6-14-2012

An Application of Con-Resistant Trust to Improve the Reliability of Special Protection Systems within the Smart Grid

Crystal M. Shipman

AN APPLICATION OF CON-RESISTANT TRUST TO IMPROVE THE RELIABILITY OF SPECIAL PROTECTION SYSTEMS WITHIN THE SMART GRID

THESIS

Crystal M. Shipman, Master Sergeant, USAF

AFIT/GCO/ENG/12-22

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/GCO/ENG/12-22

AN APPLICATION OF CON-RESISTANT TRUST TO IMPROVE THE RELIABILITY OF SPECIAL PROTECTION SYSTEMS WITHIN THE SMART GRID

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

in Partial Fulfillment of the Requirements for the

Degree of Master of Science

Crystal M. Shipman, BS

Master Sergeant, USAF

June 2012

AFIT/GCO/ENG/12-22

AN APPLICATION OF CON-RESISTANT TRUST TO IMPROVE THE RELIABILITY OF SPECIAL PROTECTION SYSTEMS WITHIN THE SMART GRID

Crystal M. Shipman, BS
Master Sergeant, USAF

Approved:

// Signed //	29 May 2012
Kenneth M. Hopkinson, PhD (Chairman)	Date
// Signed //	29 May 2012
Lt Col Jeffrey M. Hemmes, PhD (Committee Member)	Date
// Signed //	29 May 2012
Mr. Juan Lopez Jr., (Committee Member)	Date

AFIT/GCO/ENG/12-22

Abstract

This thesis explores an application of a con-resistant trust mechanism to improve the performance of communications-based special protection systems to further enhance their effectiveness and resiliency. New initiatives in the energy sector are paving the way for the emergent communications-based smart grid technology. Smart grids incorporate modern information technologies in an effort to be more reliable and efficient. However, with the benefits of this new technology comes added risk associated with threats and vulnerabilities of the technology as well as to critical infrastructure it supports. This research utilizes a con-resistant trust mechanism as a method to quickly identify malicious or malfunctioning (untrusted) protection system nodes in order to mitigate the resulting instabilities in the smart grid. The con-resistant trust mechanism enables protection system agent nodes to make trust assessments based off of the cooperative and defective behaviors the nodes exhibit. These behaviors are directly related to the frequency level each node reports during each time step. Nodes that are cooperating are given positive interaction trust values. Nodes that are defecting are given negative interaction trust values.

The feasibility and performance of this trust architecture is demonstrated through experiments comparing a simulated special protection system implemented with a con-resistant trust mechanism and without via an analysis of variance statistical model. The simulations yield positive results when implementing the con-resistant trust mechanism within the special protection system for the smart grid.

To my wonderful husband, my beautiful daughter, and my incredibly sweet son. Thank you for your unending love and support throughout this endeavor. Without it, completing the degree would not have been possible.

Acknowledgments

I would like to express my sincere appreciation to my research advisor, Dr. Kenneth Hopkinson and my committee members Lt. Col. Jeffrey M. Hemmes, and Mr. Juan Lopez Jr. for their patience, guidance, and support throughout the course of this research effort. A special thanks to Mr. Lopez for his advice, feedback, and direction that put me on a research path that allowed me to see the light at the end of the tunnel. Additionally, I am incredibly grateful for the many professors and fellow students who gave their time and effort to develop the knowledge required for this research. Special recognition and thanks goes to Maj Jose Fadul, Capt Keith Ross, Capt Addision Betances, and Mr. Nick Kerner. Without their assistance I would have not made it through. Finally, I would like to thank everyone in the Cyber Advanced Networking in Mobile Applications Laboratory (ANiMaL) especially Capt Kasperek, Capt Simpson, Capt Carbino, and Maj Ross for their support and camaraderie throughout this endeavor.

Crystal M. Shipman

Table of Contents

List of Figures

List of Tables

List of Abbreviations

An Application of Con-Resistant Trust to Improve the Reliability of Special Protection Systems within the Smart Grid

1 Introduction

1.1 Background

Threats of terrorist attacks and natural disasters highlight the importance of protecting, securing, and understanding the interdependencies of the nation's critical infrastructure (CI). Protecting and ensuring the continuity of critical infrastructure of the United States are essential to the nation's security, public health and safety, economic vitality and way of life [1]. Presidential directives have identified eighteen highly interconnected critical infrastructure key resource sectors, each of which depend on another to operate and function properly. Increasingly interconnected systems are vulnerable to threats brought on by sector dependence with the potential to trigger interrelated, cascading disturbances that can directly and indirectly affect the other infrastructures, impact geographic regions, and send ripples throughout the national and global economy [2], [3], [4].

The Energy sector in particular is highly depended upon by other sectors. This sector is responsible for the electrical power generation, transmission, and distribution of electrical power to customers. As the population of the United States grows, so does the demand for electrical power as well as the stress applied to the already antiquated power grid. Furthermore, Supervisory Control and Data Acquisition (SCADA) systems are the control systems used to monitor, operate, and control sensitive processes and physical functions of the power grid. Today's SCADA systems have been around for several

decades. They have evolved over the past 50 years from standalone, compartmentalized operations that were not concerned about security into intricately networked architectures that communicate across large distances [5]. These architectures have been upgraded to incorporate advanced information technology (IT) to improve overall process efficiency, productivity, and safety; however, security was never adequately addressed. While the basic architecture and design of the North American power grid and SCADA systems have remained relatively the same over the years, it is not sufficient to meet the power demands of the future [6], [7].

Recent initiatives promise to modernize the power grid for efficiency and reliability as well as to meet the increasing power demands of America's future by implementing smart grid technologies [7]. Implementation of the smart grid technologies require the deployment of new technologies and multiple interconnected communication infrastructures. Efforts to modernize the grid, sometimes on top of legacy systems, have created a highly vulnerable power grid infrastructure that is susceptible to many threats and vulnerabilities [8].

Special protection systems (SPS) detect system disturbances in the power grid and take predetermined actions to counteract the condition in a controlled manner [9]. Large system disturbances, such as transient instabilities, require an immediate response from the protection system in order to prevent cascading power outages. The special protection system response to system disturbances created by malfunctioning or malicious entities is what motivates this research.

1.2 Research Focus

Previous research experimented with implementing a context-specific reputation-based trust mechanism as a means to improve the special protection system decision making process in the presence of failures and disruptions attributed to malfunctioning or malicious smart grid components. This research is focused on

implementing a different trust mechanism within a special protection system to improve the reliability and efficiency of the smart grid. The primary goal of this research is to demonstrate that a special protection system implemented with a con-resistant trust mechanism can successfully function in the presence of untrusted (malicious or malfunctioning) smart grid special protection system nodes. The con-resistant trust mechanism will implement appropriate load shedding strategies to mitigate transient instabilities that can occur. It is expected that the following investigative questions will be answered:

- Does a special protection system implemented with a con-resistant trust mechanism successfully determine and execute the appropriate load shedding strategy during system wide disturbances in the presence of untrusted (malicious or malfunctioning) agent nodes?
- Does a special protection system implemented with a con-resistant trust mechanism successfully keep the system's steady frequency above the 58.8 Hertz (Hz) threshold?
- Can a special protection system implemented with a con-resistant trust mechanism perform at least as well as previous research with reputation-based trust mechanisms?

1.3 Organization

This chapter provided a brief introduction to Critical Infrastructure, Supervisory Control And Data Acquisition (SCADA) systems, the Smart Grid and Special Protection Systems (SPSs). Additionally, the chapter introduces the focus and primary goal of this research. The remainder of this document is organized as follows:

- Chapter 2 provides the background and literature review of the information required to give a complete understanding of the research effort.
- Chapter 3 introduces the goals and hypothesis of the research effort. It also includes the methodology and approach to obtaining the research goals.
- Chapter 4 presents and analyzes the results from the research experiments.
- Chapter 5 summarizes the entire research effort and provides recommendations for future work.

2 Literature Review

2.1 Overview

The purpose of this chapter is to provide a brief background on information relevant to the proposed research area. First, a review of critical infrastructure and key resources (CIKR), their associated sectors, and the importance of understanding sector interdependencies. Next, the chapter provides an overview of the electrical power grid to include relevant governance and the three major functions of the grid. Then, the chapter provides a brief introduction to industrial control systems (ICS) to include distributed control system (DCS) and Supervisory Control and Data Acquisition (SCADA) systems. Additionally, the chapter discusses the evolution and the general layout of SCADA systems. Next, the chapter provides an overview of the smart grid and related concepts. The chapter then presents the security issues and challenges associated with SCADA systems and the smart grid. Furthermore, the chapter gives a brief description of special protection systems (SPS), their purpose, and some of their limitations. Finally, the chapter provides an overview of *trust*, reputation-based trust models, and trust models used in previous research.

2.2 Critical Infrastructure

Since the early 1980's there have been several definitions of the term *infrastructure*. These definitions were often broad and left open to interpretation that focused primarily on the nation's public works and the services they provide rather than protecting them [10], [11]. It was not until 1998 when President Clinton signed Presidential Decision Directive-63 (PDD-63) that a focus was placed on identifying and protecting critical infrastructure (CI) assets at the national level.

PDD-63 mostly defines critical infrastructure as those physical and cyber-based systems essential to the minimum operations of the economy and government [12]. This directive identified eight critical infrastructure sectors to include banking and finance, emergency law enforcement services, emergency services, energy, information and communications, public health services, transportation, and water supply [12]. However, in direct response to the terrorist attacks of September 11, 2001, the United States Congress published the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act that more thoroughly defined critical infrastructure as the:

> *Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters* [13].

A little over a year later, President Bush signed the Homeland Security Act of 2002 into law that established the U.S. Department of Homeland Security (DHS). This Act introduced the term *key resources* (KR) and defines them as publicly or privately controlled resources essential to the minimal operations of the economy and government [14].

In December 2003, President Bush issued the Homeland Security Presidential Directive-7 (HSPD-7) which superseded PDD-63 and established a national policy for federal departments and agencies to identify and prioritize critical infrastructure and to protect them from terrorist attacks [15]. This directive expanded the critical infrastructure sectors to include key resources and brought the total number of sectors to 17. Four years later, these critical infrastructure key resource (CIKR) sectors were redefined in the 2007 National Strategy for Homeland Security. Furthermore, HSPD-7 authorized DHS to identify gaps in existing critical infrastructure sectors and establish new sectors to fill the gaps as needed [15]. As a result, the DHS identified Critical Manufacturing as a gap and

added it the CIKR list in March of 2008 bringing the total number of CIKR sectors to 18. Table 2.1 shows a current listing of the CIKR sectors.

Table 2.1: Critical Infrastructure Sectors and Key Resources (CI/KR) [15], [16]

CIKR Sector	Description
Agriculture & Food	Ensures the safety and security of food, animal feed, and food-producing animals; coordinates animal and plant disease and pest response; and provides nutritional assistance.
Banking & Finance	Provides the financial infrastructure of the nation.
Chemical	Transforms natural raw materials into commonly used products benefiting society's health, safety, and productivity.
Commercial Facilities	Includes prominent commercial centers, office buildings, sports stadiums, theme parks, and other sites where large numbers of people congregate to pursue business activities, conduct personal commercial transactions, or enjoy recreational pastimes.
Nuclear Reactors, Materials & Waste	Provides nuclear power.
Dams	Manages water retention structures that are major components of other critical infrastructures that provide electricity and water.
Defense Industrial Base	Supplies the military with the means to protect the nation by producing weapons, aircraft, and ships and providing essential services, including information technology and supply and maintenance.
Drinking Water & Water Treatment Systems	Provides sources of safe drinking water from community water systems and properly treated wastewater from publicly owned treatment works.
Emergency Services	Saves lives and property from accidents and disasters.
Energy	Provides the electric power used by all sectors and the refining, storage, and distribution of oil and gas. The sector is divided into electricity, oil, and natural gas.
Government Facilities	Ensures continuity of functions for facilities owned and leased by the government, including all federal, state, territorial, local, and tribal government facilities located in the U.S. and abroad.
Information Technology	Produces information technology and includes hardware manufacturers, software developers, and service providers, as well as the Internet as a key resource.
National Monuments & Icons	Maintains monuments, physical structures, objects, or geographical sites that are widely recognized to represent important national cultural, religious, historical, or political significance.
Postal & Shipping	Delivers private and commercial letters, packages, and bulk assets.
Public Health & Healthcare	Mitigates the risk of disasters and attacks and also provides recovery assistance if an attack occurs. This sector consists of health departments, clinics, and hospitals.
Telecommunications	Provides wired, wireless, and satellite communications to meet the needs of businesses and governments
Transportation Systems	Enables movement of people and assets that are vital to our economy, mobility, and security with the use of aviation, ships, rail, pipelines, highways, trucks, buses, and mass transit.
Critical Manufacturing	Transforms materials into finished goods.

Critical infrastructure and key resource (CIKR) sectors are not independent and rely on one another in order to operate and function properly. What happens in one CIKR sector can directly and indirectly affect other CIKR sectors, impact large geographic regions, and send ripples throughout the national and global economy [2]. Certain sectors, such as energy, telecommunications, transportation, and drinking water and water treatment systems, are considered ”lifeline systems” that are essential for national and economic security as well as public health and safety [11]. Merriam-Webster's dictionary defines *lifeline* as something regarded as indispensable for maintaining or protection of life [17]. The concept of ”lifeline system” was developed to evaluate performance of large, geographically dispersed CIKR networks during natural disasters such as earthquakes and hurricanes [11]. Although the potential for natural disaster to occur always exists, the lifeline concept should also evaluate performance of CIKR networks during equipment failures and malicious attacks.

2.2.1 Sector Interdependencies. During the last half of the century, technical innovations and developments in information technology and telecommunications dramatically increased interdependencies among the nation's critical infrastructure [18]. America has become an open, technologically sophisticated, highly interconnected, and complex nation with a wide array of critical infrastructure that spans important aspects of the U.S. [19]. Increasingly interconnected systems are vulnerable to threats brought on by sector dependence with the potential to trigger interrelated, cascading disturbances that can directly and indirectly affect the other infrastructures, impact geographic regions, and send ripples throughout the national and global economy [2], [3], [4]. This vast and diverse aggregation of highly interconnected assets, systems, and networks present an attractive array of targets to domestic and international terrorists and greatly magnify the potential for cascading failures in the wake of catastrophic natural or manmade disasters [11], [20], [19].

Figure 2.1 highlights some of the critical infrastructure sector interdependencies across North America. Each sector relies on other sectors in order to function successfully. For example, the energy sector, including the electric power industry, is of primary importance because it provides the essential energy needed by other sectors to function.

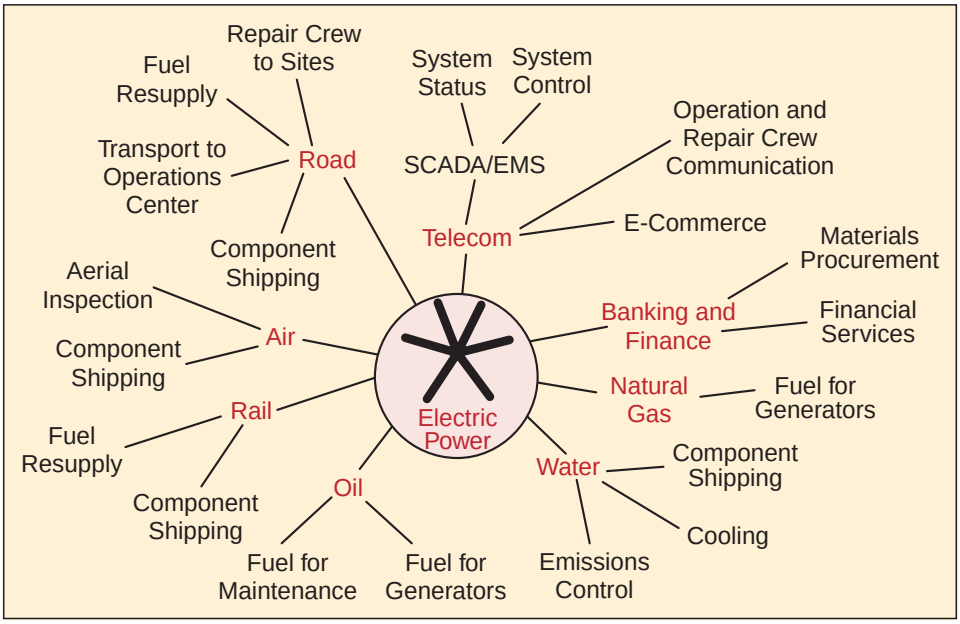

Figure 2.1: Critical Infrastructure Sector Interdependencies [2]

Modern society has come to depend on reliable electricity as an essential resource for national security; health and welfare; communications; finance; transportation; food and water supply; heating, cooling, and lighting; computers and electronics; commercial enterprise; etc. . . [3]. Coal and other fossil fuels are a major source of energy to generate the electricity needed. In Figure 2.2, the burning of fossil fuels (coal, natural gas, and petroleum) accounts for nearly 70% of the total electricity generated in the U.S. for 2011 [21]. The transportation systems sector and the oil and gas industries of the energy sector are depended upon to get the coal to the electricity generating powerplants to produce the required electricity for consumers. Identifying, understanding, and analyzing critical

infrastructure key resource sector interdependencies is critical to the security, economic prosperity, and social well-being of the nation [2].

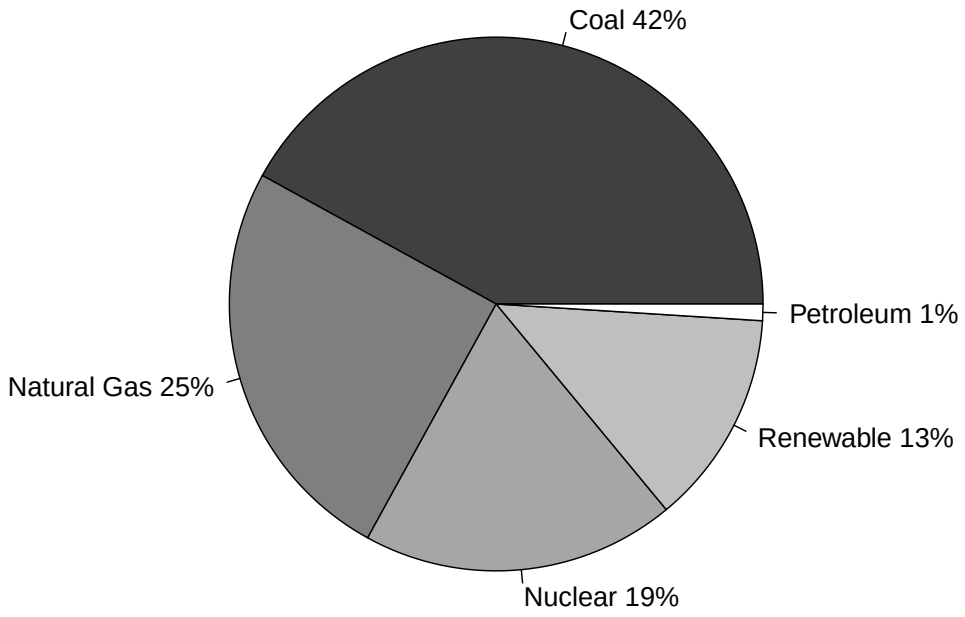

Figure 2.2: Sources of U.S. Electricity Generation in 2011 [21]

The interdependencies illustrated in Figure 2.1, clearly show how a disruption in one infrastructure can directly lead to disturbances in other infrastructures. Furthermore, how the infrastructures are interconnected can often extend or amplify the effects of a disruption [18]. For example, the energy infrastructure interdependence is not isolated to the United States. It crosses international borders to Canada and Mexico where oil and natural gas pipelines and electrical transmission lines have helped integrate the energy systems of North America [18]. Two prime examples highlighting the importance of understanding sector interdependencies and Nation's dependence on lifeline systems include the 2003 Northeast power outage and 2005's Hurricane Katrina.

On August 14, 2003, the northeastern portion of the U.S. and Canada experienced a widespread blackout that affected over 50 million people and resulted in estimated economic losses between 4 to 10 billion dollars [3], [22]. This significant event

highlighted the nation's dependence on electricity [3]. Among the multitude of causes attributed to the blackout, the lack of situational awareness by the control area operators and faulty process control system equipment that did not detect the instabilities in the power grid due were primarily identified [3], [22].

In August 2005, Hurricane Katrina devastated the Gulf Coast, damaging critical infrastructure that disrupted governmental and business functions alike, producing cascading effects that extended far beyond the physical reach of the storm [20]. Additionally, the effects caused by Hurricane Katrina highlighted the criticality of critical infrastructure sector interdependencies [11]. For example, the supply of crude oil and the refining of petroleum products were interrupted due to the loss of power at three major transmission pipelines. This loss of power resulted in a loss of 1.4 million barrels of crude oil and 160 million liters per day of gasoline production that accounted for 90 percent of the production in the Gulf of Mexico and 10 percent of the U.S. supply respectively [11].

These real world examples underscore the vulnerabilities and interdependencies of the Nation's critical infrastructure. Protecting and ensuring the continuity of critical infrastructure and key resources in the United States is essential to the Nation's security, public health and safety, economic vitality, and way of life [19].

2.3 Electrical Power Grid

The North American power grid, commonly referred to as "the grid", is a complex network of independently owned and operated infrastructures for delivering electricity from suppliers to consumers. The grid has evolved into four distinct power grids or interconnections. Three of which service the continental United States as seen in Figure 2.3. The Eastern Interconnection includes the eastern two-thirds of the U.S.. The Western Interconnection includes the western one-third of the U.S.. The state of Texas has it's own Interconnection and is called the Electric Reliability Council of Texas.

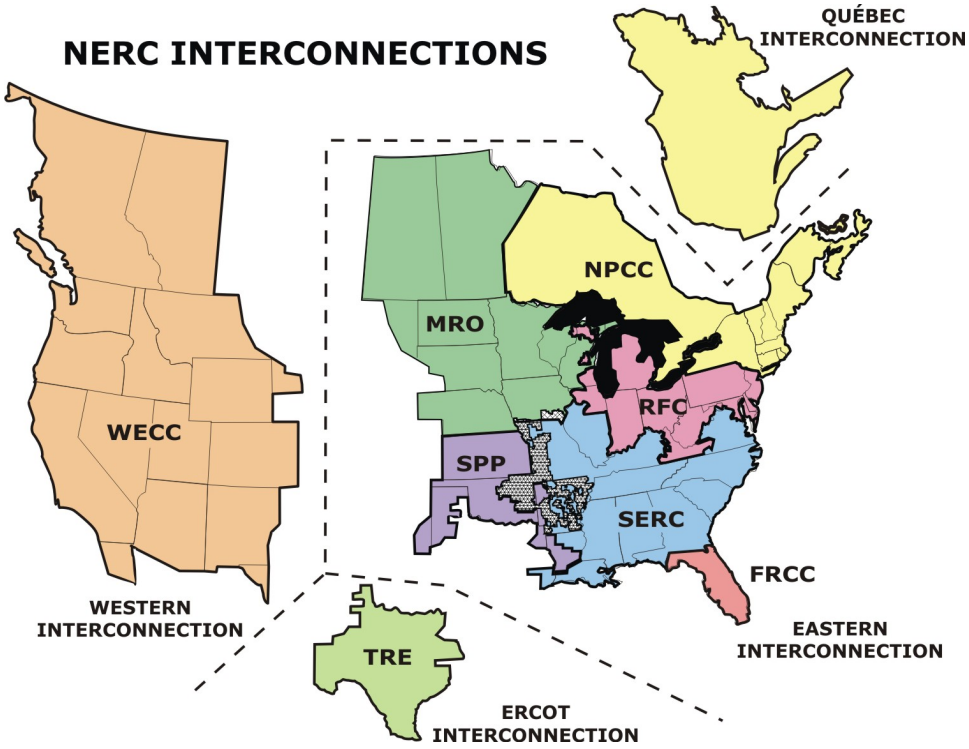

Figure 2.3: North American Power Grid Interconnections [18]

The Federal Energy Regulatory Commission (FERC) is the governmental agency that regulates the transmission of electricity between the major interconnections [23]. The North American Electric Reliability Corporation (NERC) is the self-regulating, non-profit organization whose primary purpose is to improve and maintain grid reliability as well as to develop and enforce reliability standards [24].

2.3.1 Governance. In 1968, NERC was established by the electric utility industry for the purpose of developing and promoting voluntary compliance with rules and protocols for the reliable operation of the electric power grid [24]. The U.S. Energy Policy Act of 2005 authorized the creation of a self-regulatory ”electric reliability organization” (ERO) that would span North America, with FERC providing oversight in the U.S. [25]. As a result, on July 20th, 2006, FERC certified NERC as the ERO for the United States [24]. This gave NERC the authority to develop and enforce mandatory reliability

standards. On June 18, 2007, compliance with these standards became mandatory and enforceable in the U.S. [24].

Prior to being designated as the ERO for the U.S., NERC was appointed as the electric utility industry's primary point of contact with the U.S. government for national security and critical infrastructure protection issues [24]. Under the authority of the ERO, NERC developed Critical Infrastructure Protection (CIP) reliability standards to improve the physical and cyber security of the Bulk Electric System. NERC generally defines the Bulk Electric System as all electrical generation resources and transmission systems that operate above 100 kV [26]. Table 2.2 summarizes the NERC CIP reliability standards.

Table 2.2: NERC Critical Infrastructure Protection Reliability Standards [27]

Number	**Title**	**Summary**
CIP-002	Critical Cyber Asset Identification	Identify Critical Cyber Assets assoicated with Critical Assets that support the reliable operation of the Bulk Electric System.
CIP-003	Security Management Controls	Responsive Entities must have minimum security management controls in place to protect Critical Cyber Assets.
CIP-004	Personnel & Training	Personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, are required to have an appropriate level of personnel risk assessment, training, and security awareness.
CIP-005	Electronic Security Perimeter(s)	Identify and protect the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter.
CIP-006	Physical Security of Critical Cyber Assets	Ensure the implementation of physical security program for the protection of Critical Cyber Assets.
CIP-007	Systems Security Management	Responsible Entities are required to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as other (non-critical) Cyber Assets within the Electronic Security Perimeter(s).
CIP-008	Incident Reporting and Response Planning	Ensure the identification, classification, response, and reporting of Cyber Security incidents related to Critical Cyber Assets.
CIP-009	Recovery Plans for Critical Cyber Assets	Ensure recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices.

These standards help ensure that all entities responsible for Bulk Electric Systems in North America identify and protect critical cyber assets that control or could otherwise impact the reliability of the Bulk Electric System [27]. A reliable Bulk Electric System ensures the generation of electricity and delivering that electricity to the consumer. The process of generating and delivering electricity to the consumer consists of three major functions: 1) Electricity Generation, 2) Electric Power Transmission, and 3) Electricity Distribution. An overview of the electric power system from generation to distribution to the consumers can be seen in Figure 2.4.

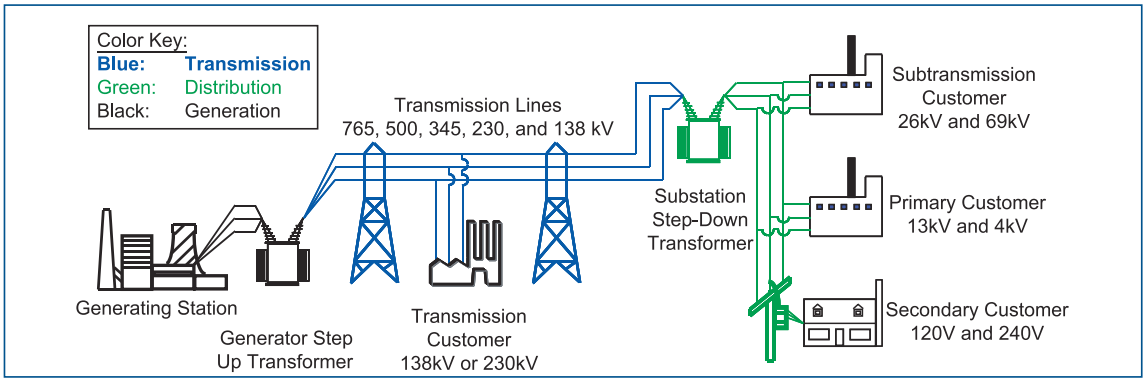

Figure 2.4: Overview of the Electric Power System [3]

2.3.2 Electricity Generation. The first major function, electricity generation, is the process of generating electricity from other forms of energy such as water, wind, nuclear, and fossil fuels. During electricity generation, maintaining a delicate balance between supply and demand is crucial. Electricity that is generated travels at the speed of light and cannot be stored in large quantities economically [18]. Therefore, the supply of electricity must not exceed the demands of the consumer and should be transmitted the instant it is produced.

2.3.3 Electric Power Transmission. Electrical power transmission is the second major function of the electric power grid and is responsible for the transfer of the electrical energy from the transmission substations at the generating power plants to electrical distribution substations over high voltage transmission lines [18]. These transmission lines not only deliver electricity to the distribution substations, they also connect the North American power grid interconnections.

2.3.4 Electricity Distribution. The final major function of the electric power grid is electricity distribution where electrical power is delivered to the consumers. The high voltage power that's transferred over transmission lines is received at the electrical distribution substations. Here, the high voltages are stepped down so that electricity can be carried over distribution lines at lower usable voltages to customers.

Control centers contain sophisticated monitoring and control systems that are responsible for balancing power generation and demand, monitoring the flows over transmission lines, planning and configuring systems to operate reliably, maintaining system stability, preparing for emergencies, and placing equipment in and out of service for maintenance and during emergencies [18]. Supervisory Control and Data Acquisition Systems are the control systems distributed throughout the electrical power industry.

2.4 SCADA

Control systems are used throughout many infrastructures and industries to monitor, operate, and control sensitive processes and physical functions [28]. Industrial Control System (ICS) is a general term that encompasses several types of control systems including Supervisory Control and Data Acquisition (SCADA) systems and Distributed Control System (DCS) [29]. Distributed control systems are generally used to control production systems confined within a local area such as a factory. SCADA systems are highly distributed and are typically used in larger-scaled environments to control

geographically dispersed assets where centralized data acquisition and control are critical to system operation [22], [29]. These systems are found throughout many critical infrastructure sectors in industries such as water distribution and wastewater collection systems, oil and gas pipelines, electrical power grids, and railway transportation systems [22].

2.4.1 Evolution of SCADA. SCADA systems have evolved over the past 50 years from standalone, compartmentalized operations into intricately networked architectures that communicate across large distances [5]. The first generation of computer-based SCADA systems, introduced in the 1960s, employed a centralized architecture with a powerful mainframe computer that was responsible for managing and performing all functions [30]. These SCADA systems were independent, closed systems that consisted of four basic components that included a central mainframe computer, remote terminal units (RTUs), the wide area telecommunications system to connect them, and an operator interface [30]. RTUs are field-based remote measurement and control units that are continuously polled by the central computer to provide current measurement values. The operator interface, also known as the Human Machine Interface (HMI), gave the human operator access to the system through map board displays. Propriety communication protocols were in use which gave the false sense of security to many SCADA system owners and operators, thus security was not a big concern at the time.

Second generation SCADA systems emerged in the 1980s and proceeded through the late 1990s. Advances in computing technology led to a more distributed SCADA architecture in which multiple stations were networked together through the introduction of local area networking (LAN) technologies [30]. This distributed architecture allowed for various SCADA functions to be spread out amongst dedicated computers which helped to improve overall SCADA system reliability. If one computer malfunctions then only that specific function is lost vice the entire system. Communication protocols were

still largely proprietary and security was still primarily an after thought. However, it was this generation when SCADA security issues started to emerge.

Since SCADA systems are based on computer technology, their designs have evolved in step with advances in computer technology [30]. The third and present generation of SCADA systems have introduced advanced computer technologies and evolved into the intricately network architectures that we know today. They are no longer the independent closed systems but instead, they are open system architectures that are highly distributed across wide area networks (WAN). The hardware devices and software protocols are no longer completely proprietary. Even though some traditional information technology security features have been implemented, the security of SCADA systems hasn't been able to keep up with emergent cyber security threats and vulnerabilities that exist today.

2.4.2 General SCADA Layout. Figure 2.5 shows the general system layout and typical components that are found throughout modern SCADA systems. The control center houses the Master Terminal Unit (MTU) or SCADA control server, the human machine interface, communications routers, and other components that are all connected by a local area network. MTUs communicate with one or more geographically distributed field sites that house the remote terminal units, Programmable Logic Controllers (PLCs), or Intelligent Electronic Devices (IEDs). The field site's basic functions are to gather information from field devices, such as sensors or actuators, and send this information to the MTU when instructed. Standard and proprietary communication protocols running over serial communications are used to transport information between the control center and field sites using telemetry techniques such as telephone line, cable, fiber, and radio frequency such as broadcast, microwave and satellite [29].

While the basic architecture and design of the North American power grid and SCADA systems have relatively remained the same over the years, it is not sufficient to

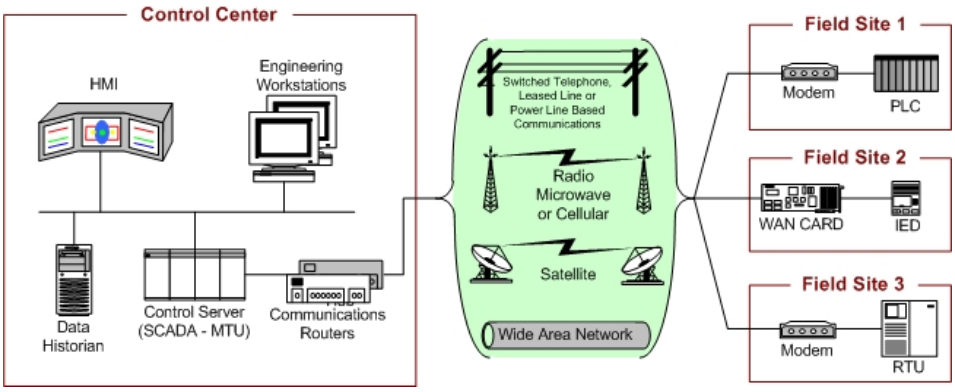

Figure 2.5: SCADA System General Layout [29]

meet the power demands of the future [6], [7]. A 2011 report by NERC predicts that, on average, peak demand for electricity will increase by almost 12 percent by the year 2021 [31]. Significant improvement to the grid is necessary in order to meet future expected demands.

2.5 Smart Grid

Today's electrical power grid infrastructure in the U.S. is not up to the task of powering America's future and is rapidly running up against its limitations [32]. According to Carol Browner, director of the White House Office of Energy and Climate Change from 2009 to 2011, "We [the United States] have a very antiquated (electric grid) system in our country . . . The current system is outdated, it's dilapidated" [33]. In an effort to modernize the grid for efficiency and reliability as well as to meet the increasing power demands of America's future, the Obama Administration awarded $3.4B for projects implementing smart grid technologies [7].

While there is no established definition of a smart grid, the term *smart grid* generally refers to developing network of transmission lines, equipment, controls, and new technologies working together to respond immediate electricity demands of the 21st Century [34]. It is a modern electric power grid that promises to improve efficiency,

reliability, and safety through automated control and modern communications technologies [35]. Ten specific capabilities that would be enabled by the emerging Smart Grid are identified in the U.S. Energy Information and Security Act (EISA) of 2007. They include the following [36]:

- Increase use of digital information and controls technology to improve the reliability, security and efficiency of the electric grid;
- Dynamic optimization of grid operations and resources, with full cyber-security;
- Deployment and integration of distributed resources and generation, including renewable resources;
- Development and incorporation of demand-response, demand-side resources and energy efficiency resources;
- Deployment of smart (real-time, automated, interactive) technologies that optimize physical operation of appliances and consumer devices for metering, communications concerning grid operations and status, and distribution automation;
- Integration of smart appliances and consumer devices;
- Deployment and integration of advanced electricity storage and peak-shaving technologies including plug-in electric and hybrid electric vehicles, and thermal storage air conditioning;
- Consumer access to timely information and control options;
- Development of standards for communication and interoperability of appliances and equipment connected to the electric grid including the infrastructure serving the grid; and

- Identification and reduction of unreasonable or unnecessary barriers to the adoption of smart grid technologies, practices, and services.

Implementation of the smart grid characteristics listed above require the deployment of new technologies and multiple interconnected communication infrastructures that are highly susceptible to a myriad of vulnerabilities. With every new technology and easy access to smart grid systems and data come new attack vectors that can be easily exploited [7].

2.6 SCADA and Smart Grid Insecurities

Supervisory Control And Data Acquisition (SCADA) systems and networks were generally thought to be secure because of their isolation from other networks. However, the growing demands for increased connectivity have introduced vulnerabilities into the grid that previously did not to exist. These SCADA architectures have been upgraded to incorporate advanced information technologies (IT) to improve overall process efficiency, productivity, and safety; however, security was never adequately addressed. Additionally, the recent initiatives in the U.S. Energy Information and Security Act (EISA) of 2007 [36] to modernize the grid with smart grid technologies, sometimes on top of legacy systems, have created a highly vulnerable power grid infrastructure that is susceptible to many threats and vulnerabilities [8].

In the 2009 National Infrastructure Protection Plan (NIPP), a *threat* is defined a natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property [19]. The NIPP also defines a *vulnerability* as physical features or attributes that renders an entity open to exploitation or susceptible to a given hazard [19]. Table 2.3 lists some general threats and vulnerabilities that apply to SCADA systems and the emerging communications-based smart grid.

Table 2.3: General Threats and Vulnerabilities affecting SCADA systems and the Smart Grid [37]

Threats	**Vulnerabilities**
Naturally occurring events	Communications
Untrained and/or distracted personnel	The Internet
Insiders with malicious intent	Grid complexity
Cyber-attack (lone actors)	Grid control system complexity
Cyber-attack (terrorism)	New systems
Cyber-attack (nation states)	New Device

This list is not all inclusive and continues to grow causing tremendous concern about the antiquated power grid as well as the emerging Smart Grid. Multiple efforts by private sector entities and federal agencies to secure control systems and the grid are underway, but challenges remain [38]. Critical infrastructure owners face technical and organization challenges in securing their control systems. Technical challenges include legacy control systems' limited processing capabilities and real-time operations which make it difficult to implement traditional information technology security technologies and best security practices [38]. Additionally, organizational challenges include the lack of a compelling business case to improve security and a reluctance to share information regarding security incidents [38]. Often owners are willing to accept the risks associated with the insecurities because of what it would cost to implement improved security measures. What is needed are cost-effective measures to mitigate the risks associated with having insecure SCADA systems and smart grid.

2.7 Special Protection Systems

Protections schemes, also known as protection systems, for the power grid are primarily designed for improving power system stability or enhancing system security [9]. Power system stability is the property of a power system that enables it to remain in a state of operating equilibrium under normal operating conditions and to regain an acceptable

state of equilibrium after being subjected to a disturbance [39]. Special protection systems (SPS) are protection systems designed to detect these system disturbances within the power grid and take predetermined actions to counteract the condition in a controlled manner, thus regaining an acceptable state of equilibrium [9]. Small system disturbances occur frequently and typically do not require a protective system response. However, large system disturbances, such as transient instabilities, always require immediate protection system response in order to prevent complete system failure. Examples of large disturbances that can cause transient instabilities in the power grid include [9]:

- Transmission faults
- Cascading outages of lines
- Generation outages
- Sudden, large load changes
- Combinations of the above

Failure to detect these system disturbances or respond in a timely manner could lead to catastrophic events like the 2003 Northeast power outage [3] discussed previously in Section 2.2.

Two examples of the most common types of special protection system schemes include generation rejection and underfrequency load shedding [40]. Generation rejection involves the selective tripping of generating units for severe transmission system disturbances which has been used as a method of improving system stability for many years [39]. The rejection of generation at an appropriate location in the system reduces power to be transferred over the critical transmission interfaces [39]. Additionally, load shedding schemes are employed to reduce the connected load to a level that can be safely supplied by available generation [39].

The use of smart grid technology makes it possible to improve legacy special protection systems. The increased bandwidth capacity in the communications-based smart grid will improve the systems' context awareness and enables better protection system decisions concerning detected system disturbances [41]. Trust, as it relates to computing environments, is a mechanism that can take advantage of the increased bandwidth feature in a communications-based smart grid to improve protection system decisions.

2.8 What is Trust?

Although the notion of trust has been extensively studied over the last half century and is widely used throughout secure information systems, no formal definition of *trust* truly exists [42], [43]. One definition of *trust* that is widely accepted came from Morton Deutsch in 1962. It states that:

> *Trusting behavior occurs when an individual perceives an ambiguous path, the result of which could be good or bad, and the occurrence of the good or bad result is contingent on the actions of another person; finally, the bad result is often more harming than the good result is beneficial. If the individual chooses to go down that path, he can be said to have made a trusting choice, if not, he is distrustful [44].*

This definition provides the basic structure of making a trusting choice. An entity makes a choice of which path to take based on the actions or reputation of another entity. Reputation-based trust is found in many computing systems where *trust* is treated as a binary concept [43]. A binary concept of trust is where an entity is either completely trusted or completely untrusted. Complete trust requires absolute knowledge of an entity which is often rare in real-world applications [43]. In contrast, completely distrusting an entity can prohibit all communications with that entity potentially rendering the entity useless.

2.8.1 *Reputation-Based Trust.*

Many different reputation-based trust models exist. The foundation of this research builds off a context-specific reputation-based trust model. In a context-specific reputation-based trust model, an entity (the truster) trusts another entity (the trustee) with respect to a certain context [43], [45]. Here, *context* is synonymous with *service*. Properties of trust within the context-specific trust model include direct and indirect trust. Direct trust of an entity evolves from an entity's direct interaction experience with other entities and is kept for future interactions and providing recommendations to other entities [45]. In this model the term *interaction* denotes an action regarding a context or service. Indirect trust happens when there is no history of direct interactions between two entities. In this case, recommendations from trusted peers with direct interactions with the entity in question are considered [45].

2.8.2 *Previous Research.*

2.8.2.1 *A Multi-Mechanism Trust Model.*

The Consolidated Trust Management System (CTMS) developed by Mark Duncan in [46], is a trust management system (TMS) that utilizes multiple trust mechanisms to make a single trust decision in satellite telecommand networks. This framework is built off the work presented in [47] where certain characteristics were taken into consideration for the development of CTMS. These characteristics include [47]:

- Multiple Trust Mechanisms: Incorporate multiple trust mechanisms in concert for a single trust decision regarding a complex trust relationship
- Open Nature: Define crucial trust relationships for known and unknown entities due to the open nature of distributed information systems

- Multiple Domains: Be aware of distributed information systems that span multiple networks and cross multiple administrative and organizational boundaries that can complicate trust relationships

- Real-Time Trust: Trust relationships in distributed information systems are dynamic and must be evaluated and established in real-time

- Scalability: A trust management system implementation must be able to scale to meet the maximum requirements of the distributed information system

- Complexity: The trust management system must be capable of modeling and managing the complicated business functions and advanced technologies often found in modern distributed information systems

The consolidated trust management system utilizes interaction and credential based trust mechanisms to calculate a trust value for a given entity. As proposed by Yu and Singh in [48], trust is determined through the number of positive interactions (cooperations) and negative interactions (defections) an entity has with another. The basic premise behind the trust calculation is that trust is easy to lose but hard to gain. For example, the level of trust an entity has towards another entity can change based on the evaluation of an interaction. If an entity perceives that another entity is cooperating during a specific interaction, its trust in the other entity will increase. In contrast, if the entity perceives the other entity had defected for a specific interaction, its trust in that entity will decrease.

Additionally, Duncan also incorporated the con-resistant trust model by Salehi-Abari and White in [49]. This con-resistant trust model is an extension of the trust mechanism proposed by Yu and Singh in [48]. A con-resistant trust model is one that is resistant to a con-man or confidence-man attack. A confidence attack is based on a sequence of interactions where a con-man entity conducts a series of consecutive cooperative interactions in an attempt to gain the confidence of the system thus elevating its associated

trust value. Then at a particular point in time, the con-man will defect, defrauding the victim. The con-man then has two choices: 1) never interact with the victim again or 2) regain the lost trust with subsequent cooperative behavior. The con-man, by regaining the victim's trust, can again con (or defect) the victim [49]. This research implements the con-resistant trust model to improve the resiliency and the decision-making process of special protection systems within the communications-based smart grid.

2.8.2.2 Reputation-Based Trust for Special Protection Systems. The reputation-based Trust Management Toolkit (TMT) for the enhanced Special Protection System (SPS) developed by Jose Fadul in [41] augments legacy power grid protection system components to better utilize the increased bandwidth capacity in smart grids and improves the decision making process in the presence of failures and disruptions attributed to malfunctioning or malicious smart grid components. It utilizes reputation-based trust values to improve smart grid protection system fault response times and resiliency to intentional and unintentional protection component and communication network errors [41]. The TMT consists of three major modules that calculate and assign a trust value for a particular entity [41]:

- Trust Assignment Module - uses context sensitive information such as, frequency information provided by individual smart grid components' to determine trust values
- Fault Detection Module - uses error signals generated by frequency disturbance monitoring devices to detect system frequency faults
- Decision Module - analyzes the current power grid conditions and assigned trust values to decide on the most reliable corrective action that minimizes the risk of failure to detect instabilities in the power grid

The reputation-based trust management toolkit utilizes a majority-rule algorithm where trust values are assigned based on a concurrence of information received from multiple

entities. The entities that agree with the trusted majority are trusted entities and the entities that disagree with the trusted majority are untrusted. Furthermore, the trust management toolkit also utilizes a greedy algorithm approach to determine which of the trusted nodes are selected for load shedding.

Trust is calculated based on current context sensitive information and does not take into account previous trust values. Hence, an entity might be completely trusted at one time step and completely distrusted on the next time step. This complete distrust of an entity at one point in time may not accurately represent the current state of the entity rendering it useless potentially causing instability in the smart grid. What is needed is a trust system that incorporates an entity's previously assigned trust values to determine its current trust value. Trust that is calculated from a historical perspective gives a more realistic view of the special protection systems' operational status.

2.9 Summary

This chapter presented the background information required for research with implementing trust within special protection systems for a communications-based smart grid. First, the chapter defined critical infrastructure and their respective sectors as well as highlighted the importance of understanding critical infrastructure sector independencies. Next, the chapter introduced the electrical power grid, it's governance, and the three major functions of the grid. Then, the chapter presented information on Supervisory Control And Data Acquisition (SCADA) control systems, the emerging communications-based smart grid and their insecurities. Next, the chapter provided information on special protection systems (SPS) and two of the most common types of SPSs. Finally, the chapter presents information on trust, reputation-based trust models and trust used in previous research.

3 Methodology

3.1 Overview

This chapter presents the methodology used to evaluate the application of a con-resistant trust algorithm in a simulated special protections systems for the communications-based smart grid. This con-resistant trust algorithm provides an additional layer of security as well as improves the reliability of special protection system during grid disturbances due to malfunctioning or malicious behaviors. The chapter begins by describing the problem definition, research goals and hypothesis, and the approach. Next, the simulation environment is discussed followed by a detailed description of the research scenario to include the implementation of the con-resistant trust mechanism, the interaction trust value calculation and the abuse case used. Additionally, the metrics used to evaluate the performance of the con-resistant trust mechanism are also discussed. Finally, the evaluation technique chosen and the experimental design are covered along with the validation of determining the sampled data are from a normally distributed population.

3.2 Problem Definition

3.2.1 Research Goals and Hypothesis. Legacy Supervisory Control and Data Acquisition (SCADA) systems and networks were generally thought to be secure because of their isolation from other networks. However, the introduction of advance computing technologies to improve reliability and functionality of SCADA systems and networks have introduced vulnerabilities that previously did not exist. Furthermore, recent initiatives proposed in the Energy Independence and Security Act of 2007 [36] to modernize the power grid with smart grid technologies, sometimes on top of the legacy systems, have created a highly vulnerable power grid that is susceptible to numerous

threats like the examples presented in Table 2.3 [8]. Additionally, these systems operate 24 hours a day, 7 days a week, making it difficult to implement the necessary security patches to mitigate their vulnerabilities. Risks associated with these vulnerabilities include critical system faults or line outages that can often result in cascading blackouts like the Northeast Power Outage that occurred in 2003 [3]. These risks can be mitigated through the implementation of additional security mechanisms, such as trust, that take into account the strict timing constraints for electrical utility operations as well as the responses to special protection system conditions. Table 3.1 summarizes the timing constraints that must be met for SCADA and protection system responses [50].

Table 3.1: Time Constraints for Electric Utility Operations [51], [52], [53], [54]

Systems	**Situation**	**Response Time**
Substation IEDs; Primary short circuit protection and control	Routine power equipment signal measurement	Every 2-4 ms
	Local-area disturbance [51]	< 4ms from event detection to sending notification [52]
		4-40 ms automatic response time
Backup protection and control; Wide area protection and control (WAPaC)	Transient voltage instability	Often $\leq$ 180 ms to convey 14+ trip signals to disconnect generators at the top generating station [53]
	Frequency instability, must respond faster than generator governors to trip generators instantaneously	Could require < 300 ms response time (by load shedding) for high rates of frequency decay; requires detection within 100 ms to allow operator response in 150 to 300 ms [53]
	Dynamic instability	A few seconds
	Poorly damped or undamped oscillations	Several seconds
	Voltage instability	Up to a few minutes
	Thermal overload	Several minutes for severe overloads, rarely less than a few seconds for minor occurrences [53]
SCADA	Emergency event notification	< 6 ms
	Routine transactions	< 540 ms [54]
	Routine HMI status polling from substation field devices	Every 2 secs

The primary goal of this research is to demonstrate that a special protection system implemented with a con-resistant trust mechanism can successfully function in the presence of untrusted (malicious or malfunctioning) smart grid special protection system nodes by implementing appropriate load shedding strategies to mitigate transient instabilities that can occur. For the purposes of this research, the terms *malfunctioning* and *malicious* nodes are synonymous and mean a node is exhibiting behavior outside of normal operation. Additionally, a *malfunctioning* or *malicious* node is acknowledged as an untrusted node. Nodes that are behaving within normal operations are acknowledged as trusted nodes. It is hypothesized that assigning trust values based on the cooperative and defective interactions between the load agent nodes in the simulated power grid will improve the special protection system decision-making process of identifying and selecting trusted nodes for load shedding.

3.2.2 Approach. Building off the reputation-based trust framework developed by Fadul [41], this research utilizes an extension of the direct interaction trust model developed by Yu and Singh [48] to detect malfunctioning behaviors during a special protection system condition that requires immediate corrective responses to mitigate instabilities within the smart grid. Corrective responses include actions, such as, generation rejection or load shedding, that improve system stability [39].

Success is determined by the special protection systems ability to accurately identify which load agent nodes are trusted and untrusted and its ability to select the minimum number of optimal trusted nodes to shed load in an attempt to keep the systems steady-state frequency above 58.8 Hz. Table 3.2 provides an example of how nodes are sorted for load shedding. Nodes are sorted in order of precedence from left to right, first by *Node Type*, then by whether or not the node is *Trusted*, next by the node's *Available Load (MW)* followed by the *Authorized Shed Amount (MW)* and *Node ID*. If the required load shed amount is 875 MW of power, then the greedy algorithm would attempt to meet

this requirement by selecting the first node (Node ID 25) in Table 3.2. If, Node ID 25 is unable to satisfy the requirement, then the greedy algorithm will choose the next node (Node ID 120). The greedy algorithm will continue down the table selecting nodes for load shedding until the load shed amount of 875 MW is satisfied. In this example, the minimum number of optimal trusted nodes for load shedding 875 MW of power is three, namely Node IDs 25, 120, and 73.

Table 3.2: Sorted Nodes for Possible Load Shedding

Node Type	Trusted	Available Load (MW)	Authorized Shed Amount (MW)	Node ID
Load	Yes	1700	340	25
Load	Yes	1607	321	120
Load	Yes	1318	264	73
Load	Yes	1098	220	72
Load	Yes	1057	211	27
Load	No	1026	205	74
Load	No	320	64	75
Load	No	97	19	70

The method used to calculate the Interaction Trust (I-Trust) value as proposed by Yu and Singh is adapted to provide a quantitative measure of I-Trust for the nodes in the system [48]. Furthermore, the direct interaction trust model is extended to include the Con-Resistant trust model proposed by Salehi-Abari and White in [49]. A con-resistant trust model is one that is resistant to a con-man or confidence-man attack. A confidence attack is based on a sequence of interactions where a node conducts a series of consecutive cooperative interactions in an attempt to gain the confidence of the system thus elevating its associated trust value.

3.3 Simulation Environment

This research uses computer simulations to demonstrate a special protection system implemented with a con-resistant trust mechanism within the smart grid. The simulators

in use are: 1) Power System Simulation for Engineering (PSS/E) [55], 2) the Network Simulator 2 (NS2) [56] and 3) the Electric Power and Communications Synchronizing Simulator (EPOCHS) [57].

PSS/E, developed by Siemen's Corporation, is an electromechanical transient commercial software simulator that is used to simulate the special protection system and the electric power grid. NS2 is an open source tool discrete event simulator for communication networks and is used in this research to represent the increased bandwidth of an Internet-like smart grid utility intranet [41]. The smart grid's communication network interconnects multiple node types such as, control centers, power generation plants, substations and customers [41]. Figure 3.1 is an abstract representation of the smart grid's communication network. Within NS2, a software agent node represents each node type. In a real world implementation, these software agent nodes would reside inside Intelligent Electronic Devices (IEDs) or smart Remote Terminal Units (RTUs). In this simulation environment, the software agent nodes communicate with each other via NS2 and with their corresponding PSS/E power simulator component via EPOCHS [41], [57].

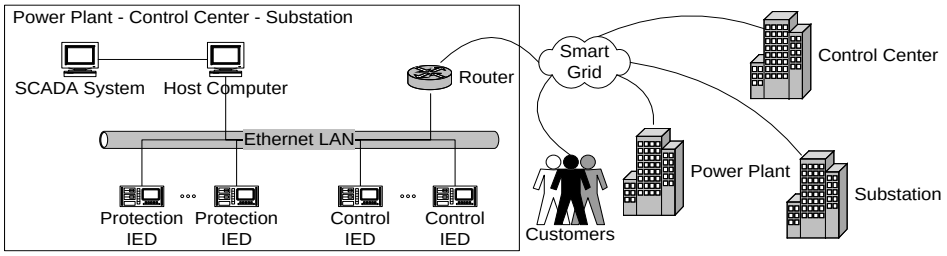

Figure 3.1: Abstract representation of a smart grid wide area network [57]

EPOCHS is a combined simulation system that federates the PSS/E electromechanical transient simulator, as well as other electromagnetic transient simulators, and the NS2 communication network simulator [57]. Figure 3.2 is a graphical representation of the EPOCHS simulation system. EPOCHS works via an Agent

Headquarters (AgentHQ) and a run-time infrastructure (RTI) as shown in Figure 3.2 to synchronize and coordinate the simulators that would otherwise run at different speeds [58]. The AgentHQ presents a unified environment to agents and acts as a proxy when agents interact with other EPOCHS components [57]. The RTI acts as the ”glue” that links all other components and is responsible for the simulation synchronization as well as the routing communication between EPOCHS' components [57].

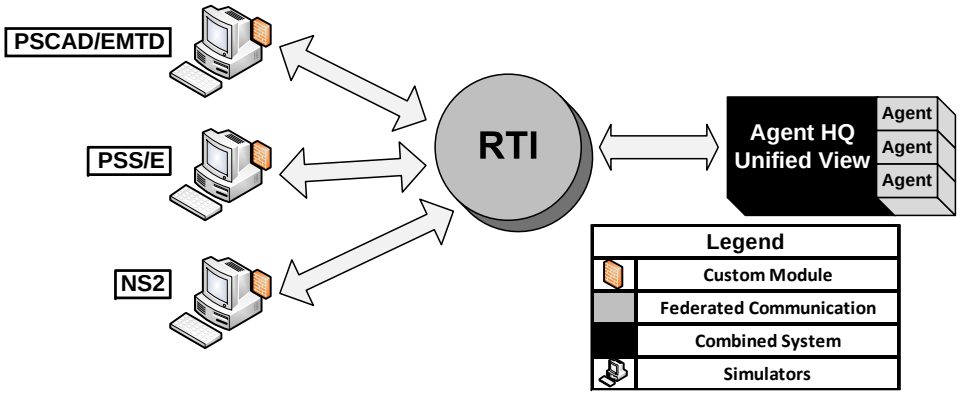

Figure 3.2: The EPOCHS simulation system [57]

Within EPOCHS, there are three specific agent type nodes. These include control, load and generator agents that correspond to their specific PSS/E power simulator components. There is one control agent node, 30 load agent nodes and 50 generator agent nodes utilized in this scenario. Each of these agent nodes have the ability to directly access and modify their corresponding power simulator component's data and to perform power grid related actions such as supervisory control and data acquisition through the communications network. This communications network is a 100 Mega bits per second (Mbps) capacity network which represents the minimum expected capacity for future Internet-like smart grids.

3.4 Research Scenario

This research scenario utilizes the modified version of the IEEE 50 generator / 145 bus power flow test case within PSS/E to demonstrate the benefits of using a con-resistant trust mechanism along with a special protection system. Modifications include modifying generator behaviors, the addition of a 500-kV transmission line, and a reduction of total system capacity [57]. As documented in [57], this test case was modified so that it is more representative of power systems that would require a special protection system mechanism.

The special protection system in this scenario monitors the power grid's frequency for system disturbances that are indicative of imminent fault and attempts to prevent the fault by using two of the most common types of special protection system schemes, namely, generation rejection and load shedding [40]. Recall from Chapter 2 that generation rejection at an appropriate location in the system reduces power to be transferred over the critical transmission interfaces [39]. Additionally, load shedding schemes are employed to reduce the connected load to a level that can be safely supplied by available generation [39].

The scenario starts out with two high capacity transmission lines down resulting in a transiently unstable power grid requiring action from a special protection system. Generator 93 was preselected by SCADA operators for power generation rejection and commanded to trip or go offline by the special protection system. Contingencies resulting from tripping of generators cause an imbalance between generation and load [59]. Depending on the percentage of power loss over total production, the frequency will reach low values. When this happens, other generating units can trip resulting in cascading events leading to power system blackouts unless additional special protection system actions are taken [59]. In this scenario, if the nominal 60 Hz system frequency falls below 58.8 Hz, then the special protection system has failed. As utilized in previous research

[41] [57] [60], 58.8 Hz is the chosen preset frequency threshold for this scenario. Operating below this threshold can cause an increase in generator turbine vibrations ultimately damaging the generator causing it to fail [39].

The additional special protection system action taken in this scenario is load shedding. The goal of the special protection system in this research is to shed enough load to keep the system's frequency above a preset level following a system disturbance such as generation loss [57]. In order to do this, the special protection system used in EPOCHS uses an algorithm to estimate this system's disturbance size and the amount of load shedding required in order to maintain system frequency above 58.8 Hz [57]. This algorithm can be seen in Equation 3.1

$$P_d = P_a + \Delta P_e(w_{0+} - w_{0-}, v_{0+} - v_{0-}) \tag{3.1}$$

Equation 3.1 shows that the size of the disturbance, P_d, is equal to the system accelerating power, P_a, which is proportionate to the change in the system's frequency, plus the change in electrical power demand ΔP_e due to the variation in frequency and voltage. P_d is the key in determining the amount of generation that has been lost. It is important to note that 0− *and* 0+*, respectively, denote the time immediately before and after the disturbance. P_a and ΔP_e can both be obtained based on wide area measurements using the generators operating status and samples of the systems frequency before and after the disturbance, but measurements must be simultaneously taken at points throughout the region.* [57].

SCADA operators have the ability to change the maximum amount of load a node can shed within the special protection system scheme. Typical load shedding strategies include shedding 10%, 15%, or 20% of the available load depending on the severity of the drop in frequency [39], [61]. In this scenario, the maximum load shed amount is set to 20% of the available load for severe drop in system frequency. Once the required load shed amount is determined, it is imposed on selected load agent nodes. A sorting algorithm is then used to determine which nodes are selected for load shedding. In the original special protection system implementation, load agents nodes are sorted based

upon their available load shed amounts. In the special protection system implemented with the con-resistant trust mechanism, load agent nodes are sorted by their assigned trust values and available load shed amounts. The *goal* or *objective* is to prevent a power outage by commanding a minimum number of nodes to load shed a calculated amount of power resulting in the power grid's system frequency remaining above 58.8 Hz [57].

3.4.1 Trust Implementation. The trust management system utilized in this research is primarily derived from the work of Yu and Singh in the field of reputation management in electronic communities where a electronic community represents a set of interacting communities or social interactions [48]. The overall goal of this trust implementation is to avoid interactions with undesirable entities, namely untrusted nodes. The interaction trust (I-Trust) mechanism consists of functions which calculate and maintain I-Trust values, based on a particular interaction marker, for each of the agent nodes communicating within the system. The interaction marker used in this scenario is the reported frequency level for each agent node. The reported frequency level is compared to the preset frequency threshold of 58.8 Hz. The I-Trust value is then calculated based upon that interaction marker. The resulting I-Trust value is then compared to a preset I-Trust value threshold. Agent nodes with an I-Trust value greater than the I-Trust value threshold are considered trusted nodes. Agent nodes with an I-Trust value less than or equal to the I-Trust threshold are considered untrusted nodes. How this I-Trust value is calculated is presented in the following subsection.

3.4.2 How Trust is Calculated. To enforce the previously described trust implementation, an I-Trust value is defined below.

- **DEFINITION 1:** T_{jx} is the trust value assigned by the I-Trust mechanism to node j for interaction marker x. It is required that $-1 < T_{jx} < 1$ and T_{jx} is initialized to zero [48].

The I-Trust mechanism calculates a trust value for agent node j based upon the interactions involving agent node j affecting marker x. Positive (good) and negative (bad) interactions can be defined in terms of game theory as cooperation and defection (non-cooperation) respectively [49]. An agent node is said to be cooperating when it is reporting a frequency value above 58.8 Hz. An agent node is said to be defecting when it is reporting frequency value equal to or below 58.8 Hz. Cooperation interaction by agent node j generates a positive evidence α and a defection interaction by agent node j generates a negative evidence β. Thus requires $\alpha \geq 0$ and $\beta \leq 0$. Values for α and β can be either statically or dynamically assigned depending on the environment in which the trust system is applied. However, trust relationships are such that trust is easy to lose and hard to gain[48]. This relationship is achieved by requiring that $|\alpha| < |\beta|$ and is implemented in DEFINITION 2 below.

- **DEFINITION 2:** After an interaction, the resultant trust value T'_{jx} is calculated by the algorithm presented in Table 3.3 which considers the previous trust value T_{jx} [48].

Table 3.3: Simple Interaction Trust Algorithm [46], [48]

T_{jx}	**Cooperation Interaction by** j	**Defection Interaction by** j
> 0	$T'_{jx} = T_{jx} + \alpha(1 - T_{jx})$	$T'_{jx} = \dfrac{T_{jx} + \beta}{1 - min(\lvert T_{jx}\rvert, \lvert\beta\rvert)}$
< 0	$T'_{jx} = \dfrac{T_{jx} + \alpha}{1 - min(\lvert T_{jx}\rvert, \lvert\alpha\rvert)}$	$T'_{jx} = T_{jx} + \beta(1 + T_{jx})$
$= 0$	α	β

Table 3.3 presents the equations used for calculating the I-Trust values and is referred to as the Simple Interaction Trust Algorithm [46], [48]. In [49], Abari and White tested this algorithm against a confidence attack. As previously stated in Chapter 2 Section 2.7.2,

a confidence attack is based on a sequence of interactions where a con-man entity conducts a series of consecutive cooperative interactions in an attempt to gain the confidence of the system thus elevating its associated trust value. Then at a particular point in time, the con-man will defect, defrauding the victim. The con-man then has two choices: 1) never interact with the victim again or 2) regain the lost trust with subsequent cooperative behavior. The con-man, by regaining the victim's trust, can again con (or defect) the victim [49]. This results in a net benefit to the con-man.

Initial results of the simple interaction trust value calculation tested against a confidence attack are presented in Figure 3.3. A series of simulations were conducted in which a trust-aware agent using the simple interaction trust algorithm in Table 3.3 interacts with a con-man agent utilizing a Simple Con-man Attack (SCA) pattern of Θ [46],[49]. Θ is defined as the number of times a node j cooperatively interacts before a single defection. This Simple Con-man Attack (SCA(Θ)) pattern was repeated for 250 individual interactions.

Figure 3.3 displays the calculated I-Trust values for each attack pattern over a range of 250 interactions. As defined in DEFINITION 1 above, the interaction trust value, T_{jx} has an initial value of zero. The values of α and β were set to 0.05 and -0.5 respectively. In this test conservative values for α and β were set so that trust builds up slowly and is reduced quickly. Even though the negative penalty for a defection, β, is set to ten times the positive reward for a cooperation, α, a con-man choosing a $\Theta > 10$ is known as trustworthy in this particular trust model and depicted in Figure 3.3 [49].

To make the simple interaction trust algorithm proposed by Yu and Singh [48] resistant to a con-man attack, Abari and White proposed implementing the following characteristics [49]:

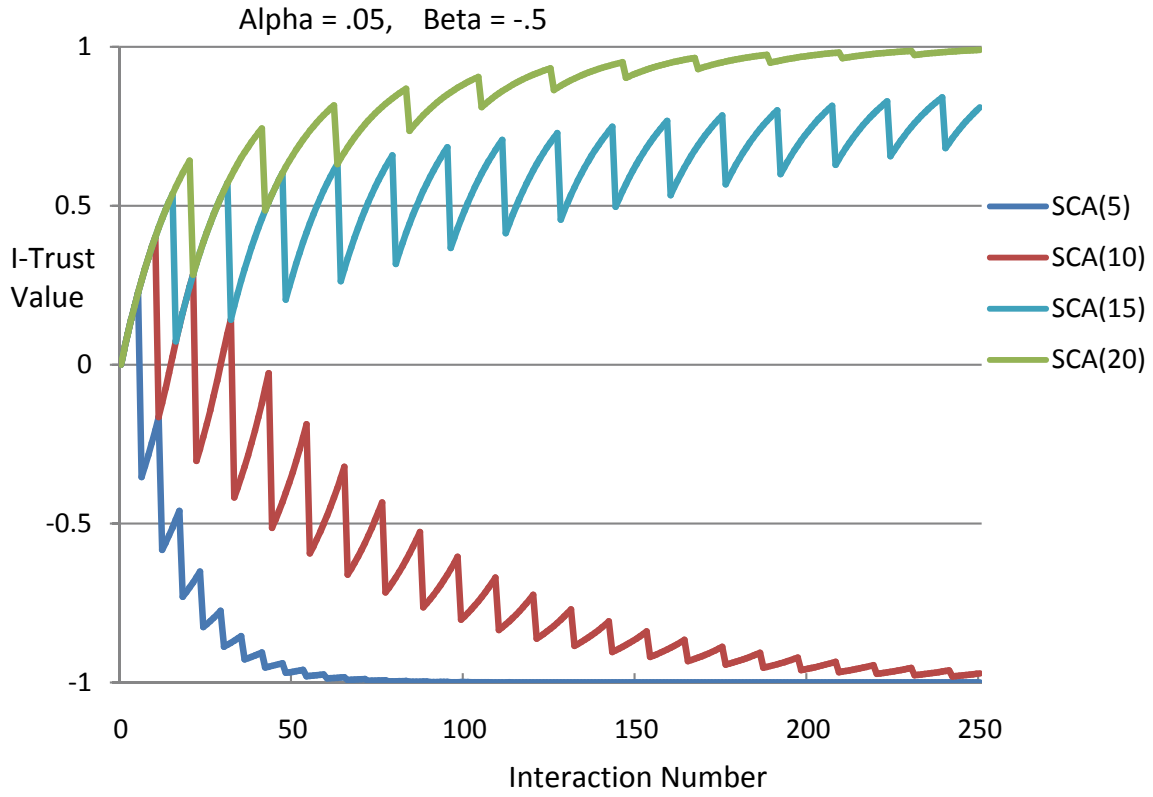

Figure 3.3: Simple I-Trust Value During Confidence Attack [46], [49]

- **Cautiously increment trust after defection:** The more the agent perceives defection, the corresponding trust value should be increased more slowly by perceiving the consecutive cooperations.

- **Larger punishment after each defection:** The more the agent perceives defection, the corresponding trust value should be dropped more sharply by perceiving each defection.

These characteristics are implemented by dynamically adjusting α and β based upon agent node interaction. The modified trust value as defined in DEFINITION 3 below.

- **DEFINITION 3:** α and β are determined for Con-Resistant trust value calculation by the algorithm in Table 3.4, where C is a constant $0 < C \leq 1$.

Table 3.4: Con-Resistant Interaction Trust Algorithm [49]

Cooperation Interaction by j	**Defection Interaction by** j
$\alpha = \min(\alpha + \gamma_c(\alpha_0 - \alpha), \alpha_0)$	$\alpha = \alpha(1 - \lvert\beta\rvert)$ $\beta = \beta - \gamma_d(1 + \beta)$
$\gamma_c = 1 - \lvert\beta\rvert$	$\gamma_d = C \times \lvert T_{jx}\rvert$

Table 3.4 presents the equations used to calculate the con-resistant interaction trust (I-Trust) values and is an extension of Yu and Singh's simple interaction trust algorithm. This extension is referred to as the con-resistant interaction trust algorithm [46], [49]. Here, α is the positive reward for cooperation and β is the negative punishment for defection just like in the simple interaction trust algorithm. However, a defection will decrease α and will increase the absolute value of β based on the characteristics listed above. Additionally, these characteristics are motivated by the fact that forgiveness is slower when several defections have happened, and punishments are bigger for those who defect more [49].

The con-resistant trust algorithm introduces additional variables in it's I-Trust value calculation. The initial value for α is preserved as α_0. Based on the equations presented in Table 3.4, α will increase for each cooperation however it will never exceed α_0 [49]. Furthermore, α is decreased at the rate of $1 - |\beta|$ which results in a large decrement for α for a high value of $|\beta|$ and a small decrement of α for a low value of $|\beta|$ [49]. Additionally, discounting factors, γ_d and γ_c as well as a constant, C, are introduced. γ_d is the discounting factor for a defection and is proportional to the absolute value of the previous I-Trust value, T_{jx}. The authors hypothesized that the discounting factor, γ_d, should be high when the target agent's I-Trust value is close to 1 (trustworthy) or -1 (untrustworthy) which is motivated by the fact "Trust is hard to earn but easy to lose" [49]. Furthermore, the authors believe that if an agent has a high value of β because of previous defections, its

α value should be increased more slowly when it is cooperating, thus γ_c should decrease as the magnitude of β increases [49].

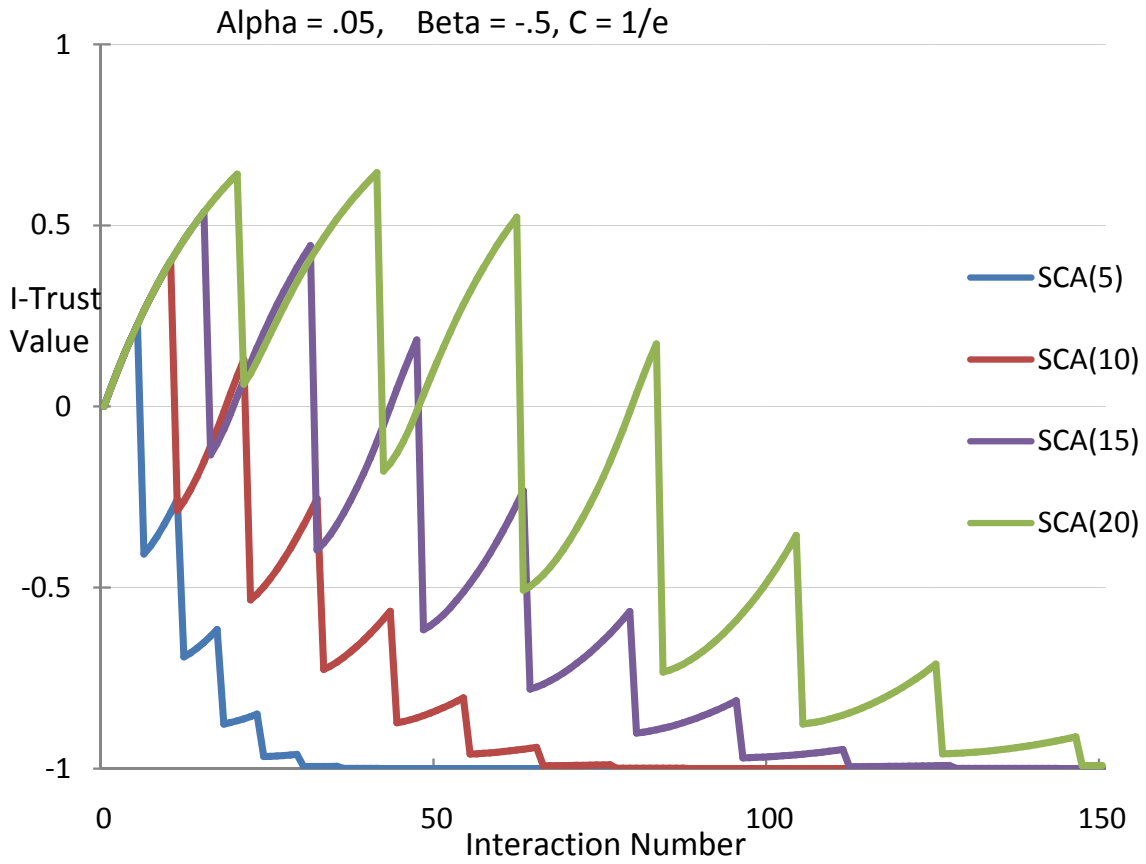

Figure 3.4: Con-Resistant I-Trust Value During Confidence Attack [46], [49]

Figure 3.4 displays the results from testing the con-resistant trust calculation against a confidence attack over a period of interactions. Simulations were run utilizing the same basic settings as previously described for the simple interaction trust calculation during a confidence attack as shown in Figure 3.3. Initial values for α and β (α_0 and β_0) were set to 0.05 and -0.5 respectively. Figure 3.4 shows that regardless of the value of Θ for a Simple Con-man Attack (SCA(Θ)) pattern, the con-man was recognized by the trust mechanism and converged to a low value of trust within 150 interactions [49]. Unlike the simple

interaction trust values, the con-resistant trust values are more severely impacted by the defection activity and none of the interaction patterns converge to a high trust value [46]. In order for the con-man to con the trust-aware agent, it would take a large number of cooperations and a change in its pattern of interactions [49].

3.4.3 Abuse Case. The abuse case used in this scenario is based upon the special protection system's ability to detect untrusted agent node behavior during system updates. Each simulation starts at time zero and runs for 50 seconds to ensure that the power system has stabilized. Throughout the simulation, the special protection system's control agent node receives updates from load and generator agent nodes every two milliseconds. These updates include the load agent nodes current operating frequency level. Additionally, the con-resistant trust mechanism calculates and reports the I-Trust values during each interaction (time step). At time 0.18 seconds, generator 93 is commanded to trip and at time 0.184 seconds it goes offline. Four milliseconds later at time 0.192 seconds, the special protection system makes the determination of which load agent nodes are trusted and untrusted. Success is determined by the special protection system's ability to accurately identify which load agent nodes are trusted and untrusted and it's ability to select the minimum number of optimal trusted nodes to shed load in an attempt to keep the system's steady-state frequency above 58.8 Hz. Conversely, if the special protection system selects and untrusted node to shed load, the untrusted node will not shed load causing the system steady-state frequency to fall below the 58.8 Hz threshold.

3.5 Performance Metrics

The primary metric used to evaluate the performance of the special protection system implemented with and without the con-resistant trust mechanism is the system frequency. The critical system frequency threshold is 58.8 Hz. Operating below this threshold can cause an increase in generator turbine vibrations ultimately damaging the generator

causing it to fail potentially leading to cascading events such as power system blackouts [39].

3.6 System Parameters

Systems parameters are characteristics of the system, that if changed will affect the performance of the special protection system implemented with a con-resistant trust mechanism. These parameters include the following:

- Frequency tolerance
- α value
- β value
- Constant, C

In Fadul's enhanced Special Protection Protection System with the Reputation-based Trust Management Toolkit [41], untrusted nodes were designated by subtracting a fixed value or tolerance from the reported frequency level. In this research, the tolerance value is randomized to simulate realistic fluctuations in frequency due to inherent noise.

The α and β values chosen in Abari and White's extension of the simple interaction trust algorithm were based on a 1 to 10 penalty ratio for cooperative to defective interactions [49]. Specifically, they choose 0.05 and -0.5 respectively for cooperation (α) and defection (β). Hundreds of interactions occur before a trust determination is made. In this research, a 1 to 3 penalty ratio is utilized for the cooperative and defective interactions, specifically 0.15 for α and -0.45 for β. Unlike previous research, this research requires a trust determination within 17 interactions (time steps). In the special protection system, there is not enough time to recover from a such a large defection penalty.

Finally, the constant C, is utilized as a multiple for calculating the defection discounting factor, γ_d, as seen in Table 3.4. In previous research [49], C is a value between

zero and one in which the authors chose $\frac{1}{e}$. In this research, $C = 0.3679$ which is equivalent to $\frac{1}{e}$.

3.7 Evaluation Technique

Performance evaluation of the special protection system implemented with a con-resistant trust mechanism using simulations is the chosen evaluation technique for this research. Additionally, the Analysis of Variance (ANOVA) and a comparison of confidence intervals via the open source R statistical package [62] [63] is the analysis procedure used to determine the statistical significance of the simulation results. An ANOVA is a statistical procedure that can be used to test the hypothesis that whether or not the means among two or more groups are equal, under the assumption that the sampled populations are normally distributed [64].

3.8 Experimental Design

To evaluate the interaction between all factors and to ensure every factor level combination is considered, a full factorial design is used. The special protection system experiments have two factors: 1) number of untrusted nodes and 2) whether the special protection system utilizes the con-resistant trust mechanism or it doesn't. There are three treatment levels of untrusted nodes: five, ten, or fifteen. The full factorial design requires three levels by two (3×2) factors which results in a total of six experiments. Each experiment is then replicated 36 times for a total of 216 simulations.

The research utilizes NS2's predefined 64 good random seed values in the rng.cc file for computer simulation experiments [65]. These random seed values are equally spaced around a 2^{31} cycle of random numbers, where each seed value is approximately 33,000,000 elements apart from each other. The seeds are selected from the rng.cc file to match past research and to aid a more direct comparison of simulation results with each replication of the experiment utilizing a unique seed. Thirty six of these seed values are

used for data collection in each test case configuration. Additionally, the seeds are used to select the untrusted nodes in each simulation. The data collected during each observation is the minimum power grid system frequency. This frequency data is then analyzed and interpreted to evaluate the effectiveness of the con-resistant trust mechanism.

Frequency data from the ”Original SPS test case with 5 untrusted nodes” is used to determine the data’s normality. Figure 3.5 is a histogram plot of the collected frequency data. Histograms are graphics commonly used to display data distributions for quantitative variables [66]. The histogram in Figure 3.5 graphically reveals the qualities of a normal bell curve and visually suggests that the sampled data collected are from a normally distributed population.

An additional plot to visually confirm that the sampled data is from a normally distributed population is a normal quantile plot. This normal quantile plot of the collected data is depicted in Figure 3.6. A normal quantile plot (also called a normal probability plot) is a specialized type of graphic that is used to determine whether or not data for a variable are normally distributed [66]. When the sample data value points in the normal quantile plot lie close to a straight line with a slope of one, this indicates that the data are normally distributed [66]. Figure 3.6 suggests that the sample data is being drawn from a normally distributed population since the sample data lands very close to the line representing the theoretical normal distribution for the sample data.

To statistically support that the sampled data are from a normal distribution, a Shapiro-Wilk normality test [67] is conducted. The Shapiro-Wilk normality statistic tests the null hypothesis that the sample data came from a normally distributed population [67]. The null hypothesis is that the population is normally distributed. If the p-value is less than the chosen alpha value, then the null hypothesis is rejected (i.e. the data are not from a normally distributed population). If the p-value is greater than the chosen alpha value, then the null hypothesis is accepted (i.e. the data are from a normally distributed

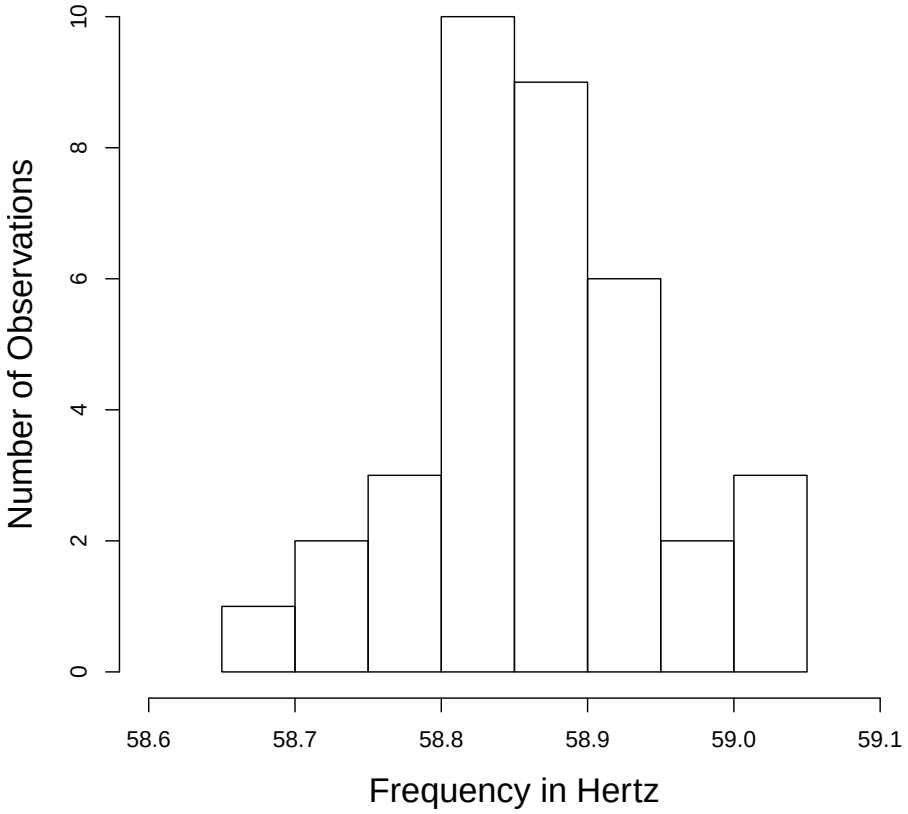

Figure 3.5: Histogram for original SPS and 5 untrusted nodes

population). The selected confidence interval level of 95% corresponds to a statistical alpha value of 5%. A Shapiro-Wilk normality test confirms the normal distribution of the sampled data with a p-value of 0.5614 and a W value of 0.9745. The W value of 0.9745 is close to one and supports the null hypothesis. At the 95% confidence interval, the samples p-value greater than 0.05 results in the overall acceptance of the null hypothesis.

3.9 Summary

This chapter presented the methodology used to evaluate the application of a con-resistant trust mechanism with a special protection system for the smart grid. The

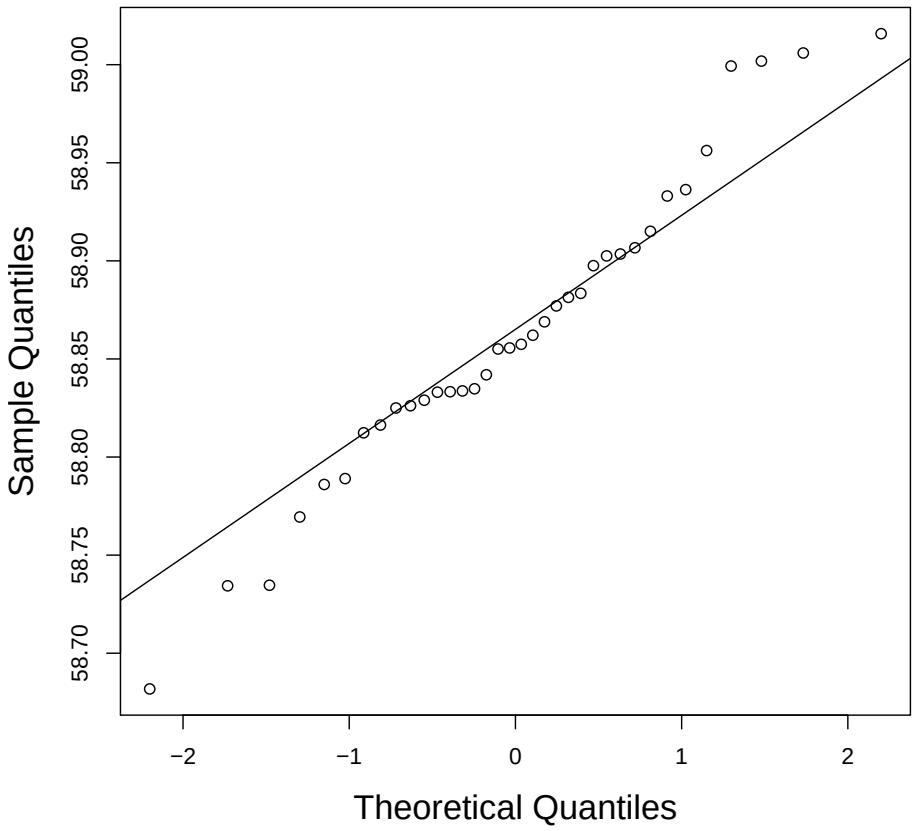

Figure 3.6: Normal quantile plot for original SPS and 5 untrusted nodes

chapter began by identifying research goals and the hypothesis. Next, the simulation environment was discussed followed by a detailed explanation of the research scenario to include the con-resistant trust implementation, how the con-resistant interaction trust (I-Trust) value is calculated, and the abuse case used. Additionally, the primary performance metric, system parameters, and the evaluation technique used to determine statistical significance of the simulation results within a 95% confidence interval are identified. Finally, an explanation of the experimental design was presented along with the validation of determining the sampled data are from a normally distributed population.

4 Results

4.1 Overview

This chapter presents the results from experimental simulations and an analysis of the results from implementing special protection system with a con-resistant trust mechanism for the communications-based smart grid utility network. First, results from con-resistant trust mechanism implementation at each of the three treatment levels of five, ten, and fifteen untrusted nodes are presented. Additionally, individual interactions of untrusted protection system nodes are analyzed for each of the three treatment levels. Finally, the chapter concludes with an overall analysis of the results to include a comparison of the research treatments as well as addressing the investigative questions introduced in Chapter 1.

4.2 Experimental Results

The primary goal of this research is to demonstrate that a special protection system implemented with con-resistant trust mechanism can successfully function in the presence of untrusted (malicious or malfunctioning) smart grid special protection system nodes. Success is determined by the special protection systems ability to accurately identify which load agent nodes are trusted and untrusted and its ability to select the minimum number of optimal trusted nodes to shed load in an attempt to keep the systems steady-state frequency above 58.8 Hz. Table 3.2 provided an example of how nodes are sorted and selected for load shedding.

Simulation results support the use of a special protection system implemented with a con-resistant trust mechanism for the communications-based smart grid over the use of a traditional special protection systems. Figures 4.1 and 4.2 show frequency levels of the original special protection system without any trust implementation and the special

protection system implemented with the con-resistant trust mechanism respectively during simulations. Results depicted in Figure 4.2 demonstrate that the special protection system implemented with the con-resistant trust mechanism can successfully keep the system's steady state frequency above the 58.8 HZ whereas the original special protection system without any trust implementation depicted in Figure 4.1 does not.

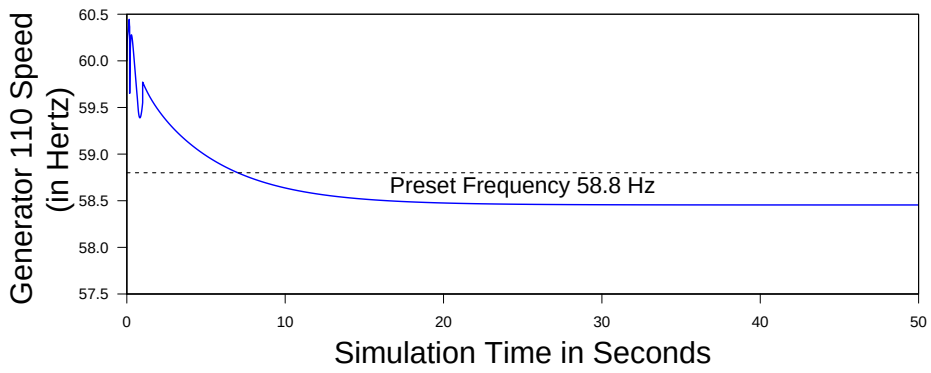

Figure 4.1: Original SPS is unable to keep the systems's frequency above 58.8 Hz

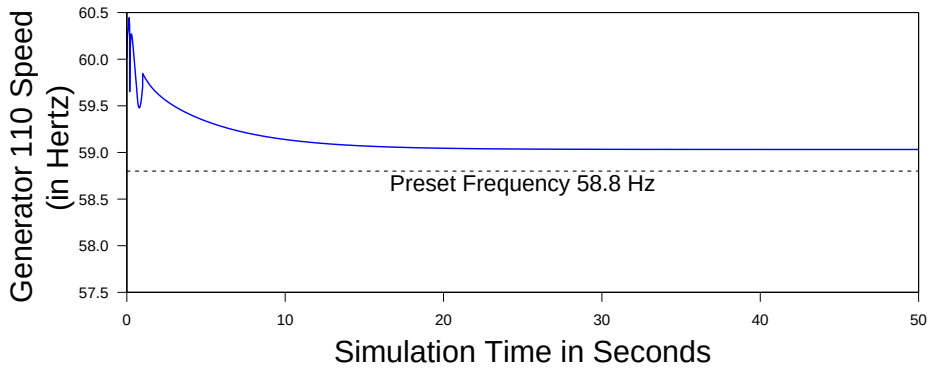

Figure 4.2: SPS implemented with con-resistant trust does keep the system's frequency above 58.8 Hz

As previously stated in section 3.7 of Chapter 3, the special protection system experiments have two factors and three treatment levels. The factors are the number of untrusted nodes and whether or not the special protection system utilizes the con-resistant trust mechanism. The three treatment levels are five, ten, and fifteen untrusted nodes.

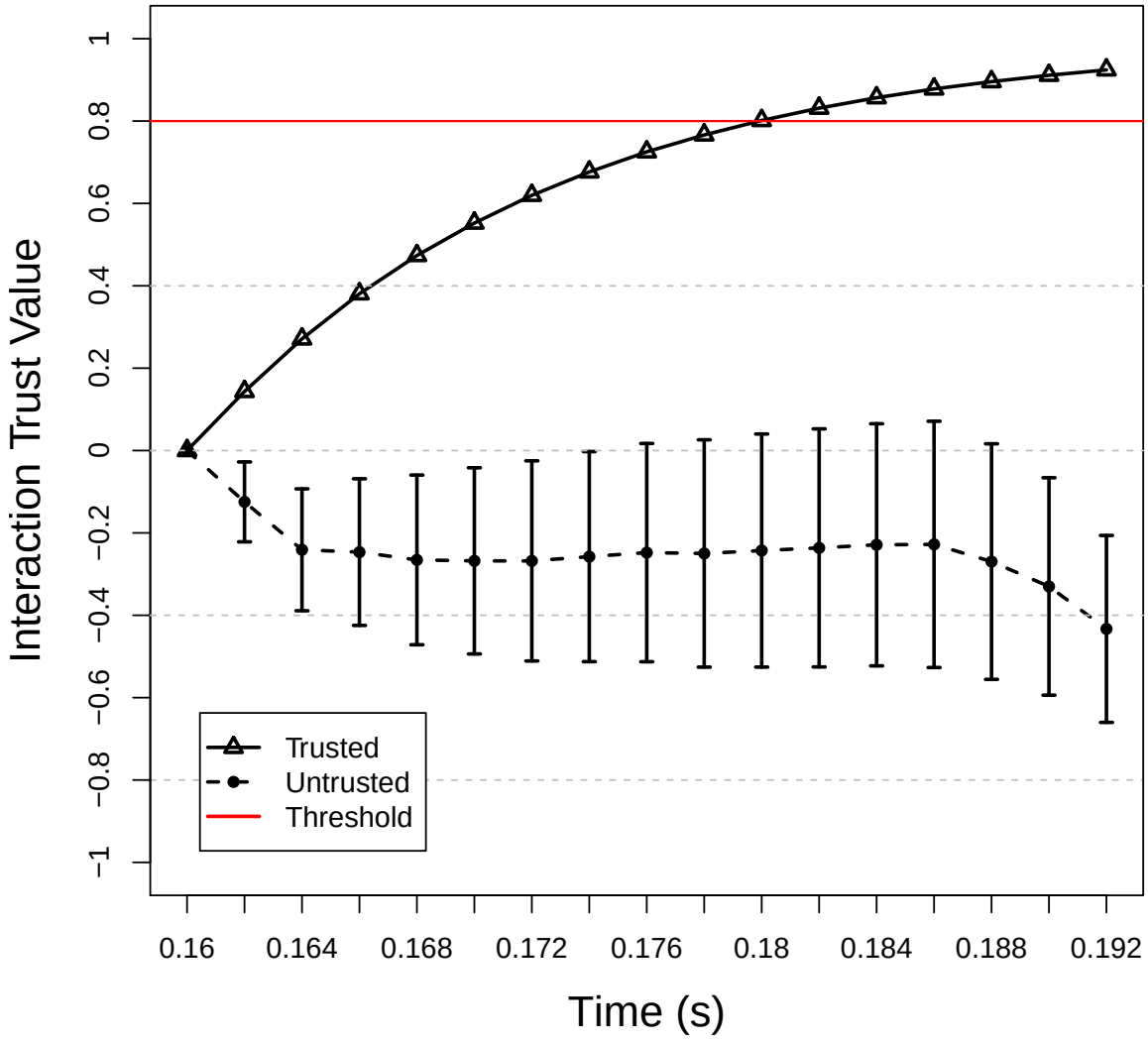

Figure 4.3: Mean con-resistant trust results with 5 untrusted nodes

Figures 4.3, 4.4, and 4.5 represent the mean con-resistant interaction trust (I-Trust) values as determined by the special protection system con-resistant trust mechanism

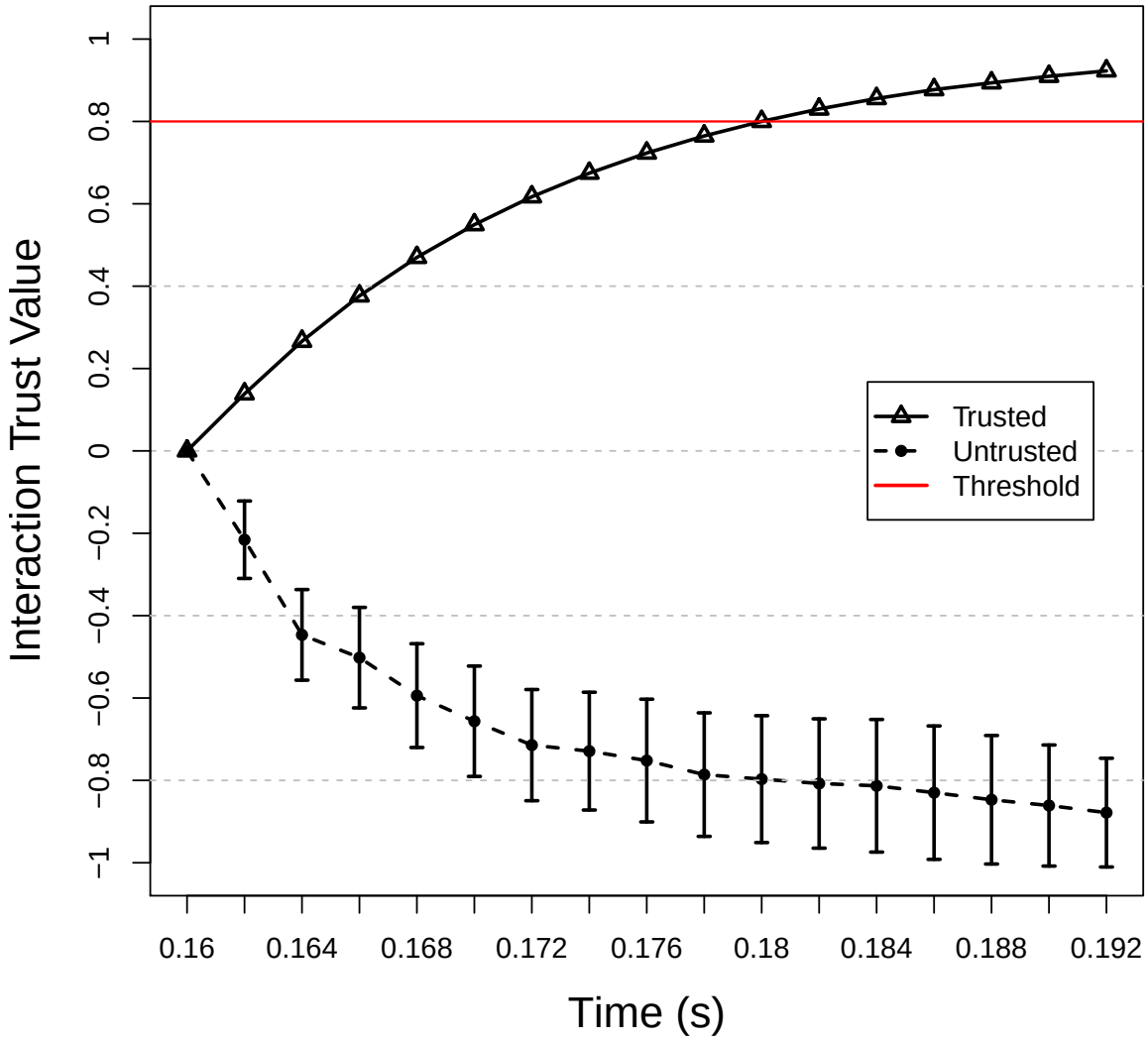

Figure 4.4: Mean con-resistant trust results with 10 untrusted nodes

during 36 simulation runs for each of the 3 treatment levels. At time 0.180 seconds, Generator 93 is commanded to trip. At time 0.184 seconds, Generator 93 goes offline. At time 0.192 seconds, the special protection system makes the determination of which load agent nodes are trusted and untrusted. The error bars represent a 95% confidence interval.

The special protection system implemented with the con-resistant trust mechanism is tuned to minimize the possibility of identifying unreliable nodes as trusted. Several experiments were conducted to corroborate this behavior. Empirical data showed that the

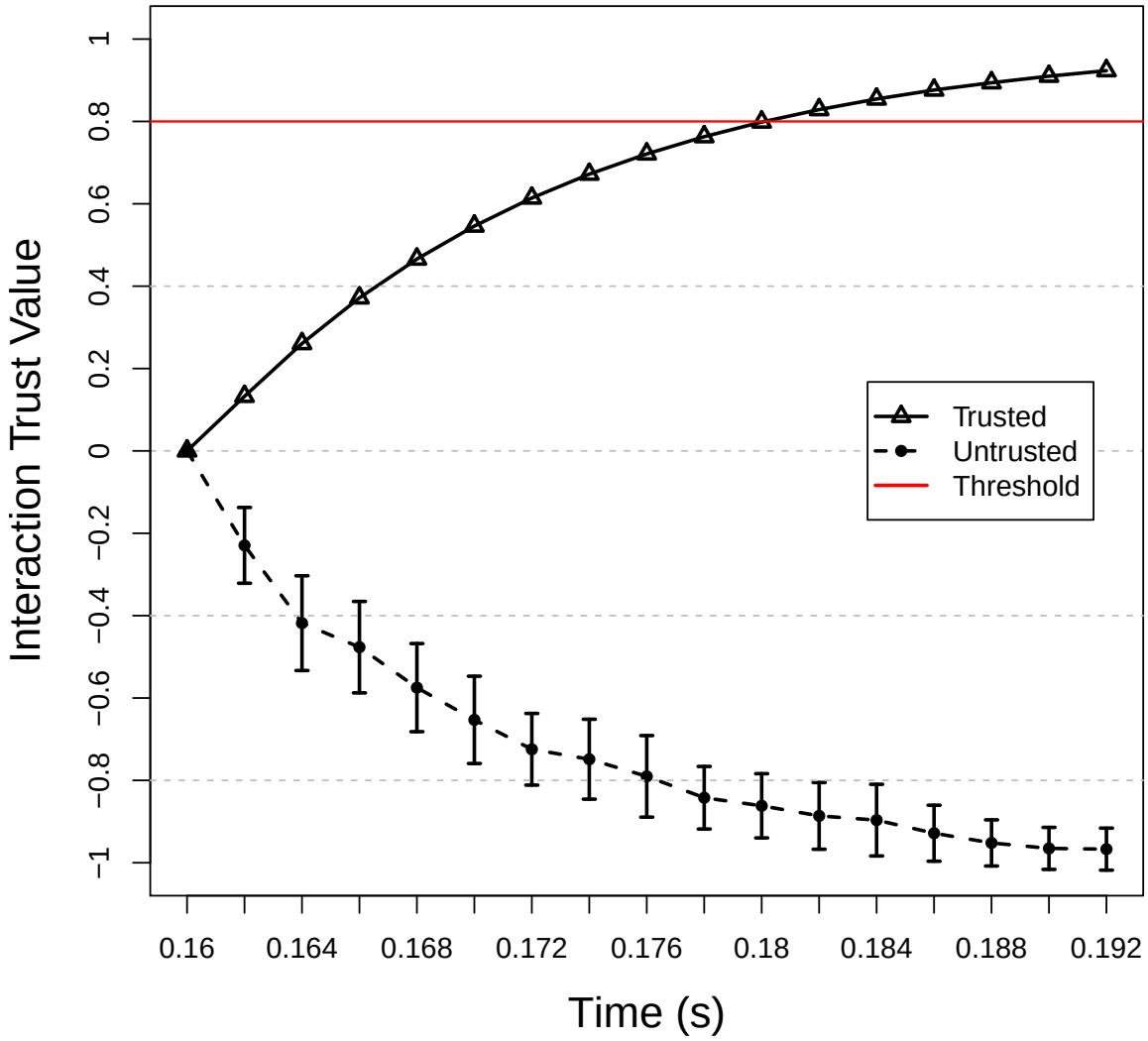

Figure 4.5: Mean con-resistant trust results with 15 untrusted nodes

mean error associated with a 95% confidence interval for the trusted nodes is negligible (< 0.0027). From this, it is evident that the system is capable of identifying nodes that exhibit cooperative behaviors with a high degree of certainty. However, it is possible for the trust mechanism to classify a node with cooperative behavior as *untrusted* for a short interval, if its frequency reading deviates significantly from the mean frequency of all nodes. For this reason, the error associated with untrusted node determination is greater than the trusted node determination.

Figure 4.3 shows that the error associated with a 95% confidence interval for five untrusted nodes increases over the course of the simulation run time. The larger error signifies a presence of false negatives, i.e. a reliable node reporting as untrusted. However, at time 0.192 seconds, when the final trust determination is made, the high and low interaction trust (I-Trust) values representing a 95% confidence interval for the five untrusted node experiment are -0.20614 and -0.66014 respectively. These values fall well below the trust threshold set by Supervisory Control And Data Acquisition (SCADA) operators and would not be selected by the special protection system for load shedding.

As the number of untrusted nodes increase, the number of false negatives decreases. This is evident with the ten and fifteen untrusted node experiments depicted in Figures 4.4 and 4.5 respectively. The high and low I-Trust values representing a 95% confidence interval for ten untrusted nodes at time 0.192 seconds are -0.74631 and -1.01031. Similarly, the high and low I-Trust values representing a 95% confidence intervals for fifteen untrusted nodes at time 0.192 seconds are -0.916 and -1.018. In both cases, the I-Trust values fall well below the trust threshold set by Supervisory Control And Data Acquisition (SCADA) operators and would not be selected by the special protection system for load shedding.

Figure 4.6 depicts the individual cooperative and defective interactions of five untrusted nodes as determined by the special protection system con-resistant trust mechanism during one simulation run. Here, the untrusted nodes interaction trust (I-Trust) values are severely impacted by the defection activity. Four out of the five (or 80%) of the untrusted nodes exhibited cooperative behaviors; however, none of the untrusted nodes' interaction patterns converged to a high I-Trust value. In order for a untrusted node to be trusted, it would take a significant number of cooperations and a considerable amount of time. However, due to the strict timing constraints of Supervisory Control And Data Acquisition (SCADA) systems and the smart grid, special protection system decisions

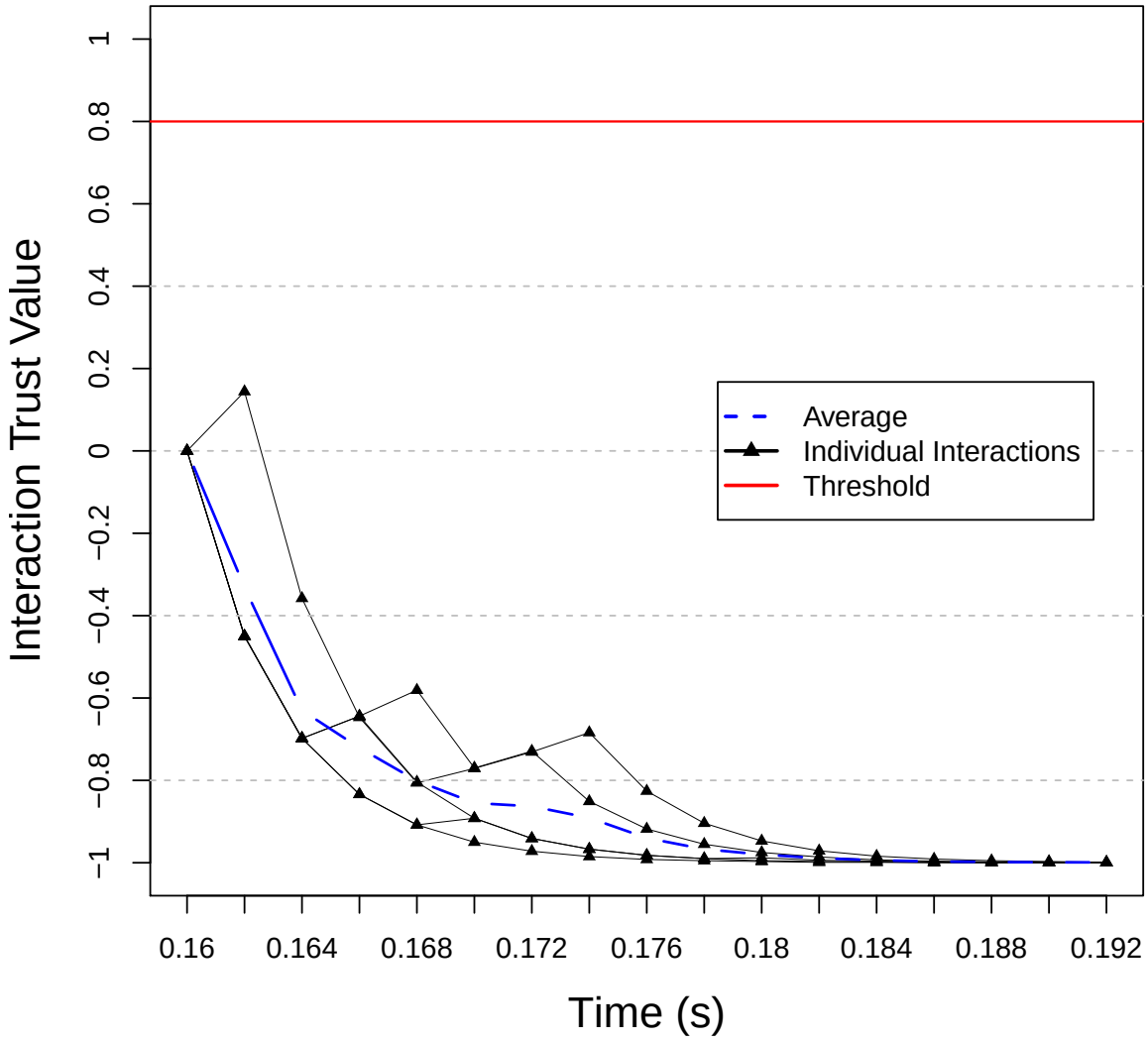

Figure 4.6: Individual cooperative and defective interactions for 5 untrusted nodes during one simulation run

have to be made quickly in order to prevent additional transient instabilities that could result in cascading power outages.

Figure 4.7 depicts the individual cooperative and defective interactions of ten untrusted nodes as determined by the special protection system con-resistant trust mechanism during one simulation run. As with the five untrusted node interactions case, the ten untrusted nodes interaction trust (I-Trust) values are also severely impacted by the

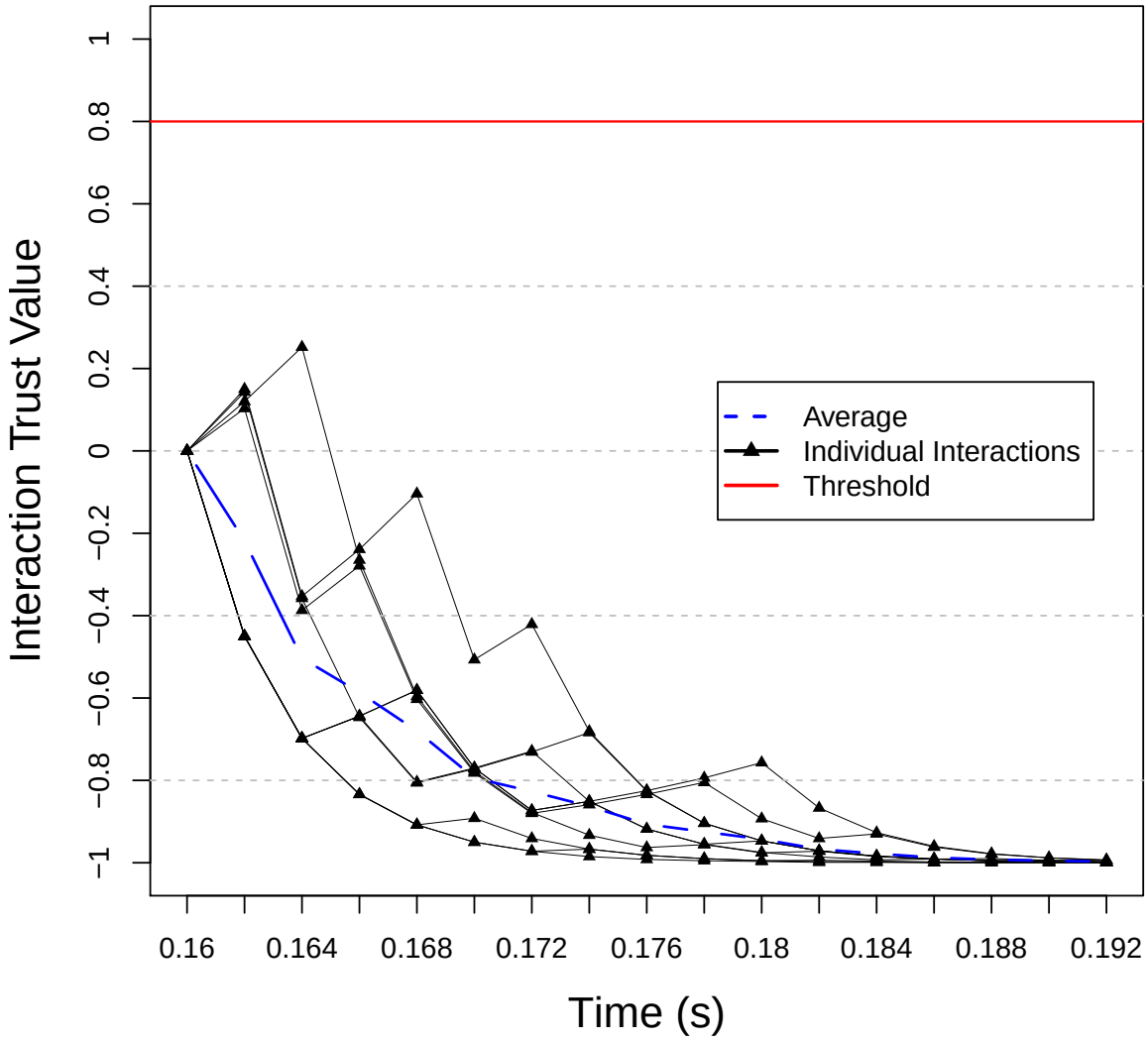

Figure 4.7: Individual cooperative and defective interactions for 10 untrusted nodes during one simulation run

defection activity. In this simulation, 90% of the untrusted nodes exhibit cooperative behaviors. Just as in the five individual untrusted node interactions, none of the ten untrusted nodes converge to a high I-Trust value. At the point in the simulation when the final trust determination is made, all of the untrusted nodes converge to a -1.0 I-Trust value.

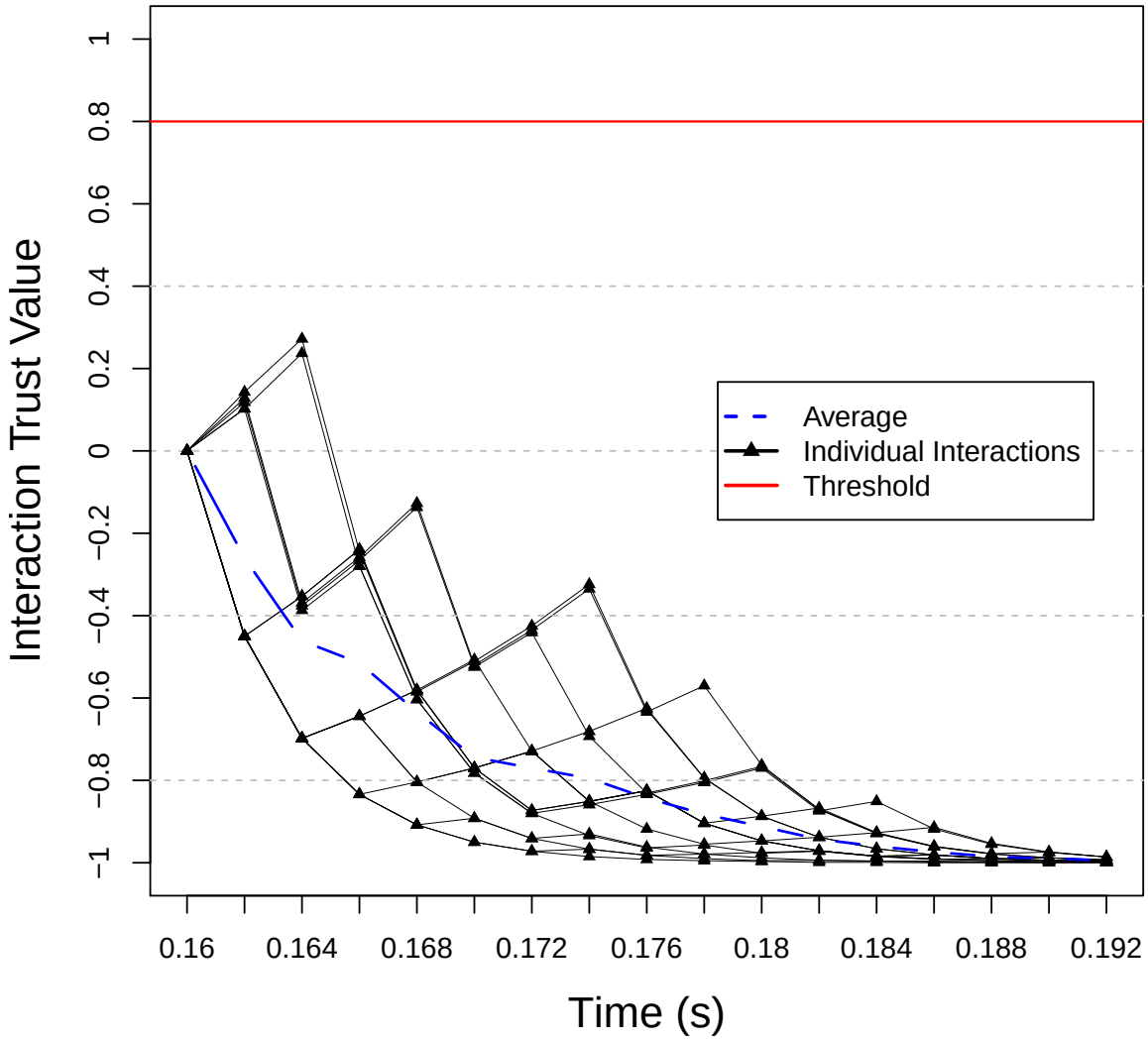

Figure 4.8: Individual cooperative and defective interactions for 15 untrusted nodes during one simulation run

Figure 4.8 depicts the individual cooperative and defective interactions of fifteen untrusted nodes as determined by the special protection system con-resistant trust mechanism during one simulation run. As with the five and ten untrusted node interaction cases, the fifteen untrusted nodes interaction trust (I-Trust) values are also severely impacted by the defection activity. In this simulation, 93.3% of the untrusted nodes exhibit cooperative behaviors. Just as in the five and ten individual untrusted node interaction cases, none of the fifteen untrusted nodes converge to a high I-Trust value. At

the point in the simulation when the final trust determination is made, all of the untrusted nodes converge to a -1.0 I-Trust value.

4.3 Overall Analysis

Comparison of the experiments conducted at each of the treatment levels, for each factor, are presented in Figure 4.9. Each bar plot represents the mean steady state frequency reported at the end of each simulation run. The error bars represent a 95% confidence interval. The graphical results in Figure 4.9 are presented as an Analysis of Variance (ANOVA) where the variance about the mean values is represented by 95% confidence intervals. The non-overlapping confidence intervals illustrate a statistically significant difference between the original special protection system without any trust mechanism and the special protection system implemented with the con-resistant trust mechanism.

Table 4.1: ANOVA numerical calculation results between SPS with no trust and SPS with con-resistant trust

```
Analysis of Variance Table

Response: Frequency
                 Df Sum Sq Mean Sq  F value    Pr(>F)
Treatment         1 6.9154  6.9154 1069.523 < 2.2e-16 ***
Levels            2 1.2876  0.6438   99.572 < 2.2e-16 ***
Treatment:Levels  2 1.1653  0.5827   90.114 < 2.2e-16 ***
Residuals       210 1.3578  0.0065
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1
```

The ANOVA numerical calculations were performed using the R statistical package [62], [63]. These calculation results are shown in Table 4.1 and indicate a significant statistical difference between the two factors (with and without trust mechanism). The p-value, Pr(>F), is less than $2.2x10^{-16}$, which is smaller than an alpha value of 0.05

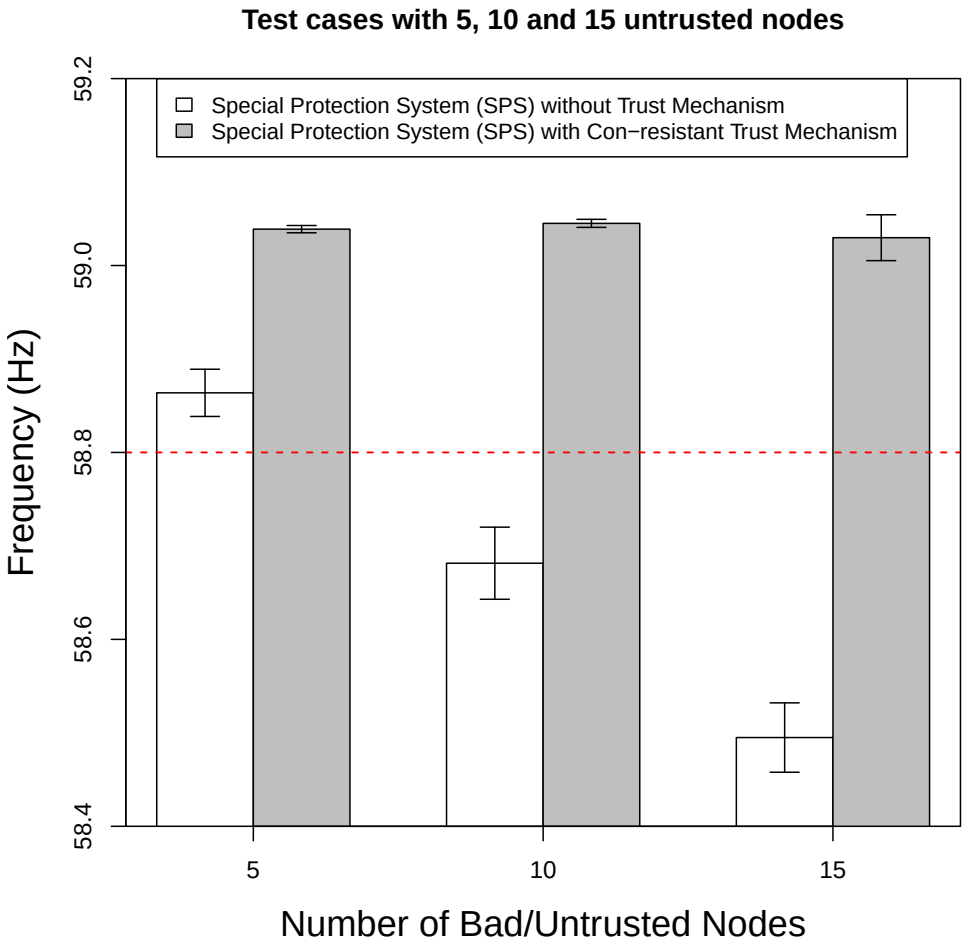

Figure 4.9: Comparison of test treatments with 5, 10 and 15 untrusted nodes

associated with a 95%confidence interval. The small p-value is convincing evidence of a statistical difference between the two factors.

Figure 4.10 shows the comparison of trust implementations conducted at each of the treatment levels, including the original special protection system without any trust implementation, the special protection system implemented with the majority-rules reputation-based trust from previous research [41] and the special protection system implemented with con-resistant trust utilized in this research. Each bar plot represents the mean steady state frequency reported at the end of each simulation run. The error bars

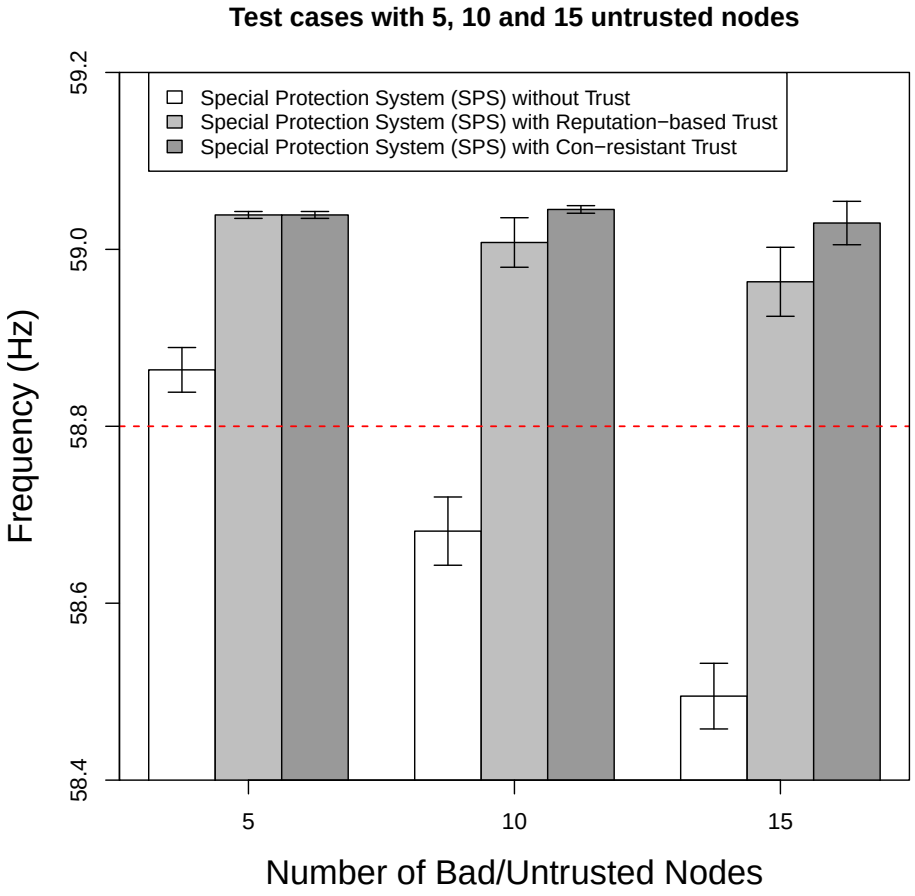

Figure 4.10: Previous research comparison of test treatments with 5, 10 and 15 untrusted nodes [41]

represent a 95% confidence interval. A visual analysis between the two trust implementations shows that the special protection system implemented with either the majority-rules reputation-based trust or the con-resistant trust is able to successfully keep the system's steady state frequency above 58.8 Hz across all three treatment levels.

Results from an ANOVA analysis shown in Table 4.2 indicate a statistical difference between the special protection system implemented with con-resistant trust and the special protection system implemented with reputation-based trust from previous research [41]. The ANOVA calculations were performed using the R statistical package [62], [63].

Table 4.2: ANOVA numerical calculation results between SPS with reputation-based trust and SPS with con-resistant trust

```
Analysis of Variance Table

Response: Frequency
                  Df  Sum Sq  Mean Sq F value    Pr(>F)
Treatment          1 0.06463 0.064630 13.9985 0.0002361 ***
Levels             2 0.06820 0.034099  7.3856 0.0007948 ***
Treatment:Levels   2 0.03993 0.019964  4.3240 0.0144454 *
Residuals        210 0.96955 0.004617
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1
```

Results from the ANOVA analysis show that the p-value, Pr(>F), is approximately 0.0002, which is smaller than an alpha value of 0.05 associated with a 95% confidence interval. The small p-value is convincing evidence of a statistical difference between the special protection system implemented with con-resistant trust and the special protection system implemented with reputation-based trust from previous research [41].

Furthermore, R's pairwise t.test was conducted between treatments levels to determine were the difference lies [62], [63]. Results from the pairwise t.test indicate a significant statistical difference between 5 and 15 untrusted nodes with an associated p-value of 0.0004 and the 10 and 15 untrusted nodes with an associated p-value of 0.0123. These p-values are smaller than an alpha value of 0.05 associated with a 95% confidence interval which is convincing evidence of a statistical difference between the 5 and 15 untrusted nodes as well as the 10 and 15 untrusted nodes. Additionally, the pairwise t.test results also indicated no statistical difference between 5 and 10 untrusted nodes in which the associated p-value was 0.29361.

4.3.1 Investigative Questions Answered. The analysis of this research indicates that a special protection system implemented with the con-resistant trust mechanism can successfully determine and execute the appropriate load shedding strategy in the presence

of untrusted (malicious or malfunctioning) protection system agent nodes during system wide disturbances. Additionally, over all the experiments, the special protection system implemented with con-resistant trust mechanism was able to successfully keep the system's steady state frequency above the 58.8 Hz threshold. Furthermore, the special protection system implemented with the con-resistant trust mechanism out performs the special protection system implemented with a majority-rules reputation-based Trust Management Toolkit at the 10 and 15 untrusted node levels.

4.4 Summary

This chapter provided the results from experimental simulations and an analysis of the results from implementing Sspecial protection system with a con-resistant trust mechanism for the communications-based smart grid utility network. First, the research analyzed if the two different test factors were able to successfully keep the system steady-state frequency above the 58.8 Hz threshold. Next, the research examined the simulation results from the special protection system implemented with the con-resistant trust mechanism at each of the three treatment levels. Additionally, individual interactions of untrusted nodes were presented and analyzed to demonstrate the cooperative and defective interaction behaviors. Finally, the chapter concluded with an overall analysis to determine the statistical significance of simulation results via an Analysis of Variance (ANOVA) and also addressed investigative questions introduced in Chapter 1. Simulation results supported the use of a special protection system implemented with a con-resistant trust mechanism for the smart grid over the use of a traditional special protection systems.

5 Conclusion

5.1 Overview

This chapter summarizes the overall conclusions of the research. First, it reviews the primary goals and results from this research effort to implement a con-resistant trust mechanism within the special protection system for the communications-based smart grid. Next, the significance of this research is discussed. Finally, recommendations for future work is presented.

5.2 Conclusions of Research

The primary goal of this research was to demonstrate that a special protection system implemented with a con-resistant trust mechanism can successfully function in the presence of untrusted (malicious or malfunctioning) smart grid special protection system nodes by implementing appropriate load shedding strategies to mitigate transient instabilities that can occur. Success was determined by the special protection systems ability to accurately identify which load agent nodes are trusted and untrusted and its ability to select the minimum number of optimal trusted nodes to shed load in an attempt to keep the systems steady-state frequency above 58.8 Hz. Simulation results support the use of an special protection system implemented with a con-resistant trust mechanism for the smart grid over the use of a traditional special protection systems. Results showed that the special protection system implemented with a con-resistant trust mechanism was able to successfully keep the system's steady state frequency above the 58.8 Hz threshold. Additionally, the special protection system implemented with a con-resistant trust mechanism successfully identified nodes that exhibit cooperative behaviors as trusted and nodes that exhibited defective behaviors as untrusted with a high degree of certainty. Finally, the overall statistical analysis of experiments conducted at each of the treatment

levels, for each factor, suggests a statistically significant difference between the two systems and supports the use of an special protection system implemented with the con-resistant trust mechanism versus an special protection system without the con-resistant trust mechanism.

5.3 Significance of Research

This research presented an alternate application of trust for special protection systems within a communications-based smart grid. While similar to previous research [41] utilizing majority-rules reputation-based trust, certain experimental parameters were changed to provide a more realistic research scenario. The results of this research demonstrates the successful functioning of a special protection system, implemented with a con-resistant trust mechanism, in the presence of untrusted (malicious or malfunctioning) smart grid special protection system nodes. Furthermore, the research demonstrated that, in this particular scenario, using this specific simulation environment, the special protection system implemented with the con-resistant trust mechanism works.

5.4 Recommendations for Future Work

This research consisted of an effort to apply an alternate application of trust to communications-based special protection systems for the smart grid. Trust, as it relates to special protection systems, can be extended in several ways. Recommendations for future work include the following:

- Implement additional abuses cases to test the robustness of the special protection system implemented with a con-resistant trust mechanism
- Incorporate a multi-trust mechanism approach to make a single trust decision about an entity regarding a complex trust relationship [47]

- Implement a context sensitive model of trust by formalizing the relationships between contexts to extrapolate values from related contexts to approximate the trust of an entity, even when all information needed to calculate the trust is not available [43]

Bibliography

[1] U.S. Department of Homeland Security, November 2010. [Online]. Available: http://www.dhs.gov/files/programs/gc_1189168948944.shtm

[2] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies," *IEEE Control Systems*, pp. 11–25, December 2001.

[3] U.S.-Canada Power System Outage Task Force and U.S. Dept. of Energy, *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*. Washington, DC: U.S. Dept. of Energy, 2004.

[4] National Infrastructure Advisory Council, *Critical Infrastructure Resilience Final Report and Recommendations*. Washington, DC: Department of Homeland Security, 2009.

[5] R. L. Krutz, *Securing SCADA Systems*. Indianapolis, IN: Wiley, 2006.

[6] C. W. Gellings, *The Smart Grid: Enabling Energy Efficiency and Demand Response*. Lilburn, GA: Fairmont Pr, 2009.

[7] T. Flick and J. Morehouse, *Securing the Smart Grid: Next Generation Power Grid Security*. Burlington, MA: Syngress, 2010.

[8] M. Brandle and M. Nadele, "Security for Process Control Systems: An Overview," *IEEE Security & Privacy*, vol. 6, no. 6, pp. 24–29, 2008.

[9] P. Anderson, *Power System Protection*. New York: McGraw-Hill, 1999.

[10] J. Moteff and P. Parfomak, *Critical Infrastructure and Key Assets: Definition and Identification*. Washington, DC: The Library of Congress, 2004.

[11] T. O'Rourke, "Critical Infrastructure, Interdependencies, and Resilience," *The Bridge*, vol. 37, no. 1, pp. 22–29, 2007.

[12] W. J. Clinton, *United States Policy on Terrorism (PDD 63)*. Washington, DC: Whitehouse, 1998.

[13] 42nd U.S. Congress, *United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001*. Washington, DC: Government Printing Office, 2001.

[14] 107th U.S. Congress, *Homeland Security Act of 2002*. Washington, DC: Government Printing Office, 2002.

[15] G. W. Bush, *Critical Infrastructure Identification, Prioritization, and Protection (HSPD-7)*. Washington, DC: Whitehouse, 2003.

[16] G. C. Wilshusen, *Congressional Testimony on Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure*. Washington, DC: U.S. Congress House of Representatives Energy and Commerce Committee, Subcommittee on Oversight Investigations (GAO-11-865T), 2011.

[17] Merriam-Webster, "lifeline," March 2012. [Online]. Available: http://www.merriam-webster.com/dictionary/lifeline

[18] U.S. Department of Energy, "Energy Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan," Washington, DC, 2010.

[19] M. Chertoff, *National Infrastructure Protection Plan*. Washington, DC: Department of Homeland Security, 2009.

[20] Government Accounting Office, *Critical Infrastructure Protection: DHS Efforts to Assess and Promote Resiliency Are Evolving but Program Management Could Be Strengthened, GAO-10-772*. Washington, DC: Author, 2010.

[21] U.S. Energy Information Admisitration, February 2012. [Online]. Available: http://www.eia.gov/energyexplained/index.cfm?page=electricity_in_the_united_states

[22] J. Weiss, *Protecting Industrial Control Systems from Electronic Threats*. New York, NY: Momentum Press, 2010.

[23] Federal Energy Regulatory Commission, "What FERC Does," May 2012. [Online]. Available: http://www.ferc.gov/about/ferc-does.asp

[24] North American Electric Reliability Corporation (NERC), "Company Overview: History," March 2012. [Online]. Available: http://www.nerc.com/page.php?cid=1%7C7%7C11

[25] 109th U.S. Congress, *U.S. Energy Policy Act*. Washington, DC: GPO, 2005.

[26] North American Electric Reliability Corporation (NERC), "Definition of Bulk Electric System," April 2012. [Online]. Available: http://www.nerc.com/filez/standards/Project2010-17_BES.html

[27] NERC, "Standards: Reliability Standards," March 2012. [Online]. Available: http://www.nerc.com/page.php?cid=2%7C20

[28] J. Brodsky and J. Radvanovsky, "Control Systems Security," in *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*. IGI Global, 2010, pp. 187–203.

[29] K. Stouffer, J. Falco, and K. Scarfone, *Guide to Industrial Control Systems Security - Final Public Draft, NIST SP800-82*. Gaithersburg, MD: National Institute of Standards and Technology, 2011.

[30] W. T. Shaw, *Cybersecurity for SCADA Systems*. Tulsa, OK: PennWell, 2006.

[31] North American Electric Reliability Corporation (NERC), "2011 Long-Term Reliability Assessment," November 2011. [Online]. Available: http://www.nerc.com/files/2011LTRA_Final.pdf

[32] Office of Electricity Delivery & Energy Reliability, "The Smart Grid: An Introduction," April 2012. [Online]. Available: http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_SG_Book_Single_Pages%281%29.pdf

[33] C. Browner, "Comments on *the christian broadcast network*," October 2009. [Online]. Available: http://www.cbn.com/cbnnews/politics/2009/October/Obama-Pledges-34B-to-Upgrade-Power-Grid/

[34] U.S. Department of Energy, "What is the Smart Grid," April 2012. [Online]. Available: http://www.smartgrid.gov/the_smart_grid#smart_grid

[35] V. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. Hancke, "Smart grid technologies: Communications technologies and standards," *IEEE Transactions on Industrial Informatics*, vol. 7, no. 4, pp. 529–539, November 2011.

[36] 110th U.S. Congress, *Energy Independence and Security Act (EISA) of 2007*. Washington, DC: GPO, 2007.

[37] North American Electric Reliability Corporation (NERC), "Reliability Considerations from Integration of Smart Grid," December 2010. [Online]. Available: http://www.nerc.com/files/SGTF_Report_Final_posted.pdf

[38] Government Accounting Office, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way but Challenges Remain, GAO-07-1036*. Washington, DC: Author, 2007.

[39] P. Kundur, N. Balu, and M. Lauby, *Power System Stability and Control*. New York: McGraw-hill New York, 1994, vol. 4, no. 2.

[40] P. M. Anderson and B. K. LeReverend, "Industry experience with special protection schemes," *IEEE Transactions on Power Systems*, vol. 11, no. 3, pp. 1166–1179, 1996.

[41] J. E. Fadul, "Using Reputation Based Trust to Overcome Malfunctions and Malicious Failures in Electric Power Protection Systems," Ph.D. dissertation, Air Force Institute of Technology, 2011.

[42] S. P. Marsh, "Formalising Trust as a Computational Concept," Ph.D. dissertation, University of Stirling, 1994.

[43] I. Ray, I. Ray, and S. Chakraborty, "An interoperable context sensitive model of trust," *Journal of Intelligent Information Systems*, vol. 32, no. 1, pp. 75–104, 2009.

[44] M. Deutsch, "Cooperation and trust: Some theoretical notes." *Nebraska Symposium on Motivation*, pp. 275–320, 1962.

[45] S. I. Ahamed, M. M. Haque, and N. Talukder, "A formal context specific trust model (ftm) for multimedia and ubiquitous computing environment," *Telecommunication Systems*, vol. 44, pp. 221–240, August 2010.

[46] M. C. Duncan, "Trust Management and Security in Satellite Telecommand," Master's thesis, Air Force Institute of Technology, Dayton, OH, March 2011.

[47] W. Zhao and V. Varadharajan, "An Approach to Unified Trust Management Framework," in *Collaborative Computer Security and Trust Management*. IGI Global, 2009, pp. 111–130.

[48] B. Yu and M. Singh, "A Social Mechanism of Reputation Management in Electronic Communities," *Cooperative Information Agents IV-The Future of Information Agents in Cyberspace*, pp. 355–393, 2000.

[49] A. Salehi-Abari and T. White, "Towards Con-Resistant Trust Models for Distributed Agent Systems," in *21st International Joint Conference on Artificial Intelligence*, 2009, pp. 272–277.

[50] G. M. Coates, K. M. Hopkinson, S. R. Graham, and S. H. Kurkowski, "Collaborative Trust-Based Security Mechanisms for a Regional Utility Intranet," *IEEE Transactions on Power Systems*, vol. 23, pp. 831–844, 2008.

[51] M. Grimes, "Scada exposed," *Proc. ToorCon*, vol. 7, 2005.

[52] D. Proudfoot, "UCA and 61850 for Dummies Siemens Power Transmission and Distribution, 2002," April 2012. [Online]. Available: http://www.nettedautomation.com/download/UCA%20and%2061850%20for%20dummies%20V12.pdf

[53] M. Adamiak, A. Apostolov, M. Begovic, C. Henville, K. Martin, G. Michel, A. Phadke, and J. Thorp, "Wide area protection - technology and infrastructures," *IEEE Transactions on Power Delivery*, vol. 21, no. 2, pp. 601–609, 2006.

[54] C. Bowen III, T. Buennemeyer, and R. Thomas, "Next generation scada security: best practices and client puzzles," in *Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop (IAW)*. West Point, NY: IEEE, 2005, pp. 426–427.

[55] Siemens Energy, July 2011. [Online]. Available: www.energy.siemens.com/us/en/services/power-transmission-distribution/power-technologies-international/software-solutions/pss-e.htm

[56] University of California, Berkley, "The Network Simulator 2 (NS2)," July 2011. [Online]. Available: http://isi.edu/nsnam/ns/

[57] K. Hopkinson, X. Wang, R. Giovanini, J. Thorp, K. Birman, and D. Coury, "Epochs: A Platform for Agent-Based Electric Power and Communication Simulation Built From Commercial Off-the-Shelf Components," *IEEE Transactions on Power Systems*, vol. 21, no. 2, pp. 548–558, May 2006.

[58] J. F. Borowski, "Reputation-Based Trust for a Cooperative, Agent-Based Backup Protection Scheme for Power Networks," Master's thesis, Air Force Institute of Technology, Dayton, OH, March 2010.

[59] P. Cote and M. Lacroix, "Benefits of Special Protection Systems in Competitive Market," in *22nd IEEE Power Engineering Society International Conference on Power Industry Computer Applications*. IEEE, 2001, pp. 192–195.

[60] L. A. Oquendo-Class, K. M. Hopkinson, X. Wang, T. R. Andel, and R. W. Thomas, "A Robust Communication-Based Special Protection System," *IEEE Transactions on Power Systems*, vol. 25, no. 3, pp. 1314–1324, July 2010.

[61] H. Lokay and V. Burtnyk, "Application of underfrequency relays for automatic load shedding," *IEEE Transactions on Power Apparatus and Systems*, no. 3, pp. 776–783, 1968.

[62] "The R Project for Statistical Computing," 2012. [Online]. Available: http://www.r-project.org/

[63] R. I. Kabacoff, *R in Action*. Shelter Island, NY: Manning Publications Co., August 2011.

[64] "NIST/SEMATECH e-Handbook of Statistical Methods," April 2012. [Online]. Available: http://www.itl.nist.gov/div898/handbook/index.htm

[65] S. McCanne, S. Floyd, and K. Fall, "NS2 (Network Simulator 2)," 1989.

[66] D. C. LeBlanc, *Statistics: Concepts and Applications for Science*. Sudbury, MA: Jones and Bartlett Publishing, 2004.

[67] S. Shapiro and M. Wilk, "An Analysis of Variance Test for Normality (Complete Samples)," *Biometrika*, vol. 52, no. 3/4, pp. 591–611, 1965.

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
14-06-2012	Master's Thesis	Aug 2010 – Jun 2012

4. TITLE AND SUBTITLE
An Application of Con-Resistant Trust to Improve the Reliability of Special Protection Systems within the Smart Grid

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Shipman, Crystal, M., Master Sergeant

5d. PROJECT NUMBER
12G292P

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
Wright-Patterson AFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER
AFIT/GCO/ENG/12-22

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Office of Scientific Research, Mathematics, Information and Life Sciences Directorate
Attn : Dr. Robert J. Bonneau
875 N Randolph St, Ste 325, Rm 3112,
Arlington, VA 22203
(703) 696-9545 (DSN: 426-9545)
Email: robert.bonneau@afosr.af.mil

10. SPONSOR/MONITOR'S ACRONYM(S)
AFOSR/NL

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES
This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

14. ABSTRACT
This thesis explores an application of a con-resistant trust mechanism to improve the performance of communications-based special protection systems to further enhance their effectiveness and resiliency. New initiatives in the energy sector are paving the way for the emergent communications-based smart grid technology. Smart grids incorporate modern technologies in an effort to be more reliable and efficient. However, with the benefits of this new technology comes added risk. This research utilizes a con-resistant trust mechanism as a method to quickly identify malicious or malfunctioning protection system nodes in order to mitigate the resulting instabilities in the smart grid. The feasibility and performance of this trust architecture is demonstrated through experiments comparing a simulated special protection system implemented with a con-resistant trust mechanism and without via an analysis of variance statistical model. The simulations yield positive results when implementing the con-resistant trust mechanism within the communications-based special protection system for the smart grid.

15. SUBJECT TERMS
Critical Infrastructure, Power Grid, SCADA, Smart Grid, Special Protection Systems, Reputation-based Trust, Con-resistant Trust

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
REPORT	ABSTRACT	c. THIS PAGE			Kenneth M. Hopkinson, Civ, USAF (ENG)
U	U	U		84	19b. TELEPHONE NUMBER *(Include area code)* (937) 255-3636 x4579 kenneth.hopkinson@afit.edu