}$$

while p varies in the span of [0, 1], the solution of linear parts of $\hat{x}(t)$ and $\hat{\lambda}(t)$, as in (3.25a), moves to the exact answers of $x(t)$ and $\lambda(t)$ as in (3.25b). In topology, it is called "deformation." A detailed illustration on choosing linear operators is displayed in [68]. In regard to the problem, two operators are selected, as follows:

(1) Linear operator:

$$L = \begin{bmatrix} \dfrac{\partial x(t,p)}{\partial t} - Ax(t,p) + BR^{-1}B^{T}\lambda(t,p) \\ \dfrac{\partial \lambda(t,p)}{\partial t} + Qx(t,p) + A^{T}\lambda(t,p) \end{bmatrix} \tag{3.26}$$

(2) Nonlinear operator:

$$N = \begin{bmatrix} B_1 x(t - t_d) \\ \chi(t)(B_1\lambda(t + t_d)) \end{bmatrix} \tag{3.27}$$

Here, the embedded parameter p is used as a small parameter. The solutions of (3.20a) and (3.20b) can be expressed as a power series of p.

$$\begin{bmatrix} \hat{x}(t) \\ \hat{\lambda}(t) \end{bmatrix} = \begin{bmatrix} x_0(t) + px_1(t) + p^2 x_2(t) + ... = \sum_{n=0}^{\infty} x_n(t)p^n \\ \lambda_0(t) + p\lambda_1(t) + p^2\lambda_2(t) + ... = \sum_{n=0}^{\infty} \lambda_n(t)p^n \end{bmatrix} \tag{3.28}$$

Setting $p = 1$ in the above series yields:

$$\begin{bmatrix} \hat{x}(t) \\ \hat{\lambda}(t) \end{bmatrix} = \begin{bmatrix} x_0(t) + x_1(t) + x_2(t) + ... = \sum_{n=0}^{\infty} x_n(t) \\ \lambda_0(t) + \lambda_1(t) + \lambda_2(t) + ... = \sum_{n=0}^{\infty} \lambda_n(t) \end{bmatrix} \tag{3.29}$$

where

$x_n(t) = \frac{1}{n!}\frac{\partial^n \hat{x}(t)}{\partial p^n}\bigg|_{p=0}$ and $\lambda_n(t) = \frac{1}{n!}\frac{\partial^n \hat{x}(t)}{\partial p^n}$.

Substituting (3.28) into (3.20a) and (3.20b), we have:

$$\begin{aligned} F = {} & L(x_0(t),\lambda_0(t)) + P^1 L(x_1(t),\lambda_1(t)) + \cdots + P^n L(x_n(t),\lambda_n(t)) \\ & + Pg^{(1)}(\hat{x}(t),\hat{\lambda}(t)) + P^2 g^{(2)}(\hat{x}(t),\hat{\lambda}(t)) + \cdots + P^n g^{(n)}(\hat{x}(t),\hat{\lambda}(t)) \end{aligned} \tag{3.30}$$

From (3.30), we rearrange the expression based on the order of P .

$$P^0:\begin{cases} L(x_0(t),\lambda_0(t))=0 \\ x_0(t)=\phi(t) \qquad , \quad -t_d\le t<0 \\ \lambda_0(t_f)=Q_f x_0(t_f) \end{cases}$$

$$\mathrm{P}^1:\begin{cases} L(x_1(t),\lambda_1(t))+g^{(1)}(\hat{x}(t),\hat{\lambda}(t))=0 \\ x_1(0)=0 \\ \lambda_1(t_f)=0 \end{cases}$$

$$\vdots \tag{3.31}$$

$$\mathrm{P}^n:\begin{cases} L(x_n(t),\lambda_n(t))+g^{(n)}(\hat{x}(t),\hat{\lambda}(t))=0 \\ x_n(0)=0 \\ \lambda_n(t_f)=0 \end{cases}$$

where

$$g^{(1)}(\hat{x}(t),\hat{\lambda}(t))=\begin{bmatrix} N_1(\sum_{j=0}^{\infty}x_j(t)p^j,\sum_{j=0}^{\infty}\lambda_j(t)p^j)\Big|_{p=0} \\ N_2(\sum_{j=0}^{\infty}x_j(t)p^j,\sum_{j=0}^{\infty}\lambda_j(t)p^j)\Big|_{p=0} \end{bmatrix}$$

$$g^{(n)}(\hat{x}(t),\hat{\lambda}(t))=\begin{bmatrix} \frac{1}{(n-1)!}\frac{\partial^{n-1}N_1(\sum_{j=0}^{\infty}x_j(t)p^j,\sum_{j=0}^{\infty}\lambda_j(t)p^j)}{\partial p^{n-1}}\Big|_{p=0} \\ \frac{1}{(n-1)!}\frac{\partial^{n-1}N_2(\sum_{j=0}^{\infty}x_j(t)p^j,\sum_{j=0}^{\infty}\lambda_j(t)p^j)}{\partial p^{n-1}}\Big|_{p=0} \end{bmatrix} \tag{3.32}$$

Solving all of the above linear time-invariant problems in a recursive manner leads to $x_n(t)$ and $\lambda_n(t)$ for all $n\ge 0$. However, by making (3.29), we can find $\hat{x}_n(t)$ and $\hat{\lambda}_n(t)$,which are the approximation of the exact answer. Therefore, the optimal control law can be expressed in the form below:

$$u^*(t)=-R^{-1}B^T\sum_{n=0}^{\infty}\lambda_n(t) \tag{3.32}$$

Theorem 2.1. (Sufficient condition of convergence)

Suppose that X and Y are two Banach spaces; define a contractive nonlinear:

$$N \overset{\Delta}{=} \begin{bmatrix} N_1[\hat{x}(t,p),\hat{\lambda}(t,p)] \\ N_2[\hat{x}(t,p),\hat{\lambda}(t,p)] \end{bmatrix} \tag{3.33}$$

where N is mapping X to Y that

$$\forall u\ ,\tilde{u};\ \|N(u)-N(\tilde{u})\| \le \gamma\|u-\tilde{u}\| \tag{3.34}$$

where u and $\tilde{u}$ are members of X , and γ is between 0 and 1.

Based on Banach's fixed point theorem, the contractive nonlinear (3-34) has a unique fixed point U which

$$N(U)=U \tag{3.35}$$

The following sequence can be generated based on the HPM:

$$U_n = N\left(\sum_{i=0}^{n-1}\hat{U}_i\right)\ ,\ n=1,\ 2,\ 3\ ,... \tag{3-36}$$

where $U \overset{\Delta}{=} \begin{bmatrix} x(t) \\ \lambda(t) \end{bmatrix}$.

Suppose that $U_0 = u_0 \in B_t(u)$ where $B_t(u) = \{u^* \in X \big| \|u^* - u\| < t \in [t_0, t_f]\}$ and then we have:

$$U_n \in B_t(u) \tag{3-37}$$

$$\lim_{n\to\infty} U_n = u \tag{3-38}$$

Proof.

Let $n=1$ in (3.36) from (3.35), so then we have:

$$\|U_1 - u\| = \|N(U_0) - N(u)\| \le \gamma \|u_0 - u\| \tag{3-39}$$

For $n = n-1$, assume $\|U_{n-1} - u\| \le \gamma^{n-1}\|u_0 - u\|$ as an induction hypothesis. Then:

$$\|U_n - u\| = \|N(U_{n-1}) - N(u)\| \le \gamma \|U_{n-1} - u\| \le \gamma^n \|u_0 - u\|. \tag{3-40}$$

Using (3.40), we have:

$$\|U_n - u\| \le \gamma^n \|u_0 - u\| \le \gamma^n t \le t \tag{3.41}$$

Equation (3.41) concludes that $U_n \in B_t(u)$, which is proved by Equation (3.37).

From (3.40), we found that $\|U_n - u\| \le \gamma^n \|u_0 - u\|$. Since $\lim_{n\to\infty} \gamma^n = 0$, there is $\lim_{n\to\infty} \|U_n - u\| = 0$, where $\lim_{n\to\infty} U_n = u$.

3.2.3 Suboptimal Control

Since it is impossible to find the control law from an infinite series as described in (19), finite series must be found. To keep the first few terms in (19), we have the k^{th}-order suboptimal control law as described by

$$u_k(t) = -R^{-1}B^T \sum_{n=0}^{k} \lambda^{(n)}(t). \tag{3.42}$$

Here the value of k can be decided based on the precision required.

With the suboptimal control law described in (3.42), the quadratic performance index can be calculated by using

$$J_k = \frac{1}{2}x^T(t_f)Q_f x(t_f) + \frac{1}{2}\int_0^{tf}\left(x^T(t)Qx(t) + u_k{}^T(t)Ru_k(t)\right) \tag{3.43}$$

where $x(t)$ is the corresponding state trajectory obtained by applying $u_k(t)$ to the original nonlinear system in (3.15) with $x(t_0)=\phi(t_0)$. The process stops if we meet the condition

$$\left|J_k - J_{k-1}\right| < \varepsilon. \tag{3.44}$$

If the error bound $\varepsilon > 0$ is chosen small enough, then the k^{th}-order suboptimal control law in (3.42) will be very close to the optimal control law $u^*(t)$, the value of performance index J_k will be very close to its optimal value J^*, and the boundary condition will also be satisfied.

Algorithm of Finding Suboptimal Control Law

Step 1: Construct Homotopy as described in (3.22), (3.23) and (3.24), and estimate the initial approximations.

Step 2: Substitute equation (3.28) and (3.29) into (3.23) and (3.24), and arrange them with respect to the order of p .

Step 3: Let $j = 0$.

Step 4: Make the coefficients of p^j be zero and solve the resulted linear TPBVP.

Step 5: Let $j = k$ and calculate the k^{th} order suboptimal control law $u^{(k)}(t)$ according to (3.28). Then, this control law is applied to the nonlinear system as described by (3.16) to corresponding state trajectory $x_i(t)$ and the cost function J_k using to (3.29).

Step 6: If the improvement satisfies $|J_k - J_{k-1}| < \varepsilon$, which ε is the selected threshold, a sufficiently small positive parameter, go to Step 7.

Step 7: Increment *j* by 1, then go to Step 5.

Step 8: Stop.

3.2.4 Numerical Example

Nonlinear oscillators usually described by a set of nonlinear ordinary differential equations play an important role in high technologies such as biology, mechanics, optics, and particularly in electronic circuits. To show the high accuracy and efficiency of the proposed method, the developed method is applied to a harmonic oscillator with retarded damping. [69]

Consider the problem:

$$\begin{bmatrix} \dot{x}_1(t) \\ \dot{x}_2(t) \end{bmatrix} = \begin{bmatrix} x_2(t) \\ -x_1(t) - x_2(t - t_d) + u(t) \end{bmatrix} \tag{3.45}$$

with the given initial conditions

$$\begin{cases} x_1(0) = 10 \\ x_2(t) = 0, \quad -t_d \le t \le 0 \end{cases} \tag{3.46}$$

The quadratic cost function to be minimized is described by:

$$J = 5{x_1}^2(2) + \frac{1}{2}\int_0^2 u^2(t)dt \tag{3.47}$$

To show the validation of the proposed method, first, let the delay be zero, i.e., $t_d = 0$. The results from the proposal method are shown in Figures 3.9, 3.10 and 3.11. And the value of the cost function of this harmonic oscillator design with the collocation method is $J = 2.2637$ and the value J is 2.2632 after 5 iterations with the proposed method. To further investigate the efficiency of this method, the amount of delay t_d is increased in the state and the performance of the system is simulated. The calculated control input $u(t)$ to the system with $t_d = 0.1, 0.2$, and 0.3 are given in Figures 3.12, 3.15, and 3.18, respectively. The corresponding state trajectories, $x_1(t)$ and $x_2(t)$, for the different delay values are shown in Figures 3.13 and 3.14, 3.16 and 3.17, and 3.19 and 3.20. The values of the cost function for three different values of delay are shown in Table 3.2.

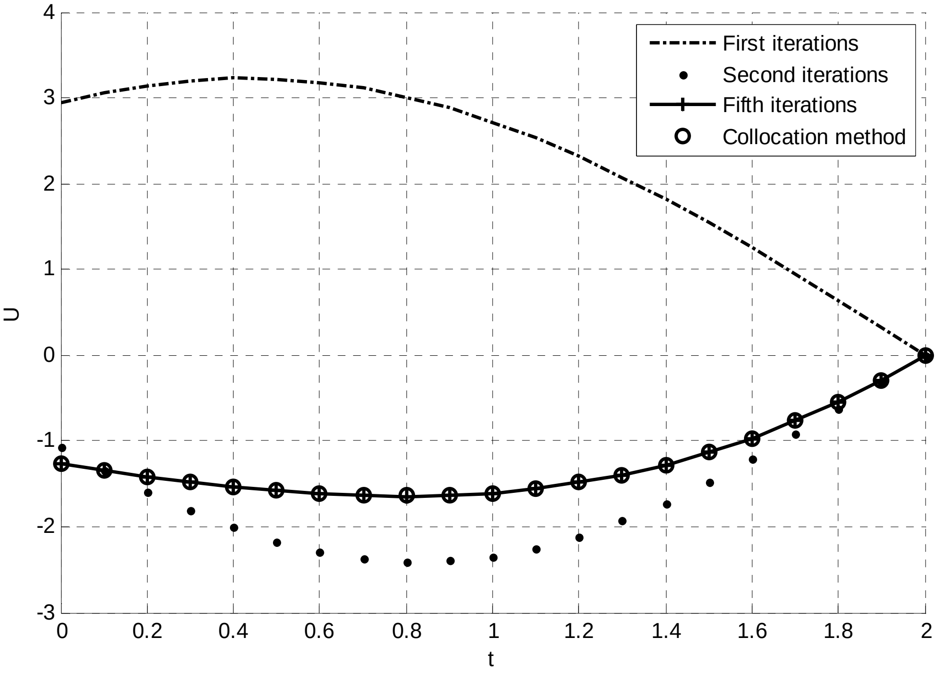


Figure 3.9: Suboptimal Control Law $(t_d = 0.0)$

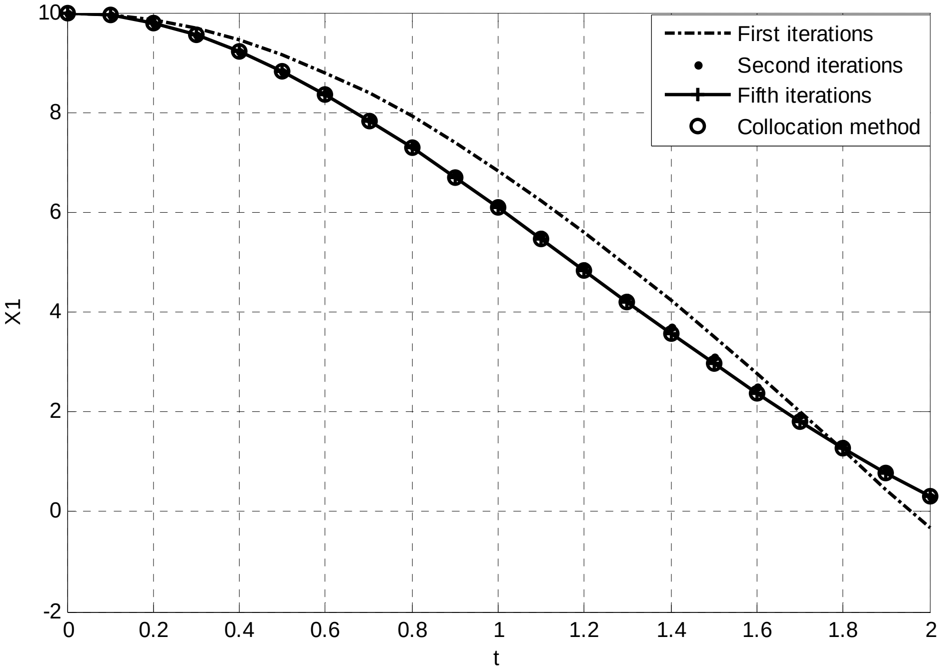


Figure 3.10: Suboptimal State Trajectory x_1 $(t_d = 0.0)$

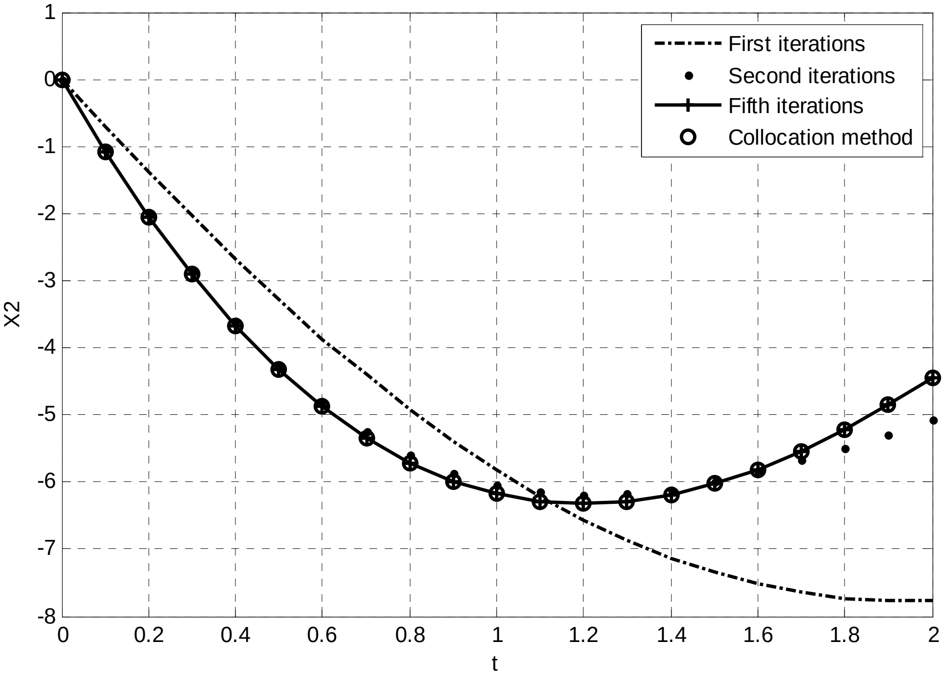


Figure 3.11: Optimal State Trajectory x_2 $(t_d = 0.0)$

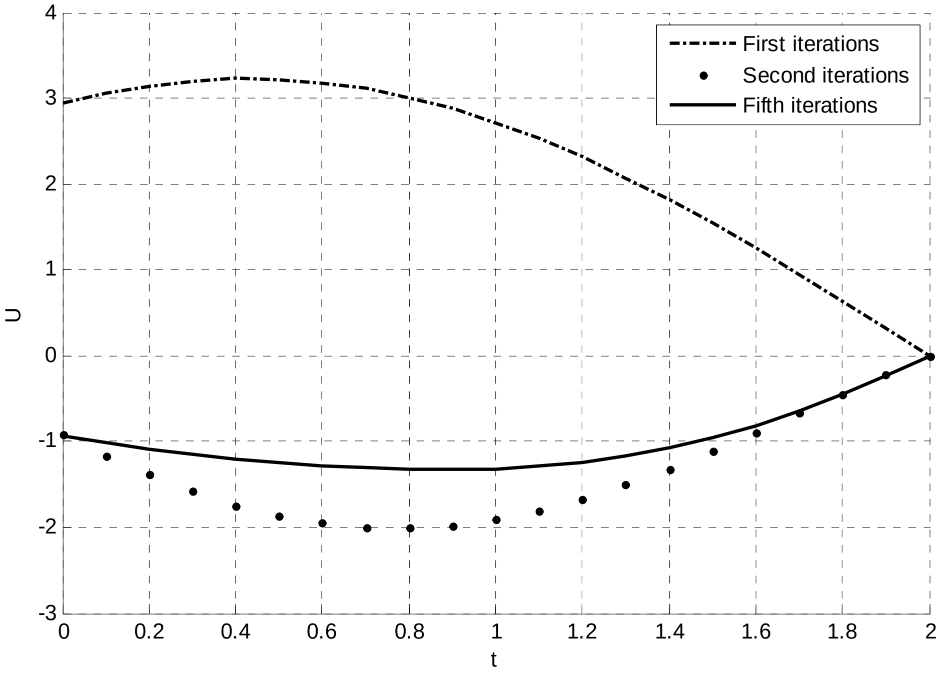


Figure 3.12: Suboptimal Control Law $(t_d = 0.1)$

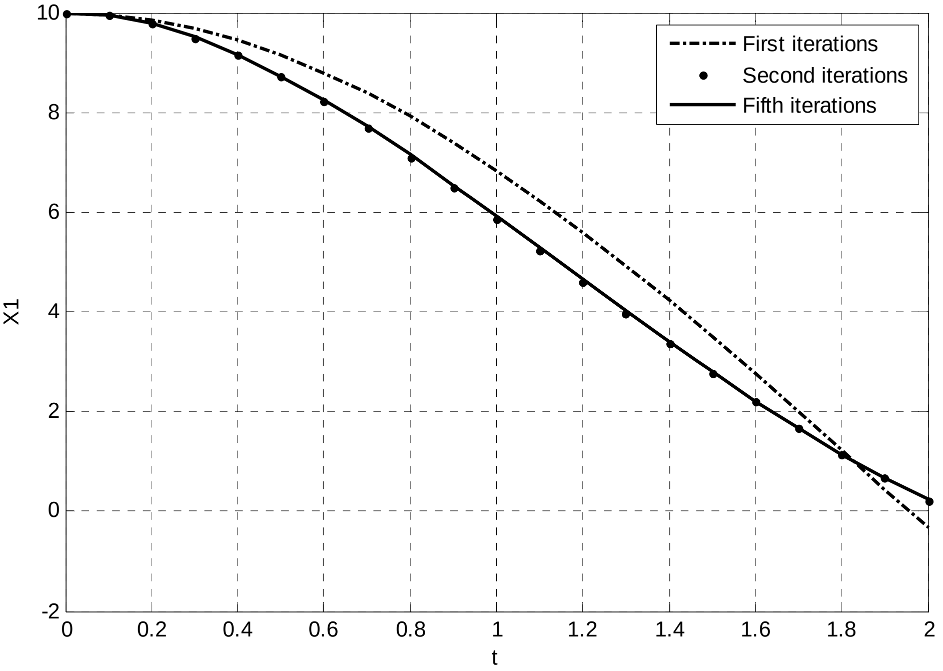


Figure 3.13: Suboptimal State Trajectory x_1 $(t_d = 0.1)$

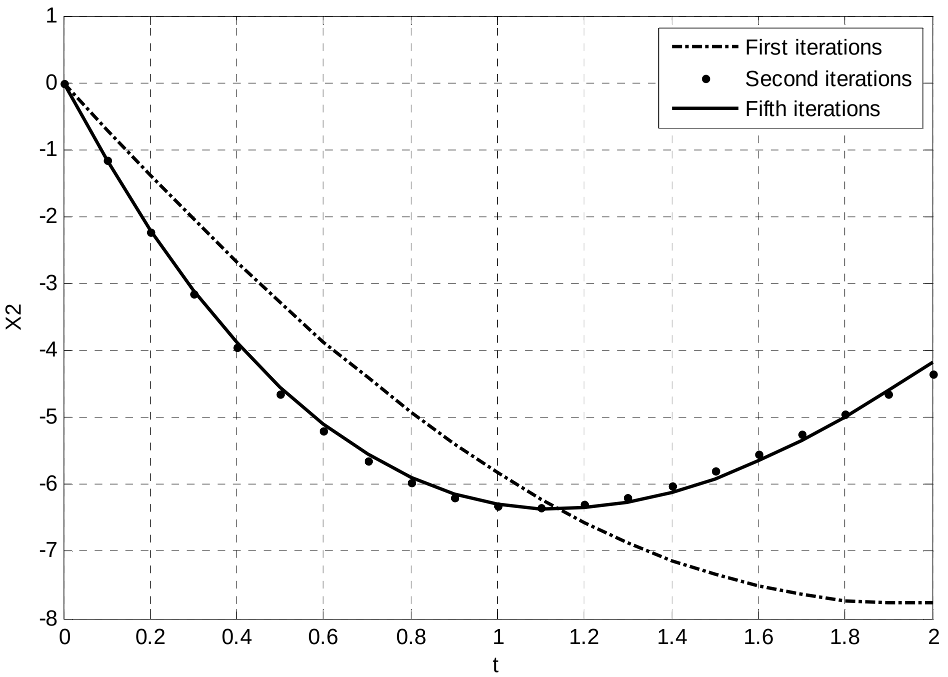


Figure 3.14: Suboptimal State Trajectory x_2 $(t_d = 0.1)$

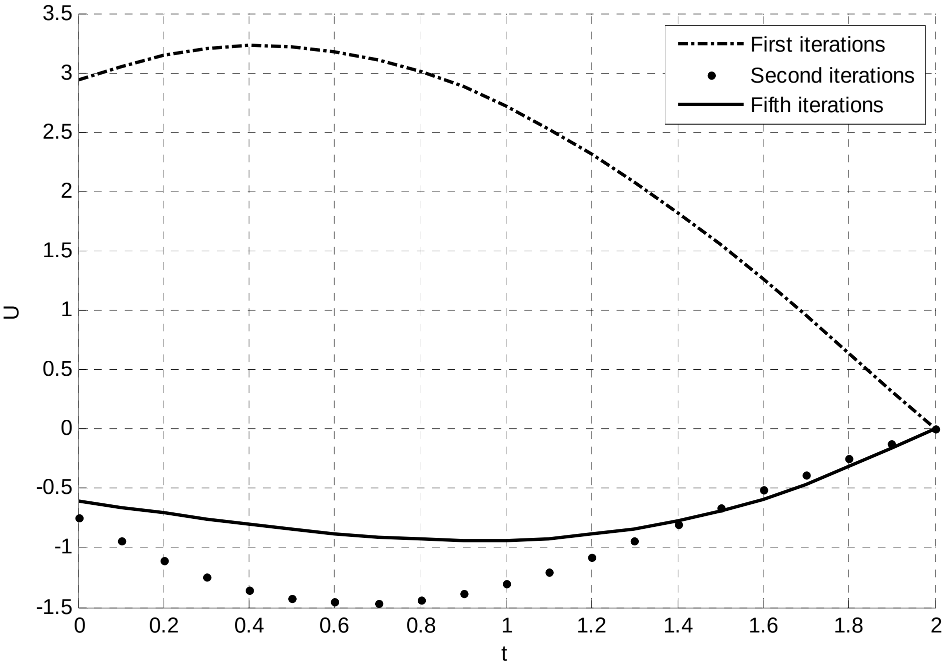


Figure 3.15: Suboptimal Control Law $(t_d = 0.2)$

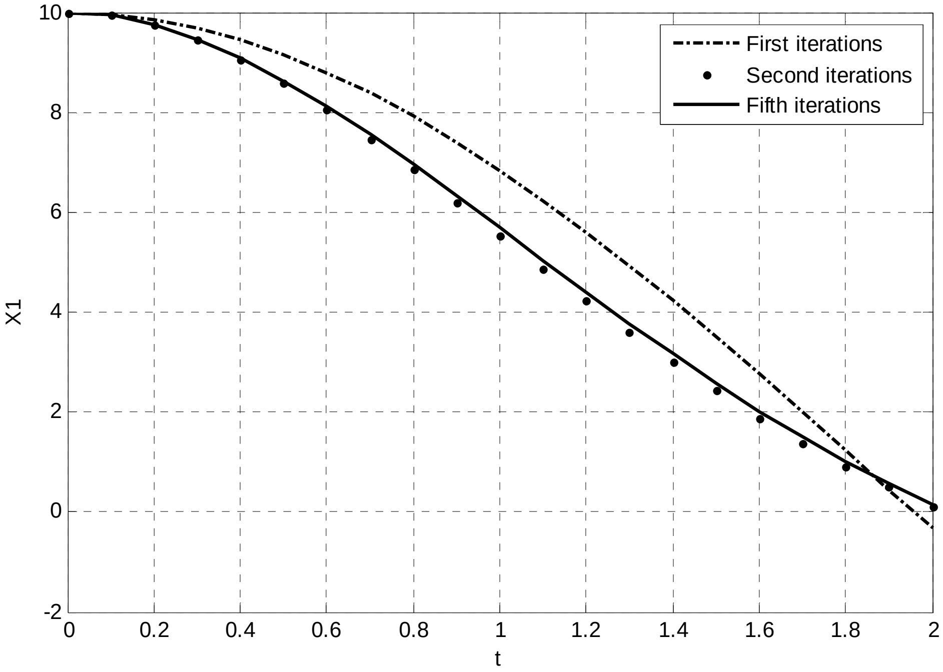


Figure 3.16: Suboptimal State Trajectory x_1 $(t_d = 0.2)$

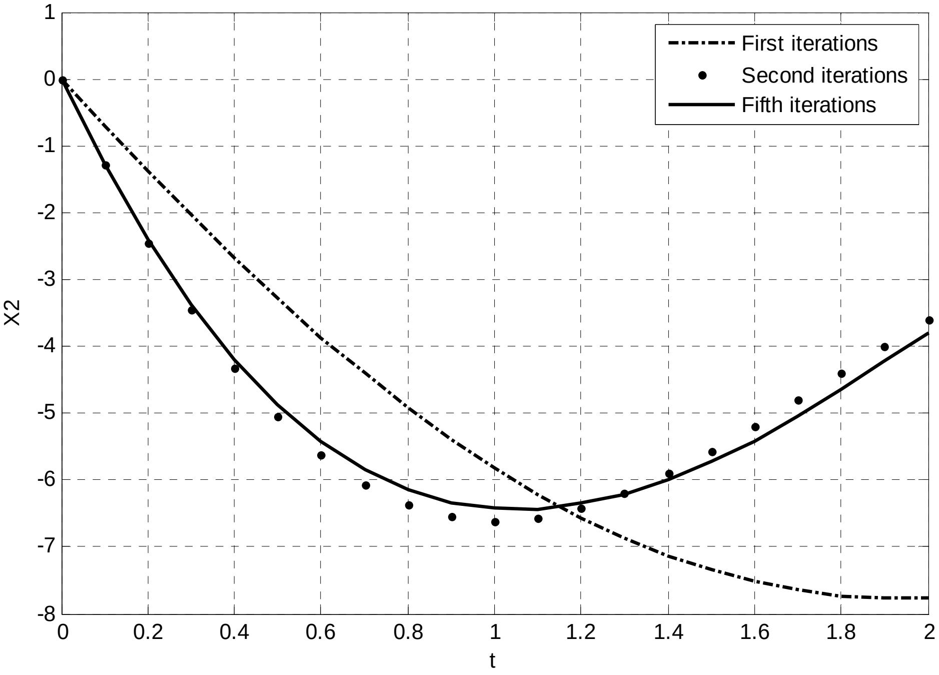


Figure 3.17: Suboptimal State Trajectory x_2 $(t_d = 0.2)$

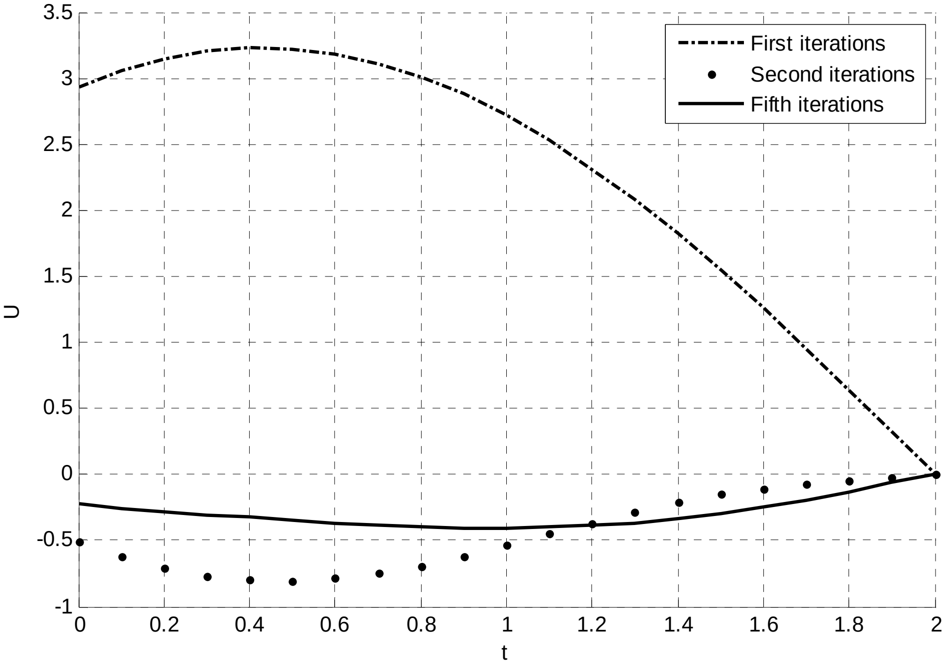


Figure 3.18: Suboptimal Control Law $(t_d = 0.3)$

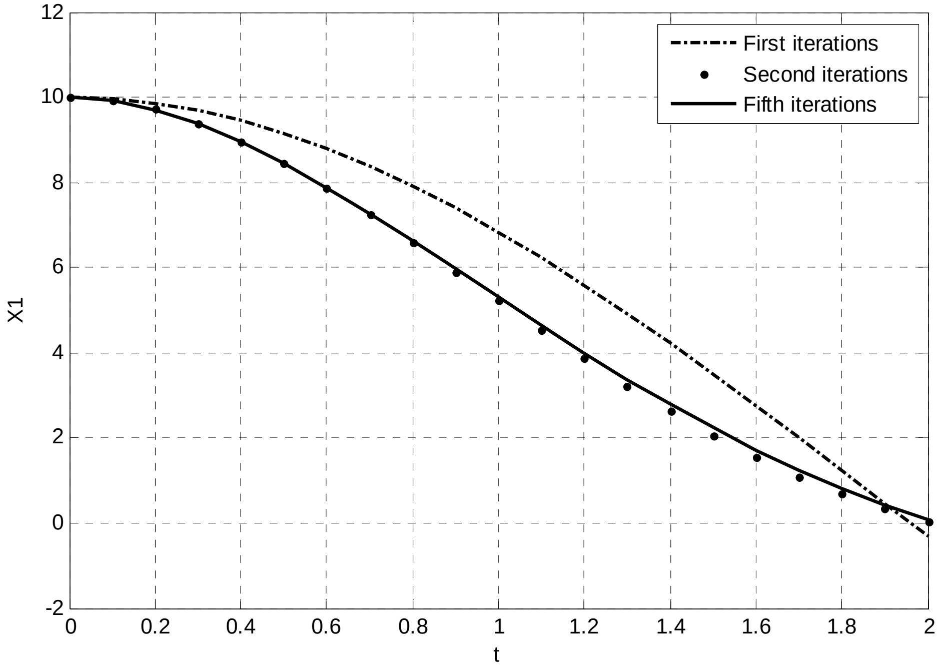


Figure 3.19: Suboptimal State Trajectory x_1 $(t_d = 0.3)$

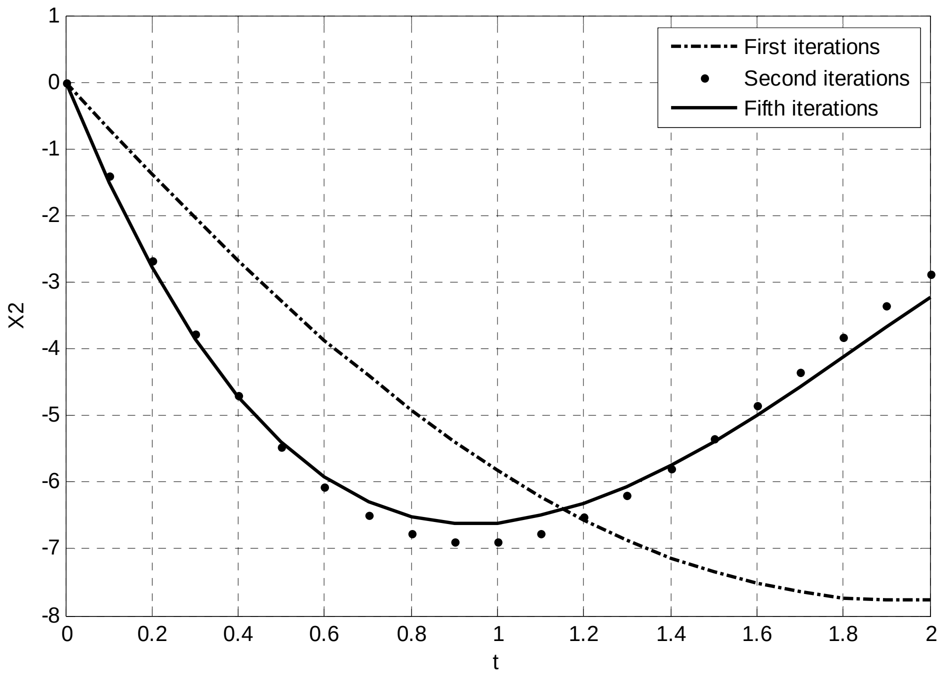


Figure 3.20: Suboptimal State Trajectory x_2 $(t_d = 0.3)$

Table 3.2: Cost Function Values for Different Delays of Different Iterations

Case	Iteration / Delay	1	2	3	4	5
1	$t_d = 0.0$	6.7164	3.7865	2.3043	2.2683	2.2632
2	$t_d = 0.1$	6.7164	2.4886	1.4711	1.4658	1.4412
3	$t_d = 0.2$	6.7164	1.2246	0.7146	0.6245	0.5916
4	$t_d = 0.3$	6.7164	0.2878	0.1213	0.1212	0.1211

3.3 Conclusion

In this chapter, the importance of time-delay in ICSs was shown. First, the natural time-delay effect of an SVPWM-based switching pattern for grid-connected three-phase current source inverter was studied. An algorithm to track the time delay in real-time to overcome the effect of time-delay produced in sensing loop was proposed. This guarantees synchronization between grid phase and inverter output. Also, the observer state feedback controller was applied to overcome the effect of time-delay in the control signal. The experimental results clearly show that the proposed approach can compensate the effect of time delay and improve quality of output inverter signal.

Then, the effect of ignoring natural time delay in optimal control design was shown. To optimize linear, time-delay control systems, an efficient iterative method is offered based on the HPM to determine the optimal control law in the form of infinite series with easy computable terms. Despite other famous methods such as the SAA and Sensitivity Approach (SA), this method avoids the difficulty of solving a sequence of linear time-varying TPBVPs of solving directly the nonlinear TPBVP or the HJB equation. Instead it only needs solving a sequence of linear time-invariant TPBVPs, which is more practical than the above-mentioned approximate methods in aspect of computational complexity. This section shows clearly that time-delay is really important in design of optimal controller. Ignoring small value of time-delay can significantly change result of optimal controller cost function. It was found that dealing with systems with time delays is difficult; hence, this is the reason that most researchers ignore delays in the controller design process.

CHAPTER 4

TIME-DELAY SWITCH ATTACK ON NETWORKED CONTROL SYSTEMS

4.1 Introduction

Networked control systems are constantly being modernized by introducing new telecommunication technologies for control and monitoring to improve efficiency, reliability and sustainability. This modernization effort relies on computers and multi-purpose networks, but causes these systems to be vulnerable to cyber attacks and greatly impacts people's lives and affects the economy.

Consider for instance, U.S. power networks; they operate with supervisory control and data acquisition (SCADA) systems. SCADA systems are industrial control systems for large scale processes that include multiple sites and operate over long distances. Despite the precautions, several cyber attacks on SCADA systems have been reported [1, 2, 70-73]. Furthermore, replacing proprietary communication networks with open communication standards causes the process control and SCADA systems to become vulnerable to cyber security risks [74].

In general, an intruder performing an attack could access the IT infrastructure of ICSs, gain access to various sensors and control signals, and manipulate them to disrupt and sabotage the system. For example, an intruder can increase a load on a particular power transformer, shut down sections of a control system, or introduce inefficiencies in the system and the plant [9, 12, 13, 75].

Investigating the methods of attacks on ICSs of sensitive infrastructures, devising measures, and security control protocols have attracted the attention of academia and industries. These industries' efforts have ended in a large amount of literature and in the production of hardware and software systems dedicated to security measures that prevent possible attacks on industrial systems. An attack called the "time-delay-switch attack" or "TDS" for short in the NCS introduced in this section. This attack can be aimed at different parts of NCS and cause inefficiency or stability issues in the system.

In this chapter, TDS attacks are introduced and how this type of attack can be injected into a NCS by a hacker is discussed. Then, the impact of introducing time delays in the sensing loop (SL) or in the Automatic Generation Control (AGC) signal, which is the only automatic closed loop between the IT and the power system on a control area, is discussed. When a hacker introduces delays in a control system, they are performing a time-delay-switch attack (TDS). The effects of this attack on another application related to the biomedical industry were also studied. This chapter also details how a TDS attack can cause any control system to become unstable. Therefore, future NCSs will have to use an advanced two-way communication and design new controllers to provide a better situational awareness of the state of a system, keeping NCS reliable and safe from TDS attacks.

4.2 TDS Attack Model on NCS

A time-delay switch attack can be injected into different parts of a NCS. It can be injected into the feedback line (signal transmitted from the plant output to the controller), the referenced signal, and the control signal in Figure 4.1, respectfully. Here, a TDS attack on the feedback line is addressed.

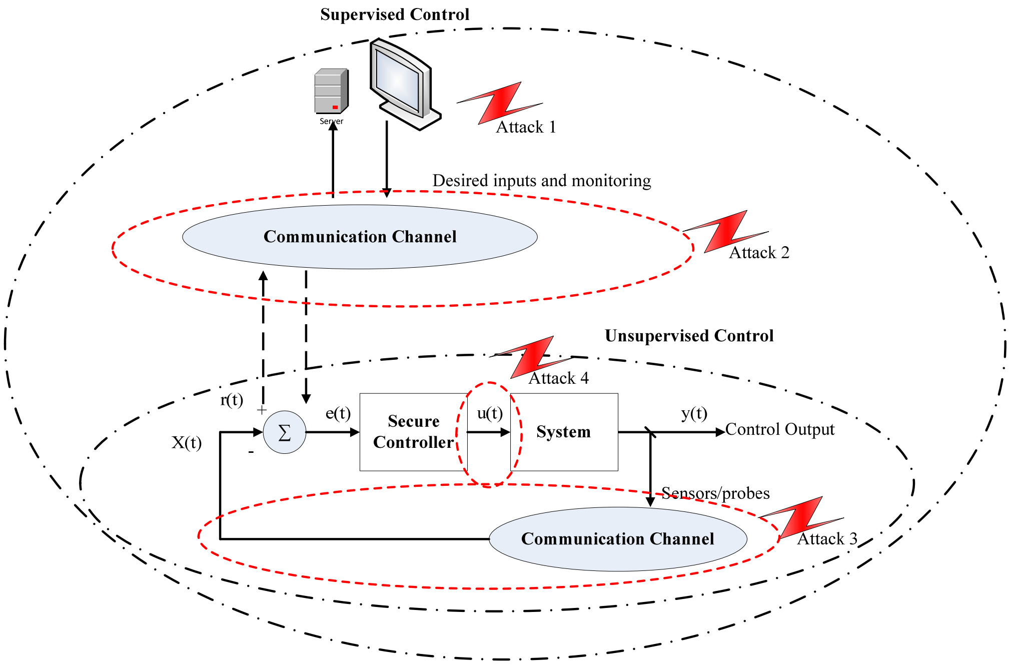


Figure 4.1: Different Places that TDS Attacks can be Injected

Consider a general LTI system, described as follows:

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) \\ x(0) = x_0 \\ y(t) = Cx(t) + Du(t) \end{cases} \tag{4.1}$$

where x and y are state and output vectors, u is the control signal and x_0 is the initial state value. Also A , B , C and D are constant matrices with appropriate dimensions.

The controller is described as:

$$U = h(y) \tag{4.2}$$

where y is the information communicated to the controller about the plant's state. The function, h , describes the plant's output and communication methodology.

An attack on the control system involves altering any component of the NCS. A general attack can be described as a function that alters any of the components of the system:

$$(\widetilde{A}, \widetilde{B}, \widetilde{C}, \widetilde{D}, \widetilde{x}, \widetilde{y}, \widetilde{u}, \widetilde{t}\,) = \Lambda(A, B, C, D, x, y, u, t) \tag{4.3}$$

where $(\widetilde{A}, \widetilde{B}, \widetilde{C}, \widetilde{D}, \widetilde{x}, \widetilde{y}, \widetilde{u}, \widetilde{t}\,)$ are the corrupted functions as a result of the attack Λ. The TDS attack can be modeled as follows:

$$\widetilde{y} = \begin{cases} y & \textit{otherwise} \\ y(t-\tau) & \textit{attack} \end{cases} \tag{4.4}$$

or

$$\widetilde{t} = \begin{cases} t & \textit{otherwise} \\ t-\tau & \textit{attack} \end{cases} \tag{4.5}$$

where τ is function of t and is a random variable time-delay that is always less than time t .

4.3 TDS Attacks in Communication Systems

An illustration of a TDS attack on a NCS through a simplified version of Figure 4.1 is shown in Figure 4.2. The plant is a power-area system controlled by the load frequency controller. The $x(t)$ is a vector of the state of power area, and is measured and transmitted to the controller via communication lines. The *u* (t) is the control signals, *r*(*t*) is the desired state, and e(t) is the difference between the desired state and the measured plant state. The intruder attacks the communication line between the plant and controller either by dropping the packets or delaying them. The plant (P) sends the state variables, *x*(*t*), as information packets to the TDS attack variants.

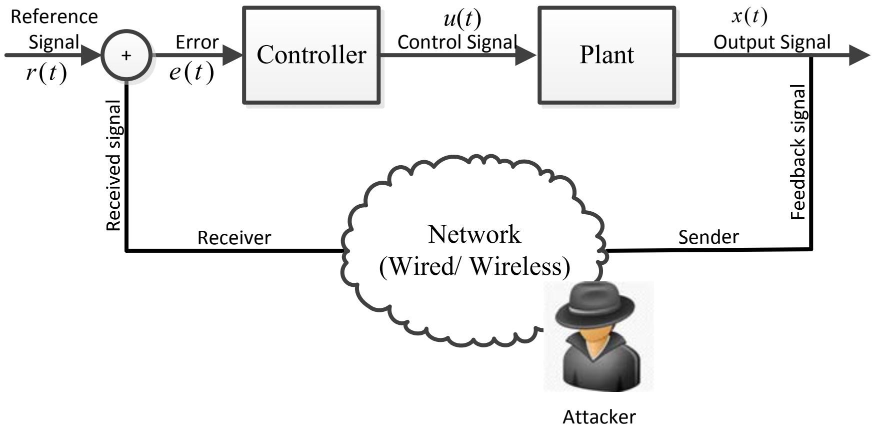


Figure 4.2: A Simplified NCS System under a TDS Attack

Replay TDS Attack. The attacker leaves the first message $x(0.1)$ intact. Then, it records and drops the second message, $x(0.2)$, and resends in its place the first message. Subsequently, it sends $x(0.2)$ instead of the third message, etc. The attacker can generalize this attack by introducing different time delays. Table 4.1 illustrates the steps of this attack where the attacker adds a delay of 0.1 sec. In the table, “TS” denotes the timestamp.

Table 4.1: Scenario 1, Sequence of Events During a Replay TDS Attack

TS	{TS, P(*t*)}	{TS, C(*t*)}	Controller Input (*e*(*t*))
0.1	$\{0.1, x(0.1)\}$	$\{0.1, x(0.1)\}$	$r(0.1) - x(0.1)$ or 0
0.2	$\{0.2, x(0.2)\}$	$\{0.1, x(0.1)\}$	$r(0.2) - x(0.2 - 0.1)$ or 0
0.3	$\{0.3, x(0.3)\}$	$\{0.2, x(0.2)\}$	$r(0.3) - x(0.3 - 0.1)$ or 0

Timestamp-based TDS Attack. The attacker reconstructs the packet, and fixes the timestamp. In this way, the timestamping detector is not able to find the time-delay attack. The attacker receives the first message from the plant, and copies the value in the buffer. Then, it substitutes the state value of the first packet inside the second message, and reconstructs the packet. Then, it sends the packet to the controller. Table 4.2 illustrates this scenario. In this table, x_1 denotes the first state value, x_2 the second state value, and so forth. Let us say that the plant sends x_2 at 0.2 sec, and attacker copies it. Now, consider that the controller get x_3 at 0.3 sec. At this time, the attacker sends x_2 instead of x_3 with a corrected 0.3 time stamp. This can happen even on encrypted scenarios if the attacker can decrypt the packet and reconstruct it with the new wrong state, and correct the time stamps.

Table 4.2: Scenario 2, Sequence of Events During Timestamps Alter TDS Attack

TS	{TS, P(t)}	{TS, C(t)}	*Controller Input*
0.1	$\{0.1, x_1(0.1)\}$	$\{0.1, x_1(0.1)\}$	$r_1(0.1) - x_1(0.1)$
0.2	$\{0.2, x_2(0.2)\}$	$\{0.2, x_1(0.2)\}$	$r_2(0.2) - x_1(0.2)$ $= r_2(0.2) - x_2(0.2 - 0.1)$
0.3	$\{0.3, x_3(0.3)\}$	$\{0.3, x_2(0.3)\}$	$r_3(0.3) - x_2(0.3)$ $= r_3(0.3) - x_3(0.3 - 0.1)$

Noise-based TDS Attack. The attacker injects fake packages into the system, making the system add the delay to the transmission of system packages. In this way, the packets from the plant are delivered to the controller with the delay.

4.4 Sabotage and Destabilizing Analysis of TDS Attack

4.4.1 Theoretical Analysis

Before commencing the proof of the destabilizing effects of TDS attacks, the assumptions and definitions are examined.

An assumption of approximation is made of the NCS by a linear time-invariant (LTI) system. Also, an assumption is made that the controller is the optimal controller with optimal gain K. This can be easily extended for other types of controllers. This dissertation focuses on the optimal controller in most of the applications, as these types of controllers are more sensitive to TDS attacks.

Let h be defined by the following (also shown in Figure 4.3):

$$h = \begin{cases} 0 & t \le t_a \\ 1 & t > t_a \end{cases} \tag{4.6}$$

Then, the NCS controller under a TDS attack can be written as:

$$u = -K\widetilde{y} = -K\left[(1-h)\,x + hx_d\right] \tag{4.7}$$

where $x_d = x(t - t_d)$, t_a is the start time of the attack.

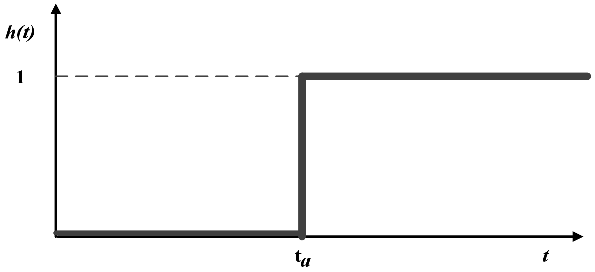


Figure 4.3: Step Function, *h(t)*

It is obvious that the system is stable for all $t \leq t_a$ by definition of the optimal controller. However, for $t > t_a$ it is not obvious whether or not the system would be stable.

Theorem: The system described in (4.1) under attack (4.7) is not efficient for any delay $t_d > 0$, and can be unstable for large values of delay.

Theorem 4-1:

Applying (4.7) to (4.1) results in:

$$\dot{X} = AX - BK\left((1-h)X + h\ X_d\right) \tag{4.8}$$

Let us write (4.8) as:

$$\dot{X} = (A - BK)X + hBK(X - X_d) \tag{4.9}$$

Define $G \overset{\Delta}{=} (A - BK)$. G is a negative definite, since the system is stable without the attack. Then, Equation (4.9) is written as:

$$\dot{X} = (G + hBK)X - hBKX_d \tag{4.10}$$

Now, let us integrate Equation (4.10):

$$X = e^{Gt+BK(t-t_a)h} X_0 - e^{Gt+BK(t-t_a)h} BK \int_0^t e^{-Gr-BK(r-t_a)h} hx_d dr \tag{4.11}$$

Suppose $t > t_a$ and $t > t_d$, such that $t - t_a \approx t$ and $h = 1$. Then, Equation (4.11) can be approximated by:

$$X \approx e^{At} X_0 - BK\left[\int_{t_a}^{t} e^{A(t-r)} X_d dr\right] \tag{4.12}$$

Since *A* is a negative definite, then for large *t*:

$$X \approx -BK\left[\int_{t_a}^{t} e^{A(t-r)} X_d dr\right] \tag{4.13}$$

Equation (4.13) represents the asymptotic behavior of the system after the attack. The Differentiate Equation (4.13) with all constant terms multiplied by e^{At}:

$$\dot{X} \approx -BKX\,(t - t_d) \tag{4.14}$$

If Equation (4.14) is shifted by $t_{d,}$ the result is

$$\dot{X}(t + t_d) \approx -BKX\,(t) \tag{4.15}$$

then:

$$\dot{X}(t + t_d) - \dot{X}(t) \approx -BK[X(t) - X(t - t_d)] \tag{4.16}$$

and

$$\dot{X}(t) - \dot{X}(t - t_d) \approx -BK[X(t - t_d) - X(t - 2t_d)] \tag{4.17}$$

therefore,

$$\dot{X}(t+t_d)-\dot{X}(t)\approx(BK)^2\int_0^t X(s-t_d)-X(s-2t_d)ds \tag{4.18}$$

Equation (4.18) means that as time progresses in increments of t$_d$, the derivative of difference $\dot{X}(t+t_d)-\dot{X}(t)$ is growing exponentially in multiples of BK for $|eig(BK)|>1$. Hence, the system is unstable.

Proof 4-2: Consider a scenario where a hacker injects a TDS attack for a period of time. In order to show that TDS attacks can destabilize the systems, the following proof is used for the hybrid system. Before commencing the proof, an assumption is made that the system can be approximated by a linear time-invariant (LTI) system, and its optimal controller has the form $u(t)=-Kx(t)$.

When under a TDS attack, the control can be described as:

$$u(t)=\begin{cases}-K\,x(t) & t\le t_a\\ -K\,x(t-\tau) & t_a<t\le t_b\\ -K\,x(t) & t\ge t_b\end{cases} \tag{4.19}$$

where τ is a set of random time delays, t_a is the start time of attack, and t_b is the end time of an attack. It is obvious that the system is stable for all $t\le t_a$ and maybe stable for $t\ge t_b$ by the definition of the optimal controller. However, for $t_a<t\le t_b$ it is not obvious that the system would be stable.

Theorem 4-2: Without loss of generality, we suppose $t_b=\infty$. Then we consider the system described in (4.1) with an attack described by (4.19). The system under attack is not stable if the hybrid dynamic model of system has at least one positive eigenvalue or at least one pole in the Right Half Plane (RHP).

Proof:

By applying (4.19) to (4.1) for $t < t_a$, we obtain:

$$\dot{x}(t) = Ax(t) - BKx(t) \tag{4.20}$$

where its characteristic equation is:

$$sI - (A - BK) = 0 \tag{4.21}$$

Solving (4.21) for "s" provides the eigenvalues of the system before an attack.

For $t > t_a$, the system is described by:

$$\dot{X}(t) = AX(t) - BKX(t-\tau) \tag{4.22}$$

Taking the Laplace transform from the above equation, we obtain

$$sX(s) = AX(s) - BKe^{-s\tau}X(s) \tag{4.23}$$

Let $X(t) = e^{st}$ be a proposed solution of (4.22), followed by

$$se^{st}I = Ae^{st} - BKe^{-s\tau}e^{st}\,. \tag{4.24}$$

Here, "s" must satisfy the characteristic equation of the delay system (4.22), i.e.

$$sI-(A-BKe^{-s\tau})=0\,. \tag{4.25}$$

In order to keep the system in the same stable situation as before the attack, the new eigenvalues should be at the same place as the eigenvalues right before the attack. So from (4.21) and (4.25), we obtain

$$BK(-I+e^{-s\tau}I)=0 \Rightarrow e^{-s\tau}I=I\,. \tag{4.26}$$

Equation (4.26) is satisfied if and only if $\tau = 0$. Then, we can conclude for $\tau > 0$, and the system (4.9) will be disturbed for those subspaces (time delays), where for larger time delays, the system will be unstable.

4.4.2 TDS Attack on Load Frequency Control in Smart Grid

In this section, the focus is on the impact of introducing time delays in the SL or in the AGC signal--the only automatic closed loop between the IT and the power system on a control area. When a hacker chooses to introduce delays in a control system, they are performing a Time-Delay-Switch attack (TDS). The research in this dissertation will show how TDS attacks can make any control system, in particular, a power control system, unstable. Therefore, future smart grids will use advanced two-way communication and artificial intelligence technologies to provide better situational awareness of power grid states, keeping smart grids reliable and safe from FDI, DOS or TDS attacks. While these technologies will facilitate the aggregation and communication of both system-wide information and local measurement, they will also have their own cyber security challenges.

It is reasonable to model a power system under a TDS attack as a hybrid system, by formulating TDS attacks as a switch action "Off/Delay-by-$t_{d,}$" where *td* is a random delay time, of sensed system states or control signals of a power system. A TDS attack on the power Load Frequency Control (LFC) system is used as an example. Consider a two-area power system with an automatic gain control under attack in Figure 4.4 [13]. The LFC sends a control signal and is updated through communication channels from/to the turbine and from the telemeter's measurements for RTUs. The communication channels are either wireless networks or wired.

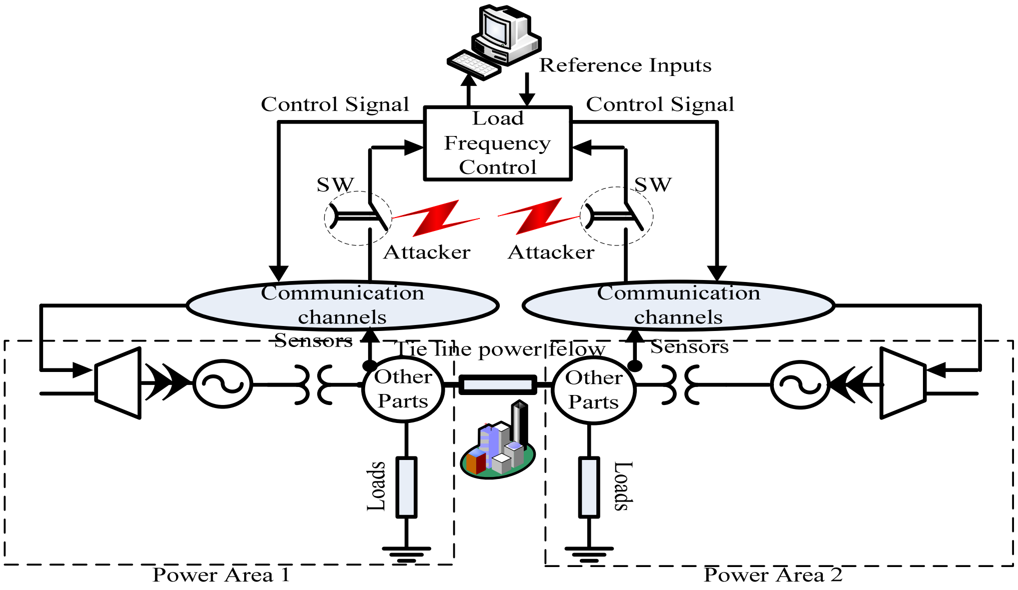


Figure 4.4: Two-area Power System with LFC under a TDS Attack

Attacks can be launched by jamming the communication channels (i.e., DOS attack), by distorting feedback signals (e.g., FDI attack), or by injecting delays (i.e., TDS attack) into the data from telemeter measurements. LFC controllers are usually designed as an optimal feedback controller. However, for the LFC controller to operate optimally, it requires real-time power states to be telemetered with negligible delays to the controllers.

Hence, sensors, communication protocols, and channels must be reliable and fast enough to guarantee optimal operation. Now, if a hacker introduces delays in the telemetered control signals or the measured states, then the LFC system will deviate from optimality, and in most cases, break down.

Model of Load Frequency Control under TDS Attack

Consider a two-area power plant with the automatic gain control under attack in Figure 4.4. The load frequency controller sends control signals to the plant and gets state feedback through the communication channels from the turbines and measurements for Remote Terminal Units (RTUs). The communication channels are wireless networks. Attacks can be launched by jamming the communication channels (i.e., DOS attack [12]), by distorting feedback signals (e.g., FDI attack [76]), or by injecting delays (i.e., TDS attack [77]) into data coming from telemeter measurements.

The LFC is usually designed as an optimal feedback controller, but in order for it to operate optimally, it requires power state estimation to be telemetered in real time. If a hacker introduces significant time delays in the telemetered control signals or measured states, the LFC will deviate from its optimality, and in most cases, the system will break down. A LFC power system was modeled as being under a TDS attack as a hybrid system in a switch action "Off/Delay-by-τ," where τ is some delay time of the sensed system state or the control signals.

A portion of the LFC multi-area interlock power system is shown, as described in [78]. More details can be found in [13]. The LFC dynamic model for the i^{th} area is given by

$$\begin{cases} \dot{x}^i(t) = A_{ii}x^i(t) + B_i u^i(t) + h(x^j(t), \Delta P_l^i) \\ x^i(0) = x_0^i \end{cases} \tag{4.27}$$

where $x \in R^5$ and $u \in R^5$are the state and the control vectors, respectively. The model of the i^{th} area is influenced by the j^{th} power area. Matrices $A_{ii}$and B_i are constant matrices with suitable dimensions, and ΔP_l^i is the power deviation of the load. The initial state vector is denoted by x_0^i for the i^{th} power area. Then the state vector is defined as

$$x^i(t) = [\Delta f^i(t) \quad \Delta P_g^i(t) \quad \Delta P_{tu}^i(t) \quad \Delta P_{pf}^i(t) \quad \Lambda^i(t)]^T \tag{4.28}$$

where Δf^i, ΔP_g^i, ΔP_{tu}^i, ΔP_{pf}^i and Λ^i are frequency deviation, power deviation of the generator, position value of the turbine, tie-line power flow and control error on the i^{th} power area, respectively [19]. The control error of the i^{th} power area is expressed as

$$\Lambda^i(t) = \int_0^t \beta_i \Delta f^i(s) ds \tag{4.29}$$

where β_i denotes the frequency bias factor.

In the dynamic model of the LFC, A_{ii}, B_i, and $h(x^j(t), \Delta P_l^i)$ are represented as

$$A_{ii} = \begin{bmatrix} -\dfrac{\mu_i}{J_i} & \dfrac{1}{J_i} & 0 & -\dfrac{1}{J_i} & 0 \\ 0 & -\dfrac{1}{T_{tu\,i}} & \dfrac{1}{T_{tu\,i}} & 0 & 0 \\ -\dfrac{1}{\omega_i T_{g\,i}} & 0 & -\dfrac{1}{T_{g\,i}} & 0 & 0 \\ \sum\limits_{\substack{i \neq j \\ j=1}}^{N} 2\pi T_{ij} & 0 & 0 & 0 & 0 \\ \beta_i & 0 & 0 & 0 & 1 \end{bmatrix} \tag{4.30}$$

$$B_i = \begin{bmatrix} 0 & 0 & \frac{1}{T_{g\,i}} & 0 & 0 \end{bmatrix}^T \tag{4-31}$$

$$h(x^j(t), \Delta P_l^i) = \sum_{\substack{i \neq j \\ j=1}}^{N} A_{ij} x^j(t) + D_i \Delta P_l^i \tag{4-32}$$

where N is the total number of power areas, J_i, ω_i, μ_i, $T_{g\,i}$ and $T_{tu\,i}$ are the generator moment of inertia, the speed-droop coefficient, generator damping coefficient, the governor time constant, the turbine time constant in the i^{th} power area and T_{ij} is the stiffness constant between the i^{th} and the j^{th} power areas, respectively. Also we have

$$A_{ij} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ -2\pi T_{ij} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{4.33}$$

and,

$$D_i = \begin{bmatrix} -\frac{1}{J_i} & 0 & 0 & 0 & 0 \end{bmatrix}^T \tag{4.34}$$

Equation (4.35) gives the extension of the dynamic model (4.27) to the multi-area power system with the attack model using Equations (4.30), (4.31), (4.32), (4.33) and (4.34).

$$\begin{cases} \dot{X}(t) = AX(t) + BU(t) + D\Delta P_l \\ X(0) = X_0 \end{cases} \tag{4.35}$$

where

$$X(t) = \left[x^1(t)\ x^2(t)\ \ldots x^N(t)\right]^T \tag{4.36}$$

$$A = \begin{bmatrix} A_{11} & A_{12} & A_{13} & \cdots & A_{1N} \\ A_{21} & A_{22} & A_{23} & \cdots & A_{2N} \\ A_{31} & A_{32} & A_{33} & \cdots & A_{3N} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ A_{N1} & A_{N2} & A_{N3} & \cdots & A_{NN} \end{bmatrix} \tag{4.37a}$$

$$B = diag\{\left[B_1^T \quad B_2^T \quad B_3^T \quad \cdots \quad B_N^T\right]^T\} \tag{4.37b}$$

$$D = diag\{\left[D_1^T \quad D_2^T \quad D_3^T \quad \cdots \quad D_N^T\right]^T\} \tag{4.37c}$$

where *B* and *D* are *5N×5N* matrices.

The optimal feedback controller is given by

$$U = -KX \tag{4.38}$$

where optimal gain *K* is a *5N×N* matrix, the control signal and state signal are 5N×5N matrixes.

The design of the optimal controller for the LFC system in the normal operation (i.e., with no attack) involves minimizing a cost function described as

$$J = \frac{1}{2}\int_0^{t_f} \{X^T(t)QX(t) + U^T(t)RU(t)\}dt \tag{4.39}$$

where the matrix $Q \in \Re^{5N\times 5N}$ is positive semi-definite and $R \in \Re^{5N\times 5N}$ is a positive definite. Then, the optimal control problem is to obtain an optimal control signal $U(t)$ that minimizes the performance index (4.39), which is subject to the dynamic of the system with no time-delay in its states.

The system with the optimal controller is described by the following equation:

$$\begin{cases} \dot{X}(t) = (A - BK)X(t) + D\Delta P_l \\ X(0) = X_0 \end{cases} \tag{4.40}$$

With the time-delay attack, the control signal will be modified by:

$$U = -K\hat{X} \tag{4.41}$$

and the new state after the attack can be modeled by:

$$\begin{bmatrix} \hat{x}_1 \\ \hat{x}_2 \\ \vdots \\ \hat{x}_N \end{bmatrix} = \begin{bmatrix} x_1(t - t_{d1}) \\ x_2(t - t_{d2}) \\ \vdots \\ x_N(t - t_{dN}) \end{bmatrix} \tag{4.42}$$

In (4.42), $t_{d1}, t_{d2}, ...$ and t_{dN} can be different/random time delays and are positive values. When $t_{d1}, t_{d2}, ..., t_{dN}$ are all zero, the system is in normal operation. A hacker can gain access to the communication link and inject a delay attack on the line to direct the system to abnormal operations.

Remark 1: In this paper, ΔP_l is considered constant. This is a reasonable case, because the stability of the power system will not be influenced by an appropriate period following a step load change [13].

This section analyzes TDS attack effects; in the upcoming chapters, the robust controller is proposed in the face of this attack. At this point, an optimal controller in normal operation (with no attack) is designed, and then the system is attacked with an on/off switch SW and the behavior of the system experiencing a TDS attack is analyzed.

The optimal control problem is to obtain optimal control $U^*(t)$, which minimizes the performance index (4.39), and is subject to the dynamic system described in (4.35) with no time-delay in state.

Simulation studies were conducted to evaluate the effects of TDS attacks on the dynamics of the system. The optimal control law can be found for the system in its normal operation. For simplicity of discussion, $N = 2$ is set, which is defined as a two-area power system. Table 4.3 shows the parameter values used in this process. Since simulation on a certain duration tracks a step load change, we also set ΔP_l^1 and $\Delta P_l^2 = 0$.

Then, the instability of the system can be studied by finding the eigenvalues of the system before and after the attack. Roots (zeros) of (4.42) determine the stability of the system. For simulation simplicity, the fifth order Pade approximation [79] was used to approximate $e^{-s\tau}$.

Table 4.3: Parameter Values for Two-Area Power System

Parameter	Value	Parameter	Value
J_1	10	ω_1	0.05
μ_1	1.5	$T_{g\,1}$	$0.12s$
$T_{tu\,1}$	$0.2s$	$T_{tu\,2}$	$0.45s$
T_{12}	$0.198 pu/rad$	T_{21}	$0.198 pu/rad$
J_2	12	ω_2	0.05
μ_2	1	$T_{g\,2}$	$0.18s$
R	$100I$	Q_f	0
Q	$100I$	t_f	∞
β_1	21.5	β_2	21

$$sI-(A-BK\frac{30240-15120s\tau+3360s^{2}\tau^{2}-420s^{3}\tau^{3}+30s^{4}\tau^{4}-s^{5}\tau^{5}}{30240+15120s\tau+3360s^{2}\tau^{2}+420s^{3}\tau^{3}+30s^{4}\tau^{4}+s^{5}\tau^{5}})=0 \tag{4.45}$$

Figure 4.5 shows the results of the system's eigenvalues before and after different TDS attacks. As τ tends to be larger than zero, the eigenvalues move from the LHP to the RHP. It clearly shows that the system becomes unstable for time delays larger than $\tau = 0.3\sec$. In Figure 4.5, the crosses, points, circles and stars denote the eigenvalues of the system with no attack and attacks with the time delays $\tau = 0.1\sec$, $\tau = 0.4\sec$ and $\tau = 0.6\sec$, respectfully. Figure 4.6 shows the maximum eigenvalue track based on different time-delay values. Figures 4.5 and 4.6 clearly show that the system becomes unstable when the delay value increases.

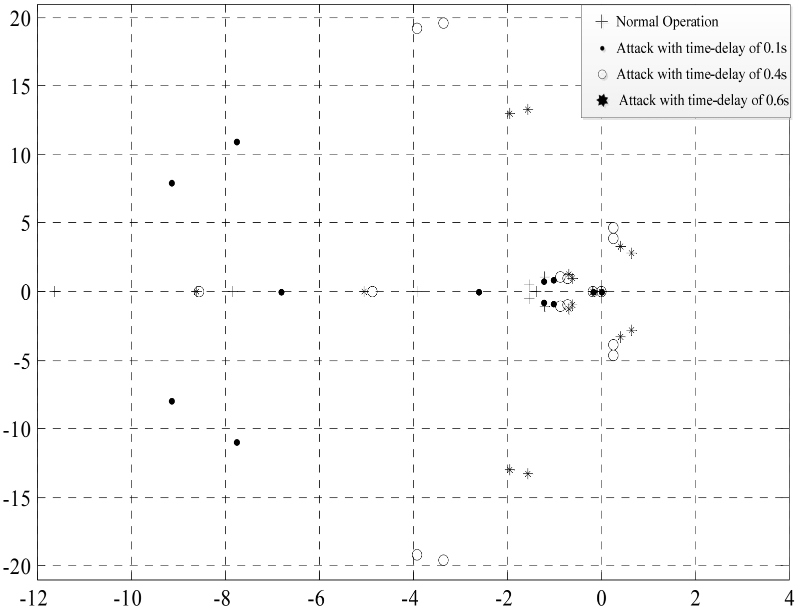


Figure 4.5: Eigenvalues of the System for Normal Operation and Attack by Different Time Delays

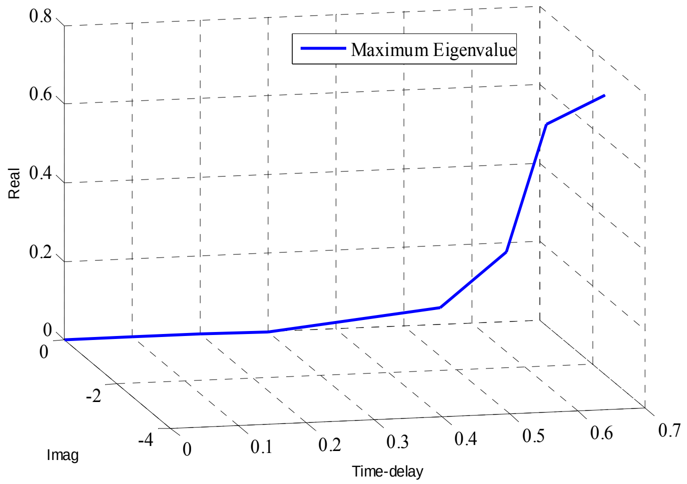


Figure 4.6: Maximum Eigenvalues for Different Time-delay Attacks

The total simulation time is 40 sec, and the hacker has access to switch SW in Figure 4.4 and starts the TDS attack with $\tau = [t_{d1} \quad t_{d2} \quad \cdots \quad t_{dn}]^T$. In Figure 4.7, the graphs (a), (b), (c) and (d) show the simulation results of the frequency deviation, the power deviation of the generator, the value position of the turbine and the tie-line power flow, respectively.

Case 1:

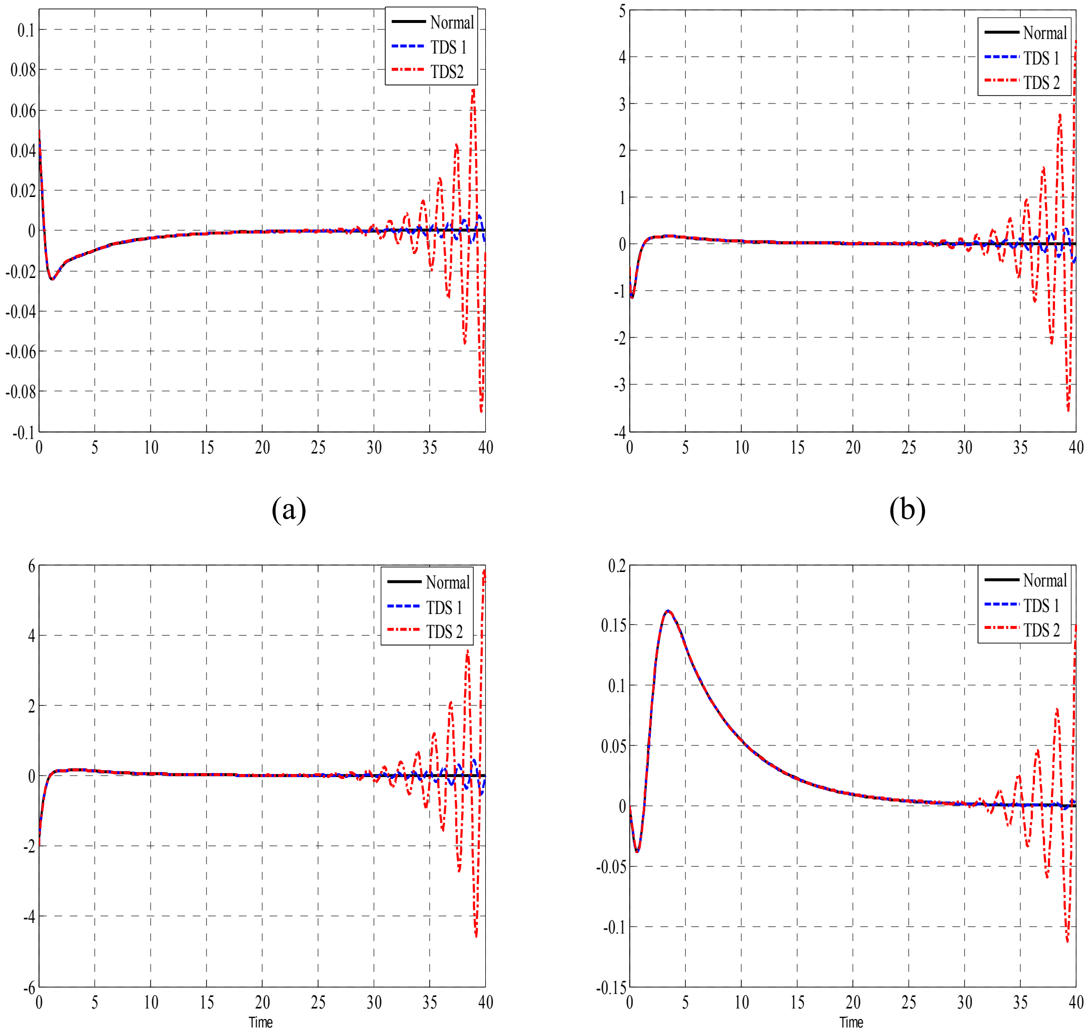
The hacker attacks all of the states at $t_a = 15s$, with the same time-delay pattern. In Figure 4.7 (a), (b), (c) and (d), the black lines show normal operation. TDS attacks 1 and 2 denote time-delay attacks with t_{d1}=0.4*,* t_{d2}=0.4*,…*, t_{d2}=0.4 seconds and with t_{d1}=0.6*,* t_{d2}=0.6*,* …, t_{d2}=0.6 seconds, respectively. It is clear that the system moves into an unstable region as it is attacked.

Case 2:

The attack starts at time $t_a = 5s$, and the hacker attacks only one state of the system. In Figure 4.8, in graphs (a), (b), (c) and (d), TDS attacks 1 and 2 denote attacks with a time delay of $t_{d1} = 0.6$ and $t_{d1} = 1$, respectively (this means that there is no time-delay attack for other states). In the case of a TDS attack at $t_{d1} = 0.3$, the system is disturbed but is still stable.

The results of Case 1 and Case 2 conclude that the hacker can cause system instability just by attacking one state of the system.

This section considers TDS attacks, a new type of attack on the cyber layer of smart grids that can sabotage the dynamic performance of power systems. The LFC power system experiencing a TDS attack is modeled as hybrid systems, and the TDS attacks are formulated as switch action "Off/Delay-by-τ" sensing channels or control inputs. Then, the destabilizing action of TDS attacks on power systems was studied using methods from hybrid system theories. A two-area LFC LTI model was simulated to evaluate the effects of TDS attacks. The results show that TDS attacks affect the dynamic performance of the LFC system, and in many cases, could destroy the system's stability, which can be launched at any time during the operation of the power system. In the following chapters, the focus is on attempts to make controllers and communication protocols robust under this type of attack.



(a)

(b)

(c)

(d)

Figure 4.7: Case 1, (a) Frequency Deviation, Δf^{K} , (b) Power Deviation of Generator, ΔP_{g}^{K} , (c) Value Position of the Turbine, ΔP_{tu}^{K} , (d) Tie-line Power Flow, ΔP_{pf}^{1}

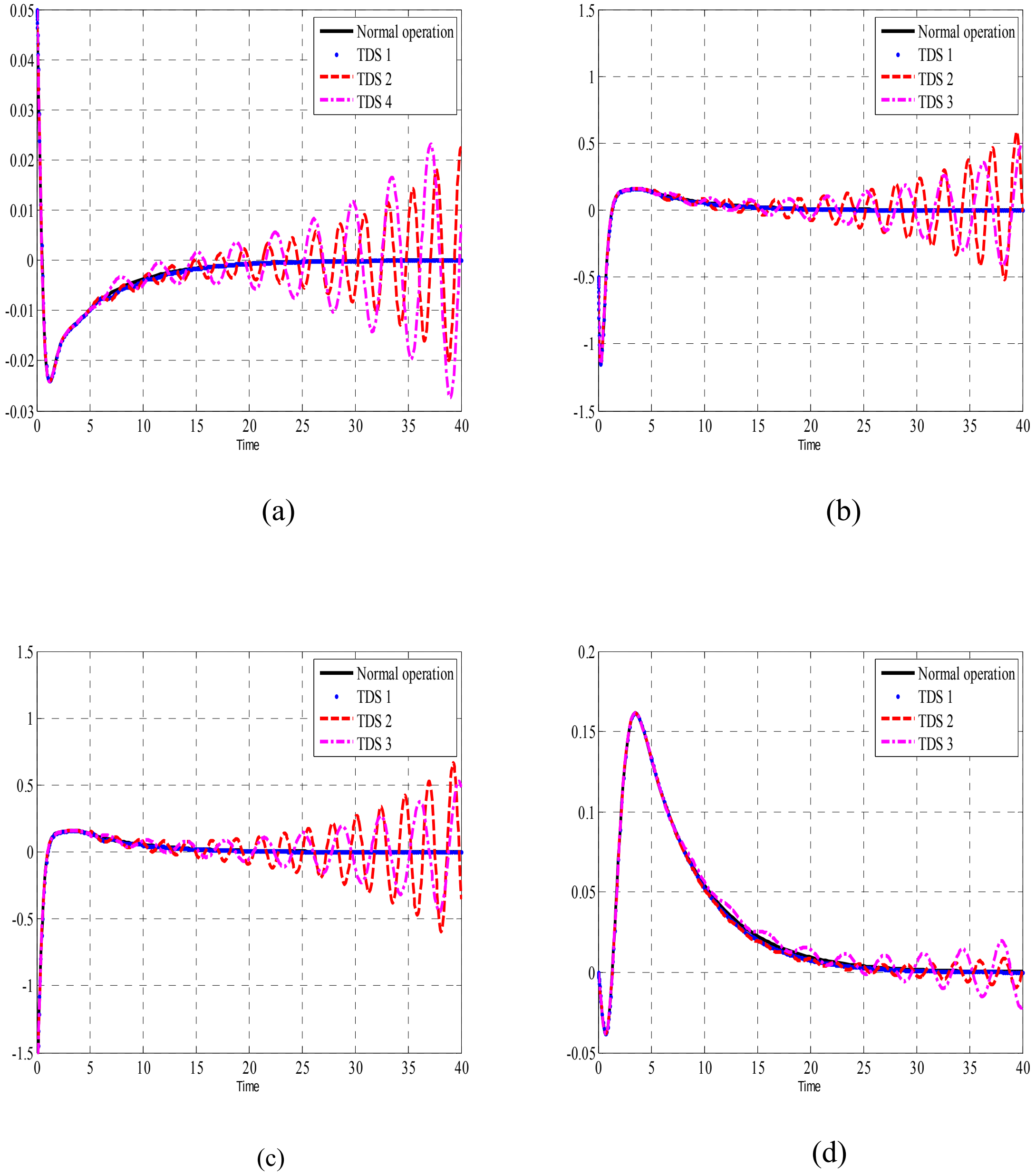


Figure 4.8: Case 2, (a) Frequency Deviation Δf^{K}, (b) Power Deviation of Generator ΔP_{g}^{K}, (c) Value Position of the Turbine ΔP_{tu}^{K}, (d) Tie-line Power Flow ΔP_{pf}^{1}

4.4.3. TDS Attack on Peace Maker, an Application in Biomedical Systems

There are many analyses and design techniques developed for LTI systems [80, 81]. However, for a nonlinear system that could possibly be time-varying, one needs a nonlinear control methodology. A major part of a nonlinear control theory studies how to extend the well-known linear methods to nonlinear systems.

One of the most complex but robust nonlinear systems is the human heart. An electrocardiogram (ECG) records potential differences between two electrodes located on the skin at predetermined positions on the chest to measure the electrical activities in cardiac tissue. A solitary cycle of an ECG consists of the activities of relaxation and contraction of the heart (called “heart pumping actions”). One can identify an ECG signal by its P, Q, R, S, and T peaks, PR and ST segments, PR and QT intervals, and QRX complex. Characteristic information obtained from an ECG can be used to assess cardiac health and identify potential heart problems. For example, important information extracted from an ECG recording is the time between successive R-peaks, which is an RR-interval. The changeability of the series of RR-intervals, known as heart rate variability (HRV), is being used to measure heart functions, such as: identifying a patient’s risk for cardiovascular failure [82], as “an indicator for mortality following myocardial infarction” [83], and as a measure of the contacts between different control mechanisms of physiology, like respiratory sinus arrhythmia.

The development of mathematical models of the heartbeat (ECG) with appropriate PQRST peaks, QRX complex, (PR, ST) segments, (PR, QT) intervals and HRV spectra has been and continues to be the subject of wide investigations with varying degrees of successes. A successful ECG model becomes a valuable tool for analyzing the various effects of physiological conditions of the outlines of the ECG and for the assessment of diagnostic ECG signal processing devices.

The type of ECG signal is the result of the propagation of electrical activities in the myocardium, and the HRV is the result of physiological and neurological controls. In 1972, Zeeman presented a set of nonlinear dynamical equations for heartbeat modeling [84, 85] based on the Van der Pol-Lienard equation. These models are based on pacemaking generated by the Sino-Atrial (SA) node, which is the dominant pacemaker, compared with the slower one produced by the Atrio-Ventricular (AV) junction. Furthermore, these models did not take into consideration the sympathetic and parasympathetic modulations responsible for HRV generation [86].

In [87], the Zeeman's 2nd-order ordinary differential equation (ODE) of the heartbeat model was modified by incorporating a switch (on/off) control variable demonstrating the pacemaker's mechanism of the contraction-relaxation for the heart. Subsequently, Jafarnia-Dabanloo et al. in 2007 [88] modified the 3rd-order nonlinear Zeeman model by adding control parameters that affect the frequency of the oscillation to control the HRV by using a neural network to produce the ECG signal.

Yet another well-known approach to model the cardiac rhythms is based on the Van der Pol oscillators. In contrast to the Zeeman models, the coupled Van der Pol oscillator models at AV node have a more active role in pace making [89]. This model allows us to consider the effect of the coupling between the SA and the AV pacemakers in normal electrophysiological dynamics.

In this section, the stability of the heartbeat model that was developed by Zeeman [84] is examined. This model captures, at least qualitatively, three essential characteristics of cardiac dynamics: (i) a stable equilibrium, (ii) a threshold for triggering the action potential, and (iii) a return to equilibrium. The model consists of a 2nd-order nonlinear ODE of the Liénard-type representing the heartbeat dynamics [90].

In this era of pervasive communication technology, distant monitoring and follow-up of patients implanted with pacemakers (PMs) and implantable cardioverter-defibrillators (ICDs) is becoming very common. Most companies fit PMs and ICDs with wireless capability that communicates information to home transmitters, then to physicians. These systems are widely used in the U.S. and are being introduced in Europe. Only recently, a tiny wireless pacemaker was launched in Europe by Nanostim [91]. The security of current and future biomedical devices is going to draw a major concern of public health in the future. Recently, the U.S. Department of Homeland Security underscored some threats affecting almost 300 medical devices [92, 93]. The latest technology in wireless pacemakers [91] makes them vulnerable to hackers that can gain access to and sabotage such medical devices. Attacks such as false data injection, denial of service and other types of attacks can make lives that depend on wireless enabled devices such as pacemakers difficult and dangerous. Therefore, it is reasonable to model the heartbeat pacemaker system under time-delay-switch (TDS) attacks and provide a possible solution. The TDS attack is a switched action "Off/Delay-by-τ," where τ specifies random delay times of the sensed system states or control signals of a system. The TDS attack on the heartbeat control system is modeled (Figure 4.9) as a hybrid system. Then, a solution will be provided using an emotional learning control to temper the effects of such an attack on the control of heartbeats in Chapter 8.

The first section of the paper introduces a common nonlinear model of heartbeat, i.e., Zeeman models. The stability of the 2nd-order heartbeat model using the indirect method is also discussed.

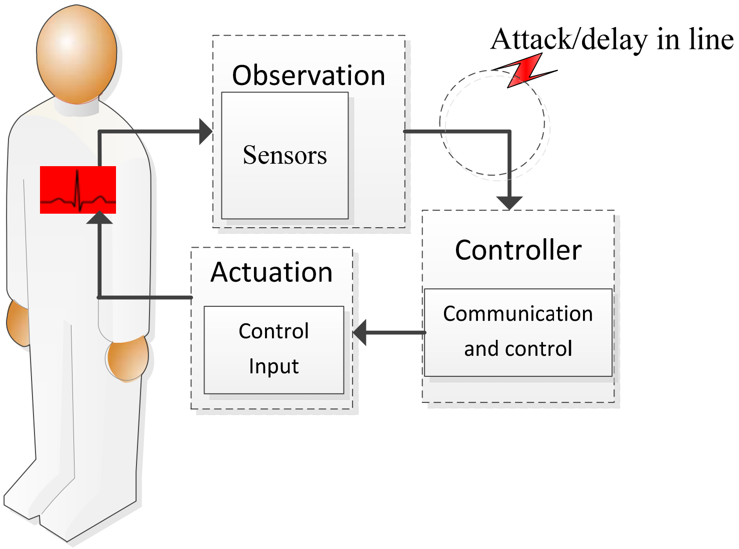


Figure 4.9: Heartbeat Control Model with Possible Control Attack

Nonlinear Heart Model under TDS Attack

Based on [84], the second-order nonlinear heartbeat model is provided by:

$$\begin{bmatrix} \dot{X}_1(t) \\ \dot{X}_2(t) \end{bmatrix} = \begin{bmatrix} -\frac{1}{\varepsilon}\{X_1^3(t) - TX_1(t) + X_2(t)\} \\ X_1(t) - x_d \end{bmatrix}, \qquad T > 0 \tag{4.43}$$

where the states $X_1(t)$ and $X_2(t)$ represent the length of a muscle fiber and a state related to electrochemical activities, x_d indicates a typical muscle fiber length, ε is a small positive constant that plays a role in fast eigenvalues of the system, and finally, T shows the tension in the muscle fiber. Parameter values are shown in Table 4.4.

Table 4.4: Parameters Value of Model (4.43)

Parameter	x_d	T	ε
value	1.024	1	0.2

Values in Table 4.4 were checked by analyzing the equilibrium point stability using the well-known Lyapunov indirect stability theorem [94]. For this purpose, let A be the Jacobian matrix of Equation 1 at the origin.

$$A = \left.\begin{bmatrix} \dfrac{\partial \dot{X}_1}{\partial X_1} & \dfrac{\partial \dot{X}_1}{\partial X_2} \\ \dfrac{\partial \dot{X}_2}{\partial X_1} & \dfrac{\partial \dot{X}_2}{\partial X_2} \end{bmatrix}\right|_{X=0} = \left.\begin{bmatrix} -\dfrac{1}{\varepsilon}(3X_1^2 - T) & -\dfrac{1}{\varepsilon} \\ 1 & 0 \end{bmatrix}\right|_{X=0} = \begin{bmatrix} \dfrac{T}{\varepsilon} & -\dfrac{1}{\varepsilon} \\ 1 & 0 \end{bmatrix} \qquad (4.44)$$

For the parameter $x_d = 0$, the eigenvalues of A have the values of 3.618 and 1.382. Both are positive and show that the origin is not stable.

The condition for the real part of the eigenvalue to be negative is $3X_1^2 - T > 0$. Hence, the system can be stable if $X_1 \geq \sqrt{\dfrac{T}{3}}$, and $X_1 \leq -\sqrt{\dfrac{T}{3}}$. These conditions can be satisfied if the value of x_d is 1.024. For $x_d = 1.024$, the stable equilibrium point is at $(1.024, -0.0497)$ in the state space. In this case, all of the trajectories, irrespective of their primary conditions, move toward the diastolic equilibrium point.

The system stays at the stable equilibrium point endlessly, until the equilibrium point is stable, except there is an exterior excitation that forces the system to move to a new equilibrium point. Based on this new stable system, a control input is added to the system (4.43), as shown below:

$$\begin{bmatrix} \dot{X}_1(t) \\ \dot{X}_2(t) \end{bmatrix} = \begin{bmatrix} -\frac{1}{\varepsilon}\{X_1^3(t) - TX_1(t) + X_2(t)\} \\ (X_1(t) - x_d) + (x_d - x_s)u(t) \end{bmatrix} \tag{4.45}$$

when the heart is in systolic state, $x_s$is an additional parameter representing a typical fiber length, and $u(t)$ shows the cardiac pacemaker control mechanism that leads the heart into diastolic and systolic states. The feedback controller can be found in the form of:

$$u(t) = -K\hat{X} \tag{4.46}$$

and the new state after the attack (or random delay of feedback line) can be modeled by:

$$\hat{X} = X(t - \tau) \tag{4.47}$$

In Equation (4.47), τ is the time delay and a positive integer. When the time delay is zero, the system works in its normal operation. The hacker can access the communication line and delay the communication line. This model is true also for the small value of delay, which can occur in the nature of the wireless sensor.

Stability Simulation and Results

The 2nd order heartbeat model to track the ECG signal using the PID controller was simulated. Then, an external TDS attack was applied to the model from a start time t_S until a final time t_F to show the performance of a classical PID controller.

Figure 4.10 shows the ECG reference tracking $X_2(t)$ using the PID under a TDS attack. The dashed line shows the PID controller tracking an ECG signal under a TDS attack, and the solid line shows the referenced ECG signal [95].

The TDS attack or feedback delay was applied to the model from $t_S = 0.4\sec$ until $t_s = 0.45\sec$ with a time delay of $\tau = 0.01\, s$. For the purpose of visual comparison, the attack period and the amount of attacks selected were a smaller amount because for a larger period and time-delay value, the classical PI controller goes outside the visual boundaries.

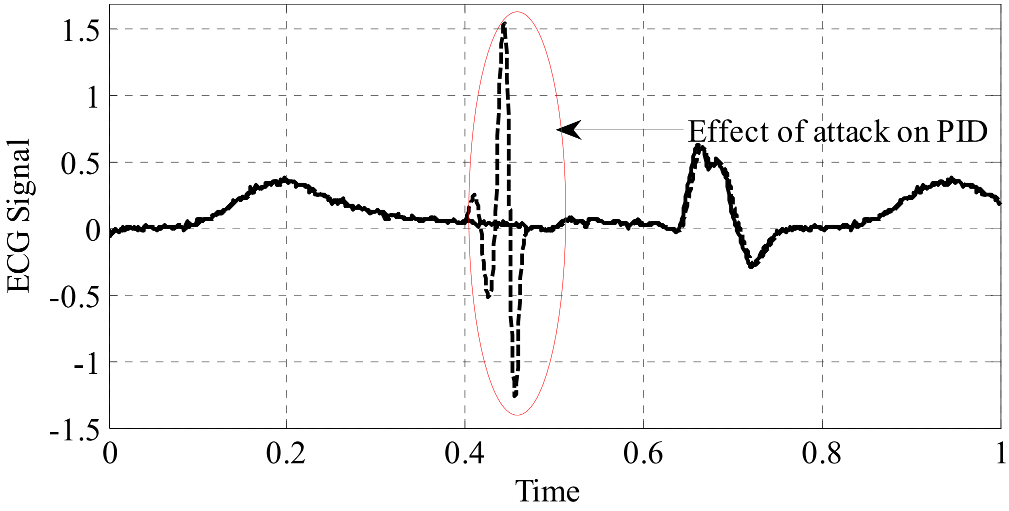


Figure 4.10: Effect of TDS Attack on PID Controller of Heartbeat Model

Based on the above simulation, it is obvious that TDS attacks can disturb and disable any control system.

CHAPTER 5

TIME-DELAY SWITCH ATTACK DETECTION

5.1 Introduction

This chapter will demonstrate how to detect a TDS attack on Networked Control Systems, and particularly in networked power control systems. Time delays injected by a hacker in a control system, in general, destabilizes the system or causes inefficiency. This is a new attack in the context of control systems (e.g., load frequency control (LFC)) on NCSs [93], which is called a "TDS attack." To avoid the damaging effects of TDS attacks, systems and controllers must be redesigned in such a way that it can detect and correct variable time delays.

A varying amount of time delays exist in almost any dynamic system in the sensing and control loops. Let us consider power systems for this section. The traditional controllers of power systems were designed based on the availabe information ignoring the existance of time delays. However, power grids constantly enhance new telecommunication technologies for monitoring, and improving the efficiency, reliability, and sustainability of supply and distribution. For example, the introduction of a Wide Area Measurement System (WAMS) provides synchronized, near real-time measurements in Phase Measurement Units (PMUs). WAMS, which are used for stability analysis of power systems, can also be used for designing efficient controllers. Nevertheless, time delays are present in PMU measurements as a result of natural transmission lines [96].

Several studies considered control systems with time delays [76, 97, 98]. The impact of time delay on the power system's stabilizing controllers was discussed in [99-103]. In

[104], the authors studied the effects of delays on the small signal stability of control systems. In [99] and [100], methods are proposed to eliminate oscillations that result from time-delayed feedback control. In [105], the authors presented a wide-area control system for damping generator oscillations. In [96], a controller was proposed using phasor measurements with delays, in which the small-signal stability of the power system was considered. A feedback controller for power systems with delayed states was proposed in [106]. The controller deals with the combined effects of the instantaneous as well as the delayed states using the quadratic Lyapunov function for systems with delays. Additional studies on control systems with delay can be found in [21, 78, 97, 107, 108] and the references therein. However, most of these   studies considered either the construction of controllers that are robust to time delays or controllers that use offline estimates of time delays. Furthermore, few studies [15, 109] considered the control of systems with time delays introduced by hackers.,It is assumed that there are no control methods that perform an online estimation of dynamic time delays and real-time control of power systems.

In this section, a simple yet effective method to address a TDS attack on the observed states of a controlled system is described. This method utilizes a time delay estimator, a communication protocol to alert for a time-delay switch attack, a buffer to store the history of controller commands, an optimal controller to stabilize or track a reference signal, and a local to the plant emergency controller to stabilize the plant if long time delays are detected. For now, only the LTI systems with state feedback will be examined.

5.2 TDS Attack Detection and Real-Time Monitoring Method

The proposed method is shown in Figure 5.1. Its basic elements are a plant model, a time-delay detector, a controller, and a computer system. The controller can either be a PID controller or an optimal feedback controller. The time-delay detector estimates the time delay in the communication channel from telemetered data. If the delay is larger than an acceptable time delay, it sends alarm signals to the controller and the emergency controller. The results of TDS detectors are used to activate the emergency controller to stabilize the system in case of an attack on the communication lines of the distant controller. If an alarm signal is received by the emergency controller, it will begin to stabilize the plant to a desired state, while the distant controller stops operating until the delay is corrected.

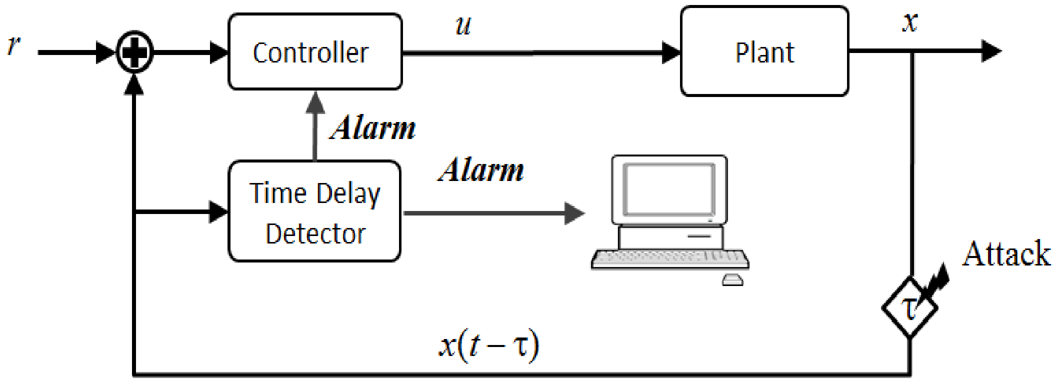


Figure 5.1: Block Diagram of Proposed Technique

Suppose the system used is the linear time invariant (LTI) or can be approximated in a region of interest by a LTI system, then it can be described by

$$\dot{x}(t) = Ax(t) + Bu(t)\,, \tag{5.1}$$

where x and u are state and control vectors, respectively. Matrices A and B are constant matrices with suitable dimensions.

Then, its solution is given by:

$$x(t) = e^{At}x_0 + \int_0^t e^{A(t-s)}Bu(s)ds\,, \tag{5.2}$$

With time delay τ, due to a time-delay switch attack or any natural delay, the solution becomes:

$$x(t-\tau) = e^{A(t-\tau)}x_0 + \int_0^{t-\tau} e^{A(t-\tau-s)}Bu(s)ds\,. \tag{5.3}$$

Let us write the solution $x(t)$ at the time t as a function of a time-delayed signal:

$$\begin{aligned} x(t) &= e^{At}x_0 + e^{A\tau}\int_0^{t-\tau} e^{A(t-s)}e^{-A\tau}Bu(s)ds + \int_{t-\tau}^{t} e^{A(t-s)}Bu(s)ds \\ &= e^{At}x_0 + e^{A\tau}\left[x(t-\tau) - e^{A(t-\tau)}x_0\right] + \int_{t-\tau}^{t} e^{A(t-s)}Bu(s)ds \end{aligned}\,, \tag{5.4}$$

In general, the time delay τ is an unknown variable. The estimation error of the time delay is $\varepsilon = \hat{\tau} - \tau$. The predicted state $\hat{x}(t)$ of the system based on the estimate of time delay $\hat{\tau}$ is given by:

$$\hat{x}(t) = e^{At}x_0 + e^{A\hat{\tau}}\left[\hat{x}(t-\hat{\tau}) - e^{A(t-\hat{\tau})}x_0\right] + \int_{t-\hat{\tau}}^{t} e^{A(t-s)}Bu(s)ds \tag{5.5}$$

where $\hat{x}(t-\hat{\tau})$ is the estimate of the delayed state given the estimate of the delay $\hat{\tau}$.

It should be noted that $x(t-\tau)$ is what is actually measured and delivered to the plant model. So, at every instance of time, the values of the variables $\hat{x}(t)$, $\hat{x}(t-\hat{\tau})$, $u(t)$, and

$x(t-\tau)$ are known to the controller. On the other hand, the current state $x(t)$ and the time delay τ are unknown. It is essential that the plant model estimates the state $x(t)$ accurately. Because of the delay an accurate estimation of $x(t)$ requires a good estimate of the delay τ, the next step will show how to estimate the delay τ.

The estimation error in state can be described by $e_m(t) = x(t) - \hat{x}(t)$, and with a delay, it is given by

$$e_m(t;\tau,\hat{\tau}) = x(t-\tau) - \hat{x}(t-\hat{\tau}) \,. \tag{5.6}$$

The idea is to estimate $\hat{\tau}$ over time as fast as possible so as to minimize the error $e_m(t;\tau,\hat{\tau})$. To do so, we select $v = 0.5{e_m}^2$. Using the gradient descent method, we set

$$\frac{d\hat{\tau}}{dt} = -\eta \frac{\partial v}{\partial \hat{\tau}}, \tag{5.7}$$

where η is the learning parameter. With some manipulation, we have:

$$\begin{aligned}
\frac{d\hat{\tau}}{dt} &= -\eta e_m \frac{\partial e_m}{\partial \hat{\tau}} = -\eta e_m \frac{\partial\left[x(t-\tau) - \hat{x}(t-\hat{\tau})\right]}{\partial \hat{\tau}} \\
&= \eta e_m \frac{\partial \hat{x}(t-\hat{\tau})}{\partial \hat{\tau}} = \eta e_m \frac{\partial}{\partial \hat{\tau}}\left[e^{A(t-\hat{\tau})}x_0 + \int_0^{t-\hat{\tau}} e^{A(t-\hat{\tau}-s)} Bu(s)ds \right]. \\
&= \eta e_m \frac{\partial}{\partial \hat{\tau}}\left[\int_0^{t-\hat{\tau}} e^{A(t-\hat{\tau}-s)} Bu(s)ds \right] - \eta e_m A e^{A(t-\hat{\tau})} x_0 \\
&= -\eta e_m \left[Bu(t-\hat{\tau}) - e^{A(t-\hat{\tau})} Bu(0) - A e^{A(t-\hat{\tau})} x_0 \right]
\end{aligned} \tag{5.8}$$

Assuming that $u(0) = 0$, which is reasonable for the initial time, we arrive at:

$$\frac{d\hat{\tau}}{dt} = -\eta \, e_m \, Bu(t-\hat{\tau}) - A e^{A(t-\hat{\tau})} x_0, \qquad 0 \le \hat{\tau} \le t \tag{5.9}$$

Equation (5.9) is used to estimate the time delay τ . This value is sent to both the controller and monitoring center to inform them about the occupancy TDS attack in the system. The alarm strategy is shown in Figure 5.1.

This method was implemented in MATLAB to verify its performance using the LFC of a two-area distributed power system. In the next section, the simulation results are presented and discussed in detail.

5.3 Simulation Result, TDS Attack Detection on Smart Grid Application

This section focuses on the LFC system, where the controller's task is to regulate the state of a networked power system. The description of a multi-interconnect LFC dynamic system can be found in Section 4.4.2. Here, we focus on a two-area power system with the attack model described in the same section (Section 4.2). It should be noted that we used the same parameter values as described in Table 4.3.

The total simulation time is 50 seconds, and the sampling period is 0.01 sec. In order to show accuracy of the proposed TDS attack detector, a negative acknowledgment is not sent to the local controller for the first simulation. The simulation was performed for three different scenarios: (1) single TDS attack on one power area, (2) simultaneous TDS attack on both power areas, and (3) complex varied TDS attack on both power areas.

1. **Single TDS Attack on First Power Area**: For this attack, a hacker attacks the third state of the first power area at 2 sec for a time delay of 3 sec, and the time delay is increased to the value of 4.5 sec at 7 sec. Figure 5.2 shows that the

detector accurately tracked and monitored the TDS attack or any natural delay of the system.

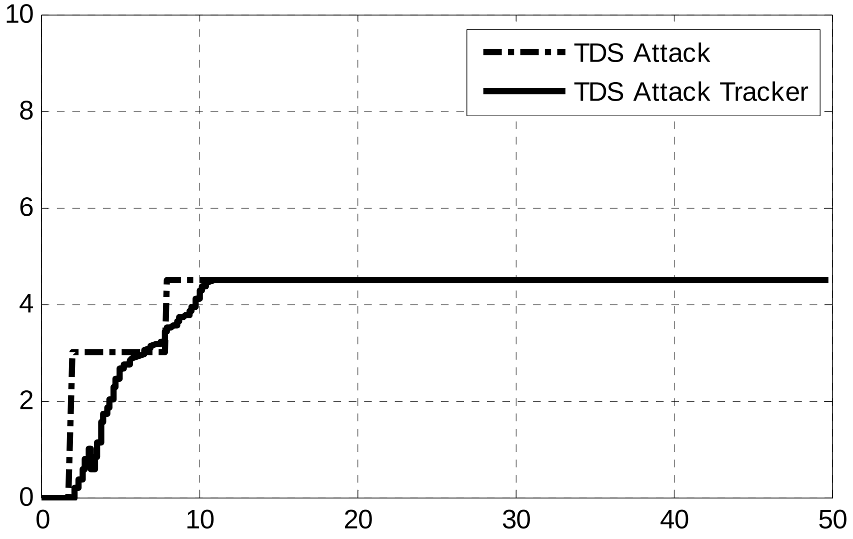


Figure 5.2: TDS Attack Detection and Tracking for Third State of First Power Area

2. **Simultaneous TDS Attack on Both Power Areas**: In this scenario, we attacked the third state of both power areas simultaneously. TDS attacks 1 and 2 were injected into the first and the second power areas, respectfully. TDS attack 1 is applied at 2 sec for a value of 3 sec and at 8 sec to the value of 4.5 sec. TDS attack 2 occurs simultaneously with TDS attack 1 at 1.5 sec and 6 sec. Figure 5.3 shows the results.

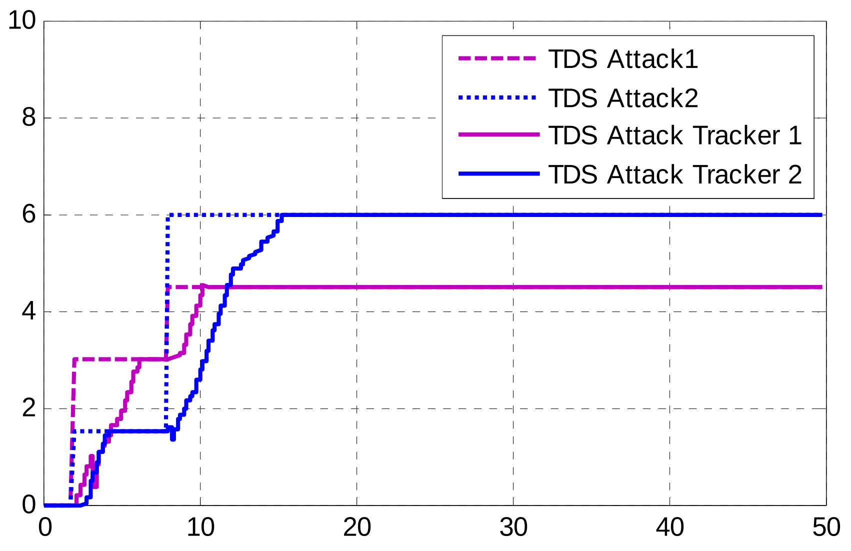


Figure 5.3: TDS Attack Detection and Tracking for Simultaneous TDS Attack on Both Power Areas

3. **Complex, Varied TDS Attack on Both Power Areas**: In the last scenario, a TDS attack was injected at different times with different time-delay values. It is assumed that a hacker injects a TDS attack into the feedback lines of both power areas. In this simulation, an attacker starts a TDS attack on the second power area (the third state) at time of 1 second for $t_{d3} = 5s$, and then increases it to $t_{d3} = 10s$ at 20 sec. Furthermore, a hacker starts to attack the first power area (third state), at 1 second with $t_{d8} = 3s$, and increased it to $t_{d8} = 4.5s$ at 30 seconds. Figures 5.4 and 5.5 show TDS attacks and TDS attack tracking in real time. Figure 5.4 shows a TDS attack on the third state of the first power area, and Figure 5.5 shows an attack at the same state of the second power area.

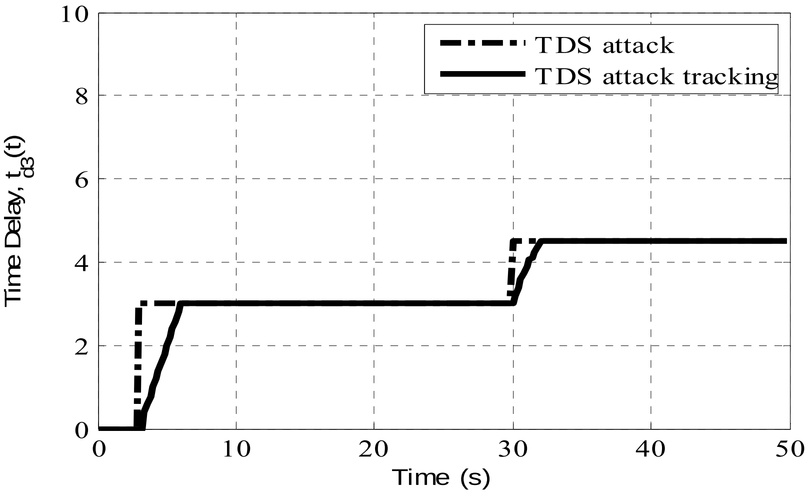


Figure 5.4: TDS Attack Detection and Tracking for the Third State of the First Power Area

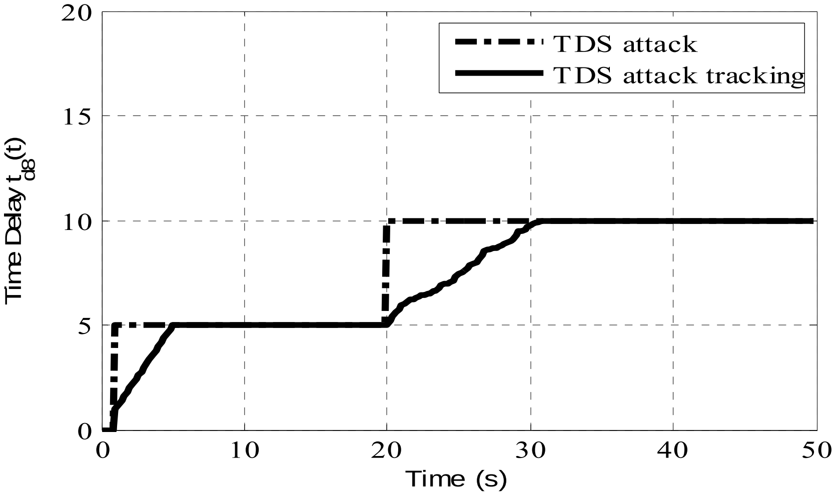


Figure 5.5: TDS Attack Detection and Tracking for the Third State of the Second Power Area

5.4 Conclusion

In summary a simple method for tracking a time-delay switch attack on NCSs was demonstrated. This method relies on a time-delay estimator that estimates and tracks time delays introduced by a hacker. The time-delay detector compares the estimated time delay with the maximum time delay and issues an alarm signal when the estimated time delay is larger than the tolerable one.

CHAPTER 6

OVERCOMING STABILITY ISSUES OF A TIME-DELAY SWITCH ATTACK ON LINEAR NETWORKED CONTROL SYSTEMS

6.1 Introduction

Too much effort has been put into the study of time-delay systems [15, 109, 110]. For example, Tan [15] proposed a neural network time-delay estimator for a class of nonlinear systems with time-varying delays, which must be trained off-line and must work well for periodic reference signals. Li et. al. [109] developed an adaptive control algorithm to guess random time delays in the Networked Control Systems (NCSs).

Li et. al. proposed an algorithm that updates delay estimation using the gradient descent method and discovers plant parameters using an improved recursive least square. The authors asserted that the method is superior to the typical networked predictive control. However, the method is complex for even the simplest linear system. Furthermore, the authors did not show the results for time-delay control compensation, or any time track of variable delays. Yet, another example of time-delay estimation is the method of variable sampling to compensate for the time delay in a networked control system. A Multi-Layer Perceptron (MLP) neural network is used to learn the time delay off-line, as well as to predict its value during the on-line control operation [110]. This method assumes that time delay is constant, so it cannot be applied to the system under varying time delay attacks. All of the control methods developed for the compensation of time delays rely on a controller either robust to a maximum time delay using off-line estimates of time delays, or approximation of time delayed signals. In this paper, a general method is proposed for the control of systems under a TDS attack. This method was developed for continuous, linear, and time-invariant systems. However, the results will be extended to a class of nonlinear systems in the future. The models and control strategies were implemented with MATLAB to demonstrate the performance through simulation.

6.2 Methodology

The proposed method involves the use of a plant model, a time-delay estimator and a PID or an optimal controller to control a LTI system with natural delays or under a TDS attack. The control scheme will detect and track time delays introduced by an attacker and guide the plant to track the reference signal to guarantee the stability of the system. Figure 6.1 shows the diagram of the proposed time delay estimator and controller.

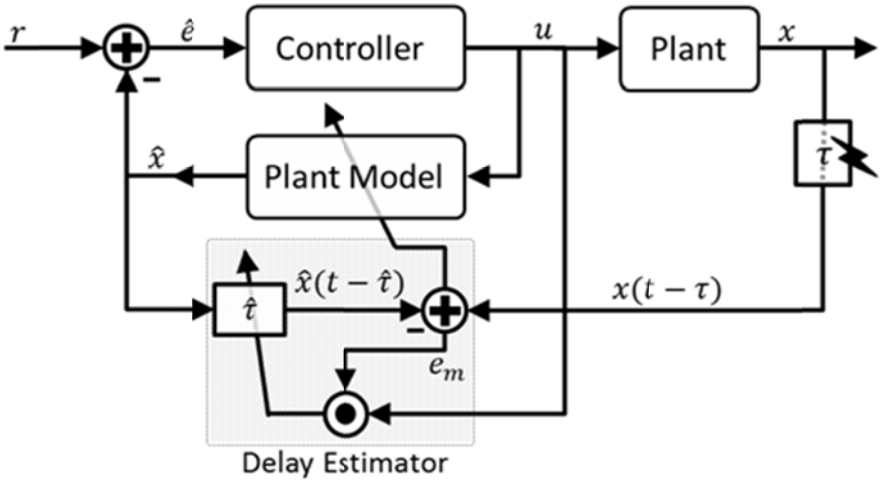


Figure 6.1: Block Diagram of Proposed Control Technique

Suppose the system in system under consideration is given by or can be approximated in a region of interest by the LTI system:

$$\dot{x}(t) = Ax(t) + Bu(t) \tag{6.1}$$

Based on Chapter 5, Equation (6.2) is used to estimate the time delay τ .

$$\frac{d\hat{\tau}}{dt} = -\eta\, e_m\, Bu(t-\hat{\tau}) - Ae^{A(t-\hat{\tau})}x_0, \qquad 0 \le \hat{\tau} \le t \tag{6.2}$$

Equation (27) is used to estimate the time delay τ . However, there are practical issues that need to be considered. Computing machines have finite memory and temporal resolution. Therefore, Equation (27) cannot be implemented without discrete approximation and boundedness assumptions. To guarantee the stability of calculations and limit the memory usage, the following condition must be added, $\tau < \tau_{\max}$. This condition will allow the construction of a finite buffer to store the history of $u(t)$ from t to $t-\tau_{\max}$. Also, this will allow for the prevention of a runaway condition on $\hat{\tau}$. It should be noted that if the delay injected by a hacker is more than $\tau_{\max}$, a trap condition signal will be sent to the supervisory control and data acquisition (SCADA) center, and the controller switches it to open the loop control to stabilize the system. This switch is robust since the controller is equipped with a plant model by which it could predict the next state.

After designing the delay time estimator, the attention is now on the combination of the plant model and controller. Let the performance error be $e(t) = r(t) - x(t)$ and the estimate of the performance error be $\hat{e}(t) = r(t) - \hat{x}(t)$. The PID controller input is defined in terms of the estimated error as:

$$u(t) = K_P\hat{e}(t) + K_D\frac{d\hat{e}}{dt}(t) + K_I\int_0^t \hat{e}(s)ds \tag{6.3}$$

and the optimal feedback controller as

$$u(t) = K\hat{e}(t) \tag{6.4}$$

where K_P, K_D, K_I and K are proportional, derivative, integral and optimal gain respectively.

The PID controller and optimal feedback controller gains can be designed in normal operation (with no TDS attacks). More detail on designing PID and optimal controllers can be found at [111] and [112], respectively.

In this case, the controller was designed to depend on the error $\hat{e}(t)$ that results from the estimate $\hat{x}(t)$. If the estimate $\hat{x}(t)$ converges to $x(t)$, then $\hat{e}(t)$ converges to $e(t)$ and is minimized by the controller such that the system $x(t)$ converges to $r(t)$. However, this is not enough. Could $\hat{x}(t)$ be estimated by knowing $x(t-\tau)$? This is an important component in finding a stable controller. To answer this question, consider the following argument. The plant model estimation equation is given by

$$\dot{\hat{x}}(t) = A\hat{x}(t) + Bu(t) \tag{6.5}$$

The delayed equation of the state is

$$\dot{x}(t-\tau) = Ax(t-\tau) + Bu(t-\tau) \tag{6.6}$$

where $x(t-\tau)$ and $\dot{x}(t-\tau)$ are measured by the plant model, $u(t-\tau)$ is unknown since τ is not known.

Accordingly, the following equation is constructed

$$\dot{\hat{x}}(t-\tau) = A\hat{x}(t-\tau) + Bu(t-\tau) \tag{6.7}$$

The elements of equation (6.7) are unknown because τ is unknown.

Multiply Equation (6.7) by a positive definite constant gain matrix *C*, and subtract the resultant $C\dot{\hat{x}}(t-\tau)$ from $\dot{\hat{x}}(t)$ of Equation (6.5). In this way the following is obtained

$$\begin{aligned}\dot{\hat{x}}(t) &= A\hat{x}(t) + C\dot{\hat{x}}(t-\tau) - CA\hat{x}(t-\tau)\\ &\quad - CBu(t-\tau) + Bu(t)\end{aligned} \tag{6.8}$$

Substituting $CBu\,(t-\tau) = C\dot{x}(t-\tau) - CAx\,(t-\tau)$ into Equation (6.8) results in

$$\begin{aligned}\dot{\hat{x}}(t) &= A\hat{x}(t) + Bu(t) + C\dot{\hat{x}}(t-\tau) - CA\hat{x}(t-\tau)\\ &\quad - C\dot{x}(t-\tau) + CAx(t-\tau)\\ &= A\hat{x}(t) + Bu(t)\\ &\quad - C\left[\dot{x}(t-\tau) - \dot{\hat{x}}(t-\tau)\right] + CA\left[x(t-\tau) - \hat{x}(t-\tau)\right]\\ &= A\hat{x}(t) + Bu(t) - C\left[\dot{e}_m(t;\tau,\tau) - Ae_m(t;\tau,\tau)\right]\end{aligned} \tag{6.9}$$

Note that the first τ is the actual delay signal that is associated with the delayed signal *x*(*t*-*τ*) itself, which is read via the communication channel. This τ is hidden and is not accessible to the control system. The second τ is associated with the plant estimator and estimate of the delay signal $\hat{\tau}$ and delayed states $\hat{x}$. Equation (6.9) is stated assuming the fact that $\hat{\tau} = \tau$. Next, $e_m(t;\tau,\tau)$ is replaced by $e_m(t;\tau,\hat{\tau})$ of Equation (5.6) to obtain:

$$\dot{\hat{x}}(t) = A\hat{x}(t) + Bu(t) - C\left[\dot{e}_m(t;\tau,\hat{\tau}) - Ae_m(t;\tau,\hat{\tau})\right] \tag{6.10}$$

The above replacement makes the current predicted estimate of the plant state $\hat{x}(t)$ dependent on the estimate of the time delay $\hat{\tau}$. In other words, an accurate estimate of the state depends on an accurate estimate of the time delay. In Equation (6.10), only if $\dot{e}_m(t;\tau,\hat{\tau}) - Ae_m(t;\tau,\hat{\tau})$ goes to zero as a result of $\hat{\tau}$ converging to τ , then $\hat{x}(t)$ will converge to $x(t)$. This means that the modeling error e_m should be exponentially damped, i.e., $\dot{e}_m(t;\tau,\hat{\tau}) = Ae_m(t;\tau,\hat{\tau})$.

Notice that the method by which the plant estimate is constructed depends on the measured states of the plant, $x(t-\tau)$, and the estimate of the state given the estimated time delay, $\hat{x}(t-\hat{\tau})$. The difference $x(t-\tau) - \hat{x}(t-\hat{\tau})$ is the modeling error signal

$e_m(t;\tau,\hat{\tau})$. The choice of the gain matrix C in equation (6.10) is dictated by balancing the requirements for having the plant model state depend on errors in time-delay estimation and guarantee that the control system remains stable. More details can be found in [113, 114].

This method was employed in MATLAB and its performance confirmed using a single-input, single-output system, as well as a LFC control of a two-area distributed power systems. In the next section, the simulation results are presented and discussed.

6.3 Controller Design Algorithm

Step 1: Initialize time-delay estimate $\hat{\tau}$, plant model state estimate $\hat{x}$ and model error e_m. Then, set the learning parameter η to a suitable value. Also, set the matrix C.

Step 2: Obtain a plant state measurement (i.e., the sensed states of the plant $x(t-\tau)$), which could be time-delayed by τ(t).

Step 3: Compute the current state estimate, $\hat{x}(t)$, using Equation (6.10).

Step 4: Compute the delayed plant state estimate $\hat{x}(t-\hat{\tau})$ based on the model's equation and the estimate of the performance error $\hat{e}(t)=r(t)-\hat{x}(t)$ and model error $e_m(t;\tau,\hat{\tau})=x(t-\tau)-\hat{x}(t-\hat{\tau})$.

Step 5: Compute the time-delay estimate $\hat{\tau}$, from Equation (6.2).

Step 6: Compute the control signal $u(t)$. For example, u can be set by using Equation (6.3) or (6.4).

Step 7: To prevent runaway conditions bound the control signal by $\pm u_{max}$, use the time-delay estimate by $\tau_{\max}$ and plant model by $\pm x_{max}$.

Step 8: Repeat Steps 2-7 until the estimate of the performance error $\hat{e} < \varepsilon$.

6.4 Simulation Results

A simple single-input, single-output system is considered under a variable time-delay attack with a variable reference signal. This test is conceived to demonstrate the usability and efficiency of this method. The simulation model is given by:

$$\begin{aligned} &\dot{x}(t) = -0.7x(t) + 2u(t) \\ &r(t) = \begin{cases} 1 - e^{-\gamma 2t} & t \le T_a \\ 4e^{-\gamma 1\,(t-Tb)}(\sin(2\pi\omega_a t) + 1) & otherwise \end{cases} \\ &\tau(t) = T_1 e^{-\lambda 1t}(\sin(2\pi\omega_1 t) + 1) + T_2(1 - e^{-\lambda 2t}) + 1 \end{aligned} \tag{6.11}$$

where the total simulation time T=500 sec. T_a=T/2, T_b=T/2.2, T_1=T_2=T/10, λ_1=0.005, λ_2=0.0005, γ_1=0.07, γ_2=0.004, ω_a=0.06, ω_1=0.005 and the sampling period is 0.01 sec.

The proposed PID controller was applied to track the reference signal under a TDS attack. Figure 6.2 shows the state of the plant in Equation (6.11) as tracking the desired trajectory *r*(*t*). The dotted line is the state of the system, while the other one is the reference signal. The tracking is almost perfect, even though the time delay varies by $\tau(t)$. Figure 6.3 shows the TDS attack detection and its tracking; the estimated time delay $\hat{\tau}(t)$ tracks the time varying time delay $\tau(t)$ that can either be injected by a hacker or occurring naturally. The dotted line is time-delay estimate, while the other is the TDS attack. Note that in the first 80 seconds of the simulation of the system operation, the plant is not tracking the reference signal because the time variable *t* is less than the time delay $\tau(t)$. For this plant simulation, a PID controller was used with the following parameters K_P=5,

K_I=2 and K_D=1.5. The time-delay estimator learning rate η=0.32 and the plant model teacher forcing effort parameter is C=2.

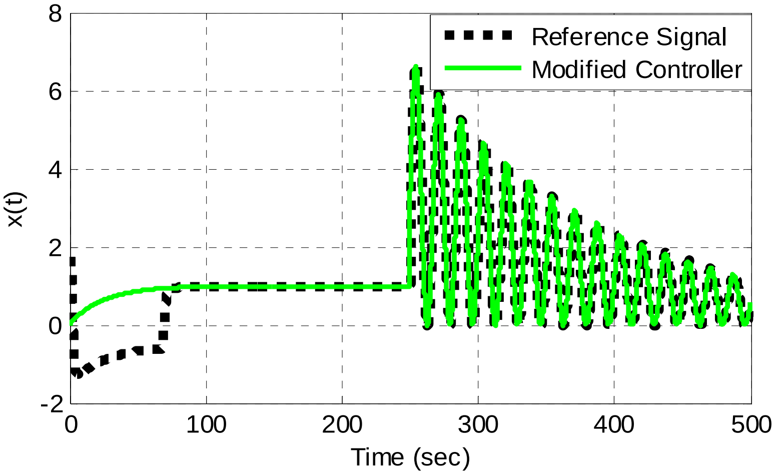


Figure 6.2: Tracking the Performance of a Single-input, Single-output System under TDS Attack

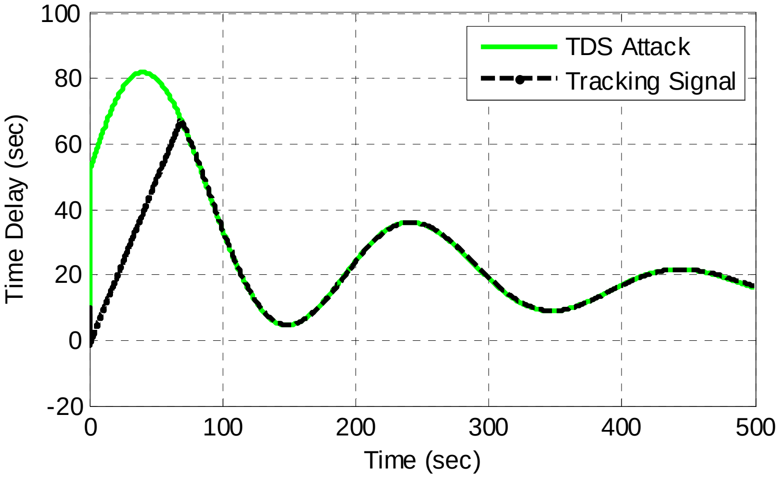


Figure 6.3: Time Delay Tracking

The simple, modified model-based control and time-delay estimation works for simple single-input, single-output systems under variable time-delay attacks; the distributed power control systems are considered where time-delay mitigation strategies are paramount. The focal point is the LFC system (mentioned in Section 4.4.2), where the controller's job is to regulate the state of a networked power system. Simulation studies were conducted to evaluate the effects of TDS attacks on the dynamics of the system.

By solving the Riccati matrix equation, the close loop control is designed in the form of state feedback. For this simulation, the discrete linear-quadratic regulator design is used from the continuous cost function called the "lqrd" function in MATLAB 2013a. For simplicity of discussion, $N = 2$ is set, which is defined as a two-area power system. Table 4.3 shows parameter values used in this process. Since simulation for certain duration tracks a step load change, we also set both ΔP_l^1 and ΔP_l^2 to be zero.

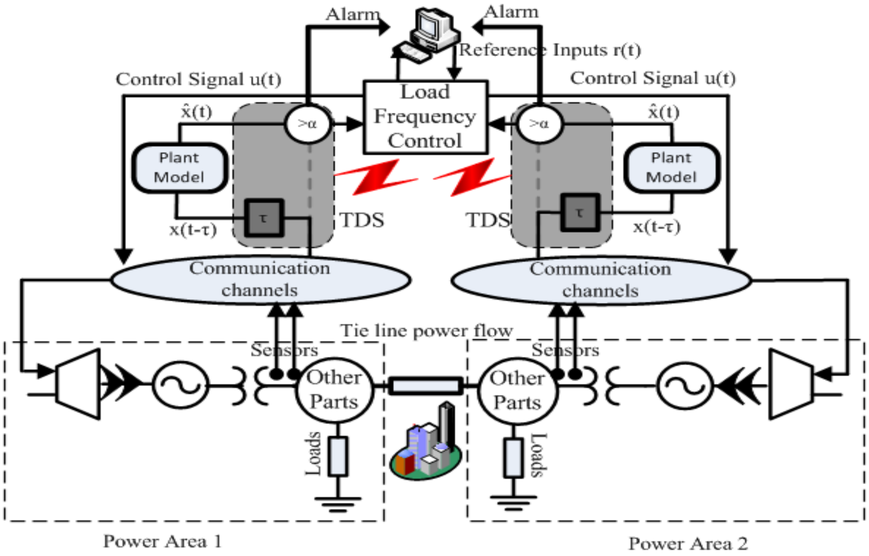


Figure 6.4: An Adaptive Load Frequency Control for a Two-area Power System Which is Robust to the TDS Attack Using the Modified Method

Scenario 1:

The hacker injects time delays into the second and eighth states at the time of 8 seconds and 24 seconds for the delay value of 1.28 seconds and 9 seconds, respectively. The LFC system equipped with the time-delay estimator performs as expected. Power states are regulated to zero, and the TDS attack is detected and time delay is tracked. Figure 6.5

shows the detection and track of the time delay, and Figure 6.6 shows all states of the two-area interconnected power system. As it is clear from the figures, the modified controller is able to control the LFC distributed system under a TDS attack. In Figure 6.6, initial delays direct the system away from the stable point, however, shortly after, time delays are estimated and the controller recovers the regulating power states to zero.

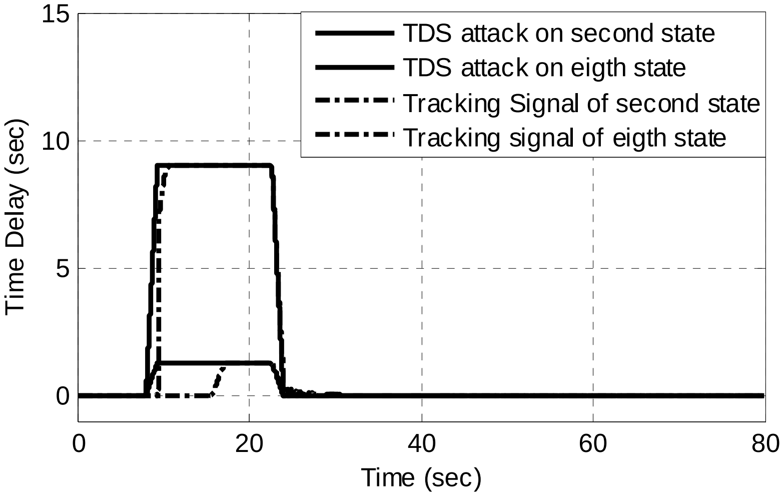


Figure 6.5: TDS Attack Tracking

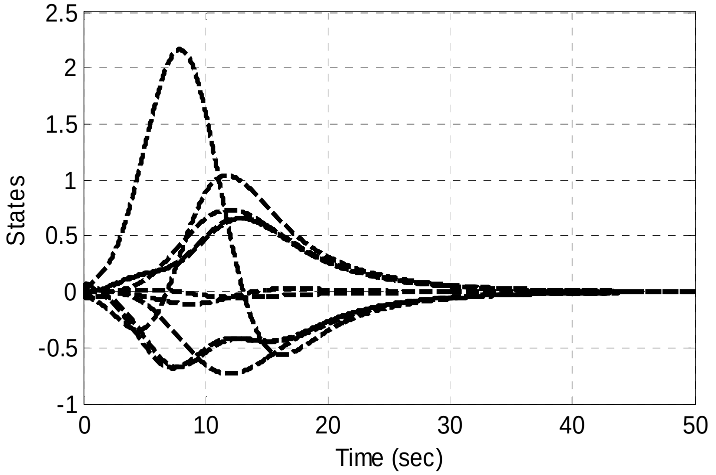


Figure 6.6: All States for Two-area LFC Power System under TDS Attack Using the Modified Optimal Controller

Scenario 2:

In this scenario, a TDS attack is injected at 1 second and 3 seconds in time for delay values of 5 seconds and 7 seconds for the second and the eighth states. Figure 6.7 shows that the tracking scheme works well and as expected, and could track the TDS attack. Figure 6.8, Figure 6.9, Figure 6.10, and Figure 6.11 show the simulation results of the frequency and power deviation of the generator, value position of the turbine, and tie-line power flow of the first power area with and without the modified control method, respectively. It shows that the system will be unstable when under a TDS attack, if the modified method is not applied. In the abovementioned figures, the TOC and MOC denote the traditional optimal controller and the modified optimal controller, respectively.

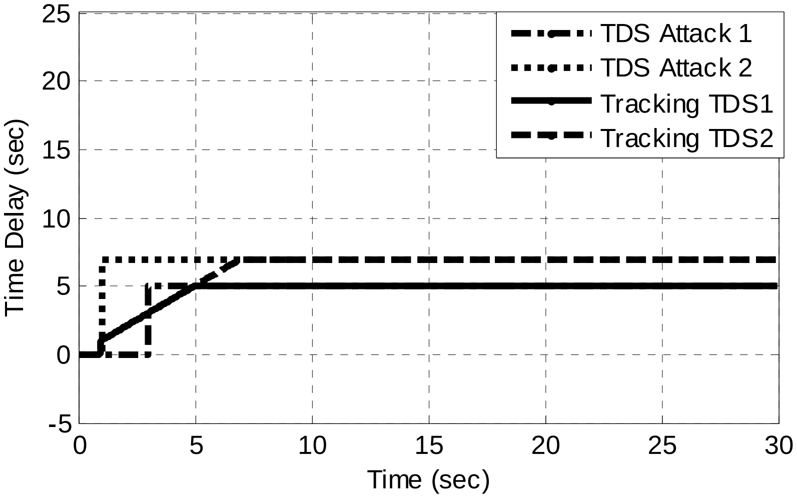


Figure 6.7: Time-Delay Tracking under a TDS Attack

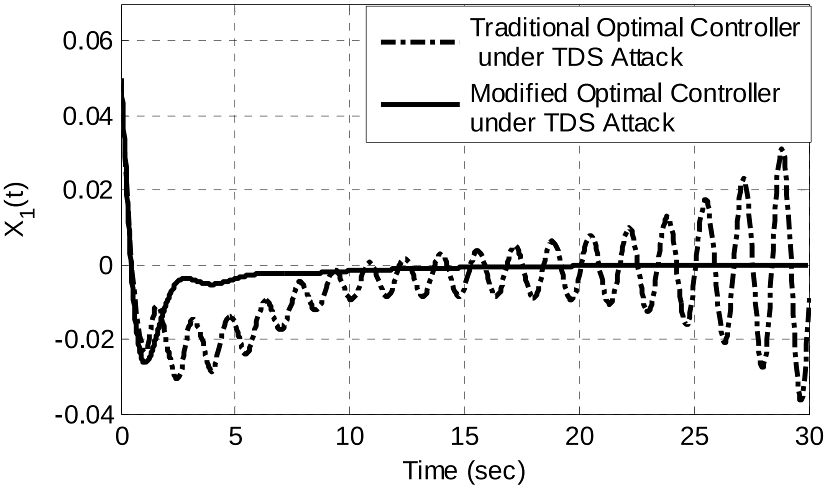


Figure 6.8: Frequency Deviation, Δf^K

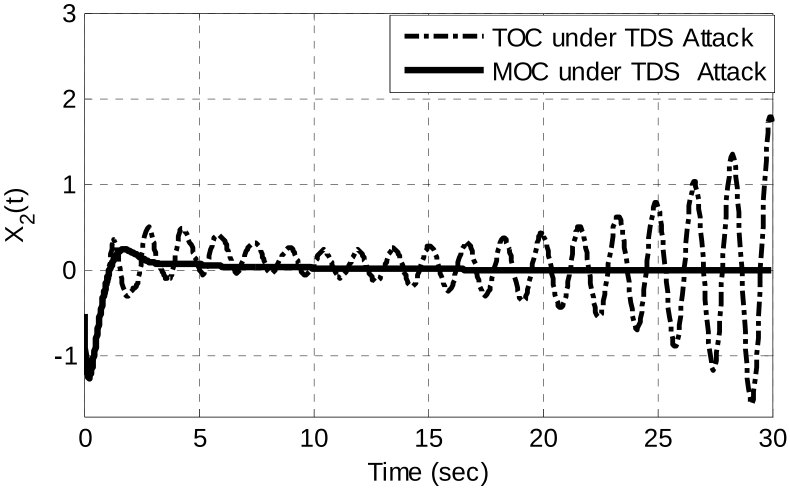


Figure 6.9: Power Deviation of Generator, ΔP_g^K

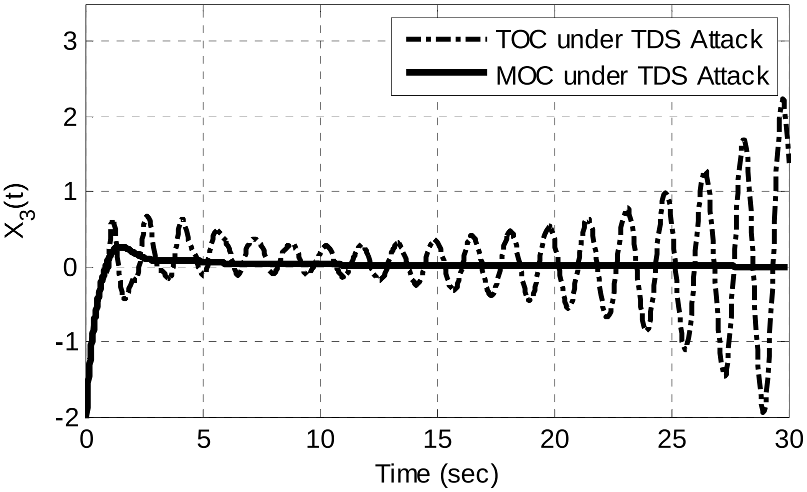


Figure 6.10: Value Position of the Turbine, ΔP_{tu}^K

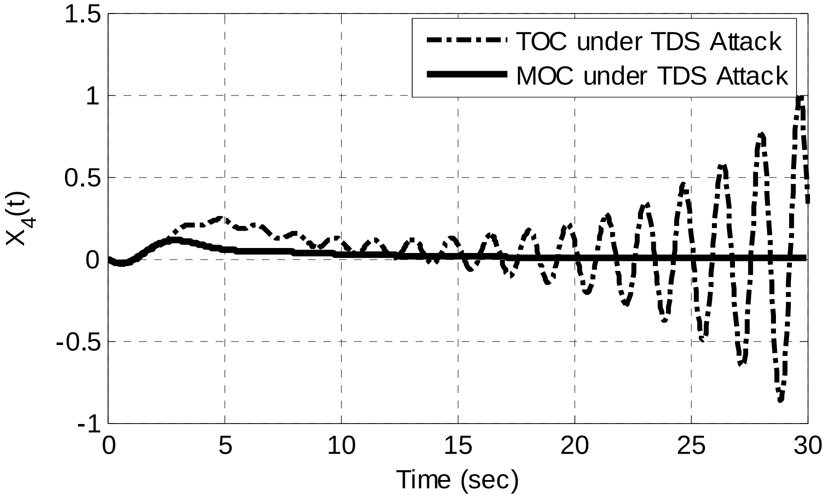


Figure 6.11: Tie-line Power Flow, ΔP^1_{pf}

Scenario 3:

This scenario is exactly the same as the second one, except that 15 percent of disturbance and noise were added to the system. As it is clear in Figure 6.12, the modified control technique could detect, track, and control the LFC system during a TDS attack and some disturbances. Figures 6.13 and Figure 6.14 show the tracking performance of the value position of the turbine system during a TDS attack for the first and the second power areas, respectively.

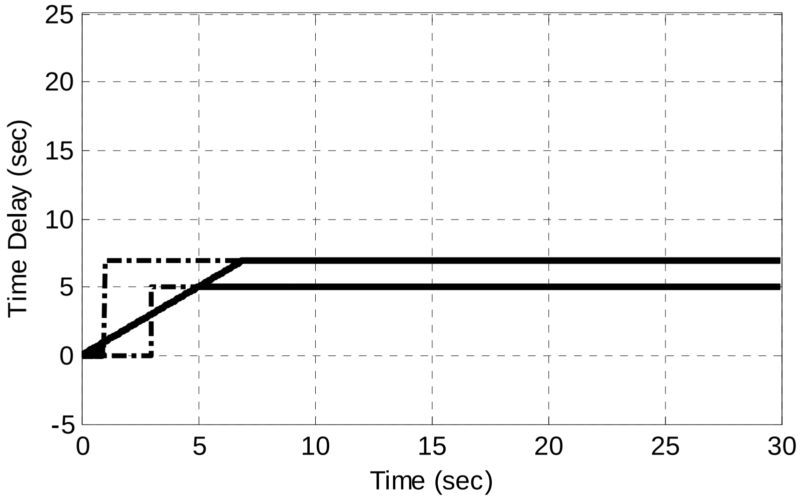


Figure 6.12: TDS Attack Tracking

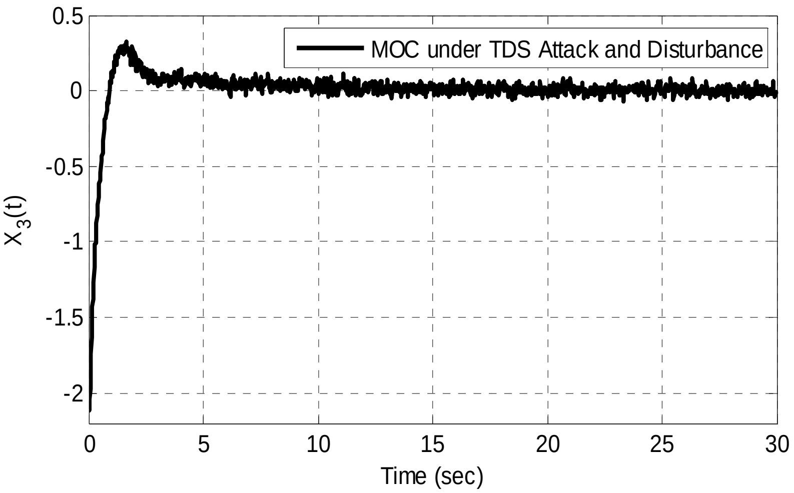


Figure 6.13: Value Position of the Turbine System during a TDS Attack for the First Power Area Control System

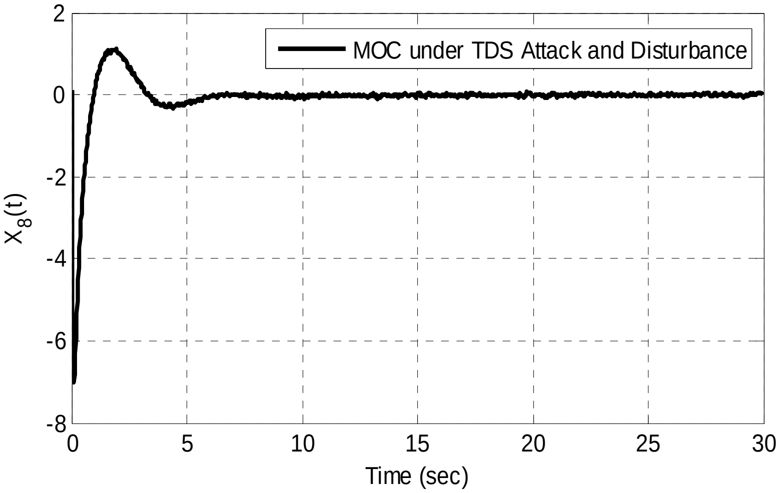


Figure 6.14: Value Position of the Turbine System during a TDS Attack for the Second Power Area Control System

6.5 Conclusion

The LTI systems were able to be controlled with variable time delays either occurring naturally or as a result of a time-delay attack by a hacker. The TDS attack was tracked with the proposed method. One kind of delay was addressed specifically, that is, the delay in the observed state of the controlled system. In this paper, only the LTI system in state feedback was examined. In future papers, research will show that it works for a class of nonlinear systems.

CHAPTER 7

CONTROL OF NONLINEAR SYSTEM UNDER A TDS ATTACK: EVALUATION OF METHODS

7.1 Introduction

In this chapter, several existing common controllers, such as the Model Predictive Controller (MPC), PID controller, and emotional learning controller (ELC) were evaluated during a TDS attack. Also, a new simple technique was proposed, called the "emergency controller," which overcomes stability issues caused by a TDS attack based on the TDS detector described in Chapter 4. The emergency controller was applied to the LFC application described in Section 4.4.2 and evaluated the ELC and other methods on the 2nd-order heartbeat model described in Section 4.4.3.

For the second application (heartbeat model), the controllability and observability of the heartbeat model are assumed and discussed in [90]. The nonlinear feedback Emotional Learning PI Control (ELPIC) technique is proposed in Section 7.2 and discussed in detail. Finally, we present experiments to verify that this method works well and as expected. The conclusion shows that this method is powerful enough to track the ECG signal and is more robust, when it is compared with the other control methods during a TDS attack or random delay in the sensing loop.

The emergency controller design is described in Section 7.4. The simulation is applied to a two-area power system with the LFC and shows the simplicity and cost-effectiveness of this technique.

7.2 Emotional Learning Controller (ELC)

The emotional learning controller (ELC) was presented by Moren and Balkenious for the first time. They began the process of evolving to evolve computational models for parts of the human brain that carry out emotional functioning. In [115], a new computational model of brain emotional learning included the amygdala, orbitofrontal cortex, thalamus, and sensory cortex, as shown in Figure 7.1.

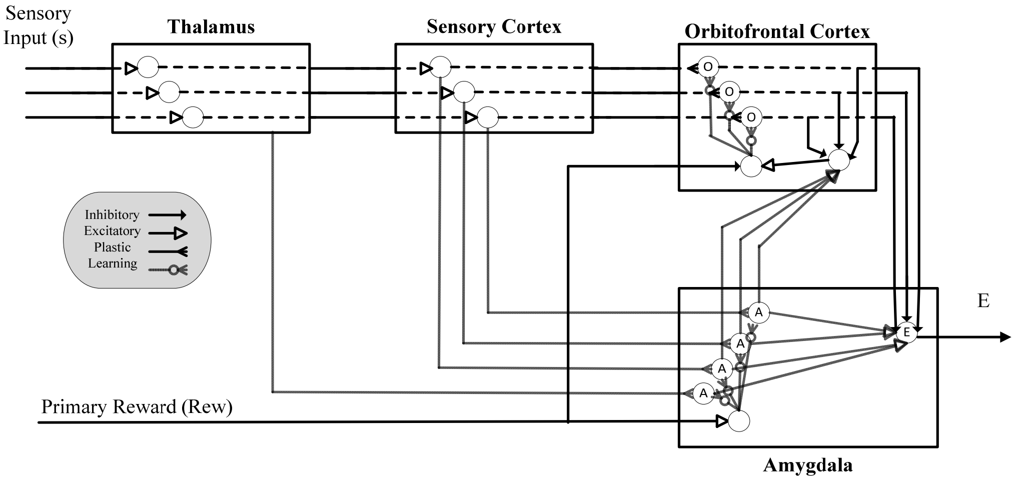


Figure 7.1: Scheme of Brain Emotional Learning Model

The amygdale is a small unit in the brain, which is involved in emotional evaluation of the stimuli. These emotional states and reactions derive “alarm signals” and “motor control commands.” Some of the inherent exciters such hunger, pain, certain smells, etc., can excite the amygdale. The amygdale responding to these stimulants is used in learning. On the other hand, the orbitofrontal cortex plays a role of a modifier of inappropriate responses and reactions of the amygdale. Numerous experiments on patients with damaged orbitofrontal-cortex revealed that they are not able to adapt themselves to new conditions [116], in the other words, previous learning does not let them understand and respond to new conditions.

The ELC consists of two sections that carry out the learning section and control section: one corresponds to information processed by the amygdala, and the other by the orbitofrontal cortex. Basically, input stimuli (signals) are processed and used to gain control of coefficients (synaptic efficacies) to affect the future process of stimuli and motor control commands. By ignoring some of the details in Figure 7.1, the computational emotional learning model of amygdale-orbitofrontal is shown in Figure 7.2.

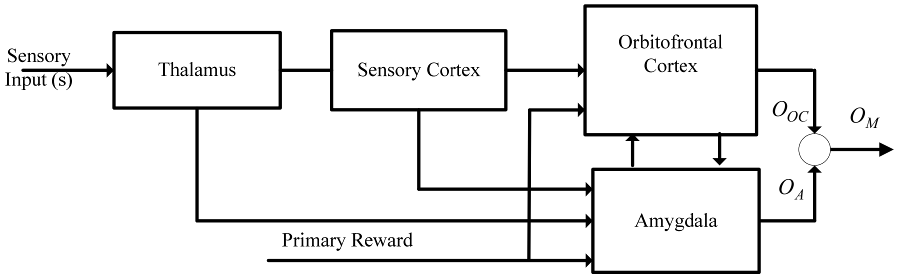


Figure 7.2: Overall Computational Model of ELC

The output of the computational model can be found as:

$$O_M = O_A - O_{OC} \tag{7.1}$$

where O_M is the model output, O_A and O_{OC} are the amygdale and the orbitofrontal cortex unit output, respectively.

The outputs of the amygdale and orbitofrontal units are described by:

$$O_A = G_A \cdot I_S \tag{7.2}$$

$$O_{OC} = G_{OC} \cdot I_S \tag{7.3}$$

where G_A is the amygdale gain, I_S is the sensory input, and G_{OC} is the orbitofrontal cortex gain. The amygdale and orbitofrontal learning laws can be modeled as:

$$\Delta G_{OC} = k_1 \cdot (O_M - I_{PR}) \tag{7.4}$$

$$\Delta G_A = k_2 \cdot Max\{0, I_{PR} - O_A\} \tag{7.5}$$

where I_{PR} is the primary reward, and $k_1$and k_2 are the rates of learning related to orbitofrontal and amygdale, respectively.

The Equation (7.5) shows that the amygdale learning uses max operation. Therefore, the amygdale gain is forced to have a consistently increasing deviation. This emphasizes the physiological fact of the amygdale unit which records what it learns.

Now, let us use Equations (7.1), (7.2), and (7.3) to find a general formula:

$$O_M = (G_A - G_{OC}) I_S \tag{7.6}$$

Based on the above equation, we can conclude that the output for of the amygdale-orbitofrontal unit in the emotional learning system depends on the amygdale and orbitofrontal gains, and the sensory inputs. It should be noted that these gains depend on the primary reward signal.

In this chapter, the sensory input of the emotional learning system is formulated with a format similar to the self-tuning PID:

$$I_S(t) = K_P e(t) + K_D \dot{e}(t) + K_I \int_0^t e(t)\,dt \tag{7.7}$$

where K_P, K_D, and K_I are the proportional gain, the derivative gain, and the integral gain, respectively. The signal $e(t)$ is the difference value between the reference value and the output value at any time instant. However, to get a better response in front of noise, PI was used instead of PID as the sensory input to the amygdale-orbitofrontal emotional learning system. The next section will show how this controller improves the performance of the system in the attack operations and tracks the reference ECG signal very well.

7.3 Simulation Result Based on ELC Controller: Evaluation of Methods

The 2nd order heartbeat model was simulated to track the ECG signal using the ELPIC. Then, an external TDS attack or random feedback delay is applied to the model from a start time t_S until a final time t_F to show the performance of the ELPIC. This is compared with the classical PID and the MPC.

Figure 7.3 shows the ECG reference tracking $X_2(t)$ using the ELPIC. The line shows the output of the model controlled by the ELPIC, and the dotted line indicates the patient's ECG referenced signal [95]. The result shows that the ELPIC tracks the reference signal accurately.

The TDS attack or feedback delay is applied to the model from $t_S = 0.4$ seconds until $t_S = 0.45$ seconds, with the time-delay of $\tau = 0.01$ seconds. For the purpose of visual comparison, the attack period and the amount of attack are selected as a lower level. Due to the larger period and time-delay value, the classical PI and MPC controllers move out of visual boundaries. Figures 7.4 and 7.5 compare the ELPIC with the classical PI and the

MATLAB's MPC. The results clearly show that the ELPIC is more robust during a TDS attack or unwanted random feedback delay.

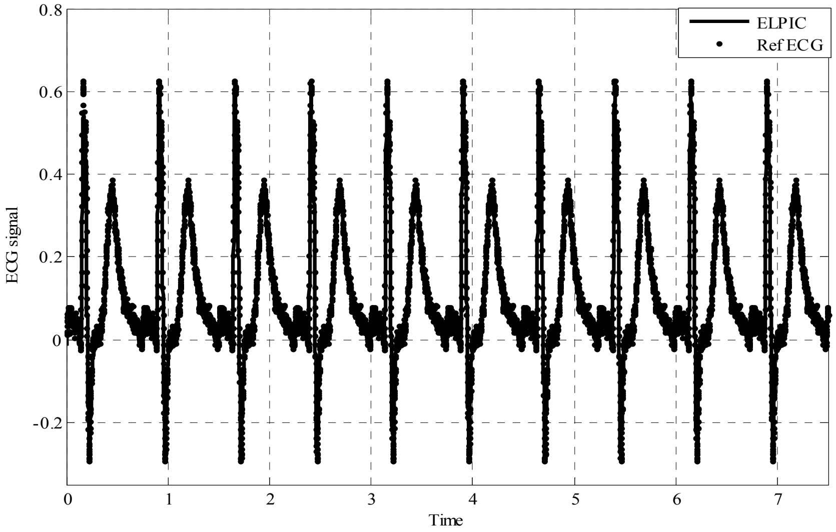


Figure 7.3: Simulation Result of ECG Tracking for Second-Order Heartbeat Model Based on ELPIC Pacemaker Signal

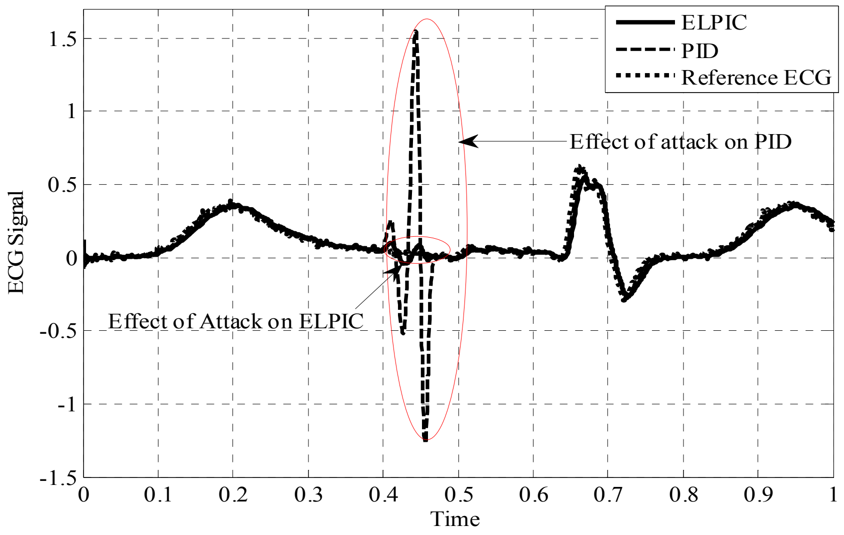


Figure 7.4: Comparison of the ELPIC and the Classical PID for ECG Tracking during a TDS Attack

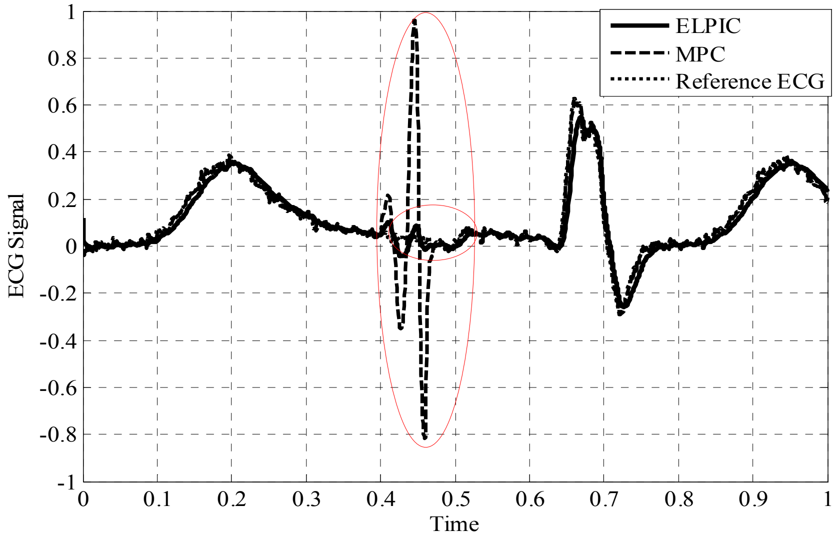


Figure 7.5: Comparison of the ELPIC and the MPC for ECG Tracking during a TDS Attack

In summary, the ELC applied to Zeeman nonlinear heart model is able to track the ECG signal with a high level of reliability. Furthermore, the robustness of the ELC's ability to control the Zeeman heart model under a time-delay switch attack was demonstrated. The stability and control of the operations are evaluated. We have also demonstrated that ELC is more robust than other common control schemes, such as the classical PID and the MPC.

7.4 Local and Emergency Controller Design

The proposed method is shown in Figure 7.6. Its basic elements are a plant model, a time delay detector, an emergency controller, and a controller. The controller can either be a PID controller or an optimal feedback controller. The emergency controller's task is to stabilize the system in case of an attack on the communication lines of the distant controller. The time-delay detector estimates the time delay in the communication channel from telemetered data. If the delay is larger than an acceptable time delay, it will generate and send alarm signals to the controller and emergency controller. If an alarm signal is received by the emergency controller, it will begin to stabilize the plant to a desired state, while the distant controller stops operating until the delay is corrected.

At this point, the time-delay estimator has been designed, and the focus is now on the controller and emergency controller. The controller can either be a PID controller or an optimal controller, depending on the requirements of the industrial application. Equation (7.8) is the PID controller, while Equation (7.9) is the optimal controller.

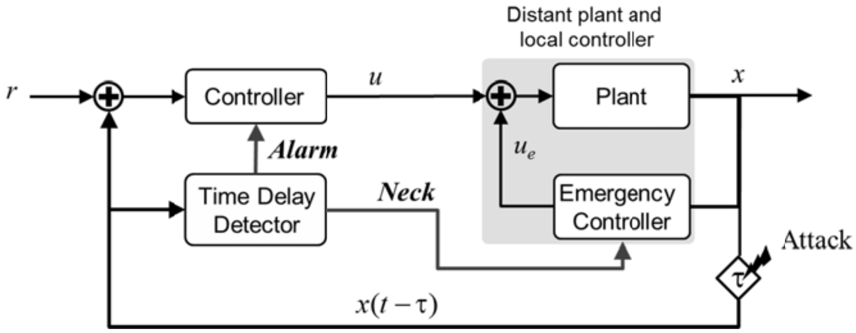


Figure 7.6: Block Diagram of Proposed Control Technique

$$u(t) = K_P e(t) + K_D \frac{de}{dt}(t) + K_I \int_0^t e(s)ds \tag{7.8}$$

$$u(t) = Ke(t) \tag{7.9}$$

where the error is $e(t) = r(t) - x(t)$. Either controller, i.e., the PID or the optimal controller, can be designed to be robust to some maximum time-delay τ_{stable}. The emergency controller sits close to the plant and operates only in case of emergency such as an attack on the communication line between the plant and controller. The emergency controller could either be a PID controller or optimal controller with the goal to stabilize the system to a particular reference trajectory r_E.

Suppose there is a time-delay attack on the system with delay τ. The time-delay estimator estimates the delay for $\hat{\tau}$. The delay estimator is described in Chapter 5. The cyber-attack detector will use the time-delay estimate to perform the following function

$$D = \begin{cases} 1 & \hat{\tau} > c\tau_{stable} \\ 0 & otherwise \end{cases}, \tag{7.10}$$

where c is a constant between 0 and 1. In case *D=1*, an alarm signal is sent to the controller to shut it down, and a negative acknowledgement is sent to the emergency controller to stabilize the plant. The control strategy is shown in Figure 7.6.

The emergency controller method was implemented with MATLAB and its performance was studied using the LFC of a two-area distributed power system. In the next section, the simulation results are discussed in detail.

7.5 Simulation Result and Conclusion Using Local Controller-Based Design

The simulation was conducted on the LFC described in Section 4.4.2 for the proposed emergency controller described in Section 7.4.

The assumption is that a hacker injects a TDS attack into the feedback lines of both power areas. In this simulation, an attacker starts a TDS attack to the second power area (the third state) at time 1 second for $t_{d3} = 5s$, and then increases it at 20 seconds for $t_{d3} = 10s$. Furthermore, a hacker starts to attack the first power area (third state), at 1 second with $t_{d8} = 3s$, and increases it to $t_{d8} = 4.5s$ at 30 seconds. We also set the $\tau_{stable} = 0.4s$ based on the stability analysis of the LFC system in Section 4.4.2. The negative acknowledgment (neck) is then sent to the emergency controller in the case where the detected value of the time delay is larger than the maximum time delay. Figures 7.7 and Figure 7.8 show the third state of the first and the second power areas under attack with a traditional optimal controller (TOC) and proposed control technique (PCT), respectively. It is clear from the results that the simulated attack makes the system unstable. The proposed technique, however, can overcome a TDS attack on the simulated system.

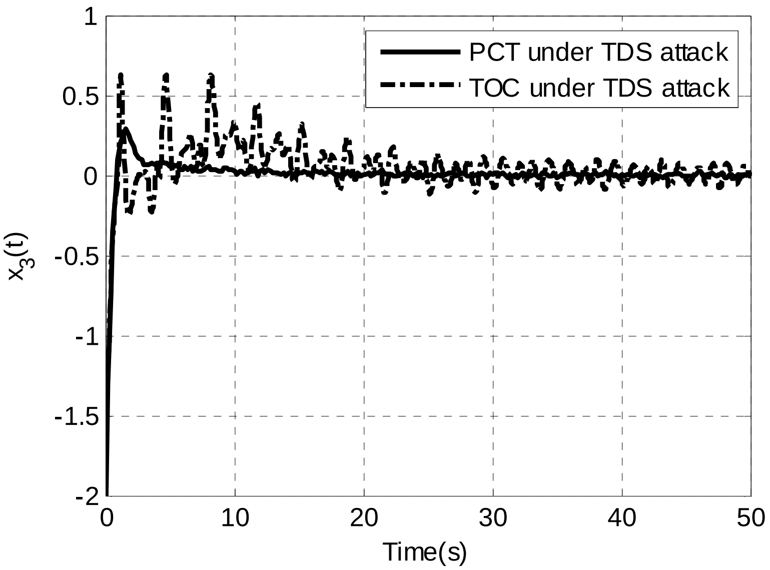


Figure 7.7: Value Position of the Turbine System during a TDS Attack for the First Power-Area Control System

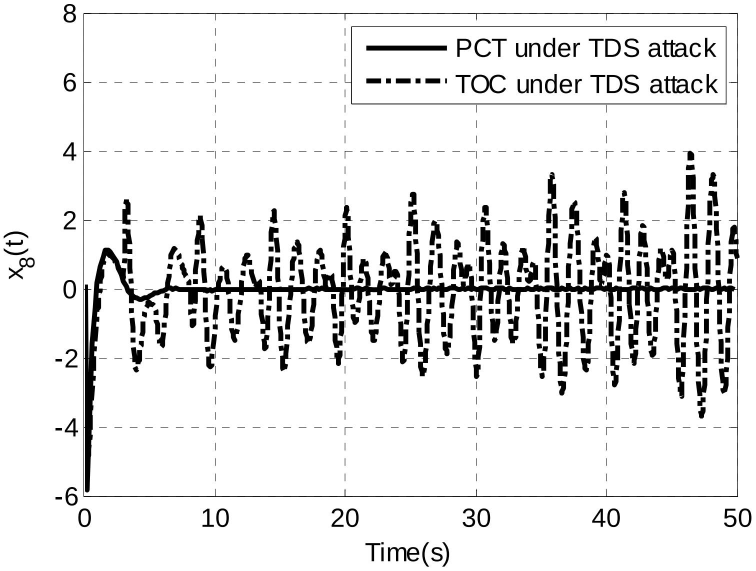


Figure 7.8: Value Position of the Turbine System during a TDS Attack for the Second Power-Area Control System

In summary, a simple and cost-effective method for overcoming the stability effects of a TDS attack on NCSs has been successfully demonstrated. The method relied on a time-delay estimator that estimates and tracks time delays introduced by a hacker. With knowledge of the maximum time delay of the control system, for which the plant remains stable and secure, the time-delay detector compares the estimated time delay with the tolerable time delay and issues an alarm signal when the estimated time delay is larger than the tolerable one. It also directs the system to an alarm state. In an alarm state, the plant is under the control of the emergency controller, local to the plant. The plant remains in this mode until the networked control system state is restored and the time-delay switch is eliminated.

CHAPTER 8

CF-TDSR: A CRYPTOGRAPHY-FREE TDS RECOVERY PROTOCOL

8.1 Introduction

In recent years, the security of control systems has raised many important research questions. For instance, NCSs, which are used to monitor and control systems distributed over a wide area, are a groundbreaking approach to control systems used in power systems. Modern power grids depend on computers and multi-purpose networks for operation. This renders them vulnerable to attacks, including high-profile cyber attacks [21, 78, 117, 118] that have a potentially major societal impact.

TDS attacks delay the transmission of measured signals from the plant output to the controller. Most communication algorithms have proposed the use of timestamps to address naturally occurring delays in the communication between plants and their controllers in the NCS [119, 120]. However, timestamping is not effective against TDS attacks, since the attackers can manipulate both the data and the timestamps.

Consider, for instance, a hacker that can manipulate both the data content and the timestamps of telemetered information (sensed from the output sensor). The data sent to the controller consists of a sequence of points of the form $(t, x(t))$, where $x(t)$ denotes the state of the plant at time t. The attacker can modify this data in one of several ways. First, manipulate the timestamps, i.e., send $(t-d, x(t))$. Second, delay the state values, i.e., send $(t, x(t-d))$. Third, change both the timestamp and the data, i.e., send $(t-d_1, x(t-d_2))$. Finally, the attacker can simply drop the packets.

Cryptographic solutions may be used to detect such attacks. For instance, the packets can be authenticated, e.g., using keyed hashes (e.g., HMAC), and computed using a key shared only by the controller and the plant. Even if the cryptographic constructs are fast and will introduce only small delays and computing overhead, they are unable to recover from denial of service (DoS) attacks, or to recover data delayed or destroyed by the hacker. The controller will be forced to request the retransmission of the lost or corrupt packets, leading to additional delays and a higher network load that can destabilize the entire system.

In this chapter, the adaptive channel allocation techniques are leveraged, along with the state predictors and time-delay detectors to address the challenges introduced by TDS attacks. Adaptive resource allocation techniques and channel adaptive methods provide substantial improvements and robust performance under many benchmarking metrics [121]. These methods utilize an adaptive allocation of communication resources as the channel conditions change with time [122].

The Cryptography-Free TDS Recovery (CF-TDSR) is introduced in this section, which requires the controller to first compare the received timestamp against an internally generated value. The CF-TDSR requires time synchronization between the plant and the controller. If a discrepancy is detected, then the telemetered information is discarded. The controller instead uses the predicted state, generated by a state predictor. If the data has been delayed, the controller compares the value of the measured states against an internally predicted value of states. If the difference exceeds a predetermined threshold, the controller drops the packet and uses the estimated state instead. In both cases, the controller sends a command signal to the data measurement unit to transmit the next data sets over multiple channels.

This chapter is organized as follows. In Section 8.2, relevant work is described. In Section 8.3, the system and hacker model are provided, along with TDS attacks. The LFC system is introduced, and the adaptive allocation method is used to demonstrate mechanisms to restore stability after a time-delay attack. In the following section, a special type of TDS attack is modeled as a DoS attack. In Section 8.4, the CF-TDSR is introduced and its ability to eliminate the effects of time delay attacks is demonstrated. In Section 8.5, the simulation results are presented and discussed.

8.2 Related Works

In this chapter, the main focus is on the role of the NCS application in power systems. The control of the NCS in power systems with time delays has been previously explored [21, 78, 96, 107, 108, 123, 124]. The researchers, however, considered either the construction of controllers that are robust to time delays or controllers that use offline estimation. At this time, there seem to be no control methods and adaptive communication protocol that implement an online estimation of dynamic time delays and real-time control of power systems to overcome TDS attacks.

The stability of power control system controllers with time delays was studied in [99-103]. The author of [104] studied the stability effects of delays to the smaller signal power systems. References [99] and [100] proposed methods to reduce oscillations resulting from time-delayed feedback control. Paper [105] introduced a wide-area control system for oscillations of a generator. Based on phasor measurements with delays, a novel controller was suggested in [96] and the power system's small signal stability was considered. In [106], a feedback controller for power systems with delayed states was proposed. The controller addresses the combined effects of the instantaneous as well as delayed states using the quadratic Lyapunov function.

Related work on time delays was discussed in Chapters 2 and 5. In conclusion, control methods developed to compensate for time delays rely either on a robust controller to a maximum time delay, on off-line estimates of time delays, or on approximations of time-delayed signals. In this chapter, a general method for the control of systems experiencing TDS attacks was also proposed. The CF-TDSR applies to continuous linear time-invariant systems.

8.3 A Unified Approach

In this section, a unified approach to model a specific case of TDS attacks as DoS attacks is proposed. Then, techniques will be investigated that address TDS attacks. Consider a LTI system described by

$$\begin{aligned} \dot{x} &= Ax + Bu + w \\ u &= -Kx \end{aligned} \tag{8.1}$$

where $x \in R^r$ and $u \in R^n$ are state and control functions, respectively. Matrices *A, B* and *K* are constant with appropriate dimensions. The $w \in R^n$ is an *n*-dimensional zero-mean Gaussian white noise process. Suppose that a TDS attack occurs with probability p. Subsequently, the result is

$$\dot{x}(t) = \begin{cases} (A - BK)x(t) + w(t) & 1 - p \\ Ax(t) - BKx(t - \tau) & p \end{cases} \tag{8.2}$$

To simplify this explanation, in (8.2), it is assumed that the same probability of attack occurs on different channels and states. If a TDS attack occurs, packets are dropped. Then, Equation (8.2) is formulated in the form of a DoS attack, as follows

$$\dot{x}(t) = \begin{cases} (A - BK)x(t) + w(t) & 1 - p \\ Ax(t) + w(t) & p \end{cases} \tag{8.3}$$

Let us calculate expectation value of $\dot{x}$ in (8.3) as:

$$\begin{aligned} E\{\dot{x}(t)\} = & \begin{bmatrix} (A - BK)E\{x(t)\} \\ + E\{w(t)\} \end{bmatrix}(1 - p) \\ & + \left[AE\{x(t)\} + E\{w(t)\}\right] \end{aligned} \tag{8.4}$$

Let $\mu(t) = E\{x(t)\}$, then we can write (8.4) as

$$\begin{aligned} \dot{\mu}(t) &= [(A - BK)\mu(t)](1 - p) + A\mu(t)p \\ &= (A - (1 - p)BK)\mu(t) \end{aligned} \tag{8.5}$$

where $E\{w(t)\} = 0$ .Next, the stability of Equation (8.5) is investigated. For the system described in (8.5) to be stable, the mean should be bounded. Therefore, this equation must have:

$$\{A - (1 - p)BK < 0\} \tag{8.6}$$

hence,

$$A - BK + pBK < 0 \tag{8.7}$$

i.e., $A - Bk + pBK$ must be a negative definite when the controller is stable, and the next result must have

$$A - BK < 0 \tag{8.8}$$

To satisfy stability, condition (8.7) must be made similar to (8.8). To do this, two defenses are introduced. First, the probability of a TDS attack on the communication channel is decreased. Second, the controller gain is changed. In the following probability equations, both cases are described.

Decrease TDS Attack Probability.

$$\dot{x}(t) = \begin{cases} (A - BK)x(t) + w(t) & 1 - p^{l} \\ Ax(t) + w(t) & p^{l} \end{cases} \tag{8.9}$$

Equation (8.9) will take the following form:

$$A(BK)^{-1} - I + (pI)^{l} < 0 \tag{8.10}$$

Therefore, we get:

$$A(BK)^{-1} - I < A(BK)^{-1} - I + (pI)^{l} < A(BK)^{-1} - I + pI < 0 \tag{8.11}$$

The condition in Equation (8.11) shows that if l > 1 channel is allocated to increase the redundancy of transmitted plant data, the total probability of faults will decrease as a result of a TDS attack. Also, we will be able to bring the controlled system closer to its original state, i.e., *A-BK* < 0. Therefore, by adaptively adding another communication channel(s), the LFC system can be stabilized. The cost of channel redundancy limits the number of communication channels that can be added to address TDS attacks. The alternative is to change the controller gain. The second approach shown below illustrates how this can be accomplished.

Change Controller Gain. Changing the controller gain *K* to stabilize the NCS is proposed. The new controller gain parameter is set to be $K_p = K/(1-p)$. In this case, a limited number of channels only need to be added. However, adjusting the controller gain *K* is subject to how well the probability of attack *p* is estimated. In Section 8.4, this control methodology is described in detail.

8.4 CF-TDSR: A Crypto-Free TDS Recovery Protocol

In this section, we introduce the CF-TDSR, a communication and control protocol that thwarts TDS attacks on networked control systems. The CF-TDSR leverages methods to detect time delays introduced by a hacker. The CF-TDSR consists of the following components (see Figure 8.1, for the system diagram). First, the smart data transmitter (Tx) adaptively allocates transmission channels on demand. Second, the plant model estimates the current plant states and helps stabilize the network controlled system when under attack. Third, the time-delay estimator continuously estimates the time delays on the channels. Fourth, the time-delay detector determines if delays are detrimental to the system. In this case, it will issue commands to inform the transmitter (plant) and controller. The last component is the proportional-integral-derivative (PID) or optimal controller to control the system (control block in Figure 8.1). The CF-TDSR will detect and track time delays introduced by a hacker and guide the plant to track the reference signal to guarantee system stability.

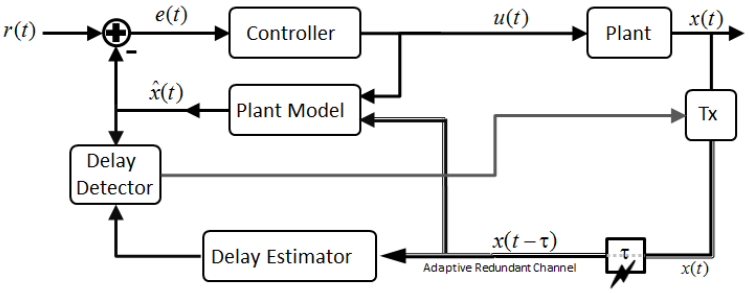


Figure 8.1: Block Diagram of CF-TDSR

The CF-TDSR is flexible and is able to support communication between the plant and the controller with and without timestamps. In the case where timestamps are used, the controller compares the controller clock and the packet time stamp and the state of the plant with the state predicted by the plant model. If there are any differences, the packet is dropped. If this is the case, the controller sends a negative acknowledgment (NACK) signal to the communication transmitter to use an adaptive channel allocation. Finally, the controller uses the state predicted by the plant model instead of the state received in the packet to control the system while it waits for the corrected packet.

In the case where timestamps are not used, the time estimator continuously estimates time delays while the plant model determines the appropriate plant state values (Chapter 5 described the time-delay estimation, and Chapter 6 described the state estimation for controller). If the estimated time delays are longer than the tolerable time delay, or if the plant state estimates are very different from the received plant states, the communicated packet is dropped. Similar to the previous case, in this case, the controller signals the communication transmitter to use adaptive channel allocation and uses its internal state estimates for control. In this way, by using the adaptive channel allocation and the robust plant state estimator, the controller is able to thwart TDS attacks.

The functionality of the delay detector elaborated above can be captured with the following mathematical formula

$$D(t) = \begin{cases} 1 & \left(|t_c - t_s| > \tau_{stable}\right) \; or \; \left(|e_m(t)| > \varepsilon\right) \; or \; \left(\hat{\tau} \geq \tau_{stable}\right) \\ 0 & otherwise \end{cases} \tag{8.12}$$

where $D(t)$ is the time-delay detection function, t_c is the time value of the clock maintained by the controller, t_s is the timestamp of the packet generated at the transmitter, and τ_{stable} is the maximum tolerable time delay, for which the system remains in the stable region. Its value can be calculated from the eigenvalues of the system, for example, finding the eigenvalues of LFC, as shown in Section 4.4.2. The difference between the transmitted state of the plant *x*(*t*) and the plant estimator record of the system state $\hat{x}(t)$ is $e_m(t) = x(t) - \hat{x}(t)$. The parameter ε is the tolerable error value. Since a TDS attack occurs with probability *p,* then *D*=1 with probability *p* and *D*=0 with probability 1-*p*. Equation (8.12) enables the detection of TDS attacks irrespective of the use of timestamps, and even if the timestamps are modified by the hacker. In the next section, each CF-TDSR component will be examined and discussed and detail.

We use Equation (5.9) to estimate the time delay, τ, considering that computing machines have finite memory and temporal resolution. Therefore, we are unable to implement Equation (5.9) without discrete approximation and boundedness assumptions. To guarantee the stability of calculations and limit the memory usage, the following condition, $\tau < \tau_{\max}$ must be added. This condition will allow for a construction of a finite buffer to store the history of $u(t)$ from t to $t - \tau_{\max}$. Also, this will allow us to prevent a runaway condition on $\hat{\tau}$.

8.5 Simulation Results and Discussion

8.5.1 TDS Attack on LFC Model

Consider a LFC system of the form:

$$\dot{x}(t) = Ax(t) + Bu(t) + w(t) \tag{8.13}$$

with the optimal controller given by:

$$u(t) = -K\hat{x}(t) = \begin{cases} -Kx(t) & 1 - D(t) \\ -K\hat{x}(t) & D(t) \end{cases} \tag{8.14}$$

where $D(t)$ is a digital random process. D(t) is 1 when a TDS attack is detected (see Equation (8.12)), and is zero otherwise. TDS attacks are detected by comparing the received timestamp from the plant against the controller time, or by using the time-delay estimator. The new state estimate, $\hat{x}(t)$, is given by:

$$\dot{\hat{x}}(t) = \begin{cases} Ax(t) + Bu(t) & 1 - D(t) \\ A\hat{x}(t) + Bu(t) & D(t) \end{cases} \tag{8.15}$$

Let the estimation error be $e_m(t) = \hat{x}(t) - x(t)$. The dynamics of the closed loop can be calculated as:

$$\dot{x}(t) = \begin{cases} (A - BK)x(t) + w(t) & 1 - D(t) and\ e_m(t) = 0 \\ (A - BK)x(t) - BKe_m(t) + w(t) & D(t) \end{cases} \tag{8.16}$$

We now investigate the stability of Equation (8.8). We want the mean of the estimation error *e_m(t)* converge to zero, for a reasonable stability criteria, and for the covariance of *e_m(t)* to remain bounded. If *e_m(t)* bounds the covariance, the state *x*(*t*) remains stable. We compute the total expectation value over both $x(t)$ and $D(t)$, knowing that $D(t) = 1$ with probability p, when there is an attack on one channel. Thus, we can express the equation of the system under attack as:

$$\dot{x}(t) = \begin{cases} (A - BK)x(t) + w(t) & 1 - p \\ (A - BK)x(t) - BKe_m(t) + w(t) & p \end{cases} \tag{8.17}$$

Therefore, the total expectation yields:

$$\begin{aligned}\dot{\mu}(t) &= (A-BK)\mu(t)(1-p) \\ &\quad + (A-BK)\mu(t)p - BK\mu_m(t)p \\ &= (A-BK)\mu(t) - BK\mu_m(t)p\end{aligned} \tag{8.18}$$

Let us now assume we add l channels to the communication channel. Hence, we have:

$$\dot{\mu}(t) = (A-BK)\mu(t) - BK\mu_m(t)p^l \tag{8.19}$$

If the term $BK\mu_m(t)p^l$ is zero, (8.19) will converge to zero and the system will be stable. Therefore, the idea is to make that term as small as possible by choosing a large l, or by using a good estimator for the system that can make this term closer to zero or bounded. If the delay injected by the hacker exceeds $\tau_{\max}$, a trap condition signal will be sent to the Supervisory Control and Data Acquisition (SCADA) center. Then, the controller switches to open the loop control to stabilize the system. This switch is robust, since the controller is equipped with a plant model through which it can predict the next state.

8.5.2 Simulation of CF-TDSR on LFC System

Simulations are conducted to evaluate the performance of CF-TDSR experiencing TDS attacks. The discrete linear-quadratic regulator design from the “lqrd” continuous cost function (MATLAB 2013a) is used to generate the optimal control law for the system in normal operation. The two-area power systems are modeled, as described in Section 4.2.2. Table 4.3 shows the parameter values used in the simulation, based on practical values and literature [21, 78]. Also, ΔP_l^1 and $\Delta P_l^2 = 0$ is set, and the sampling time is set to 0.01sec.

The goal of the simulation is to determine the ability of the CF-TDSR to quickly respond to the TDS attacks. The total simulation time is set as 50 seconds. The example assumes a powerful hacker that has access to the communication channel. The hacker starts the TDS attack with values of $\tau = [t_{d1} \quad t_{d2} \quad \cdots \quad t_{dn}]^T$. Each power area has five states. Since the two-power-area systems, *n*, are considered in this equation, the total number of states in the interconnected model is 10. Consider that the attack starts at time t_a.

The simulation is performed in three main scenarios: single power plant attack, composite TDS attack, and simultaneous composite TDS attack on a noisy system and limited available channel.

Single Plant TDS Attack

In the first investigation, a hacker has access only to the first power area, and can only launch TDS attacks on the specific channel. The existence of multiple channels that the CF-TDSR can allocate is assumed, but the demonstrated method only needs a limited number of channels. A powerful hacker can launch multiple and sequential TDS attacks.

Figure 8.2 shows the results of the experiment. Figure 8.2(a) describes the attack that was launched: the red dashed line denotes a TDS attack on the first channel that occurs at time 1-3 seconds with a delay of 4 seconds, followed by a TDS attack on channel 2 between 3-4 seconds with a delay of 2.5 seconds (blue dashed line), then a TDS attack on channel 3 between 9-20 seconds (green dashed line), and a TDS attack on channel 4, with a delay of 9 seconds, from time 25 seconds to 50 seconds. Figure 8.2(b) shows that the CF-TDSR detects each attack and requests a change of channel. The attack on channel 4 is not effective, because the system has already approached the stable region. The conclusion is that when the system is at optimal value (close to zero), it is more difficult for the TDS to destabilize the system and force the CF-TDSR to request an additional channel. Furthermore, the CF-TDSR quickly detects the attacks on different channels.

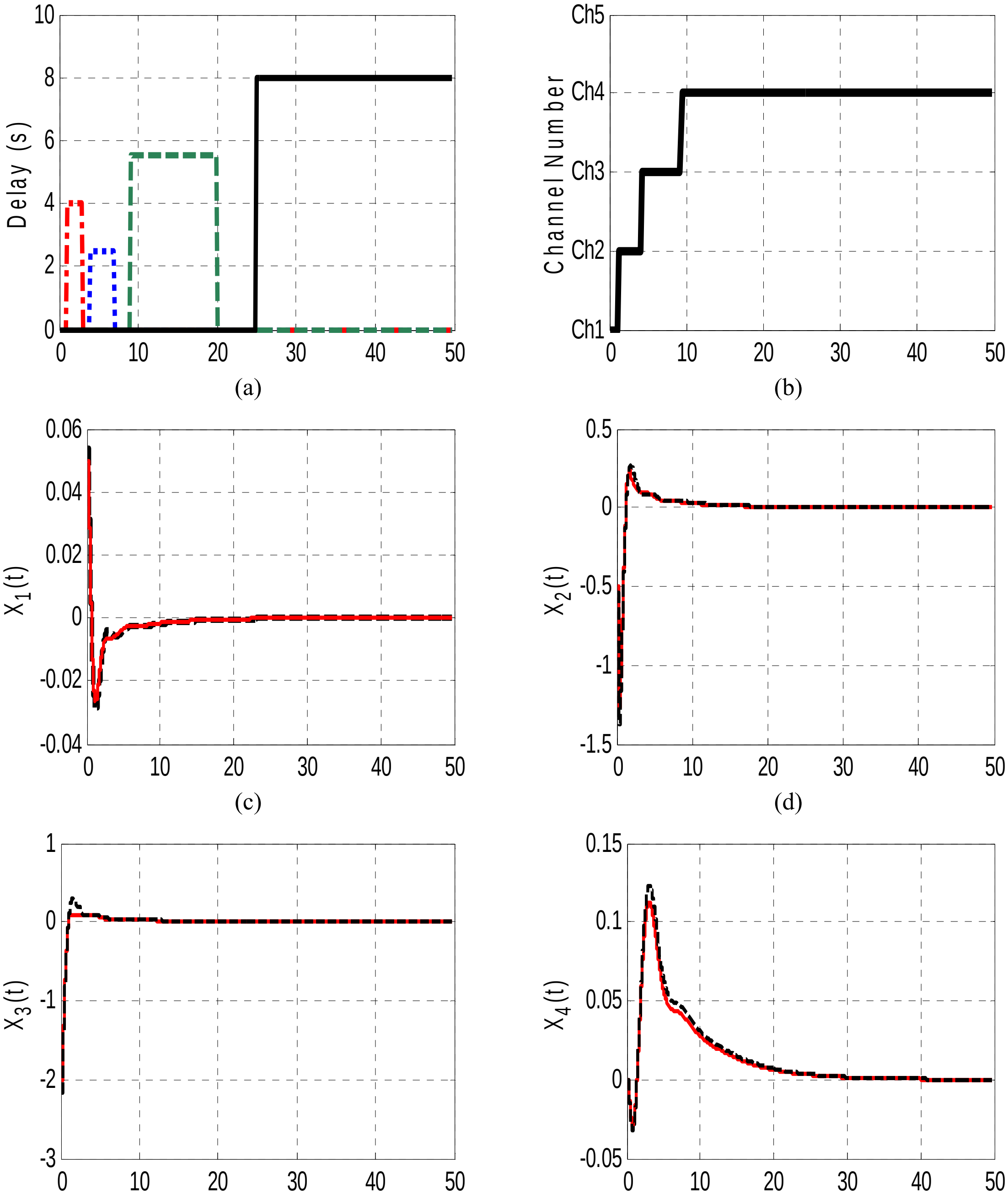
Figure 8.2(c) shows the frequency deviation, Δf^{K}, of the power system. Figure 8.2(d) shows the power deviation of the generator, Δf_{g}^{K}. Figure 8.2(e) shows the value position of the turbine, Δf_{tu}^{K}. Figure 8.2(f) shows Tie-line power flow, Δf_{pf}^{I}. These figures are proof that the states remain stable and converge to zero under a TDS attack. Figures 8.2(c)-8.2(f) compared a scenario where the state estimator is on (CF-TDSR, the red line) to the results of a scenario where the state estimator is off (black dashed line) with an unlimited number of communication channels. In both cases, the time-delay estimator and channel adaptation are on. The figures show that the CF-TDSR is clearly superior. The results show that the cost function value is improved, $\Delta J = 5.21$, when the state estimator is running and take cares of the TDS attack until a new channel is added to the system.

Composite TDS Attack

In the second investigation, a case is simulated where a hacker attacks the third state of the first and the second power areas. In this scenario, only two communication channels are available. The third state of each area provides the feedback and is ideal for the TDS attack. The attack starts at $t_a = 1$ second for the first power area, and at $t_a = 3$ seconds for the second time area, with time-delay values of $t_{d3} = 1.5$seconds (the third state of the first plant) and $t_{d8} = 3$ seconds, respectively. Figure 8.3(a) illustrates the TDS attack that was implemented.

The behavior of the LFC distributed power system under attack in three scenarios was evaluated. The first scenario called the “Baseline” runs without any modification to the communication protocol and to the controller. The second scenario called the “Adaptive” evaluates the LFC under the attack using an adaptive communication protocol. The third scenario evaluates the LFC system using the CF-TDSR, i.e., using both the adaptive communication protocol and controller design defenses.

In Figure 8.2, the *x* axis denotes the time. (a) Illustration of a sophisticated, sequential, and multi-channel attack: Each of the 4 bumps corresponds to a TDS attack launched on a different channel. (b) Evolution in time of CF-TDSR: The time when the CF-TDSR detects each attack, and requests to change the channel. The attack on channel 4 is not effective because the system has already approached the stable region. (c) The frequency deviation of the power system during the attacks. (d) The power deviation of the generator during the attacks. (e) Evolution in time of the value position of the turbine during the attacks. (f) Tie-line power flow during the attack. Figures 8.2(c) to 8.2(f) compare the CF-TDSR (red line) to a version where the state estimator is off (black line). The CF-TDSR greatly improves over a state estimator-free version.



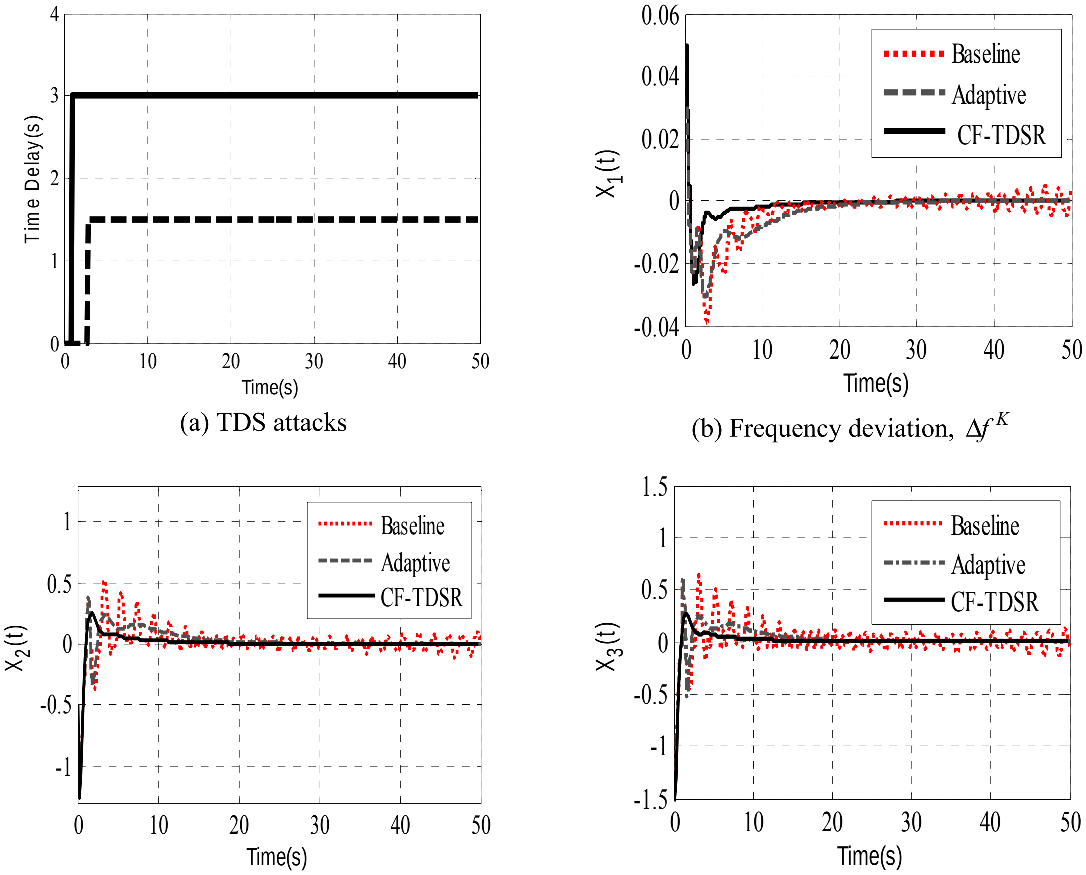
(a) (b)

(c) (d)

(e) (f)

Figure 8.2: TDS Attack on one Power Area

Figure 8.3 shows that the CF-TDSR is capable of detecting the TDS attack, and of quickly adapting the communication protocol. Note that when the CF-TDSR detects a delay larger than 0.4 sec, it sends a NACK to the sender, as suggested by the study of eigenvalues for the stability of the system [4]. Figure 8.3 (b)-(f) shows the frequency deviation, the power deviation of the generator, the value position of the turbine, and the tie-line power flow of the first power area, respectively. The figure shows that the system becomes stable only when using the CF-TDSR. The results show that the CF-TDSR works very well, even with strict limitations on the number of available channels, when all states converge to zero as expected.

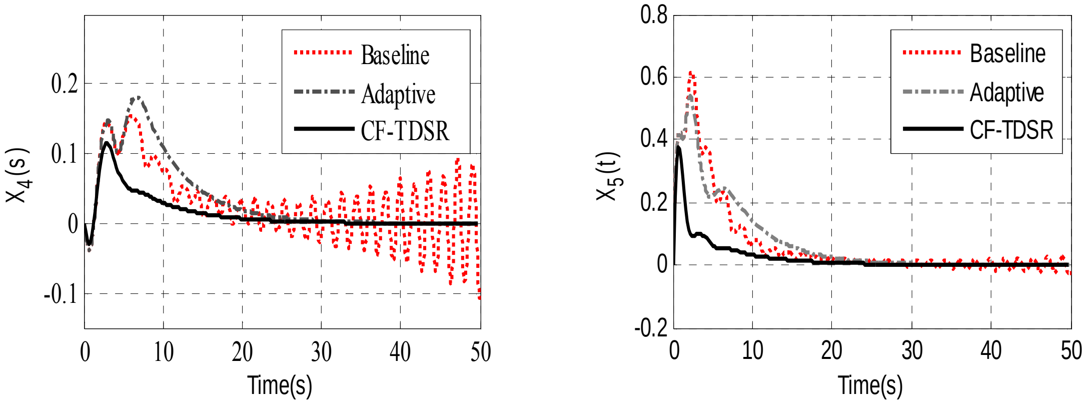


(a) TDS attacks

(b) Frequency deviation, Δf^{K}

(c) Power deviation of generator, ΔP_{g}^{K}

(d) Value position of the turbine, ΔP_{tu}^{K}



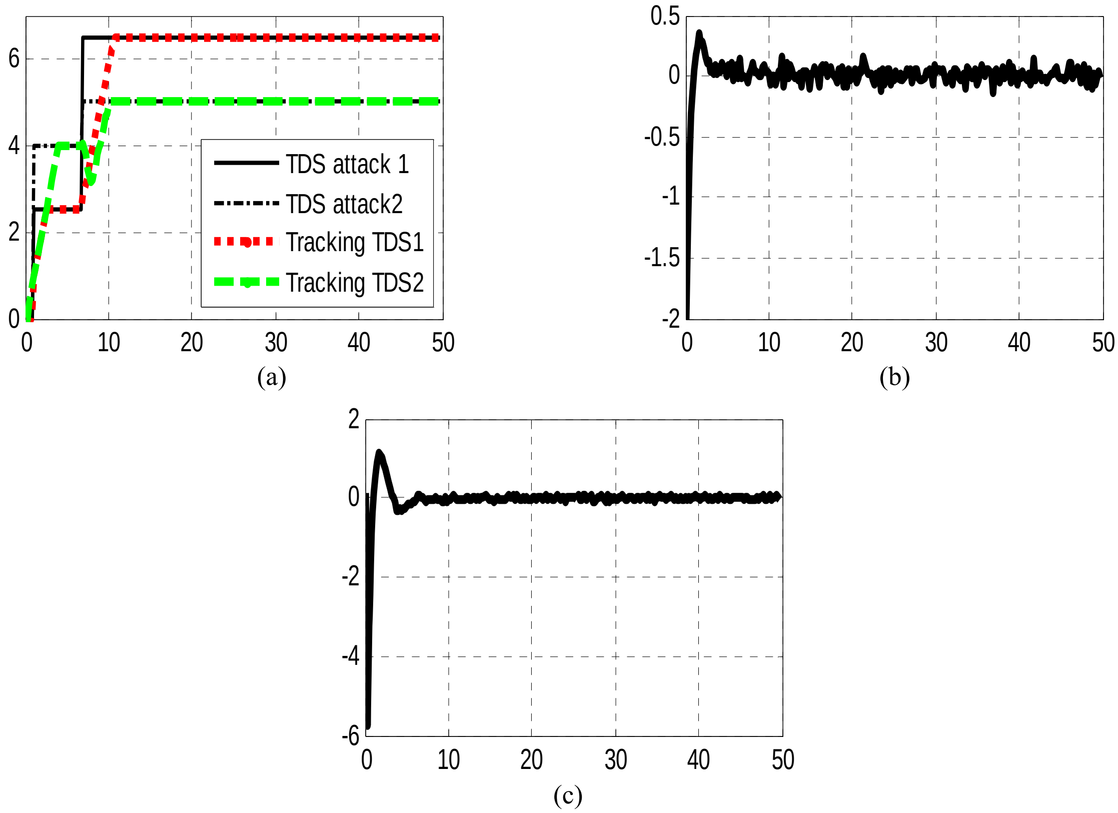
(e) Tie-line power flow, ΔP_{pf}^{1}

(f) control error

Figure 8.3: Composite TDS Attack on one State of Two-Power Area Plant

Concurrent TDS Attack for the Noisy System and Limited Available Channel

In the final experiment, the system behavior under the noise is studied. In order to accomplish this, first, 20% of white Gaussian noise is added to the communication channel. Then, a TDS attack is launched on both power areas: The attacker simultaneously launches the attack on the third state of both the first and the second power areas at time 1 second and 4 sec, with a 2-second delay. Then, the delay value is increased at time 7 sec to the value of 5 sec and 6.5 sec. In this experiment, the availability of a single communication channel is assumed. This assumption severely restricts the CF-TDSR's options. Figure 8.4 shows that even under such restrictions, the CF-TDSR is able to accurately detect and prevent the noise-based TDS attack. More specifically, Figure 8.4 (a) shows how the CF-TDSR detects and tracks the TDS attack in real time. Figures 8.4 (b) and 8.4 (c) show the third state of the first and second power areas under the noise-based TDS attack. They show that the CF-TDSR performs very well, even in the absence of additional communication channels.



(a)

(b)

(c)

Figure 8.4: TDS Attack Injected at the Same Time on Both Power Areas

8.6 Conclusion

Industrial control systems share information via a variety of communication protocols, making them vulnerable to attack by hackers at any infrastructure point. In this article, the time delay attacks were the main focus. The CF-TDSR, a communication protocol that uses adaptive channel redundancy techniques, was developed, as well as a novel state estimator to detect and obviate instable effects of a TDS attack. It was demonstrated that the CF-TDSR enabled the linear time-invariant control systems to achieve stability. The simulation experiments show the CF-TDSR enabling the multi-area load frequency control component to quickly stabilize the system under a suite of TDS attacks.

CHAPTER 9

CONCLUSION AND FUTURE WORKS

9.1 Conclusion

Based on a literature review and reviewing various types of attacks and failures in NCSs, it was found that the security of industrial control systems is very important and should be studied by researchers. Important fundamental knowledge about NCS and the security of those systems was discovered, a general attack model for the NCS was introduced.

In the third chapter, the time-delay effects of an SVPWM-based switching pattern for a grid-connected three-phase current source inverter were studied. An algorithm was proposed to track the time delay in real time to overcome the effects of time delays produced in the sensing loop. This guarantees synchronization between the grid phase and inverter output. An observer state feedback controller was applied to overcome the effects of time delays in the control signal. An optimal control design for systems with natural time delay was studied to show that controlling such systems is quite complex and is the reason most researchers ignore time delay in their control design process.

In the following chapter, a new type of attack is introduced, called the TDS attack, to the NCS. The stability analysis of a NCS during a TDS attack is studied mathematically, and the effects of TDS attacks on two different applications are simulated. First, the LFC power system under a TDS attack was modeled using hybrid systems, and the TDS attacks are formulated as switch action “Off/Delay-by-τ” sensing channels or control inputs. Then, the destabilizing action of TDS attacks on power systems was studied by using methods from hybrid systems theories. A two-area LFC LTI model was simulated to evaluate the effects of TDS attacks. The results show that TDS attacks affect the dynamic performance of the LFC system, and in many cases, could destroy the system's stability, which can be launched at any time during the operation of the power system. For the second application, we applied a TDS attack on a wireless pacemaker, and then simulated the results by creating a nonlinear dynamic model of system. We showed that TDS attacks can cause stability issues in NCS.

Afterward, a method to track and detect the TDS attack on NCS was proposed. This detection method was used to alert monitoring centers like SCADA, as well as to overcome stability issues of TDS attacks in the following chapters. Based on this detection method, a simple method for preventing a time-delay switch attack on networked control systems was demonstrated. The method relied on a time-delay estimator that estimates and tracks time delays introduced by a hacker. With knowledge of the tolerable time delay of the control system, for which the plant remains stable and secure, the time-delay detector compares the estimated time delay to the tolerable time delay and issues an alarm signal when the estimated time delay is larger than the tolerable time delay. It also directs the system to an alarm state. In an alarm state, the plant is under the control of the emergency controller, local to the plant. The plant remains in this mode until the networked control system state is restored and the time-delay switch is eliminated. This method is simple and is an inexpensive way to assure that an industrial control system remains stable and secure.

In the Chapter 6, the ability to control LTI systems with variable time delays either occurring naturally or as a result of a time-delay attack by a hacker was demonstrated. The ability to track TDS attacks with the proposed method described in Chapter 5 was also demonstrated. One specific type of delay, that is, the delay in the observed state of the controlled system, was addressed. The only system that was examined was the LTI system in state feedback. This method is general, and in the future, further research will show that it works for a class of nonlinear systems.

In the last chapter, a new protocol called CF-TDSR was proposed to overcome TDS attack effects on NCSs. The CF-TDSR was developed, which is a communication protocol that uses adaptive channel redundancy techniques and a novel state estimator to detect and obviate the destabilizing effects of TDS attacks. The CF-TDSR enabled the linear time invariant control systems to achieve stability. The proposed protocol on the LFC system was simulated, and the simulation experiments showed that CF-TDSR enables the multi-area load frequency control component to quickly stabilize following a suite of powerful TDS attacks.

9.2 Future Works

In this research, we focused on TDS attacks injected into the NCS and specialty feedback lines where a plant sends output signals to the controller through a communication channel. In the future, the effects of TDS attacks on different parts of NCS, such as the control signal and referenced signal, will be studied. A TDS attack might cause stability and ineffectual issues in NCSs that should be adjusted based on other control systems. Delaying the reference signal could cause stability problems for all control systems.

A general attack model for NCSs was introduced; however, only TDS attacks were studied. Future research will involve studying a combination of attacks such as DoS, TDS and FDI attacks. In this case, a primary requisite is the classification of attacks; another important requisite is to design a controller to be robust under these combinations of attacks. It is believed that the extension of the proposed method will stabilize the NCS under a combination of attacks or other types of attacks.

A method to detect and track TDS attacks on LTI systems was proposed. Additional future work will involve the extension of the TDS attack detection method for nonlinear systems. Subsequently, a nonlinear system will not need to be linearized, hence, the results would be more accurate.

The last recommendation for future work involves an extension of the proposed protocol to reduce and optimize the number of extra communication channels necessary by changing the transmission sampling time. This technique allows the controller to obtain the necessary information with less delay. Hence, this work needs an optimization algorithm to allocate other communication channels and/or change the sampling time of the transceiver and receiver with the cost and time savings in mind.

REFERENCES

[1] S. Gorman, "Electricity grid in US penetrated by spies," *The Wall Street Journal,* vol. 8, 2009.

[2] H. Pidd, "India blackouts leave 700 million without power," *The guardian,* vol. 31, 2012.

[3] J. Slay and M. Miller, *Lessons learned from the maroochy water breach*: Springer, 2008.

[4] P. Quinn-Judge, "Cracks in the system," *TIME Magazine (January 9, 2002),* 2002.

[5] J. Leyden, "Polish teen derails tram after hacking train network," *The Register,* vol. 11, 2008.

[6] F.-Y. Wang and D. Liu, *Networked control systems*: Springer, 2008.

[7] Y. W. Law, T. Alpcan, and M. Palaniswami, "Security Games for Risk Minimization in Automatic Generation Control," 2015.

[8] J. Weiss, "Industrial Control System (ICS) cyber security for water and wastewater systems," in *Securing Water and Wastewater Systems*, ed: Springer, 2014, pp. 87-105.

[9] Y. Liu, Ning, P., & Reiter, M. K, "False data injection attacks against state estimation in electric power grids," in *the 16th ACM conference on Computer and communications security*, New York, 2009.

[10] A. Teixeira, Amin, S., Sandberg, H., Johansson, K. H., & Sastry, S. S, "Cyber security analysis of state estimators in electric power systems," in *the Decision and Control (CDC)*, 2010.

[11] O. Kosut, Liyan, J., Thomas, R. J., & Lang, T, "Malicious Data Attacks on the Smart Grid. Smart Grid," *IEEE Transactions* pp. 645-658, 2011.

[12] S. Amin, Cardenas, A. A., & Sastry, S. S, "Safe and Secure Networked Control Systems under Denial-of-Service Attacks," in *the 12th International Conference on Hybrid Systems: Computation and Control*, San Francisco, 2009.

[13] S. Liu, Liu, X. P., & Saddik, A. E, "Denial-of-Service (dos) attacks on load frequency control in smart grids," in *Innovative Smart Grid Technologies (ISGT), IEEE PES*, 2013.

[14] P. M. Esfahani, Vrakopoulou, M., Margellos, K., Lygeros, J., & Andersson, G, "A robust policy for automatic generation control cyber attack in two area power network," in *The Decision and Control (CDC)*, 2010.

[15] Y. Tan, "Time-varying time-delay estimation for nonlinear systems using neural networks," *International Journal of Applied Mathematics and Computer Science,* vol. 14, pp. 63-68, 2004.

[16] T. J. Lim and M. D. Macleod, "Adaptive algorithms for joint time delay estimation and IIR filtering," *Signal Processing, IEEE Transactions on,* vol. 43, pp. 841-851, 1995.

[17] F. Reed, P. L. Feintuch, and N. J. Bershad, "Time delay estimation using the LMS adaptive filter--static behavior," *Acoustics, Speech and Signal Processing, IEEE Transactions on,* vol. 29, pp. 561-571, 1981.

[18] X. Li, X. Liang, R. Lu, X. Shen, X. Lin, and H. Zhu, "Securing smart grid: cyber attacks, countermeasures, and challenges," *Communications Magazine, IEEE,* vol. 50, pp. 38-45, 2012.

[19] J. Di-Battista, J.-C. Courrege, B. Rouzeyre, L. Torres, and P. Perdu, "When failure analysis meets side-channel attacks," in *Cryptographic Hardware and Embedded Systems, CHES 2010*, ed: Springer, 2010, pp. 188-202.

[20] A. Moradi, O. Mischke, C. Paar, Y. Li, K. Ohta, and K. Sakiyama, "On the power of fault sensitivity analysis and collision side-channel attacks in a combined setting," in *Cryptographic Hardware and Embedded Systems–CHES 2011*, ed: Springer, 2011, pp. 292-311.

[21] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *Smart Grid, IEEE Transactions on,* vol. 2, pp. 382-390, 2011.

[22] Y. Yuan, Z. Li, and K. Ren, "Quantitative analysis of load redistribution attacks in power systems," *Parallel and Distributed Systems, IEEE Transactions on,* vol. 23, pp. 1731-1738, 2012.

[23] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli, "False data injection attacks against state estimation in wireless sensor networks," in *Decision and Control (CDC), 2010 49th IEEE Conference on*, 2010, pp. 5967-5972.

[24] W. Wang, Y. Xu, and M. Khanna, "A survey on the communication architectures in smart grid," *Computer Networks,* vol. 55, pp. 3604-3629, 2011.

[25] A. Proano and L. Lazos, "Selective jamming attacks in wireless networks," in *Communications (ICC), 2010 IEEE International Conference on*, 2010, pp. 1-6.

[26] U. K. Premaratne, J. Samarabandu, T. S. Sidhu, R. Beresh, and J.-C. Tan, "An intrusion detection system for IEC61850 automated substations," *Power Delivery, IEEE Transactions on,* vol. 25, pp. 2376-2383, 2010.

[27] E. D. Knapp and R. Samani, *Applied Cyber Security and the Smart Grid: Implementing Security Controls Into the Modern Power Infrastructure*: Newnes, 2013.

[28] D. Jin, D. M. Nicol, and G. Yan, "An event buffer flooding attack in DNP3 controlled SCADA systems," in *Proceedings of the Winter Simulation Conference*, 2011, pp. 2619-2631.

[29] D. Lee, H. Kim, K. Kim, and P. D. Yoo, "Simulated Attack on DNP3 Protocol in SCADA System," in *2014 Symposium on Cryptography and Information Security (SCIS 2014)*, 2014.

[30] S. East, J. Butts, M. Papa, and S. Shenoi, "A Taxonomy of Attacks on the DNP3 Protocol," in *Critical Infrastructure Protection III*, ed: Springer, 2009, pp. 67-81.

[31] S. Ranjan, R. Swaminathan, M. Uysal, A. Nucci, and E. Knightly, "DDoS-shield: DDoS-resilient scheduling to counter application layer attacks," *IEEE/ACM Transactions on Networking (TON),* vol. 17, pp. 26-39, 2009.

[32] X. Carcelle, *Power line communications in practice*: Artech House, 2009.

[33] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "The EM Side-Channel (s): Attacks and Assessment Methodologies, IBM report," ed.

[34] O. Meynard, S. Guilley, J.-L. Danger, Y.-I. Hayashi, and N. Homma, "Characterization of the Information Leakage of Cryptographic Devices by Using EM Analysis."

[35] M. Enev, S. Gupta, T. Kohno, and S. N. Patel, "Televisions, video privacy, and powerline electromagnetic interference," in *Proceedings of the 18th ACM conference on Computer and communications security*, 2011, pp. 537-550.

[36] Y.-i. Hayashi, T. Sugawara, Y. Kayano, N. Homma, T. Mizuki, A. Satoh*, et al.*, "An Analysis of Information Leakage from a Cryptographic Hardware via Common-Mode Current," 2009.

[37] Y.-i. Hayashi, T. Sugawara, Y. Kayano, N. Homma, T. Mizuki, A. Satoh*, et al.*, "Information leakage from cryptographic hardware via common-mode current," in *Electromagnetic Compatibility (EMC), 2010 IEEE International Symposium on*, 2010, pp. 109-114.

[38] Y.-i. Hayashi, N. Homma, T. Mizuki, T. Sugawara, Y. Kayano, S. MINEGISHI*, et al.*, "Evaluation of information leakage from cryptographic hardware via common-mode current," *IEICE transactions on electronics,* vol. 95, pp. 1089-1097, 2012.

[39] H. Bar-El, "Introduction to side channel attacks," *Discretix Technologies Ltd,* vol. 43, 2003.

[40] A. Sargolzaei, M. Jamei, K. Yen, A. I. Sarwat, and M. Abdelghani, "Active/Reactive Power Control of Three Phase Grid Connected Current Source Boost Inverter Using Particle Swarm Optimization," in *Progress in Systems Engineering*, ed: Springer, 2015, pp. 141-146.

[41] H. Heydari and A. H. Moghadasi, "Optimization scheme in combinatorial UPQC and SFCL using normalized simulated annealing," *Power Delivery, IEEE Transactions on,* vol. 26, pp. 1489-1498, 2011.

[42] D. Shen and P. Lehn, "Modeling, analysis, and control of a current source inverter-based STATCOM," *Power Delivery, IEEE Transactions on,* vol. 17, pp. 248-253, 2002.

[43] Y. Matsuda, T. Maeda, and T. Matsumura, "Current source inverter," ed: Google Patents, 1979.

[44] S. Sato, "Current source inverter," ed: Google Patents, 2014.

[45] F. Wang, W. Shen, D. Boroyevich, S. Ragon, V. Stefanovic, and M. Arpilliere, "Voltage source inverter," *Industry Applications Magazine, IEEE,* vol. 15, pp. 24-33, 2009.

[46] M. Malinowski, K. Gopakumar, J. Rodriguez, and M. A. Perez, "A survey on cascaded multilevel inverters," *Industrial Electronics, IEEE Transactions on,* vol. 57, pp. 2197-2206, 2010.

[47] J. Rodriguez, J.-S. Lai, and F. Z. Peng, "Multilevel inverters: a survey of topologies, controls, and applications," *Industrial Electronics, IEEE Transactions on,* vol. 49, pp. 724-738, 2002.

[48] K. Kandasamy and S. K. Sahoo, "A Review of Matrix Converter and Novel Control Method of DC-AC Matrix Converter," *ijm,* vol. 1, p. 1, 2013.

[49] A. K. Sahoo, K. Basu, and N. Mohan, "Comparison of filter components of back-to-back and matrix converter by analytical estimation of ripple quantities," in *Industrial Electronics Society, IECON 2013-39th Annual Conference of the IEEE*, 2013, pp. 4831-4837.

[50] A. VanderMeulen and J. Maurin, "Current source inverter vs. Voltage source inverter topology," *Technical Data TD02004004E, Eaton,* 2010.

[51] C. Klumpner, "A new single-stage current source inverter for photovoltaic and fuel cell applications using reverse blocking IGBTs," in *Power Electronics Specialists Conference, 2007. PESC 2007. IEEE*, 2007, pp. 1683-1689.

[52] B. Mirafzal, M. Saghaleini, and A. K. Kaviani, "An SVPWM-based switching pattern for stand-alone and grid-connected three-phase single-stage boost

inverters," *Power Electronics, IEEE Transactions on,* vol. 26, pp. 1102-1111, 2011.

[53] H.-P. To, M. F. Rahman, and C. Grantham, "Time delay compensation for a DSP-based current-source converter using observer-predictor controller," in *Power Electronics and Drive Systems, 2007. PEDS'07. 7th International Conference on*, 2007, pp. 1091-1096.

[54] M. Saghaleini and B. Mirafzal, "Power control in three-phase grid-connected current-source boost inverter," in *Energy Conversion Congress and Exposition (ECCE), 2011 IEEE*, 2011, pp. 776-783.

[55] K. Ogata, *Discrete-time control systems* vol. 2: Prentice Hall Englewood Cliffs, NJ, 1995.

[56] M. Jamshidi and C. Wang, "A computational algorithm for large-scale nonlinear time-delay systems," *IEEE transactions on systems, man, and cybernetics,* vol. 14, pp. 2-9, 1984.

[57] A. Hermant, "Optimal control of the atmospheric reentry of a space shuttle by an homotopy method," *Optimal Control Applications and Methods,* vol. 32, pp. 627-646, 2011.

[58] R. Luus, X. Zhang, F. Hartig, and F. J. Keil, "Use of piecewise linear continuous optimal control for time-delay systems," *Industrial & engineering chemistry research,* vol. 34, pp. 4136-4139, 1995.

[59] J.-N. Yang, "Application of optimal control theory to civil engineering structures," *Journal of the engineering Mechanics Division,* vol. 101, pp. 819-838, 1975.

[60] O. Von Stryk and R. Bulirsch, "Direct and indirect methods for trajectory optimization," *Annals of operations research,* vol. 37, pp. 357-373, 1992.

[61] R. Bellman, "On the theory of dynamic programming," *Proceedings of the National Academy of Sciences of the United States of America,* vol. 38, p. 716, 1952.

[62] L. Pontryagin, "Optimal control processes," *Usp. Mat. Nauk,* vol. 14, 1959.

[63] R. W. Beard, G. N. Saridis, and J. T. Wen, "Galerkin approximations of the generalized Hamilton-Jacobi-Bellman equation," *Automatica,* vol. 33, pp. 2159-2177, 1997.

[64] G. Y. Tang, H. Y. Sun, and Y. M. Liu, "OPTIMAL TRACKING CONTROL FOR DISCRETE TIME-DELAY SYSTEMS WITH PERSISTENT DISTURBANCES," *Asian Journal of Control,* vol. 8, pp. 135-140, 2006.

[65] G. Tang and Y. Zhao, "Optimal control of nonlinear time-delay systems with persistent disturbances," *Journal of optimization theory and applications,* vol. 132, pp. 307-320, 2007.

[66] C. Goh and K. Teo, "Control parametrization: a unified approach to optimal control problems with general constraints," *Automatica,* vol. 24, pp. 3-18, 1988.

[67] F. Shakeri and M. Dehghan, "Solution of delay differential equations via a homotopy perturbation method," *Mathematical and computer Modelling,* vol. 48, pp. 486-498, 2008.

[68] A. Jajarmi, "Optimal control of nonlinear systems using the homotopy perturbation method: Infinite horizon case," *International Journal of Digital Content Technology and its Applications,* vol. 4, 2010.

[69] F. Khellat, "Optimal control of linear time-delayed systems by linear Legendre multiwavelets," *Journal of optimization theory and applications,* vol. 143, pp. 107-121, 2009.

[70] A. Greenberg, "Hackers cut cities' power," *Forbes, Jaunuary,* 2008.

[71] J. Meserve, "Sources: Staged cyber attack reveals vulnerability in power grid," *CNN. com,* vol. 26, 2007.

[72] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, and S. Sastry, "Challenges for securing cyber physical systems," in *Workshop on future directions in cyber-physical systems security*, 2009.

[73] J. Vijayan, "Stuxnet renews power grid security concerns," *Computerworld, Jul,* vol. 26, 2010.

[74] E. Byres and J. Lowe, "The myths and facts behind cyber security risks for industrial control systems," in *Proceedings of the VDE Kongress*, 2004, pp. 213-218.

[75] A. A. Cárdenas, S. Amin, and S. Sastry, "Research Challenges for the Security of Control Systems," in *HotSec*, 2008.

[76] A. Benzaouia, M. Ouladsine, A. Naamane, and B. Ananou, "Fault detection for uncertain delayed switching discrete-time systems," *International Journal of Innovative Computing, Information and Control,* vol. 8, pp. 8049-8062, 2012.

[77] A. Sargolzaei, K. Yen, and M. Abdelghani, "Delayed inputs attack on load frequency control in smart grid," in *Innovative Smart Grid Technologies Conference (ISGT), 2014 IEEE PES*, 2014, pp. 1-5.

[78] C.-K. Zhang, L. Jiang, Q. Wu, Y. He, and M. Wu, "Delay-dependent robust load frequency control for time delay power systems," in *Power and Energy Society General Meeting (PES), 2013 IEEE*, 2013, pp. 1-1.

[79] G. H. Golub and C. F. Van Loan, *Matrix computations* vol. 3: JHU Press, 2012.

[80] W. R. Evans, "Control system synthesis by root locus method," *American Institute of Electrical Engineers, Transactions of the,* vol. 69, pp. 66-69, 1950.

[81] J. Monreal, I. Benítez, L. Moreno, A. Lluna, and I. Díaz, "A review of linear advanced current control techniques for grid connected PV inverters," in *International conference on renewable energies and power quality (ICREPQ)*, 2009.

[82] P. E. McSharry, G. Clifford, L. Tarassenko, and L. A. Smith, *Method for generating an artificial RR tachogram of a typical healthy human over 24-hours*: IEEE, 2002.

[83] M. Brennan, M. Palaniswami, and P. Kamen, "A new cardiac nervous system model for heart rate variability analysis," in *Engineering in Medicine and Biology*

Society, 1998. Proceedings of the 20th Annual International Conference of the IEEE, 1998, pp. 349-352.

[84] E. Zeeman, "Differential equations for the heartbeat and nerve impulse," *Towards a theoretical biology,* vol. 4, pp. 8-67, 1972.

[85] R. Suckley and V. N. Biktashev, "Comparison of asymptotics of heart and nerve excitability," *Physical Review E,* vol. 68, p. 011902, 2003.

[86] P. N. Tu and P. N. Tu, *Dynamical systems: an introduction with applications in economics and biology*: Springer Berlin, 1994.

[87] D. S. Jones, M. Plank, and B. D. Sleeman, *Differential equations and mathematical biology*: CRC press, 2009.

[88] N. Jafarnia-Dabanloo, D. McLernon, H. Zhang, A. Ayatollahi, and V. Johari-Majd, "A modified Zeeman model for producing HRV signals and its application to ECG signal generation," *Journal of theoretical biology,* vol. 244, pp. 180-189, 2007.

[89] B. Van der Pol and J. Van der Mark, "LXXII. The heartbeat considered as a relaxation oscillation, and an electrical model of the heart," *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science,* vol. 6, pp. 763-775, 1928.

[90] W. Thanom and R. N. Loh, "Nonlinear control of heartbeat models," *Journal on Systemics, Cybernetics and Informatics,* vol. 9, pp. 21-27, 2011.

[91] B. News, "Tiny, wireless pacemaker due to be launched in Europe," in *BBC*, ed. http://www.bbc.com/news/technology-24535624, 2013.

[92] R. P. A. J. FINKLE, "FDA urges protection of medical devices from cyber threats," http://www.reuters.com/article/2013/06/14/us-devices-cybersecurity-fda-idUSBRE95C1IB201306142013.

[93] H. Benéıtez-Péerez, A. Benéıtez-Péerez, and J. Ortega-Arjona, "Networked control systems design considering scheduling restrictions and local faults,"

International Journal of Innovative Computing, Information and Control, vol. 8, pp. 8515-8526, 2012.

[94] H. K. Khalil and J. Grizzle, *Nonlinear systems* vol. 3: Prentice hall New Jersey, 1996.

[95] A. E. Max Lambert, Matt Dyer, Ben Byer [Online].

[96] D. Dotta and I. Decker, "Wide-area measurements-based two-level control design considering signal transmission delay," *Power Systems, IEEE Transactions on,* vol. 24, pp. 208-216, 2009.

[97] Y. Li, S. Tong, and Y. Li, "Observer-based adaptive fuzzy backstepping control for strict-feedback stochastic nonlinear systems with time delays," *International Journal of Innovative Computing, Information and Control,* vol. 8, pp. 8103-8114, 2012.

[98] A. Sargolzaei, K. K. Yen, S. Noei, and H. Ramezanpour, "Assessment of He's homotopy perturbation method for optimal control of linear time-delay systems," *Applied Mathematical Sciences,* vol. 7, pp. 349-361, 2013.

[99] I. Kamwa, R. Grondin, and Y. Hébert, "Wide-area measurement based stabilizing control of large power systems-a decentralized/hierarchical approach," *Power Systems, IEEE Transactions on,* vol. 16, pp. 136-153, 2001.

[100] H. Wu, K. S. Tsakalis, and G. T. Heydt, "Evaluation of time delay effects to wide-area power system stabilizer design," *Power Systems, IEEE Transactions on,* vol. 19, pp. 1935-1941, 2004.

[101] J. Quanyuan, Z. Zhenyu, and C. Yijia, "Wide-area TCSC controller design in consideration of feedback signals' time delays," in *Power Engineering Society General Meeting, 2005. IEEE*, 2005, pp. 1676-1680.

[102] M. S. Saad, M. A. Hassouneh, E. H. Abed, and A. Edris, "Delaying instability and voltage collapse in power systems using SVCs with washout filter-aided feedback," in *American Control Conference, 2005. Proceedings of the 2005*, 2005, pp. 4357-4362.

[103] B. Chaudhuri, R. Majumder, and B. C. Pal, "Wide-area measurement-based stabilizing control of power system considering signal transmission delay," *Power Systems, IEEE Transactions on,* vol. 19, pp. 1971-1979, 2004.

[104] F. Milano and M. Anghel, "Impact of time delays on power system stability," *Circuits and Systems I: Regular Papers, IEEE Transactions on,* vol. 59, pp. 889-900, 2012.

[105] S. Ray and G. K. Venayagamoorthy, "Real-time implementation of a measurement-based adaptive wide-area control system considering communication delays," *IET generation, transmission & distribution,* vol. 2, pp. 62-70, 2008.

[106] M. T. Alrifai, M. Zribi, M. Rayan, and M. S. Mahmoud, "On the control of time delay power systems," *International Journal of Innovative Computing, Information and Control,* vol. 9, pp. 769-792, 2013.

[107] L. Schenato, "Optimal estimation in networked control systems subject to random delay and packet drop," *Automatic Control, IEEE Transactions on,* vol. 53, pp. 1311-1317, 2008.

[108] M. S. Mahmoud, *Robust control and filtering for time-delay systems*: CRC Press, 2000.

[109] L. Chunmao and X. Jian, "Adaptive delay estimation and control of networked control systems," in *Communications and Information Technologies, 2006. ISCIT'06. International Symposium on*, 2006, pp. 707-710.

[110] N. Sadeghzadeh, A. Afshar, and M. B. Menhaj, "An MLP neural network for time delay prediction in networked control systems," in *Control and Decision Conference, 2008. CCDC 2008. Chinese*, 2008, pp. 5314-5318.

[111] K. J. Åström and T. Hägglund, *Advanced PID control*: ISA-The Instrumentation, Systems, and Automation Society; Research Triangle Park, NC 27709, 2006.

[112] K. Zhou, J. C. Doyle, and K. Glover, *Robust and optimal control* vol. 40: Prentice hall New Jersey, 1996.

[113] K. S. Narendra and A. M. Annaswamy, *Stable adaptive systems*: Courier Corporation, 2012.

[114] C. F. Cowan, P. M. Grant, and P. F. Adams, *Adaptive filters*: Prentice-Hall, 1985.

[115] J. Moren and C. Balkenius, "A computational model of emotional learning in the amygdala," *From animals to animats,* vol. 6, pp. 115-124, 2000.

[116] M. A. Shamsi-Nejad and M. R. Khalghani, "DVR control using adaptive PI controller based on human brain learning," in *Electrical Power Distribution Networks (EPDC), 2012 Proceedings of 17th Conference on*, 2012, pp. 1-7.

[117] S. Amin, A. A. Cárdenas, and S. S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in *Hybrid Systems: Computation and Control*, ed: Springer, 2009, pp. 31-45.

[118] Y. Mo and B. Sinopoli, "False data injection attacks in control systems," in *Preprints of the 1st workshop on Secure Control Systems*, 2010, pp. 1-6.

[119] J. Nilsson, "Real-time control systems with delays," Lund institute of Technology Lund, Sweden, 1998.

[120] S. Falasca, M. Gamba, and A. Bicchi, "Output-Feedback Dynamic Control over Packet-Switching Networks," in *Informatics in Control, Automation and Robotics*, ed: Springer, 2015, pp. 177-200.

[121] M. Ergen, S. Coleri, and P. Varaiya, "QoS aware adaptive resource allocation techniques for fair scheduling in OFDMA based broadband wireless access systems," *Broadcasting, IEEE Transactions on,* vol. 49, pp. 362-370, 2003.

[122] N. A. Odhah, E. S. Hassan, M. Abdelnaby, W. E. Al-Hanafy, M. I. Dessouky, S. A. Alshebeili*, et al.*, "Adaptive Resource Allocation Algorithms for Multi-user MIMO-OFDM Systems," *Wireless Personal Communications,* vol. 80, pp. 51-69, 2015.

[123] Q. Yang, D. An, and W. Yu, "On time desynchronization attack against IEEE 1588 protocol in power grid systems," in *Energytech, 2013 IEEE*, 2013, pp. 1-5.

[124] H. Jia, X. Yu, Y. Yu, and C. Wang, "Power system small signal stability region with time delay," *International Journal of Electrical Power & Energy Systems,* vol. 30, pp. 16-22, 2008.

VITA

ARMAN SARGOLZAEI

2010	B.S., Electrical and Computer Engineering Sadjad University of Technology Mashhad, Iran
2012	M.S., Electrical Engineering Florida International University Miami, Florida
2015	Ph.D. Candidate, Electrical Engineering Florida International University Miami, Florida

SELECTED PUBLICATIONS AND PRESENTATIONS

A. Sargolzaei, K K. Yen, and M. N. Abdelghani. "Control of Nonlinear Heartbeat Models under Time-Delay-Switched Feedback Using Emotional Learning Control.", International Journal on Recent Trends in Engineering & Technology, pp. 85-91,(2014)

A. Sargolzaei, K.K. Yen, and M.N. Abdelghani, "Time-Delay Switch Attack on Load Frequency Control in Smart Grid.", Advances in Communication Technology, pp. 55-64, (2013)

A. Sargolzaei, Kang K. Yen, Shirin Noei and Hamidreza Ramezanpour, "Assessment of He's Homotopy Perturbation Method for Optimal Control of Linear Time-Delay Systems.", Applied Mathematical Sciences, vol.7, no 8, pp. 349-361, (2013)

C. Lopez, A. Sargolzaei, H. Santana, C. Huerta, “Smart Grid Cyber Security: An Overview of Threats and Countermeasures”, Accepted for publication in Journal of Energy and Power System, (2015)

A. Sargolzaei, K. K Yen, K. Zeng, S. M. A. Motahari, and S. Noei, "Impulse Image Noise Reduction Using Fuzzy-Cellular Automata Method.", Published in the International Journal of Computer and Electrical Engineering, pp. 191-95, (2014)

A. Sargolzaei, K.K. Yen, and M.N. Abdelghani, "Preventing Time-Delay Switch Attack on Load Frequency Control in Distributed Power Grid", Second Revision, IEEE Transaction on Smart Grid, (2014)

S. Sargolzaei, A. Sargolzaei, M.Sc.; Mercedes Cabrerizo, Ph.D.; Gang Chen, Ph.D.; Mohammed Goryawala, Ph.D.; Alberto Pinzon-Ardila, M.D.; Sergio M. Gonzalez-Arias, M.D.; Malek Adjouadi, Ph.D, “Estimating Intracranial Volume in Brain Research: An Evaluation of Methods”, Accepted for publication at Neuroinformatics journal, (2015)

S. Sargolzaei, A. Sargolzaei, M. Cabrerizo, M. Goryawala, Q. Zhou, S. Noei, G. Chen, R. Duara, W. Barker and M. Adjouadi, “Intracranial volume estimation in patients with Alzheimer’s disease”, Accepted for publication in BMC Bioinformatics, (2014)

S. Sargolzaei, M. Cabrerizo, A. Sargolzaei, S. Noei, H. Rajaei, A. Salah Eddin, A. Pinzon-Ardila, S. M. Gonzalez Arias, P. Jayakar and M. Adjouadi, “A probabilistic approach for pediatric epilepsy diagnosis using brain functional connectivity networks”, Accepted for publication in BMC Bioinformatics, (2014)

H Sasani, H Ramezanpour, G Darmani, S Noei, A. Sargolzaei, "A MODAL SERIES REPRESENTATION OF GENESIO CHAOTIC SYSTEM.", Published in the International Journal of Instrumentation and Control Systems pp. 1-10, (2012)

S Noei, S Sargolzaei, H Ramezanpour and A. Sargolzaei, "Fuzzy-Cellular Automata Method for Noise Cancelation of Satellite and Radar Images and Maps.", Published in the International Journal of Emerging Technology and Advanced Engineering, pp. 404-408, (2012)

A. Jajarmi , H. Ramezanpour , A. Sargolzaei, P. Shafaei, "Optimal Control of Nonlinear Systems Using the Homotopy Perturbation Method: Infinite Horizon Case.", Published in the International Journal of Digital Content Technology and its Applications (JDCTA), pp. 114-122, (2010)

A. Sargolzaei, Amir Moghadasi, Kang Yen, Arif Sarwat, “Time-Delay Analysis on Grid-Connected Three-Phase Current Source Inverter based on SVPWM Switching”, Published in IEEE Symposium on Computational Intelligence Applications in Smart Grid, Orlando, USA, pp. 9-12, (2014)

A. Sargolzaei, Kang Yen, MN Abdelghani, "Delayed Inputs Attack on Load Frequency Control in Smart Grid.", Published in The Innovative Smart Grid Technologies (ISGT) conference, IEEE(PES), USA, pp. 19-22, (2014)

A. Sargolzaei, M Jamei, K.K. Yen, A. Sarwat "Active/Reactive Power Control of Three Phase Grid Connected Current Source Boost Inverter Using Particle Swarm Optimization.", Progress in Systems Engineering, Springer International Publishing, pp. 141-146, (2015).