3-2008

Evaluating Security and Quality of Service Considerations in Critical Infrastructure Communication Networks

Gregory R. Roberts

EVALUATING SECURITY AND QUALITY OF SERVICE CONSIDERATIONS IN CRITICAL INFRASTRUCTURE COMMUNICATION NETWORKS

THESIS

Gregory R. Roberts, Captain, USAF

AFIT/GCO/ENG/08-05

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 United States Government.

AFIT/GCO/ENG/08-05

EVALUATING SECURITY AND QUALITY OF SERVICE CONSIDERATIONS IN CRITICAL INFRASTRUCTURE COMMUNICATION 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 in Cyber Operations

Gregory R. Roberts, B.S.C.I.S, M.A.C.R.I.M

Captain, USAF

March 2008

AFIT/GCO/ENG/08-05

EVALUATING SECURITY AND QUALITY OF SERVICE CONSIDERATIONS IN CRITICAL INFRASTRUCTURE COMMUNICATION NETWORKS

Gregory R. Roberts, BS, MA

Captain, USAF

Approved:

_____/signed/_____	_26 Feb 08_
Dr. Kenneth M. Hopkinson (Chairman)	Date
_____/signed/_____	_26 Feb 08_
Dr. Richard A. Raines (Member)	Date
_____/signed/_____	_26 Feb 08_
Maj Paul D. Williams, PhD (Member)	Date
_____/signed/_____	_26 Feb 08_
Capt Todd R. Andel, PhD (Member)	Date

Abstract

This thesis demonstrates the benefits of utility communication based on Internet technology, some dangers in using Internet technology in establishing a utility intranet connecting protection and control systems, and compares three different approaches to making reservations for routing traffic in the utility intranet based on different levels of background traffic. A model of expected background traffic on a national utility intranet is presented. The Utility Communication Architecture 2.0 and the International Electrotechnical Commission (IEC) 61850 began laying the groundwork in 2002 in establishing an infrastructure allowing power substations, program logic controllers, remote terminal units, intelligent electronic devices, and other devices to effectively and efficiently communicate over a utility intranet that is based on Internet standards using commercial of the shelf (COTS) components. This intranet will almost certainly be based on Internet standards due to their widespread use, low cost, and easy migration path over time. Even though it's based on Internet technology the utility intranet will allow utilities to connect to one another without exposing them to threats from the Internet. This will provide utilities with the needed insight into other areas of the power grid enabling them to better manage its operation. The Electrical Power Communication Synchronization Simulator (EPOCHS) is used in this thesis to run simulations that models network traffic over a power infrastructure in order to show the effects of using different protocols, bandwidth reservations, and varying levels of background traffic will have on the quality of service of intranet traffic, with the end result of improving the

insight the different regions of the utility intranet will have with each other. EPOCHS provides the required simulation environment needed to integrate a network simulator with an electromechanical power simulator to run the simulations.

This research discusses the benefits of utility communication, the likely pitfalls in the use of Internet technology for protection and control systems, and technologies that can help mitigate those pitfalls. A total of 48 different simulation configurations are performed based on background traffic, reservation type, IP transport protocols, and routing scheme used to determine which configuration is best suited for use on a utility intranet.

Acknowledgments

I would like to express my sincere appreciation to my faculty advisor, Dr. Kenneth Hopkinson, for his guidance and support throughout the course of this thesis effort. This research would not have been possible without his assistance and insight. I'd also like to thank my son, his mother, and our dog for putting up with me through this demanding time.

Gregory R. Roberts

Table of Contents

Page

List of Figures

Page

List of Tables

Page

List of Abbreviations

ACKs	Acknowledgements
AFB	Air Force Base
AGC	Area Generation Control
API	Application Programming Interface
CIL	Critical Infrastructure Lab
CongWin	Congestion Window
COTS	Commercial off the Shelf
DARPA	Defense Advanced Research Projects Agency
DiffServ	Differentiated Services
DOE	Department of Energy
EMTDC	ElectroMagnetic Transients including DC
EPOCHS	Electrical Power Communication and Synchronization Simulator
EHV	Extremely High Voltage
GE	General Electric
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISO	Independent System Operator
KV	Kilovolt
LSP	Label Switched Path
LSR	Label Switch Router
MB	Megabytes
MIB	Management Information Base
MISO	Midwest Independent System Operator
MOM	Message-Oriented-Middleware
MPLS	Multiprotocol Label Switching
MW	Megawatts
NAM	Network Animator
NERC	North American Electric Reliability Corporation
NSF	National Science Foundation
NS2	Network Simulator 2

PPRN	Package to solve single/multicommodity network flow problems
PSCAD	Power Systems Computer Aided Design
PSLF	Positive Sequence Load Flow
PSS/E	Power System Simulator for Engineers
QoS	Quality of Service
RSVP	Resource ReSerVation Protocol
RTU	Remote Terminal Unit
RTI	Run Time Infrastructure
SCADA	Supervisory Control and Data Acquisition
SPS	Special Protection Schemes
UCA	Utility Communications Architecture
TCP	Transmission Control Protocol
UFLS	Underfrequency Load Shedding
U.S.	United States
UDP	User Datagram Protocol
WAMS	Wide Area Measurements System

EVALUATING SECURITY AND QUALITY OF SERVICE CONSIDERATIONS IN CRITICAL INFRASTRUCTURE COMMUNICATION NETWORKS

I. Introduction

Background

The electric power grid of North America is a complex set of interconnected systems spanning thousands of miles. The grid must be operated so a balance is maintained between supply and demand. This process is made even more complex by the restructuring of the power grid, to include deregulation and competitive markets for electricity. The restructuring has changed the organizational structures of the electricity supply industry as well as the operations of power systems. To ensure interoperability between the various systems, information needs to be shared amongst the operators in different regions in a timely manner.

The population of the United States has continued to grow and the demand for power keeps increasing. Even though the demand for power continues to increase, the communications infrastructure of the power grid and the power grid itself has grown at a slower pace. This situation can and usually does result in power outages that can cascade to affect a much larger area because the grid is run closer to capacity as the demand continues to increase. The lack of communications infrastructure was highlighted during the 14 August 2003 blackout when logs showed operator interaction as the crisis unfolded was severely inhibited.

The Midwest Independent System Operator's (MISO) state estimation system stopped receiving updates on its systems when the Supervisory Control and Data

Acquisition (SCADA) information from nearby CINergy's domain stopped arriving on lines that failed during the beginning stages of the blackout. The MISO power system operators failed to notice the fact that SCADA information was not being displayed and did not receive the resulting alarm. The lack of operator awareness was one of the major reasons for the blackout in MISO's region. None of the other neighboring regions had a clear picture of what was unfolding and they normally don't, even under the best of conditions. This resulted in the blackout cascading far beyond the Ohio-based First Energy's borders [1].

The above example is complicated with the recent deregulation of the electric power grid. In order to promote competition within the electric market, deregulation mandates the delivery of status information about operational and market conditions to legitimate market participants. Real time exchange of data may take place between and among control centers, power plants, transmission substations, distribution substations, residential customers, industrial customers, and commercial customers for operational tasks and market trading. Figure 1 provides an example of the proposed interactions of the grid participants of a deregulated power market. The communication infrastructure of the power grid is not capable of disseminating operational and market data, and status information with the flexibility, robustness, and timeliness to meet today's standards [2].

The power industry has shown it is ready to move to the next generation of communication systems to better connect the power grid and allow it to meet its increased demands, thus preventing a cascading blackout as described in the above

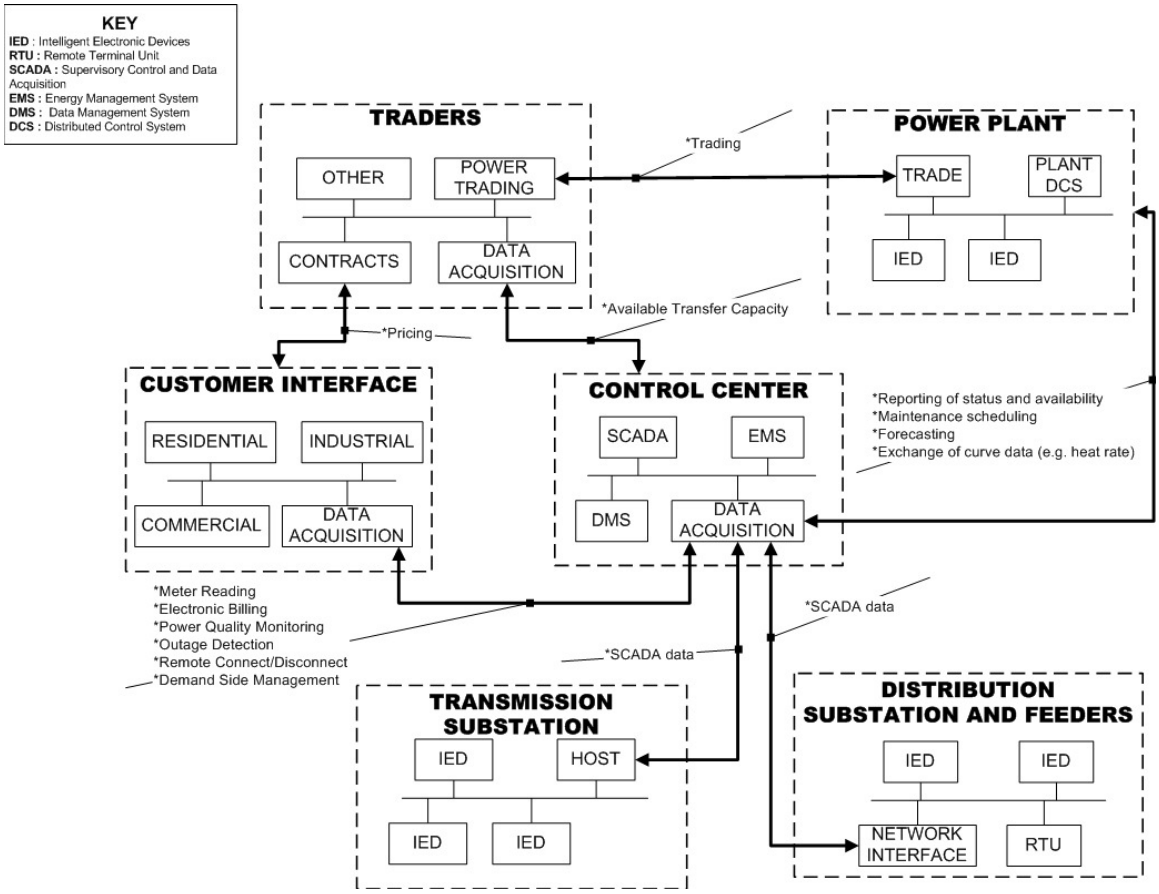

Figure 1. Deregulated Electric Power Market [2]

scenario. The advent of UCA 2.0 [3], IEC 61850 [4], and wide area measurement systems (WAMS) in the western U.S. are examples of three initiatives that are helping migration toward a future utility intranet. The utility intranet will enable the communication elements of the power grid to be interconnected much the same way as the components of the power grid are currently integrated. The network will allow for better communication, protection and control of the grid, insight into other areas, and sharing of data and power amongst the various regions of the grid. Care must be taken to ensure the protocols, security, quality of service (QoS), network capacities, and routing

schemes used are properly equipped to handle the demands communicating on the power grid will require. QoS for the power grid is defined as the delivery of data in a timely manner with adequate bandwidth, reliability, security, and redundancy to meet the communication requirements the grid will require [5].

Ensuring the reliability of the power grid is also critical because of the increased threat our SCADA systems that protect our critical information infrastructure face. The United States (U.S.) military has discovered evidence in Afghanistan that al-Qaida terrorist groups were researching SCADA systems and cyber terrorism is quickly becoming a target of interest for terrorist groups [6]. Based on this threat, more must be done to provide better insight into the different parts of the power grid so different regions can be alerted to such events.

Since 1965 there have been 9 major North American Blackouts and from 1979 to 1995 there were 162 disturbances reported by the North American Electric Reliability Corporation (NERC). Based on the analysis of the blackouts and disturbances it was determined a high percentage of these disturbances were partly caused by inadequate real-time monitoring and operating control systems, communication systems, and delayed restoration problems [7].

Unless something is done to improve the communications infrastructure of the power grid, events like the ones that led to the August 2003 blackout could become more common. As we keep running the power system closer to its limits, thus making it less stable, something must be done to improve the monitoring technology in order to assist in stabilizing the grid.

The research described in this document advocates the establishment of a long-term research program whose goal is to establish a next generation communication networking infrastructure that will enhance the sharing of critical information about the status of the power grid amongst the various regions of the grid. This infrastructure can be referred to as a utility intranet that connects the power grid to enable the sharing of time critical information about its status. The infrastructure will take into consideration the various types of traffic expected to be found on the utility intranet and explore ways to reserve bandwidth in middleware and routers to ensure delivery of the most critical of traffic.

Problem Statement

I read several chapters from the final report of the 2003 blackout [1] and one of the recurring themes from this report is the lack of situational awareness throughout the grid. Lack of situational awareness has been a theme in every major blackout in North America in recent history, yet we are making slow progress in this critical infrastructure mission area. While the situational awareness within one region may be sufficient, the regions lacked the insight into other areas of the grid to properly stabilize it.

The current communications technology that interconnects the grid is insufficient to handle the communication demands required to ensure its reliable operation as the grid becomes more stressed. NERC consists of eight regional reliability councils, shown in Figure 2, which assist in improving the reliability of the North American power grid. The regions consist of members from all segments of the electric power industry. To

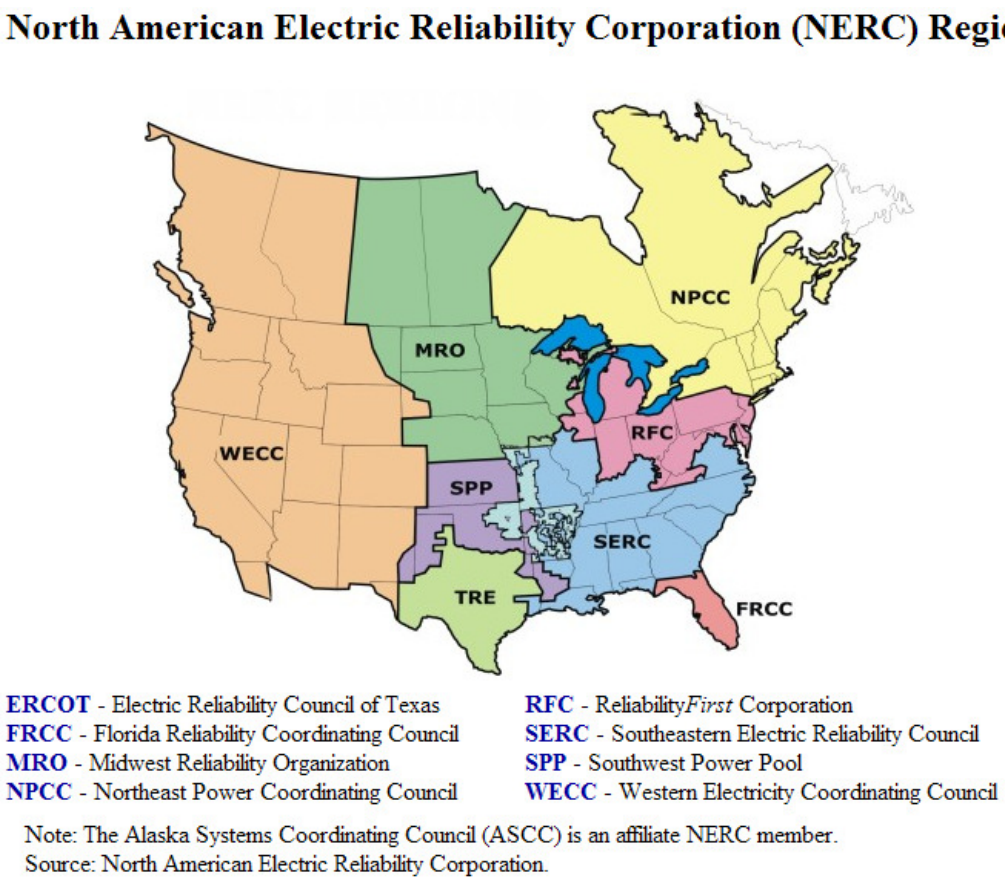

Figure 2. NERC Regions [8]

assist with the operation of the power grid the various NERC regions contain balancing authorities.

There are a total of 131 balancing authorities (Figure 3) in the North American Power Grid. They have the responsibility to integrate resource plans ahead of time, maintain load-interchange-generations balance within a Balancing Authority Area, and supports interconnection frequency in real time [8]. Balancing authorities are spread

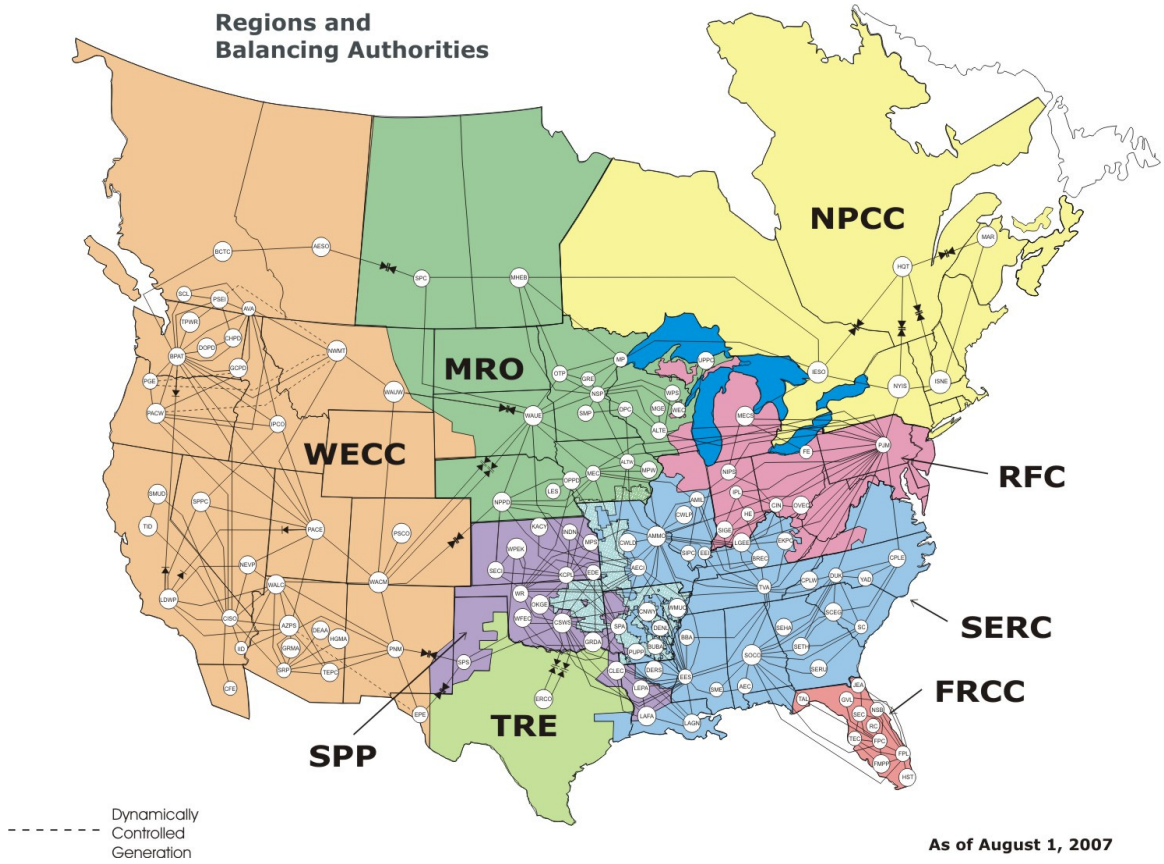

Figure 3. NERC Balancing Authorities [9]

throughout the NERC regions and are essential for the efficient operation of the power grid. Along with the NERC regions, balancing authorities must have proper insight into the various parts of the grid, both within and among the different NERC regions, if they are to assist in preventing cascading outages.

The key to preventing cascading outages is to enable better insight by different utilities into other utilities area of responsibility. A communication system needs to be established to replace the archaic system currently being utilized by the power industry to meet these demands. This proposed system is known as a utility intranet, as mentioned earlier in this paper.

A scheme needs be put in place to monitor the power grid and provide detailed status of power generation and load on the grid. The scheme used in this research is a special protection scheme (SPS). The SPS monitors the grid via the use of agents and provides essential information via the utility intranet to other buses on the grid.

Previous work looked at how greater communication might impact the grid using a SPS as an example. This thesis looks at the impact unreliable communication might have on such schemes.

This research will also take into account the different types of background traffic that may be found on the utility intranet. To overcome the delays that can be caused by the background traffic, bandwidth reservation techniques are used to ensure mission critical traffic gets to its destination in a timely manner. Delays of milliseconds can be costly when dealing with the effective and safe operation of the power grid.

When the Internet was created, it was not designed for the time sensitive, critical protection and control demands that is common with the power grid. Also, the current communications structure of the power grid was not designed for this type of communication. A lot of the components of the current power grid are proprietary and don't interact well with components from other manufacturers. With the advent of the UCA 2.0 and IEC 61850, components are now being deployed that can support the increased communication needs of the power grid. This will provide for better communication to meet the faster responses, better coordination, and increased correctness needed by the power community [10].

Our experiments use the size and frequency of expected traffic while using different protocols with various levels of background traffic in a power protection and control scenario involving bandwidth reservations in network communication. This research demonstrates how effective middleware can be if all the traffic is known, understood, and passes through the middleware layer. Otherwise, the experiments demonstrate the best way to handle reservations is from making them in the router where all the utility intranet traffic will pass.

Where bandwidth reservations are made can have an impact on the QoS and reliability of network traffic and will be crucial to the development of a future utility intranet. This thesis explores the consequences of no reservations, making reservations in middleware, and finally making reservations in routers while also dealing with competing background traffic and SPS agent traffic.

Preview

In summary, the composition of a utility intranet based on Internet technology is needed is order to ensure reliable communication of an overburdened power grid and to help prevent cascading blackouts like the one on 14 August 2003. Protocols based on Internet Protocol (IP) networks will be evaluated to ensure the utility intranet uses the most adequate protocol. In this thesis we conduct experiments comparing the effectiveness of making reservations in middleware and routers, thus ensuring reliable delivery of SPS agent traffic using different protocols and different levels of background traffic. The EPOCHS simulation system will be used to link Network Simulator 2 (NS2)

and Power System Simulator for Engineers (PSS/E) simulators into a federation of simulators for running the experiments.

This chapter provided an introduction of the research subject area and presented a brief overview of the problem set. Chapter II introduces the reader to the subject matter and gives background information on research that has already been conducted in this area. Chapter II also describes how this research is different from previous research on the same topic. Chapter III gives a full explanation of the methodology and details the approach used in conducting the experiments. Chapter IV compares the different experiments conducted and presents the results is a logical manner. Finally, Chapter V summarizes the experiment results, explains the significance of the research, and presents areas for future research.

II. Literature Review

Chapter Overview

This chapter gives an introduction to background material that gives a detailed overview of the research areas of this thesis. It will also describe research that has been conducted in wide area protection and control systems and describe some of the basic concepts of the utility intranet. Next, a discussion of the benefits of using networked communication in implementing a wide area protection and control system that meets the needs of the power grid is presented. Finally, I will discuss how this thesis differs from the previous research that's been conducted in this area.

Background

As stated earlier, since 1965 there have been 9 major North American Blackouts and from 1979 to 1995 there have been 162 disturbances reported by NERC. Lack of situational awareness was a contributing factor in a majority of those cases. In order to lessen the severity and number of blackouts and disturbances it's essential to share information about the status of the power grid in a timely manner amongst the various regions. The dynamics of the power grid are normally global in nature, but the configuration of grid status data is normally constrained to a single substation where it originated. Considering the complexity and interconnection of the power grid, it’s essential to share as much information as possible about its status.

Power system equipment is designed to operate within certain limits and any deviation to those limits can have serious consequences if actions to alleviate the situation are not taken immediately. If an event occurs that causes the system to operate

outside valid limits, it may cause a further series of actions that switch other equipment out of service, thus causing cascading outages resulting in a widespread blackout [11].

An example of the above scenario is a single transmission line is open due to some type of event happening on the grid. The result is extra megawatts (MW) being transmitted on the remaining lines. If one of the remaining lines has too much load on it due to the opening of the other line, it could also open due to relay action. Now the remaining lines have too much load on them and can overheat and also go down, thus causing that area of the grid to have a blackout. If this situation is not observed by the other control centers the outage could cascade and eventually cause a widespread blackout.

The events of 14 August 2003 highlighted the inadequacy of the current communication system of the power grid. A critical monitoring system failed and regions outside the region directly affected by the failure failed to notice the outage. Protection and control system operators were unable to make sense of fluctuating voltages and line frequencies that occurred over a period of several hours. This prevented operators from taking corrective action that could have prevented or at least lessened the effect of the cascading outage [1].

Because of proprietary equipment traditionally used on the power grid, communicating high demand, time-sensitive traffic is often difficult, if not impossible. A network structure should be built to enable effective communication on the next generation utility intranet. In order to accomplish this we need to explore the different

protocols available on the Internet, bandwidth reservation techniques, and the architecture of a future utility intranet.

Recent efforts, such as the UCA 2.0, IEC 61850, and Wide Area Measurement Systems (WAMS) Project in the Western U.S., have shown the industry is committed to establishing a common architecture with real time intelligent agents to improve the functionality of the North American power grid. A communication infrastructure that enables the sharing of time-sensitive information in a timely manner is essential. The technology will be based on UCA 2.0 and IEC 61850 standards to ensure compatibility.

IEC 61850

The electrical power grid of North America involves almost 3,500 utilities that keep supply and demand in balance while abiding by the loading constraints of transmission lines. All along, transmission lines are operating nearer towards their safety limits. Communication on the power grid is being conducted with rudimentary communications technology and is also being performed with power communication equipment that is decades old. The result is stability problems being created much quicker than they can be corrected [5]. To correct this problem, components that will make up the future communications infrastructure of the power grid should be IEC 61850 compliant. IEC 61850 standard is a superset of the UCA 2.0 and is leading the way towards next-generation communication systems in order to meet the increased demands of the electric power grid.

The traditional approach to sharing information among substations is through the use of standard Remote Terminal Unit (RTU) protocols that are designed for operating

over bandwidth limited serial links. While many of these systems still exist, the new standard is to use Ethernet technology, thus enabling high speed communication among substations. IEC 61850 ensures standardization so communication on the grid can take advantage of technology and dramatically reduce the overhead cost of establishing substation automation that goes far beyond the simply RTU approach used in most systems today.

IEC 61850 is a new approach to substation integration and automation that leverages modern computer and networking technology to maximize reliability and performance while minimizing installation, design, and commissioning costs. Since its inception in 2002, IEC 61850 is used in hundreds of substations world-wide for substation automation and is growing daily [4]. As legacy equipment is phased out it will most likely be replaced with IEC 61850 compliant equipment and standards.

The standard is based on object oriented models of how devices look and behave to network applications. IEC 61850 standard specifies the protocol standard, communication requirements, functional characteristics, structure of the data in the devices, and how conformity to the standards should be tested for substation integration. The bottom line is IEC 61850 reduces the cost of substation design, installation, commissioning, and operation combined with the ability in implement new and improved functionality. This is not available using legacy RTU communication schemes that have been used in substations of the past and are still used in substations throughout the North American power grid [4].

Wide Area Monitoring

The Department of Energy (DOE) conducted research beginning in 1989 to assess and determine research and development needs of the electric power system operation. As a result, the WAMS Project was launched in 1995 by the DOE jointly with Bonneville Power Administration and the Western Area Power Administration [12]. The WAMS project intent was to enhance control and operation of the power grid as a means for serving customer demands in an environment with increased competition, additional services, and narrower operating margins. With the growth, increased strain, and pattern of instability on the Western power grid, this effort was deemed essential if the Western grid was to remain stable with increased system efficiencies and capacity. While the WAMS project is promising it puts a lot of strain on the underlying communication infrastructure especially if it is going to be used in conjunction with a utility intranet.

To increase the efficiency and effectiveness of WAMS the concept of agents as used in this research could be incorporated. Agents not only provide protection for local components, but they are also intelligent and can act, respond, monitor, and share information among other agents throughout the communication infrastructure of the grid. The current grid architecture can be categorized as information starved because of its lack of situational awareness. By upgrading the communication infrastructure and implementing agents that examine system behavior and share information in near real-time the grid will be better suited to meet the increased demands, improve stability, and more efficiently operate to improve profit margins. This research uses SPS agents for communicating protection and control traffic among the various substations in the

simulations. A detailed overview of agents and how they are utilized is given in Chapter III.

Transport Layer Protocols

The utility intranet will almost certainly consist of COTS components that are compliant with current Internet technology and meet IEC 61850 standards because to do otherwise would be very expensive. Based on this, it's important to evaluate the two most popular transport layer protocols of the Internet that will most likely be used for the utility intranet.

At the network layer, the IP service model provides a best effort delivery service. The best effort delivery service means the network layer will make every effort to ensure packets are delivered but it makes no guarantees. IP does not guarantee sequential delivery of packets, doesn't guarantee the integrity of the packets, and doesn't guarantee orderly delivery of the packets. As the amount of traffic on the network increases, the probability of it being successfully delivered to the destination is hampered. For these reasons, IP is said to be an unreliable service [13]. Because of this, it's required that we take a look at two of the more popular transport layer protocols on IP based networks.

Transmission Control Protocol

While the network layer provides logical communication between the hosts, it's the transport layer that provides logical end-to-end communication between processes. Since the IP layer doesn't guarantee delivery, it can be supplemented at the transport layer with Transmission Control Protocol (TCP). TCP provides transmission guarantees to ensure packets aren't lost and never delivered to their destination host in an unreliable

manner. This makes the combination of TCP/IP a viable choice of protocols for use on a utility intranet.

Reliability is ensured by guaranteeing transmissions through the use of acknowledgements (ACKs). When the destination host receives a packet it responds with an ACK to inform the sending host the packet has been received. If an ACK has not been received by the sending host after a certain amount of time it will retransmit the lost packet, thus ensuring reliable delivery.

TCP is said to be connection-oriented because the processes involved in the communication must send some preliminary information to each other in order to establish the session. The connection is only maintained at the end processes. The routers and link layer switches are not involved in establishing or maintaining the session except as a medium for packets to traverse. State information is maintained by the end processes and the connection is taken down when all communication is finished.

A TCP connection is a full-duplex, point-to-point service. Full duplex simply means one process can send packets to the destination process while at the same time receive packets from the destination process. The connection between the two processes is said to be point-to-point because the connection is only between two hosts. There is a single sending host and a single receiving host on each end of the communication. It's not possible to send multicast messages with TCP since this involves having more than one receiving host. If one wants to do this they will have to use User Datagram Protocol (UDP), which is discussed in the next section.

TCP uses flow control and congestion control to help prevent hosts, routers, and data link layer switches from being overwhelmed with traffic. With flow control each receiving host has a buffer for receiving incoming packets and the available space in the buffer is advertised to the sender so the sender doesn't send more traffic than the receiver can handle. The amount of space left in the buffer is sent in the ACK messages from sender to receiver. The sender needs to know the amount of space free in the buffer so it doesn't overwhelm the receiver's ability to process traffic that is received. Even though this action may prevent the sender from overwhelming the receiver with information, there are still a lot of nodes on the Internet that are competing for resources. To ensure the other routers and data link switches on the network aren't overloaded with traffic, TCP uses congestion control.

Congestion is caused when too many sources on the network are sending data faster than the network can reliably handle. Congestion can cause packets to be lost at the routers due to buffer overflows and can cause packets to be delayed due to queuing in the routers. In order to handle these situations, TCP uses a three phase congestion control mechanism. Congestion is tracked by each side of a connection by an additional variable called CongWin (congestion window). CongWin limits the rate that data can be introduced to the network by the sender. The first phase of congestion control is known as slow start.

When the connection is first established the sending host sends one packet. Each subsequent round the sender exponentially increase the number of packets it sends until it reaches a threshold. The sender will send one packet, followed by two packets the next

round, followed by four packets the next round, etc., and it keeps doubling until the threshold is reached. At this point phase two begins with an additive increase. In the additive increase phase one additional packet is sent each round until a timeout event occurs or the sender receives three duplicate ACKs. If a timeout event occurs the CongWin is reset to one and the slow start phases begins again. If the sender receives three duplicate ACKs the CongWin will be cut in half and the CongWin will grow linearly. Receiving a timeout is more indicative of congestion in a network then receiving three duplicate ACKs. The behavior of TCP's congestion control is shown in Figure 4.

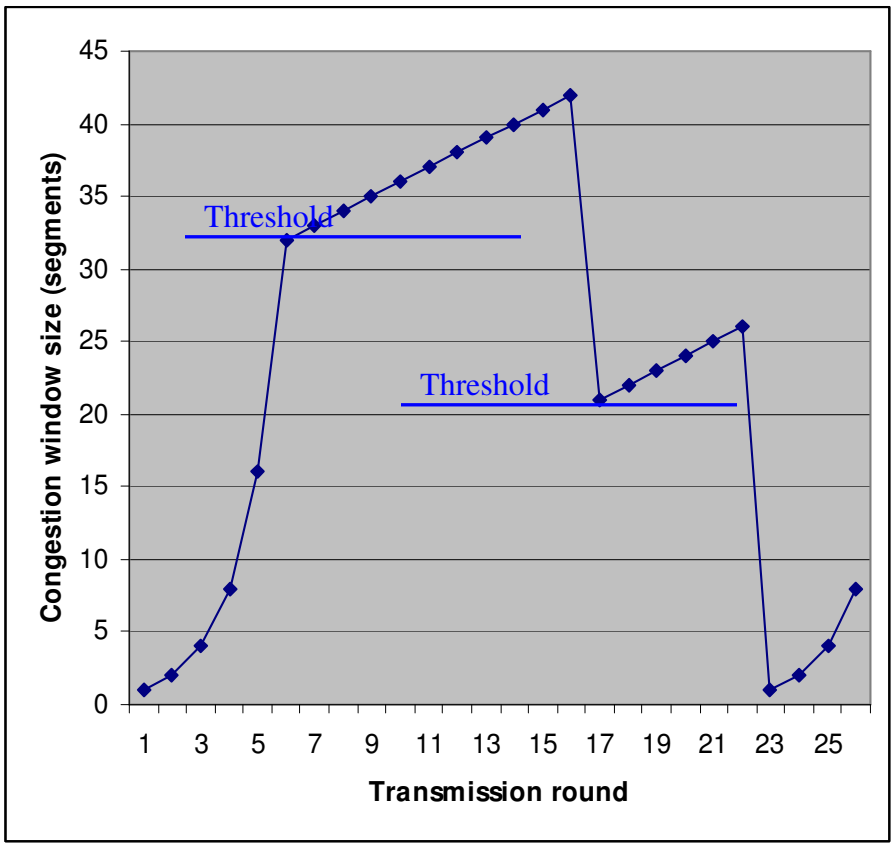

Figure 4. TCP Slow Start Graph

TCP is ideal for emails, file transfers, and other applications that are not time sensitive, but problems can arise when TCP is used to send data in a time critical manner. Since TCP is point-to-point it's not sufficient for sending data to more than one host which is needed in power monitoring systems. Protection and control data must be priority number one and TCP doesn't provide any provisions for prioritizing traffic. Because of the overhead in establishing a session along with the slow start ramp up phase of TCP, timely delivery of time-sensitive data can be hampered. As network utilization increases TCP's congestion control mechanism begins taking action, which can delay time-sensitive data. If a TCP connection is already established between hosts and a new event occurs that needs to be transmitted, it's difficult to establish a new TCP connection or ramp up an already established connection. The above behavior is inherent to TCP and makes it less than ideal for protection and control data of the power grid.

We have identified sources of background traffic that we project will be present in a utility intranet, to include fault data that might be 2.4 Megabytes (MB) in size and is described in Chapter III. The blackout of 14 August 2003 consisted of a series of cascading outages that originated in Ohio, traveled around the Great Lakes Region in Michigan, through Canada, and into New York. In all, the blackout that began in Cleveland, Ohio and cascaded to the Northeastern U.S. took a total of seven minutes, lasted for four days in some areas, and cost billions of dollars [1]. As the blackout cascaded, event after event occurred on the power grid causing a significant increase of

event traffic. The inherent behavior of TCP can cause the time sensitive traffic to be delayed when it's needed the most.

User Datagram Protocol

User Datagram Protocol (UDP) is a connectionless, best-effort, bare-bones protocol for the transport layer of the Internet. UDP is said to be connectionless because there is no handshaking between the sending and receiving transport layer entities. UDP is bare-bones because all UDP does on top of IP is take messages from the application, add source and destination ports for multiplexing and demultiplexing service, and adds a length and checksum field before passing the segment to the network layer.

Unlike TCP, UDP support multicast transmission whether it's one-to-many or many-to-many. UDP is also advantageous over TCP when transmitting time sensitive data. There is no handshaking thus saving time, no connection has to be established between nodes eliminating a source of transmission delays, data is transmitted immediately when it is sent and there are no queuing delays at the routers. It is obvious UDP is the preferred method over TCP for transmitting time sensitive data.

The downside of UDP is that it is not reliable. It is a send-and-forget transport layer protocol because it sends data and doesn't provide any mechanisms to ensure delivery of the data. If UDP is utilized, some mechanism must be added at the application layer to ensure reliability of transmitted data. Based on this, UDP by itself is not a preferred method for sending data across the utility intranet because the protection and control data of the power grid must have guaranteed delivery.

Neither TCP nor UDP is a sufficient transport layer protocol for the time-sensitive, reliability guaranteed needs the communication system of the power grid will require without modifying them in some way. There have been some middleware approaches to traffic management and engineering that have been developed to assist in meeting these needs.

Middleware Approaches to Traffic Management

Even tough TCP and UDP offer certain advantages, they fail to meet the needs of power grid communication during times of line faults and other major events due to the increased need for bandwidth. It's essential for power protection and control equipment that's communication dependent to be able to communicate during these events, especially during times of cascading outages. Neither TCP nor UDP offer guaranteed bandwidth on the communication network of the power grid, thus are not the solution without having assistance from another mechanism. This research promotes the use of a two-prong approach using both middleware-based traffic engineering and bandwidth reservations. This approach allows the network to efficiently and effectively handle routing background traffic and the occasional traffic spike that will result from line faults and other events. This research is centered on bandwidth reservations.

In a distributed environment like the power grid, middleware is defined as the software layer that lies beneath the applications layer and above the operating system, provides common abstractions across a distributed environment, and helps manage the complexity and heterogeneity inherent in distributed systems [14]. The large diversity of

software, hardware, and vendors on the power grid makes a middleware approach very attractive.

The middleware approach mentioned above for traffic engineering or traffic management is a strategy where the nodes on a network coordinate their traffic in order to reduce network congestion, enhance reliability on the network, and respond better to network disruptions. Astrolabe [15] and GridStat [2] are two such middleware systems that have been researched for potential use on the power grid.

Astrolabe

Astrolabe, developed by a group at Cornell University, Ithaca, NY, is a highly scalable monitoring system that is able to track variables system wide. It's a information management service that monitors the dynamically changing state of a collection of distributed resources. Astrolabe reports summaries of this information to its users.

Astrolabe uses zones to gather, aggregate, and disseminates information. All zones are represented by an identifier except for the root zone. Zones can be overlapping if they have one or more hosts in common and non-overlapping of they don't have any host in common. Figure 5 shows an example of a three level zone tree in Astrolabe. The top level is the root zone and has three child zones. Each zone has an attribute list known as a Management Information Base (MIB) and runs an Astrolabe agent on each host. The zone hierarchy is specified by the system administrator when he initializes the zone's agent [15].

Astrolabe does not rely on bandwidth reservation, but instead uses a peer-to-peer gossip protocol to probabilistically ensure updates are received. Using the gossip

protocol results in a system that's robust against many types of disruption; including patterns of localized network disruption typical of network overloads and distributed denial of service attacks [16].

Representatives from the agents within each zone are elected to take responsibility for running the gossip protocol. If something happens to the agent or it becomes unsuitable, the protocol will automatically elect another agent to take its place. As long as a reasonable amount of update messages arrive over time, lost updates will not be an issue.

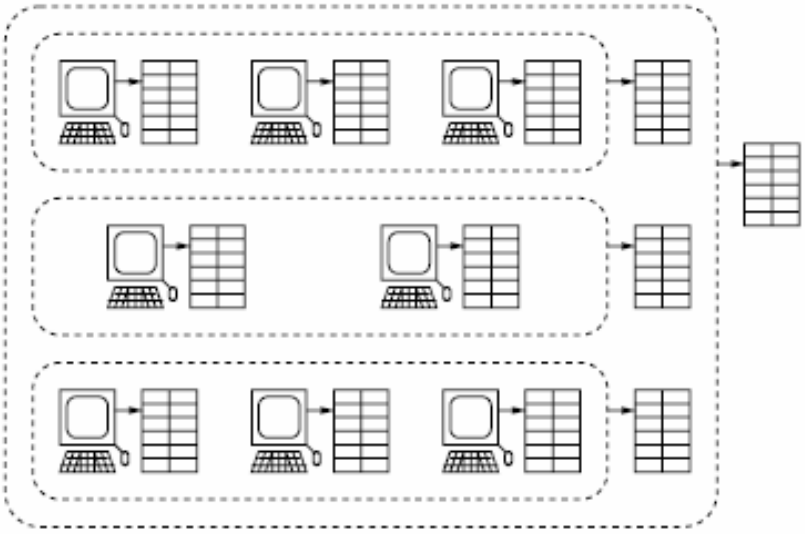

Figure 5. An example of a three-level Astrolabe zone tree [15]

Several experiments were conducted evaluating Astrolabe to see if it meets the communications demands of the power grid. The conclusions drawn were that Astrolabe is well suited to the monitoring needs of the electric power grid for disturbances that take place over a time scale of minutes or more. The drawbacks to Astrolabe are the gossip

rates have to be set very rapidly or it will be too slow for notifications when an urgent event occurs, it operates continuously and that could be a security concern in some settings, and it has week consistency [16].

GridStat

GridStat is a Message-Oriented-Middleware (MOM) that distributes data via message exchange. MOM provides an abstraction of a message queue that's available across the network. Users can pull messages based on a queuing order without direct interactions with the publisher. One of the specializations of MOM is its publisher-subscriber and status dissemination capabilities.

Status dissemination middleware is specialized for status variables and has a strong implication of real-time behavior. The publisher produces at a known rate and the middleware must meet the real-time requirements of its subscribers. Also, as the variables are updated with additional state information, the variable can be filtered to meet the needs of the subscriber thus saving bandwidth. The filtering is made possible by a number of QoS requirements imposed on the variables tracked by the status dissemination middleware. This is not possible with traditional publisher-subscriber middleware.

As shown in Figure 6, nodes can be in the form of a publisher, subscriber, or both. The interaction is handled by the status routers that make up the communication infrastructure and forwards status variables to subscribers. The publishers don't care who subscribes to its published variables and the subscribers are able to subscribe to variables and state the given rate of updates needed and the required level of redundant paths. If

the subscriber's demands can't be meet they are informed immediately by the applicable QoS broker [2].

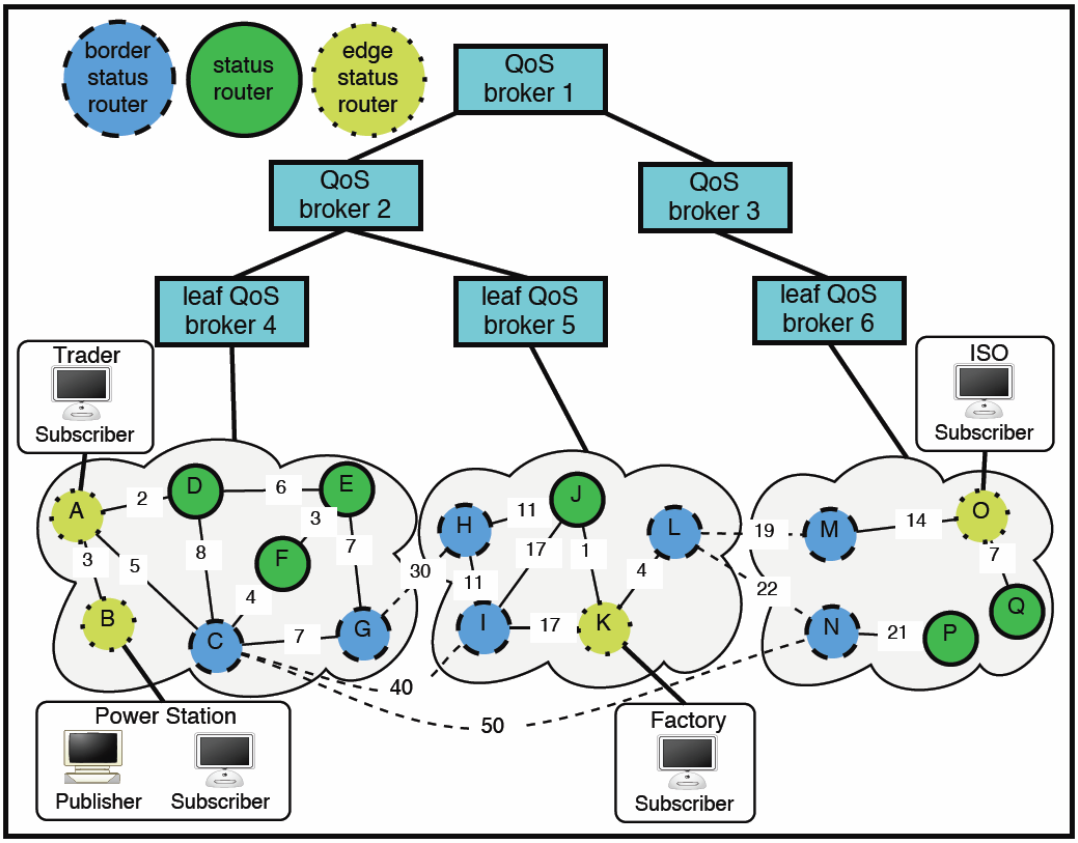

Figure 6. Detailed Architecture of GridStat [2]

Quality of service can be guaranteed because all traffic sources have to register with the middleware system. The middleware system ensures the quality of the network traffic is less than the capacity of the network. If traffic sources exceed their registered network usage levels, don't register with the system, or request QoS parameters that can't be meet by the system, the applicable QoS broker will inform the subscriber its request

can't be meet. Table 1 shows an example of QoS properties and policies for a typical GridStat system.

GridStat is work in progress and more work needs to be accomplished before it can be released on a large scale. An alternative method to traffic management on a network is through bandwidth reservations at the network layer.

Table 1. QoS Properties and Policies [2]

QoS Property	Policy
Delivery Guarantee	best-effort, at-most-once, at-least-once, exactly-once
Message Priority	FIFO, EDF, priority
Overflow Control	ANY, FIFO, LIFO, or message priority

Bandwidth Reservations

Bandwidth reservations are another way to regulate network traffic through the use of reservations in routers. Two popular ways of making reservations for network traffic is through the use of Multiprotocol Label Switching (MPLS) and Resource Reservation Protocol (RSVP). If an application requires 5 MB of bandwidth, a reservation can be made guaranteeing the application the required amount of bandwidth needed along its path of traversal. The reservation is not impacted by other types of traffic and amount of traffic present on the network.

MPLS has been enhanced to tunnel traffic through the routers to avoid congestion and maximize available bandwidth. The header for MPLS traffic (known as a label) lies

between the data link header and network header on each packet. The placement of the label allows it to traverse quickly through the routers on a network without requiring the IP header to be read at each hop. The labels are only significant between the two devices involved in the communication. At each hop, the label is read and given a new label upon its ingress to the router. The incoming interface and label value determines the outgoing interface and label value. Each packet is routed to its next hop based on the new value of the label.

The routers along a MPLS path are known as label switch routers (LSR). The final path a packet takes along a MPLS reservation is known as its label switched path (LSP) and consists of several LSR. LSPs are data driven if established when a certain flow of data is detected and are control driven if established prior to data transmission. The MPLS label mentioned in the prior paragraph is encapsulated in the packets moving from one point to another. Since the labels are at the beginning of the packet the hardware is able to quickly switch the packets between links along its LSP [17].

MPLS also assists traffic engineering by providing functionality that helps control network traffic by easing network congestion by establishing alternate routes for LSP. This helps spread the traffic load over the network. MPLS can also establish routes for certain types of traffic or certain classes of users. If an event happens on the power grid that requires quick reaction from other entities on the grid, MPLS can establish a path for power event traffic that reserves enough bandwidth to efficiently handle the event's traffic.

Another network layer reservation protocol that can be used is RSVP. RSVP is designed to reserve resources in unicast or multicast delivery paths across a network that meets some predefined QoS parameters. RSVP is not a routing protocol but integrates with current routing protocols to reserve resources at each node along a route. With RSVP, the receiver of the traffic flow is responsible for initiating, maintaining, and releasing the reservation.

There are two major issues with the above reservation protocols. First, traffic spikes for reservations are not handled efficiently. If a traffic spike occurs over a reservation and the bandwidth is exceeded, the extra traffic will be treated as best effort and may or may not make it to its destination. Second, bandwidth is wasted when not being used by the reservation traffic. The power grid is too critical a resource to accept this type of behavior.

Research Overview

Thus far in this chapter, I've presented you with some background information that has driven my research and some research that has already been conducted on this topic. A discussion follows into how this research incorporates some of what has already been accomplished and how it differs in utilization of communication protocols, background traffic, and federation of simulators to show the benefits of a properly constructed utility intranet.

In order to properly simulate real-world traffic on a utility intranet all types of traffic and loads need to be generated and propagated throughout the network. A model for expected background traffic is presented and traffic is generated based on low traffic,

moderate traffic, and heavy traffic loads along with regular event traffic that power system equipment will be generating. The background traffic provides for more realistic scenarios of the data that will traverse the links of a utility intranet.

Approximately 48 separate scenarios and 480 simulations were conducted testing the various levels of background traffic utilizing TCP and UDP network layer protocols. Both protocols are tested to show how responsive they are to various levels of traffic based on the reservation scheme used.

Power systems of the past were controlled by large regional power pools that didn't contain significant amounts of communication elements, thus power system simulations have modeled power systems without considering the large amounts of protection and control systems that are currently being utilized. In order to properly conduct the simulations, a tool is needed that can simulate the communication infrastructure of the power grid along with the real-time scenarios that include load surges, outages, and other forms of dynamic stress that's prevalent in the power system.

This research uses the EPOCHS simulator because of its unique capability to combine simulation environments. EPOCHS can combine network simulators with power system simulators to create a realistic scenario for providing high-quality simulations of electric power scenarios while simultaneously modeling the behavior of communication protocols like TCP and UDP in realistic networks [18].

By using EPOCHS to combine power system scenarios with behaviors of network protocols based on various levels of background traffic, reservation types, and SPS agents to communicate substation behavior, this research proves beneficial to the power industry

as they move forward to develop and implement the communication infrastructure and routing schemes of the utility intranet. A detailed discussion of each of these areas is presented in the next chapter.

Summary

This chapter provided some background information and literature review to help in understanding the problems facing the communication infrastructure of the North American power grid. First, a discussion of the problem set and how the power industry is migrating to a common infrastructure to help stabilize the grid was presented. Next, an overview of TCP and UDP was included because they are the likely transport layer protocols that will be used on the utility intranet. Next, a discussion of some middleware and bandwidth reservations techniques for traffic engineering was detailed. Finally, an overview of this research and how it integrates prior research is given.

III. Methodology

Chapter Overview

The previous two chapters gave an introduction and some background material needed to understand the methodology used to solve this problem set. This chapter explains the methodology used in this research. First, an explanation is given of the different simulators needed for this research. Second, an overview of the IEEE 145-bus 50-generator test case and SPS is given. Third, the types of background traffic used in this research and expected to be found on a utility intranet is explained. Finally, an explanation of the various configurations is given for the 48 different scenarios simulated in this research.

Network Simulator 2

A network simulator is needed to model network traffic on the utility intranet. I have chosen to use NS2 [19] for this research. NS2 was first developed in 1989 and is supported by Defense Advanced Research Projects Agency (DARPA) and National Science Foundation (NSF), in collaboration with other research agencies. NS2 is a discrete event simulator whose target environment is the research community. The simulator provides support for running simulations via TCP/IP and UDP/IP along with multicast protocols over wired and wireless networks. We use NS2 to model the communication requirements that support the infrastructure of an electric power grid.

Power System Simulator for Engineers

PSS/E is a power simulation software package developed by Siemens Corporation in 1976 and has become the most comprehensive, technically advanced, and widely used commercial program of its type. It's a premier power system simulator used by electrical transmission participants worldwide for probabilistic analyses and advanced dynamic modeling capabilities. The simulator provides transmission planning and operation engineers with a broad range of methodologies for use in the design and operation of reliable networks [20]. PSS/E is the power system simulator of choice for this research.

EPOCHS Simulator

Most power simulation tools were built to model power systems of the past which were controlled by large regional power pools without significant communication elements. Power systems are now turning to control and protection systems that take advantage of communication networks. EPOCHS integrates various research and COTS products to successfully model the power grid with communication sharing mechanisms fully integrated [18].

EPOCHS provide a way to simulate load surges, outages, and other forms of stress in realistic scenarios while incorporating communication protocols to facilitate sharing of this information to improve situational awareness. The EPOCHS simulator combines General Electric's (GE) Positive Sequence Load Flow (PSLF) Software [21], Seimen's PSS/E electromechanical transient simulator [22], Power Systems Computer Aided Design (PSCAD) ElectroMagnetic Transients including DC (PSCAD/EMTDC) electromagnetic transient simulator [23], and NS2 [19] created by the University of

California at Berkeley into one federation as shown in Figure 7. This federation of simulators allows electric power engineers the ability to study electrical power and control systems that depend on network communication.

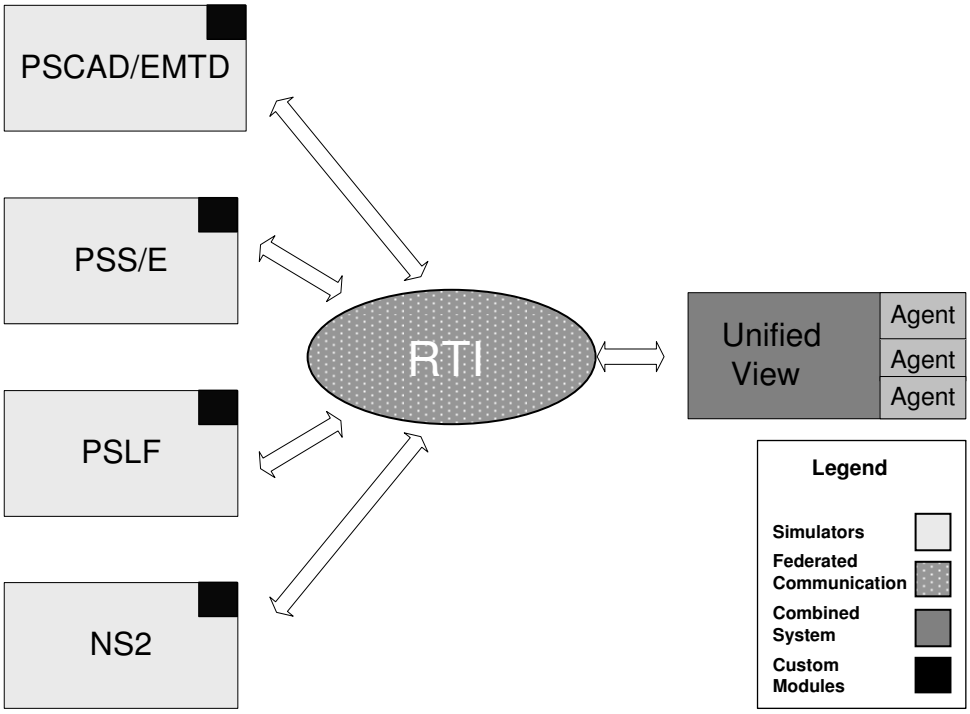

Figure 7. EPOCHS Simulation System

The two simulation components of EPOCHS used for this research are PSS/E and NS2. The hub of EPOCHS that ties the simulators together is its run time infrastructure (RTI). The RTI is responsible for routing messages to other components and ensures time synchronization amongst the different parts of the federation. The RTI ensures that if an event occurs at a certain time in one simulator then it also occurs at the identical time in the other simulators that are a part of the federation. This is crucial because

simulators have a requirement that no event can occur in a simulator that has a time stamp earlier than a time stamp that has already been completed. This requirement is a critical component of EPOCHS since the electric power grid relies heavily upon time sensitive traffic in order to protect the grid against faults.

Once the different simulators have been synchronized to operate together, the users of the system need a way to communicate with the simulators. Synchronization is accomplished through the use of agents. In EPOCHS, agents are computer programs that are autonomous, interactive, and have the ability to communicate over a network. Agents have the ability to interact with each other and their environment on a simulator and can operate on power grids through the use of modern power equipment. Using this definition, an agent headquarters (AgentHQ) presents a unified view to agents and acts as a proxy between the software agents, network simulator, and the power simulator. The AgentHQ is initiated at every synchronization point during the simulation and calls each of the agent's request and action methods giving them the opportunity to calculate their operations for the next time step. The agents used in this research are those contained in the SPS described later.

The protection devices that operate in the electric power grid have traditionally operated and responded to local problems only. The grid has lacked the ability to communicate and have insight into other regions of the grid. This presents problems when information that is needed is not readily available from local devices in order to protect the grid and assist it to operate in a more efficient manner. The autonomous

design of software agents, their ability to share information and coordinate actions has increased the extensibility of the grid without drastically changing its architecture.

In order to support the operation of software agents on the power grid a hardware device is needed that has the computational, communication, and I/O capabilities to meet agent demands. EPOCHS uses agent based intelligent electronic devices (IEDs) for this purpose so software agents can perform the necessary protection and control functions needed. Figure 8 provides a depiction of how agent based IEDs can be employed on a utility intranet. See the IEEE paper by Hopkinson [18] for more details on the EPOCHS simulator.

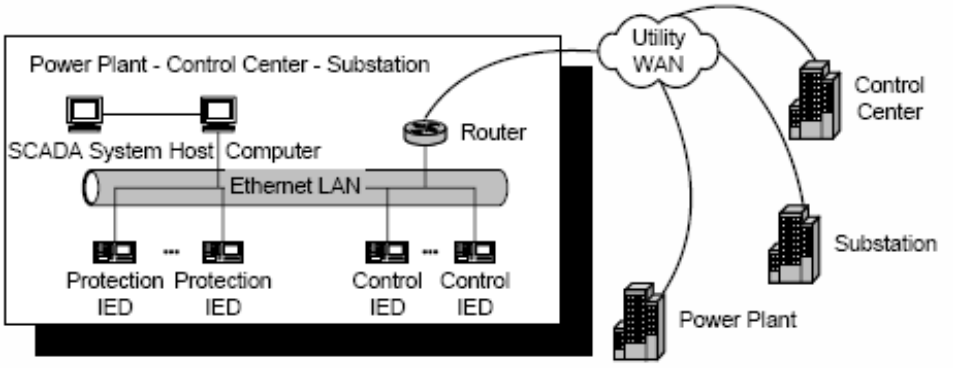

Figure 8. Placement of Agent Based IEDs on a Utility Intranet [10]

Cygwin

In order for NS2, PSS/E, and EPOCHS to operate as a cohesive whole they must be run from a platform compatible with NS2. NS2 requires Linux application programming interface (API) functionality in order to run simulations. In order to provide this functionality on a Windows machine, a virtual machine or other environment

is needed to emulate a Linux operating system. Cygwin meets the bill by providing a Linux-like environment on a Windows 9x/2000/XP operating system.

System Studied

The simulations conducted in this research make use of IEEE's 145-bus 50-generator test case [24]. This 145-bus 50-generator test case has a large share of its generation concentrated in the northeast region and high load concentrated in the southwest region. This test case is a published power system that has been modified to emulate the types of large power flows between areas that are typical in the Western U.S. power grid. Figure 9 provides a visual depiction of the IEEE test case.

The 145-bus 50-generator test case has been modified so it is more representative of a power system that requires SPS protection. The six generators located at buses 93, 104, 105, 106, 110, and 111 are represented with two-axis machine models equipped with IEEE-type AC4 exciters. The remaining 44 generators are represented by classical machine models. Every generator is equipped with basic steam turbines and employs governors with a 5% droop setting. Once the governors have responded, system analysis is performed before new load reference set points are established by the area generation control (AGC) subsystem.

The test case has been modified by adding a 500-kV line from bus 1 to bus 25 in the same corridor as the bus 1 to bus 6 tie line (Figure 10). All lines in the figure are part of the default 145-bus 50-generator test case and the bus 1 to bus 25 branch is the modified portion for this research. This addition is also highlighted by the bus 1 to bus

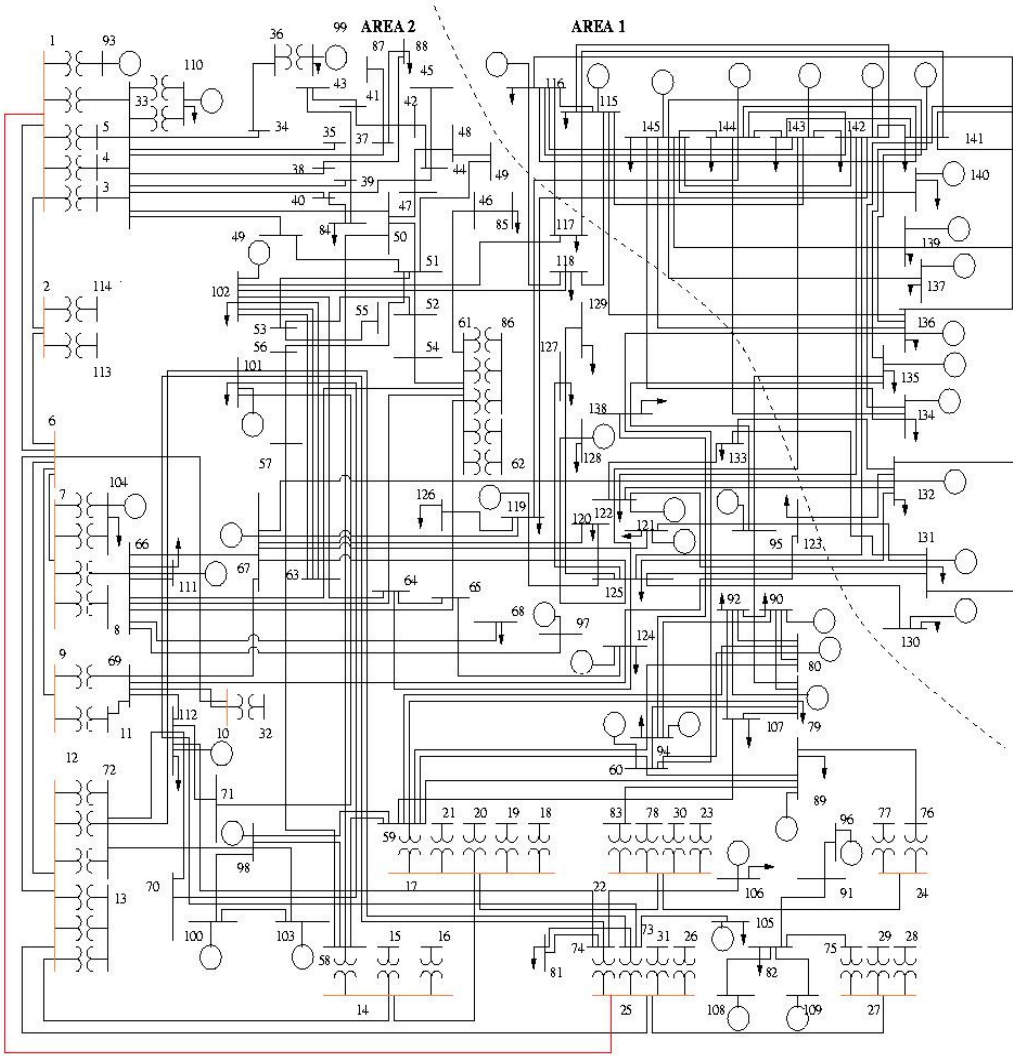

Figure 9. IEEE 145-Bus 50-Generator Test Case

25 branch in Figure 9**.** The addition increases the number of branches in the system from 453 to 454. The intent of the modification is to create a system that requires the use of a SPS in order to maintain system stability. Normally power systems can sustain the lose of one tie line but require quick action by the SPS if a second tie line is lost and not quickly cleared. The IEEE 145-bus 50-generator test case already has one 500-kV tie line that has faulted from bus 1 to bus 6. By causing an additional fault on the 1-25 bus

tie line the power system will quickly become unstable if the SPS doesn't take corrective action immediately. This scenario causes the SPS to generate agent traffic needed for stable operation of the power system and requires a robust communication architecture to ensure timely delivery of agent traffic even in the presence of background traffic.

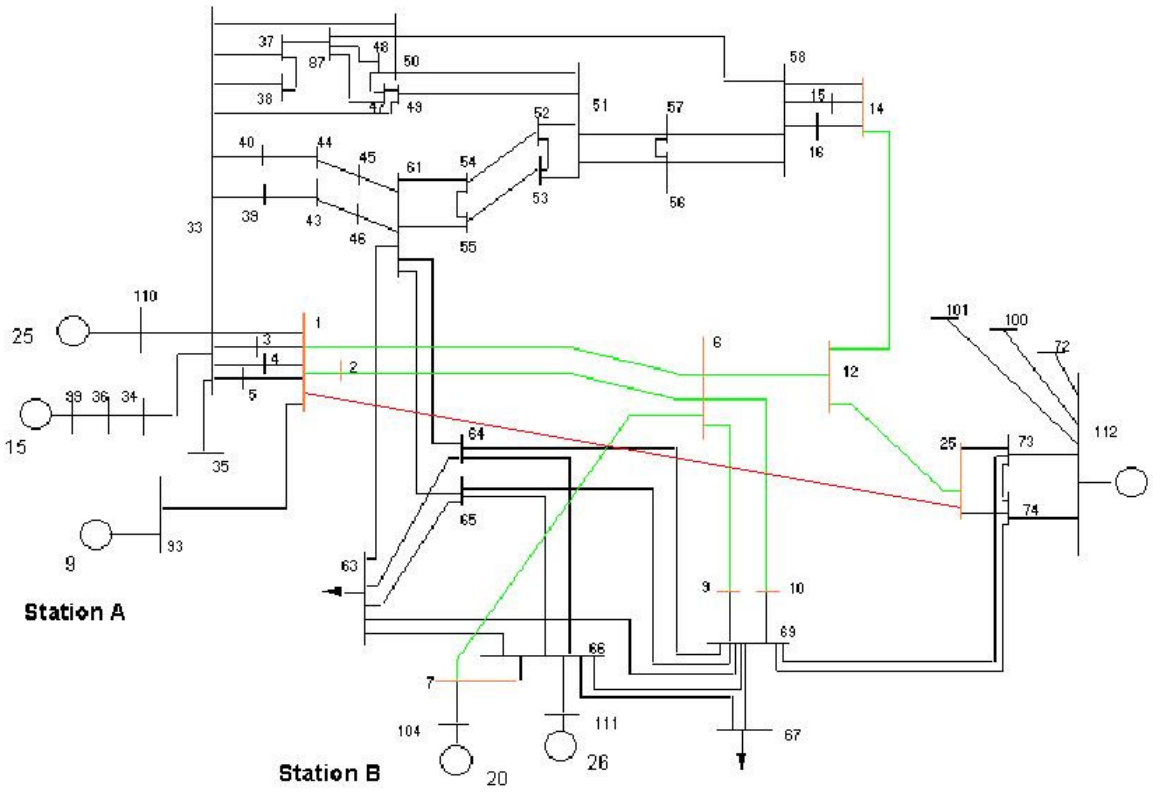

Figure 10. Detailed View of 1-25 Bus Tie Line

Another modification is the total system capacity has been reduced to 30050.00 MW. The lower system capacity makes the 4277 MW power flow along the 500-kV transmission corridor more critical in the modified power system test case than it is was in the original version. This also causes the admittance load to be abnormally high. In

order to correct the admittance load problem, the test case has been rebalanced by setting the percentage of admittance load to 5.02%. The remaining 94.98% of system load had been set to constant active and reactive power.

Whenever two 500-kV tie lines are tripped and the SPS takes action, generation has to be rejected and load shed in order to stabilize the power grid. For the simulations run in this research, it has been determined the generation is taken offline from generator 93 since it directly impacts the 1-25 bus tie line. The various loads are shed from buses 14, 25, 27, 63, and 69 because they are on the load side of generator 93.

SPS Overview

SPS are mechanisms designed to counteract and stabilize power system instability. They are designed to detect one or more predetermined system conditions that have a high probability of causing unusual stress on the power system. If the SPS fails to accurately detect the defined conditions or fails to carry out the required preplanned remedial action, the results can be serious and costly system disturbances [25].

SPS are needed because power system instability usually results in dire consequences covering large areas. A loss of a generator synchronism for a single group of generators with respect to another group of generators results in a transient instability, thus a widespread blackout. Disturbances such as the loss of generation, loads, or tie lines all result in stability problems that stimulate power system electromechanical dynamics. The responses from the system typically involve deviations in frequencies,

voltages, and generator phase angles. The most common SPS in use today employ generation rejection and load shedding [25].

The SPS used in this research is designed to react to a severe line fault in a major extremely high voltage (EHV) line where another outage of a EHV line in the same corridor has already taken place. The goal of the SPS is to prevent instability and preserve the integrity of the power system within a safe operating frequency range. The SPS will shed enough load to keep the power system's frequency above a preset level after a loss of a critical tie line. An algorithm is employed by the SPS that determines the amount of load to shed and generation to drop in order to hold the system's frequency above a preset level based on wide area measurements. The algorithm is explained later.

The SPS is designed for wide area protection and acts in a system oriented manner. It requires synchronized information periodically sampled across the power system. This receipt of this information by the SPS is heavily dependant on the underlying communication infrastructure. The wide area protection systems reliance on the communication infrastructure requires a simulator that implements the functionality of power system and network functionality. The EPOCHS system described earlier is the only platform that provides these combined capabilities. The proposed SPS system has been tested with a modified version of the IEEE 145-bus 50-generator test case. The results show promise for use of a SPS like the one described here in the future. The SPS experiments also show the value of EPOCHS for use in experiments requiring the use of both power system and network simulators.

Algorithm to Estimate Disturbance Size

An algorithm is needed to determine the amount of generation to drop and load to shed to stabilize the power grid after an electromechanical disturbance. The SPS used in this research employs the algorithm shown in Figure 11 for the purpose of calculating system shortfall based on the size of a power system disturbance. It's necessary to determine the exact amount of voltage loss due to a power system disturbance so the load can be shed and generation dropped in a timely manner for grid stabilization.

$$P_d = P_a + \Delta P_e(\omega_{0+} - \omega_{0-}, u_{0+} - u_{0-})$$

Figure 11. Algorithm to Estimate Disturbance Size [18]

P_d is the size of the disturbance and is equal to the system accelerating power, P_a, which is proportionate to the change in the system's frequency, plus the change in electrical power demand ΔP_e due to the variation in frequency and voltage. The time immediately before a disturbance is represented by *0-* and the time immediately after a disturbance is denoted by 0_+. P_d is the key to determining the amount of generation that has been lost. Generation and load agents must send data points to the SPS main agent and action taken within a fraction of a second to prevent power system instability [18]. This requirement makes the underlying communication architecture and routing scheme critical to the successful implementation of the SPS, especially in the presence of competing background traffic.

SPS Architecture

The SPS is required in order for the power system to react rapidly and reliably to electromechanical instabilities. Because generator rejection and load shedding requires fast information updates and rapid response to commands the communication requirements of a SPS are different than those of traditional SCADA systems. SPS is composed of three types of agents: main SPS agent, load agents, and generator agents. In the IEEE 145-bus 50-generator test case, the main SPS agent is location at bus 1, a 500-kV substation. This agent is responsible for identifying extreme contingencies, such as the loss of two tie lines, and performs both generator rejection with preset units and load shedding with real-time measurements. Generators have been chosen for rejection based on simulation studies.

The main SPS agent communicates with generation and load agents to gather information such as data values, including generator's connection status, angular frequencies, active power outputs, and frequency derivatives. The main agent also communicates with agents located at major system and load buses to collect voltage and frequency measurements and the load that's available for shedding.

Generator agents are located at power plants and they send their measurements to the main agent at bus 1 upon request. If requested by the main agent, generator agents will also reject generation. Load agents are mainly location at distribution substations. When requested by the main SPS agent, load agents will shed load. Load agents also perform underfrequency load shedding (UFLS). UFLS can occur if the frequency

reaches a threshold value of 57-58.5 Hz after a remote load shedding scheme with a preset frequency of 58.8 Hz fails to hold the frequency above 58.5 Hz [18].

Background Traffic

Once the utility intranet is operational, it will most likely be utilized for many purposes by the electric power community. Table 2 identifies some of the likely data that will be found on a power industries utility intranet.

The background traffic modeled in this research for a utility intranet is dictated in Table 2. For low traffic loads, the background traffic will consists of white sources only, medium traffic loads will consist of light gray and white traffic sources, and heavy traffic loads will consist of dark gray along with light gray and white traffic sources as depicted in Table 2.

Table 2. Background Traffic Rates [26]

Background Traffic Type	Distribution	Packet Size	Rate
SCADA	Constant	64 Bytes	1 every Second per Bus
Power Quality Data	Poisson	35 Bytes	1 every Second per Bus
UCA 2.0	Poisson	128 Bytes	1 every 20 Seconds per Bus
Power Trading	Constant	1,400 Bytes	1 every 2.2 Seconds per Bus
Internal Comm	Poisson	1 Mbytes	1 every .2 Seconds per Bus
Office – Substation	Poisson	64 Bytes	1every 10 Seconds per Bus
Event Notification	Poisson	2.4 Mbytes	1 every 10 Seconds (Bus chosen at random)

SCADA Data

Higher polling rates due to increased bandwidth available in the new communications infrastructure are a likely reason for SCADA traffic to migrate to a utility intranet. Some types of SCADA data include injections, real and reactive power flows, voltage status, and breaker status. In current systems information is sent from each SCADA device once every three or four seconds.

Power Quality Data

Power quality data is defined as changes in the harmonics of the system. Arc welders, DC inverters and converters, and voltage dips are all types of power system harmonics. A report is produced stating harmonics exist and identifies the harmonics detected.

UCA 2.0 Data

Future power system communications equipment that connects control centers, SCADA masters, and power plants must be compatible with the UCA 2.0 standard. UCA 2.0 compliant devices are still in their infancy so it's too early to know exactly what types of traffic will be generated by these devices. For now we are estimating 128 bytes per packet once every 20 seconds per bus.

Power Trading Data

There is increased interest in the power industry for demand pricing for its customers based on current market conditions. Customers who choose this option will be updated every 5 minutes with the current nodal market price of power. An example of power trading data is a hot water heater. The water heater will receive price data and

based on the price, the water heater decides when to operate and when to remain idle. The exact format isn't currently known but it is expected individual nodal price updates will be less than 100 bytes in size.

Internal Communication Data

Routine day-to-day employee communication is likely to take place on the utility intranet. Types of internal communication include emails, design and blueprint information, and other routine communication between power plants, substations, engineering offices, ISOs, etc. These files can range from a few bytes in size to several megabytes. Internal communication data is strictly on an internal basis and will occur at a significantly lower level than that found on the Internet.

Office-Substation Data

This type of data includes SCADA signals directing buses to take action and commands requesting settings in substations to change values.

Event Notification Data

Data will be sent from event/fault recorders when an event occurs. An example of an event is a lightening strike followed by a series of circuit breakers that trip as a result of the lightening strike. Event data can be very large as compared to other types of traffic on the network. Event traffic is sent after a fault on the system thus doesn't normally interfere with the current situation. When a fault occurs and is followed by another fault the event traffic can quickly interfere will other traffic. This will become apparent when simulations are run with heavy background traffic and events are caused on the system.

Once a utility intranet is operational the types and amount of background traffic may differ significantly from that modeled in Table 2. This was just an attempt to model the background traffic and show how it can impact the functionality of the communication infrastructure when it overwhelms the bandwidth in the presence more critical, time sensitive SPS agent traffic.

Simulation Setup

A total of 48 different simulations were run as laid out in Table 3. Each simulation is based on the amount of background traffic present on the network, if a bandwidth reservation is used and if so, what type (router or middleware), the type of transport layer protocol used, and the routing scheme used in the simulation. Each simulation will be executed 10 times for a total of 480 simulations.

Each of the 480 simulations will be run with bus 1 to bus 6 already tripped. During the simulation another 500-kV branch, which is the 1 bus to 25 bus, will have a fault at time 0.0 and will trip at .078 seconds, at this time agent traffic is generated. The simulation continues to run until the power grid is stabilized.

The bandwidth of each link in the network was set to 1 MB/second. This speed corresponds to the typical DSL connection found in many U.S. households. The propagation delay was set to 0.5 milliseconds per link.

A real-life model of a section of the power grid will be a lot larger than the IEEE 145-bus test case used in this research. To more effectively model a realistic power grid,

Table 3. Experiment Scenarios

Background Traffic Load	Reservation Type	Protocol	Routing Scheme
None	No Reservations	UDP	Shortest Path & PPRN
None	No Reservations	TCP	Shortest Path & PPRN
None	Middleware	UDP	Shortest Path & PPRN
None	Middleware	TCP	Shortest Path & PPRN
None	Router Reservations	UDP	Shortest Path & PPRN
None	Router Reservations	TCP	Shortest Path & PPRN
Light	No Reservations	UDP	Shortest Path & PPRN
Light	No Reservations	TCP	Shortest Path & PPRN
Light	Middleware	UDP	Shortest Path & PPRN
Light	Middleware	TCP	Shortest Path & PPRN
Light	Router Reservations	UDP	Shortest Path & PPRN
Light	Router Reservations	TCP	Shortest Path & PPRN
Medium	No Reservations	UDP	Shortest Path & PPRN
Medium	No Reservations	TCP	Shortest Path & PPRN
Medium	Middleware	UDP	Shortest Path & PPRN
Medium	Middleware	TCP	Shortest Path & PPRN
Medium	Router Reservations	UDP	Shortest Path & PPRN
Medium	Router Reservations	TCP	Shortest Path & PPRN
Heavy	No Reservations	UDP	Shortest Path & PPRN
Heavy	No Reservations	TCP	Shortest Path & PPRN
Heavy	Middleware	UDP	Shortest Path & PPRN
Heavy	Middleware	TCP	Shortest Path & PPRN
Heavy	Router Reservations	UDP	Shortest Path & PPRN
Heavy	Router Reservations	TCP	Shortest Path & PPRN

the settings for background traffic were set to those shown in Table 4. These settings are needed to model a larger area of the power grid and to ensure we generate enough traffic to show a variation in results of the different scenarios. The formula (new idle time = 1000/(any number)). In this research the any number is 125, so each node in the test case actually represents 125 nodes on the power grid. As shown in Table 4, the

Table 4. Background Traffic Settings

Traffic Type	Time Between Bursts in MS Old Value / New Value
SCADA	1000 / 8
Power Quality Data	1000 / 8
UCA 2.0	20000 / 160
Power Trading	2200 / 18
Internal Comm	200 / 2
Office – Substation	10000 / 80
Event Notification	10000 / 50

old value is divided by 125 to get the new idle time for the traffic type. As the idle time goes down, a larger power grid is simulated. In this research the simulated power grid is representative of a (145 * 125) 18,125-bus power grid. Several modifications were tested in order to get the simulations to show enough variation from one background load to the next. The event packet size also had to be changed to 175 bytes along with a 50 ms idle time to generate enough traffic in order to ensure we showed enough of a difference in results when run with heavy background traffic versus middle background traffic.

Background Traffic Load

The real test of a utility intranet is how it performs under stress. In order to test this theory this research has been divided into four basic scenarios based on the level of background traffic present. As shown in Table 3, there are four basic scenarios being tested. The first scenario is run with no background traffic, followed by the second scenario with light background traffic, then the third scenario with medium background traffic, and the last scenario with heavy background traffic.

Reservation Type

The four basic scenarios are further broken down based on the type of reservation scheme used. Each background traffic level is simulated with no reservations, reservations through the middleware, and reservations through routers on the network. It's assumed the middleware reservation system has imperfect knowledge of traffic on the network so 5% more traffic may appear and bypass the middleware system than was anticipated, where router reservations have perfect knowledge of traffic on the network. When middleware and router reservations were used, NS2's internal routing algorithm was modified to allow us to select a packet's destination based on flow ID. Protection traffic was given a high priority and ran over reserved channel space while background traffic was given a low priority and ran over unreserved space. When no reservations were used the simulation used NS2's default internal algorithm and all traffic had the same priority.

Reservations made through routers and middleware are created based on their flow-ID. All reservations are 2 MB in size and go from bus 1 (where main SPS agent is located) to each of the 50 generators and from bus 1 to the 5 buses were the loads to be shed during the simulations are located. The reservations are repeated in the reverse direction so all flows are full duplex for a total of 110 reservations.

Other reservation protocols like RSVP [27] and MPLS [28] have been used to reserve bandwidth for time critical applications, but these protocols reserve bandwidth in networks that can only be used by the traffic the bandwidth was reserved for and no other. When the reservation is not being used by the reservation party, the bandwidth is

wasted. In this research reservation bandwidth is available for background traffic to use when agent traffic doesn't actively using the reservation. When agent traffic is sent over its reservation and background traffic is present and the queue is full, it overrides the background traffic and enough background traffic is dropped to ensure room at the end of the queue for agent traffic. If there is already room in the queue the agent traffic will go to the back of the queue. Background traffic will not be allowed further use of the reservation unless there is sufficient capacity to process all agent traffic in the queue. The behavior of the queues is described later.

Transport Layer Protocol

To allow us the ability to compare the performance of protocols, each background traffic level and reservation type is simulated using both TCP/IP and UDP/IP transport layer protocols. TCP is reliable, but doesn't perform well in time sensitive situations. UDP is inherently unreliable, but can be more suited when time is of an essence. The protocols and their functionality were described in Chapter II.

It's critical that all agent traffic is accounted for, which is a problem with unreliable protocols like UDP. To overcome this shortfall, UDP scenarios were modified so all agent traffic is resent every 2 ms until the source receives an acknowledgment message back from the destination. UDP was modified so it sends acknowledgements back to the source for all agent traffic. These modifications ensure the same reliability standards as TCP.

It's important to note that background traffic always uses UDP while agent traffic uses either UDP or TCP based on the simulation type. When running simulations and

background traffic exists, we always want the background traffic to stay at the light, medium, or heavy traffic loads during the entire simulation. If TCP were used then the background traffic would throttle down when congestion was encountered on the network.

Routing Scheme

Each background traffic level, reservation type, and transport layer protocol is simulated with both shortest path and PPRN routing schemes for a total of 48 different scenarios. The shortest path routing scheme used is the Floyd-Warshall Algorithm. A single execution of the algorithm will find the shortest path between all vertices on a weighted, directed graph. It compares all possible paths through a graph between each set of vertices and incrementally improves the estimate of the shortest path between two vertices until the estimate is known to be optimal [29].

The other routing algorithm used in the simulations is the PPRN multicommodity network flow solver [30]. PPRN was developed in the Statistics and Operations Research Department at Universitat Politecnica de Catalunya, Barcelona Spain as a way to calculate how to allocate bandwidth reservations in a network through the use of network flows. Multicommodity flows are fast, relatively simple, and can be conveniently applied to ensure reservations will be available to critical traffic and guard against interruption from less important data sources.

Queues

As background traffic increases on the network, we eventually exceed the amount of traffic the routers can process, thus some traffic will have to be dropped or the

simulation will come to a halt. When no reservations are used the traffic is dropped from the queue using the drop tail method. This method is a first-in-first-out queue where the packet in the back of the waiting list is dropped once the queue is overflowed. For this research, queue sizes were set to 260 packets.

When the system uses reservations, a different approach is used based on reservation type. For router reservations, packets with a flow ID of 0 (background traffic) are chosen at random and dropped from the queue. If there is no background traffic left and the queue is full of agent traffic, then packets with a flow ID ≥ 1 (agent traffic) are randomly chosen and dropped. Middleware reservations work similar to router reservations except for the fact middleware is not aware of 5% of the traffic on the network. That being stated, long as agent and background traffic are present in the queue, agent traffic has a 5% change of being chosen to drop and background traffic a 95% change of being dropped. Based on this concept, as traffic loads increase, router reservations should be more efficient than middleware reservations.

Summary

This chapter began by giving an overview of the different simulators needed to allow us to conduct this research. Next, an overview of the IEEE 145-bus 50-generator test case and SPS used in this research was given. Next, a description of the different types of background traffic that can be expected to be found on a utility intranet is presented. Lastly, a detailed view of how the simulations are configured and setup was given. Chapter IV will go over the results of the simulations and outline some of the key findings from the 48 different scenarios that were tested.

IV. Analysis and Results

Chapter Overview

This chapter provides a detailed explanation of the results of the simulations run based on the methodology described in Chapter III. The results from each set of simulations are presented based on the routing scheme used. Simulations using the Floyd Warshall Shortest Path algorithm is presented followed by simulation results using the PPRN generated routing scheme. Next, the two schemes are compared to show how they differ. Finally, an explanation is given explaining the various differences in run times because of background traffic loads. All findings presented are analyzed and interpreted, and conclusions drawn based on analysis of results.

Several abbreviations have been used throughout Chapter IV. Those abbreviations are explained below:

NR = No Reservations
MR = Middleware Reservations
RR = Router Reservations
NBG = No Background Traffic
LBG = Light Background Traffic
MBG = Medium Background Traffic
HBG = Heavy Background Traffic
NR/UDP = No Reservations/User Datagram Protocol
NR/TCP = No Reservations/Transmission Control Protocol
MR/UDP = Middleware Reservations/User Datagram Protocol
MR/TCP = Middleware Reservations/Transmission Control Protocol
RR/UDP = Router Reservations/User Datagram Protocol
RR/TCP = Router Reservations/Transmission Control Protocol

Floyd Warshall Shortest Path Scenarios

The overwhelming result of all simulations is UDP scenarios ran quicker than TCP scenarios, as shown in Figure 12. This is a result of the congestion control mechanism inherent to TCP and the modifications made to UDP to ensure reliability of packet delivery. As the background traffic increases the simulation run time also increases. This is especially true with TCP since congestion control increasingly becomes a factor as the queues become overwhelmed at certain nodes.

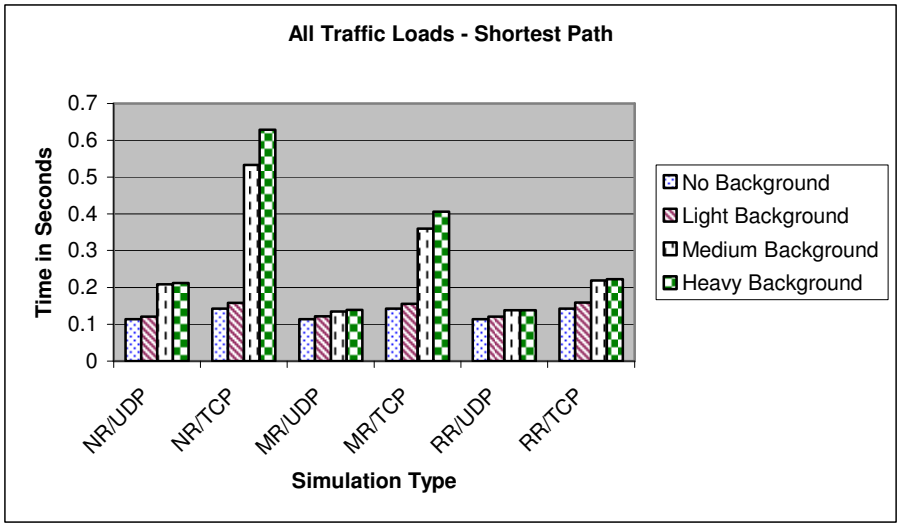

Figure 12. Scenario Comparison for Shortest Path Simulations

UDP Shortest Path Scenarios

Reservation type played a key role in determining how long each simulation ran as background traffic levels increased. Background traffic levels increased the simulation run times because of the congestion it caused on the network. As shown in Figure 13, the reservation type didn't matter much until the network reached middle and heavy

background traffic levels. At that point the middleware and router reservations were more efficient. As traffic levels increased, the middleware and router reservations were 74 ms faster on average than simulations run with no reservations.

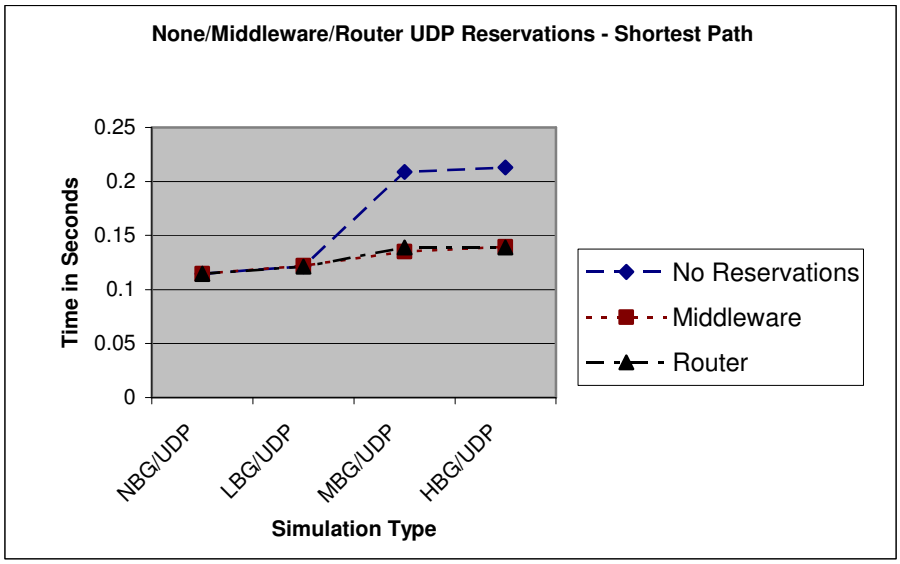

Figure 13. UDP Reservations for Shortest Path Scenarios

The difference in simulation times is the likely result of competing traffic on the links and inefficient routing schemes when no reservations are used. When reservations were used, the agent traffic was given a priority over background traffic and less likely dropped. With the no reservation scheme, agent traffic is dropped if the queue is full when it arrives versus background traffic being dropped and agent traffic being allowed into the queue. Agent traffic doesn't have a reservation and its priority is the same as background traffic thus the longer run times. There wasn't much difference in the middleware and router reservation schemes. The likely cause is UDP lack of congestion control and the modification that guarantees delivery of packets. So the middleware

approach of having a 5% chance of dropping agent traffic when agent and background traffic are in the queue and the queue is full didn't play a significant role. When agent traffic was dropped, it was quickly retransmitted and didn't have to wait since UDP transmits packets as quickly as possible.

Table 5 displays the average load shed and standard deviation for each of the shortest path scenarios. It important to note that with the bandwidth allocated, there was sufficient bandwidth to accommodate all traffic so there wasn't much congestion or dropped packets with simulations not containing background traffic. This resulted in all no background traffic scenarios running the same amount of time. As more background traffic is generated, run time is longer and amount of load that's shed from the power grid varies thus a higher standard deviation. On average, the longer it takes the SPS to get all required data to make a decision the more unreliable its estimate of the amount of load to shed. If more trials for each simulation were run the standard deviations should be more consistent with this theory.

Table 6 lists the average amount of load shed per bus as compared to the average convergence time (explained later) for each scenario type. All simulation types averaged between 16% and 19% of their total load being shed. Simulations run using UDP shed less load per bus on average than simulations run using TCP. The difference can be attributed to the faster convergence time of UDP thus more accurate information to make decisions. It's important to note that all UDP simulations for a particular background traffic load typically converges at the same time and it is also the case for TCP simulations run with no and light background traffic loads. For UDP simulations, the

similar times can be attributed to the SPS getting the required information quick enough to make a decision before the network gets congested with background traffic. Once the SPS makes a decision the network begins to get congested and the final run times will vary as the background traffic load increases. The convergence time in all scenarios for bus 25 is always before the rest of the buses because bus 25 has a direct link to the main SPS agent at bus 1, thus less congestion to deal with and quicker responses.

Table 5. Load Shed in MW for Shortest Path Routing Scenarios

Simulation Type	Average	Standard Deviation	Simulation Type	Average	Standard Deviation
NBG/NR/UDP	879.43	0.00	MBG/NR/UDP	879.89	1.34
NBG/NR/TCP	960.84	0.00	MBG/NR/TCP	953.61	10.43
NBG/MR/UDP	879.43	0.00	MBG/MR/UDP	905.55	47.17
NBG/MR/TCP	960.84	0.00	MBG/MR/TCP	954.84	8.98
NBG/RR/UDP	879.43	0.00	MBG/RR/UDP	890.70	5.29
NBG/RR/TCP	960.84	0.00	MBG/RR/TCP	954.97	11.96
LBG/NR/UDP	880.53	1.17	HBG/NR/UDP	879.81	1.70
LBG/NR/TCP	954.12	1.46	HBG/NR/TCP	954.17	10.11
LBG/MR/UDP	880.43	2.03	HBG/MR/UDP	914.74	33.25
LBG/MR/TCP	953.48	3.23	HBG/MR/TCP	957.99	12.48
LBG/RR/UDP	879.67	0.69	HBG/RR/UDP	886.99	5.18
LBG/RR/TCP	952.69	2.69	HBG/RR/TCP	947.44	28.42

Convergence time is the time the SPS main agent at bus 1 receives all the data it needs to make a decision on how much load to shed and which buses to shed load from. Table 6 lists the average convergence time for each scenario type. The longer it takes for

the SPS to converge, the less accurate the information needed to make decisions. When the average convergence time is within a few milliseconds the percent shed may vary slightly but not enough to make a significant difference. More simulations are needed to prove longer simulation run times result in a greater percentage of load shed per bus.

Table 6. Per Bus Comparison of Convergence Time and Percent Load Shed – Shortest Path

Convergence Time / NBG	**NR/UDP**	**NR/TCP**	**MR/UDP**	**MR/TCP**	**RR/UDP**	**RR/TCP**
	0.112 ms	**0.140 ms**	**0.112 ms**	**0.140 ms**	**0.112 ms**	**0.140 ms**
Bus 14	17.14%	18.73%	17.14%	18.73%	17.14%	18.73%
Bus 25	16.89%	18.50%	16.89%	18.50%	16.89%	18.50%
Bus 27	17.17%	18.73%	17.17%	18.73%	17.17%	18.73%
Bus 63	17.17%	18.73%	17.17%	18.73%	17.17%	18.73%
Bus 69	17.17%	18.73%	17.17%	18.73%	17.17%	18.73%
Convergence Time / LBG	**NR/UDP**	**NR/TCP**	**MR/UDP**	**MR/TCP**	**RR/UDP**	**RR/TCP**
	0.116 ms	**0.156 ms**	**0.117 ms**	**0.156 ms**	**0.115 ms**	**0.156 ms**
Bus 14	17.16%	18.60%	17.16%	18.58%	17.14%	18.57%
Bus 25	16.91%	18.37%	16.91%	18.36%	16.90%	18.34%
Bus 27	17.19%	18.60%	17.19%	18.59%	17.17%	18.57%
Bus 63	17.19%	18.60%	17.19%	18.59%	17.17%	18.57%
Bus 69	17.19%	18.60%	17.19%	18.59%	17.17%	18.57%
Convergence Time / MBG	**NR/UDP**	**NR/TCP**	**MR/UDP**	**MR/TCP**	**RR/UDP**	**RR/TCP**
	0.124 ms	**0.343 ms**	**0.124 ms**	**0.284 ms**	**0.124 ms**	**0.208 ms**
Bus 14	17.15%	18.59%	17.65%	18.61%	17.36%	18.62%
Bus 25	16.90%	18.36%	17.39%	18.38%	17.11%	18.39%
Bus 27	17.18%	18.59%	17.68%	18.61%	17.39%	18.62%
Bus 63	17.18%	18.59%	17.68%	18.62%	17.39%	18.62%
Bus 69	17.18%	18.59%	17.68%	18.62%	17.39%	18.62%
Convergence Time / HBG	**NR/UDP**	**NR/TCP**	**MR/UDP**	**MR/TCP**	**RR/UDP**	**RR/TCP**
	0.127 ms	**0.395 ms**	**0.127 ms**	**0.339 ms**	**0.125 ms**	**0.209 ms**
Bus 14	17.15%	18.60%	17.83%	18.68%	17.29%	18.47%
Bus 25	16.90%	18.38%	17.57%	18.44%	17.04%	18.23%
Bus 27	17.18%	18.60%	17.86%	18.68%	17.32%	18.48%
Bus 63	17.18%	18.60%	17.86%	18.68%	17.32%	18.48%
Bus 69	17.18%	18.60%	17.86%	18.68%	17.32%	18.48%

Figure 14, Figure 15, Figure 16, and Figure 17 show the average completion time as compared to the average convergence time for each of the four UDP scenario types. As expected, the average convergence time always occurs before the average completion time. Once the SPS had converged, it still communicates its decision to the other generation and load agents distributed throughout the power grid that are affected by its decision, thus the longer completion times. One point worth noting is with the no reservation scenarios. As the traffic level increases, the difference in convergence time versus completion time begins to increase in greater amounts than it does with middleware and router reservations. The likely cause is the increased levels of background traffic on the network combined with agent traffic not getting priority treatment as it does with middleware and router reservations, thus more dropped agent traffic causing longer simulation run times.

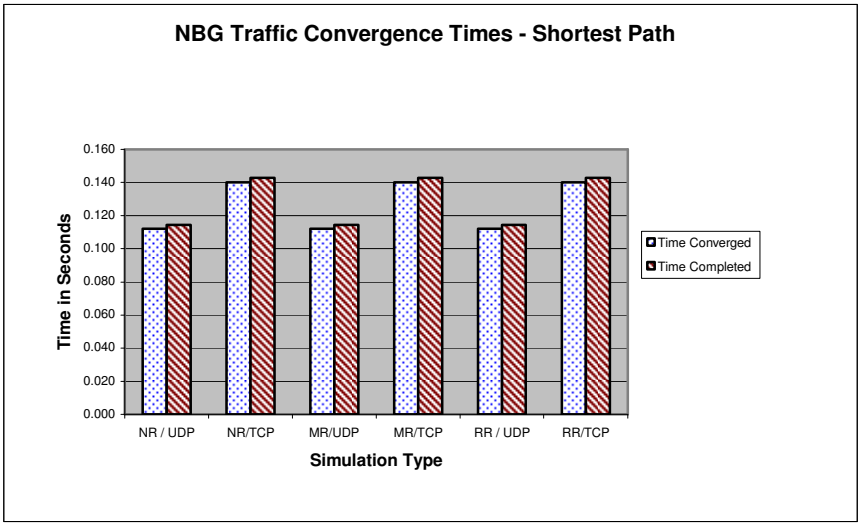

Figure 14. NBG Traffic Convergence Times for Shortest Path Scenarios

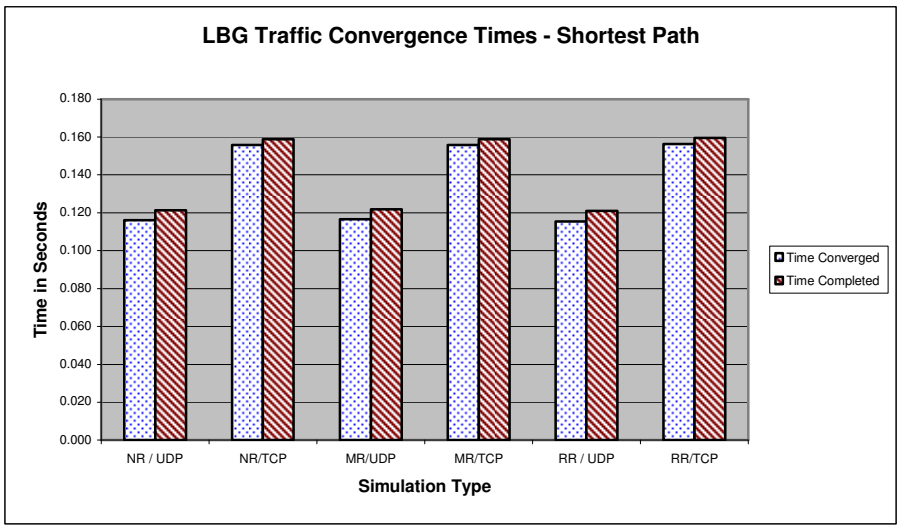

Figure 15. LBG Traffic Convergence Times for Shortest Path Scenarios

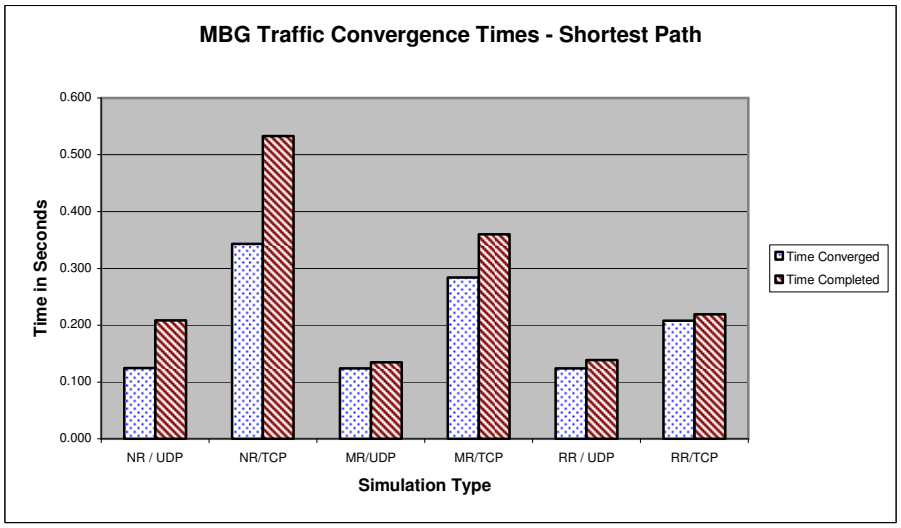

Figure 16. MBG Traffic Convergence Times for Shortest Path Scenarios

TCP Shortest Path Scenarios

Simulations running TCP ran longer than UDP scenarios across all background traffic loads. Many of the patterns mentioned in the previous section were repeated in the

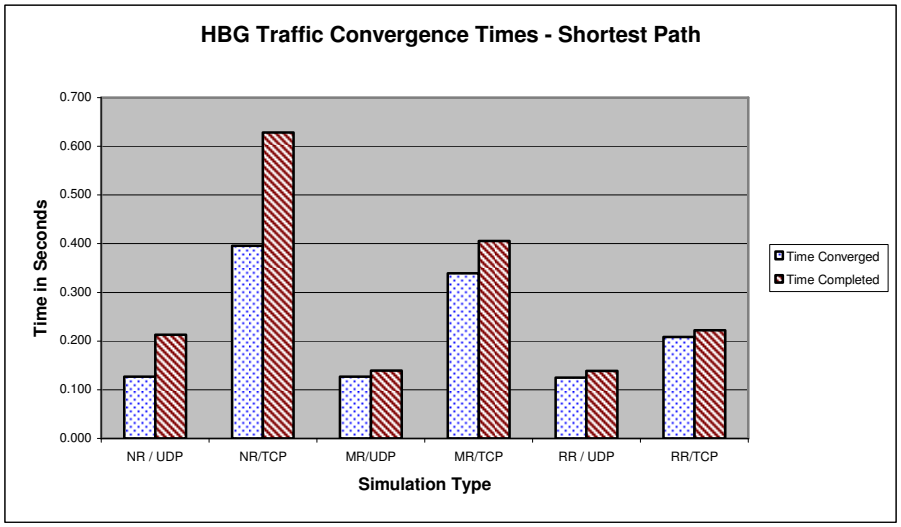

Figure 17. HBG Traffic Convergence Times for Shortest Path Scenarios

TCP scenarios. I concentrate on the differences between the two protocols. Figure 18 shows the pattern of behavior for the TCP scenarios.

Unlike UDP were there wasn't a significant difference between middleware and router reservations, there was a noticeable difference in all reservation types with medium and heavy background traffic loads. Router reservations ran on average 183 ms faster than middleware reservations and 406 ms faster than no reservation scenarios with a heavy background traffic load. Since routers have insight to all agent traffic on the network they help ensure faster running times in both UDP and TCP scenarios. The difference in router and middleware reservation run times in TCP and UDP scenarios can again be attributed to the congestion control mechanism inherent to TCP.

The percent of load shed per bus was greater in TCP scenarios as shown in Table 6. Since TCP scenarios ran longer on average than UDP scenarios the amount of load

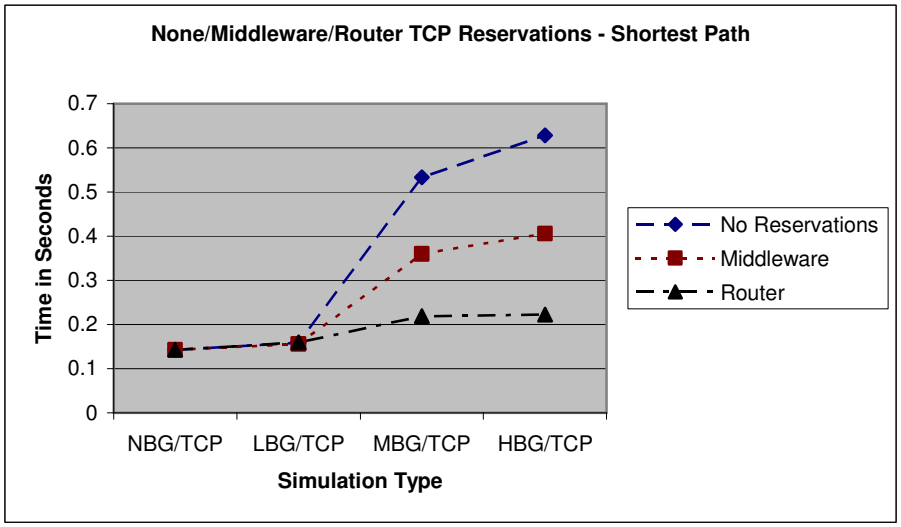

Figure 18. TCP Shortest Path Scenarios

shed was usually greater because the information wasn't as accurate. This is caused by the delay in data getting from the main SPS agent to the load and generation agents and back. The result was convergence times greater in TCP scenarios than their UDP counterpart (see Figure 14, Figure 15, Figure 16, and Figure 17).

Convergence time in TCP scenarios with no and light background traffic vary little because the congestion control mechanism isn't engaged often enough until the network gets congested and that doesn't happen until the background traffic reaches the medium and heavy levels. This also causes the completion time in medium and heavy traffic loads to increase dramatically with no and middleware reservations.

PPRN Multicommodity Flow Solver Scenarios

Scenarios using the PPRN routing scheme also converged and ran faster when using UDP versus TCP, as shown in Figure 19. Just like the shortest path simulations, as

the background traffic increased the simulation run time also increased. This was emphasized the most when no reservations were used.

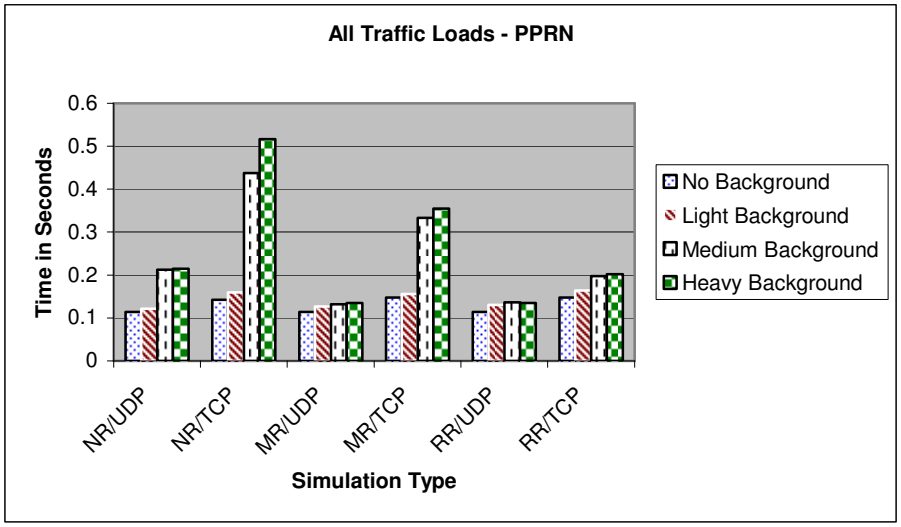

Figure 19. Scenario Comparison for PPRN Simulations

UDP PPRN Scenarios

The difference in middleware and router reservations was negligible in performance using PPRN just as they were with the shortest path scenarios. Figure 20 displays the average completion time for all PPRN UDP simulations. The difference was insignificant in all reservation schemes run with no and light background traffic because the bandwidth was sufficient to handle the traffic load. As the background traffic level increases to medium and heavy loads the middleware and router reservations run about 79 ms faster than with no reservations.

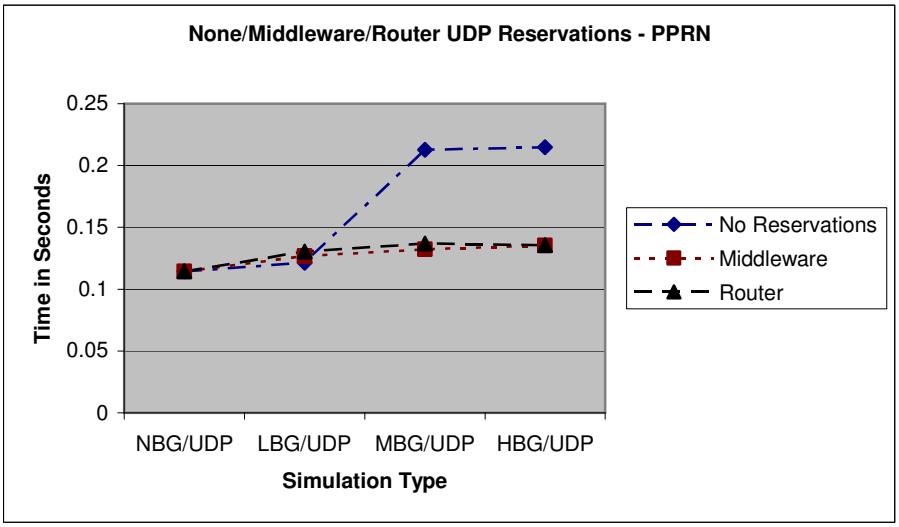

Figure 20. UDP Reservations for PPRN Scenarios

Table 7. Load Shed in MW for PPRN Routing Scenarios

Simulation Type	Average	Standard Deviation	Simulation Type	Average	Standard Deviation
NBG/NR/UDP	879.43	0.00	MBG/NR/UDP	881.71	1.62
NBG/NR/TCP	960.84	0.00	MBG/NR/TCP	954.31	11.08
NBG/MR/UDP	910.63	0.00	MBG/MR/UDP	967.06	60.06
NBG/MR/TCP	1040.00	0.00	MBG/MR/TCP	1073.22	6.84
NBG/RR/UDP	910.63	0.00	MBG/RR/UDP	972.74	66.38
NBG/RR/TCP	1040.00	0.00	MBG/RR/TCP	1081.12	11.97
LBG/NR/UDP	879.87	0.93	HBG/NR/UDP	882.25	2.78
LBG/NR/TCP	952.26	2.76	HBG/NR/TCP	954.83	8.39
LBG/MR/UDP	941.84	29.89	HBG/MR/UDP	977.07	72.23
LBG/MR/TCP	1038.03	11.16	HBG/MR/TCP	1084.70	9.08
LBG/RR/UDP	956.55	49.52	HBG/RR/UDP	939.24	33.83
LBG/RR/TCP	1038.72	6.63	HBG/RR/TCP	1085.71	9.75

Table 7 shows the average load shed for each simulation type and the standard deviation for the values. Agent traffic ran unimpeded in the no background traffic scenarios so all simulations ran in identical times. For several simulation types the longer the simulation ran the standard deviation increased. This was not the case across the board and it can most likely be attributed to only running 10 simulations per configuration. If more simulations were run, I think the difference in standard deviations would be more consistent with run times. There would likely be more variance in standard deviation times as the simulation run time increases.

Some of the standard deviations in Table 5 and Table 7 are significantly larger than other standard deviations. While the run times were consistent, the standard deviations for the amount of load shed seem to be out of range for simulations with similar run times. The high standard deviation is usually caused by one simulation shedding a lot more load than the other simulations run with the same configurations. The difference can be attributed the SPS algorithm. The algorithm may not be operating optimally for all simulations and may need tuning.

As shown in Table 8, UDP scenarios shed less load thus less percentage per bus than TCP scenarios. Just as with the shortest path scenarios, this can be attributed to the faster convergence times of UDP versus TCP simulations.

Figure 21, Figure 22, Figure 23, and Figure 24 show the average convergence time compared to the completion time for each scenario type. Again, the average completion time is always greater than the average convergence time and router

Table 8. Per Bus Comparison of Convergence Time and Percent Load Shed – PPRN

Convergence Time / NBG	**NR/UDP**	**NR/TCP**	**MR/UDP**	**MR/TCP**	**RR/UDP**	**RR/TCP**
	0.112 ms	**0.140 ms**	**0.11 ms**	**0.144 ms**	**0.11 ms**	**0.144 ms**
Bus 14	17.14%	18.73%	17.75%	20.27%	17.75%	20.27%
Bus 25	16.89%	18.50%	17.49%	20.02%	17.49%	20.02%
Bus 27	17.17%	18.73%	17.78%	20.28%	17.78%	20.28%
Bus 63	17.17%	18.73%	17.78%	20.28%	17.78%	20.28%
Bus 69	17.17%	18.73%	17.78%	20.28%	17.78%	20.28%
Convergence Time / LBG	**NR/UDP**	**NR/TCP**	**MR/UDP**	**MR/TCP**	**RR/UDP**	**RR/TCP**
	0.115 ms	**0.156 ms**	**0.113 ms**	**0.152 ms**	**0.115 ms**	**0.160 ms**
Bus 14	17.15%	18.56%	18.35%	20.23%	18.64%	20.25%
Bus 25	16.90%	18.33%	18.09%	19.99%	18.37%	20.00%
Bus 27	17.18%	18.56%	18.39%	20.24%	18.67%	20.25%
Bus 63	17.18%	18.57%	18.39%	20.24%	18.68%	20.25%
Bus 69	17.18%	18.57%	18.39%	20.24%	18.68%	20.25%
Convergence Time / MBG	**NR/UDP**	**NR/TCP**	**MR/UDP**	**MR/TCP**	**RR/UDP**	**RR/TCP**
	0.126 ms	**0.304 ms**	**0.120 ms**	**0.274 ms**	**0.121 ms**	**0.183 ms**
Bus 14	17.18%	18.60%	18.85%	20.92%	18.96%	21.07%
Bus 25	16.93%	18.37%	18.57%	20.66%	18.68%	20.82%
Bus 27	17.21%	18.60%	18.88%	20.92%	18.99%	21.07%
Bus 63	17.21%	18.61%	18.88%	20.92%	18.99%	21.08%
Bus 69	17.21%	18.61%	18.88%	20.92%	18.99%	21.08%
Convergence Time / HBG	**NR/UDP**	**NR/TCP**	**MR/UDP**	**MR/TCP**	**RR/UDP**	**RR/TCP**
	0.126 ms	**0.344 ms**	**0.121 ms**	**0.221 ms**	**0.121 ms**	**0.187 ms**
Bus 14	17.20%	18.61%	18.75%	21.15%	18.31%	21.16%
Bus 25	16.94%	18.38%	18.48%	20.88%	18.04%	20.91%
Bus 27	17.22%	18.61%	18.78%	21.15%	18.34%	21.16%
Bus 63	17.22%	18.62%	18.78%	21.15%	18.34%	21.16%
Bus 69	17.22%	18.62%	18.78%	21.15%	18.34%	21.16%

reservations are more consistent across all background traffic loads. With no reservation scenarios the difference between convergence time and completion time tends to increases as the traffic level increases but with middleware and router reservations the time difference varies little. This is attributed to the fact middleware and router

reservations have more complete knowledge of all traffic types on the network, thus are less likely to drop agent traffic needed to stabilize the grid.

TCP PPRN Scenarios

As shown in Figure 19, TCP scenarios ran longer than UDP scenarios across all background traffic loads. This is the expected outcome since it follows the logic presented earlier for shortest path scenarios. Figure 25 shows the average run time for all TCP simulations. Simulations containing no and light background traffic completed in similar times because enough traffic wasn't generated to enable the benefits of using middleware and router reservations. As background traffic levels reach medium and heavy loads, router reservations clearly show they are more efficient than middleware reservations and middleware reservations are more efficient than simulations

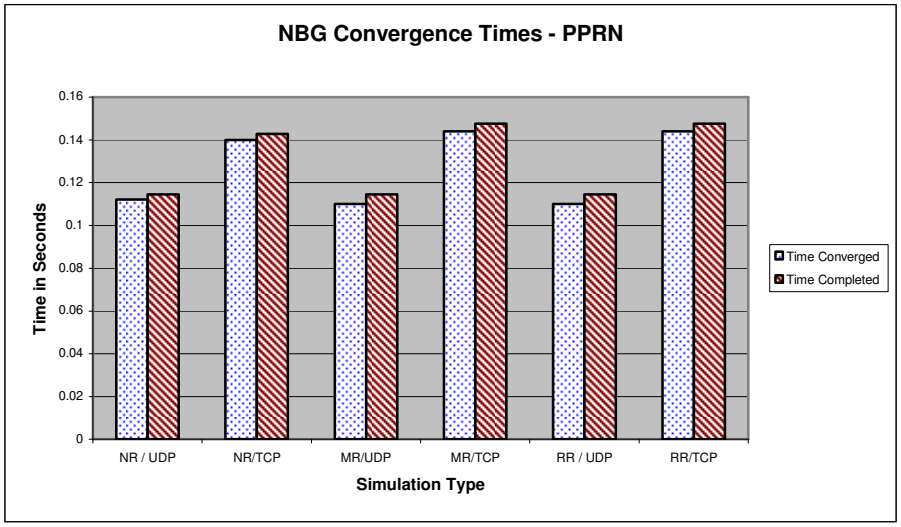

Figure 21. NBG Traffic Convergence Times for PPRN Scenarios

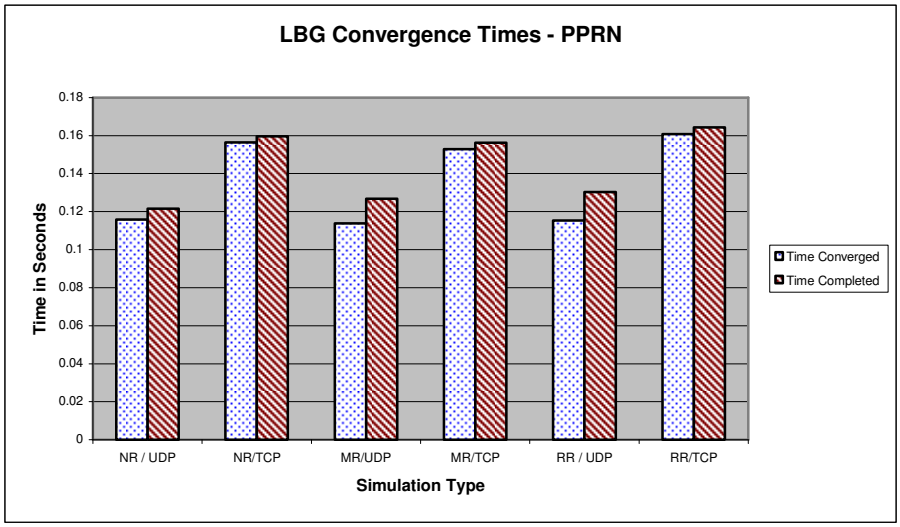

Figure 22. LBG Traffic Convergence Times for PPRN Scenarios

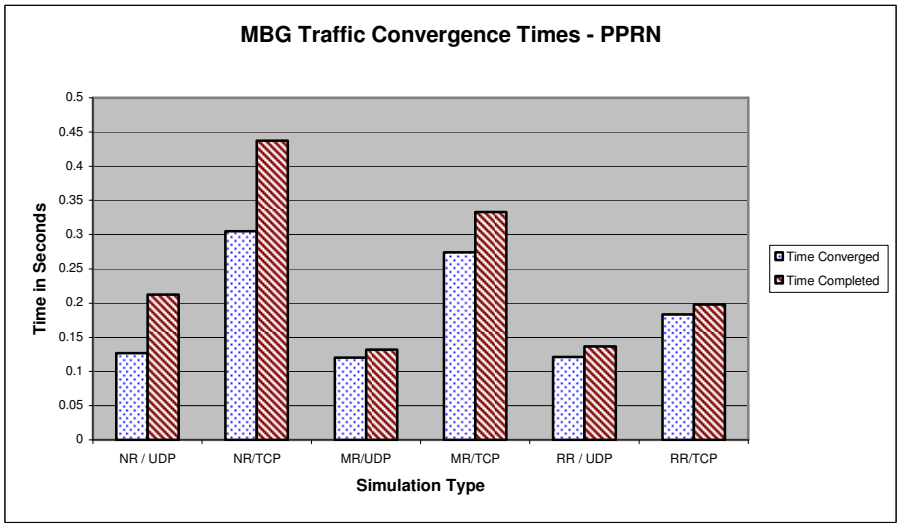

Figure 23. MBG Traffic Convergence Times for PPRN Scenarios

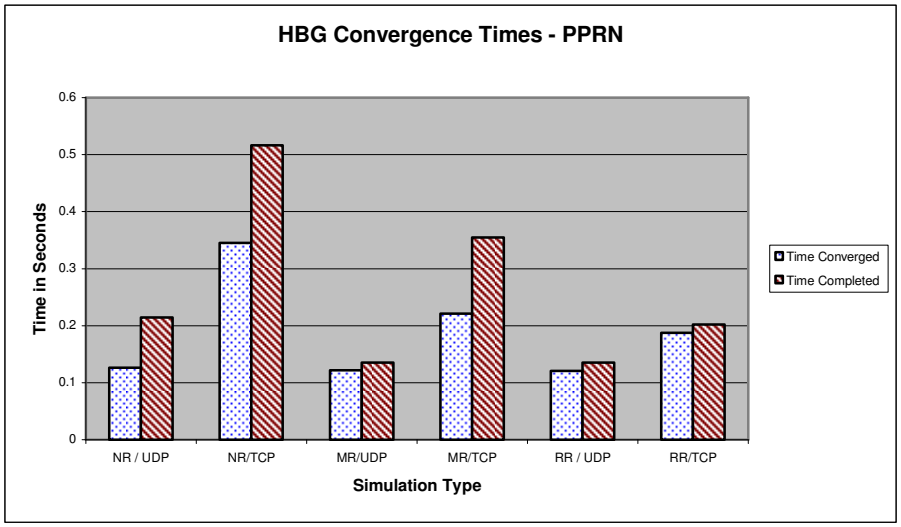

Figure 24. HBG Traffic Convergence Times for PPRN Scenarios

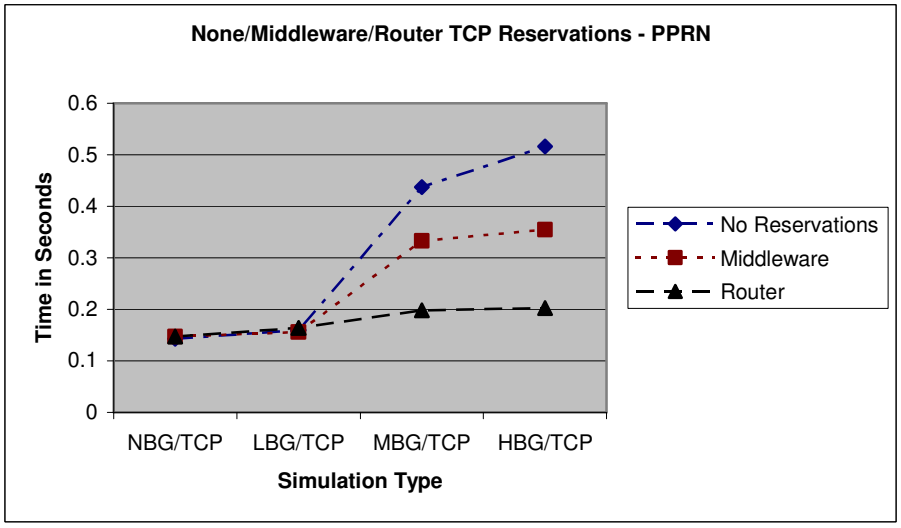

Figure 25. TCP Reservations for PPRN Scenarios

run with no reservations. Router reservations ran 152 ms faster than middleware reservations and 314 ms faster than no reservation simulations with a heavy background traffic load.

As the background traffic load increases for each simulation type (e.g. router reservation scenarios with no/light/medium/heavy background traffic loads) the amount of load shed per bus is greater (Table 8). While not consistent across the board for every bus that has load shed, if more simulations were run per configuration, I think this theory would be proven true.

Comparison of Shortest Path and PPRN Scenarios

Comparison of results shown in Figure 26 and Figure 27 don't show a clear pattern of difference in the no background and light background traffic scenarios. Without stressing the bandwidth both routing schemes finish in similar times making it difficult to draw any further conclusions. As background traffic increases, it appears the PPRN routing scheme is more effective as shown in Figure 28 and Figure 29. This can

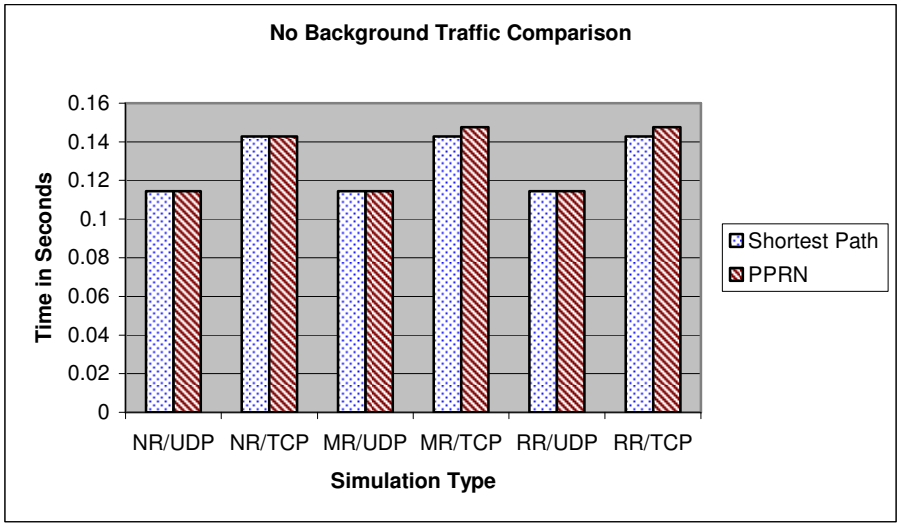

Figure 26. NBG Traffic Comparison of Shortest Path and PPRN Run Times

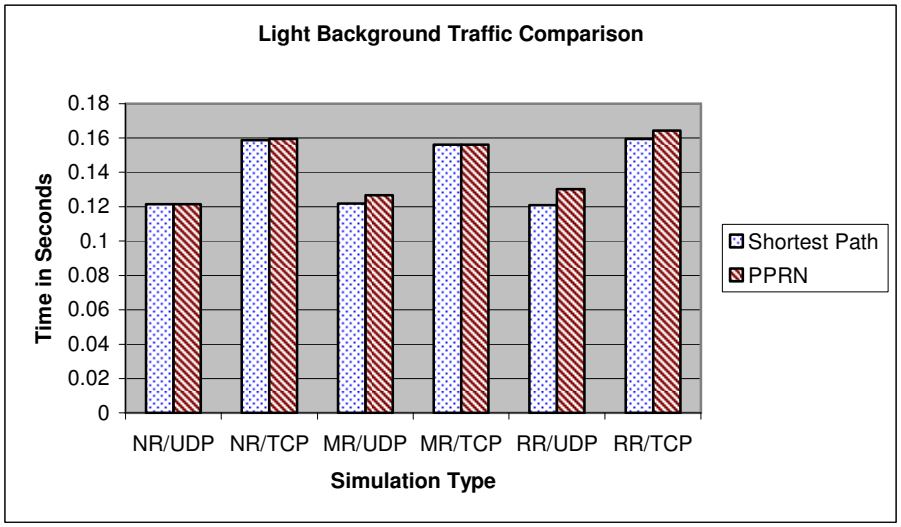

Figure 27. LBG Traffic Comparison of Shortest Path and PPRN Run Times

be attributed to the fact that certain routes become saturated with the shortest path scenarios while PPRN looks for the most efficient routing based on the layout of the network and reservations required. A comparison of the average convergence time for all scenarios is shown in Figure 30 and is consistent with the average completion time results just mentioned.

Simulation Run Time Explanation

Next, an explanation is needed as to why there is a difference in run times even though SPS agent traffic has a priority over background traffic and uses the same route for each reservation for each shortest path simulation and the same route for each reservation for each PPRN simulation. Figure 31 shows the dropped packets while running scenarios (from top left to right) with no, light, medium and heavy background

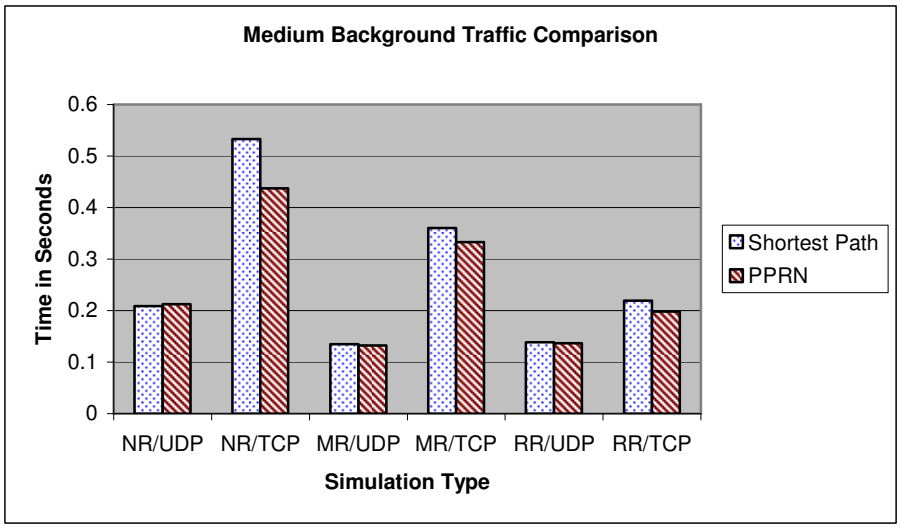

Figure 28. MBG Traffic Comparison of Shortest Path and PPRN Run Times

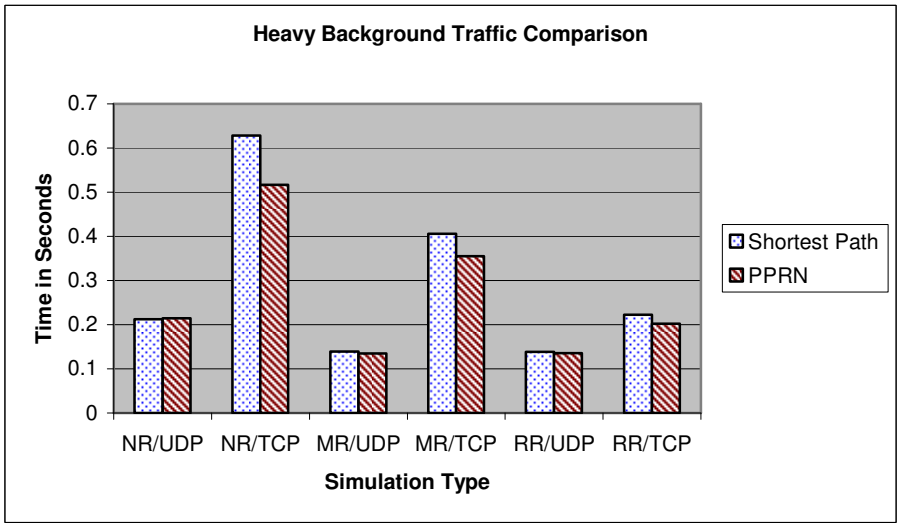

Figure 29. HBG Traffic Comparison of Shortest Path and PPRN Run Times

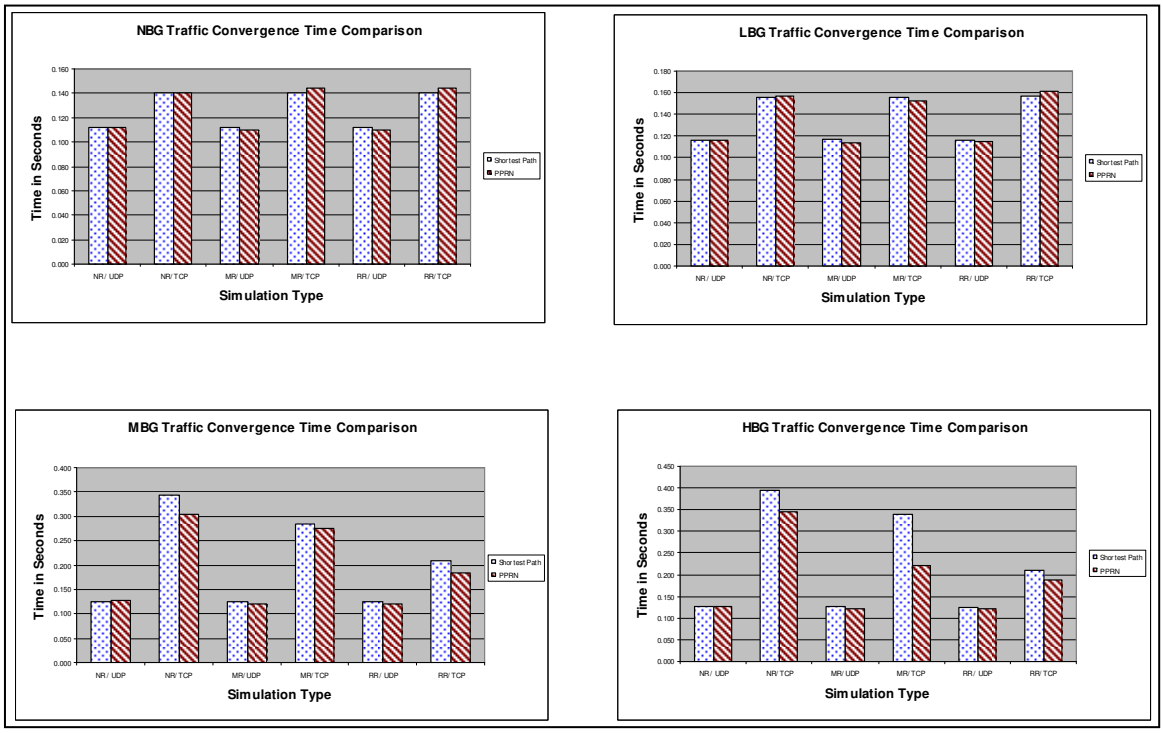

Figure 30. Comparison of Shortest Path and PPRN Convergence Times

traffic loads with router reservations using TCP and shortest path routing in network animator (NAM). The light color traffic is background traffic and the darker color traffic is agent traffic. Nodes 1, 25, and 73 are the congested nodes in this configuration and consist of the majority of dropped packets. I choose a similar time in each simulation (140 ms) to stop the simulation and take a snapshot. This time was chosen because of the increased activity at the critical nodes during the simulation.

When run with no background traffic, the simulations didn't have any dropped packets, thus the similar run times for each simulation. While light background traffic scenarios had dropped packets at nodes 25 and 73, it wasn't significant and there wasn't any SPS agent traffic dropped, only background traffic. The medium and heavy background traffic scenarios had significantly more dropped packets to include some

agent traffic at node 25. With the increased traffic on the network, the agent traffic has to wait from the back of the queue in order to be transmitted and when dropped, retransmitted, thus helping explain the increased run times as the simulations go from no to heavy background traffic loads.

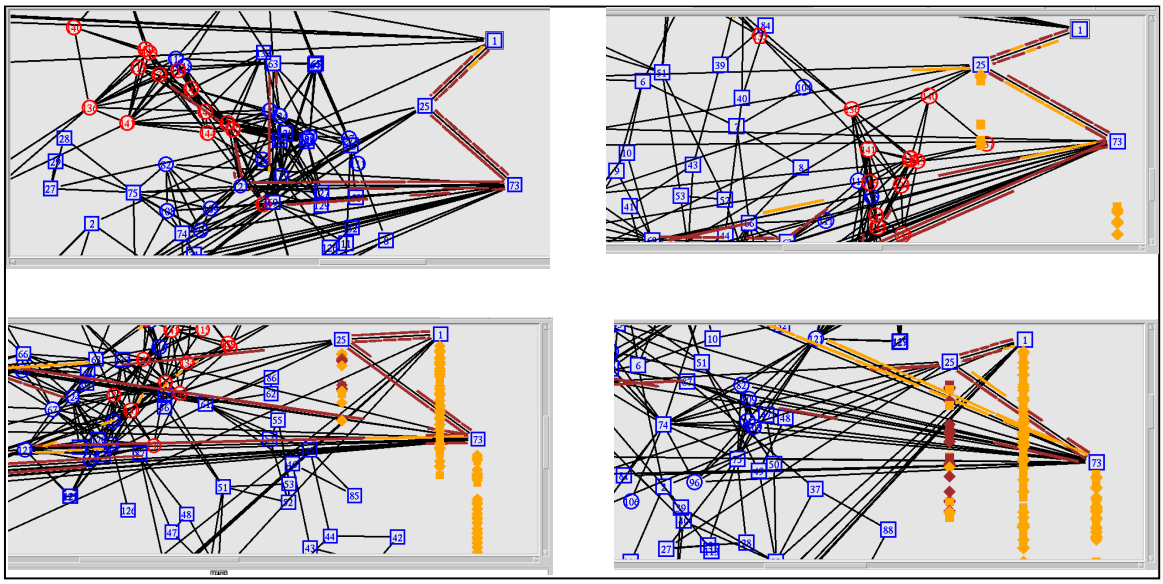

Figure 31. Dropped Packets for Shortest Path, Router, TCP Scenarios

In order to show how backed up the queues get in the critical nodes identified above I used a network visualization tool created by another graduate student [31]. The tool, called NetViz, reads in the NAM file and displays the simulation similar to how it does in NAM except NetViz also shows the queues as they fill. Figure 32 shows the same simulations as Figure 31 but in NetViz with the queues displayed. As expected, once the queues fill, packets begin dropping from the saturated nodes.

The NAM display is repeated in Figure 33 using the PPRN routing scheme for the same scenario. There isn't a significant increase in dropped packets until medium and

heavy background traffic is introduced. The dropped packets are at nodes 1 and 25. All dropped packets are background traffic and all agent traffic appears to make it through the first time. PPRN doesn't drop as many agent packets, explaining why PPRN routing schemes are slightly faster for medium and heavy background traffic than the shortest path scenarios.

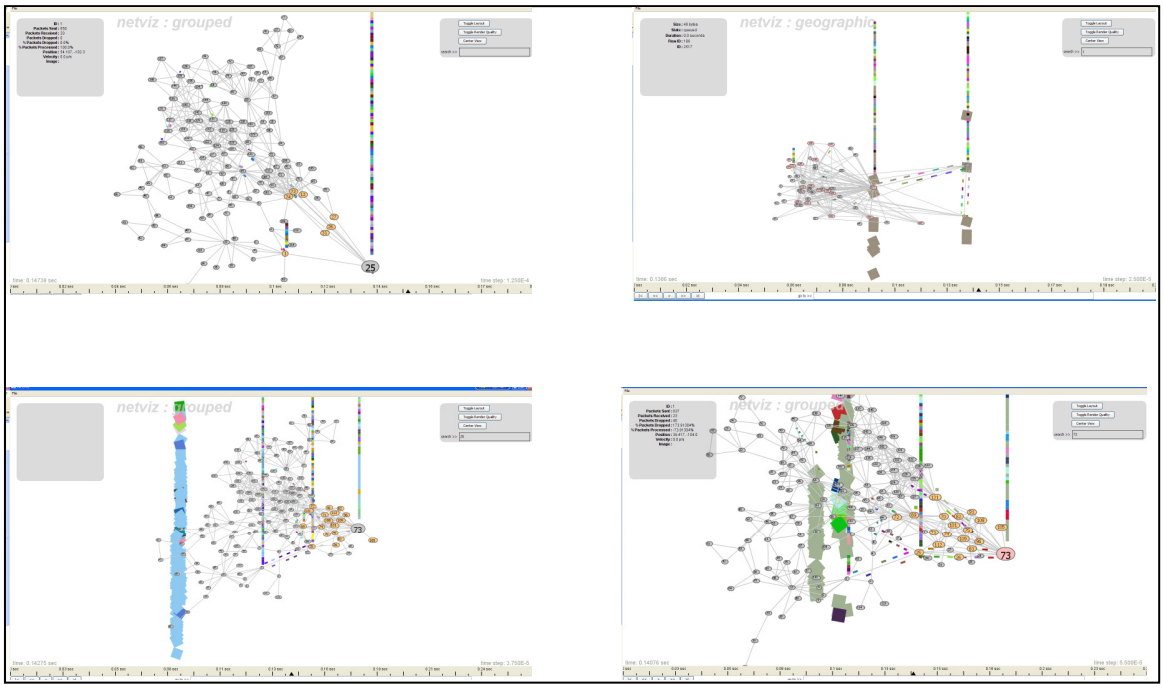

Figure 32. Dropped Packets for Shortest Path, Router, TCP Scenarios in NetViz

Summary

This chapter gave an explanation of the results obtained from running the various simulations. First, the Floyd Warshall Shortest Path UDP and TCP results were presented followed by the PPRN UDP and TCP results. Next, a comparison was made between the results from the two routing methodologies. Finally, an explanation was

given explaining the various differences in run times based on the level of background traffic and routing scheme used.

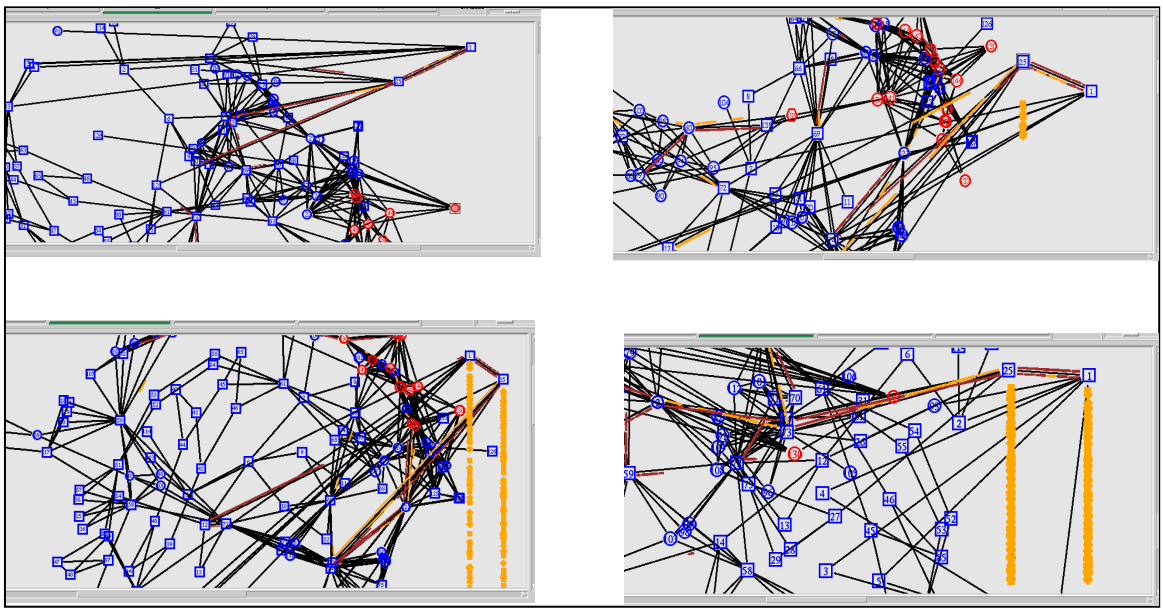

Figure 33. Dropped Packets for PPRN, Router, TCP Scenarios

V. Conclusions and Recommendations

Chapter Overview

This chapter provides conclusions, recommendations, and potential impact of this thesis. First, an overview of the problem is given followed by conclusions based on the results of the simulations. Next, the significance of this research, impact it can have on the development of a future national utility intranet, and protection it can assist in providing the critical information infrastructure is given. Finally, recommendations for follow-on research are discussed.

Research Overview

The power grid of North America has been operating under increased stress in a deregulated environment. The demand for power is steadily increasing as the population increases, thus making the power grid less stable. Despite this, the transmission capacity of the grid has remained static. A rise in disturbances can be expected with any system as system utilization increases. Without the proper insight into the different regions of the power grid, operators and equipment can't be expected to react in a timely manner to stabilize the grid. The current communications system of the power grid provides inadequate situational awareness amongst the various regions. These events were highlighted during the cascading blackout on 14 August 2003 that lasted four days in some areas and costs the economy of the U.S. billions of dollars. The neighboring regions of Ohio-based First Energy failed to notice the lack of data arriving on their monitoring systems and the resulting alarms. The failure of those monitoring systems was critical, and was one of the contributing factors to the blackout that cascading far

beyond First Energy's borders. One way to assist in correcting this problem is to create a national utility intranet to enhance communication on the power grid, thus providing better insight to the various power system operators.

The power industry is moving towards the next generation communications system to meet the increased demands being placed on the power grid. Such efforts as IEC 61850, UCA 2.0, and WAMS in the Western U.S. are proof the electrical power industry is moving toward a utility intranet based on Internet standards, but private to the power industry. The utility intranet will provide the monitoring, protection, and control needed by the power community to properly manage system stability. All newly developed power grid equipment will be developed meeting the previously mentioned standards so the communications system of the power grid will become interconnected over time, just as the power grid itself is integrated. This equipment will slowly replace older technology and improve situational awareness throughout the grid.

While a utility intranet is a great starting point, care must be taken to ensure it meets the performance needs of the power community. A utility intranet will provide many advantages to enhance monitoring of the power system over the serial link systems in place in most parts of the power grid today. Capacity, communication protocols, security, QoS parameters, competing background traffic using the same bandwidth, reservations systems, and routing schemes must be evaluated to ensure the communications system meets the time-sensitive, bandwidth intensive demands placed on it by the power grid.

Conclusions of Research

This research explores the use of a SPS for counteracting and stabilizing power system instability. The SPS is highly dependent on the underlying communication architecture for rapidly and reliably responding to electromechanical instabilities like the one described in the previous section. While using the SPS, experiments were conducted using different routing schemes while exploring different transport layer protocols in the presence of competing background traffic. All simulations tested the performance of not using reservations, followed buy middleware and router reservations.

A total of 480 simulations were run based on 48 different scenarios. A total of 10 simulations were run per configuration. While not ideal, it did provide enough data to make some sound conclusions. First, UDP performed faster than TCP across all background traffic load scenarios for the shortest path and PPRN routing schemes. The difference was greatest when simulations were run with no reservations, followed by middleware reservations, and finally router reservations.

Based on the above results the protocol of choice for the utility intranet is UDP. This choice is made possible because of the modifications made to UDP to guarantee delivery of packets. Without the modifications, UDP wouldn't provide the reliability needed to meet the time-sensitive needs of the power grid.

Both the Floyd Warshall Shortest Path and PPRN routing schemes had similar performance times with no background and light background traffic loads. As the background traffic loads increased to the medium and heavy levels, PPRN routing functioned more efficiently. This was a result of the shortest path routes being more

congested than PPRN routes since PPRN attempts to spread the load in a smart manner while the shortest path only uses the shortest path route for each commodity.

When there wasn't any background traffic or the background traffic was at the light level, all reservations schemes performed in similar fashions. As background traffic levels increased, middleware and router reservations proved superior then not having any reservations. Overall, router reservations performed best because of their complete knowledge of all SPS agent traffic on the network.

As the power community develops a utility intranet, this research promotes the use of PPRN using router reservations with the modified UDP transport layer protocol. This configuration should be sufficient to meet the QoS requirements demanded by the power grid even in the presence of significant levels of background traffic.

Significance of Research

The results of this research can be used by the power community as they determine the best way to implement a utility intranet. This research uses IEC 61850 and UCA 2.0 compliant methodologies and doesn't require any modifications to meet the specifications of the next generation power system equipment.

There have been other middleware and router approaches to bandwidth reservations on an intranet but the approach presented in this research is more robust and flexible. Middleware typically doesn't have knowledge of all the traffic on a network, thus can drop time-sensitive packets. By using router reservations, all traffic is accounted for and not likely to be dropped. Reservation schemes like RSVP and MPLS typically waste bandwidth when the reserving party is not utilizing the reservation, but the

approach presented here allows other traffic sources to use the reservation as long as the reservation is not needed by the reserving party.

It's important we secure the critical infrastructure of our country to protect our vital interest. Currently, an outage caused in one area of the power grid can cascade to affect a much larger area. If the U.S military was marshalling for a large scale deployment and a blackout occurred that affected the entire east and west coast it could have a serious impact on our ability to deploy in a timely manner. The results of this research can go a long way to providing the better insight needed by the power community to prevent such large scale blackouts.

Recommendations for Future Research

The following topics are suggestions for follow-on research to this thesis and potential areas for future research in this subject area.

SPS Simulations

The simulations in this research were run with a SPS that requires three messages with any timestamp from each load and generation agent. The original SPS used in this thesis requires three messages from each load and generation agent with identical time stamps all received within 100 ms of each other. The scenarios could be run with SPSs that have different requirements to see if the results are consistent and still meet the QoS requirements of the utility intranet.

Integrate with Trust Based System

Research was conducted by Coates [32] that addresses trust-based security mechanisms for a national utility intranet. Both research efforts can be combined to

conduct simulations while implementing the security requirements of his research. Security of the data traversing the utility intranet is crucial but it can't interfere with the time-sensitive requirements needed to ensure a stable power grid. This would go a long way to implementing a utility intranet that also meets security requirements.

Integrate with AFIT's Critical Infrastructure Lab

The initial steps have been taken to integrate this research with the newly developed critical infrastructure lab (CIL) at AFIT. Outages can be caused on the CIL and fed to the simulator to see how it will be handled. The goal is show how we can prevent outages in one area from cascading throughout the grid. The CIL gives us a realistic environment to conduct such simulations and show a lot of potential for growth.

Summary

This chapter provided a big picture of the problem set followed by a summary of the results of this research. The significance and potential impact this research can have on the creation of a national utility intranet and protection it can provide to the power sector of our countries critical information infrastructure is given. Lastly, some recommendations for future research are presented.

Appendix A: Software needed to run Simulations Described in Thesis

Listed below is the recommended software needed in order to properly set up and run a simulation as demonstrated in this thesis:

A. TortoiseCVS version 1.8.31 or later version in order to download and upload code on the CVS server. Any version control software can be used in place of TortoiseCVS if desired.

B. WinMerge version 2.6.8.0 or later version in order to compare different versions of the same file to see what has been modified. This is especially useful for comparing the contents of the Makefile file.

C. A copy of the latest EPOCHS code to include swap files.

D. The latest version of Cygwin in order to provide a Linux-like environment for Windows.

E. Network simulator version 2 to be run inside of Cygwin.

F. PSSE in order to run the power flow simulations that will integrate with NS2 via EPOCHS.

G. PPRN in order to solve multicommodity network flow problems with linear/nonlinear objective function and with/without linear side constraints. PPRN is viewed as a general package for solving a high variety of network flow problems [33].

Appendix B: Procedures for Setting up and Running Simulations

Procedures/Instructions

The following instructions will guide one trough the steps required to run a simulation combining NS2, PSS/E, and EPOCHS simulators as described in this thesis. All software and programs should be installed on the 'C' partition of your computer.

1. Ensure you get an account on the CVS server to allow you to check in and out code.

2. Ensure you have TorToiseCVS version 1.8.31 or later installed. Another program that allows you to connect to the CVS repository is sufficient. This program will allow one to connect to the CVS repository to download the latest EPOCHS code for running simulations. The following settings are needed for TotoiseCVS:

   a. CVSROOT: :ssh:username@telemark.afit.edu:22/home/afiten3/CVS/hybrid

   b. Protocol: Secure shell(:ssh:)

   c. Server: telemark.afit.edu

   d. Port: 22

   e. Repository folder: /home/afiten3/CVS/hybrid

   f. User name: your username

   g. Module: location where you are downloaded files (EPOCHS)

3. Ensure Cygwin and NS2 are installed on your simulation computer. When installing Cygwin be sure to install all options and not just the default options.

4. Ensure all EPOCHS files are copied into the "c:/EPOCHS" folder.

5. Ensure all swap files are copied to the "c:/ken/swap/" folder. These files are used so NS2 and Cygwin can talk to each other. NS2 and Cygwin will each write and read from the swap files. The AgentHQ in EPOCHS will manage the read/write process.

6. Install PSS/E and when prompted choose "60 Hz".

7. Ensure you copy all PSSE files to “c:/Program Files/PTI/PSSE30/PSSLIB/” directory. Ensure the “mypssedll” directory is copied directly under the “PSSLIB” directory.

8. Before and between running simulations always go to “/ken/swap” and run the “reset.bat” command from a DOS window. This command deletes old files from previous simulations.

9. Before running a simulation go into "/EPOCHS/background_scenario/background_agent_code/convert_ieee.cpp" file and make the following changes at the beginning of the file:

a. The simulations will be executed with either UDP or TCP agents for each simulation. Make sure all "#define" agent statements are commented out except for "#define UDP_Agents" or "#define TCP_Agents" depending on the type of simulation you are running.

b. Go down a few lines until you see "#define BACKGROUND_TRAFFIC", "#define LIGHT_PERIODIC_TRAFFIC", "#define MEDIUM_PERIODIC_TRAFFIC", and "#define HEAVY_PERIODIC_TRAFFIC" commands in the code. Use the following settings:

1. No background traffic: leave all background traffic statements commented out.

2. Light background traffic: uncomment “#define LIGHT_PERIODIC_TRAFFIC".

3. Medium background traffic: uncomment "#define LIGHT_PERIODIC_TRAFFIC" and "#define MEDIUM_PERIODIC_TRAFFIC".

4. Heavy background traffic: uncomment “#define LIGHT_PERIODIC_TRAFFIC" and "#define MEDIUM_PERIODIC_TRAFFIC" and "#define HEAVY_PERIODIC_TRAFFIC".

c. Now you will identify which type of reservation your simulation will utilize. A few lines further down you will see "#define NO_RESERVATIONS", "#define ROUTER_RESERVATION", and "#define MIDDLEWARE" lines of code. Use the following settings:

1. No reservations: uncomment ""#define NO_RESERVATIONS".

2. Router reservations: uncomment "#define ROUTER_RESERVATIONS".

3. Middleware reservations: uncomment "#define MIDDLEWARE".

10. After all changes are made it's time to compile the code. Following the below steps:

a. Open a windows command window.

b. In order for “nmake.exe” to execute you have to set the environment in Windows to the correct settings, so navigate to “c:/Program Files/Microsoft Visual Studio/VC98/Bin/” and run “VCVARS32.BAT”.

c. Navigate to "/EPOCHS/background_scenario/background_agent_code/" in a windows command window.

d. Run "nmake /f makefile.vc" from windows command prompt.

e. Run "vc_convert_ieee.exe" from the same directory.

f. The "vc_convert_ieee.exe" file reads in "/EPOCHS/background_scenario/ background_agent_code/nscript/dd50_exp2_01_20.cmf" file.

g. This command also creates a "nscript.tcl" file in the "/EPOCHS/background_scenario/background_agent_code/nscript/" directory. Copy the "nscript.tcl" file to the "/ken/swap/" directory.

11. After completing the above steps and before running a simulation, make the following changes to “/EPOCHS/ns-allinone-2.29/ns-2.29/queue/queue.cc”:

a. If you are doing router reservations uncomment “#define DROP_RANDOM”.

b. If you are doing middleware reservations uncomment “#define DROP_WEIGHTED_RANDOM”. The “DROP_WEIGHTED_RANDOM” function is set to allow 10% of non-reservation traffic to traverse the router to the application.

c. If you aren’t using reservations it doesn’t matter since the file will not be used. When using router or middleware reservations only one of the statements will be commented out and only one statement will be used, never both.

12. Open the file "/EPOCHS/ns-allinone-2.29/ns-2.29/classifier/classifier-hash.cc" and run each simulation with one of the following two options turned on for each simulation:

a. Uncomment "#define IGNORE_FLOW_ID" to use routing based on the shortest hop. Leave "#define HIGHEST_PROB_FLOW_ID" commented out.

b. Uncomment "#define HIGHEST_PROB_FLOW_ID" to use routing based on the optimized routing scheme produced by PPRN. Leave "#define IGNORE_FLOW_ID" commented out.

c. Run "make.exe" from a Cygwin window in "/EPOCHS/ns-allinone-2.29/ns-2.29/".

d. Copy "/EPOCHS/ns-allinone-2.29/ns-2.29/ns.exe" to "/ken/swap".

13. Before proceeding please see "Random Number Generator Seed in TCL" and "Random Noise Generation" sections at the end of this appendix for introducing randomness and noise into the simulations.

14. Now you are ready to begin the simulation you just setup. Open a windows command window and two Cygwin command windows.

15. In a DOS command prompt run "/ken/swap/reset" to erase old files.

16. In one Cygwin window navigate to "/ken/swap/" and type in "gdb ns.exe". Then type "run nscript.tcl". This will start the NS2 simulator.

17. Go to "start → programs → PSSE 30 → Dynamics_30 4000 Buses (pssds4)". This will start the PSS/E simulator.

18. Now it's time to configure PSS/E for the simulation. Follow the below steps:

a. Choose "LOFL" (Load Flow) from the buttons across the top of the window.

b. Choose "CASE" from the first row of buttons.

c. Navigate to "/EPOCHS/PSSE Files/xiaoru_psse_code/dd50fl_exp2_detailc.sav" and click "Open".

d. Choose "Fact / Rtrn" from the buttons on the first row.

e. Choose "File → Input → Read dynamics model data (DYRE)".

f. Choose "Select…" next to "DYRE file", choose "/EPOCHS/PSSE Files/xiaoru_psse_code/dd50dy_exp2_detail.dyr".

g. Choose "Select…" next to "CONEC file", choose "/EPOCHS/PSSE Files/xiaoru_psse_code/my_conec.flx".

h. Choose "Select…" next to "CONET file", choose "/EPOCHS/PSSE Files/xiaoru_psse_code/my_conet.flx". Click "OK".

i. Next choose "Edit → Dynamics Data (ALTR) → Solution parameters".

j. Set "Acceleration" and "Delta" and "Frequency filter" to ".002" and click "OK" and then "Exit".

k. Now choose some additional parameters to observe during the simulation. For this research I choose "CHAN → Angle" and enter nodes "67, 93, 99, 104, 110, 111, 117, 124, 132" and click "OK" after entering each node. When finished click "No More". Choose "Exit".

19. Click "STRT" to begin the PSS/E simulation engine.

20. PSS/E will prompt for a "Channel Output File", click "Cancel".

21. PSS/E will prompt for a "Snapshot file", click "Cancel".

22. Choose "RUN" and enter ".000" in the "Run to" text box and click "OK".

23. Click on "Disturbance → Line Fault → Select…" and choose from "Node 1" to "Node 25". Click "OK" and "OK" again.

24. Choose "RUN" again and enter ".07" in the "Run to" text box and click "OK".

25. Click on "Disturbance → Trip Branch → Select…" and choose from "Node 1" to "Node 25". Click "OK" and "OK" again.

26. Choose "RUN" again and enter "2" in the "Run to" text box and click "OK". If the simulation doesn't finish, keep adding a second to the simulation until it completes. It shouldn't run longer than one second. After the simulation completes you need to collect the output files to analyze. Locate and analyze the following files in the "/ken/swap/" directory:

a. three_values.txt

b. final_stats.txt

c. threshold_values.txt

d. center_spd_continuous.txt

e. center_spd_values.txt

f. gen_pmo.txt

g. pdelta_values.txt

Random Number Generator Seed in TCL

The following TCL instructions need to be added to the beginning of each "nscript.tcl" file to seed the random number generator with a different value to ensure the simulations don't produce the exact results with each execution:

```
#RANDOM NUMBER GENERATOR SEEDING

 # seed the default RNG
 global defaultRNG
 $defaultRNG seed 0

# set the random number seed here
   ns-random defaultRNG
```

By setting the random number generator seed to '0' the system will set the seed based on the current time of the day and a counter.

Bibliography

1. Force, U.S.-C.P.S.O.T., *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*. 2004. p. 238.

2. Gjermundrod, K.H., et al., *Flexible and Robust Status Dissemination Middleware for the Electric Power Grid*. 2003, Washington State University: Pullman, Washington. p. 51.

3. IEEE, *UCA Version 2.0*. November 1999.

4. IEEE, *61850*. 2002-2004.

5. Hauser, C.H., D.E. Bakken, and A. Bose, *A Failure to Communicate.* IEEE, 2005(March/April 2005): p. 9.

6. Njemanze, H., *SCADA Security Protections Are On The Increase*, in *Pipeline and Gas Journal*. 2007. p. 3.

7. Xie, Z., et al., *An Information Architecture for Future Power Systems and Its Reliability Analysis.* IEEE, 2002: p. 7.

8. Council, N.A.E.R., *NERC Operating Manual*. 15 June 2005.

9. NERC. *North American Electric Reliability Corporation*. 2007. Last Upate Date: August 2007. [cited; Available from: http://www.nerc.com/regional/.

10. Giovanini, R., et al., *A Primary and Backup Cooperative Protection System Based on Wide Area Agents.* IEEE, 2005: p. 9.

11. Wood, A.J. and B.F. Wollenberg, *Power Generation Operation and Control*. 2nd ed. 1996, New York, New York: John Wiley & Sons, Inc. 569.

12. Mittelstadt, W.A., et al., *The DOE Wide Area Measurement Systems (WAMS) Project - Demonstration of Dynamic Information Technology for the Future*

Power System, in *EPRI Conference on the Future of Power Delivery*. 1996: Washington, DC. p. 17.

13. Kurose, J.F. and K.W. Ross, *Computer Networking, A Top-Down Approach Featuring the Internet*. 3rd ed, ed. A.-W. Computing. 2005: Pearson Education, Inc. 821.

14. Bakken, D., *Middleware*. Chapter in the Encyclopedia of Distributed Computing, ed. J. Urban and P. Dasgupta. 2002: Kluwer Academic Publishers.

15. Van Renessee, R., K.P. Birman, and W. Vogels, *Astrolabe: A Robust and Scalable Technology for Distributed System Monitoring, Management, and Data Mining.* ACM Transactions on Computer Systems, 2003. 21(2).

16. Birman, K.P., et al., *Overcoming Communications Challenges in Software for Monitoring and Controlling Power Systems.* IEEE, 2005: p. 14.

17. Vasu, J. and S. Latifi, *An Overview of MPLS and Constraint Based Routing.* IEEE, 2001: p. 7.

18. Hopkinson, K., et al., *EPOCHS: A Platform for Agent-Based Electric Power and Communication Simulation Built From Commercial Off-the-Shelf Components.* IEEE, 2006. 21: p. 11.

19. Fall, K. and K. Varadhan, *The ns Manual*. 2007: University of California at Berkeley.

20. *PSSE - Transmission System Analysis and Planning*. 2007. Last Upate Date: [cited; Available from: http://www.siemens.com.

21. *PSLF Manual*. 2003, General Electric.

22. *PSS/E User's Manual*, Shaw Power Technologies Inc.: Schenectady, NY, USA, 2004.

23. *PSCAD/EMTDC Manual Getting Started*, Manitoba HVDC Research Center: Winnipeg, Manitoba, Canada, 1998.

24. *IEEE Committee*, in *Transient stability test system for direct stability methods*, IEEE Trans. Power Syst. p. 37-43.

25. Anderson, P.M. and B.K. LeReverend, *Industry Experience with Special Protection Schemes.* IEEE, 1996. 11(3): p. 14.

26. Hopkinson, K.M., *Overcoming Communication, Distributed Systems, and Simulation Challenges: A Case Study Involving the Protection and Control of the Electric Power Grid Using a Utility Intranet Based on Internet Technology*. 2004, Cornell University. p. 245.

27. Braden, R., et al., *Resource ReSerVation Protocol (RSVP) - Functional Specification, RFC 2747*. September 1997.

28. Davie, B., et al., *MPLS using LDP and ATM VC Switching, RFC 3035*. January 2001.

29. Wikipedia. *Floyd-Warshall Algorithm*. 2008. Last Upate Date: 9 January 2008. [cited 28 January 2008]; Available from: http://en.wikipedia.org/wiki/Floyd-Warshall_algorithm.

30. Castro, J. and N. Nabona. *PPRN*. 2006. Last Upate Date: 20 November 2007. [cited November 2007]; Available from: http://www-eio.upc.es/~jcastro/.

31. Belue, M., *Network Visualization Design Using Prefuse Visualization Framework*, in *Electrical and Computer Engineering*. March 2008, Air Force Institute of Technology: Wright Patterson Air Force Base, Ohio.

32. Coates, G.M., *Collaborative, Turst-Based Security Mechanisms for a National Utility Intranet*, in *Electrical and Computer Engineering*. June 2007, Air Force Institute of Technology: Wright Patterson Air Force Base, Ohio. p. 262.

33. Castro, J. *PPRN*. December 2006. Last Upate Date: [cited; Available from: http://www-eio.upc.es/~jcastro/.

Vita

Captain Gregory Rufus Roberts graduated from North Pitt High School in Greenville, North Carolina. He entered the Air Force in June 1985 immediately after graduating. Captain Roberts spent his first 15 years as a communications-computer operations and communications-computer programming specialist. He was stationed at Pope Air Force Base (AFB), Anderson AFB, Barksdale AFB, Osan AB, Langley AFB, and was deployed during the first Gulf War in his enlisted years. Captain Roberts achieved the rank of Master Sergeant before deciding to receive his commission in 2000 where he remained in the communications career field as a communications-information officer. Capt Roberts wears the master communications badge.

Capt Roberts received his Bachelor of Science in Computer Information Systems from Saint Leo University in May 2000 and received his Master of Art in Computer Resource and Information Management from Webster University in March 2003. He was stationed at Scott AFB and Barksdale AFB as an officer before coming to the Air Force Institute of Technology to get a Master of Science Degree in Cyber Operations. While at Barksdale, Captain Roberts was the Cyber Operations Flight Commander for the 8th Information Warfare Flight. He was responsible for leading a section of five personnel in planning and executing special information operations inside the Combined Air and Space Operations Center in direct support of the Eighth Air Force Commander and Commander, U.S. Strategic Command.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
27 March 2008	**Master's Thesis**	Aug 2006 – Mar 2008

4. TITLE AND SUBTITLE

Evaluating Security and Quality of Service Considerations in Critical Infrastructure Communication Networks

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Roberts, Gregory R., Captain, USAF

5d. PROJECT NUMBER
JON # 08-175

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/ENG)
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GCO/ENG/08-05

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Office of Scientific Research (AFOSR/NM)
ATTN: Dr. David Luginbuhl
875 N. Randolph St
Ste 325 Rm 3112
Arlington, VA 22203 Com: (703) 696-6207 DSN: 426-6207 email: david.luginbuhl@afosr.af.mil

10. SPONSOR/MONITOR'S ACRONYM(S)

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

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT
This thesis demonstrates the benefits of utility communication based on Internet technology, some dangers in using Internet technology in establishing a utility intranet connecting protection and control systems, and compares three different approaches to making reservations for routing traffic in the utility intranet based on different levels of background traffic. A model of expected background traffic on a national utility intranet is presented. The Utility Communication Architecture 2.0 and the International Electrotechnical Commission (IEC) 61850 began laying the groundwork in 2002 in establishing an infrastructure allowing power substations, program logic controllers, remote terminal units, intelligent electronic devices, and other devices to effectively and efficiently communicate over a utility intranet that is based on Internet standards using commercial of the shelf (COTS) components. This intranet will almost certainly be based on Internet standards due to their widespread use, low cost, and easy migration path over time. Even though it's based on Internet technology the utility intranet will allow utilities to connect to one another without exposing them to threats from the Internet. This will provide utilities with the needed insight into other areas of the power grid enabling them to better manage its operation. The Electrical Power Communication Synchronization Simulator (EPOCHS) is used in this thesis to run simulations that models network traffic over a power infrastructure in order to show the effects of using different protocols, bandwidth reservations, and varying levels of background traffic will have on the quality of service of intranet traffic, with the end result of improving the insight the different regions of the utility intranet will have with each other. EPOCHS provides the required simulation environment needed to integrate a network simulator with an electromechanical power simulator to run the simulations.
This research discusses the benefits of utility communication, the likely pitfalls in the use of Internet technology for protection and control systems, and technologies that can help mitigate those pitfalls. A total of 48 different simulation configurations are performed based on background traffic, reservation type, IP transport protocols, and routing scheme used to determine which configuration is best suited for use on a utility intranet.

15. SUBJECT TERMS
Supervisory Control and Data Acquisition, Special Protection Schemes, Wide Area Measurements System, Transmission Control Protocol, User Datagram Protocol, Quality of Service, Run Time Infrastructure, Intelligent Electronic Device, Electrical Power Communication and Synchronization Simulator, Network Simulator 2, Power System Simulator for Engineers, Extremely High Voltage

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
REPORT	**ABSTRACT**	**c. THIS PAGE**			Kenneth M. Hopkinson, PhD, ENG
U	**U**	**U**	**UU**	111	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-3636, ext 4579; e-mail: kenneth.hopkinson@afit.edu

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