REPUTATION-BASED TRUST FOR A COOPERATIVE, AGENT-BASED BACKUP PROTECTION SCHEME FOR POWER NETWORKS

THESIS

John F. Borowski, Major, USAF

AFIT/GCO/ENG/10-04

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government.

AFIT/GCO/ENG/10-04

REPUTATION-BASED TRUST FOR A COOPERATIVE, AGENT-BASED BACKUP PROTECTION SCHEME FOR POWER NETWORKS

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

John F. Borowski, BS

Major, USAF

March 2010

AFIT/GCO/ENG/10-04

REPUTATION-BASED TRUST FOR A COOPERATIVE, AGENT-BASED BACKUP PROTECTION SCHEME FOR POWER NETWORKS

John F. Borowski, BS

Major, USAF

Approved:

Dr. Kenneth M. Hopkinson, (Chairman)	1 Mar 2010 Date
Lt Col Brett J. Borghetti, PhD (Member)	26 Feb 2010 Date
Lt Col Jeffrey W. Humphries, PhD (Member)	22 Feb 2010 Date

AFIT/GCO/ENG/10-04

Abstract

This thesis research explores integrating a reputation-based trust mechanism with an agent-based backup protection system to improve the performance of traditional backup relay methods that are currently in use in power transmission systems. Integrating agent technology into relay protection schemes has been previously proposed to clear faults more rapidly and to add precision by enabling the use of adaptive protection methods. A distributed, cooperative trust system such as that used in peer-to-peer file sharing networks has the potential to add an additional layer of defense in a protection system designed to operate with greater autonomy. This trust component enables agents in the system to make assessments using additional, behavioral-based analysis of cooperating protection agents. Simulation results illustrate the improved decision-making capability achieved by incorporating this cooperative trust method when experiencing abnormal or malicious communications. The integration of this additional trust component provides an added push for implementing the proposed agent-based protection schemes to help mitigate the impact from wide-area disturbances and the cascading blackouts that often follow. As the push for electric grid modernization continues, an agent-based trust system including this type of behavioral-based analysis will also benefit other smart components connecting critical grid control and monitoring information systems.

Acknowledgments

I first would first like to thank my wife and children for their unending support and encouragement. Their love and understanding was essential in pursuit of this endeavor. I also express my sincere appreciation to my faculty advisor, Dr. Kenneth M. Hopkinson, for his guidance and direction throughout the course of this thesis effort. The insight and experience was certainly appreciated. Finally, I thank my research committee members, Lt Col Brett J. Borghetti and Lt Col Jeffrey W. Humphries for their expertise and generous assistance.

John F. Borowski

.

Table of Contents

Page

List of Figures

Page

List of Tables

Page

REPUTATION-BASED TRUST FOR A COOPERATIVE, AGENT-BASED BACKUP PROTECTION SCHEME FOR POWER NETWORKS

I. Introduction

RESEARCH into the improvement of protective relays used for the protection of electrical power transmission and distribution systems has further increased following findings released after the investigations into the August 2003 blackout affecting the Northeastern United States and Canada. The instability resulting from cascading outages was identified as a primary cause of the uncontrolled blackout spreading across a wide geographic area [59]. This research has been ongoing since the mid-1980's when the North American Electric Reliability Corporation (NERC) sponsored a study indicating that protective relays were involved in 75 percent of major power system interruptions [48]. The importance of proper protection settings is amplified during times of system disturbance.

1.1 Background

Many problems involving relay failures are not exposed until external fault conditions occur or the system is operating at or near its limits. As part of the Energy Independence and Security Act of 2007, grid modernization was directed to ensure that electricity could be reliably and securely provided to meet future growth requirements [1]. While grid interconnections have become a standard method of ensuring redundant paths between power sources and load destinations in a grid, these modernization efforts are looking at better integration of communications networks to provide increased control

opportunities. As a result, the electric grid is becoming more unified which may intensify cascading problems that result when a relay causes a trip at an undesired time.

Improved network capabilities have enabled grid modernization efforts. Utility companies are able to gather more information, quicker than ever before. Utilizing more readily available commercial off the shelf (COTS) products has changed the industry from revolving around proprietary technology to integrating more open communications standards [55]. Increased information has helped improve the situational awareness of supervisory control and data acquisition (SCADA) system operators and enabled industry to base business decisions around real-time data. However, this integration has also opened the system to remotely executed computer-based network attacks.

Power and other utility networks are increasingly the subject of attack [19], [20], [22], and [56]. Threats to the power grid and other elements of critical infrastructure are likely to occur at times of war preparation such as during the mobilization and deployment phases [44] to cause delays and backlogs at key logistics locations [16] and [31]. Other research [63] focused specifically on attack strategies designed to amplify the cascading effects of grid failures. Improving the reliability and security of the grid protection elements and the underlying communications networks will have a direct impact on the ability of the US armed forces to continue to deploy and rapidly project force where needed anywhere around the globe.

1.2 Overview and Goals

Transmission line protection systems are particularly vulnerable to these types of cyber attacks. The physical and network protection in place is insufficient given their

capability to control switch gear and the flow of electricity [55]. As modernization increases there has been a larger focus on improving the security of control networks. This thesis introduces a reputation-based trust mechanism to help supplement more traditional network protection mechanisms and will augment the layered security approaches as recommended in [14]. The research goal will also enable system operators to gather more insight into the behavior of essential control components using both operational and nonoperational data.

Public standards such as IEC 61850 and the transition to internet technology have increased interoperability but also made the power networks more vulnerable to attack. A peer-to-peer (P2P) based trust scheme will enhance the effectiveness of the other network protection mechanisms such as intrusion detection systems and firewalls. This thesis shows that cooperative information sharing produces improved decision-making capability through coordinated fault verification to reduce grid area isolation and enables more responsive breaker reactions to system faults when compared to traditional fault clearing mechanisms. As this type of trust system is refined, it can be of extreme importance, adding reliability and security to a utility network, especially if integrated into a segregated Utility Intranet [14].

1.3 Organization

The following chapters discuss agent-based technology and its applications in transmission network protection as well as cooperative trust arrangements in peer-to-peer systems. Chapter II covers established research in the areas of the power grid, traditional and proposed protection mechanisms, cooperative trust systems, and potential threats to

grid security. Chapter III details the methodology used for assessing the ability of an agent-based cooperative trust protection mechanism. This mechanism must recognize behavior that might cause incorrect or unreliable decision making and react appropriately, producing correct results more rapidly than traditional backup protection mechanisms. Chapter IV gives an analysis of why important features were included in the trust scheme and provides the experimental results from simulated scenarios. Finally, Chapter V summarizes this thesis work and its contributions and suggests future research opportunities in this area.

II. Literature Review

The power grid is just one element of a nation's critical infrastructure, however many of the other elements essential to support society depend upon a reliable flow of power to function. A relatively new invention in the history of humanity, people have quickly come to rely on the electrical energy produced and transported by the power grid on a daily basis. This lucrative and indispensable industry has recently become a more commonly suggested target for both physical and cyber attack due to society's dependence on it. Attacks on the system are likely to be the work of professionals, accomplished by organized crime and state-sponsored terrorist or military groups [18].

Environmental problems also afflict this complex system and previous research efforts typically focused on improving system stability, security, and reliability with respect to these types of issues. Power system companies are integrating more networked communications into their corporate and control systems because it provides them with additional information to make better business and system control decisions and has become economical to do so. As the strain on existing grid systems continues to increase and more attention is given to network based attacks on the system, some research efforts have shifted to the cyber security needs of power systems typically revolving around identity credentials and policy-based trust as discussed in [5].

Real-time information requirements have presented some difficulties in fully utilizing the security benefits that these trust systems offer, warranting further study into other layered protection mechanisms. Additionally, modernization will increase network reliance, necessitating this investigation into using reputation-based trust to improve

system coordination. This chapter on related literature is broken into four main parts. The first describes the electrical grid and gives some insight into why interest in its security is increasing. The second part describes current grid protections mechanisms and research efforts to transition to a more decentralized networked protection environment. The third section reviews the use of trust as a measure of communications reliability and how collaborative trust has been applied in existing peer-to-peer networks. The final section covers the increased need for cyber security in SCADA systems.

2.1 Background on the Power Grid

Electric power has been generated commercially since the late 1800's and has constantly been under a state of expansion and interconnection. The three primary reasons for this expansion as stated in [40] include benefits from economies of scale, improved load factor and increased generation reserves. Together, these three factors have helped make electricity more affordable and reliable for a greater number of people. A basic understanding of electricity, the main components in a power grid and a history of system vulnerabilities is essential to understanding the current requirement for modernization.

2.1.1 Electricity, the Fundamentals

There are four basic descriptors used when discussing electricity in power systems [40]. The first term is voltage. Voltage (V) refers to the difference in electric potential and can be expressed as one Joule of energy that is needed to move one Coulomb of electrical charge. Differences in electric potential cause charge to flow

through a line. The second descriptor current (I) describes the rate of this flow and is measured in amperes in which one ampere is one Coulomb per second. These two terms are often referred to together when using Ohm's Law given as

$$V = IR \tag{2.1}$$

where V is the voltage, I is the current, and R is the resistance (the third term). Resistance is determined by the characteristics of the material through which the current flows and is measured in ohms. Increasing resistance in series (longer transmission lines) increases the overall resistance where as increasing in parallel (increased aggregate load) decreases the overall resistance [40]. Thus there is a linear relationship between voltage and current that depends upon the resistance. For a given voltage, if the resistance decreases the current should increase. This is particularly evident in ground shorts where an excessive current typically engages protection mechanisms to isolate the fault and prevent circuit damage.

The potential for transmission line damage can be explained by resistive heating as discussed in [40]. Heat is measured in energy per unit time as is referred to as power (P), our fourth term. Power is most often generally referred to by the equation

$$P = IV \tag{2.2}$$

which describes power as current multiplied by voltage and results in a measure of watts or Joules per second. Using Ohm's Law, this equation 2.2 may also be rewritten as

$$P = I^2R \tag{2.3}$$

to more clearly show the relationship between current, resistance, and power.

This relationship is significant when discussing changes that occur in different parts of the systems. As a rule, current and resistance cannot be adjusted independently [40]. This relationship can come into play in two distinct types of scenarios. First, in some circumstances such as in home usage, voltage is held constant. Decreasing circuit resistance causes current to increase and since the current term is squared, current has more of an impact on the power than the resistance. In the second scenario more applicable to transmission and distribution line design, current is held constant with respect to the power lines and is dependent upon the aggregate end loads. Since power losses from resistive heating are not desired, line resistance should ideally be minimized. The selection of a conductor for use as a line material is important since tradeoffs exist between performance and cost. This selection must account for topography as well. As the power supply is increased during times of peak demand, current across the line increases, resulting in additional line heating. This resistive heating can result in line sag that is associated with a primary cause of short circuits and their resultant power outages.

The four terms previously discussed do not encompass all power system descriptors require for system protection. There are additional characteristics associated with alternating current (AC) that need explanation. AC was selected for use in power systems due to the ease of using transformers to raise and lower voltages, optimizing energy conservation. Higher voltages prevented transmission losses, but lower voltages were needed for safer end-use applications. AC is traditionally depicted as a sine wave. The current reverses direction twice each cycle at a frequency that has been standardized at 60 cycles per second in the US.

The two most significant characteristics associated with AC systems are reactance (X) and impedance (Z). Reactance is associated with the ability to oppose the current flow and is either classified as inductive if it resists changes in current or capacitive if it resists changes in voltage. If there is any reactance, there will be a phase shift between the voltage and the current sine waves. This reactance measure is combined with resistance to create a measure called impedance. Impedance deals with the aggregated resistance or desire to flow and may be represented in complex number notation. These two terms are used by protection mechanisms to determine fault conditions and location.

2.1.2 Main Power Grid Components

When analyzing the state of a power grid and its ability to balance power requirements, researchers typically divide the grid into segments based on function. The electric power grid is comprised of four major components (as seen in Figure 1) that work in harmony to deliver a consistent supply of power exactly when and where it is needed. The first part of the power grid is the generation capability. The source of power used in generation can come from many different resources, typically

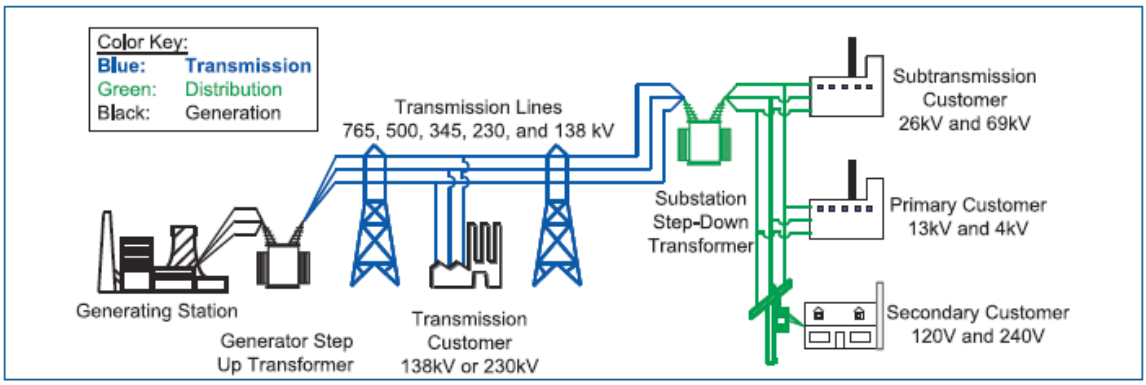

Figure 1. Basic depiction of typical electric grid components as described in [59]

acknowledged as coal, oil, or nuclear but now includes more green options such as wind and solar energy. Regardless of the actual physical source, generation is involved with transforming that resource into electrical power. Once in this form, it is able to be transformed (typically to a higher voltage) and transported to other regions.

Now that the electrical voltage has been generated, it flows to other locations in the grid on the transmission system. The transmission system is characterized by high-voltage transmission lines generally recognized by tall steel towers. It is used for transporting electricity over long distances using higher voltages to reduce line heating and resistive power losses as discussed in the previous section.

Transmission systems connect geographically separated regions that may not have their own generation capability or need additional generation capabilities. The US power grid is broken into three regions (as seen in Figure 2), each with its own generating and

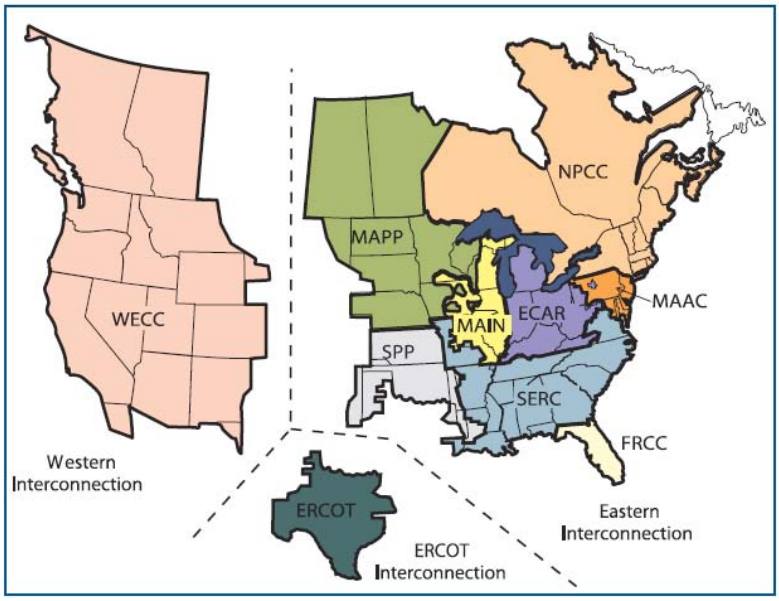

Figure 2. Three interconnections of North American power grid as described in [58]

transmission capabilities. There are limited DC connections between these regions, but they are typically thought of as isolated grids among themselves. As explained by NERC in [45], together the generation and transmission components comprise the bulk power system. Bulk power is suitable for general purpose electrical operations, but additional conditioning is more likely needed for sensitive operations.

The transmission systems in each grid are then linked to distribution systems at power substations. The voltage is gradually stepped down to lower voltages that are generally considered safer and are more suitable for final customer use before being distributed to end users. These distribution systems generally cover a smaller geographical region and may have been isolated from other regions at one time. Distribution systems cover the final portion of the journey from generation source to load destination.

The final component in the electrical grid is the load or power demand. Individual loads are important for customers and billing components of power supply companies, however for planning purposes these individual loads are aggregated in terms of quantity and timing. Individual loads are very dynamic, changing in both predictable and unpredictable cycles. Planners are able to use these historical cycles along with current environmental and social data to try to balance generation to meet the required loads across the system (both typical and unexpected). As loads increase, there is an increased likelihood of system overload if generating stations do not keep up with the growing demand. The electricity generated for the power grid must be used almost immediately after it is produced. It cannot be stored or routed as easily as other utilities

such as water, sewage or gas. Electricity must be carefully monitored and controlled ensuring that the power generated meets the required loads.

2.1.3 Monitoring and Control Systems

Information systems that provide monitoring and control functions are the lifeline of the power industry. They allow for responses necessary to provide the reliability and stability required to create an uninterrupted flow of power. The power industry has made progress on modernizing its monitoring and control systems to improve performance and awareness of system status. This progress has usually been done for the utility companies' self interest. Companies are able to capitalize on the interconnections between regions, trading power production capabilities to balance the overall system in the most cost-effective manner. They are able to get feedback from the components in the system enabling more rapid reactions to periods of increased demand.

Monitoring and control functions are provided by SCADA system components inserted throughout the grid. SCADA systems generally provide centralized control and monitoring for a wide geographic region. Devices read system data, automatically react to adverse conditions using protection devices and then typically report back to a system operator monitoring the overall system. This operator can also make inputs to the system by adjusting or overriding automatic controls based on more complete situational knowledge. These computer systems aggregate data to help build a complete picture of the system and improve situational awareness for operations personnel.

The influential ability created by advanced control systems and recent integration of open communications systems such as the internet has made SCADA systems an

attractive target for cyber attacks [47]. The US government has focused attention on securing the components of its critical infrastructure against cyber and physical attacks in a series of publications between 1998 and 2010 that included presidential directives such as [9], [10], and [13] as well as planning documents [1] and [12].

2.2 Protecting the Electrical Grid

Improving the reliability of electrical flow has often focused on improving the performance and security of power grid protection components. One branch of research has focused on the improving communications networks and cyber-security. Connection points between the utility networks and the rest of the internet can be secured using traditional mechanisms such as firewalls, intrusion detection devices and cryptographic protocols [25]. This type of research has received a lot of attention as the government revealed evidence of foreign attempts at network mapping [19] and as cybercrime organizations threaten to breach network security from around the globe [62].

An alternate focus on grid protection has revolved around increasing system stability by improving fault clearing methods. Fault clearing time is defined in [3] as the time necessary to identify a fault condition, make a decision about whether or not to take an action, and take the action to help isolate a section of the grid. While there are many components that help provide this function, fault clearing is primarily dependent upon circuit breakers that physically open or close a circuit and the protective relays that help determine when a circuit breaker should operate and direct that operation [40]. This branch of research primarily looks at improving the interactions of physical devices such as circuit breakers and relays and the capability to provide human operators with

additional system knowledge or improved interfaces to make better decisions. Research done in conjunction with this thesis has been accomplished with respect to this second focus on protection.

2.2.1 Circuit Breakers

Circuit breakers open and close a circuit based on input from another device and rely on a form of energy to open and/or close. When the breaker is closed, current is able to flow through the circuit. When the breaker is opened, the flow of current is interrupted until the breaker is reclosed. Breakers can be designed for different functions taking advantage of various mediums and their associated characteristics to terminate the electric flow. The commands to open or close the breaker can be directed by a system operator in response to stability needs or may be generated by an automated monitoring device known as a protective relay in response to a fault condition.

2.2.2 Transmission-Line Relay Protection

A relay is the device that detects abnormal power conditions and signals a circuit breaker to interrupt the current [24]. There are a variety of relay types used in the power grid, each with a purpose specific to the protection needed. Transmission lines are typically provided redundant protection and protection is needed from phase faults (faults between transmission lines) and ground faults (faults between a transmission line and a point of zero potential such as the ground or a tree) [40]. The distance relay and the differential relay as described in [24] and [53] provide the bulk of the protection from these types of faults for the transmission system.

Distance protection relays use impedance measurements (as discussed in Section 2.1.1) to determine if a fault is located within their protection zone. The impedance of a transmission line is generally well known [24] and tested to verify reliable and expected performance. Impedance is dependent upon the line material and construction. Impedance should stay consistent along the length of the line as long as the line type is the same allowing the location of the fault to be determined with a relatively high degree of accuracy. If the impedance measurement falls into the fault zone that was established by system designers based on grid components and architecture, the relay will trigger the appropriate circuit breakers to open. The research in this thesis focuses on this common type of transmission line protection.

A second type of protection mechanism is often integrated into a protection scheme to detect other types of faults. Differential protection is increasingly being used with relay communications methods such as pilot wire relaying to measure the difference in current at both ends of a transmission line. Relays at each end of the line send and receive measurements from the opposite end of the line they are protecting. Since the difference between measurements should be zero, the appropriate circuit breakers are tripped if the magnitude of difference is above a set value.

2.2.3 Fault Clearing Using Circuit Breakers and Protective Relays

Power circuit breakers and protective relays work in conjunction to provide autonomous monitoring and control functions necessary to clear fault conditions in power systems by interrupting the flow of power to a portion of the circuit [40]. Efforts to improve the operation of these devices have been ongoing since the 1950's when

Kimbark described conditions required to rapidly clear faults from the power system [30]. More rapid fault clearing has a stabilizing effect by reducing the loss of synchronization and limiting the associated transient fluctuations.

While faster fault clearing is essential, it is only one component of improving the system reliability. Proper analysis of fault location and system conditions are just as vital. This analysis enables the protective devices to clear the fault in a way that minimizes the effects caused when isolating a portion of the grid. Relays must be sensitive and intelligent enough to select only the circuit breakers that need to open to clear the fault. If too many circuit breakers are open (or if the area they cover encompasses too large a region) more loads will be disconnected from the generation devices. It is typically better to take additional time to perform more complete analysis and open only the appropriate breakers than it is to open selected breakers as rapidly as possible.

In order to gather the appropriate information necessary for this analysis, different types of protective relays have been installed in the electrical grid. These different types help increase the selectivity of a relay. Relay implementations as discussed in [36] have been integrated into different regions of the power grid accounting for what they are protecting and the type of protection that is required. Generators require different safeguard mechanisms and settings than transmission lines do. Backup systems require different settings than primary systems. As the grid has been interconnected, improper settings have had a bigger impact and amplified the results of improper protection settings [59].

2.2.4 Interest in Relay Improvement from 2003 US Blackout

The impact that improper relay settings can have on a system were brought to light from the findings following the August 2003 blackout affecting regions of the northeastern United States and portions of Canada [59]. Mismanaged relay settings were directly related to the cascading effects that caused the blackout to cover such a wide region. The relays did not fail but operated as designed and intended according to their improper implementations. Had system operators been able to mitigate one of the primary causes of the disturbance through better situational awareness, it is likely the cascade would not have occurred. Better relay coordination may be able to prevent cascading effects in the future.

After several lines isolated regions of the grid due to ground faults from contact with overgrown trees, the relay responsible for the cascade reacted to an overload situation as opposed to an actual ground fault [59]. The generation losses from the isolation coupled with the operator's failure to reduce the overall load caused the relay's power information readings to fall in the impedance zone. The relay read the conditions as if it was experiencing a three-phase fault instead of an overload and its backup protection tripped the appropriate circuit breaker as it was designed to according to its settings.

The findings released in that study recommended reviewing relay settings. Many relays had been improperly configured or manufacturer preset configurations had not been adjusted for the current implementation and topography. In particular, the committee acknowledged backup relays should normally be configured to check for

phase problems or fault conditions as opposed to overloads. Overloads can often be short-term problems that occur as a system adjusts to fluctuations. By triggering an improper circuit breaker trip in a situation such as this, these relays may spread the outage that they were attempting to contain.

Additional interest in relay improvement was generated by two cascading blackouts that occurred in the European Union [60] and [61]. The 2003 blackout in Italy and the 2006 blackout originating in Germany both resulted in part from N-1 criteria not being met and from a lack of coordination with neighboring regions after multiple line trips caused power imbalances between the now isolated regions [60] and [61]. The N-1 security rule as defined in [60] refers to the ability of a system to continue operations even if a single incident such as loss of a generation facility or transmission line occurs. It is aimed at preventing cascading effects. Ultimately in both situations, those conditions were not met. Findings indicated that better unified protection was needed for these increasingly interdependent systems and that relays operated incorrectly 15% of the time in the Italian blackout [60]. Increased relay research can help improve the coordination of protection efforts and improve system stability.

2.2.5 Existing Relay Implementations in Backup Protection

Currently, backup protection systems have been integrated into relay protection schemes to provide redundancy should the primary protection fail to operate. Primary (zone 1) protection typically protects the first 85% of the line connected to a relay while backup (zone 3) systems cover a larger area [53]. Zone 2 protection can also be used to cover an area that encompasses the entire first line and a portion of the adjacent line [24].

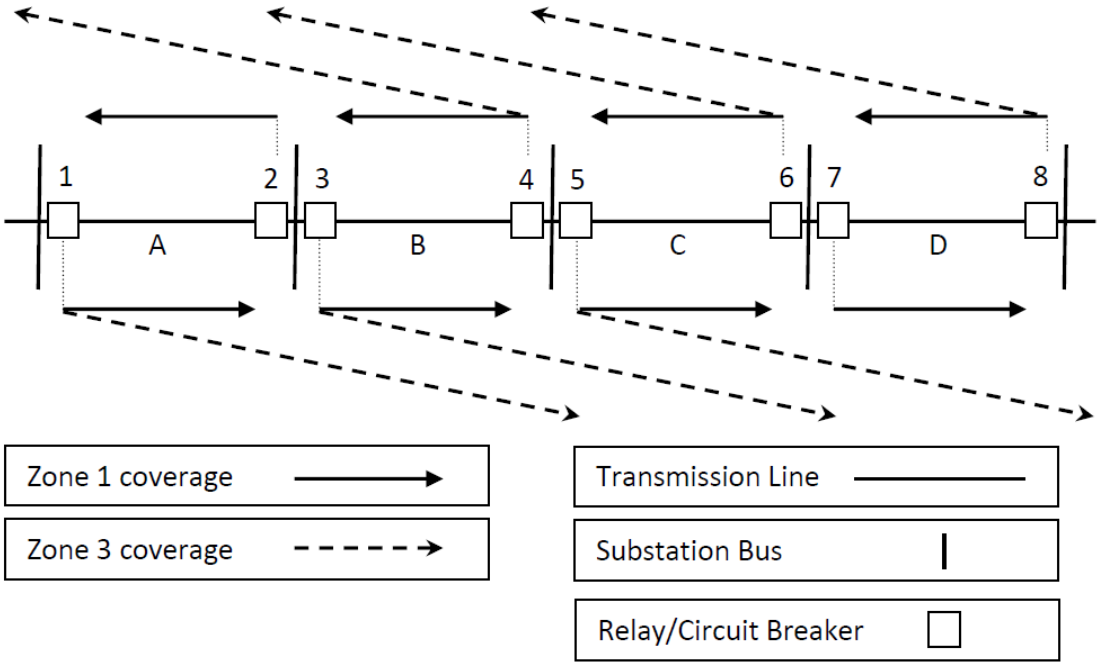

Figure 3. Transmission Line Relay Protection Zones. Primary protection is provided by zone 1 coverage which protects approximately 85% of primary line while zone 3 coverage covers the primary line, and extends past 100% of adjacent line to provide backup protection for that line. For example Relay 3 provides zone 1 coverage for line B and zone 3 coverage for line C. Relay 4 would also provide zone 1 coverage for line B but zone 3 coverage for line A instead since it is directional. Relay 1 and relay 6 would provide zone 3 coverage for line B. A zone 2 protection scheme (not shown) would extend past the zone 1 coverage, but would be less than zone 3 coverage area. [53]

Zone 3 systems provide multi-line protection, including the line that a relay is directly connected to as well as lines protected by adjacent neighbors [53]. As described in [59], some operators have stopped using zone 3 relays on high-voltage lines and reset zone 2 relays to serve the purpose of a zone 3 relay. For this research, zone 1 and zone 3 protection regions were included as part of the protection scheme while the zone 2 region was not based on the coverage area. These protection zones can be seen in Figure 3.

When a fault occurs, the fault location and actions taken by other relays will determine if a relay needs to take action. Using direct communications between relays to coordinate circuit breaker opening at both ends of a transmission line as in pilot schemes [7], designers are able to create a more effective protection scheme.

This electrical fault protection has increased in importance as current systems are stressed to their limits [58]. Transmission line protection mechanisms are of crucial importance to the protection of the entire grid. Designers must give proper consideration to relay settings when creating primary and backup protection schemes. Both the line length and its relative importance in connecting geographically dispersed generating locations with destination loads determine the characteristics required for planning proper operation of the protection systems. Benefits of using schemes with increased relay coordination such as pilot schemes must be weighed against the decreasing costs of these more resource intensive systems.

2.2.6 Proposed Agent-based Backup Protection for Transmission Lines

As costs for more advanced communications networks continues to decline, researchers have proposed replacing traditional protective relays with relay Intelligent Electronic Devices (IED) [64] that provide increased protective capabilities. In this research, an agent was defined to be a software component able to interact and act autonomously based on the results of its interactions. The IED's that were created would be able to read power system information and react to that information. They would also share information with neighboring nodes to include passing along any protective actions that they have taken.

This agent-based approach would fit into the current monitoring and control scheme and could pass information to a master control center as well. It would allow agents to use remotely acquired information to make more correct decisions locally. Preliminary research as shown in [64] has demonstrated that this agent-based protection scheme has the ability to clear electrical ground fault conditions more rapidly, while still allowing the system to analyze the complete set of information required when making protection decisions. The agents work together cooperatively as described in [14] to provide protection according to a preauthorized set of rules.

2.2.7 Current Wide Area Agent Implementations in the Power System

The additional computing power provided by integrating intelligent agents in a system such as this is of additional benefit in a SCADA scheme when compared to traditional relay implementations. Agent-based relay research has also been initiated for adaptive relay schemes. These schemes provide protection that changes with the external environment based on feedback from other parts of the system.

New power systems in China have already been incorporating agents to provide features such as this as described in [11] and [70]. These agent implementations enable communications between relays and central servers. The agents assist in fault protection using additional data gathered through collaboration. This increased information requirement entails more inter-device communications, necessitating additional methods to secure the information exchanges. This security is likely to come through network protection mechanisms such as cryptography and firewalls as well as other tools described in [6].

2.3 Increased Need For Cyber Security and Better Information Sharing

2.3.1 SCADA Modernization Efforts and Security Impacts

Since the mid 1990's, the evolution and modernization of electrical grid control mechanisms have attracted attention in the cyber security community. Computer-based control systems were introduced to provide more advanced computational power and better data processing. Digital technologies resulted in improved information handling and provided operators with automated, coordinated options to aid their decision-making abilities. Systems typically revolved around a centralized computer located in a control center that would communicate with remote system components over a wide area network. The resulting systems are much more capable and interoperable, but have also made the systems more vulnerable to exploitation from malware, hackers, and cyber attack [55].

Modernization is necessary for improved grid stability and information sharing. The increased situational awareness enables operators to create flexible response options to prevent outages and minimize disruptions. The additional protection requirements when integrating interoperable components are likely to increase security and reliability of the system as a whole. The previous practice of security by obscurity goes against Kerchkhoff's principle that states that the system design should not require secrecy to function securely [29]. Believing proprietary technology is a security measure works only until the specifications are discovered. Once discovered, the system becomes more vulnerable and can be exploited more easily, often without notice.

2.3.2 Communication Needs for Grid Modernization

Security needs continue to increase as the interdependence of the electric grid and communications systems grows more complex. New information transactions are occurring to provide operators, customers and providers with the information they require to make effective, timely decisions. The current infrastructure is mostly based off internet protocol (IP) technology to provide the required real-time information transfers. IP-based technologies such as transmission control protocol (TCP) and user datagram protocol (UDP) are used to for information exchanges and have enabled the use of extensible markup language (XML) tagging to help with data format issues [54].

As discussed in [57], IP provides basic address identification information to help route information transfers from one point in a network to another. It helps identify components and lets them talk to each other. TCP is a connection-oriented protocol designed for reliable communication between two nodes in a network. It guarantees that all the data will be received in the correct order. UDP on the other hand is connectionless and does not provide for error correction or guaranteed delivery. It does however provide for more rapid data delivery as a connection does not need to be established. It also has a lower overhead since less information needs to be transferred in each given message. These conditions make UDP the fastest and least complicated way to transmit data resulting in its use for most real-time applications. XML standardizes the data format and creates tags that help applications identify and exchange information in an interoperable manner [54]. It has helped synchronize database information and enabled data sharing for new and innovative purposes.

2.3.3 The Smart Grid Transition and New Threats

These improvements in network and tagging abilities have helped shape the path towards incorporating technology to improve grid reliability and optimize energy generation and distribution. The most significant challenge in moving towards this goal is protecting the information that will be required to improve grid awareness and make optimizing decisions. Interconnections will be incorporated in new devices that make power control decisions based on preference information that may be pulled from financial databases. Security measures will need to be implemented cooperatively to protect the system as a whole from cyber and physical threats.

Attacks against electric utilities are becoming more attractive due to the effects that can be created. Customer databases are large and contain financial and personal information. These systems receive more cyber security attention than control equipment because they are more closely related to corporate networks. However, as researchers look towards the transition, the security focus is becoming more encompassing. In [55], Shaw writes that directly controlling switch equipment and transformers is the biggest threat to grid stability. Protective relays are positioned at locations where they have the potential to interrupt failures from spreading and cascading. More advanced relays have more complex communications needs and thus require a different level of protection than they originally did.

If access to relays is granted, hackers would be able to directly control breaker actions and protection settings. As the age of the Smart Grid approaches where information is widely shared, it is likely that relays at remote locations will link to the

control and corporate networks to allow remote status checking and setting adjustment. Additional layers of security such as trust measurements from behavior observation can be used for distributed, autonomous protective actions that should help mitigate some of the effects if an intrusion were to occur and traditional protective schemes fail.

2.4 Reputation-Based Trust and Agents in Distributed Systems

Researchers have acknowledged a need to secure networked SCADA communications in [14]. The inclusion of agents in these control systems using an autonomous information exchange implementation creates a P2P network among the intelligent agents. Agents can learn who to interact with either at initialization or through topology discovery methods during routine operations. Agents can interact through communication to determine the reliability of other agents.

2.4.1 Using Trust to Measure Reliability of Distributed Communications

The reliability of other agents could be tracked using a trust system. Trust as a concept has been formalized by Dr. Stephen Marsh in [35] where he described it as a degree of confidence in information obtained from a known or unknown source when the outcome of a decision using that information is uncertain. Trust is also a central concern in many multi-agent distributed systems where agents base decisions on information obtained from other agents. This information can be obtained directly, indirectly, or with some combination of methods as discussed in [51].

When implementing a trust system, to aid in decision making agents need to put a value on information obtained from others using a trust metric, where a trust metric is

defined as system measurements used to quantify the reliability of other agents. This value can come in the form of user satisfaction scores common in e-commerce situations and in P2P systems. Typically, P2P systems are thought of as file-sharing systems such as Gnutella, Kazaa, and BitTorrent or communications systems such as Skype. A typical problem in these P2P networks is that there is a lack of accountability due to the anonymous nature of the network and the potential for misuse is increased based on that anonymity. Ensuring appropriate peer behavior using trust management systems has been discussed in papers such as [5], [33], [42], [51], and [65].

Trust as described in these systems generally is based off of policy, reputation or a combination of these descriptors. Trust can be established at the individual or system level. It can be subjective and is subject to change, making an extensive record of historical actions not necessarily representative of future performance. The time period that must be tracked is dependent upon the system, the type of protection, and tolerance that is acceptable. Policy-based trust is implemented in networks using credentials such as passwords or keys and often provides access control functions as described in [5]. Combining policy-based trust with reputation-based trust is becoming more common as suggested in [33] and [39].

2.4.2 Reputation-Based Collaborative Trust Systems

In reputation-based trust systems, there are a variety of methods for computing and storing trust. Trust is usually based off of a trust value that is dependent upon a history of interactions that are rated on a scale of success. Trust can either be calculated by directly tracking interactions or expanded to create a more system-wide view by

accepting the values created by another node. While typically used in implementations for online file-sharing or e-business rating systems, these reputation-based schemes can play a part in helping improve the overall security when implementing agent-based protective measures in the power grid. The intelligent agent computing power could be harnessed for distributed trust calculations.

Decentralized trust computations take the burden off a centralized server and take advantage of resources that exist in the system. Agents have immediate access to knowledge and can share information when required, minimizing the distance that data requests have to travel over the network. Theses local trust values can be aggregated where necessary to improve a single agent's overall view of the network.

One such system, described in [28] is called EigenTrust. This system focuses on using both direct and indirect experiences to calculate a trust value using a concept known as transitive trust. Peers rate other peers with whom they have had a direct interaction. To expand their view, these trust values are exchanged with other peers in order to aggregate ratings and reevaluate peers or provide a peer with a trust value indirectly. It continues spreading information this way to spread trust values globally throughout the system.

A second collaborative reputation-based trust system, Project NICE, was developed at the University of Maryland for decentralized applications using shared resources. Lee, Sherwood and Bhattacharjee worked on establishing a distributed scheme for trust inference in P2P networks at UMD that efficiently stored user reputation information in a distributed manner [32]. Their work focused on a decentralized trust

inference scheme that could be used to infer trust across an arbitrary number of levels while requiring a limited amount of storage at each node. Agents created local trust values using the algorithm they deemed appropriate.

2.4.3 Explanation of the Trust System Used in this Research

The trust system implementation used in this research was inspired by the work done for Project NICE. As described by Lee in [32], the NICE platform was used for cooperative distributed applications. In the original implementation, applications using this protocol bartered resource certificates to gain access to remote services.

The idea behind this certificate exchange was that agents could redeem issued certificates at a later time to receive resources or storage as a payment scheme. The NICE protocol used network communications to share information and exchange certificates required for trust decisions. There are three main steps in a typical implementation. First, an agent advertises the resources it has to offer and its location. Second, an agent needing resources arranges bartering and trading of resource certificates. Finally, a distributed trust valuation is accomplished based on the results of the transaction, creating a value for the interacting nodes.

Depending on the computing resources available and implementation desired, trust values can be stored either locally or remotely (or a combination of methods can be used). As discussed in [32] each method has its own advantages and disadvantages. Remote storage of trust values typically requires a public key system to digitally sign trust and identity information using a hash algorithm creating a trust cookie in the process. In contrast, local storage methods reduce the communications requirements and

can reduce some of the time needed for the verification associated with the sending and retrieval of trust values.

These methods of distributed reputation-based trust management can be successfully applied in an agent-based power system protection scheme. When integrated with other forms of traditional network protection, they are an essential component helping add security and reliability to the data exchanges. This additional layer of trust verification can help operators identify behavior-based anomalies rapidly for time-sensitive critical infrastructure protection.

III. Methodology

THIS chapter presents an original methodology for integrating reputation-based cooperative trust as an additional layer of security for backup protection systems. The new agent scheme integrates behavioral-based analysis with an agent-based protection scheme. Independent, distributed intelligent agents can use the reputation information from this analysis to improve decision-making and responses. The data obtained while observing the behavior of cooperating agents can also be used to make a judgment regarding the reliability of any information obtained from the observed agent.

There are three main goals for this chapter. First, this chapter will describe the approach taken to integrate the peer-to-peer cooperative trust scheme that was adapted for use in this agent-based protection environment. Second, it explains the simulation setup and the methodology that was selected to obtain significant and meaningful results by describing the integrated model and tools upon which this research was based. Third, it reviews the original malicious simulation scenarios that a particular implementation of the cooperative trust scheme could encounter and explains the experimental parameters used in this agent-based backup protection system.

3.1 Research Objectives

As described in Chapter II, it is essential that protection systems implement relay settings appropriate for the situation and operating conditions. Research has shown that intelligent agents embedded into protective components such as relays have the ability to add system stability [64]. This stability is gained as agents acquire remote information ad assemble it into a more complete situational picture to make an increased number of

correct decisions more rapidly than traditional methods allow, especially when exposed to a more open communications network.

The transition to a more interconnected Smart Grid requires additional information sharing to help improve system operator situational awareness. Agents have the ability to analyze information and behavior improving this awareness. The information can be exchanged between central systems and protection agents to enable operators to remotely review system status and settings and make complementary adjustments that support those made automatically by the agents. This improved system awareness will prevent situational lapses that often result in cascading outages.

Grid transformation requires a renewed focus on cyber security due to the increased reliance on the communications infrastructure. Modernization necessitates evaluating component vulnerabilities. Solutions to protect against exploitation need to increase security while maintaining interoperability and real-time data exchange. Traditional network security measures need to be modified to meet time restrictions and typically introduce unacceptable delays into the system. The proposed agent-based protection scheme integrates a reputation-based trust system that provides behavioral-based analysis with limited overhead.

A reputation-based trust system was integrated with an intelligent agent designed to be compatible with work accomplished in [64] enabling the new agent to perform additional analysis of other agent behavior. The new agent's success was determined by performance comparison with the original agent scheme and with traditional protection mechanisms during times of malicious communications to validate the hypothesis that the

reputation-based trust component could clear faults no slower than traditional protection mechanisms and produce a higher percentage of correct behaviors than the agent-based scheme originally proposed in [64].

Performance of the new trust agent was measured through simulation by comparing the time needed to clear an electrical fault condition using the backup protection provided by the new agent incorporating the trust scheme with the time associated with traditional zone 3 distance relay settings that are traditionally on the order of one second [24]. To account for the effects of malicious behavior, the correctness of the agent actions were also annotated and compared with the actions taken by the original agent created in [64]. The definition for correct behavior was adapted from performance classifications given in [7]. A correct decision was defined by an agent disregarding fraudulent messages and not extending the isolated portion of the grid beyond what was required to clear the fault.

3.2 Collaborative, Reputation-Based Trust Approach

3.2.1 Trust Implementation for Protection Agent

For this project, a simplified implementation of the NICE algorithm was implemented based around stand-alone simulator code provided by Lee [32] for an extended paper at http://www.cs.umd.edu/projects/nice/. The modified implementation maintained most of the capabilities that were proposed by the original research, but minimized the traffic that needed to be exchanged between nodes by using local trust storage. Due to the unique and predictable message traffic that would be sent throughout

the agent protection system, many of the values could be standardized by message type. Other features were adjusted to fit this unique application.

The authors recommended that remote storage be used to add some protection from denial-of-service attacks. This forces the requesting node to prove their trust to the serving node and prevents malicious nodes from forcing agents to search other peers for a non-existent trust value. Limiting the agents with whom communications are allowed to a specific subgroup reduced the need for this type of protection in this agent implementation.

Initial experimentation using this trust algorithm was designed to take advantage of local trust computation and storage. Trust valuations were not shared throughout the system to create global trust values and the scheme was designed to operate without cookie exchanges to reduce message size and network traffic. In fact, no additional communications were exchanged between agents. This format replicated Wang's original experimental results from [64] while validating the trust computation methods. Nodes would not share trust information in this setup, nor could they replace untrusted nodes with trusted ones.

3.2.2 Agent Communications Topology

Agent nodes were arranged in a structure created for joint system protection and were statically arranged to communicate with a preselected set of neighbors. This arrangement ensured communications with agents who would traditionally provide safety should protection efforts fall back on non-agent methods if communications were interrupted or terminated. In this implementation, agents would not be able to form

cliques only with other highly trusted agents as it could leave gaps in protective coverage. Agents have to be more selective in choosing trusted agents from their limited agent pool, basing decisions around the established topology as well as the trust metrics.

Preset communications were established for a given agent with three distinct groups. The first group consisted of any other agent sharing primary protection of the line. The second group was more extensive. This group included agents who augmented the primary protection by providing backup protection for that same line segment. The third group consisted of any intermediary agents located between the original agent and agents providing backup protection who were not responsible for protecting that given line segment.

Agent communications were then broken into two components. The first component was agent communications with the local power system interface which will be described in more detail in Section 3.2.3. The second component was agent-agent communications described in Section 3.2.4. These two components were used in conjunction to first obtain local power system conditions and then send that information to an agent belonging to one of the specified groups.

3.2.3 Communications Between Agents and Power System

Agent interactions with the power system included three types of messages. The first two types were a query and response for local state information. In response to a query, the agent obtained voltage and current measurements for each of the three phases of electric power as well as fault indications for the primary and backup protection zone and any primary or backup signals sent to the breaker directing a trip. The third

classification was a message to the breaker directing a breaker trip or directing the breaker to block the previously observed trip signal. The information obtained from the power system was temporarily stored to be exchanged with other agents.

3.2.4 Agent-Agent Communications

Communications messages between agents were classified as one of three types as well. The first two types were considered routine. First, each time period agents queried other agents for conditions at the remote location with information query messages. Second, agents would respond to a query by sending the local data that was obtained from their power system query using an information response message. The last type of message exchanged between agents was the set equipment message. It was intended to be used when an agent was unable to clear a fault itself. This message was defined as an advisory message to another agent that local protection mechanisms failed and coordinated help was necessary to clear the fault condition from a remote location.

The information query and response messages were sent to each agent with whom communications were preselected. This included the other primary agents, backup agents, and any intermediary agents. The set equipment messages were originally limited to the neighboring agent in either direction, but could be expanded to include the next logical agent in line depending upon the conditions and trust implementation that was selected. Reputation information was not exchanged between agents in this implementation. Trust metrics were based on direct observations. An inherited trust scheme that relied on referral information from others as described by [5] could potentially be integrated, but is not necessary and generates additional problems.

3.2.5 Cycle of Repeated Agent/Power System Interactions

Wang's original experiments were replicated after incorporating the NICE-inspired trust computation and storage system. In the simulations in [64], agents primarily communicated only with their immediate neighbors responsible for the shared protection of a line segment. This was expanded for use in the improved trust system as described in the previous section to better enable fault and system state verification.

Agent communications occurred in a cycle where the local power system conditions were first obtained. The agent then checked response messages that were received to determine if other agents detected any fault conditions. Agents used this information to verify if agent behavior matched known malicious activity and identified bad agents. Next, each agent responded to any messages querying for remote system or verified and reacted to set equipment messages. Finally, it queried all agents in the applicable protection regions for current state information and waited for responses.

3.2.6 Trust Metric Computations

In this new research designed to expand upon the work in [64], trust between agents was based on the interactions from status queries and the applicable response messages to focus on agent availability as opposed to message integrity. Observed behavior was also compared against predefined conditions that were used to identify malicious agents. Behaviors such as improperly sending set equipment messages or failing to trip a breaker when conditions warranted a trip were used to define malicious agents. Other implementations could be created that would not only depend on the frequency of communications, but also on comparisons of remote readings with local

measurements to include a measure of quality or correctness into the rating. For simplicity, this implementation only validated remote readings when sending or receiving set equipment messages.

The simple example in Figure 4 demonstrates how trust metrics are developed and maintained for a pair of communicating neighboring nodes. The number of query (Q) messages sent and responses (R) received are tracked for each agent with whom communications has been directed, in this case agents 4 and 5. A successful interaction, defined as a response to a query message, is stored as a 1. An unsuccessful interaction is stored as a 0. A trust rating is then calculated for each individual agent by dividing the number of responses received by the number of queries sent as

$$Trust\ rating = \frac{\#\ responses\ received\ (in\ last\ 100\ time\ steps)}{\#\ queries\ sent\ (in\ last\ 100\ time\ steps)} \qquad (3.1)$$

These computations result in a trust rating for each paired agent between 0 and 1. A positive rating represents an agent that is trusted to some degree. A higher ratio of successful interactions equated to a higher trust rating for that neighbor. An agent that is not trusted will be classified as bad using additional analysis, in which case it will receive a discontinuous rating of -1. Behavior resulting in a classification of bad can be seen in Table 1. This table is used to check for malicious behavior and can be tailored for a specific implementation to create the desired effects by adjusting the restrictions.

Table 1. Observed Behavioral Conditions Used to Classify an Agent as Bad

Condition #	Behavior
1	Agent sends false set equipment messages (in excess of the established threshold of 3 in the last 0.05 seconds)
2	Agent trip action fails during valid fault conditions

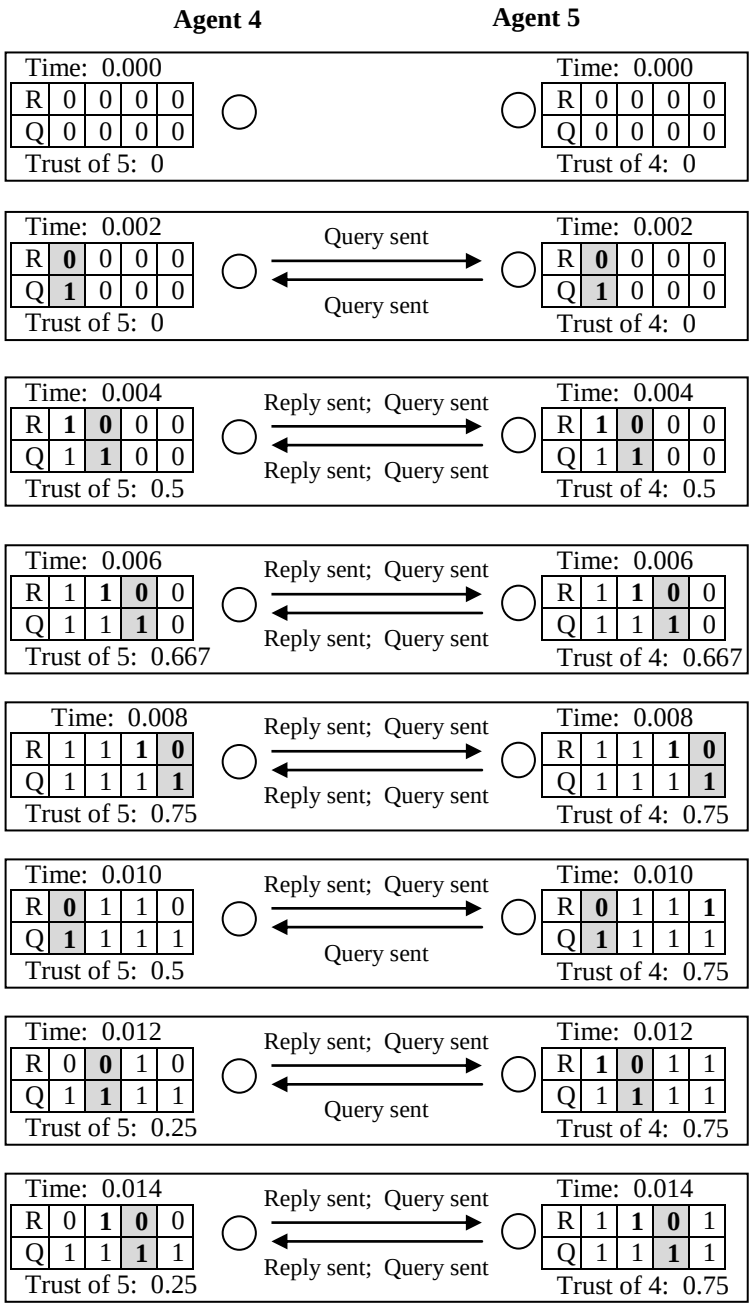

Figure 4. Example of trust computations: Shows seven information exchanges. Demonstrates how completed information exchanges are tracked to arrive at a current value of trust for a neighboring node.

The data an agent uses to compute trust values must be timely. In the simulations, request and response messages were sent approximately every 2 milliseconds. Older data in the trust computation is replaced with more recent data using a sliding window scheme. As shown in Figure 4, agents start with a trust value of 0 and slowly build trust by responding to data query messages as shown from the time period from 0.000 to 0.008. In the provided example, Agent 5 stops sending response messages from time 0.010 to 0.012 causing its trust valuation to be lowered. This lack of reliable communication indicates that it may not perform as expected during critical situations.

Ideally, agents want to respond to every query message, achieving the maximum trust rating of 1. Realistically, a trust rating of close to 1 is all that can typically be achieved due to the time delay required for message propagation. Unless an agent stops communication (which is not likely during normal operation) it will repeatedly send information queries (one each time period) as opposed to a scheme where an agent must wait for a response before sending its next query. In this manner, an agent will always have an outstanding query that has not yet been answered, resulting in an optimal trust rating lower than the theoretical maximum.

3.2.7 Reducing Trust and Using the Trust Metrics

Trust valuations are lowered if agents stop responding to information requests. Agents may stop responding to requests due to issues such as communication failure or interference, internal faults of either the sending or receiving agent, programmed behavior (malicious or benign) or a variety of other issues. Trust values may also be lowered if communications meet specified preprogrammed conditions such as sending

conflicting information, advertising faults when none actually exist or failing to take proper corrective actions. The trust values are then used when an agent sends or receives a message to or from another agent directing different equipment settings to assess that information source or destination. An agent with a trust value above the threshold can be assumed to be acting in the best interest of the protection system, whereas an agent with a rating below the cutoff can be assumed to have an issue with providing reliable information updates and thus protection. The information received from an agent below the threshold should be considered more carefully before it is acted upon.

The scheme must also be able to classify an agent with whom it has previously interacted as a bad agent. In this implementation, an agent classified as bad will receive a trust rating of -1 to indicate that it is not trusted and distinguish it from an agent with whom communications have not been established or were terminated using the behaviors depicted in Table 1. This rating is based on behavior and verification of message content and overrides the independent calculations associated with responding to queries. While this classification can be made for many reasons, an agent must consider the decision carefully before making this assignment. In some cases, the scheme may not be able to distinguish whether the agent is malicious or faulty, however there would still be benefit in reverting to an alternate protection scheme.

This implementation does not implement a procedure to recover from a bad classification. This is primarily due to the fact that maintenance would be required to either fix the protection components or the software at the remote location. An out of band process is recommended to reset the system after corrective actions are completed.

3.2.8 Decision Matrix Guiding Agent Behavior

To gain insight as to how the trust system would help the agents make decisions under different scenarios, a mechanism for detecting and responding to observed abnormal behavior was developed. The rule set that was proposed in [64] was modified to account for the addition of trust information and behavior analysis. The modified rules are presented as Table 2. This is similar to the rule set that helps guide alerts in an Intrusion Detection System. The agents needed guidance to react in a manner so as to increase the overall protection of the system under a majority of the test scenarios depicting both normal and abnormal system conditions.

The matrix detailed a set of rules that can be described using conditional statements. If a certain condition was met, one action was taken; if not met, a different action was taken. The rules now incorporate results from trust computation as additional conditions that must be satisfied to help decide which actions should be taken. Additionally, the rules were modified to let an agent adjust trust levels and classify and agent as bad if the observed behavior matched conditions specified in Table 1.

3.3 Collaborative Agent-based Protection System Simulation Tools

This research focused on integrating cooperative, reputation-based trust to support the agent-based scheme used for transmission system protection in [64]. The research presented here built upon the original experiments that show compact trip zone coverage and simultaneously reduced fault clearing time as presented in that research. The experiments covered here were run using the Electric Power and Communication

Table 2. Decision Matrix for Agent Behavior: Trust Inclusive Agent-Based Protection Scheme Modified from [64] (original rules shaded, trust changes in italics)

Rule No.	Situation	If…	Then…	Action
1	The relay sends a trip signal (to local CB indicating a zone 1 fault was detected)	there are no corresponding zone 3 relay operations in the agent's transmission region of concern from *trusted* agents and *trusted* agents exist	the relay sent an incorrect trip signal	Stop the breaker trip
		any of the *trusted* relays in the concerned region send a validated trip signal	the relay sent a correct trip signal	Monitor the breaker for operational failure – *Adjust relay trust levels if necessary*
		another situation occurs	Situation is Uncertain 1	Continue to Rule 2
2	Uncertain 1	there is a fault in the zone 1 protection zone	there was a correct relay trip	Monitor the breaker for operational failure – *Adjust relay trust levels if necessary*
		there is not a fault in the zone 1 protection zone	there was an incorrect relay trip	Prevent the breaker from tripping – *Continue to monitor for fault conditions and adjust relay trust levels if necessary*
3	The relay sends a trip signal (to local CB indicating a zone 3 fault was detected)	at least one *trusted* agent indicates a zone 1 relay trip in the concerned region	the relay operated correctly, continue to trip if fault is not cleared in allotted time	Monitor the breaker for operational failure – *Adjust relay trust levels if necessary*
		there was no zone 1 relay trips from *trusted* agents in the concerned region	Situation is Uncertain 2	Continue to Rule 4
4	Uncertain 2	there is a fault in the zone 1 protection zone	there was a local relay failure	Trip the breaker and monitor the breaker for failures – *Adjust relay trust levels if necessary*
		there is a fault in the zone 3 protection zone	there was a remote relay failure	Trip the breaker and monitor the breaker for failures – *Adjust relay trust levels if necessary*
		there is not a fault in the zone 3 protection zone	there was an incorrect zone 3 relay operation	Stop the breaker trip – *Adjust relay trust levels if necessary*
5	Operational failure of breaker is noted	breaker fails to operate correctly in time allotted	the breaker is malfunctioning and not providing local protection	Send set equipment notification messages to the agents in the concerned region
6	A set equipment notification message is received when relay operations are in progress	message is received from adjacent agent in same direction as indicated fault and *trusted* agents verified fault conditions	remote breaker failure occurred in agent's protection zone	Trip the breaker and monitor the breaker for failures – *Adjust relay trust levels if necessary*
		message is received from adjacent agent in opposite direction as indicated fault and fault conditions are verified with *trusted* agents in that direction	remote breaker failure occurred outside agent's protection zone	Trip the breaker and monitor the breaker for failures – *Adjust relay trust levels if necessary*
		message is received from a more distant / *non-trusted* agent or fault is not verified	Situation is Uncertain 3	Continue to Rule 8
7	A set equipment notification message is received when no relay operations are in progress	message is received from a trusted agent and fault conditions are verified with *trusted* agents in appropriate direction	remote breaker failure occurred	Trip the breaker and monitor the breaker for failures – *Adjust relay trust levels if necessary*
		message is received from an agent who is *not trusted*	Situation is Uncertain 3	Continue to Rule 8
8	Uncertain 3	fault conditions are identified/verified and any time delay to allow intermediate agents to clear the fault has passed	possible remote relay and breaker failures	Trip the breaker and monitor the breaker for failures – *Adjust relay trust levels if necessary*
		fault conditions are not identified/verified when time delay has expired	there is no fault in the system, invalid message	No control action is required – *Adjust relay trust levels if necessary*

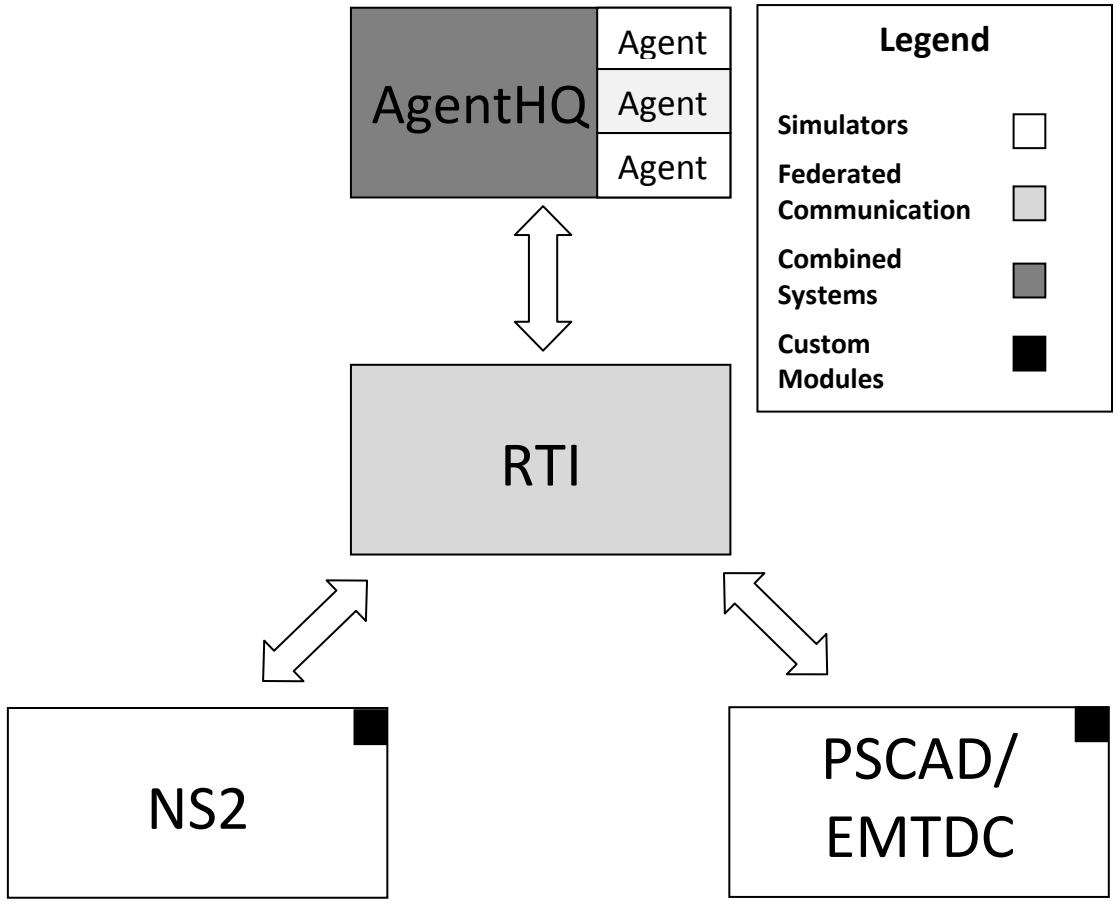

Figure 5. EPOCHS infrastructure: Depicting interactions between the NS2 communications simulator, the PSCAD/EMTDC power simulator and the EPOCHS agents. The Runtime Infrastructure (RTI) is a central interface location allowing for time synchronization and message passing [23]

Synchronizing Simulator (EPOCHS) to synchronize the Power System Computer Aided Design (PSCAD) power system simulator and the NS2 network simulator as seen in Figure 5.

3.3.1 EPOCHS

In order to model the complex relationships between the electric power infrastructure and communications networks, a simulation tool needs to combine information from different

systems to create one complete picture of the scenario. Researchers at Cornell University developed EPOCHS to link power system simulations to communications simulators. EPOCHS uses an agent-based framework to combine different simulations using their built-in interfaces enabling communications events to be involved in other power scenarios.

Hopkinson wrote that "EPOCHS was designed to link multiple simulations into a distributed environment (federation)" [23]. Combining simulators is becoming more popular as an approach to model complex interconnected systems. While standardization efforts are underway to enable better information sharing between simulators, many simulations include COTS products for which no source code is available. EPOCHS' use of agents helps combine information from both simulation systems, providing integration designed so that the simulations advance at the same clock rate.

This technique enables researches to use the best simulator for their needs without sacrificing quality for the sake of interoperability. EPOCHS used an agent headquarters and a run-time infrastructure as shown in Figure 5 to synchronize and coordinate simulations that would otherwise run at different speeds. In this simulation, the EPOCHS agent headquarters synchronized the PSCAD simulator with the NS2 communications simulator to allow agents to communicate with each other and interact with the power simulation. Time steps were set at 0.002 seconds for this follow-on experimentation.

3.3.2 PSCAD/EMTDC

PSCAD (Power System Computer Aided Design) is a commercial tool used to generate graphical representations of power systems for simulation use. In conjunction

with the EMTDC (Electromagnetic Transients including DC), electro-magnetic transients simulation engine, these programs allow for the analysis of power systems during system disturbances. They also allow parameters to be varied to simulate control actions taken in response to environmental changes. By providing the user with time domain instantaneous responses (also known as electromagnetic transients) through a graphical user interface, these systems allow for better analysis and understanding than previous text only simulators [34].

PSCAD/EMTDC was used to create the transmission network and display system measurements during the experiments. Measurement data and status values were exported to be used by the agents providing system protection. The simulations were kept in synch using EPOCHS and communications between agents took place using NS2. This communications simulator provided the agents with a way to exchange information before interacting with the power simulator again.

3.3.3 NS2

NS2 (Network Simulator 2) is used to simulate discrete events for network simulation. Development began in 1995 with support from Lawrence Berkeley Labs, Xerox PARC, University of California at Berkeley, and University of Southern California [46]. Due to the public availability of the source code, NS2 is widely used in research for large scale communications simulations and protocol investigation. Coding is based around C++ for processing performance combined with Tcl scripts for simulation control. This split programming adds flexibility and separates mechanism from policy when designing simulations [8].

The implementation used for the experiments combined NS2, the RTI, the AgentHQ and agents into a single executable. The ability to create protocol stubs within NS2 allowed the RTI to interface between the different components in a synchronized manner [8]. A single executable for these components provided performance enhancements compared to running additional programs. The simulation required corresponding networks for both the power system and communications infrastructure.

3.4 Experimental Environment

A simplified transmission line network was created in PSCAD consisting of two power sources, one at either end separated by three substations and connected together by four transmission lines as depicted in Figure 6. Every transmission line is protected with two circuit breakers. The breakers are located at either end of the line and each is controlled by a distance relay. The distance between substations is depicted in that figure as well since it is not shown to scale.

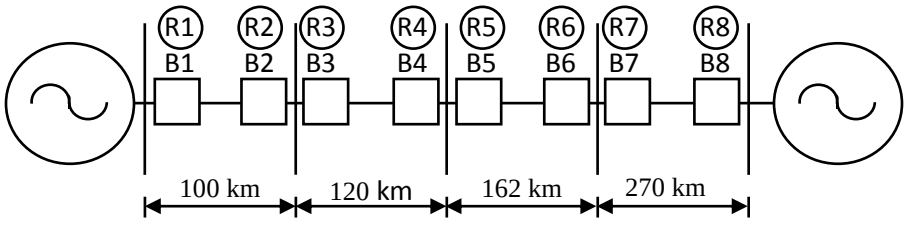

Figure 6. Simulated 400 kV power system used in the experiments: Depicts a generation source at either end, four transmission lines, and eight circuit breakers (B1-B8), each protected by an IED relay (R1-R8) [23]. Transmission line lengths are provided since diagram is not to scale.

The original experiments in [64] were designed to protect a 400 kV high-voltage transmission system against a three-phase fault using distance protection methods. In the simulations, request and response messages were sent approximately every 2 milliseconds. Communications between agents included measurements taken from current transformers, voltage transformers, and anti-aliasing filters. Relay protection was provided by distance and time-delay relays using traditional settings. The distance relays used the discrete Fourier transform (DFT) to obtain inputs. Experiments were conducted based on two different situations. The first situation involved incorrect operation of a zone 1 relay. In the second scenario, circuit breakers were designed to fail in the closed position, failing to open when directed by their respective relay.

3.4.1 Original Communications Setup

In the work done by Wang, agents communicated at a very simplified level and no background traffic was simulated, eliminating effects caused by network congestion. Each substation bus resulted in a one millisecond propagation delay added to communications. The messages between agents consisted of requests for system state (voltage, current, breaker status, etc.) at another agent location, requests for an agent to set a breaker at their location and any applicable replies to those requests. Agents would then make use of that information to collaboratively clear a fault in as small a region as possible. Agent communications were limited to a node's immediate neighbors or immediate neighbors plus an additional agent protecting the adjacent line.

3.4.2 Revised Communications Setup

The revised communications setup for these experiments included a more complete range of agents to help coordinate protective actions. Communications were needed with all agents responsible for providing zone 1 protection of the primary line and each adjacent line segment. This allows agents to verify fault conditions in zone 1 segments, zone 3 segments and adjacent line segments that it was not responsible for protecting based on the interactions with those agents. Agents observing a zone 3 relay signal would monitor the appropriate agents responsible for primary protection to verify that they attempted to trip their local breakers and the success or failure of that trip. They could use this data to observe whether the agent was working correctly or not and determine if they needed to take action. This action could be accomplished without waiting the traditional amount of time to see the effects of the stabilization attempt at their location.

Additionally, when trust was lost with an agent responsible for primary protection, the set equipment request could be sent to the next agent in line available to take protective actions. The receiving agent had the option to either trip immediately or first verify that the fault was not actually cleared before tripping the breaker at their location. If the fault was cleared by the agent who was believed to be untrustworthy, the agent would be exonerated otherwise they would be classified as bad. By increasing the number of set equipment message recipients, the trust system improved clearing time.

This and the original research are stepping stones for improved relay communications that could be incorporated into larger SCADA protection schemes.

During the transition to a Smart Grid, data retrieved from monitors and passed between agents could also be used to update the central control facility. These updates would provide the system operator with additional details necessary for improved situational awareness. The intelligent agent protection scheme forms the cooperative environment upon which the remainder of this research is based.

3.5 Experimental Situation and Issue Requiring Backup Protection

These revised rules from Table 2 that guide agent actions must remain applicable when using trust in the normal non-malicious environment and should enable the system to match the performance achieved in the original experiments. This research first attempted to replicate the performance of the original agent-protection scheme using scenarios based around Wang's second case in [64]. In this simulation set up, a fault was triggered at the midpoint of the line protected by Breaker 5 and Breaker 6 as shown in Figure 7. A fault at a location such as this should be caught by the primary zone 1 protection provided by relays 5 and 6 as well as the zone 3 backup protection from relays 3 and 8.

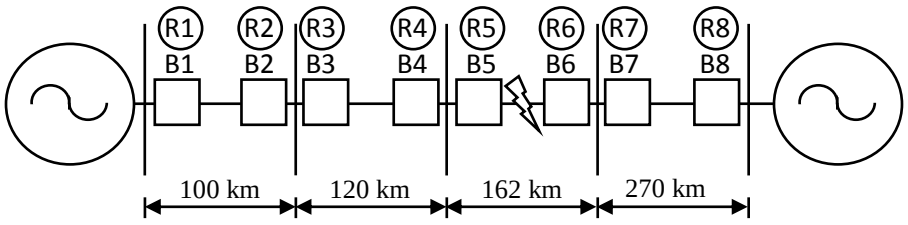

Figure 7. Experimental transmission grid showing fault location: Fault depicted at the midpoint between breaker 5 (B5) and breaker 6 (B6).

In this case, the relay providing signals to breaker 5 notices that the breaker fails to open and sends a trip signal to relay 4 to clear the fault by cutting out the smallest amount of line. Relay 4 attempts to trip breaker 4. Unfortunately, this breaker fails to open as well and relay 4 sends a signal to relay 3 to open that breaker. Breaker 3 receives the signal from relay 3 and operates correctly, clearing the fault in less time than traditional protection measures would. During the original experimentation, the fault was cleared at 0.188 seconds with the agent system as opposed to 1.592 seconds with a traditional relay backup protection system.

The other case that was considered in [64] involved a false trip signal detected at Breaker 5. The agent based scheme used the information from cooperating agents to block this false trip signal and prevent the breaker from opening. The improved trust scheme must be able to continue to act correctly to this issue when subjected to malicious behavior. Since protection capability is dependent upon communications from partner agents, the robustness of the trust scheme must continue to protect from false breaker trips even when information update messages are not sent by a neighboring agent or if they receive false set equipment requests. This feature was tested using two scenarios. In one, Agent 4 did not send any message traffic to Agent 5. In the second, Agent 4 sent false set equipment requests to Agent 5.

3.6 Experimental Scenarios Used in the Analysis

Additional experimental scenarios mimicking potential real-world issues that might be experienced were created to test the cooperative trust scheme. Eight new

Table 3. Experimental Scenarios: Non-Optimal/Malicious Agent Communications

Scenario #	Situation depicted
1	Baseline case – no malicious behavior
2	Agent 5 will not send information response messages
3	Agent 5 will not send set equipment messages
4	Agent 5 will not send information response or set equipment messages
5	Agent 5 sends false set equipment messages
6	Agent 4 will not send information response messages
7	Agent 4 will not send set equipment messages
8	Agent 4 will not send information response or set equipment messages
9	Agent 4 sends false set equipment messages

scenarios were developed, intended to mimic conditions that might be experienced by a protective agent. These studies are based around a situation where a three-phase fault occurs between breakers 5 and 6. Both breakers 5 and 4 will fail to operate when they receive a trip signal, however this information is not known to the agents until fault clearing is attempted. These scenarios are presented in Table 3.

In this research, a look at the overall system behavior was warranted since some individual relays were designed to fail. To review, for these scenarios correct behavior was defined as tripping the breaker only when an actual fault condition exists and only isolating the minimum area between working breakers. The baseline scenario was added to depict the normal communications environment. The other scenarios replicated effects from some type of malicious activity aimed at interrupting or adding message traffic between agents. There was not rule in Table 1 that used a lack of communication on its own to classify an agent as bad. This was primarily due to the lack of a trust redemption mechanism.

3.7 Experimental Parameters Varied for the Trust System

Different trust implementations were developed by varying some of the parameters involved with either trust computation or actions taken when trust was lowered or lost. The experimental trust-based implementations were tested initially varying four parameters from Table 4 using a full factorial design for each of the first five scenarios from Table 3. This was done to verify assumptions regarding the dependency between trust system thresholds and percentage of network traffic lost. Final experimentation was accomplished using all nine scenarios and reducing the number of parameters to two by holding the number of interactions tracked constant at 100 using the sliding window scheme and the trust system threshold constant at 0.75. Agents were initialized with a trust rating equal to the trust system threshold for this implementation. The results were compared with the non-trust-based agent system's performance in each of those nine scenarios.

The number of interactions tracked was kept rather small to ensure that only the most recent information was used to compute trust. Protection mechanisms need to be

Table 4. Trust System Parameters Varied in Experiments

Level	# of Interactions Tracked	Trust System Threshold Value (0-1)	Add additional breaker to trip list	Likelihood network traffic is lost
Low	50	.95	When below trust threshold	1%
High	**100**	**.75**	When an agent is classified as bad	10%

responsive to system failures that may be hidden for long periods of time [38]. The trust system threshold values were selected based on the likelihood that network traffic was lost. Previous research suggested a range of values for lost UDP traffic in a communications network with typical minimum values of 1% or less and maximum values of less that 10% [4], [15], [21], [26], and [69]. These figures will differ depending upon the type of underlying communications network supporting the protection plan as described in [43] and [52]. Current work is under way to investigate protection for these communication lines [49] and improve the communications reliability to provide better system protection [66].

3.8 Methodology Synopsis

To summarize, this research will use simulation to conduct experiments integrating a reputation-based trust system with a proposed backup protection system for power networks revolving around agent-based communications. The simulations will use EPOCHS to synchronize the inputs and outputs from the PSCAD/EMTDC power system simulator with the NS2 communications network simulator as described in [64]. Trust will be built between agents cooperating to provide backup protection through regular status query and response messages. Information obtained from the response messages will assist in behavioral analysis and enable the agent to build a more complete picture of system events. The trust system used in this protection scheme is inspired by the distributed model for Project NICE [32] using a modified implementation to take advantage of the unique situation posed by its application to the power system.

The scenarios designed for the experiments demonstrate the ability of the proposed trust-based protection system to provide more correct decisions than the original agent-based protection implementation when presented with behavior mimicking malicious activity as well as during normal operating conditions. The reputation-based trust system will also enable more timely protective actions to take place. In turn the additional analysis and improved system information is effective in preventing the stability problems that contribute to cascades, further improving upon the traditional distance relay protective mechanisms.

IV. Results and Analysis

THIS chapter presents results from the experimental simulations and an analysis of the impact from incorporating cooperative trust into a backup protection scheme for power transmission networks. First, results from the initial inclusion of a trust monitoring system will be covered. Second, investigative questions regarding the importance of different system characteristics and dependence of some variables will be examined. Third, results from each of the scenarios used in the simulation experiments will be presented. Finally, an overall analysis of the results will be given in the last section in this chapter.

4.1 Initial Trust Monitoring Scheme

Results from the experiments were favorable. The first set of experiments was conducted to replicate the original results of Wang's research while adding the appropriate trust structure. The trust values were computed and stored however no actions were taken using the trust computation results. This experimentation was done solely to provide information that could be used as part of a centralized control monitoring system providing system operators additional situational awareness about device status, network communications, and agent behavior. The results demonstrate that the system could perform at least as well as the original system while documenting behavioral abnormalities and providing additional status information.

In these case studies, the fault at 0.3 seconds between agent 5 and agent 6 caused agent 5 and agent 6 to properly detect a fault and send a signal to open their respective

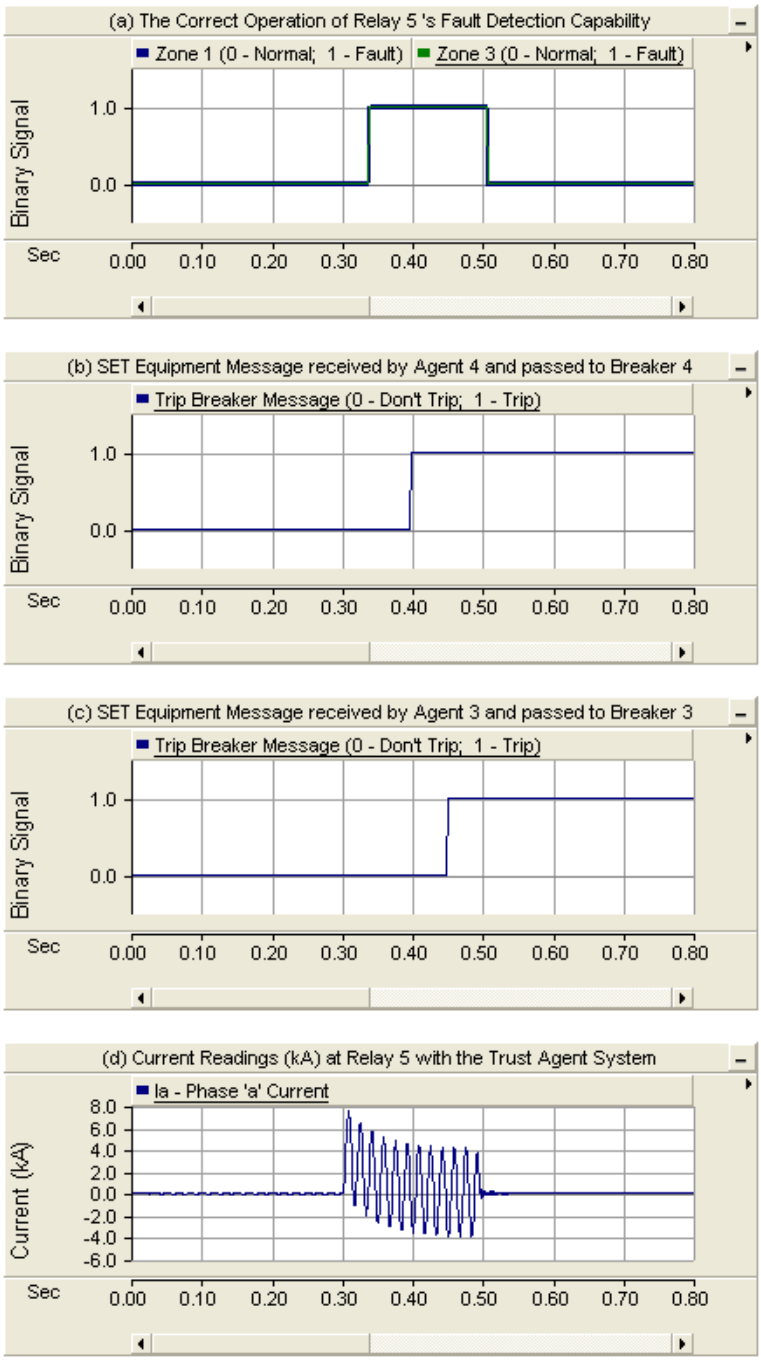

Figure 8. Fault clearing of agent-based protection system with trust scheme: Initial experiment results showing the agent-based protection system with integrated cooperative trust able to replicate the results achieved in [64]. Fault at 0.3 seconds cleared at 0.488 seconds by agent 3 and recognized by agent 5 at 0.506 seconds.

circuit breaker as a result of primary protection trip signals as seen in Figure 8a. The agent at relay 5 providing backup protection notices that the breaker does not open when provided with a proper signal. Agent 5 sends a set equipment message to agent 4 as seen in Figure 8b. Agent 4 notices its breaker does not open and it sends another set equipment message to agent 3 as shown in Figure 8c. Agent 3 is finally able to clear the fault at approximately 0.488 seconds as shown from the current readings at relay 5 graph in Figure 8d.

The results of this initial test appear identical to the results used by the system without a trust component, because the trust information was gathered, but not used in decision analysis. Unfortunately, this method of trust implementation would not add any additional assistance to the agent's decision making capability since it was not used locally. To be of use in this type of system, this trust data would need to be collected by a central monitoring station and interpreted there. The impact created would improve the situational awareness of the operator and could help network analysis. Any action to remedy the situation would have to be taken from his remote location. Further experiments showed that more timely decisions were made if agents used these metrics autonomously for corrective actions. They also showed using these trust metrics resulted in a higher percentage of correct decisions when faced with malicious activity.

4.2 Investigative Questions Answered

Prior to developing the final trust implementation this research examined the parameters that were selected and analyzed their impact on the experimental scenarios. In the second set of experiments, parameters were varied as depicted in Table 4 for the

first five scenarios in Table 3. The purpose of this round of experimentation was to verify the relative importance of each message type to the trust scheme. By establishing a relationship between trust system settings and corresponding agent reactions, proper system settings were verified and experiments documented failures resulting from improper system setup.

Results from these experiments showed that use of the trust system was effective in reducing fault clearing times when malicious activity was present in the system. The original agent system typically reverted to traditional standby backup protection mechanisms (as used in non-agent based protection systems shown in Figure 9) when faced with a malicious situation that prevented authorized set equipment messages from

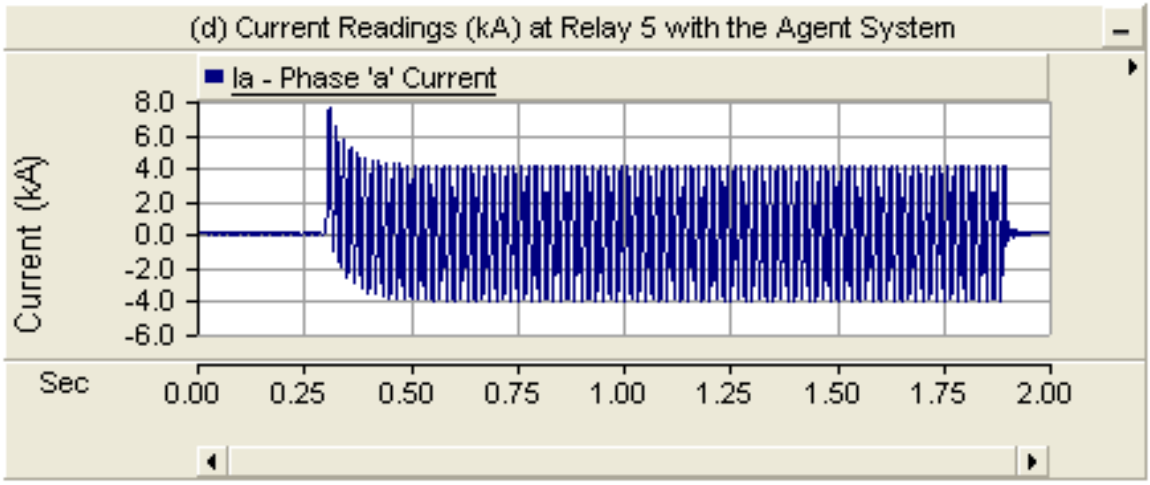

Figure 9. Fault clearing of traditional transmission line backup protection: Results from traditional transmission line backup protection system based off a time delay of 1.5 seconds as set in [64]. This is representative of the typical time it would take to clear a fault in most current implementations set on the order of 1 second [24] and [59]. The agent system needed to provide better performance in both normal situations and during periods of malicious activity more closely approximating results achieved during normal activity and shown in Figure 8.

being sent. When the original system was faced with situations where unauthorized set equipment messages were sent to agents, the lack of a mechanism to check the trustworthiness of the sender caused an immediate breaker trip without first observing or verifying fault indications.

The modified agent-based protection system including the trust calculations was able to recognize an abnormal situation only when it caused a lack of trust. If recognized, it could then react more quickly to the situation. This established the first fundamental rule. The system must be programmed to recognize and react to specific behaviors. If a specific behavior or action was recognized as matching a condition described in Table 1, the agent was able to override the respective trust computation and distrust that agent completely. A software based design allowed for the reprogramming of agents enabling their decision making abilities to be upgraded, assisting with adaptive protection capabilities.

A second lesson learned dealt with properly setting threshold trust values used for agent classifications. Original parameter settings causing situations where the actual trust rating was close to or below the trust threshold limit validated the assumption that additional information must be considered in certain circumstances such as monitoring to verify if an agent tripped or not. Initial experiments simulating a 10% loss of message traffic and a trust threshold value of .95 required to classify an agent as good helped demonstrate the improper agent reactions.

Although acting as programmed, an excessive number of agents were classified below the trust threshold. Because they should have been trusted, extraneous set

equipment messages were sent into the system without proper reason. Set equipment messages were originally limited to an agent's immediate neighbors (one in each direction). The new implementation included an option to send set equipment messages to the next logical agent in line as well, bypassing agents that did not meet the trust threshold. These additional set equipment messages consumed communications bandwidth and forced agents to do more work, but improved protection. This feature enabled the trust system to isolate the fault more rapidly and reliably while increasing the isolation area by the smallest amount. However, without proper safeguards, these extra messages resulted in unnecessary circuit breaker trips that extending the recommended isolation zone. When a message arrived from an agent that was more than one hop away, actions were delayed. The more distant agent waited to verify the effect of any actions of the agent that did not meet the trust threshold to determine if an extended breaker opening was required.

A third lesson was observed during this experimentation. Normal information exchanges between agents established trust, but also verified remote agent actions. In both systems, the set equipment messages were used to inform of a local protection problem. However in the original system, the information from the response messages was only used to block a false local fault observation. In the expanded trust system, information from remote agents was also used to verify fault conditions in multiple line segments to improve coordinated protection as well as for the trust calculations.

When these response messages were lost, it directly affected the trust calculations and caused temporary periods where an agent acting in a trusted manner (and able to

clear faults) was incorrectly labeled with a low trust rating. To fix this problem, instead of reacting solely on instantaneous information, the trust system was remodeled to incorporate recent power system state information from the last 0.01 second. This accounted for a realistic degree of information loss in the system and improved data verification. Additionally, set equipment messages were sent twice to increase the probability that they would reach their intended agent adding redundancy.

Adding redundancy to communications networks in power control systems was recommended in [66] and [67]. Redundancy was added to the trust system fault verification modules ensuring that adjacent node status was not lost due to a temporary communication interruption or missed message using a sliding window to track signals and measurements from the past 0.01 seconds. While communications redundancy is often thought of as creating multiple independent paths between nodes, the implemented method of resending and tracking recent information also created communications redundancy. Agents validated local and remote power system settings more correctly after its incorporation better compensating for parameter simulating lost network traffic. It allowed for collaborating information that was obtained in different time slices while ensuring the relative timeliness of reactions to that information. These changes added to the trust agent implementation prevented the isolation region from be expanded unnecessarily.

These preliminary experiments also helped standardize trust system parameters used for the final set of experiments. In the trust implementation, the trust threshold value was set accounting for at least twice the max expected value of a message being

lost. Since the system relied on query and response messages, there were multiple opportunities for a complete trust transaction to be interrupted. As a result in the final set of experiments, the trust threshold was established at .75, analytically accounting for the expected value of lost network traffic, expected propagation delay, and processing time associated with the agent communications. This value limited the number of occasions when trust calculations accidentally fell below the threshold.

Experimental results were similar when the number of tracked interactions was varied. This was expected because the malicious scenarios evaluated in this research did not attempt to exploit this aspect of the trust scheme. However in an actual implementation, the number of interactions tracked should be set according to the importance that minor fluctuations have on the system, the trust update mechanism selected, and the level of risk that an organization is willing to accept. The fewer transactions tracked, the more rapidly temporary periods of communication interruption will be forgotten. Trust will be lost and regained more quickly in this situation. In the final experiments, tracked interactions were held constant at 100 resulting in a complete information refresh every 0.2 seconds as opposed to 0.1 seconds with 50 tracked interactions. This value should be adjusted after identifying the risk to threats attempting to exploit reputation lag vulnerability [27]. More complex schemes that layer multiple trust ratings by tracking short and long time windows can help mitigate some of this risk.

Additionally, it was noted that extending the list of agents to whom set equipment messages were sent only if an agent was classified as bad, was not as effective as an approach that relied also on the comparison of the calculated trust metric with the

threshold value. Using solely the bad category limited the effectiveness of the system to only those situations that met a scripted preprogrammed behavior. Loosening the restrictions and allowing the set messages to be sent to an extended set of recipients added robustness, but increased the computational cost at each extended recipient. This new policy enabled bypassing agents who might be later classified as bad. To prevent premature reactions to these messages, a time delay was added to prevent the more distant agent from opening a breaker without verifying that the fault was not cleared by the less trusted neighbor. This delay was set at 0.05 seconds to account for the time required for that agent to open its breaker and stabilizing effects of clearing the fault to be noted in the voltage and current readings.

Finally, signal verifications taking place between the interacting nodes enabled additional protection to be integrated into the system. Agents were able to take action based on more immediate system feedback instead of waiting for timers to expire using traditional mechanisms. They were able to directly compare readings and cross check these readings with set equipment requests. This helped reduce the fault clearing time in certain situations improving system stability.

4.3 Final Trust Scheme Results and Analysis

In the final trust scheme that was created, the additional verification and redundancy integrated into the system resulted in a more successful trust system implementation providing additional protection in the face of malicious agents. The trust

Table 5. Final set of parameters used for trust system experimentation and analysis

Selected Trust Implementation	# of Interactions Tracked	Trust system threshold for good agents	Likelihood network traffic is lost
No Trust Scheme	Not applicable	Not applicable	1%
			10%
Add additional breaker to trip list when computed trust value is below trust threshold	100	.75	1%
			10%
Add additional breaker to trip list only after an agent is classified as bad	100	.75	1%
			10%

system made correct decisions in all nine scenarios with the improved backup protection mechanisms clearing faults in less than 1.0 seconds in all cases regardless of whether breakers were added to the set list if they were below the trust threshold or only if they were classified as bad. This was a significant improvement over the original agent scheme with no trust integration. Table 5 shows the breakdown of parameters for experiments that were run for each scenario.

4.3.1 Sign Test for Median

Due to the relatively small sample size (25 simulation runs were accomplished at each experimental setup) it was not reasonable to expect that the underlying distribution was normal. First, nonparametric methods were used to compare the median values obtained from experimentation using both the Sign Test for Median and the Wilcoxon Signed-Rank Test (Appendix A contains more detailed analytic results using reduced median times of 0.3 and 0.5 seconds that are closer to settings associated with zone 2

protection [24]). For each of these tests, the null hypothesis states that the median trip time is greater than or equal to 1.092 seconds accounting for a recommended time delay on the order of 1.0 second [24] and [59]. The alternative hypothesis is that the median is less than 1.092 seconds. In each of the scenarios, exactly 0 of the cases was observed to - be greater than or equal to 1.092 seconds. The observed value of each of the test statistics Q_+ is 0. It is assumed that the Q_+ is binomially distributed with p=1/2 [41]. In this case n=25 and the P value is 0.000 [37], [50], and [68]. With a P value this small (less than our alpha of .05), we reject the null hypothesis. There is strong statistical evidence that the improved trust scheme is able to reduce the time required to clear the fault.

4.3.2 Wilcoxon Signed Rank Test

Additional statistical significance is provided using the Wilcoxon Signed-Rank Test since our experimental results are reasonably symmetric. In this test, a value for W of 0 was calculated again. When W = 0 with 25 samples, the P value for this test is less than .005 [41]. This is too small to have occurred by chance. As a result, the null hypothesis can be rejected and it is statistically accurate to state that the improved agent-based protection scheme integrated with cooperative, reputation-based trust metrics is able to clear faults more quickly than currently used traditional backup protection schemes. In fact both sets of tests show that it is statistically correct to say the agent implementation can clear faults in less than 0.592 seconds and often less than the 0.392 seconds more typical of a zone 2 relay when encountering the tested scenarios.

4.3.3 Significant Results Regarding Clearing Time and Correct Actions

In six of the nine scenarios, the trust system improved results compared to the original agent-based system either by reducing clearing time (the original implementation reverted to traditional mechanisms in Scenarios 3, 4, 7, and 8) or by making improved decisions (not tripping solely based on receiving instructions to trip as in Scenarios 5 and 9). The most rapid clearing times were associated with the trust implementation that send additional set equipment messages if an agent dropped below the trust threshold at both 1% and 10% traffic lost. Had an additional rule been added to classify an agent as bad if their trust dropped below a lower threshold, the times might have been improved for the alternate scheme where additional agents were sent set equipment messages only if they were identified as bad. This would have added to the complexity of the rule set and had the potential to classify agents as bad without any malicious activity having occurred.

4.3.4 Results From Original Agent-Based Protection Scheme with No Trust

The original agent scheme that did not incorporate a trust scheme was used as a reference point to compare the effectiveness of the different trust implementations versus what occurred when the original agent system faced these scenarios. In the scenarios revolving around set equipment messages being lost (Scenarios 3, 4, 7, and 8), the non-trust agent implementation reverted to traditional relay backup mechanisms as seen in Figure 10. This resulted in the fault being cleared at the pre-established time delay set for the backup protection (1.5 seconds), reducing the benefits of a communicating agent system. Additionally, because trusted relationships were assumed, there were incorrect

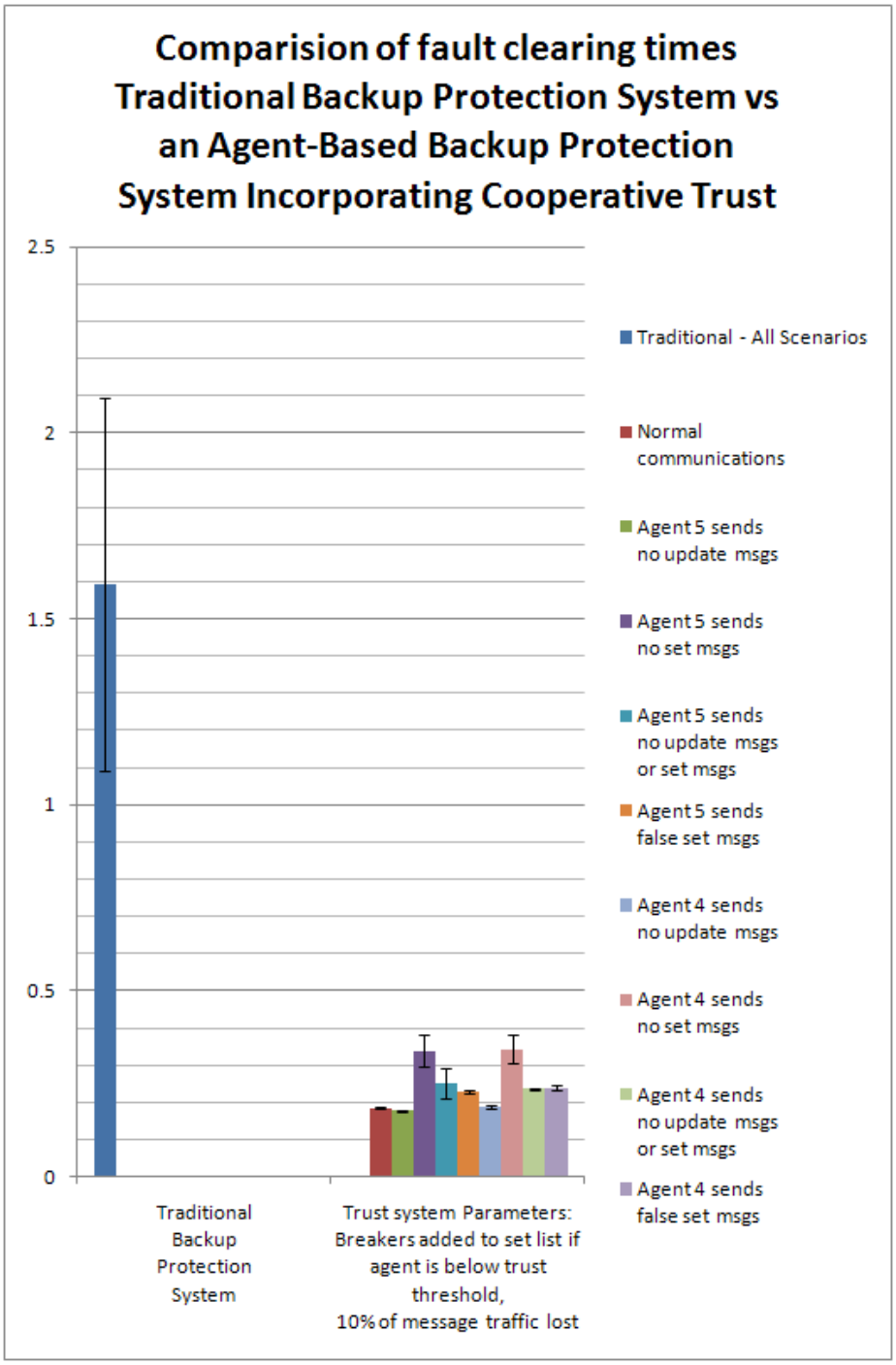

Figure 10. Fault clearing times using original scheme without trust mechanism: Comparison of fault clearing times (with a 99% confidence interval) between traditional backup protection and the original agent based scheme that did not incorporate a trust mechanism.

responses observed in Scenarios 5 and 9. In these instances, as soon as an agent received a set equipment message from a neighbor, it attempted to trip its breaker immediately isolating regions of the power grid unnecessarily. As a result, in 22.2% of the scenarios, there was an incorrect response and in 44.4% of the scenarios the system reverted to traditional backup protection resulting in non-optimal decisions being made in 66.7% of the situations.

4.3.5 Results From Trust Implementation 1 (Agent Below Good Threshold)

In contrast, the trust implementations that created an extended net of recipients for set equipment messages did not revert to the traditional backup protection mode and did not trip when extraneous trip signals were sent. Specifically, the best implementation was the one that sent set equipment messages to the next agent in line if an agent that was supposed to receive a set equipment message fell below the established trust threshold for good classification. The improved trust scheme was able to better identify fault location and clear the fault based on the expanded set of information that it was able to obtain and analyze. By interacting with all agents responsible for protecting the specified segment of transmission line, an agent was more likely to verify any zone 1 or zone 3 fault signals that were observed.

By verifying these signals, the agent was able to adapt to malicious behavior and reduce clearing time as shown in Figure 11. Signal verification was used to cross reference readings from multiple locations and remote current measurements were used to prevent creating an isolation zone that was larger than required. These verifications,

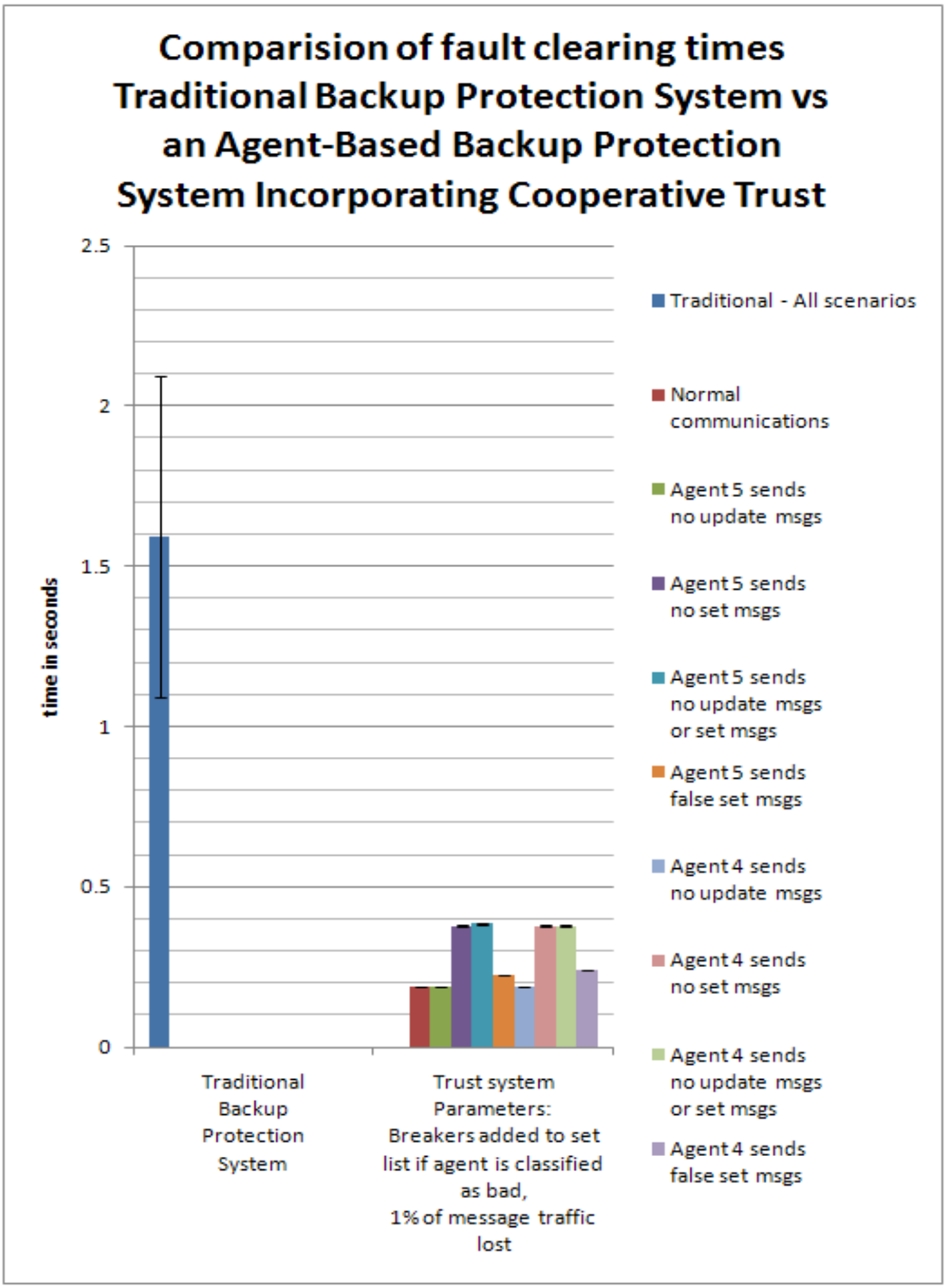

Figure 11. Fault clearing times: set messages extended if below threshold. Fault clearing times with a 99% confidence interval for agent implementation where set equipment messages are sent to an extended set of recipients if trust metric is below established threshold. Scenario 1 – Normal communications through Scenario 9 – Agent 4 sends false set msgs are listed.

lengthened the overall time to clear the fault compared to normal communications situations but the tradeoff in ensuring that breakers did not trip unnecessarily was worth the delay.

The difference in performance with the original system was obvious especially when comparing Scenarios 3, 4, 5, 7, 8, and 9. The difference in performance with the second trust implementation where the set of agents receiving set equipment messages was only extended when an agent was classified as bad was less noticable. During the worst case scenario when 10% of message traffic was lost the difference in performance was limited to being statistically significant only during Scenario 8. Under more normal operating characteristics (1% of message traffic lost) however, the differences were noticable under both Scenarios 4 and 8. This tradeoff requiring weighing additional verification and programming versus fault clearing time must be determined by the user selecting the implementation and the computing resources they have available.

In Scenarios 2, 4, 6, and 8, trust levels were properly established at lower levels for the agent that was not responding properly to information queries. In Scenarios 2 and 6, that agent did send a set equipment message when it realized that it was broken enabling a response time more closely aligned with the time established in the baseline Scenario 1 where no malicious behavior occurred. In Scenarios 3 and 7, the agent was trusted but refused to send set equipment messages. The agents were able to compensate, but clearing time took longer than normal and longer than the time required when the respective agents were identified by lower trust metrics. In Scenarios 5 and 9, the agents who knowingly tried to send improper set equipment messages were appropriately

labeled as malicious, the continued set equipment messages were ignored and actions were taken accordingly and appropriately when a valid fault signal was received. Faults were cleared after the appropriate signals were verified as valid using multiple sources. In other situations where agents were identified as not acting in accords with proper behavior, the system had the option to label them as malicious when this behavior was noted, enabling better response actions in the future.

4.3.6 Results From Trust Implementation 2 (Agent Classified as Bad)

In the alternate trust implementation that reduced the occasions where set equipment messages were sent to an extended net of agent to those when conditions led to an agent's classification as bad, results were similar to the previous trust implementation. It outperformed the original agent-based scheme as well as traditional backup protection mechanisms as shown in Figure 12. The only occasions when these extended set equipment messages were sent were during Scenarios 5 and 9. As a result, the only real statistical difference between this implementation and the previous trust implementation that had fewer restrictions on extending the set equipment message list was found from experiments done with Scenarios 4 and 8 where trust was lost and the agent did not try to let others know that it experienced failure and needed protection help.

4.3.7 Results for Alternate Cases Requiring Blocking a False Signal

The second protection case involving Breaker 5 receiving a false signal to trip again produced favorable results for the reputation-based agent protection system. When

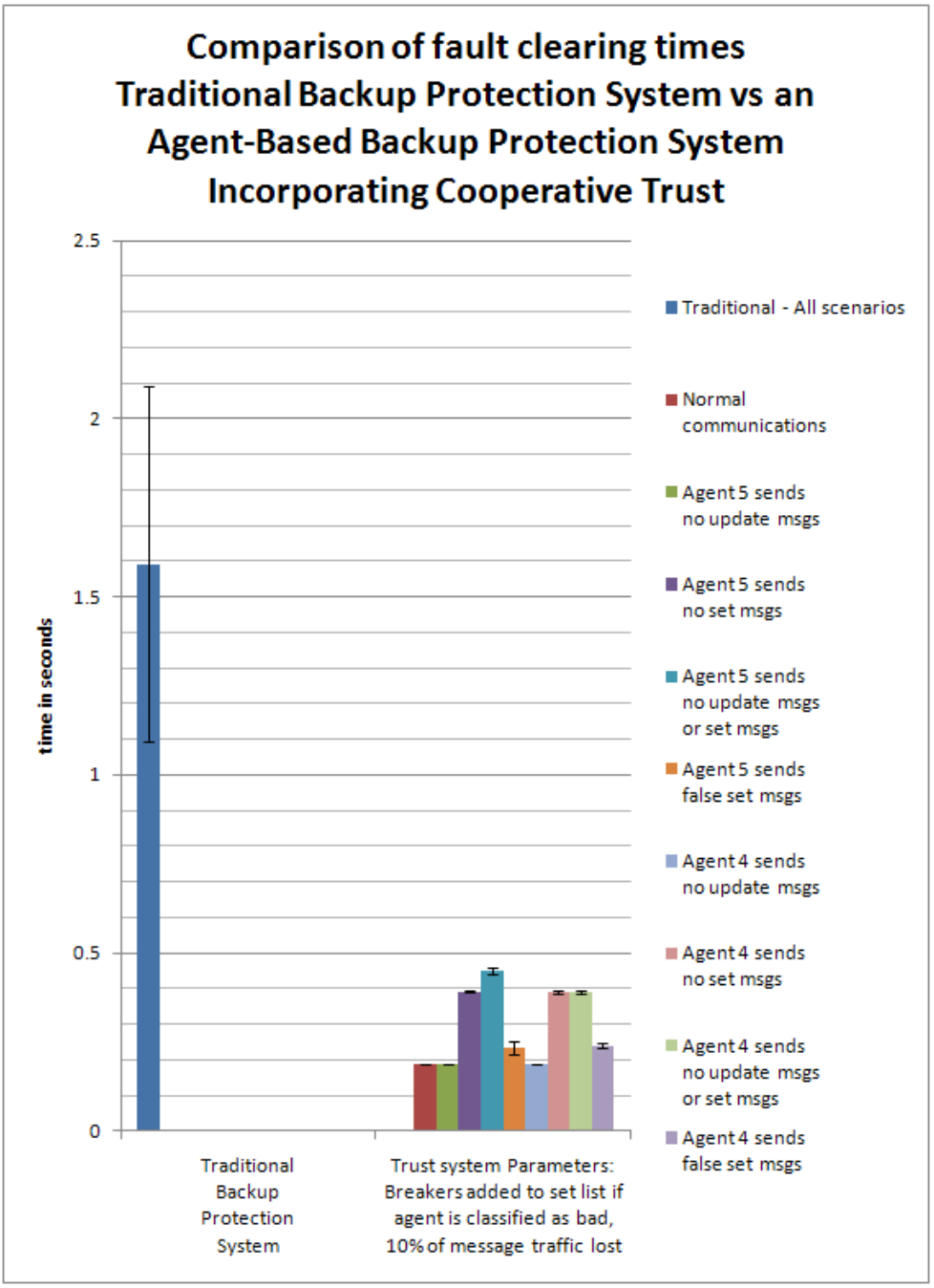

Figure 12. Fault clearing times: set messages extended if agent classified as bad. Fault clearing times with a 99% confidence interval for agent implementation where set equipment messages are sent to an extended set of recipients if agent is classified as bad. Scenario 1 “Normal communications” through Scenario 9 “Agent 4 sends false set msgs” are listed.

experiments were run using either of the two trust implementations, the false trip signal was successfully blocked and power continued to flow. This was a result of ensuring that agents who were not trusted did not delay protection efforts. Waiting for untrusted agent information either caused too long of a delay or resulted in an incorrect decision being made. The non-agent based detection scheme is not prepared for this situation and would trip a breaker as shown in Figure 13. The original agent scheme that did not incorporate

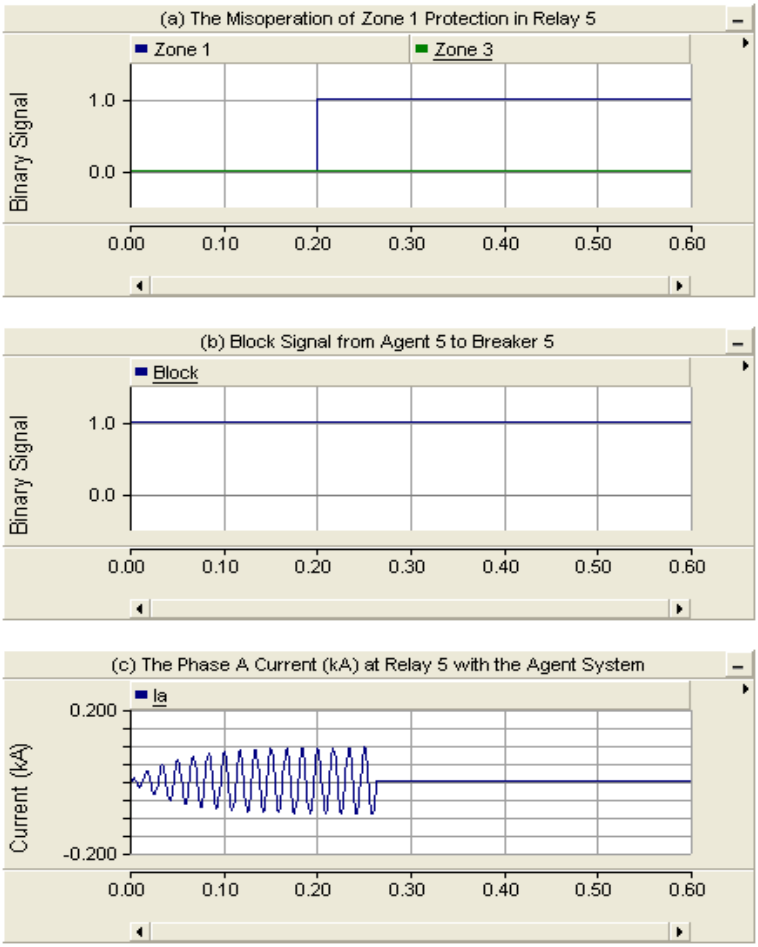

Figure 13. Original agent system trips breaker due to false signal. Shows false trip signal sent to Breaker 5 at 0.20 seconds (a). Relay 5 failed to block the false signal in graph (b) resulting in the breaker tripping and stopping the current flow seen in graph (c).

this trust component was unable to successfully react to the situations where information updates were not sent from a neighboring agent and when the neighboring agent sent false signals to trip the breaker. In the situation where communications were interrupted, the breaker tripped as it would in the non-agent system [64] as shown in Figure 13. In the other situation, the breaker tripped immediately after the agent received the false set equipment message because it did not verify the lack of a fault condition. The reputation based cooperative trust scheme met the protection condition established in [64] by continuing to allow current to flow (as shown in Figure 14) under abnormal communications conditions and when subjected to malicious agent actions.

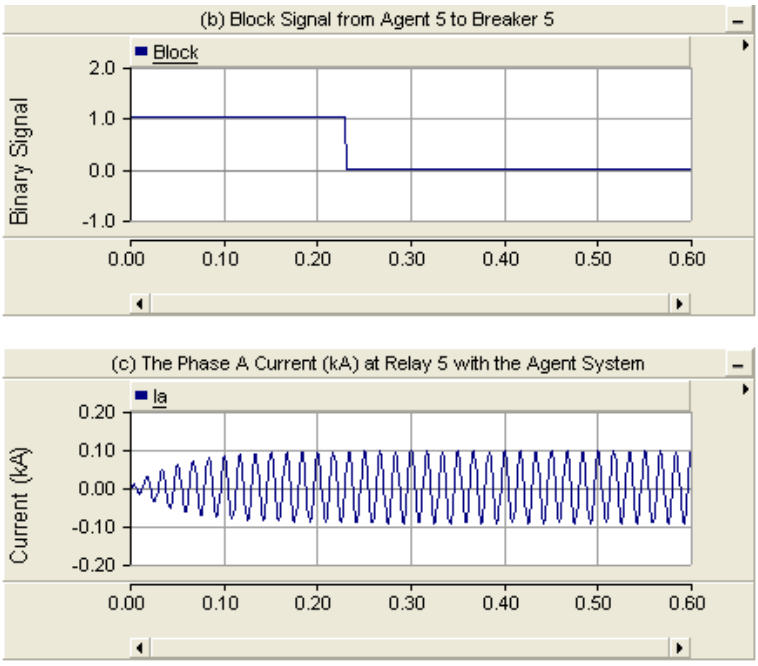

Figure 14. Correct blocking of false trip signal with the trust system. When a false trip signal was sent to Breaker 5 at 0.20 seconds, Agent 5 is rapidly able to block Breaker 5 from tripping using information from trusted agents to ensure the current continued to flow.

4.4 Summary

As discussed in the Chapter II, cyber security measures and improved situational awareness are going to be essential as the grid undergoes modernization. Malicious activity is on the rise and hackers have already demonstrated their ability to access the networks of companies around the world. Because elements of critical infrastructure provide essential services, they become high-priority targets.

The reputation-based trust mechanism proposed by this research has shown its effectiveness in reducing fault clearing times compared to traditional protection mechanisms. These mechanisms need to be prepared to make correct decisions in the face of potential malicious activity. By comparing fault clearing times, the agent-based backup protection systems incorporating the trust component are more effective at providing protection than systems without this component. A summary graph comparing the results of all experiments performed is included as Figure 15 and Figure 16. The experiments showed that trust implementations reduced clearing times below 0.5 seconds under each of the selected scenarios, well below the traditionally established settings of 1 to 2 seconds [24] and [59]. These agent based systems even cleared faults more rapidly that the 0.3 seconds normally associated with zone 2 relays [24] under normal conditions and often even when subjected to malicious behavior.

The suggested implementations should be combined with traditional network security measures and physical security efforts to provide proper defenses. If improperly applied, this enhanced protection has the potential to disrupt time-critical protection

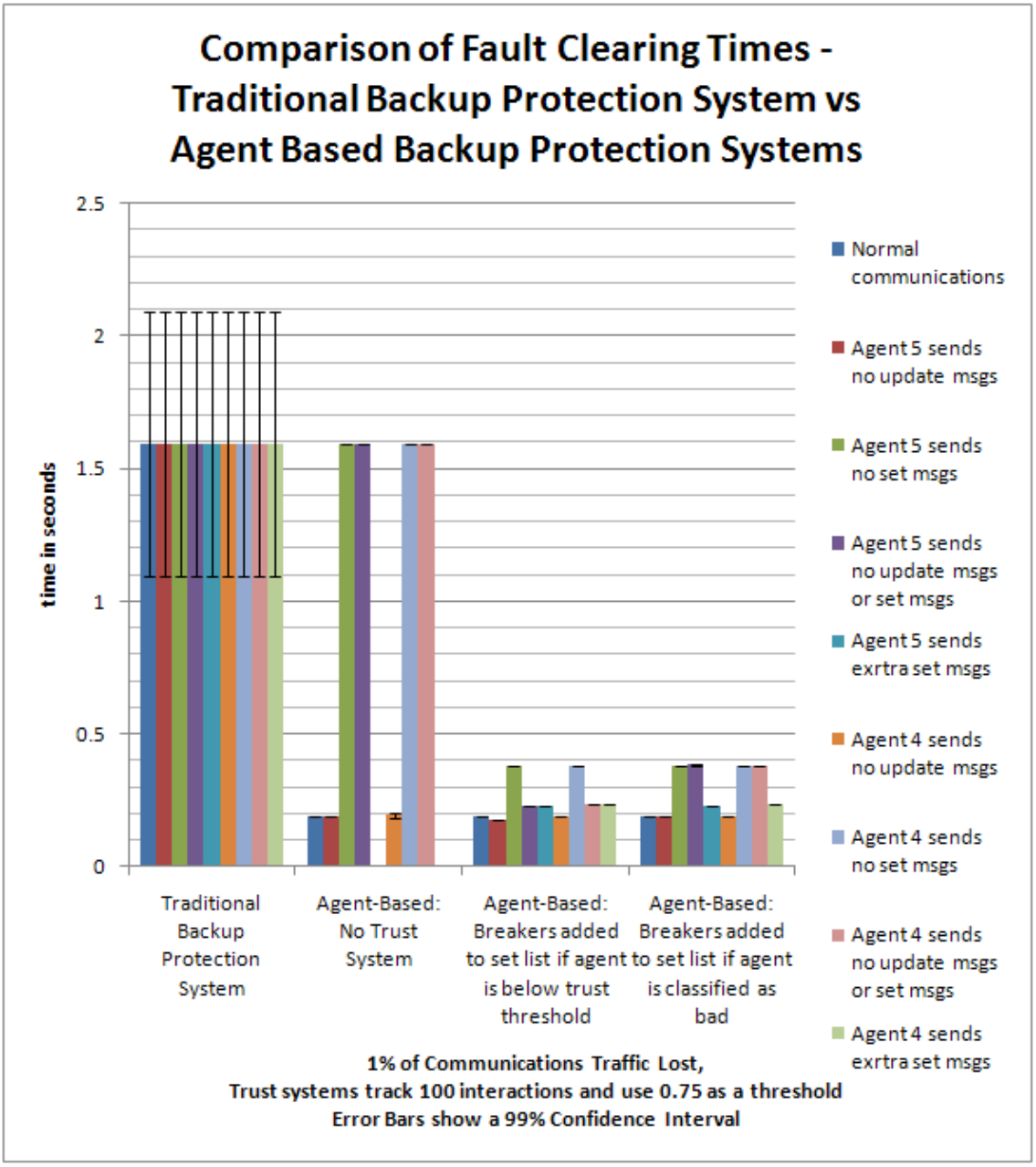

Figure 15. Fault clearing time summary at 1% message traffic loss. For traditional relays fault clearing times were constant, set with a 1.5 second operating time. The original agent-based scheme significantly reduced the clearing time but in certain cases reverted to traditional protection methods or operated incorrectly. The improved agent-based schemes suggested in this research compensated for malicious behavior and cleared the fault in a shorter time period without extending the isolation zone at 1% message traffic loss.

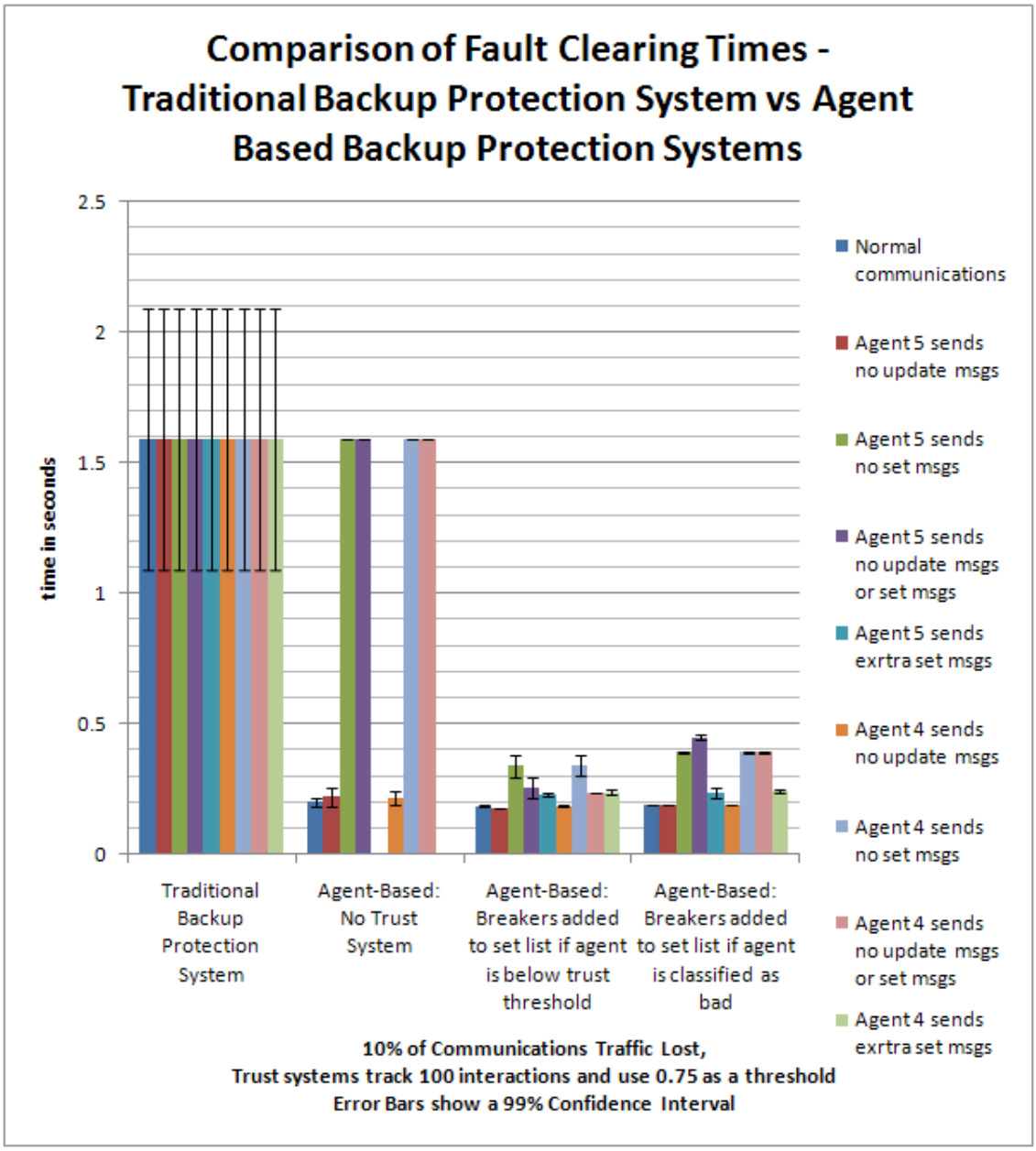

Figure 16. Fault clearing time summary at 10% message traffic loss. For traditional relays fault clearing times were constant, set with a 1.5 second operating time. The original agent-based scheme significantly reduced the clearing time but in certain cases reverted to traditional protection methods or operated incorrectly. The improved agent-based schemes suggested in this research compensated for malicious behavior and cleared the fault in a shorter time period without extending the isolation zone at 10% message traffic loss.

devices by adding delays where none previously existed. While delays are better than interrupted or miscommunications in many instances, in the power grid they are unacceptable. Adding behavioral-based analytic methods for trust metric calculation aids in ensuring information reliability and improves resulting system stability.

Layering an additional collaborative protection scheme as suggested by this research, increased the security of the entire control system. This scheme can make use of existing computing and network resources to provide additional information necessary for making proper protection decisions and improving the situational awareness of control operators. Agents used reputation information as a criterion for judging the trustworthiness of information received during data transactions and will have the ability to send this additional information to control centers for data analysis. This analysis can monitor the protection system for signs indicating a faulty agent or possible larger system attack.

V. Conclusions and Recommendations

THIS thesis investigated the proposal that integrating reputation-based cooperative trust as an additional layer of security for backup protection systems would improve system performance and awareness. The proposed scheme significantly reduced the amount of time required to clear faults when backup protection use was necessary and made a higher percentage of correct decisions compared to the original agent-based scheme that did not include a trust component. As grid modernization continues and more intelligent devices are integrated into the SCADA control systems, incorporating reputation-based trust systems into these devices has the potential to be of great benefit in improving the reliability, stability, and security of this element of our critical infrastructure.

This chapter will first summarize results obtained from the multiple experimental simulations and cover conclusions that can be drawn. Next, it will emphasize why this research needed to be accomplished and how it will impact and change the power control community. Finally, it will cover recommendations for future research topics in this area.

5.1 Conclusions of Research

Initial findings from the reputation-based trust integration with agent-based backup protection are very promising. Even in its simplest implementation, the trust system has the ability to provide additional information to monitoring or control centers while adding little overhead and achieving identical performance to systems that did not implement trust. The additional information captured provides valuable feedback for

evaluating the state of the system and creating improved awareness of networks and component behavior.

The potential for a more robust implementation is even greater and has been demonstrated using the specific scenarios discussed in this research. When faced with malicious behavior that is not stopped with traditional network protection measures, the trust system will account for malicious activity determined by behavioral analysis. The trust system enabled more rapid fault clearing (greater than a 50% improvement) without increasing the isolated grid area to help prevent outages from cascading. Transmission line protection must account for malicious activity such as denial of service and rogue control commands in the future. While a trust-based system will not protect from every type of attack, it has shown to be effective without adding a lot of communications overhead. Layering trust mechanisms with other defensive elements will help architects design more complete grid protection.

5.2 Significance of Research

The incredible power afforded one who is able to affect relay or other switching device behavior results from the direct control that they possess on critical power delivery equipment. These components are located at key junctures that have the potential to affect multitudes of people. They are designed to break a chain of power failures and must act responsively and properly. The additional trust layer is invaluable in limiting the effect an attacker has on this vital equipment.

The Air Force, Department of Defense and other governmental agencies can benefit from this research that applied reputation-based trust in a unique cooperative

environment. Power and other utility networks are increasingly the subject of attack [19], [20], [22], and [56]. Trust systems have the potential to thwart attempts to compromise these systems. Threats to the power grid and other elements of critical infrastructure are likely to occur during times of war preparation such as the mobilization and deployment phases [44]. Interviews and writings in [16] and [31] describe how disruption to information systems and supporting infrastructure could cause delays and backlogs at key logistics locations. Other research [63] focused specifically on attack strategies designed to introduce cascade style effects into the power grid. Improving the reliability and security of the grid protection elements and the underlying communications networks will have a direct impact on the ability of the US armed forces to continue to deploy and rapidly project force where needed anywhere around the globe.

The additional information tracked by the trust system is definitely of benefit in a layered security infrastructure. Trust metrics provides insight about system behavior that was not previously captured. As grid modernization progresses, the behavioral-based analysis that this type of system provides can be similarly implemented in other smart components that connect corporate and control information systems. Regardless of how monitoring and control is accomplished in future SCADA systems, network designers take connectivity information into account and allow control operators to make adaptive adjustments from both environmental conditions and the trust metrics.

5.3 Recommendations for Future Research

A protection system implementing this additional measure of information reliability will realize additional benefits as widely distributed intelligent agents work

together to ensure system stability. Research should continue to develop protection settings tailored for specific applications for further validation. The trust-inclusive, agent-based backup protection system proposed here is a first step towards improving the robustness of agent-based protection and should be incorporated into future protection architectures.

This research has the potential to be expanded in a number of directions. In the future, the first logical step should focus on expanding the decision making capabilities to include scenarios where more than one agent may be malicious. Additional information validation methods will need to be incorporated into the system. The current implementation focused on cross-referencing power system data with locality data to clear the fault in a manner that affects the smallest area should be continued. Creating more complex network topologies will help validate the system's performance when faced with a more interconnected grid structure and ensure actions continue to limit the isolation area. This system has the potential to be incorporated into the electrical grid on a wider basis. Expanding the trust computations to include additional data validation as well as its implementation in more decision scenarios will help create a more robust scheme.

Another step might be to investigate this or an alternate reputation-based trust scheme implemented in conjunction with a policy-based trust scheme such as cryptography. When used together, the system could take advantage of additional layers of security. If the coding is optimized, some of the other distributed aspects of the trust computations such as increased validation using shared trust cookies as discussed in [32]

could be integrated. This combined scheme should improve protection without adding additional network traffic beyond what is required for the cryptographic system. A digitally signed cryptographic token can then be incorporated allowing for distributed cookie storage or trust metric calculations. The more robust implementation can permit additional trust inheritance and global trust value computations while improving message authentication and decreasing the potential for successful message spoofing.

A final direction that future research could take would be to incorporate a reputation-based trust system such as this into other smart devices that will be increasingly used in the next generation grid. Devices will have the potential to be used in demand reduction schemes and would allow end users to be directly wired into the central control scheme. In these schemes it would be more desirable that a device respond appropriately when needed. The time delays associated with cryptographic encoding have less of an impact on system protection since the real-time requirement is less stringent. A trust-based scheme would have the potential to select the most trustworthy devices in these cases to ensure that proper actions could be directed in a timely manner to create the appropriate system effects.

5.4 Summary

Information and cyber security are becoming more essential our critical infrastructure network protection every day. In a recent 60 Minutes interview, the former US Chief of National Intelligence reported, “If I were an attacker… I probably would sack electric power on the U.S. East Coast, maybe the West Coast, and attempt to cause a cascading effect” [1]. Proper relay operation is critical to ensuring that this does not

occur. Without better communications methods and protection schemes, malicious users would be able to create effects that could plunge entire regions into darkness and instigate chaos. Traditional security mechanisms must be augmented by additional measures such as trust verification that provide adaptive protection capabilities for these components that provide an essential service to society.

Appendix A. Experimentation Results By Scenario

Table 6. Performance statistics for Scenario 1 – no malicious behavior. Approximately equal performance for all implementations.
Trust schemes tracked 100 interactions and the trust threshold was set at .75.
Binomial distributions for Sign Test for Median from [37], [50], and [68].
Statistical table information for Wilcoxon signed-rank test verified from [41].
Interpret Wilcoxon Signed Rank Test results in chart as two items (rank score on top, p value on bottom).

Implementation	No trust scheme		Add to set list if below trust threshold		Add to set list only if bad	
% Traffic Lost	1	10	1	10	1	10
Sample Mean (s)	0.188	0.20096	0.18808	0.18544	0.18808	0.18848
Maximum (s)	0.188	0.292	0.19	0.19	0.19	0.19
3rd Quartile (s)	0.188	0.188	0.188	0.188	0.188	0.188
Median (s)	0.188	0.188	0.188	0.188	0.188	0.188
1st Quartile (s)	0.188	0.188	0.188	0.188	0.188	0.188
Minimum (s)	0.188	0.188	0.188	0.176	0.188	0.188
Sample Std Dev	0.00000	0.03173	0.00040	0.00508	0.00040	0.00087
n	25	25	25	25	25	25
Std Error	0.00000	0.00635	0.00008	0.00102	0.00008	0.00017
99.5% Error	0.00000	0.01775	0.00022	0.00284	0.00022	0.00049
99% Confidence Interval Low (s)	0.188	0.18321	0.18786	0.18260	0.18786	0.18799
99% Confidence Interval High (s)	0.188	0.21871	0.18830	0.18828	0.18830	0.18897
# samples > 0.392s	0	0	0	0	0	0
Sign Test Median=0.392s	0.0	0.0	0.0	0.0	0.0	0.0
Wilcoxon Signed Rank Test Median=0.392s	0 0.005	0 0.005	0 0.005	0 0.005	0 0.005	0 0.005
# of samples > 0.592s	0	0	0	0	0	0
Sign Test for Median - 0.592s	0.0	0.0	0.0	0.0	0.0	0.0
Wilcoxon Signed Rank Test Median=0.592	0 0.005	0 0.005	0 0.005	0 0.005	0 0.005	0 0.005

Table 7. Performance statistics for Scenario 2 – Agent 5 does not send response messages. Approximately equal performance for all implementations. Trust schemes tracked 100 interactions and the trust threshold was set at .75. Binomial distributions for Sign Test for Median from [37], [50], and [68]. Statistical table information for Wilcoxon signed-rank test verified from [41]. Interpret Wilcoxon Signed Rank Test results in chart as two items (rank score on top, p value on bottom).

Implementation	No trust scheme		Add to set list if below trust threshold		Add to set list only if bad	
% Traffic Lost	1	10	1	10	1	10
Sample Mean (s)	0.188	0.21904	0.176	0.17736	0.18808	0.18856
Maximum (s)	0.188	0.408	0.176	0.188	0.19	0.19
3rd Quartile (s)	0.188	0.188	0.176	0.178	0.188	0.19
Median (s)	0.188	0.188	0.176	0.176	0.188	0.188
1st Quartile (s)	0.188	0.188	0.176	0.176	0.188	0.188
Minimum (s)	0.188	0.188	0.176	0.176	0.188	0.188
Sample Std Dev	0.00000	0.06180	0.00000	0.00250	0.00040	0.00092
n	25	25	25	25	25	25
Std Error	0.00000	0.01236	0.00000	0.00050	0.00008	0.00018
99.5% Error	0.00000	0.03457	0.00000	0.00140	0.00022	0.00051
99% Confidence Interval Low (s)	0.18800	0.18447	0.17600	0.17596	0.18786	0.18805
99% Confidence Interval High (s)	0.18800	0.25361	0.17600	0.17876	0.18830	0.18907
# samples > 0.392s	0	1	0	0	0	0
Sign Test Median=0.392s	0.0	0.0	0.0	0.0	0.0	0.0
Wilcoxon Signed Rank Test Median=0.392s	0 0.005	1 .005	0 0.005	0 0.005	0 0.005	0 0.005
# of samples > 0.592s	0	0	0	0	0	0
Sign Test for Median - 0.592s	0.0	0.0	0.0	0.0	0.0	0.0
Wilcoxon Signed Rank Test Median=0.592	0 0.005	0 0.005	0 0.005	0 0.005	0 0.005	0 0.005

Table 8. Performance statistics for Scenario 3 – Agent 5 will not send set equipment messages. Trust implementations outperform original agent implementation. Trust schemes tracked 100 interactions and the trust threshold was set at .75. Binomial distributions for Sign Test for Median from [37], [50], and [68]. Statistical table information for Wilcoxon signed-rank test verified from [41]. Interpret Wilcoxon Signed Rank Test results in chart as two items (rank score on top, p value on bottom).

Implementation	No trust scheme		Add to set list if below trust threshold		Add to set list only if bad	
% Traffic Lost	1	10	1	10	1	10
Sample Mean (s)	1.592	1.592	0.3784	0.33856	0.3784	0.39176
Maximum (s)	1.592	1.592	0.382	0.402	0.382	0.402
3rd Quartile (s)	1.592	1.592	0.378	0.396	0.378	0.396
Median (s)	1.592	1.592	0.378	0.39	0.378	0.39
1st Quartile (s)	1.592	1.592	0.378	0.228	0.378	0.388
Minimum (s)	1.592	1.592	0.378	0.226	0.378	0.382
Sample Std Dev	0.00000	0.00000	0.00100	0.07693	0.00100	0.00601
n	25	25	25	25	25	25
Std Error	0.00000	0.00000	0.00020	0.01539	0.00020	0.00120
99.5% Error	0.00000	0.00000	0.00056	0.04303	0.00056	0.00336
99% Confidence Interval Low (s)	1.59200	1.59200	0.37784	0.29553	0.37784	0.38840
99% Confidence Interval High (s)	1.59200	1.59200	0.37896	0.38159	0.37896	0.39512
# samples > 0.392s	25	25	0	10	0	12
Sign Test Median=0.392s	1.0	1.0	0.0	0.2122	0.0	0.5
Wilcoxon Signed Rank Test Median=0.392s	325 unable to reject	325 unable to reject	0 0.005	91 .025 - .05	0 0.005	160 unable to reject
# of samples > 0.592s	25	25	0	0	0	0
Sign Test for Median - 0.592s	1.0	1.0	0.0	0.0	0.0	0.0
Wilcoxon Signed Rank Test Median=0.592	325 unable to reject	325 unable to reject	0 0.005	0 0.005	0 0.005	0 0.005

Table 9. Performance statistics for Scenario 4 – Agent 5 will not send information response or set equipment messages. Trust implementations outperform original agent implementation.

Trust schemes tracked 100 interactions and the trust threshold was set at .75.

Binomial distributions for Sign Test for Median from [37], [50], and [68].

Statistical table information for Wilcoxon signed-rank test verified from [41].

Interpret Wilcoxon Signed Rank Test results in chart as two items (rank score on top, p value on bottom).

Implementation	No trust scheme		Add to set list if below trust threshold		Add to set list only if bad	
% Traffic Lost	1	10	1	10	1	10
Sample Mean (s)	1.592	1.592	0.22608	0.25304	0.38408	0.44888
Maximum (s)	1.592	1.592	0.228	0.454	0.394	0.5
3rd Quartile (s)	1.592	1.592	0.226	0.228	0.386	0.456
Median (s)	1.592	1.592	0.226	0.226	0.384	0.448
1st Quartile (s)	1.592	1.592	0.226	0.226	0.382	0.44
Minimum (s)	1.592	1.592	0.226	0.226	0.378	0.414
Sample Std Dev	0.00000	0.00000	0.00040	0.07253	0.00363	0.01776
n	25	25	25	25	25	25
Std Error	0.00000	0.00000	0.00008	0.01451	0.00073	0.00355
99.5% Error	0.00000	0.00000	0.00022	0.04057	0.00203	0.00993
99% Confidence Interval Low (s)	1.59200	1.59200	0.22586	0.21247	0.38205	0.43895
99% Confidence Interval High (s)	1.59200	1.59200	0.22630	0.29361	0.38611	0.45881
# samples > 0.392s	25	25	0	3	1	25
Sign Test Median=0.392s	1.0	1.0	0.0	0.0001	0.0	1.0
Wilcoxon Signed Rank Test Median=0.392s	325 unable to reject	325 unable to reject	0 0.005	6 0.005	1 0.005	325 unable to reject
# of samples > 0.592s	25	25	0	0	0	0
Sign Test for Median - 0.592s	1.0	1.0	0.0	0.0	0.0	0.0
Wilcoxon Signed Rank Test Median=0.592	325 unable to reject	325 unable to reject	0 0.005	0 0.005	0 0.005	0 0.005

Table 10. Performance statistics for Scenario 5 – Agent 5 sends false set equipment messages. Trust implementations outperform original agent implementation. Original implementation tripped without valid fault condition.
Trust schemes tracked 100 interactions and the trust threshold was set at .75.
Binomial distributions for Sign Test for Median from [37], [50], and [68].
Statistical table information for Wilcoxon signed-rank test verified from [41].
Interpret Wilcoxon Signed Rank Test results in chart as two items (rank score on top, p value on bottom).

Implementation	No trust scheme		Add to set list if below trust threshold		Add to set list only if bad	
% Traffic Lost	1	10	1	10	1	10
Sample Mean (s)	n/a	n/a	0.22608	0.22864	0.22608	0.23512
Maximum (s)	n/a	n/a	0.228	0.284	0.228	0.39
3rd Quartile (s)	n/a	n/a	0.226	0.226	0.226	0.226
Median (s)	n/a	n/a	0.226	0.226	0.226	0.226
1st Quartile (s)	n/a	n/a	0.226	0.226	0.226	0.226
Minimum (s)	n/a	n/a	0.226	0.226	0.226	0.226
Sample Std Dev	n/a	n/a	0.00040	0.01156	0.00040	0.03427
n	25	25	25	25	25	25
Std Error	n/a	n/a	0.00008	0.00231	0.00008	0.00685
99.5% Error	n/a	n/a	0.00022	0.00647	0.00022	0.01917
99% Confidence Interval Low (s)	n/a	n/a	0.22586	0.22217	0.22586	0.21595
99% Confidence Interval High (s)	n/a	n/a	0.22630	0.23511	0.22630	0.25429
# samples > 0.392s	n/a	n/a	0	0	0	0
Sign Test Median=0.392s	n/a	n/a	0.0	0.0	0.0	0.0
Wilcoxon Signed Rank Test Median=0.392s	n/a	n/a	0 0.005	0 0.005	0 0.005	0 0.005
# of samples > 0.592s	n/a	n/a	0	0	0	0
Sign Test for Median - 0.592s	n/a	n/a	0.0	0.0	0.0	0.0
Wilcoxon Signed Rank Test Median=0.592	n/a	n/a	0 0.005	0 0.005	0 0.005	0 0.005

Table 11. Performance statistics for Scenario 6 – Agent 4 does not send response messages. Approximately equal performance for all implementations. Trust schemes tracked 100 interactions and the trust threshold was set at .75. Binomial distributions for Sign Test for Median from [37], [50], and [68]. Statistical table information for Wilcoxon signed-rank test verified from [41]. Interpret Wilcoxon Signed Rank Test results in chart as two items (rank score on top, p value on bottom).

Implementation	No trust scheme		Add to set list if below trust threshold		Add to set list only if bad	
% Traffic Lost	1	10	1	10	1	10
Sample Mean (s)	0.19216	0.21624	0.188	0.186	0.188	0.18872
Maximum (s)	0.292	0.396	0.188	0.192	0.188	0.19
3rd Quartile (s)	0.188	0.246	0.188	0.19	0.188	0.19
Median (s)	0.188	0.188	0.188	0.188	0.188	0.188
1st Quartile (s)	0.188	0.188	0.188	0.188	0.188	0.188
Minimum (s)	0.188	0.188	0.188	0.176	0.188	0.188
Sample Std Dev	0.02080	0.05074	0.00000	0.00548	0.00000	0.00098
n	25	25	25	25	25	25
Std Error	0.00416	0.01015	0.00000	0.00110	0.00000	0.00020
99.5% Error	0.01164	0.02838	0.00000	0.00306	0.00000	0.00055
99% Confidence Interval Low (s)	0.18052	0.18786	0.18800	0.18294	0.18800	0.18817
99% Confidence Interval High (s)	0.20380	0.24462	0.18800	0.18906	0.18800	0.18927
# samples > 0.392s	0	1	0	0	0	0
Sign Test Median=0.392s	0.0	0.0	0.0	0.0	0.0	0.0
Wilcoxon Signed Rank Test Median=0.392s	0 0.005	1 0.005	0 0.005	0 0.005	0 0.005	0 0.005
# of samples > 0.592s	0	0	0	0	0	0
Sign Test for Median - 0.592s	0.0	0.0	0.0	0.0	0.0	0.0
Wilcoxon Signed Rank Test Median=0.592s	0 0.005	0 0.005	0 0.005	0 0.005	0 0.005	0 0.005

Table 12. Performance statistics for Scenario 7 – Agent 4 does not send set equipment messages. Trust implementations outperform original implementation. Trust schemes tracked 100 interactions and the trust threshold was set at .75. Binomial distributions for Sign Test for Median from [37], [50], and [68]. Statistical table information for Wilcoxon signed-rank test verified from [41]. Interpret Wilcoxon Signed Rank Test results in chart as two items (rank score on top, p value on bottom).

Implementation	No trust scheme		Add to set list if below trust threshold		Add to set list only if bad	
% Traffic Lost	1	10	1	10	1	10
Sample Mean (s)	1.592	1.592	0.3784	0.342	0.3784	0.38992
Maximum (s)	1.592	1.592	0.382	0.4	0.382	0.402
3rd Quartile (s)	1.592	1.592	0.378	0.394	0.378	0.394
Median (s)	1.592	1.592	0.378	0.388	0.378	0.388
1st Quartile (s)	1.592	1.592	0.378	0.288	0.378	0.386
Minimum (s)	1.592	1.592	0.378	0.226	0.378	0.378
Sample Std Dev	0.00000	0.00000	0.00100	0.06811	0.00100	0.00593
n	25	25	25	25	25	25
Std Error	0.00000	0.00000	0.00020	0.01362	0.00020	0.00119
99.5% Error	0.00000	0.00000	0.00056	0.03810	0.00056	0.00332
99% Confidence Interval Low (s)	1.59200	1.59200	0.37784	0.30390	0.37784	0.38660
99% Confidence Interval High (s)	1.59200	1.59200	0.37896	0.38010	0.37896	0.39324
# samples > 0.392s	25	25	0	9	0	9
Sign Test Median=0.392s	1.0	1.0	0.0	0.1148	0.0	0.1148
Wilcoxon Signed Rank Test Median=0.392s	325 unable to reject	325 unable to reject	0 0.005	60.5 0.005	0 0.005	97 .025 – 0.05
# of samples > 0.592s	25	25	0	0	0	0
Sign Test for Median - 0.592s	1.0	1.0	0.0	0.0	0.0	0.0
Wilcoxon Signed Rank Test Median=0.592	325 unable to reject	325 unable to reject	0 0.005	0 0.005	0 0.005	0 0.005

Table 13. Performance statistics for Scenario 8 – Agent 4 does not send response or set equipment messages. Trust implementations outperform original implementation.

Trust schemes tracked 100 interactions and the trust threshold was set at .75.

Binomial distributions for Sign Test for Median from [37], [50], and [68].

Statistical table information for Wilcoxon signed-rank test verified from [41].

Interpret Wilcoxon Signed Rank Test results in chart as two items (rank score on top, p value on bottom).

Implementation	No trust scheme		Add to set list if below trust threshold		Add to set list only if bad	
% Traffic Lost	1	10	1	10	1	10
Sample Mean (s)	1.592	1.592	0.238	0.2356	0.37848	0.39064
Maximum (s)	1.592	1.592	0.238	0.24	0.38	0.408
3rd Quartile (s)	1.592	1.592	0.238	0.238	0.378	0.394
Median (s)	1.592	1.592	0.238	0.238	0.378	0.39
1st Quartile (s)	1.592	1.592	0.238	0.238	0.378	0.386
Minimum (s)	1.592	1.592	0.238	0.226	0.378	0.382
Sample Std Dev	0.00000	0.00000	0.00000	0.00500	0.00087	0.00610
n	25	25	25	25	25	25
Std Error	0.00000	0.00000	0.00000	0.00100	0.00017	0.00122
99.5% Error	0.00000	0.00000	0.00000	0.00280	0.00049	0.00341
99% Confidence Interval Low (s)	1.59200	1.59200	0.23800	0.23280	0.37799	0.38723
99% Confidence Interval High (s)	1.59200	1.59200	0.23800	0.23840	0.37897	0.39405
# samples > 0.392s	25	25	0	0	0	11
Sign Test Median=0.392s	1.0	1.0	0.0	0.0	0.0	.345
Wilcoxon Signed Rank Test Median=0.392s	325 unable to reject	325 unable to reject	0 0.005	0 0.005	0 0.005	112.5 unable to reject
# of samples > 0.592s	25	25	0	0	0	0
Sign Test for Median - 0.592s	1.0	1.0	0.0	0.0	0.0	0.0
Wilcoxon Signed Rank Test Median=0.592	325 unable to reject	325 unable to reject	0 0.005	0 0.005	0 0.005	0 0.005

Table 14. Performance statistics for Scenario 9 – Agent 4 sends false set equipment messages. Trust implementations outperform original implementation. Original implementation trips breaker without valid fault conditions.
Trust schemes tracked 100 interactions and the trust threshold was set at .75.
Binomial distributions for Sign Test for Median from [37], [50], and [68].
Statistical table information for Wilcoxon signed-rank test verified from [41].
Interpret Wilcoxon Signed Rank Test results in chart as two items (rank score on top, p value on bottom).

Implementation	No trust scheme		Add to set list if below trust threshold		Add to set list only if bad	
% Traffic Lost	1	10	1	10	1	10
Sample Mean (s)	n/a	n/a	0.238	0.23816	0.238	0.24072
Maximum (s)	n/a	n/a	0.238	0.296	0.238	0.296
3rd Quartile (s)	n/a	n/a	0.238	0.238	0.238	0.238
Median (s)	n/a	n/a	0.238	0.238	0.238	0.238
1st Quartile (s)	n/a	n/a	0.238	0.238	0.238	0.238
Minimum (s)	n/a	n/a	0.238	0.226	0.238	0.238
Sample Std Dev	n/a	n/a	0.00000	0.01299	0.00000	0.01155
n	25	25	25	25	25	25
Std Error	n/a	n/a	0.00000	0.00260	0.00000	0.00231
99.5% Error	n/a	n/a	0.00000	0.00726	0.00000	0.00646
99% Confidence Interval Low (s)	n/a	n/a	0.23800	0.23090	0.23800	0.23426
99% Confidence Interval High (s)	n/a	n/a	0.23800	0.24542	0.23800	0.24718
# samples > 0.392s	n/a	n/a	0	0	0	0
Sign Test Median=0.392s	n/a	n/a	0.0	0.0	0.0	0.0
Wilcoxon Signed Rank Test Median=0.392s	n/a	n/a	0 0.005	0 0.005	0 0.005	0 0.005
# of samples > 0.592s	n/a	n/a	0	0	0	0
Sign Test for Median - 0.592s	n/a	n/a	0.0	0.0	0.0	0.0
Wilcoxon Signed Rank Test Median=0.592	n/a	n/a	0 0.005	0 0.005	0 0.005	0 0.005

Appendix B. Performance Charts for Data by Scenario

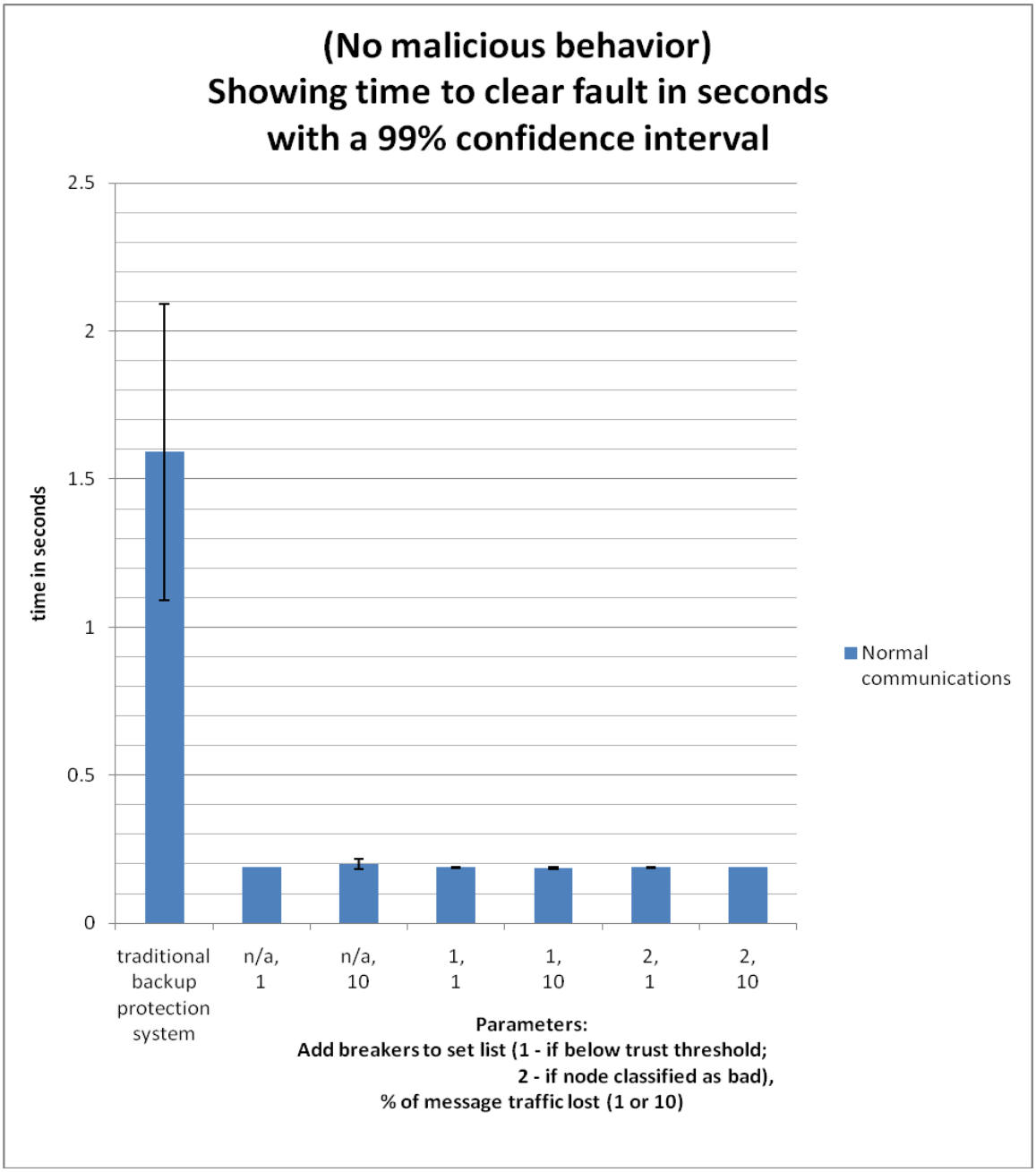

Figure 17. Fault clearing times for Scenario 1, no malicious behavior. Approximately equal performance for all implementations under normal circumstances.
n/a – signifies original agent scheme with no trust component.
Trust schemes track 100 interactions and trust threshold set at 0.75.

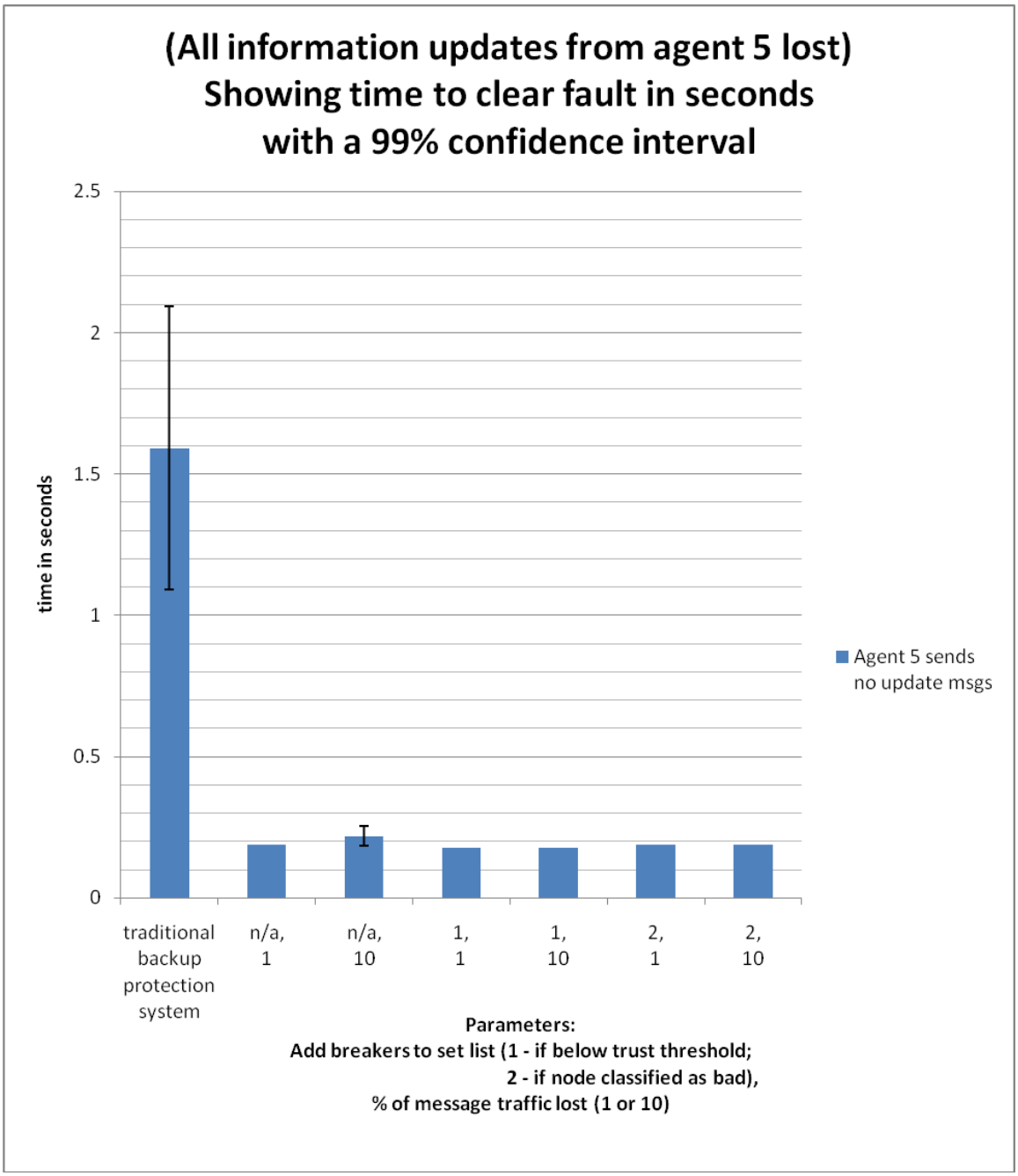

Figure 18. Fault clearing times for Scenario 2, Agent 5 sends no response messages. Approximately equal performance for all agent implementations.
n/a – signifies original agent scheme with no trust component.
Trust schemes track 100 interactions and trust threshold set at 0.75.

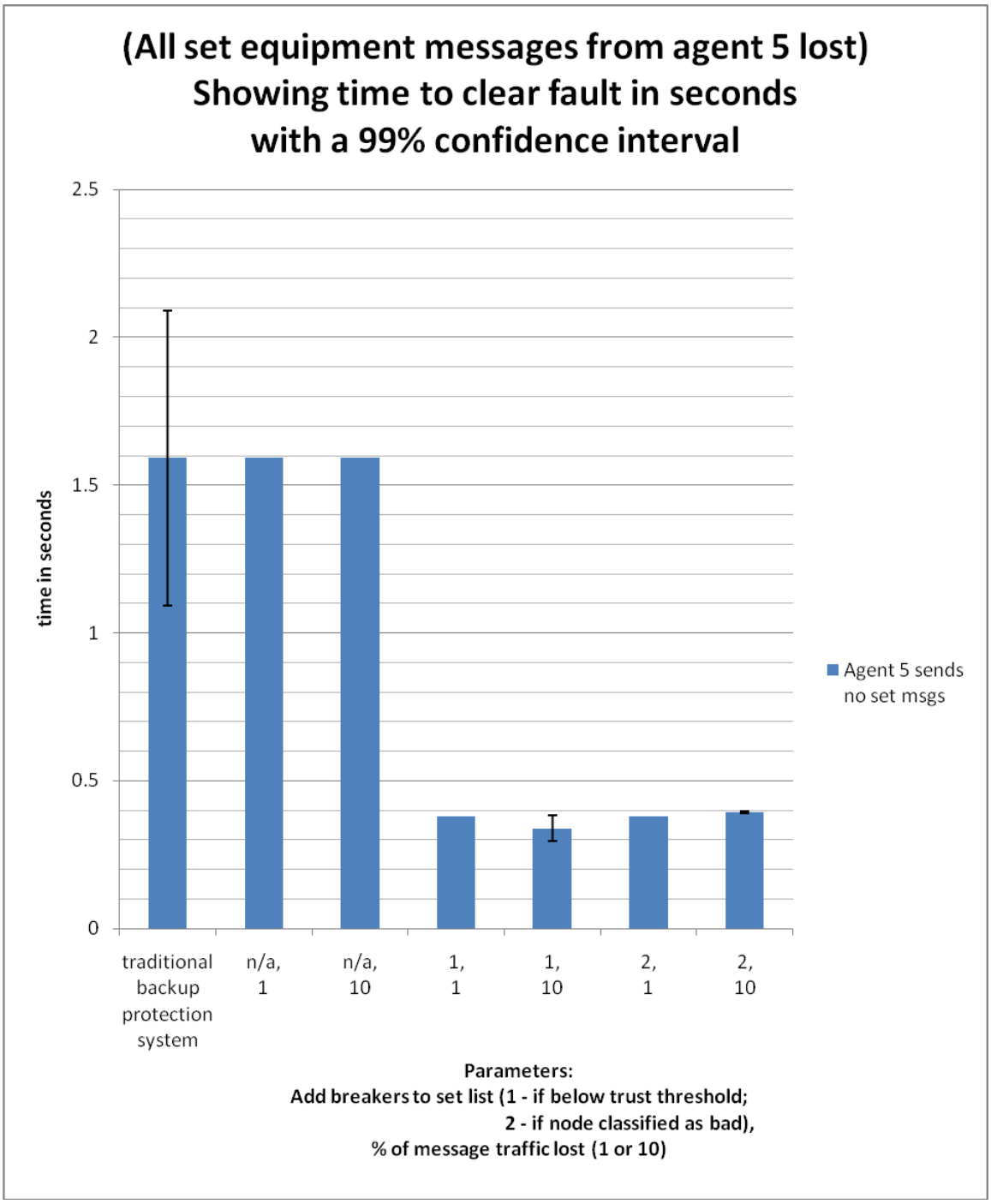

Figure 19. Fault clearing times for Scenario 3, Agent 5 sends no set equipment messages.
Trust system outperforms original agent implementation.
n/a – signifies original agent scheme with no trust component.
Trust schemes track 100 interactions and trust threshold set at 0.75.

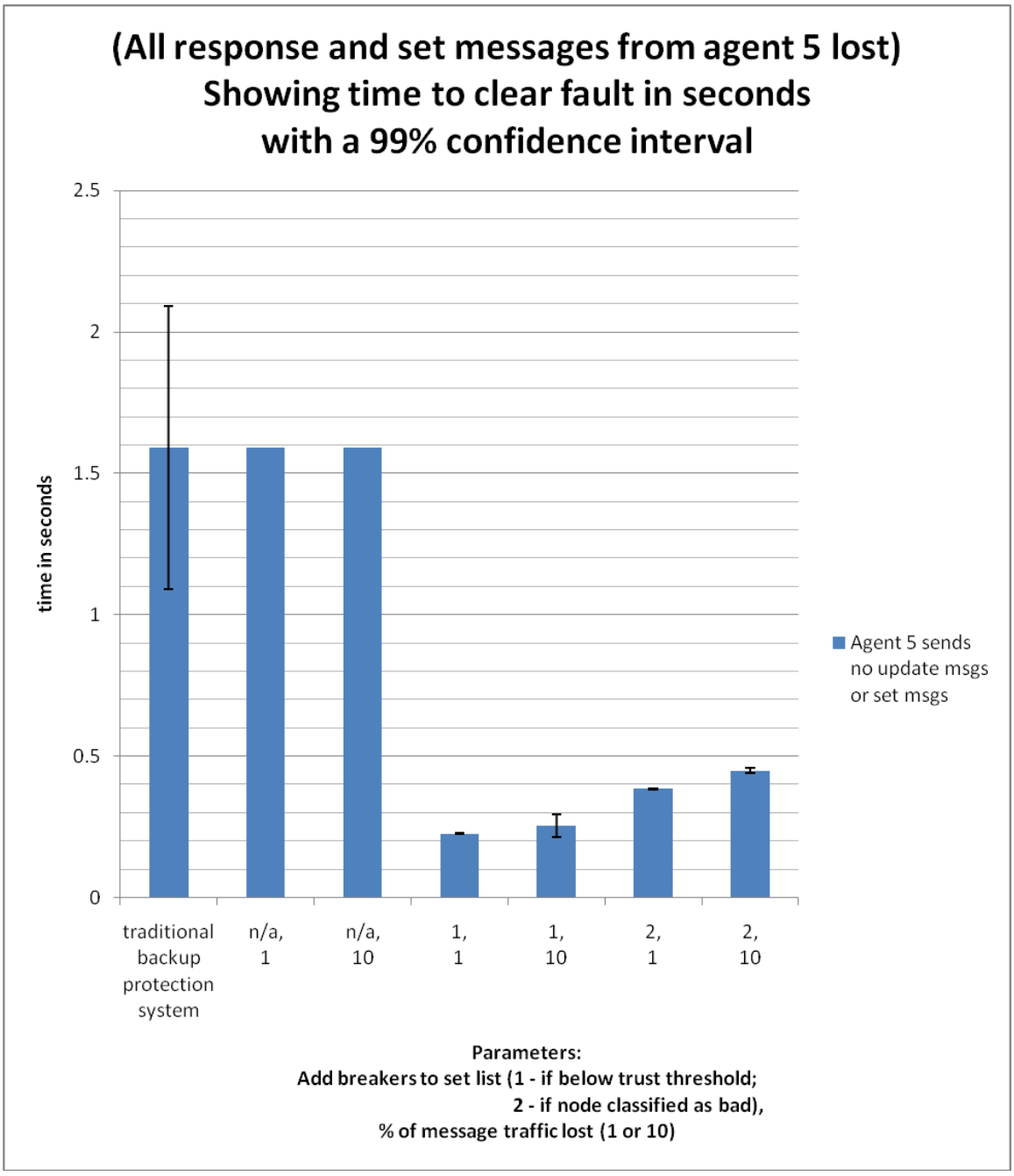

Figure 20. Fault clearing times for Scenario 4, Agent 5 sends no response or set equipment messages. Trust system outperforms original agent implementation.

n/a – signifies original agent scheme with no trust component.

Trust schemes track 100 interactions and trust threshold set at 0.75.

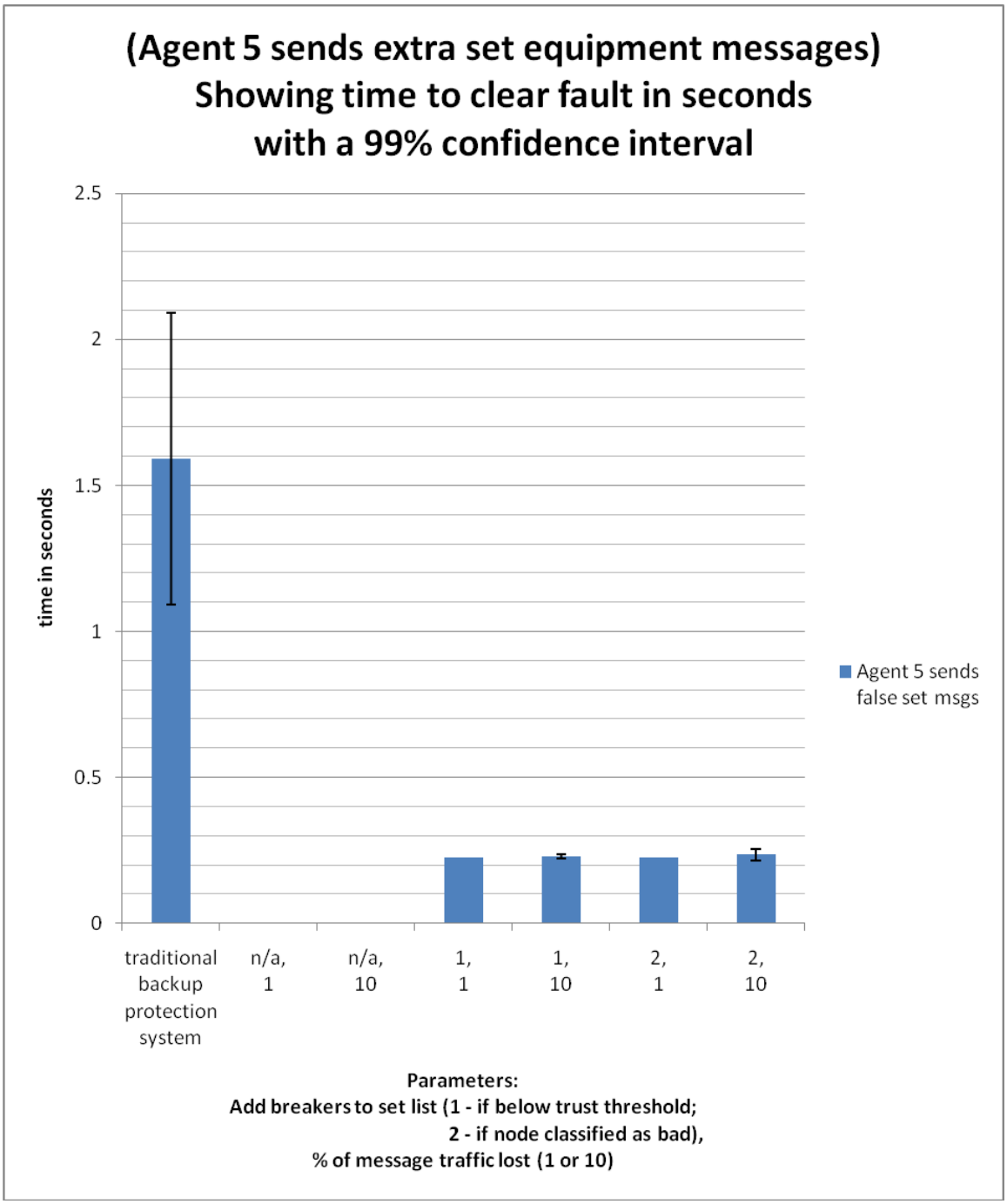

Figure 21. Fault clearing times for Scenario 5, Agent 5 sends false set equipment messages. Trust system outperforms original agent implementation. Original implementation tripped prior without actual fault.
n/a – signifies original agent scheme with no trust component.
Trust schemes track 100 interactions and trust threshold set at 0.75.

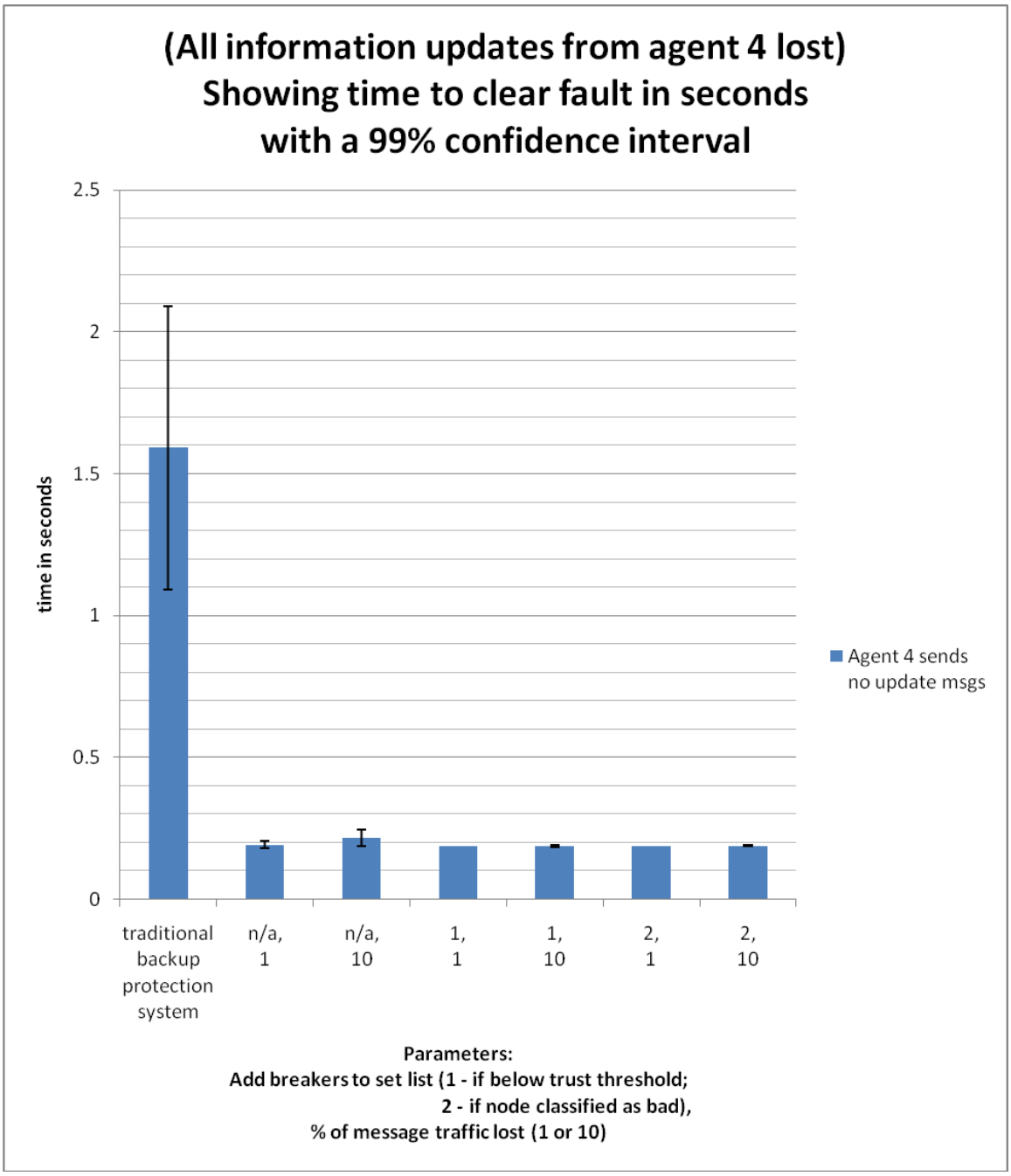

Figure 22. Fault clearing times for Scenario 6, Agent 4 sends no response messages. Approximately equal performance for all agent implementations.
n/a – signifies original agent scheme with no trust component.
Trust schemes track 100 interactions and trust threshold set at 0.75.

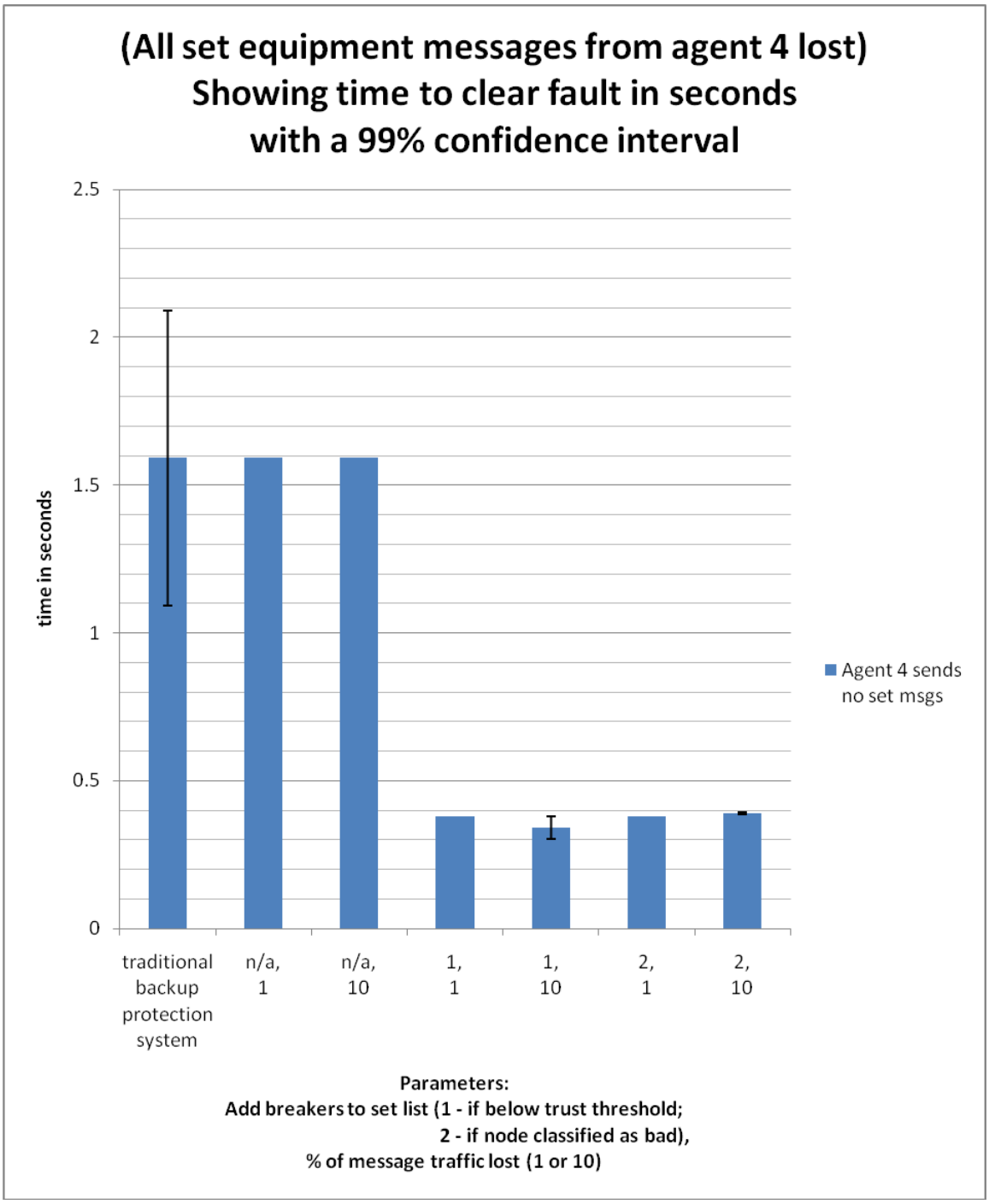

Figure 23. Fault clearing times for Scenario 7, Agent 4 sends no set equipment messages.
Trust system outperforms original agent implementation.
n/a – signifies original agent scheme with no trust component.
Trust schemes track 100 interactions and trust threshold set at 0.75.

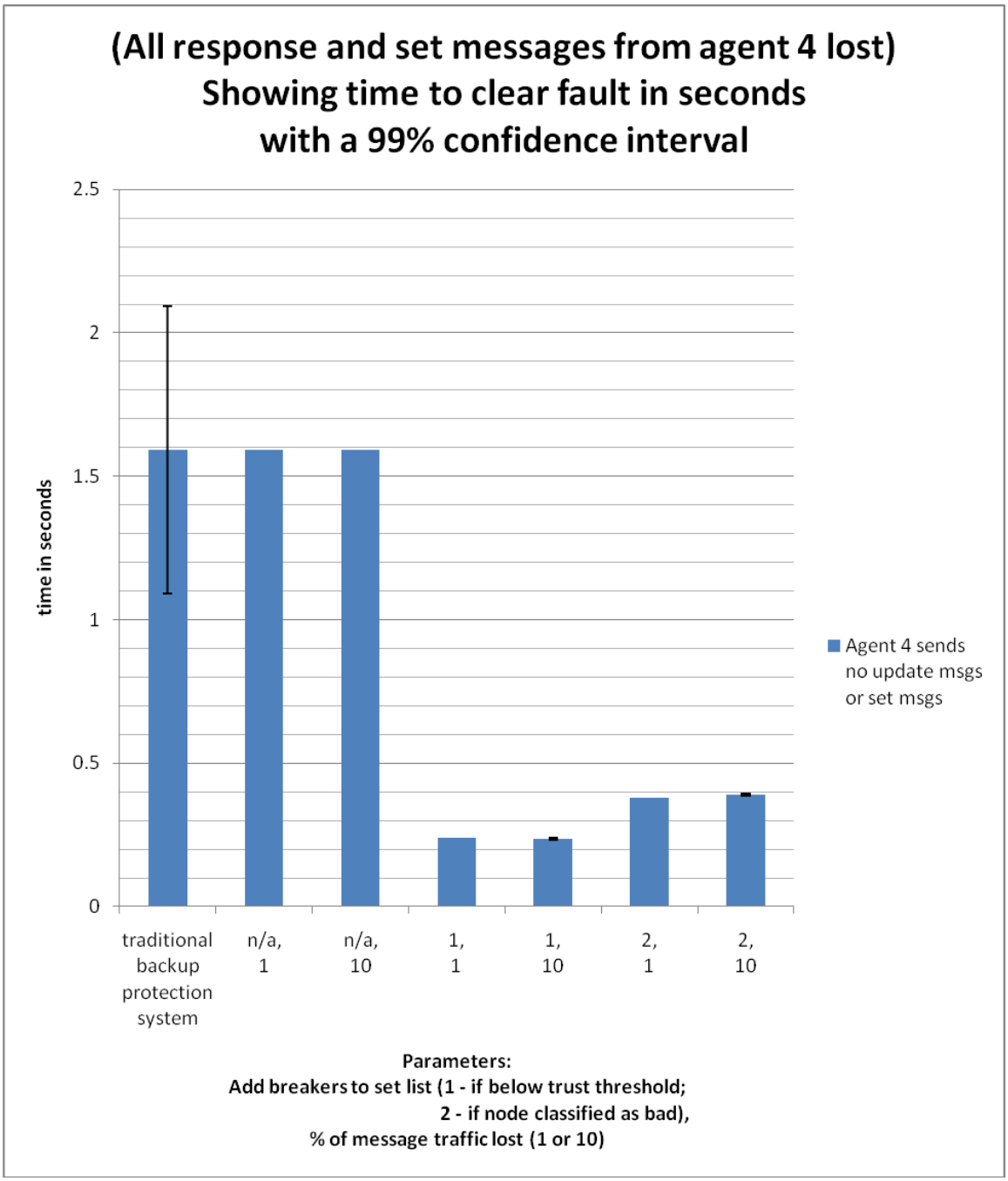

Figure 24. Fault clearing times for Scenario 8, Agent 4 sends no response or set equipment messages. Trust system outperforms the original agent implementation.

n/a – signifies original agent scheme with no trust component.

Trust schemes track 100 interactions and trust threshold set at 0.75.

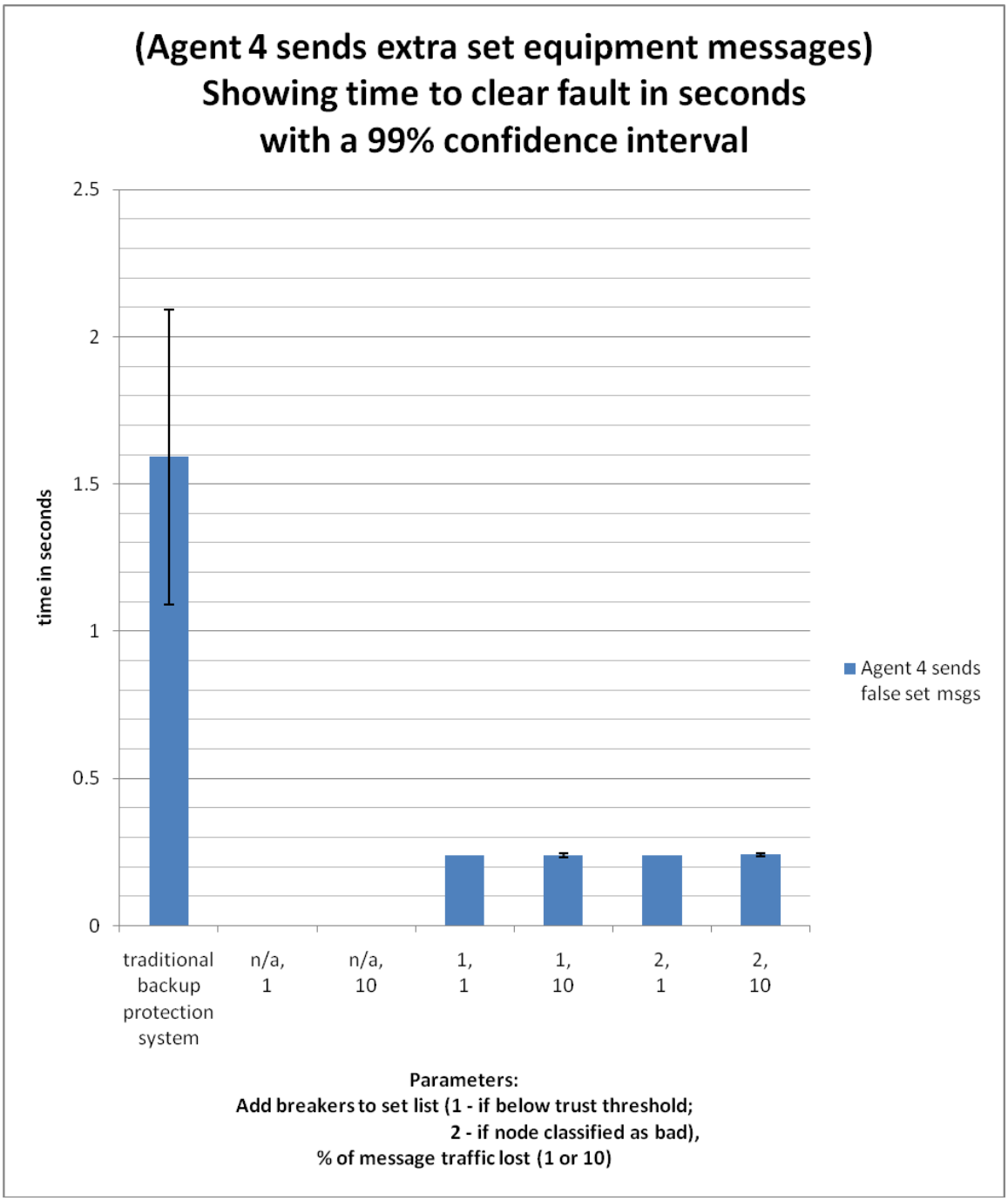

Figure 25. Fault clearing times for Scenario 9, Agent 4 sends false set equipment messages. Trust system outperforms original agent implementation. Original implementation tripped without actual fault.
n/a – signifies original agent scheme with no trust component.
Trust schemes track 100 interactions and trust threshold set at 0.75.

Appendix C. Agent Action and Trust Calculation Pseudocode

Agent Interaction Pseudocode: This pseudocode guides agent behavior between time synchronization events. It covers the general events an agent might encounter and how it adjusts trust metrics for another agent.

Require: PSCAD simulator and agent server and clients to be synchronized in time

Agent/PSCAD information update
- Agent obtains local PSCAD power readings (Voltage and Current for 3 phases)
- Agent obtains local fault detection results (zone 1 and zone 3 coverage zones)
- Agent obtains local equipment status (breaker settings)

Agent action period
- Check local response messages as they arrive
  - Update trust metrics
  - Check for/verify faults in zone 1, zone 3 and in opposite direction
- Trip breaker if fault exists in zone 3 and not cleared by primary agents
- Process all stored messages
  - Respond to all information queries
  - Process all set equipment requests
    - If from 1-hop neighbor and fault is verified – trip breaker
    - If from 2-hop neighbor, fault is verified
      - If 1-hop neighbor did not clear fault – trip breaker
  - Ensure data from response messages updates local view of system
- Send information queries to appropriate agents
- Check/update trust values and cross reference information
- If you observe zone 1 fault and verified
  - Send set equipment to neighbor sharing protection
- Resend any necessary set equipment messages for redundancy
- Verify success or failure of breaker trips
- Block local trips if fault conditions not verified by any trusted agent

Prepare for time resynchronization

Trust Interaction Pseudocode: This pseudocode guides trust structure development and demonstrates general trust computations

Create a trust history used for quick lookup of trust metrics in the local storage implementation

Create a trust store to track trust cookies for each node
- Create a trust cookie for each node to track behavior

Update trust cookie and history each time a query message is sent
- Increment query and response queue counters and place correct value in the query queue

Update trust cookie and history each time a response message is received
- Place correct value in the response queue
- Check contents of response vs observed conditions and override trust metric if necessary

Update trust cookie and history each time a set equipment message is received
- Check contents of set equipment message vs conditions and override trust metric if necessary

Bibliography

1. *60 Minutes; Cyber War: Sabotaging the System*. Prod. Graham Messick. CBS, 8 Nov 09. 13 Nov 09 http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml.

2. 110th US Congress. *Energy Independence and Security Act of 2007*. 4 Jan 2007. 11 Nov 09 http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:h6enr.txt.pdf.

3. Anderson, P. M. *Power System Protection*. Hoboken NJ: Wiley-Interscience, 1999.

4. Anjum, Farooq, Moncef Elaoud, David Famolari, Abhrajit Ghosh, Ravichander Vaidyanathan, Ashutosh Dutta, Prathima Agrawal, Toshikazu Kodama, and Yasuhiro Katsube. "Voice Performance in WLAN Networks—An Experimental Study," Paper presented at the *GLOBECOM '03. IEEE Global Telecommunications Conference (IEEE Cat. no.03CH37489)*, (2003).

5. Artz, Donovan and Yolanda Gil. "A Survey of Trust in Computer Science and the Semantic Web," *Journal of Web Semantics: Science, Service and Agents on the World Wide Web* (15 Mar 07). 30 Dec 09 http://www.isi.edu/~gil/papers/jws-trust-07.pdf.

6. Barnes Ken and Briam Johnson. "Introduction to SCADA Protection and Vulnerabilities," *Idaho National Engineering and Environmental Laboratory*, (March 2004). 10 Jan 10 http://www.inl.gov/technicalpublications/Documents/3310860.pdf

7. Blackburn, J. Lewis and Thomas J. Domin. *Protective Relaying: Principles and Applications, Third Edition.* Boca Raton FL: CRC Press, 2007.

8. Breslau, Lee., Deborah Estrin, Kevin Fall, Sally Floyd, John Heidermann, Ahmed Helmy, Poly Huang, Steven McCanne, Kannan Varadhan, Ya Xu, and Haobo Yu. "Advances in Network Simulation", *IEEE Computer*, 33: 59-67 (May 2000).

9. Bush, George W. *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Washington DC: The White House, February 2003.

10. Bush, George W. *National Strategy to Secure Cyberspace*. Washington DC: The White House, February 2003.

11. Calderaro,V., V. Galdi, A. Piccolo, and P. Siano. "Adaptive relays for overhead line protection," *Electric Power Systems Research*, 77: 1552-1559 (October 2007).

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

13. Clinton,William J. *Presidential Decision Directive/NSC-63*. Washington DC: The White House, 22 May 98. 4 Jan 10 http://www.fas.org/irp/offdocs/pdd/pdd-63.htm.

14. Coates, Gregory M., Kenneth M. Hopkinson, Scott R. Graham, and Stuart H. Kurkowski. "Collaborative, Trust-Based Security Mechanisms for a Regional Utility Intranet," *IEEE Transactions on Power Systems*, 23: 831-844, (Aug. 2008).

15. Funasaka, Junichi, Yusuke Takemoto, and Kenji Ishida. "Parallel Downloading Method using HTTP over UDP for High Loss Rate and Delay Networks," *Proceedings of the Eighth International Symposium on Autonomous Decentrlized Systems*, 555-561 (2007). 10 Jan 10 http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=04144715.

16. Gannon, John C., Assistant Director of Central Intelligence for Analysis and Protection. "National Intelligence Council: Perspective on the Cyberthreat." Address to the National Security Telecommunications and Information Systems Security Committee. (3 Apr 01). 10 Jan 10 http://www.dni.gov/nic/speeches_telecommunications.html.

17. Giovanini, Renan, Kenneth Hopkinson, Denis V. Coury, and James S. Thorp. "A Primary and Backup Cooperative Protection System Based on Wide Area Agents," *IEEE Transactions on Power Delivery*, 21: 1222-1230, (July 2006).

18. Goodman, Seymour E. and Herbert S. Lin, eds. *Toward a Safer and More Secure Cyberspace*. Committee on Improving Cybersecurity Research in the United States, National Research Council. Washington DC: The National Academies Press, 2007.

19. Gorman, Siobhan. "Electricity Grid in US Penetrated by Spies," *The Wall Street Journal Online*, (8 Apr 09). 26 Oct 09 http://online.wsj.com/article/SB123914805204099085.html.

20. Harris, Shane. "China's Cyber-Militia," *National Journal Magazine*, (31 May 08). 10 Jan 10 http://www.nationaljournal.com/njmagazine/cs_10080531_6948.php.

21. He, Eric, Jason Leight, Oliver Yu, and Thomas DeFanti. "Reliable Blast UDP: Predictable High Performance Bulk Data Transfer," *IEEE Cluster Computing* (2002). 10 Jan 10 http://www.evl.uic.edu/cavern/papers/cluster2002.pdf.

22. Holland, Steve and Randall Mikkelsen. "UPDATE 2 – US Concerned Power Grid Vulnerable to Cyber-attack," *Reuters*, (8 Apr 09). 10 Jan 10 http://www.reuters.com/article/idUSN0853911920090408.

23. Hopkinson, Kenneth, Xiaoru Wang, Renan Giovanini, James Thorp, Kenneth Birman, and Denis Coury. "EPOCHS: a platform for agent-based electric power and communication simulation built from commercial off-the-shelf components," *IEEE Transactions on Power Systems*, 21: 548-558, (May 2006).

24. Horowitz, Stanley H. and Arun G. Phadke. *Power System Relaying*. England: Wiley, 2008.

25. Igure, Vinay M., Sean A. Laughter, and Ronald D. Williams. "Security Issues in SCADA Networks," *Computers & Security*, 25: 498-506, (Oct 2006).

26. James, J. H., Chen, Bing, and Laurie Garrison. "Implementing VoIP: A Voice Transmission Performance Progress Report," *IEEE Communications Magazine*, 36-41 (Jul 2004). 11 Jan 10 http://www.viskan.net/material/articles/2004_IEEE_VoIP_Transmission_Performance.pdf.

27. Josang, Audun, and Jennifer Golbeck. "Challenges for Robust Trust and Reputation Systems," In 5th International Workshop on Security and Trust Management (STM 2009), Saint Malo, France, September 2009. 24 Feb 10 http://persons.unik.no/josang/papers/JG2009-STM.pdf.

28. Kamvar, Sepandar D., Mario T. Schlosser., and Hector Garcia-Molina. "The Eigentrust algorithm for reputation management in P2P networks," In *Proceedings of the 12th International Conference on World Wide Web*, 640-651. Budapest, Hungary, May 20 - 24, 2003.

29. Kessler, Gary C. "An Overview of Steganography for the Computer Forensics Examiner," *Forensic Science Communications*, 6: 1-27, (2004).

30. Kimbark, Edward W. *Power System Stability*. Wiley-IEEE Press, March 1995.

31. Krekel, Bryan. "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," *The US-China Economic and Security Review Commission*, Northrop Grumman Corp, (9 Oct 09). 10 Jan 10 http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20report_16Oct2009.pdf.

32. Lee, Seungjoon, Rob Sherwood, and Bobby Bhattacharjee. "Cooperative peer groups in NICE," *Computer Networks*, 50: 523-544 (15 Mar 06).

33. Li, Huaizhi and Mukesh Singhal. "Trust Management in Distributed Systems," *Computer*, 45-53 (Feb 2007).

34. Manitoba HVDC Research Centre Inc. *User's Guide: A Comprehensive Resource for EMTDC (Transient Analysis for PSCAD Power System Simulation)*. 2005. 13 Nov 09 https://pscad.com/resource/File/PSCADV421Student/EMTDC_Users_Guide_V4.2.pdf.

35. Marsh, Stephen. *Formalising Trust as a Computational Concept*. PhD Thesis, Department of Computing Science and Mathematics, University of Sterling, 1 Apr 94.

36. Mason, C. Russell. The Art & Science of Protective Relaying. New York: Wiley, 1956. 6 Jul 09 http://www.gedigitalenergy.com/multilin/notes/artsci/index.htm.

37. Mathematic.uni-stuttgart.de. "Tabelle_Binomial.pdf." 19 Jan 10. http://www.mathematik.uni-stuttgart.de/studium/infomat/WiS_Surulescu_SS09/uebungen/Tabelle_Binomial.pdf.

38. Mazlumi, Kazem and Hossein Askarian Abyaneh. "Relay coordination and protection failure effects on reliability indices in an interconnected sub-transmission system," *Electric Power Systems Research*, 79: 1011-1017, (Jul 09).

39. McCoy, Damon, Doug Sicker, and Dick Grunwald. "A Mechanism for Detecting and Responding to Misbehaving Nodes in Wireless Networks," *2nd IEEE Workshop on Networking Technologies for Software Define Radio Networks*, 48-54 (Jun 07).

40. Meier, Alexandra von. *Electric Power Systems, a Conceptual Introduction*. Hoboken NJ: Wiley- Interscience, IEEE Press, 2006.

41. Milton, J. Susan and Jesse C. Arnold. *Introduction to Probability and Statistics: Principles and Applications for Engineering and the Computing Sciences*. St. Louis: McGraw Hill, 2003.

42. Mokhtar, M. R., U. Wajid, and W. Wang. "Collaborative Trust in Multi-Agent System," *2007 Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*, 30-34 (2007).

43. Moxley, Roy and Ken Fodero. "High Speed Distribution Protection Made Easy: Communications-Assisted Protection Schemes for Distribution Applications," *58th Annual Conference for Protective Relay Engineers*, 18-26 (2005).

44. Mulvenon, James C. and Richard H. Yang. *The People's Liberation Army in the Information Age*. Chapter 9: 181 (1998). 26 Oct 08 http://www.rand.org/pubs/conf_proceedings/CF145/.

45. NERC. "About NERC: Understanding the Grid." n. pag. 30 Dec 09. http://www.nerc.com/page.php?cid=1|15.

46. "ns-2: User Information." 2 Nov 09. n. pag. 13 Nov 09. http://nsnam.isi.edu/nsnam/index.php/User_Information.

47. Patnaik, Ansh. "Reducing the Risk of Cyber Threats in Utilities Through Log Management," Electricity Today, 22: 36-37 (January/February 2010). 24 Feb 10. http://my.texterity.com/electricitytoday/20100102/?pg=36.

48. Phadke, A. G. and J. S. Thorp. "Expose Hidden Failures to Prevent Cascading Outages," *IEEE Computer Applications in Power*, 9: 20-24 (July 1996).

49. Pool, Percy E. and Larry Young. "Wire Line Subcommittee: P1692 Guide for the Protection of Communication Installations from Lightning Effects." n. pag. 10 Jan 10. http://www.ewh.ieee.org/soc/pes/pscc/index.html#Wire_Line_Subcommittee_(SC-6).

50. Prenhall.com. "Cumulative Binomial Distribution Table." n. pag. 19 Jan 10. http://wps.prenhall.com/wps/media/objects/1060/1085467/Binomial_CDF_Table.doc.

51. Ramchurn, Sarvapali D., Dong Huynh, and Nicholas Jennings. "Trust in multi-agent systems," *The Knowledge Engineering Review*, 19: 1-25 (2004).

52. Schweitzer, Edmund O. III, Ken Behrendt, Tony Lee, and D. A. Tziouvaras. "Digital Communications for Power System Protection: Security, Availability, and Speed," *7th International Conference on Developments in Power System Protection*, 94-97 (Apr 01).

53. Sleva, Anthony F. *Protective Relay Principles*. Boca Raton FL: CRC Press, 2009.

54. Shahidehpuor, Mohammad and Yaoyu Wang. *Communication and Control in Electric Power Systems: Applications of Parallel and Distributed Processing*. Hoboken, NJ: IEEE Press, John Wiley and Sons, 2003.

55. Shaw, William T. *Cybersecurity for SCADA Systems*. Tulsa OK: PennWell Corp., 2006.

56. Smith, Michael. "Spy Chiefs Fear Chinese Cyber Attack," *The Sunday Times*, 29 Mar 09. 10 Jan 10 http://www.timesonline.co.uk/tol/news/uk/article5993156.ece.

57. Stevens, W. Richard. *TCP/IP Illustrated, Vol 1*. New York: Addison Wesley, 1994.

58. Thorp, James S., Xiaoru Wang, Kenneth Hopkinson, Denis V. Coury, and Renan Giovanini. "Agent Technology Applied to the Protection of Power Systems," *Securing Critical Infrastructure*, Grenoble, October 2004.

59. U.S.-Canada Power System Outage Task Force (USCPSOTF). *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*. April 2004. 22 Mar 09 https://reports.energy.gov/.

60. UTCE. *Final Report of the Investigation Committee on the 28 September 2003 Blackout in Italy*. April 2004. 13 Aug 09 http://www.rae.gr/cases/C13/italy/UCTE_rept.pdf.

61. UTCE. *Final Report – System Disturbance on 4 November 2006*. Belgium, 2007. 13 Aug 09 http://www.entsoe.eu/fileadmin/user_upload/_library/publications/ce/otherreports/Final-Report-20070130.pdf.

62. Wall, David S. "Cybercrime and the Culture of Fear: Social Science Fiction(s) and the Production of Knowledge about Cybercrime," *Information, Communication & Society*, 11: 861-884 (2008).

63. Wang, Jian-Wei and Li Li Rong. "Cascade-Based Attack Vulnerability on the US Power Grid," *Safety Science*, 47: 1332-1336 (December 2009).

64. Wang, X. R., K. M. Hopkinson, J. S. Thorp, R. Giovanni, K. Birman, and D. Coury. "Developing an Agent-based Backup Protection System for Transmission Networks," *Power Systems and Communications Infrastructures for the Future*, Beijing, (September 2002).

65. Wang, Yu, Qiuyue Zhang, and Ying Jiang. "A Trust Management Model Based on Multi-agent System," *2008 ISECS International Colloquium on Computing, Communication, Control, and Management*, 449-453 (2008).

66. Ward, S., T. Dahlin, and W. Higinbotham. "Improving Reliability for Power System Protection," *2004 Annual Protective Relay Conference*, Atlanta GA, (28-30 Apr 04).

67. Ward, S., T. Dahlin, and B. Ince, "Pilot Protection Communication Channel Requirements," *57th Annual Conference for Protective Relay Engineers*, 350-391 (30 Mar – 1 Apr 04).

68. WCUPA.edu. "binomial table." n. pag. 19 Jan 10. http://courses.wcupa.edu/rbove/eco252/bintabl1.doc.

69. Zheng, Haitao and Jill Boyce. "An Improved UDP Protocol for Video Transmission Over Internet-to-Wireless Networks," *IEEE Transactions on Multimedia*, 9: 356-365 (Sep 01).

70. Zhu, Yongli, Shaoqun Song, and Dewen Wang. "Multiagents-based wide area protection with best-effort adaptive strategy," *International Journal of Electrical Power & Energy Systems*, 31: 94-99 (February-March 2009).

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
25-03-2010	Master's Thesis	May 2008 – March 2010

4. TITLE AND SUBTITLE

Reputation-Based Trust for a Cooperative, Agent-Based Backup Protection Scheme for Power Networks

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Borowski, John F., Maj, USAF

5d. PROJECT NUMBER
10-173

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, Building 640
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GCO/ENG/10-04

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory, Information Grid Division
Attn: Dr. John Matyjas
525 Electronics Parkway
Rome, NY 13441
(315) 330-4255 (DSN: 587-4255); email: John.Matyjas@rl.af.mil

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/RIGE

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

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This thesis research explores integrating a reputation-based trust mechanism with an agent-based backup protection system to improve the performance of traditional backup relay methods that are currently in use in power transmission systems. Integrating agent technology into relay protection schemes has been previously proposed to clear faults more rapidly and to add precision by enabling the use of adaptive protection methods. A distributed, cooperative trust system such as that used in peer-to-peer file sharing networks has the potential to add an additional layer of defense in a protection system designed to operate with greater autonomy. This trust component enables agents in the system to make assessments using additional, behavioral-based analysis of cooperating protection agents. Simulation results illustrate the improved decision-making capability achieved by incorporating this cooperative trust method when experiencing abnormal or malicious communications. The integration of this additional trust component provides an added push for implementing the proposed agent-based protection schemes to help mitigate the impact from wide-area disturbances and the cascading blackouts that often follow. As the push for electric grid modernization continues, an agent-based trust system including this type of behavioral-based analysis will also benefit other smart components connecting critical grid control and monitoring information systems.

15. SUBJECT TERMS
Cooperative systems, Power transmission protection, Protective relaying, Wide-area networks

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Kenneth M. Hopkinson, PhD, (ENG)
U	U	U	UU	122	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-6565, x4579 kenneth.hopkinson@afit.edu

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39-18