SMART GRID RELAY PROTECTION AND NETWORK RESOURCE MANAGEMENT FOR REAL-TIME COMMUNICATIONS

A DISSERTATION SUBMITTED TO THE
GRADUATE DIVISION OF THE
UNIVERSITY OF HAWAIʻI AT MĀNOA
IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

IN

ELECTRICAL ENGINEERING

DECEMBER 2017

By

Jiapeng Zhang

Dissertation Committee:

Yingfei Dong, Chairperson
Matthias Fripp
Depeng Li
Galen Sasaki
Yao Zheng

I dedicate my dissertation work to my family. A special feeling of gratitude for my beloved parents, and grandparents. Their encouragement is always the source of my determination to keep moving forward.

ACKNOWLEDGMENTS

Over the past five years, I have been received support and encouragement from a great number of people. Without their help, it would be difficult for me to move toward completion of my study.

First and foremost, I would like to express my sincere gratitude to my advisor Prof. Yingfei Dong for his excellent guiding, caring, and patience in support of my Ph.D. study and research. His guidance helped me build solid knowledge on my research area, and his experience helped me get through the most difficult time during this study.

Besides my advisor, I would like to thank the rest of my dissertation committee: Prof. Matthias Fripp, Prof. Depeng Li, Prof. Galen Sasaki, and Prof. Yao Zheng, for their insightful and constructive comments to make this research more completed.

I would like to thank Prof. James Yee and Prof. Rui Zhang for their advice to my qualifying examination and comprehensive examination.

I would also like to thank my friends and classmates. I was inspired through the discussion with them, and I did benefit quite a lot from working and learning with them.

Last but not the least, I would like to thank my family: my parents Shaochun Zhang and Lujia Yi, for their wholehearted support and encouragement in my life.

ABSTRACT

Smart Grid (SG) significantly improves the computing and communication capabilities of power systems. As a result, smart power generation, distribution, and protection are realized using more intelligent devices. These improvements provide many opportunities to better address issues in existing systems, such as cascading failures in traditional grids. Through the investigation of several large blackouts, malfunctional distance relays have been recognized as one of the critical causes of cascading failures. To deal with the false trips of relays and cascading failures, many monitoring and protecting methods have been proposed on traditional grids. However, many areas are still needed to be further investigated. In this dissertation, we focus on three issues related to SG protection. We first proposed an effective resource management scheme for agent-based remote relay protection. Second, we investigated cyber attacks on relay protection systems, analyzed their impacts, and explored how to mitigate these attacks. Third, we proposed a synchronized routing framework for real-time delivery of measurement and control data. We briefly introduce these three research areas in the following.

To protect remote relays from hidden failures, several agent-based protection schemes have been investigated. However, they do not consider the details in network resource management and different failure cases. We propose a set of resource allocation schemes to address the practical deployment issue of these protection schemes. Our results show that the basic agent-based protection consumes significant amounts of network resources and cannot effectively support many new SG applications, and is unable to deal with communication link failures. We further improve the proposed basic scheme, and develop backup schemes to handle network failures. Furthermore, when utilizing power system knowledge, we can make the resource allocation more efficient. Our evaluation shows that our proposed schemes can use less network resources while achieving the required system reliability. Moreover, we also investigate Peer-to-Peer (P2P) agent protection schemes. We propose an effective resource management scheme and a backup scheme in the P2P mode. The results show that P2P

protection can fulfill the reliability requirement using less resources.

It is well known that the reliability of power systems is a difficult challenge. To address this problem, basic agent-based protection and agent-reputation-based protection are developed for future smart grid to enhance the reliability of relay protection. While effective in many situations, these schemes may be exploited by malicious attackers to disrupt the power system, or even trigger cascading failures in the system. Unlike occasional faulty behaviors, cyber attacks deliberately target various components in power systems, which cannot be resolved from the perspective of device reliability. Currently there is limited work on how such attacks are carried out, and to what degree damage can be achieved. The goal of our research is to better understand the problem, by examining the potential methods to attack the relay protection system, and evaluating their effectiveness. We also explore how to mitigate potential cascading failure damage due to cyber attacks.

As the accurate measurement and sampling of system states are the foundation of SG monitoring and protection applications, we develop a synchronized framework to achieve predictable delivery for large-scale real-time applications. With the synchronized time as a global reference, we design the synchronized routing framework and evaluate its effectiveness with different packet scheduling schemes. The results show that we can adjust service order of packets according to their urgency. Compared with existing packet scheduling schemes, by using both upstream and downstream delay information, the proposed method has a larger adjustable range, and achieves much better efficiency and predictability.

In summary, we have explored remote relate protection, relay cyber security, and real-time communication related problems in SG, and proposed several solutions, including network resource management, analysis and defense of attacks on smart relays, and synchronized real-time packet delivery. Our future work will focus on more detailed issues within each problem, such as advanced agent-protection structure, refined attack and defense strategies, and improved measurement accuracy of network delays.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

Electrical grid is one of the most complex systems in today's world. Many existing grids have been running for decades. While these grids can still carry out their tasks in power delivery, they are often inefficient and unscalable. For example, currently only a moderate proportion of fuel energy is converted to electrical power, and lots of the power is generated only to meet the peak demand. To address the problems and improve service quality and efficiency, Smart Grid (SG) is being developed to replace the traditional grid. In SG, more intelligent power generation and consumption plans can be realized, and more environment-friendly renewable resources can be utilized efficiently. One key challenge of SG is scalability, especially as renewable energy will be generated distributedly across large areas from many devices.

While we are concentrating on the efficiency of power system, in recent years, several large blackouts occured in Europe and US also draw more concerns in security and reliability of the system. Millions of people were affected in these blackouts, and the damages were significant. In many cases, a blackout starts from the failure of a line or a substation that causes the cascading failure and then spreads across the system. As a result, the visibility of failure is becoming a critical issue in the design of SG, and many investigations have been performed to improve system reliability, by integrating advanced computing and communication techniques in SG to carry out system control both locally and across wide-areas. With the state information collected from critical locations in the power grid in real-time, the control system can have a more clear view of the grid and perform better control.

With the advanced features provided by SG, the next question is how to enhance system reliability. Although several methods have been proposed to address the hidden failure problem of protection relays, there are still many remaining issues to be investigated. In addition, cascading failures and related real-time protection schemes are still not well un-

derstood. Moreover, control and protection methods need the support of system state measurement, which raises higher requirements for the SG communication networks. Motivated by these problems, our work focuses on three research areas: Smart Remote Relay Protection, Attacks on Smart Relay Protection, and Synchronized Routing. We will briefly introduce our research in the following.

Smart Remote Relay Protection. To prevent transmission lines from interrupted by device failures, various kinds of local and remote relays are deployed in today's power systems, so that failed components can be isolated. Among the devices, directional relays (especially remote Zone 3 relays) are essential to provide local and remote-backup protection. However, these relays suffer from hidden failures. A hidden failure is a failure that is exposed as the consequence of another event. Sometimes these small failures can cause unexpected trips and further spread out as cascading failures. To address the hidden failure problem, many solutions have been proposed, and many new solutions are still in development for different system requirements. With the advanced communication integrated in SG, agent-based relay protection attracts attention from researchers. The core idea of agent-based solution is, when a relay detects a contingency, it first contacts a control agent for a decision (e.g., whether to trip or not). The control agent then collects information from the system and informs the query relay what to do in the next step. In this way, a relay will unlikely incorrectly trip a line. We can divide agent-based solutions into two types: Master-Agent-based (MA) and Peer-to-Peer-based (P2P).

The existing solutions [1, 2] focus on the functions of agents and assume a dedicated communication network will be used. This assumption is not practical as it is inefficient, expensive and sometimes infeasible to achieve such requirements. In addition, there will be a growing number of real-time applications to be developed and deployed in the smart grid. Many of these applications will require large amounts of network resources. As a result, the dedicated network is not cost-effective and often is impractical. To address this problem, we need to carefully design the allocation of resources for sensitive communication data, such as real-time protection traffic.

Furthermore, the communication network in SG may experience failures. As a result, queries may not be received by a control center, and the enquiring relay may not receive a response from the control center, which makes the relay under the threat of hidden failures and other issues such as malicious attacks. To address the problem, we propose a backup mechanism for MA-based relay protection schemes. The backup mechanism significantly improves the reliability of the protection schemes. With disjoint backup paths, the improved protection is able to handle single communication link failures. However, full disjoint paths may be not always available, as this approach may require many bandwidth resources and specific network topology features. To deal with these problems, we further explore power system information, and develop a power-aware protection scheme. The power-aware scheme enhances the resource utilization. In addition, we explore P2P-based schemes to address the limitations of MA-based protection schemes. We also investigate the resource requirement for basic P2P-based protection, and improve its reliability with backup paths.

Attack on Smart Relay Protection. Today's electric power industry has been taking advantage of the tremendous capabilities provided by advanced computing technology and communication networks. Control and protection equipment, SCADA, remote control and monitoring, and many other applications have been dramatically enhanced with these technologies. However, the vulnerabilities in these distributed connected systems also provide many opportunities for malicious attakers to disrupt our power supply. For example, a vendor of the operating system may leave behind a backdoor which is unknown to a power system administrator, and this backdoor may be used to change system configuration and cause unexpected issues; or, an authorized employee may be blackmailed by a third party to change the device configurations in substations in order to discredit a competitor's product. Unattended facilities like substations are the basic components of electricity grids, which contain many fundamental assets, such as buses, switches, breakers, remote terminal units (RTUs) and smart intelligent electronic devices (IEDs). Many communication devices also reside in substations. Unlike manned control centers and power plants with strong monitoring and protection, usually very limited security mechanisms are deployed at unat-

tended substations located in remote areas [3]. This often makes malicious physical and cyber attacks on substations much easier for attackers. Consequently, compromised devices (especially protection devices) may cause serious issues for the integrity of the power grid.

Smart remote relay protection is critical to the stability of future smart grids. Various protection mechanisms have been designed to improve traditional relay protection schemes in smart grids (e.g., agent-based protection [1, 2, 4] and agent-reputation-based protection [5, 6, 7]). While these protection mechanisms benefit from the advanced communication technology, it also increases the chances for remote attacks. Security vulnerabilities of these systems may be exploited against these protection schemes. However, to the best of our knowledge, very little research has been done to examine the impact of cyber attacks on these protection schemes.

To address this issue, we focus on cyber attacks to relay protection systems in this dissertation. We examine three attack strategies in attacking relay agents, and analyze their effectiveness. Assume that an attacker's goal is to disrupt as many transmission lines as possible. We will first examine how *direct* and *indirect* attacks to relays can be conducted in SG, and how cascading failures can be triggered by these attacks. We analyze the number of potential line trips due to different types of attacks. We observe that basic agent protection schemes cannot effectively prevent these attacks; we then improve the basic scheme with a majority-based trip confirmation scheme. We also investigate the enhanced P2P agent-reputation-based protection, and demonstrate its weakness. Although the reputation-based protection scheme helps enhance the reliability, response time, and processing efficiency of relay protection systems, an attacker can exploit such scheme to trigger cascading attacks. We will analyze how likely cascading failures can be *indirectly* triggered under the reputation-based protection scheme, and compare it with the ordinary cascading failures caused by *direct* attacks to relays in the system. Based on our observations, we propose two methods to mitigate the potential damages of cascading due to cyber attacks.

Synchronized Routing. Smart grid control applications rely on the collected system information to make control decisions. Many applications require sampling data to be

transmitted and received within specific periods. Violations of data delay requirements not only make them useless, but also will further affect the accuracy of the control, and degrade the reliability of the system. How to support the large-scale real-time applications has been a challenging problem for a long time. Since SG is expected to inter-connect many utilities across states, the design of its communication network must also deal with this problem. Traditional methods [8, 9] either use over-provision to ensure resources for specific flows to achieve guaranteed delivery, or statistically reservation for specific traffic classes. These methods lack the scalability for large-scale deployment, and cannot fully utilize available resources. In addition, it is hard for these methods to handle dynamic network conditions and path failures.

In this research, we address the above problem by proposing a synchronized routing framework. Our idea is to use the synchronized time as a global reference to explore more efficient traffic delivery. As synchronization is already required for smart grid data to be used in real-time control or post-contingency analysis, its infrastructure will be equipped with time synchronization technology. Then its communication network can be synchronized as well. By periodically measuring packet delays in the network, a router can estimate the delays of packets on given paths, and it can share its knowledge with other routers as well. Using the delay information, we develop a packet scheduling scheme to adjust service order of packets at a router. With the global reference, we can achieve better coordination among routers. Compared with existing scheduling schemes, we can better adjust the priority of packets. Besides, the reference time will also provide an opportunity to address the inter-domain service across large areas.

In summary, our research focuses on the control and protection of smart grid. First, we have studied MA and P2P agent-based relay protection to prevent hidden failures, in order to mitigate critical factors that often triggers cascading failures. We have proposed communication network resource management schemes and backup mechanisms, using the power system information, to improve the reliability of agent-based protection. Second, we have also examined the potential cyber attacks to better understand how these attacks

can be launched. We analyzed the effect of these attacks, and proposed several methods to address cascading failures caused by these attacks. Third, we have proposed the synchronized routing framework, using synchronized time as a global reference, for real-time data delivery in smart grid.

The remainder of the dissertation is organized as follows. In Chapter 2, we will introduce the basics of traditional grid and smart grid. We also review existing work on remote protection relay, cyber attack, cascading failure, and real-time data delivery. In Chapter 3, we will provide a big figure of our research, explain the three research areas, and discuss the potential issues. In Chapter 4, we will present detailed solutions on remote relay protection. We focus on network resource management and system reliability improvement. In Chapter 5, we will discuss the effect of cyber attacks to smart relay protection. We analyze different direct and indirect attacks on relay protection agents, and propose improvements to mitigate attack damages. In Chapter 6, we will present our work on real-time delivery, with the focus on packet scheduling, and present the performance evaluation of the proposed scheme. We will conclude the dissertation in Chapter 7.

The research in this dissertation resulted in a list of journal and conference papers [10, 11, 12, 13, 14].

CHAPTER 2
RELATED WORK

In this chapter, we will discuss the existing systems and schemes related to our investigation and provide related background information. First, we will introduce traditional power grid and its limitations, and introduce smart grid, including its basic concept, communication technologies, information delivery frameworks, applications and their requirements. We will further illustrate existing power system protection schemes, point out their advantages and drawbacks, and then we will briefly present our ideas. Moreover, we will review potential cyber attacks on relay protection agents, and figure out the limitations of current protection schemes. In addition, we will present existing solutions in real-time data transmission.

2.1 Traditional Power Grid

An electrical grid is an interconnected network, which delivers electrical power from suppliers to consumers. The grid consists of (1) generating stations that produce electrical power, (2) high-voltage transmission systems that carry power from generating sources to demand locations, and (3) distribution systems that connect individual customers within an area. In traditional power grids, the transmission system was built to deliver power from a utility's generator across town to its distribution company; today, the system is being used to deliver power across very large regions, e.g., across multiple states [15].

Traditional electricity grid is unidirectional, as shown in Fig. 2.1 - it is a strictly hierarchical system where a power plant is at the top of the supply chain that ensures power delivery to the customers at the end of the chain. The efficiency of the grid is very low and it only converts about one-third of fuel energy into electricity. Among the output, about 8% is lost along the transmission lines and about 20% is only used to meet the peak demand only [16], which occurs infrequently and causes huge wastes during normal periods. Traditional grids have been running for decades. For example, in the northeastern United States,

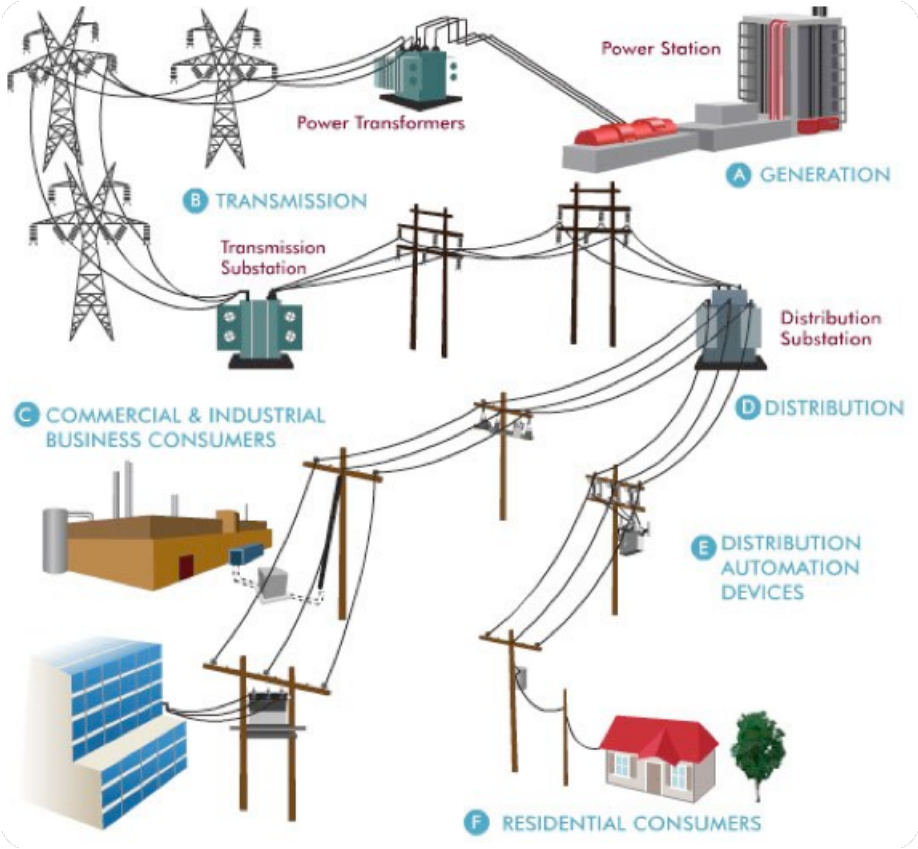


Figure 2.1: Traditional Grid Model [16]. Traditional Grid has centralized control with basic data network in the transmission stage; in the distribution stage consumers can only passively operate without data exchanged.

the majority of the transmission systems were originally constructed during the 1960s, with the devices more than 50 years old.

Nowadays the system continues growing in size, scale, and complexity, which are making it difficult to schedule even for routine maintenance [15]. Although the science of asset management has been applied by many utilities to prioritize new operation tasks to ensure reliability, the aging infrastructure requires upgrade and evolution to address numerous challenges. For example, no real-time information about the service parameters are exchanged among different components; with the safe margins exhausted, the system is at the edge of instability. In a word, the lack of information delivery and processing capabilities in traditional power grid makes it inefficient, hard to ensure reliability and rather complex

to integrate with newly developed applications, especially distributed renewable energy.

2.2 Smart Grid

2.2.1 Smart Grid Basics

A smart grid enhances the traditional power grid with two-way flows of electricity and information to create an automated and distributed advanced energy delivery network, with intelligent devices that exploits the rapid increase of computing power and ubiquitous communication networks [17, 18]. SG can deal with risks from different aspects such as power generation, transmission, distribution, and consumption, and come up with the corresponding real-time strategies. The vision of smart grid is characterized by the use of more sensors, faster communication technologies, higher computation ability and more accurate control methods, which finally forms a comprehensive architecture [19]. The National Institute of Standards and Technology (NIST) provided a conceptual model as a reference for the standardization of different components of the electric power system, shown in Fig. 2.2.

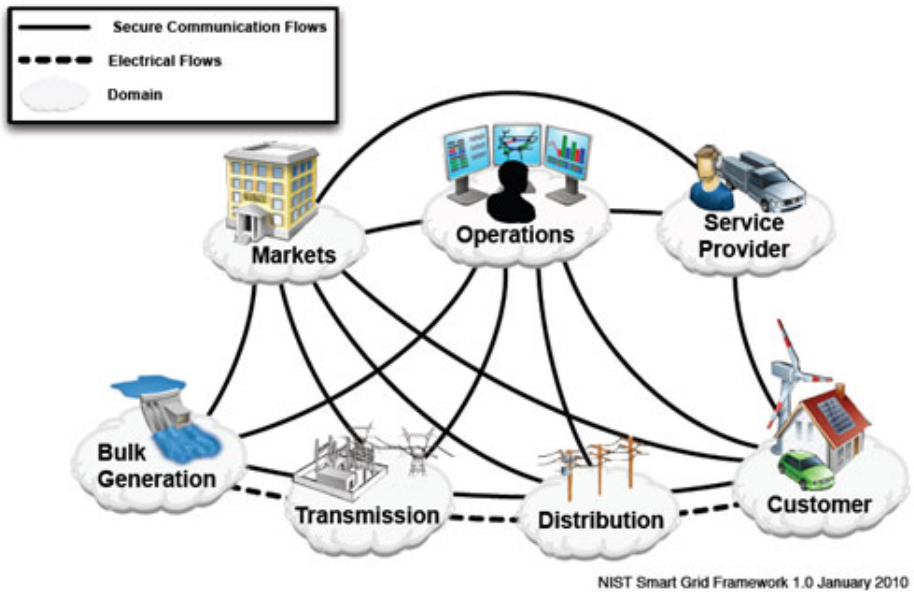


Figure 2.2: The NIST Conceptual Model for SG [20].

The challenges that the smart grid is facing can be characterized as follows: Reliability,

Efficiency, Affordability, Security, Environment/Climate Change and Global Competitiveness [21]. To better address these challenges, the infrastructure, management and protection systems are the critical components of SG, where the infrastructure system is further divided to three subsystems - energy, information, and communication. The traditional energy system is being upgraded for better power generation, transmission, and distribution.

The generation system should take the advantage of renewable resources (e.g., solar, wind, etc.) and adopt the new paradigm of distributed generation (e.g., localized small scale generators or power systems), in which a micro-grid can connect or disconnect from the main macro-grid whenever necessary, in order to improve the system quality and reliability. For the transmission system, a smart control center will enable new analytical and monitoring features to improve power utilization, power quality, and security. Distribution within the SG will become more flexible with the deployment of distributed generators; on the other hand, as more distributed generators participate in the grid, the control of the power flow within the grid will become more complicated as well, calling for intelligent devices and distribution methods.

When many utilities integrated into large power systems, in order to improve reliability, better visibility into the operations is required, especially for conditions that cannot be immediately sensed in a control center. This requirement leads to the implementation of supervisory control and data acquisition (SCADA) system in the old days. However, there is the need to continue visibility improvement, which has been demonstrated in several large-area blackouts, such as the US-Canada power outage in 2003 [22]. Thus a modernized information system is needed for interoperability of data exchanges and integration with existing and future devices, systems, and applications. Among the requirements, a very important function of SG is the monitoring and measurement of the grid status, which requires real-time and on-demand data collection. To achieve the goal, many SG technologies have been developed and many new SG applications are still in development, e.g., Automatic Metering Infrastructure (AMI) and Phasor Measurement Unit (PMU) technology [23].

2.2.2 Smart Grid Data Collection

The evolution to SG emphasizes the application of computer monitoring, analysis, optimization, and control in the generation, transmission, and distribution grids. Meeting these challenges requires not just the update of power system, but also the data delivery and processing infrastructure. As the first step, data corresponding to the status of the system should be generated from end entities. Then the data will be gathered and processed at the local or higher level control center, used for grid status monitoring, user appliance control, and other features.

PMU is a very popular technology in the future SG, which performs advanced system data collection. PMU measures the phasor (represented in sinusoidal signals) of an electrical grid, for example, the magnitude, phase, and angle of voltage, to determine the health of the system. PMU readings are obtained from widely geographically separated locations in a power grid and all devices are synchronized using the global positioning system (GPS) radio clock, which records measurements that occur at the same time. To fulfill the requirement of SG, the data rate of PMU is much faster than traditional SCADA system (retrieves data from every 2-4 seconds up to 5 minutes [24]), usually between 30 to 60 Hz, while newer PMUs have the option to increase the sampling rate to 100 Hz or even 200 Hz in some cases [25, 26].

With the help of PMU, better protection information is gathered, and many protection applications are enabled in SG. System operators can use the sampled data to estimate and predict the state of the power grid and respond to system conditions in a rapid and dynamic fashion, making the power system more robust to catastrophic failures. For example, protective relay settings can be adjusted based on the measured real-time SG conditions (current, voltage, and temperature, etc.), which addresses the "over-sensitivity" of relays.

A Phasor Data Concentrator (PDC) is usually used in the network to collect data from different PMUs. After receiving the data, it sorts and groups the PMU packets depending on their creation time stamps. Then the processed data flow is sent to the control center of the grid for further analysis. Depends on the requirements, a PDC can also gather information

from other PDCs. PMUs and PDCs comprise the Wide Area Monitoring System (WAMS), the hierarchical architecture is shown in Fig. 2.3.

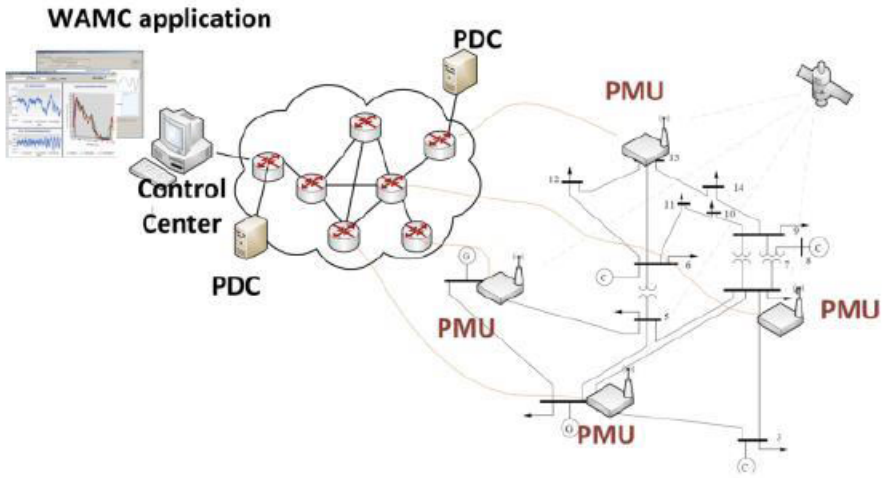


Figure 2.3: WAMS Architecture [26].

As large amount of information is generated in SG, advanced information management should also be supported, including information analysis, integration, and optimization. Since data are exchanged between multiple applications, perhaps from different departments or utilities, a unified data format is needed for all participants to understand. Meanwhile, the information is generated and used by existing applications, new applications should also consider the use of such information for higher efficiency.

2.2.3 Smart Grid Communications

The reliability of the power system is dependent on its ability to deliver electric power from generation to load without disruption, which lies in the increased situational awareness and wide-area power system control. Adding redundancy and providing enough margins for the power system will enhance the reliability; on the other hand, operating the grid under the limit will decrease the efficiency because the capacity is not fully used [23]. To balance the reliability and efficiency, the accurate information of system status is of great importance (especially when renewable energy is considered such as wind and solar) and reinforces the

needs to improve the communication infrastructure in SG.

2.2.3.1 Communication Media

The communication technologies used in SG can be characterized into two groups: wired and wireless. Typical wireless technologies include Wireless Mesh Network, ZigBee, Cellular Network, and Satellite communication. These technologies offer low installation cost, rapid deployment, large coverage area, mobility, and are more suitable for remote end applications where the installation of wired networks is not cost-effective. However, wireless communications are the sub-optimal choice for real-time applications that require extreme accuracy, due to the relatively higher delays and potential path failures in wireless communications. Wired communication, especially fiber-optic technology, with its high bandwidth capacity and electromagnetic and radio interference immunity, makes it ideal for real-time system control. Powerline communication (PLC) is also considered as a good candidate because the existing infrastructure decreases the installation cost of the communications infrastructure, but its data rate is much slower [27] than optic-fiber and is only suitable for a small area, such as within a substation.

2.2.3.2 Communication Protocols

An important issue of the communication system is end-to-end communication management, where heterogeneous communication subsystems are used. There is a growing trend towards the use of TCP/IP technology because of the maturity of a large number of standards, the availability of tools and applications that can be applied to SG environments. However, TCP does not support real-time guarantees in terms of delay requirements, and its retransmissions and acknowledgements will even worsen the delay situation [28]. As a common practice, UDP is usually used for time-efficiency. To support the exchange of information between different elements, the communication standards and protocols should play a key role in smart grid development. The standardized communication interfaces ensure that information is accessible, interoperable, and the implementation of functionality across

different domains is cost-effective. Several protocols have been developed to satisfy various application constraints.

- Distributed Network Protocol (DNP3)
- IEEE C37.118
- IEC 61850

DNP3 is a set of communications protocols used between components in process automation systems. It plays a crucial role in SCADA systems, because it is primarily used for reliable and secure communications between control centers and RTUs or IEDs. The protocol can use serial communication, or it can be used over packet-oriented networks such as TCP/IP and UDP/IP. DNP3 has been adopted as the IEEE 1815 standard in 2010 for communications in electric power systems. Meanwhile, interoperability standards are under development to support a transparent mapping between IEEE 1815 and IEC 61850.

The IEEE C37.118 standard defines the exchange of synchronized phasor measurements used among power grid applications. The standard defines communications rules for PMU and PDC. Since the measurement points are distributed across the network, the protocol is implemented on top of a routable protocol, such as TCP/IP or UDP/IP. To address the synchronization of measurements, GPS is used. In the future IEEE 1588 standard will be used to provide the same function, thus partially remove the need for GPS in some PMU units.

IEC 61850 is a family of standards designed for electrical substation automation. More precisely, the mapping to communication protocols defined in IEC 61850-8-1 and IEC 61850-9-2, was originally designed within substations at the transmission level, but is now expected to provide communications between substations, control centers, and domains. Its goal is to increase the scope of the old IEC 6180 to the whole electric network and provide its compatibility with Common Information Model (CIM) for monitoring, control, and protection applications [27]. The abstract data models defined in IEC 61850 have been mapped to a number of protocols that can run over TCP/IP, UDP/IP, and switched Ethernet [18].

As Internet Protocol is widely used in public communication networks, a lot of applications will use the UDP/IP for data transmission across the network. Since UDP does not provide checksum and retransmission, the specific protocols are responsible for detecting corruption in data. In this case, the protocols are rolled up into the application layer, and transmitted as a whole. This is important to critical power applications, such as the system protection, because lost or damage of data will lead to serious consequences.

2.2.3.3 Existing Smart Grid Communication Framework

More and more SG applications in developing are real-time applications that have strict delay requirements. For example, PMU data delivery time should not be longer than a full power cycle [29]. Besides, different applications used in the power grid also have a wide range of data delivery requirements. These requirements are identified as quality of service (QoS), which includes latency, rate, criticality and quantity of data. The communication network should be able to provide various levels of services to the applications, to ensure the data delivery to be predictable, reliable, and in the expected format. In order to fulfill those requirements for real-time communication, two frameworks have been proposed.

(1). GridStat. GridStat [23, 24, 30] is a framework designed to manage network resources to achieve low-latency, reliable delivery of information. The designing goal of GridStat is to fulfill the requirements of providing flexible and robust communication for power grid systems. The framework collects information produced in the network and sends the information to one or multiple other locations, following pre-defined QoS parameters. The middleware design approach of GridStat allows developers to focus on application needs rather than thornier issues involved in wide-area communications.

GridStat consists of two planes, the management plane and the data plane, which handle network management and data delivery separately, as shown in Fig. 2.4. The management plane consists of a hierarchy of QoS brokers that allocate resources and adapts the network in reaction to changing power system configurations or communication network failures. Data plane components are responsible for forwarding data from each source to potentially many

destinations as directed by management-plane components. The data plane of GridStat uses the publish-subscribe communication model. The data periodically generated at a source (publisher) will be distributed to destinations (subscribers) without the publisher and subscriber having to track each other. This introduces the flexibility in data delivery by allowing changing the characteristics of existing subscriptions at runtime. GridStat operates on a dedicated network and has complete control over the available resources, which takes advantage of the highly static nature of the topologies between publishers and subscribers in the power grid, by pre-allocating paths between the data producers and other potential recipients, in order to guarantee quality of service (including rate, latency and redundancy, etc.) of the requested data [31].

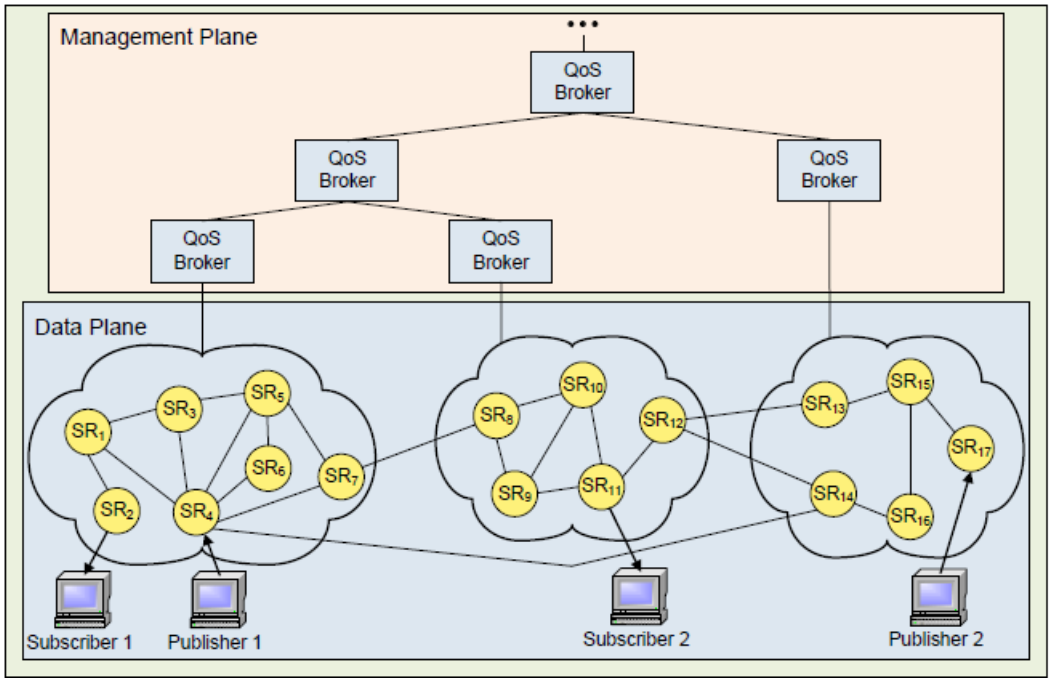


Figure 2.4: GridStat Architecture [24].

The routers used in the data plane WAN have three types: edge status routers, border status routers, and other routers. An edge status router connects to end users (publishers or subscribers), provides proxy to the management plane devices and performs data delivery. A border status router connects two domains in the data plane, where more com-

plex routing algorithms are applied, in order to utilize the resources more effectively. The other routers simply perform data forwarding and do not have additional functionality. All routers within a domain connect to the leaf QoS broker in the management plane - these brokers have complete knowledge of their own administrative domains and resources, and they also cooperate with the parent broker if inter-domain data delivery is needed. The publisher-subscriber communication is implemented by using multicast, together with rate filtering at the status routers to limit the resources needed to support the property. Spatial redundancy is implemented by applying appropriate forwarding rules at routers with multiple disjoint paths, e.g., n paths are able to handle $n-1$ path failures. Additionally, GridStat employs static routing, because in a critical infrastructure such as the electric power grid, most communications are predetermined, thus static routing is generally considered more efficient than dynamic routing in this case.

(2). NASPI. The North American Synchrophasor Initiative (NASPI) was formed to improve the reliability of the power grid while meeting the increased power demand, focusing wide-area measurement, monitoring, and control [23, 32, 33]. The goal of the project is to create a robust, widely available, and secure synchronized data measurement infrastructure. It provides different monitoring and analysis tools for better planning and reliable operation in the power grid. NASPI plans to deploy hundreds of thousands of Phasor Measurement Units across the US power grid, sampling at 30 to 120 samples per second. These data give direct access to the state of the grid at any given instant and will be shared by hundreds of applications. PMU data used by NASPI applications have varying requirements classified into four classes based on different application requirements, e.g., transient stability control as one of the most critical applications, followed by open loop control and visualization. NASPI network (NASPInet) is the "industrial grade" communication infrastructure being developed providing secure, standardized, distributed, and expandable PMU data delivery, as shown in Fig. 2.5. Its design is influenced by GridStat. NASPInet consists of Phasor Gateways (PGWs) and a Data Bus (DB). The DB includes a Wide Area Network (WAN) and other associated functions to provide basic connectivity, QoS, traffic data monitoring,

cyber security and policy enforcement over information being delivered across NASPInet. PGW serves as the access point of entities, e.g., utilities and monitoring centers to the DB. The basic communication is unicast between utilities while the publisher-subscriber based multicast data sharing are also considered.

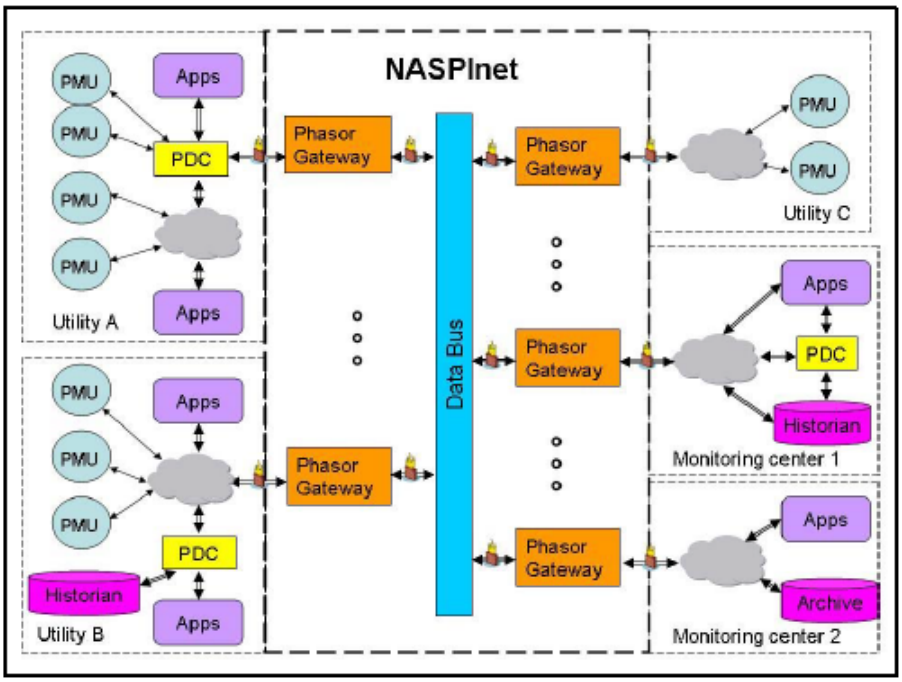


Figure 2.5: NASPInet Conceptual Architecture [32].

As one of the most critical applications, control and protective systems have stringent requirements for communications, some must have deterministic guarantees. Due to the communication limitations, real-time controls on todays power grids are mostly local, in which the data and control actions are located in a substation. The modernized communication frameworks envision to provide faster and more reliable data delivery service, which raises the opportunity to design new protection schemes from a global view. Intelligent devices (e.g., protective relays) will be able to communicate with devices in other substations/areas or the global control center, either to provide local states or receive instructions. With more information gathered, the protection should be more effective.

However, the limitations of GridStat and NASPI are obvious. First, since it is scheduled

to be implemented using dedicated networks, a large installation cost is expected. As today's power grid is becoming larger and larger, and more SG substations have not been deployed yet. Besides, more and more SG applications and services are being developed, many of which are real-time applications and require large amount of resources. GridStat allocates resources between each of the senders and receivers to guarantee the service latency. Although we can allocate "sufficient" bandwidth at the planning stage of the network, the fast growing applications may still cause potential congestions. Moreover, the static paths between the two ends are prone to deliberate attacks. Therefore, many reliable and efficient schemes are desired to address these issues. Our work focuses on some issues in these areas.

2.2.4 Smart Grid Applications

With the help of high speed communication networks, synchronized phasor data can be delivered within a few seconds to milliseconds [23]. The availability of these measurements makes it possible for new and improved applications, especially the critical remote control and protection applications.

Protection system is an important component in SG, which protects system reliability by addressing inadvertent compromises of the grid infrastructure due to user errors, equipment failures, and natural disasters. Two types of schemes are considered in protection, (1) failure prediction and prevention, and (2) the failure identification, diagnosis, and recovery. With the PMU data, stability regions and operational margins can be computed to efficiently identify potential weak points in the power grid. If a failure happens, the failure identification, diagnosis, and recovery function will locate and identify this failure, to avoid further cascading events. The critical issue to the successful protection is the quality of control. Once a potential failure is forecasted, or certain components of the grid experience failures, accurate and proper control actions should be taken. For critical protection, the requirement of control is rather stringent, e.g., the command should be received at remote areas and performed in certain order within the specified time period.

Today as local controls still work in the designed manner, the integration of local power

micro-grids requires a coordinated control method to take care local events while making decisions from a global perspective. The concept leads to wide-area control, whose main objective is to improve the overall stability of the power system. Since the control system is becoming more and more stressed each year, distributed control is combined with traditional centralized control for higher efficiency. The control components in the order of increasing complexity are: frequency control, regional voltage control, small signal stability control, voltage stability control, and transient stability control [19]. The existing control is becoming more difficult as it requires more status variables, higher computation ability, and more rapid communications, especially for online real-time adjustments at the time of event (at the time frame of milliseconds), e.g., addressing disturbances or actions to be performed in a strict order.

In addition to wide-area control and protection, another category of applications is the enhancement of control functions, e.g., system state estimation, contingency analysis, and situational awareness. The availability of phasor measurements at a much faster rate makes it possible for operators to get a more complete view of the grid status than the slowly collected data from existing SCADA systems. Most existing state estimation methods are slow without the availability of synchronized phase angles. Since the state measurement of the system is the basic parameter for wide-area control, the direct measurement can be applied immediately and produce new protection and control algorithms to cover a wider geographic area. As an example, with the renewable generation being connected to the macro-grid, analyzing the details in the system to predict oscillation and taking control is difficult, thus it is crucial to detect and report the occurrence of such situation in real-time [23].

2.3 Existing Power System Protection Schemes

Power system protection deals with the protection of power grid from faults through the isolation of error-functioning components from the rest normal network. Modern power systems (and smart grid alike) use different types of local and remote relays to isolate such

conditions and stop disturbances from spreading. In the protection system, distancel relays (including remote Zone 3 relays) are critical in protecting transmission lines as primary and backup protection, and they are universally deployed in protection systems [34, 35].

2.3.1 Distance Protection Relays

Distance protection relays are one of the most common relays used for power transmission lines [34]. The operation of a distance relay is determined by the impedance measured by the relay, which is used to estimate the distance from the relay to a fault. We usually have three protection zones as shown in Fig. 2.6 [1]. Protection Zone 1 is the basic protection of a distance relay, which covers about 80% of the length of a transmission line. The protection Zone 2 covers a little more than Zone 1, usually about 120% of the length of a transmission line. Protection Zone 3 covers the first transmission line and also about 80% of the second line. We can adjust the relay settings for Zone 1, Zone 2, and Zone 3 protection, and construct both primary protection and backup protection with different delays. Normally, we use Zone 1 as the primary protection, which is almost immediately triggered when a fault is detected, e.g., with a delay of a few milliseconds. We use Zone 2 and Zone 3 protection as backup mechanisms, which are triggered after given tripping delays when a fault is detected. These tripping delays are often determined by the protection distance, e.g., a Zone 2 protection may waits for 0.3 second, and a Zone 3 protection may wait up to 1 second [1, 2].

2.3.2 Hidden Failure

Hidden failures have been considered as one of the main sources of large scale disturbances [36, 37, 38]. It is defined as "a permanent defect that will cause a relay or a relay system to incorrectly and inappropriately remove a circuit element(s) as a direct consequence of another switching event" [39]. A hidden failure occurs when incorrect system states or control actions are triggered by another system event. It may induce widespread cascading failures such as the Northeastern blackout in 2003, which is initialized by a false

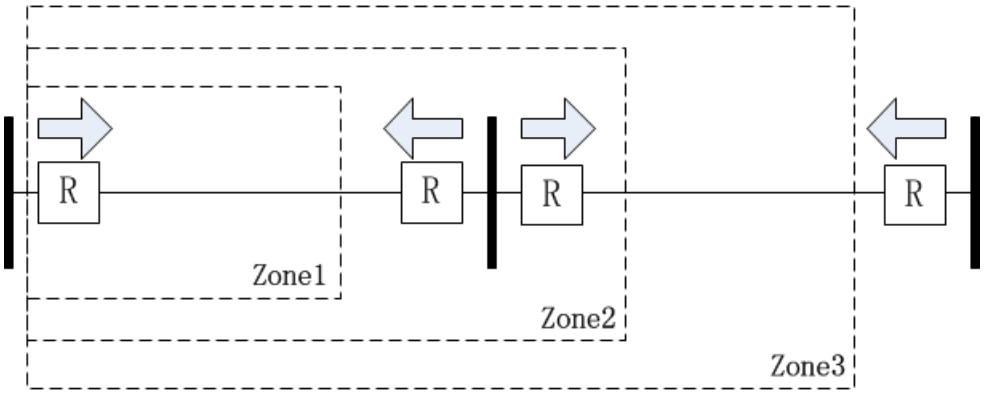


Figure 2.6: Distance Protection Relays: Zone 1, Zone 2, and Zone 3 [1].

relay trip [22].

There are primarily two types of hidden failures: hidden failures related to mal-behavior of hardware and hidden failures related to specific settings, human errors, and negligence. A typical form of hardware related hidden failure is that, a relay contact is always open or closed, regardless of the current system status. This type of hidden failures can hardly be improved by introducing communication and information exchange. For the second type, with advanced communication network, a relay can receive instructions from a control center, which minimizes the consequence of the hidden failure. Although solutions to hidden failures on traditional power systems have been extensively investigated [1, 39, 40], it is still extremely challenging to completely prevent such failures on increasingly complicated large-scale power systems.

The false trips of Zone 3 relays are often associated with hidden failures [40], as shown in past events. Such false trips have been identified as one of the main causes of blackouts (about 70% [37, 41, 42]). In the meantime, Zone 3 protection is also considered essential to power systems as many systems still rely on such protection in practical operation [34, 35]. To prevent false trips, control decisions may be made by gathering more information from other protection devices.

A protection scheme is proposed in [43] to improve the reliability of protective relays. As the first step, an exhaustive search is performed in the power grid to identify critical

locations where lines will have potential hidden failures as well as consequences of such failures. Then at potential places that may result in serious consequences, three relays are deployed for each transmission line . Based on the pre-defined system state, if it is "stressed", at least two relays must detect the contingency in order to trip the line. The idea is to minimize the "possible false tripping" rather than maximizing the correct action. With more advanced communication technology and infrastructure being applied in smart grid, a promising scheme is proposed by using real-time data collected from the grid.

2.3.3 Agent-based Protection

Agent-based protection methods use a query-response model to avoid Zone 3 false trips. Modern microprocessor-based digital relays are more reliable and efficient than traditional electromechanical ones. A software agent can be deployed at each relay. When a Zone 3 relay r detects a remote disturbance from a transmission line l, it will send a query to a Master Agent (MA) to verify if such a disturbance has been detected by other relays associated with the same transmission line. The MA then queries all related relays to pull their readings. After the MA receives all responses from these relays, it can determine if the disturbance on line l is a real fault or simply a temporary error. The MA sends a decision to relay r to inform it how to react.

Two types of protection schemes can be developed: Centralized-MA based and Peer-to-Peer (P2P)-based protection [1, 2, 44]. In an MA-based scheme, a master agent is setup in the grid, which is usually at the area control center. The benefit of a centralized scheme is that the MA has a global knowledge of the system because device status will be periodically retrieved from each substation. When PMUs are deployed, the collected information can be more accurate than existing schemes. In a P2P-based scheme, each relay is equipped with certain processing ability, which serves as an MA for itself and a few related relays. Once a relay senses an abnormal condition, it will communicate with other primary and Zone 3 relays to check whether it is a "real" error or simply a disturbance. Using P2P mode can greatly shorten the response time, which is critical in emergency cases. The potential

disadvantage of P2P mode is that most relays are only aware of local status, e.g., several neighbor buses and lines. Sometimes we need to consider whether the action of a relay will affect the global system, especially in areas with extremely high reliability requirements. As an alternative, a hybrid scheme combining both MA-based and P2P-based schemes deserves further exploration. The hybrid scheme has advantages from both methods, and is able to balance both response latency and reliability requirements.

Ideally, such a solution can eliminate most over-sensitive trips of Zone 3 relays, assuming that there is only one transmission line error in the system and the query-response process can be completed before a relay r is tripped based on its setting. However, as we have mentioned in previous section, the network delay requirement may be violated in real networks. Moreover, the existing agent-based schemes assume ideal dedicated network paths between protection relays and their master agent for real-time monitoring and control [1, 2, 45], without considering the details of network resource condition and potential reliability problems. Therefore, we have to consider practical network issues (e.g., network resource management and potential failure of communication links) to further improve the reliability of Zone 3 protection, which will be illustrated in the following chapters.

For the backup communication protection, fast reroute (FRR) [46] is a promising technology to enable fast traffic recovery upon link or router failures for mission critical services, which can recover impacted traffic flows at the level of 50ms. In the IP domain Loop-Free Alternates (LFAs) and not-via technology have been used for recovery upon the failure of a default next-hop [47]. As a basic scheme, routers may use HELLO request to detect whether a neighbor router is reachable. If a few intervals pass (e.g., can be within several seconds) [48] and the sending router has not received an ACK, then a failure is detected. In addition, with more advanced technologies such as Bidirectional Forwarding Detection (BFD), the forwarding path failure can be detected within 50ms [49]. The basic FRR schemes primarily consider how to bypass the failed nodes or links, and do not focus on specific performance requirement. On the other hand, in Multiprotocol Label Switching (MPLS), resource reservation protocol (RSVP) traffic engineering (RSVP-TE) can be ap-

plied on pre-established paths to provide guaranteed service. This technology can better help in design of backup schemes. In addition to the normal MPLS paths for normal communication, a second path from each node to the destination should also be setup in the network. Certain amount of resources will be reserved for backup usage. With BFD, a failure can be detected in real-time scale, and the failure will be reported in the network, to all nodes that may use the affected paths (e.g., using multicast). As a result, each affected node will be aware of the failure, and FRR will take place that backup paths are to be used. By using the pre-established backup paths, packets can be quickly rerouted to their destinations. The backup scheme may degrade link utilization a little, but it can significantly improve the reliability of agent-based protection when failures occur, by dramatically decreasing the convergence time (compared with traditional network convergence time of tens of seconds) and considering end-to-end performance requirement.

2.4 Smart Relay Attacks and Protection

Backup protection mechanisms are integrated into relay protection systems to provide redundancy if the primary protection does not work. Traditionally it is is considered more important to make sure that power supply is available when needed [50]. In smart grid, advanced communication technologies enable more promising protection schemes such as agent-based protection and reputation-based trust relay protection. However, existing protection schemes focus more on reliability and efficiency rather than potential malicious cyber attacks to the system. Different from the traditional mechanical or environmental threats, a well-planned cyber attack can involve an intelligent adversary with the capability to bring the system out of service [51]. With new technologies utilized, malicious attackers now have more choices to disrupt the power system [3, 52, 53, 54]. More specifically, by exploiting the potential vulnerability of protection schemes, attackers may penetrate the network and gain access to critical system components [55, 56, 57]. In this section, we will review the related work in relay protection schemes, and discuss their limitations.

2.4.1 Category of Cyber Attacks

Cyber attacks in smart grid can be classified into the following four types [52, 53]:

Device Attack: device attack aims to compromise (control) one or multiple grid devices. This attack is usually the initial step of a more sophisticated attack, in which the compromised devices can be used to launch further attacks. For example, the compromised circuit breaker may be used to trip a transmission line.

Data Attack: data attack attempts to modify critical data or command transmitted in the network so that the accuracy of decision making may be degraded.

Privacy Attack: privacy attack aims to acquire private information. As detailed information is collected periodically or in a real-time manner, this may reveal the critical data of users and operators.

Network Availability Attack: availability attack usually takes place in the form of Denial-of-Service (DoS). The goal is to consume communication and computation resources, and cause delay in the processing of critical data.

2.4.2 Advanced Relay Protection Scheme

To enhance the reliability of relay protection operation, basic agent-based protection and enhanced agent-reputation-based protection are proposed.

Basic Agent-based Relay Protection: modern microprocessor-based digital relays enable us to develop agent-based relay protection schemes, which are more reliable and efficient than traditional electromechanical ones [1, 2, 7, 58]. A relay in the system consists of three main components: a software relay agent, a sensor measurement mechanism, and a circuit breaker, as shown in Fig. 2.7. A relay agent can communicate with a control center or peer relays to determine which action to take when relay sensors detect a potential issue.

Enhanced Agent-reputation-based Relay Protection: this reputation-based scheme was developed to further improve the reliability of agent-based relay protection, by utilizing communications and trust information [6, 7, 59] among peers in smart grid. Under P2P protection mode, a relay agent periodically exchange messages with a set of preselected

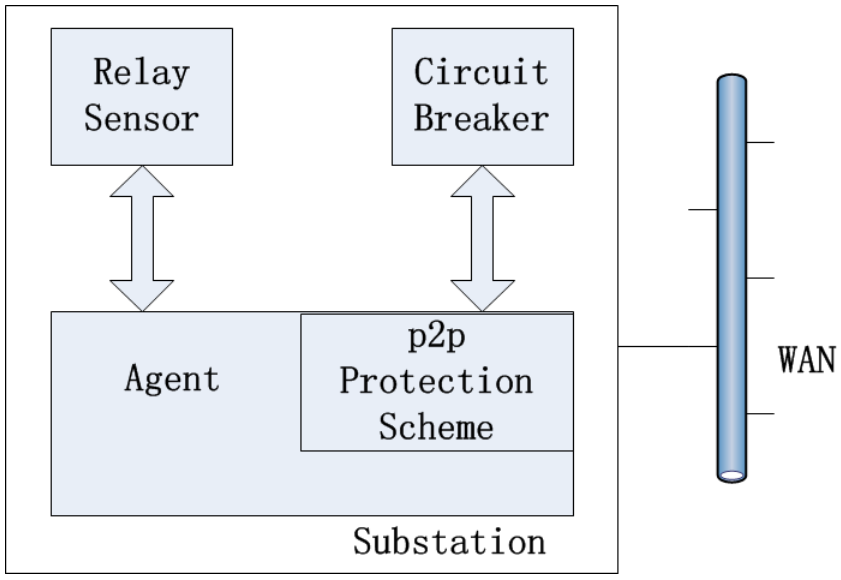


Figure 2.7: Agent-based Relay Protection Architecture.

relays in a protection area to monitor each other's reading. Here, a *protection area* is used for protecting a transmission line. It usually consists of two primary relays at each side of the protected line, and several neighbor lines where its Zone 3 backup relays are located. In the basic trust evaluation scheme proposed in [6], a relay uses the responsiveness and consistency of peer replies to estimate the trustworthiness, e.g., using the number of received updates within a given period to generate a trust value of each other based on EigenTrust [60]. The update message includes the operational responses of conventional relays, the status of circuit breakers, or the current and voltage values. The reputation of a remote relay is then determined by the local agent at a relay, and is used to help make trip decisions. (For potential advanced metrics, not examined in [6], a remote reading could be compared with a local reading to further evaluate the trust value for the peer relay.)

2.4.3 Trip Confirmation in Reputation-based Relay Protection

Confirming a trip based on reputation is conducted in the following steps:

(i) When the sensor component of a primary relay detects a local fault, the primary relay agent will immediately send a trip signal to its circuit breaker to trip the line, and send a

request to another trusted Zone 3 relay (with a trust value above a threshold) to verify if the line fault is viewed by the remote relay. If the response indicates the trip is incorrect, the agent will reclose the circuit breaker, but a trip may already occur. In addition, if the agent cannot get a response from a trusted remote relay, it will revert to a traditional relay action with a regular delay.

(ii) If a relay protection component sends a trip signal to its circuit breaker indicating a Zone 3 fault is detected, at least one trusted relay agent (either a primary relay or backup relay agent) in the same protection area must detect a corresponding Zone 1 fault [1, 6]. This mechanism assumes that the trusted relays are not compromised and work normally. As a result one reply from the trusted peers will be sufficient, even if there may be different answers from other peer relays. In addition, this scheme may also speed up the decision making process.

(iii) If a trip request is received by a relay agent from another trusted agent, whether the relay operation is in progress (e.g., a fault is detected), if it is confirmed by a trusted agent, the relay will trip the line. Normally, the trip request is sent from a primary relay to its Zone 3 backup relays at the same side (facing the same direction as the primary relay). According to the trust mechanism, one trusted reply is sufficient to continue the process.

2.4.4 Definition and Cause of Cascading Failure

In a cascading failure a triggering failure produces a sequence of secondary failures [61, 62]. A cascading failure usually starts from a minor failure, e.g., a transmission line trip or short circuit, followed by a series of other components outages. If proper control is not taken within a certain period of time, the contingency will soon spread through the power grid and eventually results in serious consequences [63, 64]. In the initial stage of many cascading failures, the malfunction of protection relays is one of the primary reasons - NERC (North American Electric Reliability Council) studies of major disturbances have shown that more than 70% of the major disturbances involved relaying systems, not necessarily as the initiating event, but contributing to the cascading nature of the event [36].

Initialized by one or more events, cascading outages can cause large-scale blackouts, and result in massive disruptions of electricity service. The initial events are usually from diverse sources, such as disturbances caused by natural disasters, human errors, or cyber attacks. It has been reported that millions of cyber attacks can happen everyday [65], which pose a tremendous challenge to the power system operation.

In summary, our work will investigate relay protection schemes from the perspective of cyber security. We assume that smart devices can be compromised, if the attacker spends certain amount of resources attacking the devices. Our focus is how the attacker can trip transmission lines in power system by exploiting existing relay protection schemes, with given amount of available resources. We identify several potential attack strategies, and analyze their effects to relay agents.

2.5 Synchronized Routing

2.5.1 Service Framework

Supporting large-scale real-time applications across multiple domains is a challenging topic. Since smart grid will connect geographically separated areas, and many of the critical applications (e.g., monitoring and protection) have "hard-requirement" for data latency, we need to carefully design the SG communication network. A lot of researches have been proposed to address the quality of service for data delivery across Internet, primarily based on resource reservation. Two important service frameworks are: *IntServ* and *DiffServ*.

IntServ (Integrated Services) [8, 9] provides end-to-end guaranteed or controlled load service on a per flow (individual or aggregate) basis, and requires the maintenance of per-flow state at each router (e.g., per flow signaling messages). It also implements classification, scheduling, and buffer management on the per-flow basis. Before the communication is set up, RSVP (Resource Reservation Protocol) is used to reserve sufficient resources for a flow. The key limitation of IntServ is scalability: maintaining per-flow state will be much more difficult when the number of flows goes up.

DiffServ (Differentiated Services) [8] is proposed to address the problems associated with IntServ, which is based on a per-aggregate-class based service. DiffServ redefines the seldom used bits in a packet header to be DSCP (Differentiated Service CodePoint). These bits are then used to indicate the type-of-service (TOS) for a packet. In DiffServ, packets with the same TOS will be treated as the same class. When a packet enters the DiffServ domain, the boundary router updates the DSCP, then each core router within the domain will serve the packet in a per-hop behavior (PHB) based on the DSCP bits. There is no need to maintain per-flow state in DiffServ, which addresses the scalability problem of IntServ.

2.5.2 Scheduling Methods

The delay of a data packet consists of three parts: propagation, transmission, and queuing delay. The propagation delay is related to the distance, the medium, and the speed of light. The transmission delay is determined by the size of packet and the bandwidth of a link. Today, with the advanced communication technology such as fiber optics, the propagation and transmission delays are no longer the primary issues. The queueing delay is the waiting time that a packet spends in a router until it is transmitted, and this part is usually dominating the end-to-end delay of a packet. To control the queueing delay, various service frameworks apply different scheduling policies. We summarize the existing scheduling disciplines as following:

(1). First Come First Serve (FCFS) [66] is the simplest scheduling policy. It does not consider any performance assurance but serves all packets in the order of their arrival times. FCFS is the simplest mechanism to be implemented. Because of this, many communication networks especially those focusing on providing best-effort still favor FCFS.

(2). Generalized Processor Sharing (GPS) [66, 67] provides good flow isolation, by assuming that multiple flows are divisible and can be served simultaneously. Each flow i is assigned a weight ω_i. If there are N flows and the link capacity is C, flow i will be guaranteed the rate of $r_i = \frac{\omega_i}{\sum_{j=1}^{N} \omega_j} \cdot C$. However, the assumption of GPS makes it impractical to be realized since the service of data has to be packetized. To address this problem, Packetized

Generalized Processor Sharing (PGPS), also known as Weighted Fair Queuing (WFQ) is proposed to provide the approximation of GPS. The packets under PGPS are served in the increasing order of their computed departure time under GPS.

(3). Earliest Deadline First (EDF) [68, 69] assigns each flow i a delay bound d_i. For a packet arriving at time t_0, it will be assigned the sending deadline of $t_0 + d_i$. EDF applies a greedy algorithm that packets are served in an increasing order of their assigned deadlines. EDF is usually coupled with admission control or traffic shapers to isolate flows and provide guaranteed rates.

(4). Modified First-in-First-out (FIFO+) [70] measures the average delay of packets from different flows on each hop. For each packet i departing from hop j, the difference between the particular delay seen by the packet and its class average delay is computed, defined as service offset a_i. Then at the next hop $j + 1$, assume the arrival time is t_0, the priority of packet i will be $t_0 + a_i$, which represents the time packet i "should have arrived" according to average service.

(5). Coordinated EDF (CEDF) [71] is developed with the goal of minimizing end-to-end delays with coordination between the deadlines on a packet's path. The key is to determine how to partition delay among all hops along a path. The limitation of CEDF is it is difficult to provide predictable performance, and the allocation of total delay may not be suitable for a dynamic network, or a path with link failures.

(6). Core-Jitter Virtual Clock (CJVC) [9] proposed as a mechanism for achieving guaranteed service without per-flow states at core routers. The key idea in CJVC is the dynamic packet state that encodes scheduling parameters in each packet's header at the time it arrives at the edge routers. Each packet has an eligible time, and this time is no smaller than the deadline of the previous packet from the same flow to ensure the service order.

(7). Coordinated Multi-hop Scheduling (CMS) [72, 73] exploits property of coordination, in which excessive latency or unfairness incurred at an upstream node can be compensated at a downstream node, or the priority of a packet that arrives ahead of scheduled time can be reduced at a downstream node. The definition of CMS is as following: for a packet k

from flow i arriving at the hop j, its priority is defined as:

$$f(n) = \begin{cases} t_{i,1}^k + \delta_{i,1}^k & j = 1 \\ d_{i,j-1}^k + \delta_{i,j}^k & j > 1 \end{cases}$$

where $t_{i,1}^k$ is the arrival time of the packet at the first hop, and $\delta_{i,j}^k$ is a local adjustment variable with a finite range. The adjustment variable is pre-determined based on the statistical pattern of incoming traffic at each hop, thus its effect is limited in dynamic traffic.

In summary, the reservation-based methods have limitations due to their scalability, as the number of real-time applications is greatly increased; meanwhile, these methods are not always applicable in resource-constrained environments, e.g., wireless links in SG. Coordination of routers have been examined in several projects, however, they only focus on a local or partial view and have limited service adjustment ability. We will explore the global synchronized time as a reference to address these existing issues, for both intra-domain and cross-domain applications. As introduced in Chapter 6, two important aspects of the proposed research are: synchronized delay measurement and routing/scheduling design using the measurement. Our research will help provide real-time data delivery in smart grid, which can benefit applications like monitoring and protection.

CHAPTER 3
MAIN CONTRIBUTIONS

In this chapter we present the complete view of this dissertation, including three main research areas: remote relay protection, attack on smart relay protection schemes, and synchronized routing for predictable real-time communications.

First, we investigated agent-based relay protection in order to better understand how protection systems in smart grid work, how network resources should be managed, and how this enhanced protection can improve the reliability of smart grid. We proposed a basic resource management scheme for Master Agent-based protection. Then we improved the reliability of MA-based protection with backup paths. We further consider power system information to help backup path selection to utilize network resources more efficiently. In addition, we also proposed a resource management scheme and a backup scheme for P2P-based protection. Our results show that certain amount of resources are required to support MA-based protection, and system reliability is improved with the proposed backup scheme. When power system information is applied, we can fulfill the reliability requirement with less resources. Our evaluation also shows that P2P-based protection can achieve similar system reliability as MA-based protection while using less resources.

Second, in addition to understanding relay protection system, we examined potential cyber attacks on P2P agent-based protection schemes. Currently there is very little research on the related area. We first investigated different attack strategies to understand how direct and indirect attacks can affect relay agents. We also investigated how these attacks can trigger cascading failures in the system. We analyzed the effects of these attacks to understand how much damage can be achieved in the system. We observed that basic agent-based protection schemes cannot effectively deal with malicious cyber attacks, while a majority-based P2P protection can achieve certain improvement. We also investigated reputation-based trust relay protection, and observed that this scheme can be exploited by an attacker to target critical system components to trigger cascading failures, if the

system defense strength is relatively low. Based on our observations, we proposed several improvements to mitigate potential cascading damage due to cyber attacks on the reputation schemes.

Third, many critical SG applications have strict delay requirements. In most existing communication frameworks, data delivery latency is guaranteed using reservation based methods (e.g., pre-allocation of network bandwidth), which usually result in low resource utilization, and is hard to deal with network failures. As the number of real-time applications will be significantly increased, much higher bandwidth is required. Thus, enhancing the resource utilization is critical for the scalability of SG. To address this problem, we proposed a synchronized routing framework, utilizing the global synchronized time available in SG. Our results demonstrate that the proposed scheduling method has larger adjustable ability than existing scheduling methods, and can better fulfill the delay requirements of real-time packets.

We outline the three research areas of the dissertation in the following, and more details are presented in Sec. 3.1, Sec. 3.2, and Sec. 3.3:

1. Reliable Remote Protection for SG

   - Basic protection scheme: different from previous work that assumes dedicated links are used for protection, we first explore the problem of network resource management in real world deployment for master-agent (MA) based protection schemes. We identify the requirements for protection applications and design corresponding resource management schemes.

   - Improvement for basic protection: considering multiple simultaneous failures are rare in the network, we improve the resource utilization by focusing on single and two hidden failures in the system. We also enhance the reliability by adding backup paths in existing protection schemes.

   - Power-aware protection: to better protect the system, the basic primary path selection may choose the most reliable paths. However, as different buses and lines have different importance, we build backup paths for relays by considering system reliability

requirement, in addition to the above topology-based methods.

- Peer-to-Peer (P2P) relay protection schemes: a single MA can be easily damaged by disasters or cyber attacks, which will leave the system unprotected from hidden failures. We investigate P2P schemes as each relay can make its own control decision. We further investigate resource management for P2P relay protection.

2. Cyber Attacks on Relay and Protection

   - Understanding potential cyber attacks: attacks can be conducted directly to critical relay agents, or indirectly from neighbor agents. Furthermore, an attacker may also target certain critical relay agents to trigger cascading failures. We will look into the detailed attack process, and analyze the effects of these attacks, as well as their resource requirements.

   - Attack on reputation-based trust scheme: a basic agent-based protection can be improved by introducing reputation-based trust. As a result, the efficiency of agent-based protection can be further enhanced. However, current protection schemes focus reliability and efficiency (e.g., faster response to occasional faulty behavior) rather than handling deliberate attacks. We observe that even critical system components are well protected, an attacker can still exploit the reputation protection schemes to implement a cascading attack.

   - Improvement to existing protection schemes: the trip decision for basic agent protection schemes can be improved by requiring confirmation from the majority number of neighbors. We should also improve the defense strength of neighbor devices of the critical components. In addition, trip requests to critical relay agents can be disabled to increase the resistance of power grid to cascading-aware attacks.

3. Synchronized Data Delivery Architecture

   - Limitation of existing work: smart grid applications require high quality data communication networks. Existing solutions on data delivery primarily rely on over-reservation of network resources, which results in low utilization and may not always

feasible. They also cannot deal with large scale dynamic networks, e.g., a link may fail. The global time synchronization provides us an unique opportunity to build a new framework for real-time data delivery.

- Synchronized real-time transmission framework: in the communication network, knowing the approximate delay of a packet to a node helps us determine its proper data service order at a router. The delay is defined as the time between the sending of a packet from a source to the arrival at its destination. For a real-time packet, considering both its elapsed upstream delay and its estimated downstream delay will help ensure the on-time delivery of the packet. Two key components in the proposed framework are:
  - Delay Measurement: with synchronized time, routers can estimate real-time delay to each other and exchange their delay estimates in real-time. Upon receiving an update, a router can determine the expected delay from the router to a destination. The accuracy of measurement is critical to the real-time service.
  - Routing and Scheduling: based on the synchronized information, the proposed framework can help in two aspects: (1) By choosing a path with less potential congestion to the destination. (2) When an output link is overloaded, we can adjust the service order of output packets appropriately. Currently our work focuses on the scheduling part.

3.1 Smart Remote Relay Protection

Motivation. As device failures due to aging, natural disasters, or malicious attacks can cause serious damages to power system components and transmission lines, and generate large disturbances across the systems, current power transmission systems use various local relays and remote relays to isolate such failures and prevent disturbances from wide spreading. Among these protection devices, distance relays (including remote Zone 3) are essential to transmission lines for remote backup and broadly deployed in current systems [34, 35].

However, over-sensitive remote Zone 3 relays caused certain unexpected trips and further spread cascading failures in many cases [37, 39].

Although many solutions have been developed in traditional power systems to address this issue [38, 40, 41], they failed to eliminate the problems. As shown in recent large scale failures [37], these solutions did not stop the cascading failures due to remote relay failures in many cases. And it is noticed that many failures were made worse by cascading outages, which can be initiated by relatively small disturbances [62].

Existing Work and Limitation. The advanced communication network in SG enables us to achieve more intelligent, effective, and precise control of power systems. In this research direction, several agent-based solutions [1, 2] have been proposed to utilize SG communications to deal with the false trips of Zone 3 relays. However, existing solutions did not consider practical network issues and simply assumed dedicated communication paths in ideal network conditions. Besides, more and more new SG control and monitoring applications will be deployed across large areas for high efficiency, reliability, and intelligent protection [17, 23, 74, 75], which will consume more network resources. Therefore, we have to carefully assign and manage communication network resources to support operation of more SG applications.

Our Contribution. We first present a *static reservation scheme*. This static reservation is the baseline study because existing methods do not carefully consider resource management. For a given power grid, we select a node to be the master agent (MA) for protection control. We estimate the required network resource to support communication between relays and the MA. The resource allocation is based on the time requirement before a relay incorrectly trips a line. Through this step, we know whether a network can support the protection application, and how many similar applications can be run simultaneously.

Furthermore, we improve the basic resource management scheme with *smart reservation*, which considers the situation of only a single or two hidden failures in the system. The motivation is to make bandwidth use more efficient. The evaluation results show significant decrease in the amount of resources for reservation; and as the system becomes larger, the

saving will be much more significant. We also improve the reliability of agent protection by using *backup paths* for each of the reserved primary paths. Resource will be reserved on the backup paths as well. With the help of backup paths, the most common single communication link failure can be handled.

Third, we also consider the *selection of primary path for better system reliability.* Assume different links have different reliability, by choosing the *most reliable path* from a relay to the MA, we can minimize the failure probability of a primary path. Similar to the basic static reservation, we need backup paths to enhance the reliability as well. We further improve the resource utilization by *considering requirement from power system aspects.* By providing differentiated backup protection to critical/non-critical buses and lines, we can save more resources compared with using simple topological knowledge. With the assumption of a single hidden failure in the system, we propose an improved protection scheme that saves even more network resources.

Finally, in the centralized protection scheme, an MA node receives queries from other relays and makes a decision based on the collected system data. This mechanism usually works under normal conditions. However, since the MA is the single node responsible for the protection decision, if it is shut down due to disasters or cyber attacks, the entire grid protection application may fail, and false tripping of relays cannot be properly handled. To address this problem, the idea of *Peer-to-Peer (P2P)* based mechanism was discussed, but not fully investigated. Since existing methods do not carefully consider resource management or network conditions, we extend our MA-based resource management scheme, and develop several P2P-based protection schemes and corresponding resource management schemes. Similar to MA-based protection scheme, we explore the resource management problem in P2P protection schemes, with different assumptions. We compare effects of different backup schemes. The evaluation shows that with different system reliability requirements, we can use different strategies to build backup paths to achieve more efficient use of network bandwidth.

3.2 Attack on Smart Relay Protection

Motivation. Electricity system is rather critical in nearly all aspects of our society. With the integration of advanced computing and communication technologies, the Smart Grid is expected to greatly enhance efficiency and reliability of future power systems. To achieve the goal, different mechanisms have been proposed, such as agent-based protection, and improved reputation-based relay protection. These protection schemes emphasize solutions to accidental faulty behaviors of relays. With trust information applied, the decision making may be more efficient and accurate when dealing with exposed hidden failures.

On the other hand, as millions of electronic devices are inter-connected via communication networks throughout critical power facilities, cyber security is becoming a more and more critical issue, which can have a dramatic impact on the normal operation of power grid. We should not only focus on improving the efficiency of protection system, but also examining their potential limitations, as such weakness may be utilized by malicious attackers to disrupt the system.

Existing Work and Limitation. Existing relay protection schemes primarily focus on the operation reliability of relays, e.g., whether there is a mechanical problem or whether a command (such as breaker action message) can be sent normally. However, the assumption of these improvements is that neighbor devices of a relay are indeed "trustworthy", e.g., they are working at the normal state. In the current stage potential cyber attacks on protection systems are not considered, which assumes (i) a relay agent is not manipulated, and (ii) the communication network is operational. Because the trusted peer protection agent handles situations using status verification and protection behavior confirmation, this can be exploited by malicious attackers as well. For example, when a relay decides (or is requested to trip a line), a *single confirmation* from a trusted peer agent is required to confirm the action. Trusted relays are critical in protection, they may not be easily compromised; however, agents are not absolutely immune to attacks neither.

Our Contribution. First, we investigate effects of different cyber attacks on agent-based relay protection schemes, as there is very little research in this area, to the best

of our knowledge. We characterize the potential attacks into three categories: random attack, area-based attack, and cascading-aware attack. We divide the power system to a set of protection areas, with each area containing a primary line and several backup lines. We assume that a relay protection agent can be compromised if an attacker spends certain amount of resources attacking the agent. The goal of the attacker is to disrupt the system by tripping as many lines as possible. Attacks can also be classified as direct or indirect attacks to relay agent. We analyze potential damages of these attacks to the system. Through the analysis, we better understand how these attacks can affect the system. Our results show that basic agent-based protection schemes can be exploited by attackers to produce more damages than directed attacks.

Second, we observe that by using a majority-based confirmation rule, the damages of attacking the basic agent protection can be significantly lowered. We also investigate the attack on reputation-based protection. We notice that the weakness of existing reputation schemes can be exploited by the attacker to compromise critical relays, and then trigger cascading failures. We analyze the possibility of triggering cascading failures in the system for both direct cascading attacks, and reputation-based cascading attacks. The results show that if system defense is low, the reputation-based scheme may even make it easier for the attacker to launch a cascading attack, either with a higher probability, or consuming less resources. We consider that both the critical devices and their neighbor devices need a higher defense level. In addition, the system can also disable trip requests to critical relays for better security. This may degrade the efficiency a little, but can increase the difficulty of deliberate cyber attacks that intend to trigger cascading failures.

3.3 Synchronized Real-time Data Delivery

Motivation. Smart grid is more than an energy network, it should provide intelligent distribution and consumption, as well as diagnose, self-healing, and protection. These functions are achieved mainly by the integration of information and communication technologies. In smart grid, the communication network is responsible for gathering and routing data,

monitoring all nodes and acting upon the data received. Our expectation of this data delivery network can be summarized as high performance, highly reliable, scalable, ubiquitous, and secure.

Following several large blackouts around the world, there arises the need for a more effective way to monitor, control and protect, so that incidents would not escalate and cascade into a big collapse. The real-time feature is emphasized as a design requirement. In this direction, one of the areas that has been rapidly gaining interests is the Wide Area Monitoring Systems (WAMS). The core idea of WAMS is collecting critical data from a large region of the power grid through the use of synchronized phasor measurement unit (PMU), which takes synchronized measurements at rates of 30 to 120 samples per second. IP-based networks are favored in turns of reduced cost, configuration complexity, and can maximize the network scalability.

Existing Work and Limitation. Most of the WAMS applications have very strict delay requirements for delivery. For example, PMU data should be delivered within 20ms. The late arrival of some real-time data usually means the information will be of little use, or there will be serious consequences due to delayed operations. This imposes a relatively high requirement for the communication network. Traditionally, many methods have been proposed based on the pre-estimation of application requirements and the corresponding reservation of network resources. The reservation methods can be characterized as *hard guarantee* and *soft guarantee*. Hard guarantee ensures each application is allocated with dedicated and sufficient resources for communication, while soft guarantee manages resources based on different application classes. Both methods have their limitations. Hard guarantees usually result in a low utilization of network resources and less scalable infrastructure; while soft guarantees can not distinguish the data urgency among applications of the same class, especially in complicated situations when the priority of applications must be changed.

Our Contribution. We explore a new direction - *the predictable real-time delivery*. The main idea is that each router in the communication network uses knowledge of the end-to-

end delay estimation to determine the service priority of packets. As the knowledge is real-time, it provides an accurate view of the network, and routers can work in a cooperative and adaptive way. A few methods in the similar direction primarily focus on local adjustments since they did not explore globally synchronized information. Without knowing the global state, the adaptivity of transmission service can be limited. We identify the potential improvements by using globally synchronized data. On one hand, the knowledge helps determine the service order of packets when traffic congestion happens; on the other hand, it may also help determine a path to the destination with less potential congestion. We choose a global time as the reference, thus the time synchronization technology is the fundamental component to build this framework. As smart grid is designed to have a precision time resolution, the synchronization technology is integrated in most critical areas, and it can be used by the proposed communication network. We have proposed a synchronized routing framework and evaluated the effectiveness of its scheduling scheme. Our results show that our scheduling scheme has a larger adjustment range than existing scheduling schemes, and can better fulfill the delay requirements of real-time data.

In summary, first we developed resource management schemes for smart remote relay protection. Second, we investigated the potential cyber attack and defense for relay protection systems. Third, we proposed a synchronized routing framework for predictable delivery.

CHAPTER 4
SMART REMOTE RELAY PROTECTION

In power grids, distance relays are widely used to protect the transmission lines from short circuit faults. However, some over-sensitive remote relays were tripped due to various reasons and generated cascading failures in recent large scale blackouts. In smart grids, as digital relays with advanced microprocessors will take the places of traditional relays, several protection methods have been proposed to deal with false trips. These methods show great potential but do not address problems related to the communication networks. In this chapter, we propose several network resource management schemes using both network topology and power system information to improve the reliability of protection system.

4.1 Background

In the emerging smart grid, many intelligent devices are employed to monitor and control power system components, which allows us to achieve more effective protection for dealing with the false trips of remote relays. These devices communicate with power control systems on real-time networks, provide instant system status, and conduct precise control. In this research direction, agent-based protection systems have been designed [1, 2] to utilize SG real-time communications to prevent the false trips of remote relays. The existing methods simply use TCP/UDP transport protocols to deliver monitor and control messages without bandwidth and delay guarantees, and simply assumed ideal dedicated communication network paths. They did not address practical network issues due to many potential errors such as simple traffic congestion, routers/links errors or misconfigurations, or malicious attacks that cause bandwidth and delay violations on communication paths. Meanwhile, more and more SG applications and services are being developed and deployed, thus we cannot simpy assume a dedicated network without failures.

To fill this gap, we first focused on methods for basic network resource management for ensuring bandwidth and delay guarantees, and we further propose a simple backup

method [10]. We also designed a power-aware protection scheme [12] by exploiting known information about power systems in order to define power line priorities based on their importance. As we mentioned in the previous chapter, there are two types of agent-based protection schemes — the Master Agent (MA)-based and P2P-based schemes. They have different resource reservation requirements. We also investigate the the resource management in P2P schemes [11].

4.2 MA-based Resource Management

4.2.1 Basic Reservation Scheme

Existing agent-based protection schemes assume an ideal network and do not consider resource management. Here we present a basic solution to reserve network bandwidth for each application in the MA scheme to address the potential network congestion issues. We will use this scheme as a baseline and propose several improved schemes. In such a scheme, we first determine a location to put the MA on a network and then figure out the corresponding reservations on each communication link for each Zone 3 protection relay. We use a hop-distance heuristic to locate the MA at approximate the center of the topology. When we build a spanning tree of the topology with the MA as the root, we make the tree have the minimum height. For the ease of discussion, we assume that all links have the same weight and identical capacity. We use B to denote the entire set of buses for a power transmission network. Then, we sort the buses in B based on their hop counts to the MA in a decreasing order. For bus $b \in B$, we identify the set of power transmission lines L_b that connect b with other buses; for power line $l \in L_b$, we then find the set of relays R_l associated with this line, including both primary and backup relays. In an agent-based protection process, four steps between a relay r and the MA introduce communication delays: (i) A query is sent from a Zone 3 protection relay r to the MA, when it sees a temporary issue (e.g., a voltage surge); (ii) Once the MA receives the query from r, the MA checks with other related relays $\{r'$: $r' \in R_l$ and $r' \neq r\}$; (iii) A response is sent from each r' to the MA; (iv) the MA makes a

decision based on the responses and sends its decision to r. To avoid a false trip at r, the total delay for the above four steps cannot exceed the delay requirement configured at r. As we know the delay requirement from a relay to the MA, we can ensure the transmission delay via link capacity reservation.

We determine the delay requirement from a relay to the MA based on the following procedure. For $l \in L_b$, we find two relays r_1 and r_2 from R_l, who have the *largest* and the *second-largest hop count* h_{r_1} and h_{r_2} to the MA, respectively. (When network links have different capacities, we can then use the minimum path delay for this step.) The delay requirement of Zone 3 protection of each relay is initialized to a default value D_0. (For ease of illustration, we assume that all Zone 3 relays have the same requirement. However, the requirement of each relay could be different constants, and we can represent them as $D_0(r_i)$ for relay r_i.) To ensure the delay requirement in the Zone 3 protection procedure, we proportionally divide the total delay requirement between these two relays: in case that one is a Zone 3 relay starting the query process and another is among the relays that respond to the MA. That is, the delay requirement between r_1 and the MA is set to $d_1 = \frac{h_{r_1} \cdot D_0}{2(h_{r_1}+h_{r_2})}$; the delay requirement between r_2 and the MA is set to $d_2 = \frac{h_{r_2} \cdot D_0}{2(h_{r_1}+h_{r_2})}$. For other relays of l, their round trip delay requirements are set as no larger than d_2, because their path lengths to the MA are equal or smaller than the length from r_2 to the MA. There is no need to make the other relays to respond faster than r_1 and r_2. (As a relay may be used to protect multiple different lines, it may have different settings. In general, we use the minimal setting of a relay as its preset delay for Zone 3 protection.) The delay assignment algorithm is given in Algorithm. 1.

Once we have the delay assignment for each relay, we can then reserve corresponding bandwidth on the path from the relay to the MA. As the path has h_r hops from a relay r to the MA, we equally divide the path delay requirement d_r at each hop as per hop delay requirement d_r/h_r, as in many existing methods. (We will further discuss other advanced assignment methods in the next section based on more concrete system requirements for comparison.) For ease of illustration, we assume all the request and response packets have

Algorithm 1 Delay Requirement Assignment Algorithm for Zone 3 Protection Relays.

Input: Transmission Line set L of a Power Network and Delay requirements for Zone 3 relays

Output: Delay Assignment D for Zone 3 Relays

Method:

1: **for** each relay r in the system **do**
2: $d_r = \infty$ ▷ Initialize all delay assignments of relays
3: **end for**
4: **for** each line $l \in L$ **do**
5: Find relay r_1 and relay r_2 in R_l ▷ Find two relays furthest from the MA with hop counts h_{r_1} and h_{r_2}
6: determine d_1 for r_1 and d_2 for r_2
7: **if** $d_{r_1} > d_1$ **then** ▷ d_{r_1} is the current assignment for r_1
8: $d_{r_1} = d_1$ ▷ Assign a new delay requirement to r_1
9: **end if**
10: **if** $d_{r_2} > d_2$ **then** ▷ d_{r_2} is the current assignment for r_2
11: $d_{r_2} = d_2$ ▷ Assign a new delay requirement to r_2
12: **end if**
13: **for** each relay $r \in L_l$ and $r \neq r_1$ and $r \neq r_2$ **do**
14: **if** $d_r > d_2$ **then** ▷ d_r is the current assignment
15: $d_r = d_2$ ▷ Assign d_2 to r
16: **end if**
17: **end for**
18: **end for**

the same size of L_0. Then, the capacity to be reserved at each communication link l on the path j from r to the MA is: $C_{rsv}(l,j) = \frac{L_0 \cdot h_r}{d_r}$, where d_r is the delay assignment of relay r obtained based on Algorithm. 1. When we consider that k paths from different relays share a link, the total reservation on a communication link l is denoted as $C_{rsv}(l)^{Total} = \sum_{j=1}^{k} C_{rsv}(l,j)$, where $C_{rsv}(l,j)$ is the reservation for r whose path j contains link l, and k is the total number of paths containing link l. We present the bandwidth reservation algorithm in Algorithm. 2. Note that this requirement is only for a *single* protection application.

As we mentioned, with the development of SG, more control and monitoring applications will be deployed, such as the Zone 3 protection or Phasor Measurement Unit (PMU) applications. When we have to support many real-time applications, the reservation with the above scheme will quickly grow in proportional to the number of applications. Given a network with fixed network link capacity, we can find out how many applications can be

Algorithm 2 Bandwidth Reservation Algorithm for Zone 3 Protection Relays.

Input: Relay Zone 3 Delay Assignment D.
Output: Bandwidth Reservations on Link Set L.
Method:

1: **for** each network link $l \in L$ **do**
2: $b_{rsv}(l) = 0$;
3: **for** each path from r to the MA containing link l **do**
4: $b_{rsv}(l) = b_{rsv}(l) + C_{rsv}(l, r)$;
5: **end for**
6: **end for**

support on the network. As we know, there are many potential applications that have the similar or higher level of traffic requirements as Zone 3 protection. Zone 3 protection is just one of many control and protection schemes.

4.2.2 Improved Reservation Scheme

When using the static method presented in the above, the number of applications that can be assigned on a linke l is determined as $MIN\{\frac{C_l}{\sum C_{rsv}(l)}\}$, where C_l is the total capacity of link l. For example, in the 39-Bus system, assume the corresponding communication link capacity is 5T1 ($1.544Mbps \cdot 5$), for all links [33]. Then on such a system, if consider all applications to be the same priority such as Zone 3 protection, with similar reservation requirements, we can then support at most 26 such applications on this system; for many other applications (such as PMU applications) that usually have high bandwidth requirements, only a few real-time applications can be supported on this network.

We also consider more specific conditions in practical systems to further improving network efficiency. In general, we usually see very few relay errors simultaneously. In most cases, we often have a single failure in the system. As a result, only one protection area is involved in communications with the MA. In such a single failure case, we do not have to reserve bandwidth for all relays at the same time, instead we reserve the maximum bandwidth requirement if multiple relay-to-MA paths are overlapping on a link. Given the system topology, for each power transmission line l_p, we can identify its protection area that includes a set of relays R_s that are responsible for the protection. We divide these relays into

two sets: primary relay set R_p and backup relay set R_b. In general, a relay knows which line it is monitoring. Then for a transmission line, the abnormal reading at a backup relay will result in a fixed set of relays R_s communicating with the MA. (As primary relays will take actions almost immediately when abnormal readings are detected, in general they do not need to consult the MA for making a decision.) Notice that usually a communication link l is shared by different subtrees that the reservation on the link should fulfill the requirement of all subtrees. However, due to the high requirement of the reliability of power system, a single failure at a relay is the most common error so that not all relays in the subtrees have data to send.

We provide an example for demonstration. Fig. 4.1 shows the IEEE 13-Bus system, and Fig. 4.2 shows two protection areas for the system. Area 1 and Area 2 are partially overlapped protection areas for power transmission lines $Line_1$ and $Line_2$, respectively. The two target transmission lines are marked as the red bold line between r_3 and r_4 and the green dotted line between r_1 and r_2. Here we have seven relays: four relays only belong to Area 1 (red rectangles r_3, r_5, r_8, and r_{10}); one relay only belongs to Area 2 (the green triangle r_2); and two relays are used in both areas (blue solid rectangles r_1 and r_4). Assume for relay r_i, the required capacity on a link l is $b_{rsv,i}(l)$. On communication link $Line_5$, Area 1 needs a bandwidth reservation of $\sum_{i=1,3,4,5,8,10} b_{rsv,i}$, while Area 2 needs a bandwidth reservation of $\sum_{i=1,2,4} b_{rsv,i}$. Under the condition of single relay failure, only one area would communicate with the MA across communication link $Line_5$, although this link is on the paths for all seven relays to the MA. When any of Zone 3 relays $\{r_1, r_5, r_8, r_{10}\}$ sends a request to the MA, traffic will be generated for protection Area 1. For protection Area 2, r_4 is the only Zone 3 relay. It may send a request to the MA due to abnormal readings on $Line_1$. It is obvious that reserving the larger requirement of these two areas on the link will achieve the protection of both areas.

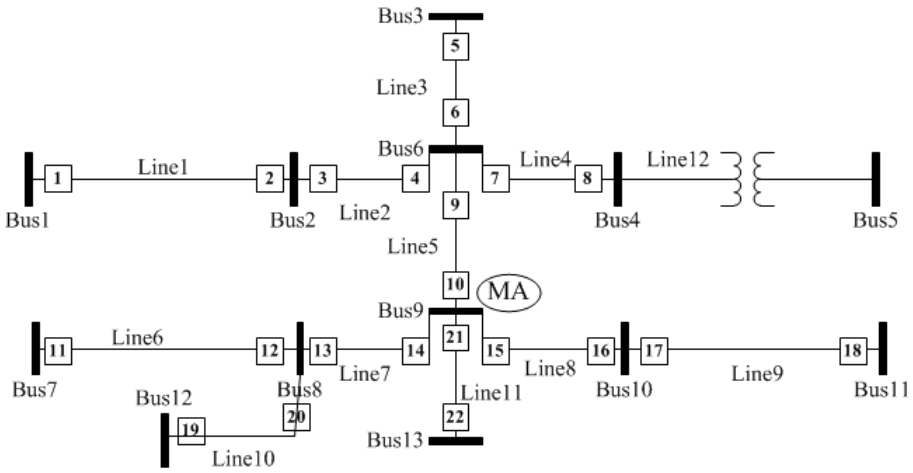


Figure 4.1: IEEE 13-Bus System.

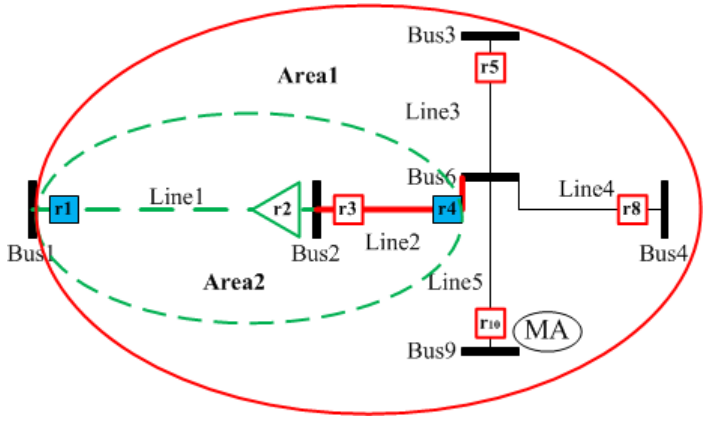


Figure 4.2: Example of Protection Areas.

4.2.3 Better Reliability with Backup Paths

In real-world deployment, the system faces various issues due to the unreliability of communication networks, such as link failures, natural disasters, or configuration errors. When power devices have problems, the co-located communication network usually also experiences difficulties. Although these failures may seldom occur, they are very hard to completely eliminate. The ideal network conditions (assumed in the previous methods for transmitting queries and responses) are compromised in such situations. The delay guarantee for such messages may be violated because the communication paths may not always available.

To support these critical data exchange, we propose to use *backup paths* to address this issue in order to further improve the effectiveness of agent-based Zone 3 protection.

Algorithm 3 Backup Path Algorithm for Zone 3 Protection Relays.

Input: All Communication Links L_c and Network Topology.
Output: Backup Path Set P_b with Bandwidth Reservation
Method:

for each link $l \in L_c$ **do** ▷ Single link failure can be handled
  Identify primary path set P_a affected by the failure of l
  for each $p \in P_a$ **do**
    Find a shortest backup path for p (The backup path may consist of two parts: the part not overlap with p and the one overlap with p)
    For relay r associated with path p, decide how to divide delay requirement D_0 at each hop i on its backup path $p_{bp}(r)$
    for each hop i along the backup path $p_{bp}(r)$ **do**
      l_i is the forward link from hop i to the MA
      Set delay requirement at i using link weight w_i as $D_r(i) = D_0 \cdot \frac{w_i}{\sum_{i \in p} w_i}$
      Reserve bandwidth at l_i is $B_{rsv}(i) = \frac{L}{D_r(i)}$
      if l_i is not overlapped with the primary path of r **then**
        Set reservation $C_{rsv}(i) = B_{rsv}(i)$
      else
        Identify the reservation $C_{rsv,pr}$ on the primary path
        set reservation for r as $C_{rsv}(i) = max\{B_{rsv}(i), C_{rsv,pr}(i)\}$ ▷ Primary path and Backup path would not be used at the same time
      end if
    end for
  end for
end for

Algorithm. 3 shows how we conduct backup paths for primary paths. First, for each relay has a backup path, we need to ensure that the communication network can support this. Because we assume the communication network has the similar topology as the power network, a bus may only have a single path to the MA. Thus, for these buses, we need to add a few more communication links to form a second path for the relay, which is different from its primary path. After finding a shortest backup path p, we design different methods to divide the delay requirement from a relay to the MA along that backup path. The first method is to equally divide the delay requirement at each hop, as in the basic delay assignment for primary paths. The second method considers the hop distance from a relay

to the MA on a path. The weight at a hop i is computed as $w_i = \frac{\sum_{j \in p} h_p(i)}{h_p(i)}$, where $h_p(i)$ is the hop count from hop i to the MA. The motivation is that communication links closer to the MA usually are shared by more paths than those further away from the MA. The third method considers the loads of different links on a path. We first compute the proportion of available capacity on link $l_i \in p$ as $a(l_i) = 1 - \frac{C_{rsv}(l_i)}{C(l_i)}$, where $C_{rsv}(l_i)$ is the reserved capacity on link l_i and $C(l_i)$ is the total capacity. Here link l_i is the forward link from hop i to MA. Then, the weight at each hop i for a relay r is $w_i = \frac{\sum_i a(l_i)}{a(l_i)}$. The last method is to consider both hop distance and link load in the delay assignment. We first follow the above steps to get the weights based on hop distance and link load, denoted as $w_{i,dst}$ and $w_{i,load}$. We then calculate the combined weight at hop i as $w_i = w_{i,dst} \cdot w_{i,load}$. After we have the weight for each hop/link, we can devide the delay requirement at a link i as $D_r(i) = D_0 \cdot \frac{w_i}{\sum_{j \in p} w_j}$

4.3 Power-aware MA-based Protection

Motivation. Without network link failures, a primary path is able to handle the query process. However, in practical networks, links may fail. We need to deal with such failures for remote relay protection. As a single link failure is the most common case, we can handle it by using a backup path that is completely not overlapping with the primary path. However, there are several limitations in the backup scheme: (1) The network topology may not have another path that is a completely different from the primary path of some buses. (2) The length of a non-overlap backup path is often relatively long: for a fixed path delay, a longer path means a short delay and more bandwidth use at each link on the path, which is inefficient and may create unnecessary hot spots in the network. (3) A link on a non-overlap backup path may not have enough capacity to support the backup requirement. The first and the second limitation can only be fixed by changing network topology, thus we focus on the third limitation and we propose to utilize power system information to select backup paths and manage resources more effectively.

Assume we have historical data about a power network. Therefore, we know which power line carries more load and how likely it may fail, and we can assign a priority to

each power line. Using such information, we can then decide how to allocate the limited network resources to maximize the system reliability. However, since we do not have such information available in this project, we then use PowerWorld Simulator to generate such information as presented in the following.

Based on such known information of power systems, we use $P_f(S \mid line_i)$ to denote the probability that tripping a power line leads to a system failure in simulation. As such data give us the importance of power lines, we can prioritize them in protection. Assume there are N_l lines that may result in system failures. We equally divide the total system requirement P_f^S to these N_l lines. In this way, we expect the probability $P_f(S \cap line_i)$ does not exceed $\frac{P_f^S}{N_l}$ for each of them. From the following equation

$$P_f(S \cap line_i) = P_f(S \mid line_i) \cdot P_f(line_i) \tag{4.1}$$

we have:

$$P_f(line_i) = \frac{P_f(S \cap line_i)}{P_f(S \mid line_i)} \tag{4.2}$$

Consider that the failure of a line is usually due to the false trip of a relay at one of the two ends of the line. Then we can equally divide the requirement of $P_f(line_i)$ to the relays at two ends of the line. For a remote protection relay, when it sees a temporary issue, it sends an query to the MA and waits for the MA's response. If the query cannot reach the MA or the decision from the MA cannot be received by the relay within the required time, a false trip may happen. This case occurs if both a primary path and its backup path of a relay fail at the same time. Under the single link failure assumption, this only happens if the failed link are used by both paths. We can define the probability as:

$$\begin{aligned} P^{relay\ false\ trip} &= P_f^{the\ overlap\ links} \\ &= \sum_{j \in N_{ol}} \Big[P_f(link_j) \cdot \prod_{n \neq j} \big(1 - P_f(link_n)\big) \Big] \end{aligned} \tag{4.3}$$

Algorithm 4 Backup Path Selection Algorithm for Buses

Input: Bus Set B and Communication Link Set L_c.
Output: Backup Path for Each Bus.
Method:

1: **for** each bus $u_i \in B$ **do**
2: Find the smallest false trip probability $P_{min}^{relay\ false\ trip}$ for relays on u_i
3: Calculate the minimum required failure probability for a backup path of u_i as:
4: **if** u_i does not have critical relays **then**
5: Set $P_{f,req}(u_i) = 1$
6: **else**
7: $P_{f,req}(u_i) = P_{min}^{relay\ false\ trip}$
8: **end if**
9: Find all backup paths set P_{bp} to MA that are different from the primary path
10: Sort paths in P_{bp} based on hop count in an ascending order
11: Start from the first path in P_{bp}
12: **for** each backup path $p \in P_{bp}$ **do**
13: Compute the overlap link set N_{ol} between u_i's primary path and p, then Calculate $P_f^{the\ overlap\ links}$
14: **if** $P_f^{the\ overlap\ links} \leq P_{f,req}(u_i)$ **then**
15: Select path p as the backup path
16: **end if**
17: **end for**
18: **end for**

where N_{ol} is the set of overlap links between the primary and backup paths of the relay. Thus our goal is to find a backup path that has $P_f^{the\ overlap\ links}$ and can meet the minimum requirement of $P^{relay\ false\ trip}$. (Similar to finding a primary path, we find a backup path for a bus, instead for its relays.) The backup path selection procedure is presented in Algorithm. 4. After a backup path is selected, resources are also reserved on the path, as shown in Algorithm. 5. In case that a link does not have enough capacity to support all backup paths on it, the reservations are carried out with a specified order. For power lines that may blackout the system, their remote relays are "critical" and will be first considered. If a line is not expected to crash the system, we consider the consequence of tripping this line less important. The goal is to ensure that we can fulfill "critical" relays' requirement as much as possible.

Usually a bus contains more than one remote protection relays. We observe that many of the relays are used to protect different power lines. From this observation, we notice that it is

Algorithm 5 Backup Path Bandwidth Reservation Algorithm for Remote Protection Relays.

Input: Zone 3 Relay Set R, Delay Assignment D, and Relay Query Packet Size S_I.
Output: Backup Path Bandwidth Reservations on Link Set L.
Method:

For each relay $r \in R$, find the powerline l_p it is located on and assign the probability $P_f(system \mid l_p)$ as the weight of relay r
Sort the set R using the weight assigned in the above step in a descending order
Start from the first relay in R
for each relay $r \in R$ **do**
    Devide its delay requirement D on each link of its backup path $P_{bp}(r)$, for link i, its assigned delay is $d(i)$
    for each network link $l \in P_{bp}(r)$ **do**
        Current reservation on l is $b_{rsv}(l)$, total capacity of l is $C(l)$
        Required capacity by relay r at link l is $C_{bp}(l,r) = S_I/d(l)$
        if l is also used in the primary path of relay r **then**
            Reservation of primary path on l is $C_{pr}(l,r)$
            if $C_{pr}(l,r) \leq C_{bp}(l,r)$ **then**
                $C_{bp}(l,r) = C_{bp}(l,r) - C_{pr}(l,r)$
            else
                $C_{bp}(l,r) = 0$
            end if
        end if
        if $b_{rsv}(l) + C_{bp}(l,r) \leq C(l)$ **then**
            $b_{rsv}(l) = b_{rsv}(l) + C_{bp}(l,r)$;
        end if
    end for
end for

possible to further reduce the required network resources. A bus may have multiple remote relays for protecting different power lines. In common cases, they will not simultaneously communicate with the MA. This provides us another opportunity to further reduce the required bandwidth on communication links. Assume only one relay experiences a hidden failure or only one power line has disturbances. For example, in the IEEE 39-bus system, only bus 26, 28, and 29 have two remote relays protecting the same line; remote relays on other buses all protect different power lines. In this case, we only need to reserve bandwidth for relay r_i with the most strict delay requirement on a bus. Because other relays on that bus do not have delay requirements as high as r_i, the reserved capacity is sufficient for them to communicate with the MA.

4.4 P2P-based Protection

In the master-based relay protection, the MA receives a query from a substation relay and makes a decision based on system states whether the relay should trip or not, and then sends the decision back to the query relay. Under normal network conditions, this mechanism works properly. However, as the MA is the only node responsible for making decisions, if it is shut down due to cyber-attacks or physical damages, the entire power system will lose the centralized protection, and relays may trip and cause unforeseen instability in the system.

As modern relays are powerful devices, we propose to use a P2P mechanism to deal with the potential unavailability of MA. The key observation is that *a relay usually only need to check with a small group of related relays to protect a line.* In this scheme, a relay at a substation communicates with other related relays about the state of local and remote power lines. With these responses, the relay can make a justified decision by itself whether to trip or not. An obvious advantage of this scheme is that the average response delay is much shorter than the master-based scheme, because a relay usually only asks other relays nearby, much closer than the MA. (This advantage may be elaborated when a relay need to make a very quick decision for special cases, even when the MA is still available.) As in the MA-based scheme, we also build both primary paths and backup paths for the P2P-based schemes.

Building Primary Path in P2P-based Schemes. The process is as following:

(1). **Identify Related Relays and Form a Peer Group.** For each transmission line, we need first identify the set of related primary and remote relays for a power line and form a relay peer group for the line, as in Sec. 4.2.2.

(2). **Make a Decision.** When the query relay receives replies from other peers, it uses a voting scheme to decide the action. For example, if relays with positive confirmations outnumber relays that do not see the fault, the query relay will assume that there is a real fault in the transmission line, and will trip the line when its primary relay fails to do so; otherwise, it assumes no fault.

(3). **Build Primary Path for Each Relay.** We have the following assumptions here.

(i) A relay will communicate with all other related peers. (ii) At one moment, there is only one hidden failure exposed [9], e.g., one relay has abnormal reading. Moreover, if there is only one hidden failure in the system, a single response from a peer is sufficient to make the decision. (iii) At this step, the effect of link failure to the protection is not considered; and we will discuss backup schemes in the following.

With the proposed P2P scheme, even if the MA is not available unexpectedly, relays in the system are still able to make correct decisions to prevent the false trips of power lines.

In the P2P scheme, we have two types of delays: (i) the (maximum) delay to send a query to other related relays, and (ii) the (maximum) delay for other relays to send their responses back to the query relay. The round trip delay should not exceed a pre-defined time period D_0 to avoid false trips. To make sure the decision can be made within the required time period D_0, we need to reserve network resources for a path from a relay to another peer relay. The relay delay requirement to and from a peer relay can be set to $D_0/2$. Assume the path consists of H hops and each query has size L_0, the required resource on each link is $L_0/(\frac{D_0/2}{H})$.

Backup Path for P2P Schemes. As in the master-based scheme, the P2P scheme can also use backup paths to deal with communication path failures. Unlike the master-based scheme where the reservation is required between each bus and the master agent, in the P2P scheme, we can reduce the network usage by answering the following questions: (1). Does the P2P scheme need to backup for all of its primary paths between peer relays? (2). For the backup path used in the P2P scheme, whether to use overlapped or non-overlapped paths? For the first question, we consider that a minimum of two replies is sufficient for the query relay to make a decision, given the fact that two relays have hidden failures simultaneously is very low [1]. In addition, in [43], it is considered that, if the system is not in a "stressed state", which means the system is not close to unstable operational conditions, a relay can even make a decision without the responses from other peer relays. For the second question, due to the specific topology of a system, non-overlap paths can be much longer than the normal paths, especially for the P2P scheme in which primary

paths are mostly just a few hops. As an alternative, overlapping backup paths may be used if we can still meet the system requirement. The advantage is obvious: overlapping paths are shorter, thus consume less network resources at each link. The backup path selection process and the resource reservation process are shown in Algorithm. 6 and Algorithm. 7. Note that since some relays are protecting multiple lines, for example, r_i and r_j protect $line_k$ and $line_l$ simultaneously, then they can both be used as a *backup protection relay pair* for the two lines. In this way, when we protect $line_k$ with r_i and r_j, we only need to find one additional backup path for protecting $line_l$, which save resources instead of using two different backup paths.

Algorithm 6 Backup Path Selection Algorithm for P2P Schemes

Input: Power Line Set L_p, Communication Link Set L_c and Required Backup Path Number N_u.
Output: Backup Paths Between a Relay and Its Peer Relays.
Method:

Initially there is no backup path for any relay in the system
for each power line $l_n \in L_p$ **do**
    Find all Zone 3 remote backup protection relays R_b and primary protection relays R_p
    For each relay, set the number of required backup peers as $N' = N_u$ ▷ For each relay, we hope it has backup paths to N_u peers
    for each relay $r_i \in R_b$ **do**
        Denote peer relays of r_i as $R'_i = (R_b \cap R_p) \not\supseteq r_i$
        Denote the current backup peers of r_i, whose backup paths already found, as R_x, its size is N_x
        if $N_x \geq N_u$ **then**
            Continue to next relay in R_b
        else
            We still need to find $N'_i = N_u - N_x$ number of backup peers
        end if
        for relay r_j in R_x **do**
            Exclude r_j from R'_i ▷ We already have backup path to r_j
        end for
        Find N'_i number of peers from R'_i, which have the shortest hop count paths as the backup peers of r_i ▷ The paths between each of the found relay and r_i should be different from their primary paths, they can have overlapped links with the primary paths or be totally non-overlapped
    end for
end for

Algorithm 7 Backup Path Bandwidth Reservation Algorithm for P2P Schemes

Input: Relay Zone 3 Delay Assignment D_0, Power Line Set L_p, Communication Link Set L_c.

Output: Backup Path Reservation for Each Relay and Its Backup Peers.

Method:

For each communication link $l \in L_c$, its reservation is $b_{rsv}(l)$
for each power line $l_n \in L_p$ **do**
    Find all Zone 3 remote backup protection relays R_b and primary protection relays R_p
    for each relay $r_i \in R_b$ **do**
        for each relay $r_j \in (R_b \cap R_p)$ and $r_i \neq r_j$ **do**
            if r_j is not a backup peer of r_i OR path between r_j and r_i is already reserved **then**
                Continue to next relay
            end if
            Denote the path from r_i to r_i as $path$
            Assume $path$ has H hops, then on each link l of $path$, the reservation of r_i is $C_{bp,rsv}(r_i, l) = \frac{L_0}{D_0/H}$ ▷ L_0 is the packet size
            for each link $l \in path$ **do**
                $C(l)$ is capacity of l
                if l is also used in the primary path of r_i and r_j **then**
                    The primary path reservation on l is $C_{pr,rsv}(r_i, l)$
                    $C_{bp,rsv}(r_i, l) = max\Big(C_{bp,rsv}(r_i, l) - C_{pr,rsv}(r_i, l), 0\Big)$
                end if
                if $b_{rsv}(l) + C_{bp,rsv}(r_i, l) \leq C(l)$ **then**
                    $b_{rsv}(l) = b_{rsv}(l) + C_{bp,rsv}(r_i, l)$
                end if
            end for
        end for
    end for
end for

Performance Analysis. We can compute the failure probability of a power system, $P_f(S)$, as shown in Equation. 4.4 $\sim$ 4.6. We assume that the false trips of one critical line will result in a system failure, and there are different critical lines under different system load states. The total failure probability of the system is the sum of probability $\{system\ fails\ and\ line_i\ fails\}$. Then, based on the known historical information of a power system, we use $P_f(S \mid line_i)$ to denote the conditional probability that tripping a power line leads to a system failure in simulation. With the above data given, the $P_f(S \cap line_i)$ will be determined by the probability that a power line is falsely tripped, denoted as $P_f(line_i)$. As

we have mentioned before, the malfunction of Zone 3 remote relay is a common reason for false trips. With the deployment of agent-based protection, under normal conditions, we can deal with such potential malfunctions. However, the failure still exists if either of the primary relays on a power line cannot obtain correct responses from the MA or other peers. Thus, the probability directly relates to the false trip probability of a relay, $P^{relay\ false\ trip}$, as in Equation. 4.6, where $relay_{i,1}$ and $relay_{i,2}$ are the two relays at each end of $line_i$ (assume each time only one relay is exposed to a hidden failure). We will see that different primary and backup paths selection will affect the false trip probability of a relay as shown in the later section.

$$P_f(S) = \sum_{line_i \in S} P_f(S \cap line_i) \tag{4.4}$$

$$P_f(S \cap line_i) = P_f(S \mid line_i) \cdot P_f(line_i) \tag{4.5}$$

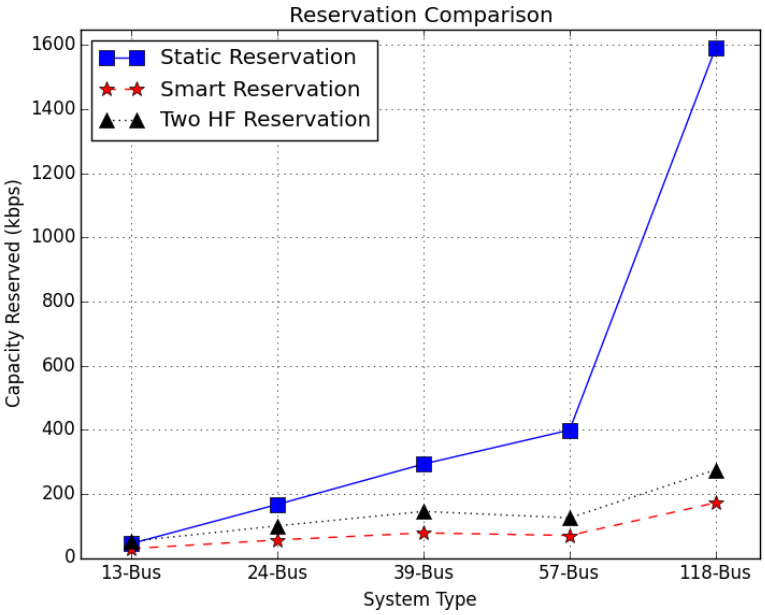
$$P_f(line_i) = P^{relay_{i,1}\ false\ trip} + P^{relay_{i,2}\ false\ trip} \tag{4.6}$$

4.5 Performance Evaluation

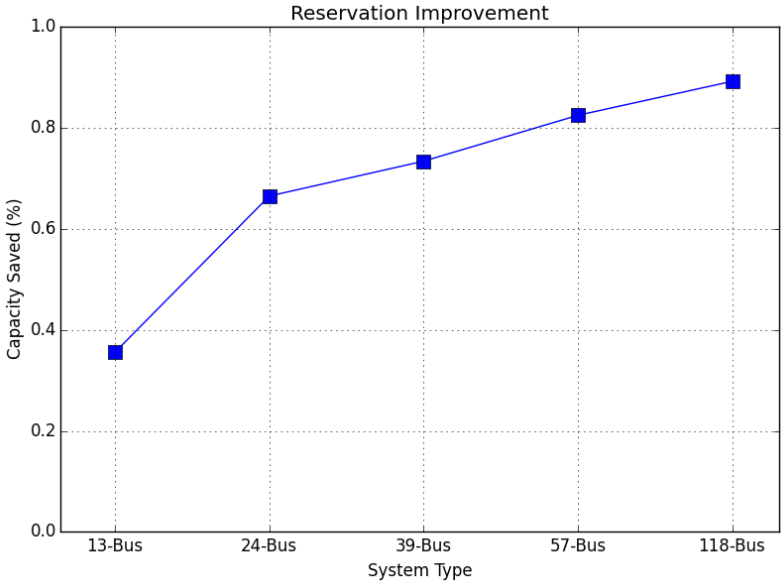
4.5.1 Comparison of Basic and Smart Schemes

We first present the numerical result to demonstrate the advantage of the smart reservation scheme, compared with the basic scheme. As shown in Fig. 4.3a, we considered five different power systems, ranging from IEEE 13-bus, 24-bus, 39-bus, and 57-bus, to 118-bus. The top curve shows the maximum bandwidth reservation required for the basic scheme. The bottom curve shows the maximum bandwidth reservation of the proposed smart scheme. (The middle curve is for the double hidden failure case, as explained in Subsection 4.5.2.) Clearly, the larger the power network, the more link bandwidth the smart scheme can save, compared with the basic scheme. Furthermore, Fig. 4.3b shows the percentage of bandwidth

saved by the smart scheme compared with the basic scheme, ranging from 37% to almost 90%.



(a) Bandwidth Requirement



(b) Improvement of the Smart Scheme

Figure 4.3: Comparison of Static and Smart Reservation on Five Power Systems.

4.5.2 Dealing with Simultaneous Hidden Failures

Using the Master agent in the power system helps us prevent false relay trips due to hidden failures. When a power device has hidden failures, it does not mean that it is totally damaged; instead, only some of its normal functionalities are out of order. Due to the high reliability requirement of power systems, a device are built to work for a long period of time without maintenance. For example, its mean time to failure (MTTF) should be higher than 100,000 hours [76] while its mean time to repair (MTTR) is about 1 hour [77]. This yields a rather low device failure probability of 10^{-5}. However, the probability for hidden failures is much higher, e.g., the hidden failure probability of a line is given as 10^{-2} [36]. If we assume hidden failures are mostly triggered by Zone 3 relays [41, 37], then the hidden failure probability of a line can be represented as:

$$P(HF\ of\ a\ line) = 1 - P(a\ relay\ is\ normal)^k.$$

Assume we have k Zone 3 relays for this line. We analyzed the five power systems (IEEE 13-bus to 118 bus systems), and found that the average number of Zone 3 relay per transmission line is between 3.1 to 5.6. Plugging into the above formulas, we have the hidden failure probability at the level of 10^{-3} per line. We can see that the case of three simultaneous relay hidden failures is rare (about 10^{-9}). So, we do not have to consider three or more simultaneous hidden failures. As current power grid reliability requirements ranges from "three nines" (99.9%) to "five nines" (99.999%) [78], we still have to investigate the cases where two hidden failures simultaneously happen in the system. To address this issue, we extend the smart reservation scheme to deal with two simultaneous failures. Instead of reserving bandwidth for the maximum requirement on a link for multiple overlapped relay-to-MA paths, we reserve bandwidth for top-two requirements among these paths. We show the results of this scheme as the middle curve in Fig. 4.3a. The maximum reserved capacity on a link is a little higher than the single-hidden-failure case.

4.5.3 Effectiveness of Backup Schemes

We use the IEEE 39-bus system (Fig. 4.4) to demonstrate the effectiveness of the backup scheme. The 39-bus system has 34 transmission lines and all buses connected by these lines have at least two paths to the MA, except bus 19. As we assume the communication links follow the pattern of power lines, we can find backup paths on this network for most relays. For bus 19, we add a communication link between bus 19 and bus 21 for the reliability purpose. Assume bus 21 is the closest bus for bus 19. All links have an identical capacity of $1.5Mbps$. Assume that the failure probability of a communication link is about 10^{-5} [79], which is rather close to the system failure requirement. Thus, the main consideration of backup paths here is to handle a single link failure.

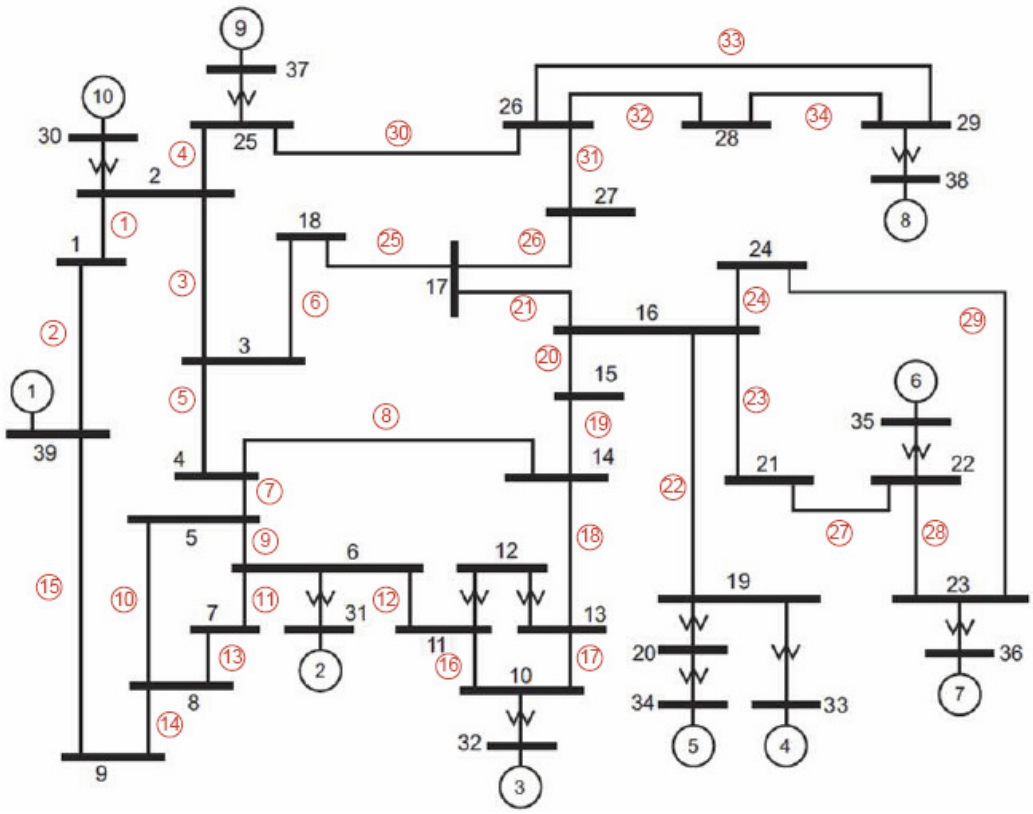


Figure 4.4: IEEE 39-Bus System [1].

We can further improve the above backup scheme with the smart reservation scheme,

as we usually only see a single link failure. To deal with such a single failure, within a set of power lines, we find out the one that requires the largest capacity on a specified link and make a corresponding bandwidth reservation. Notice that since a backup path may be longer than a primary path, the per-hop reservation for a backup path may also be larger. We evaluate such a scheme on the IEEE 39-bus system, and summarize the results of maximum link reservation in Table. 4.1. For the cases in the first row, we add up the reservations of all relays on a link; for the second row, we reserve link bandwidth under the assumption of single hidden failure. The four columns are corresponding to the four delay weight assignment methods discussed in the above. We can see that, in general, the smart backup scheme requires much less capacity than the basic backup scheme. In the basic backup scheme, the hop distance and link load both help reduce bandwidth by lowering the maximum bandwidth reservation on links. For the smart scheme, the equal division and the load-based delay assignment outperform the other two.

Table 4.1: Comparison of Maximum Link Reservation for Basic and Smart Backup Schemes.

	Equal Division	Hop Distance	Link Load	Combination
Basic (Kbps)	835	790	741	729
Smart (Kbps)	85	153	76	149

4.5.4 Building Power System Knowledge

To build power system knowledge, we use the PowerWorld simulator [80] to obtain the conditional probability $P_f(S \mid line_i)$. As we know, more reactive loads cause more system losses, and result in various instability issues which may lead to system failures. We follow the methods used in [81, 82], and gradually increase the reactive loads of all PQ buses that have non-zero reactive loads, by setting $load_{new} = load_{base} \cdot (1 + x)$. The increase step of x is 10% of the base load each time. At each system load setting, we examine system contingency by tripping a random selected power transmission lines to check if the system

fails (shown as a blackout in PowerWorld). We vary x in a range of $(0, 3.3)$, because a blackout usually happens when $x \geq 3.4$, even if we do not trip any line. As a result, we have $P_f(S \mid line_i) = \sum_{k=0}^{3.3} P(x = k) \cdot I_{failure}(line_i)$, where $I_{failure}(line_i)$ equals to 1 if a system failure happens; otherwise, it is 0. For $line_i$ whose tripping may cause system failures, we obtain its $P_f(S \mid line_i)$ based on the above procedure, as shown in Table.4.2. We use these data for optimizing backup path selection later.

Table 4.2: $P_f(S \mid line_i)$ Obtained via Simulations.

Line	$P_f(S \mid line_i)$	Line	$P_f(S \mid line_i)$
22	0.0420	27	0.0115
3	0.0115	31	0.0070
14	0.0017	15	0.0017
21	0.0017	5	0.0008
6	0.0008	7	0.0008
9	0.0008	12	0.0008
19	0.0008	23	0.0008
34	0.0008		

4.5.5 Performance of Primary Selections and Backup Paths without/with Power Knowledge

We evaluate the proposed schemes on the IEEE 39-bus system. The system setup is the same as in Subsection 4.5.3. We assume all query and response packets have the same size of 80 bytes, e.g., a simple PMU packet. We set the system failure requirement to 10^{-6}, which is a higher requirement than current power grid [78], and set the communication link capacity to $1.5Mbps$ (one T1 line) [33] with a failure probability no more than $P_f(link) = 10^{-5}$ [83]. In this case, the probability of two or more links fail simultaneously is about 10^{-8}, which is much smaller than the system requirement. Thus, in this subsection, we only consider a single link failure.

To evaluate the two primary path schemes and corresponding backup path schemes, we assign the failure probability of a communication link according to the amount of transmitted power on the corresponding power line. (Assume each communication link connects the same buses as its power line.) For lines with more than 200MW power (in 39-bus system, under normal condition, we have 17 lines with real power more than 200MW, which is about 50% of all power lines), we set their corresponding links with $P_f(link) = 10^{-6}$; otherwise, $P_f(link) = 10^{-5}$. As shown in Table.4.3, when using primary paths only, neither primary selection scheme alone can achieve the system requirement (10^{-6}), as shown in the first row. The reliability-based primary-path selection does a little better than the shortest path selection. After adding backup paths, both schemes can fulfill the system requirement and achieve similar system reliability, as shown in the second row.

Table 4.3: Comparison of System Reliability.

Failure Probability	Shortest Hop Count Based	Reliability Based
Primary Path Only	1.58×10^{-6}	1.32×10^{-6}
With Backup Path	1.18×10^{-7}	1.22×10^{-7}

Using Power Knowledge to Improve System Reliability. As discussed in Section. 4.3, we can handle a single link failure on a primary path by using a completely non-overlap backup path for each relay as a *topology-based backup selection*. However, this method consumes more resources. We utilize power system knowledge to address this issue. As shown in Table. 4.2, we observe 15 lines that may lead to system failures under different load settings. Therefore, we prioritize these lines and their protection relays to better use network resources. Here we set $P_f(link) = 10^{-5}$ for all links. Compared with using complete non-overlap backup paths, such a power-aware backup path selection significantly reduces the bandwidth reservation on almost every link, and the average bandwidth saving across all links is about 18%. Fig. 4.5 shows the comparison of reservations on links. We sort them from high to low for easy illustration.

In the above, we compare the maximum required link reservation on the 39-bus system

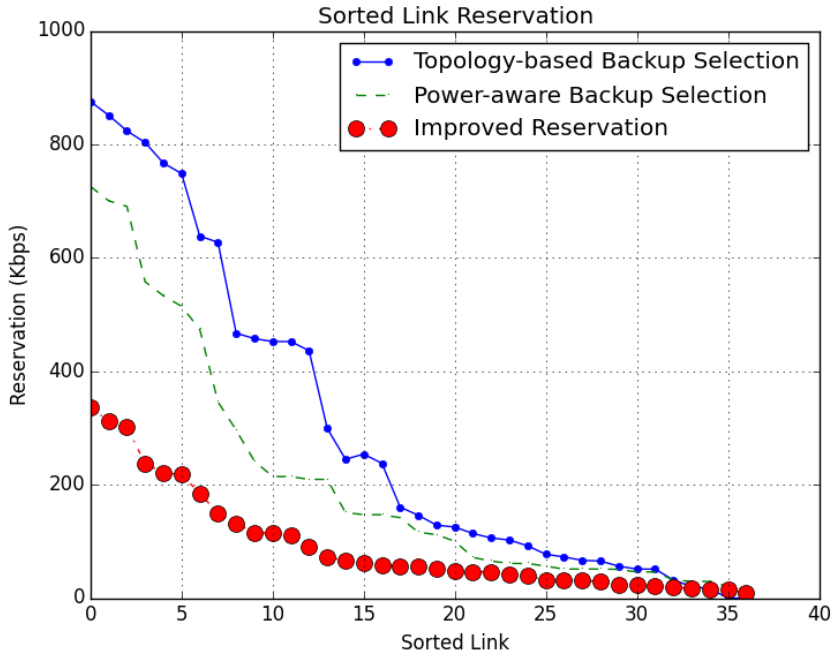


Figure 4.5: Backup Path Selection without/with Power Knowledge.

for using non-overlap backup paths and partially overlapped backup paths with the system failure requirement $R_S = 10^{-6}$. To further show how the proposed power aware scheme can reduce link reservations, we also test it with system failure requirement $R_S = 10^{-5}$. Assume the single link fails with $P_f(link) = 10^{-5}$. As shown in Table. 4.4, compared with the non-overlap path scheme, the power-aware scheme can significantly reduce bandwidth reservation (29% less) while still meeting the system reliability requirement. In the second row, we set the value of non-overlap path scheme as the "base" of 100%.

Table 4.4: Comparison of Maximum Link Reservation for Different Backup Path Schemes and Requirements.

	Topology-only $R_S = 10^{-6}$	Power-aware $R_S = 10^{-6}$	Power-aware $R_S = 10^{-5}$
Max Reservation (Kbps)	878	725	625
Percentage (%)	100	82	71
Failure Probability	0	1.0×10^{-7}	5.7×10^{-7}

Handling a Bottleneck Link. When some links do not have enough capacity, we

assign higher priorities to the protection relays of important lines based on the power knowledge to further improve the system reliability. We compare three simple resource reservation orders in the following. The first order is to start to allocate bandwidth from the most important relay to least important one; the second order use the opposite order for comparison; the third order is to allocate bandwidth using random bus orders (here we compute the average of 20 random orders). To show the case that some relays may not obtain the required bandwidth on a link, we make link 19 as the bottleneck and reduce its capacity from 1.5 $Mbps$ to 550 $Kbps$. We set the system requirement as 10^{-6}, and the failure probability of links as 10^{-5}. We observed that the relays without enough reservation vary in the different orders. For the latter two orders, some relays do not obtain enough bandwidth for their paths, for example, relays protecting Line {3, 5, 6, 15, 19, 21, 31}. However, these lines have higher probabilities in causing system failures if improperly tripped. The system failure probabilities for different orders are shown in Table. 4.5. It is obvious that considering the priority of remote relays significantly improves the system reliability when there are bottlenecks.

Table 4.5: Comparison of System Reliability for Different Relay Reservation Orders.

	From the most critical relay	From the least critical relay	In random bus order
Failure Probability	1×10^{-7}	1.5×10^{-6}	6.7×10^{-7}

Smart Reservation. A bus may have multiple remote relays for protecting different power lines. In common cases, they will not simultaneously communicate with the MA. This provides us another opportunity to further reduce the required bandwidth on communication links. Assume only one relay experiences a hidden failure or only one power line has disturbances. For example, in the IEEE 39-bus system, only bus 26, 28, and 29 have two remote relays protecting the same line; remote relays on other buses all protect different power lines. In this case, we only need to reserve bandwidth for relay r_i with the most strict delay requirement on a bus. Because other relays on that bus do not have delay requirement as high as r_i, the reserved capacity is sufficient for them to communicate

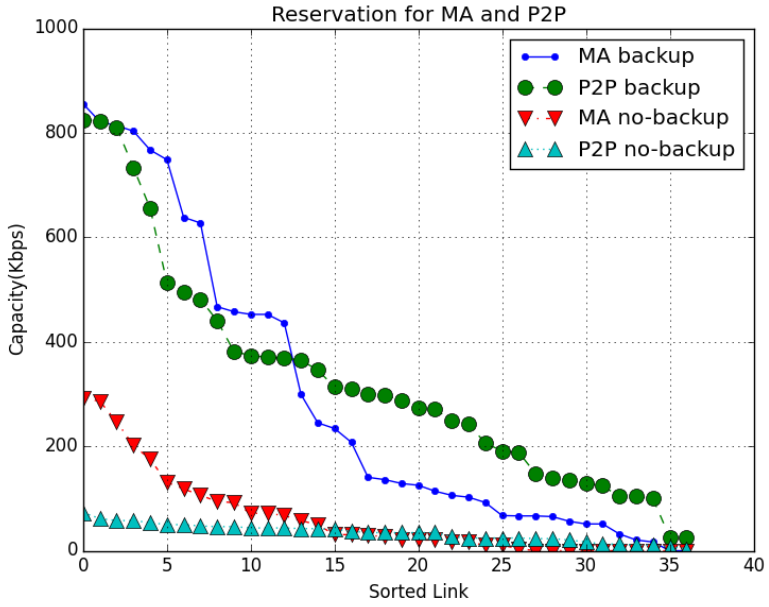
with the MA. Again, we set the system requirement as 10^{-6} and $P_f(link) = 10^{-5}$. The maximum required capacity on a link decreases from 725 $Kbps$ to 366 $Kbps$, a nearly 50% saving. As shown in Fig. 4.5, on average, we save about 39% capacity on each communication link. The overall system failure probability is 1×10^{-7}, still meeting the system reliability requirement.

4.5.6 Comparison of MA-based and P2P-based Protection Schemes

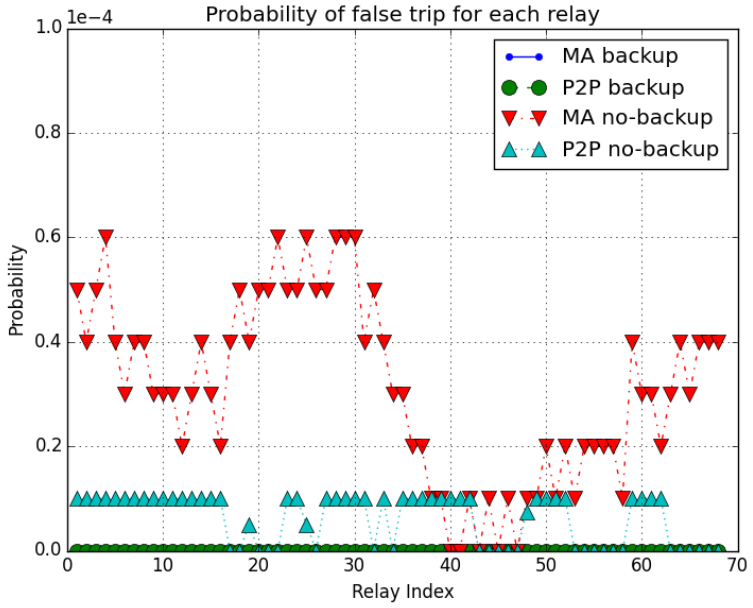
We follow the method in [1], assume at a single moment, there is only one hidden failure exposed in the system: a disturbance is applied to a power line that the relay with a hidden failure will sense the disturbance, and the communication network has a single link failure at most. We compare the resource requirement for the protection and the false trip probability of each relay, under four schemes: the MA scheme without backup paths, the P2P scheme without backup paths, the MA scheme with backup paths, and the P2P with backup paths. For the primary path selection, both the MA scheme and the P2P scheme use the shortest path to the master node or peers. For the backup path selection, both schemes use non-overlap backup paths.

The result for resource requirement is shown in Fig. 4.6a. Without backup paths, the P2P scheme consumes the minimum resources since the distance to peers are shorter than in the MA scheme. However, adding backup paths to both schemes significantly increases the resource usage. Fig. 4.6b shows the false trip probability of each relay in the system. Under the single link failure condition, in the MA scheme without backup paths, if the primary path of a relay fails, it cannot communicate with the MA and will result in a false trip. As we can see, more relays in the MA scheme are affected than in the P2P scheme. For the P2P scheme, since each peer can send its response to the query relay, the false trip occurs if all paths to the relay's peers fail, which means the failed link is shared by all paths to the peers. Intuitively, this probability is much lower than the failure of a primary path in the MA scheme. With non-overlap backup paths, both the MA scheme and the P2P scheme can handle a single link failure, in which all relays have zero failure probability.

Combining the relay false trip probability with the power data ($P_f(S \mid line_i)$), the system failure probability is shown in Table. 4.6.



(a) Resource Requirement for Protection Schemes without/with Backup Paths.



(b) False Trip Probability of Each Relay with a Single Link Failure.

Figure 4.6: Comparison of MA and P2P schemes.

Table 4.6: System Failure Probability Under MA and P2P Schemes without/with Backup Path.

	MA without backup	MA with backup	P2P without backup	P2P with backup
$P_f(S)$ $(\times 10^{-6})$	2.62	0	0.55	0

As we can see from Table. 4.6, without backup paths, the system reliability in the P2P scheme is about 4-times better than that of the MA scheme. Note that the P2P scheme can meet the 10^{-6} requirement but the MA scheme cannot. This matches the results from Fig. 4.6b that the failure of a primary path of a relay has more influence in the MA scheme, because all relays must first contact the MA and then receive a decision from the MA. While we can protect relays from false trips using non-overlap backup paths, judging from the resource requirement from Fig. 4.6a, the cost of non-overlap backup path in the two schemes do not have much difference. The potential difference between the two is the response delay.

Table 4.7: Path Hop Count in MA Schemes.

	Max	Min	Average	**Actual**
Primary Path	6	0	3.2	**6.4**
Backup Path	10	0	6.2	**12.4**

Table 4.8: Path Hop Count in P2P Schemes.

	Max	Min	Average	**Actual**
Primary Path	3	0	2.0	**2.0**
Backup Path	12	0	5.7	**5.7**

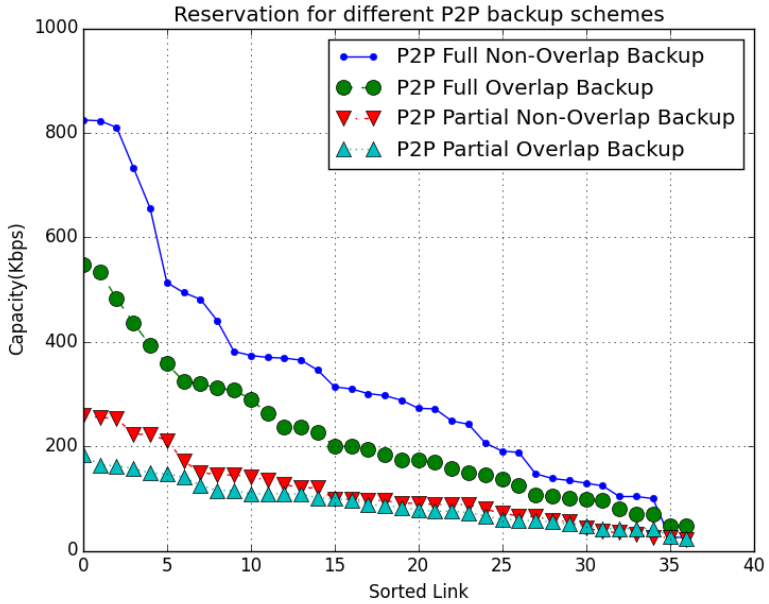
The response delay counts from the time when the query is sent until a decision returns the query relay. This delay is closely related to the path distance (hop count), especially when the traffic load is light most of the time. We compute the maximum, minimum and average hop counts for both the MA scheme and the P2P scheme. For the MA scheme,

the primary/backup path distance is between a bus and the MA bus. The result for the MA scheme with non-overlap backup paths is shown in Table. 4.7. As a comparison, the result of the P2P scheme with non-overlap backup paths is shown in Table 4.8. In the P2P scheme, paths exist between each pair of "corresponding relays". Note that in both the MA and P2P schemes, the minimum hop count is 0. The reason is that, in the MA scheme, there are a few relays locating at the same bus with the MA; for the P2P scheme, in the 39-bus system, relay (64,67) and relay (66,68) are located at bus 28 and 29, respectively, and they are protecting the same lines. Thus the communication between these relays are within a substation. (We assume the indexes of relays for a power transmission line i are $2 \cdot i$ and $2 \cdot i - 1$.). In addition, although the average path length between (the MA and a non-MA bus) or (P2P peers) are similar, in the MA scheme the query process takes two round-trip delays. While in the P2P scheme, there is only one round-trip delay (as shown in the "Actual" column of Table. 4.7 and Table. 4.8). As link loads are not heavy most of the time, a shorter path benefits the protection with faster response delays.

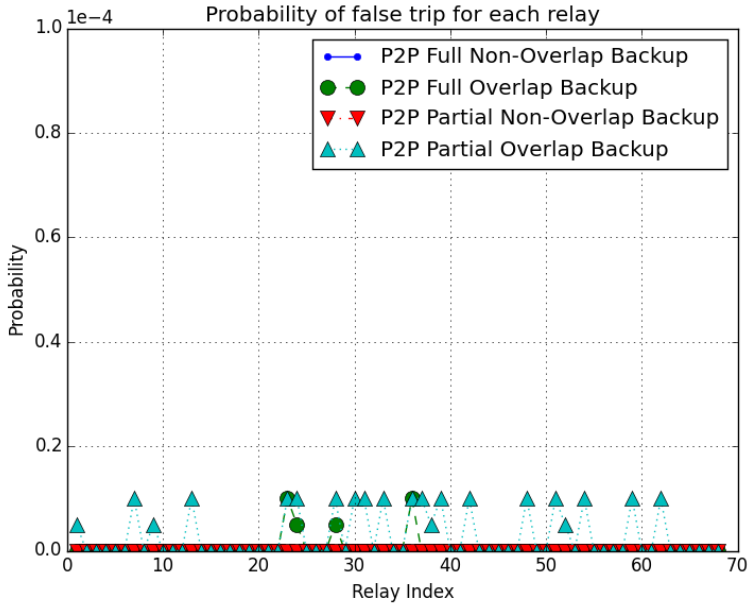
Compare the Effect of Full Backup vs. Partial Backup Paths and Overlapped Backup vs. Non-overlapped Backup Paths. The above case is the worst case resource requirement for the P2P scheme since a non-overlap path between each pair of "corresponding relays" are reserved. As a comparison, the shortest-hop-count overlap backup path is tested in the P2P scheme. Similar to the non-overlap scheme, resources for each "corresponding relay pair" is reserved as well. We examine the "stressed case" and assume two replies returning from peers will enable the query relay to make a correct decision.

Fig. 4.7a shows network resource requirements for each protection scheme. Clearly, using overlapping backup paths requires dramatic lower resources, compared to using non-overlap backup paths (curves marked with "Full Backup"), because overlapping paths are much shorter and thus we usually need reserve less bandwidth on links.

Fig. 4.7b shows the false trip probability of relays. We see that only four out of about 68 relays are affected when using overlapping paths. Since two responses are enough for making a decision to deal with false trips, an alternative way is to only reserve two backup



(a) Resource Requirement for P2P Schemes without/with a Backup Path for Each Relay.



(b) Relay False Trip Probability for P2P Schemes without/with Backup Path for Each Relay with a Single Link Failure.

Figure 4.7: Comparison of P2P Schemes without/with a Backup Path for Each Relay.

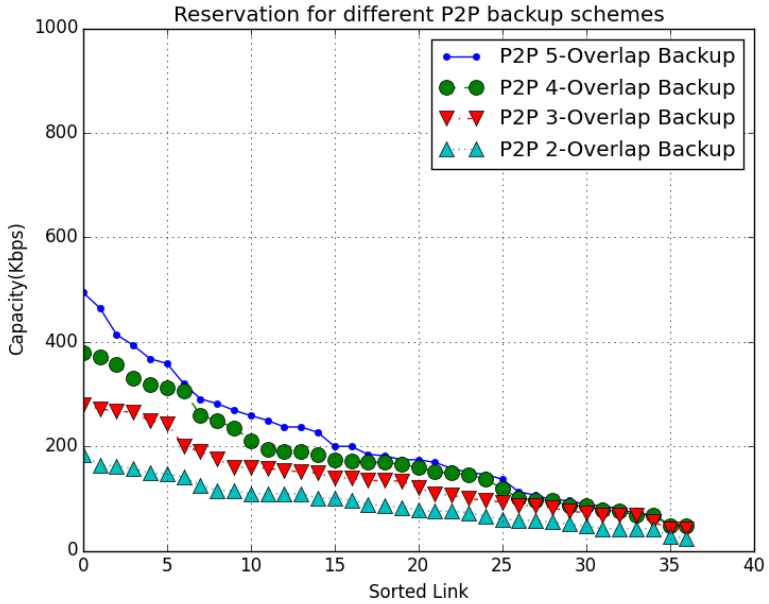
paths to two peers of a relay, using either non-overlap or overlapping paths. Fig. 4.7a and Fig. 4.7b also show that the resource requirement further decreases because now each relay only reserves for two backup paths (curves marked with "Partial Backup"), because some long paths are avoided and some paths are shared for the proteciton of different lines.

When using non-overlap backup paths, all relays can handle the single link failure; while using overlapping backup path uses less resources at the cost of a few more potential false trips. Table. 4.9 shows how the total resource requirement and the changes of system reliability for different backup schemes. "Full" means that each relay has backup paths to all its peers, and "Two BP" means that each relay has only two backup paths to two of all its peers.

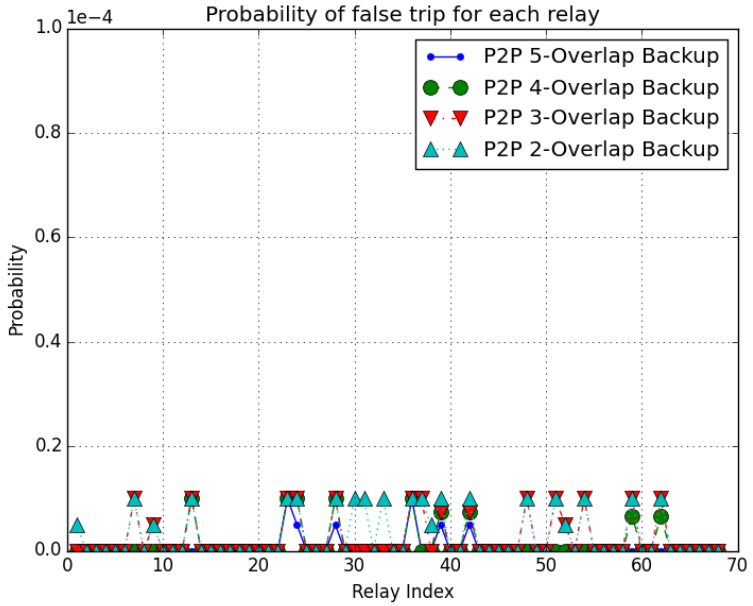
Table 4.9: Total Resource Requirement and System Failure Probability without/with Backup Path for Each Relay.

	Full Non-Overlap	Full Overlap	Two BP Non-Overlap	Two BP Overlap
$Resrouce$ $(Kbps)$	12140	8104	4131	3372
$P_f(S)$ $(\times 10^{-7})$	0	0.2	0	2.76

Compare the Effect of the Number of Overlapped Backup Paths in P2P Schemes. We try to identify how many overlapped backup paths should be used in the P2P scheme by varying the number of backup paths for each relay from two to five. We choose the shortest hop count path as a backup path, and allow this path to have overlapping links with its primary P2P path. The results are shown in Fig. 4.8a and Fig. 4.8b. As we can see, the more backup path we use, the less number of relays that will have false trips. The resource requirement is as expected: the more backup paths we use, the more resources we consume. We show the total resource requirement in Table. 4.10. Besides, with the number of backup paths increased, the average relay failure probability $\overline{P_f(relay)}$ is decreased, as shown in Table. 4.11. The overall failure probability of the system is shown in Table. 4.12. A significant point is that, when we increase the number of overlap backup paths from two



(a) Resource Requirement for Different Numbers of Overlapped Backup Path in P2P Schemes.



(b) Relay False Trip Probability for Different Numbers of Overlapped Backup Path in P2P Schemes with a Single Link Failure.

Figure 4.8: Comparison of P2P Schemes with Different Numbers of Backup Path.

to five, the resource cost doubles, but the reliability is improved by ten-folds. While the trends of improvement are different in Table. 4.11 and Table. 4.12, the reason is that power lines are not of the same importance: for some lines, the false trip may lead to severe system failure, while others are not. By providing more backup paths, the critical relays are better secured.

Table 4.10: Total Resource Requirement for Different P2P Schemes.

	2 Overlap Backup	3 Overlap Backup	4 Overlap Backup	5 Overlap Backup
$Resource$ $(Kbps)$	3372	5122	6646	7638

Table 4.11: Number of Potential Failure Relay and Their Average Failure Probability under Different P2P Schemes.

	2 Overlap Backup	3 Overlap Backup	4 Overlap Backup	5 Overlap Backup
$Number$	21	16	9	6
$\overline{P_f(relay)}$ $(\times 10^{-6})$	2.8	2.2	1.2	0.6
$\frac{Normalized}{\overline{P_f(relay)}}$	4.67	3.67	2	1

Table 4.12: System Failure Probability under Different Backup Path Numbers in P2P Schemes.

	2 Overlap Backup	3 Overlap Backup	4 Overlap Backup	5 Overlap Backup
$P_f(S)$ $(\times 10^{-7})$	2.76	2.5	1.0	0.29

4.6 Conclusion

In summary, we investigate the agent-based protection in this chapter. We propose a basic resource management scheme, and improve its reliability using backup paths. We propose a power-aware backup path selection mechanism, and use the power system knowledge to help us improve the resource utilization. We investigate the P2P protection scheme and its resource requirements. We also build backup paths for the P2P protection to improve its reliability. The evaluation shows that P2P-based schemes can improve the system reliability while utilizing network resource more effectively than MA-based schemes.

CHAPTER 5
ATTACKS ON SMART RELAYS AND PROTECTION

Smart Grid, as the combination of power grid and communication network, is considered as a revolutionary and evolutionary regime of existing power grids. While higher power efficiency and more accurate control can be achieved (especially in protection systems), smart grid is also vulnerable to malicious cyber attacks since it is no longer a closed dedicated network. As better protection schemes continue being developed, there is still very limited work in examining potential threats to these schemes and how much damage can be achieved. In this chapter, we investigate the security of backup relay protection in smart grid. We examine potential attacks to basic P2P agent-based protection and agent-reputation-based relay protection, and analyze effects of these potential attack strategies.

5.1 Background

In today's power industry, microprocessor technology and advanced communication network have been utilized. Protection-related solutions like SCADA, PMU, and other control and monitoring applications are implemented to enhance efficiency and reliability of the system. To deal with the hidden failure problem in relay protection, new schemes like agent-based protection and agent-reputation-based relay protection have been proposed. The key component of these protection schemes is to enable communication among a set relays when there are potential failures occurring. The shared information among protection relays can help each relay make better decisions, as it is considered that simultaneous accidental problems are rare in practical. In addition, the mechanism is further improved with agent-reputation-based schemes, so that different trust values can be assigned to distinguish potential unreliable replies from relays having problems.

However, while greatly improving reliability and efficiency, these advanced technologies also enable individuals and organizations to disrupt the system through cyber attacks. Unknown bugs and backdoors in software, unauthorized access to confidential information, and

malicious modification of critical data are threatening normal operations of power system (e.g., triggering cascading or blackout). In addition, unlike manned control centers and power plants with strong monitoring and protection, usually very limited security mechanisms are deployed at unattended substations located in remote areas [3]. This often makes malicious physical and cyber attacks on substations much easier for attackers. Consequently, compromised devices (especially protection devices) may cause serious issues for the integrity of the power grid.

5.2 Motivation

We first present a few simple examples to show the potential vulnerabilities of basic agent-based protection and basic agent-reputation-based schemes. We use a part of the IEEE 13-bus system as shown in the Fig. 5.1 to demonstrate how attacks can be conducted. As many other smart grid projects, we assume the communication network has the same topology of the power system, while each substation contains a router for communication.

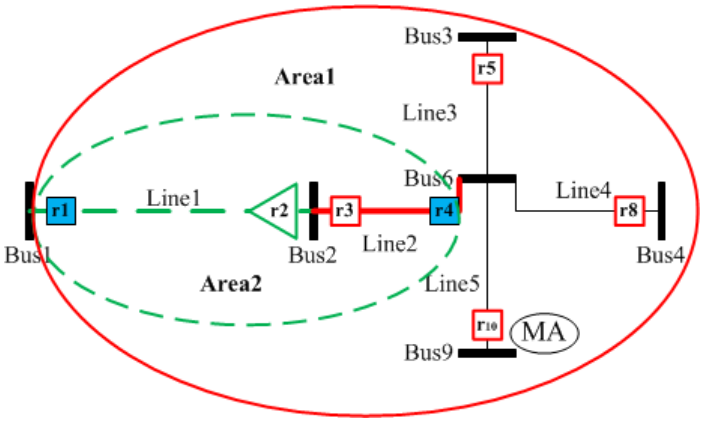


Figure 5.1: Examples of Cyber Attacks on Relay Protection.

Example 1: If an attacker compromised a relay, e.g., r_3 in the system, it can not only trip the $Line_2$, but also may trip other relays via fake status reports. For example, if relay r_1 has a hidden failure and falsely detects a fault on its remote $Line_2$, which is actually in a normal state, r_1 will send an query to r_3. The attacker can use the compromised r_3 to

confirm the query. As only one trusted relay is required to confirm the basic agent-based protection and agent-reputation-based protection scheme, r_1 will trip $Line_1$, resulting in a false trip. If the attacker compromises two relays in the same protection area, it can easily trip other relays in the same area.

Example 2: An attacker compromises $Router_2$ at Bus_2 and $Router_6$ at Bus_6, it can then drop packets passing them. So, all primary and backup relays protecting the transmission $Line_2$ will not receive the line status updates, and they will have no knowledge about their peers' states. When there is a fault at $Line_2$, if the primary relay r_3 or r_4 does not respond, the backup relays will revert to the traditional protection, because the trip requests from r_3 or r_4 is considered untrusted. As a result, the level of protection is lowered to the same level of the traditional protection, which is insufficient for the requirements of smart grid.

Example 3: Hybrid attack. An attacker compromises relay r_1 and r_4, and $Router_6$ at Bus_6. Its goal is to trip relay r_8. The attacker can modify or drop the packets from relay r_3, r_5, and r_{10} through $Router_6$. Then the attacker can issue a trip request from r_4 to r_8, and confirm the request with r_1. Because the reply packets from r_3, r_5, and r_{10} are either modified or dropped, this positive confirmation will be taken by r_8, and then the $Line_4$ will be tripped. In this way, the attacker may not directly compromise a relay, but it can still indirectly trip this Zone 3 backup relay with the help of compromised relays.

As we mentioned, agent-based relay protection schemes have been demonstrated to be effective in many situations. However, as we can see from the examples, the new technologies and protection schemes may also be exploited by malicious attackers to disrupt the power delivery system. Meanwhile, these schemes are assumed to be working correctly under normal conditions (e.g., the devices and communication network are functional correctly). These motivate us to investigate the problem of potential cyber attacks to smart relay protection, with the assumption that the network devices can be compromised by attackers. We investigate how the attacker can disrupt the relay protection system with certain amount of resources, and analyze the potential effect.

5.3 Attacks on Relay Protection Schemes

A compromised relay agent can trip its local circuit breaker, and issue fake status reports. As an advanced feature for agent-based protection, a compromised primary relay can send requests to backup relays in the same protection area in order to indirectly trip them. When a hidden failure of a relay is exposed, another compromised relay can be used to trip the affected remote relay through fake confirmations.

Three attack methods and their effects are examined to understand their potential threats. The attacker tries to maximize the number of tripped lines. Assume each unit of attack resource is used to attack one relay agent once. We denote the total amount of attack resources as N_A, the number of repeated attacks on a relay as K, the number of lines in an initial set of a cascading failure as n_k, the number of extra lines tripped in a cascading failure as n_m, and the defense strength of a relay as P_f. The notations are summarized in Table. 5.1.

Table 5.1: Notations Used in Analysis.

Term	Definition
N_A	Number of attack resource
n_k	Initial line set in a cascading failure
n_m	Extra line set in a cascading failure
P_f	Defense strength of a relay
B_v	Set of buses in the system
L_e	Set of lines in the system
$d(avg)$	Average node degree of a network
A	Set of protection areas in the system
R	Set of protection relays in the system
r_p	Primary relays of a line
K	The maximum number of repeated attacks on a relay
C_i^j	The combination of select j objects from a set of i objects

We introduce the system model as following. We denote the set of buses: B_v =

$\{b_1, b_2, \cdots, b_i\}$, and a set of transmission lines $L_e = \{l_1, l_2, \cdots, l_k\}$ for a power system. A transmission line $line_i$ has two primary relays $r_p(i,1)$ and $r_p(i,2)$. Both relays may also be used as backup relays for other transmission lines. A protection area A_i is set up to protect a transmission line l_i, which contains the protected line and several lines on which the backup relays of l_i are located. Denote the set of protection areas as $A = \{A_1, A_2, \cdots, A_i\}$. We also define the defense strength of a relay: when a relay r_i is under an attack, it will survive the attacker with a probability P_f ($0 \leq P_f \leq 1$), depending on its defense strength. Relays may have different levels of defense strength, such as no defense (i.e., $P_f = 0$), or low defense (e.g., $P_f = 0.2$), or high defense (e.g., $P_f = 0.8$).

To characterize potential cascading failures, assume a specific system topology with certain loads may have one or multiple cascading failure sequences. When a set of lines $L_k = \{l_1, l_2, \cdots, l_{j_0}\}$ are tripped, they can trigger a cascading sequence of extra lines $C_k = \{l_1, l_2, \cdots, l_j\}$ to trip [84, 85]. Assume the size of the initial line set L_k is n_k, and the size of extra cascading sequence of C_k is n_m, which may follow a distribution (e.g., a Poisson distribution) [84, 85]. To examine different cases, we first determine the potential n_k for a topology, and then randomly select lines to be in the extra set. The affected lines may be neighbors or separated, as the phenomenon reported in [86]: cascading lines may be geographically separated.

5.3.1 Potential Attack Strategies

To examine the potential attack damages, we identify *three basic methods to attack relays for trip transmission lines*: (i) An attacker can compromise a primary relay of a line, and then **directly** trip the line; (ii) An attacker exploits agent-based or reputation-based protection mechanism to **indirectly** trip a relay, by sending a trip request from a compromised primary relay to a backup relay and confirming the request with another *compromised* peer relay; (iii) An attacker can trigger a cascading failure by tripping a set of relays that initializes a cascading sequence. Furthermore, an attacker may use three different attack strategies to select relays to attack:

(1). **Random Relay Selection**: the attacker may only know the IP address of the relays, then a set of relays (at most N_A) are randomly selected and attacked by the attacker. Each compromised relay can trip its local line. If the attacker obtains the knowledge of the relay locations, the compromised relays in the same protection area may trip more lines indirectly in that area. The random attack also has a low probability to trigger cascading failures in the system. In both cases the damage may be amplified.

(2) **Area-based Relay Selection.** Assume the attacker knows the partial or completed topology of a power system and its protection areas, it can select relays based on the importance of protection areas. For example, it can simply use the degree of an area to represent the importance of the area *in a basic area-based attack* to select target relays before the attack starts. Furthermore, if the attacker has the complete real-time knowledge of the system, it can use an *iterative selection strategy*, in which it evaluates the importance of areas based on the current system status after each attack step (e.g., attacking x relays in each round), and selects an area based on its current importance. The iterative selection is the best case in the area-based attack method for an attacker, because the attacker can maximize the attack damages based on its real-time observation. However, in order to achieve this, the attacker must pay extra efforts to monitor the system in real time.

In an area-based attack, the two primary relays of a selected area will be attacked. If an attack is successful, both the local line and the backup lines of an attacked area may be tripped. An area-based attack may also trigger cascading failures in some cases, which depends on the system state. The algorithms of iterative area-based attack and basic area-based attack are shown in Algorithm. 8 and Algorithm. 9 respectively.

In an iterative area-based attack, as the attacker knows the current system state (e.g., which lines are tripped for each protection area), the attacker will selectively repeat the attack steps on the important relays that are still not compromised yet in the previous attack steps. In this way, the attacker can choose the critical areas based on the real-time system status. On the other hand, basic area-based attack has assigned resources for all target areas before the attack, thus if an attack to a relay is not successful (assume the

Algorithm 8 Iterative Protection Area-based Attack.

Input: Transmission Line Set L of a Power Network and Attack Resource N_A
Output: Target Line Set L' to Be Attacked
Method:

1: The attacker will attack two primary relays of each selected area, the total number is at most $\frac{N_A}{2}$
2: **for** each line $l_i \in L$ **do**
3: l_i corresponds to protection area A_i
4: The attacker computes the number of lines not tripped in A_i as $n'(i)$
5: **end for**
6: The attacker greedily selects the area with potentially most corresponding lines to trip
7: After one selection, the attacker tries to compromise the two primary relays of the selected area.
8: When the attack is successful, the attacker trips the potentially affected lines, continues monitoring the network, and updates the number of potential lines for each protection area
9: The attacker repeats the selection and attack

attacker does not know the real-time situation), the attacker will continue attacking other relays.

(3). **Cascading-aware Relay Selection**: if the attacker knows the sets of lines that can trigger cascading failures, he can focus on attacking these lines. When a cascading is triggered, compared with direct attacks to relays, more lines can be tripped with fewer resources. Thus the efficiency of the attack can also be increased. To the attacker, the protection relays of the initial lines are critical targets. The method of assigning multiple attack resource units to one relay (repeatedly attacking the same relay) can be used in a cascading-aware attack to amplify the effect. The requirement that the attacker knows the triggering lines of cascading and the current system state makes it a considerable difficulty for the attacker to conduct this attack. However, if the attacker manages to obtain the information (e.g., as an insider), it may cause serious damage to the system.

5.3.2 Analysis of Attack Strategies

(1). Effect of Random Attack on Local Lines

For a compromised relay, it can trip its local primary line. When two compromised

Algorithm 9 Basic Protection Area-based Attack.

Input: Transmission Line Set L of a Power Network and Attack Resource N_A
Output: Target Line Set L' to Be Attacked
Method:

1: The attacker will attack two primary relays of each selected area, the total number is $\frac{N_A}{2}$
2: **for** each line $l_i \in L$ **do**
3: l_i corresponds to protection area A_i
4: The total number of lines in area A_i is $1 + n(i)$ ▷ $n(i)$ is the number of neighbor lines in the protection area A_i
5: **end for**
6: The attacker greedily selects the area with potentially most corresponding lines to trip
7: After one selection, the attacker continues selecting the other target areas until all resources are used

relays are on the same line, they both affect the same local line. Given the amount of attack resource N_A and a total of R relays in a network, we assume $N_A \leq R$. Assume the attacker randomly picks a relay to attack with one unit of attack resource. We represent the number of lines with two relays attacked (case 1) as j; there will be $(N_A - 2j)$ lines with one relay attacked (case 2). Therefore, the probability that $(N_A - j)$ local lines are attacked is:

$$P(N_A - j) = \frac{C_{\frac{R}{2}}^{(N_A-2j)} \cdot 2^{(N_A-2j)} \cdot C_{\frac{R}{2}-(N_A-2j)}^{j}}{C_R^{N_A}} \tag{5.1}$$

Here, we first select $(N_A - 2j)$ lines from a total of $\frac{R}{2}$ lines (case 2). Since each of these lines only have one relay attacked, and each line has two relays, there will be $2^{(N_A-2j)}$ choices. Then, we select the j lines with two relays attacked (case 1) from the remaining $\frac{R}{2} - (N_A - 2j)$ lines.

Assume the defense strength of a relay is P_f. For each line with two relays attacked, the probability that this line will be tripped is $(1 - P_f^2)$; and for each line with one relay attacked, the probability that this line will be tripped is $(1 - P_f)$. We denote the number of tripped lines as $T(j)$ when $(N_A - j)$ lines are attacked. The expectation of $T(j)$ can be

defined as:

$$E\big(T(j)\big) = (N_A - 2j)(1 - P_f) + j(1 - P_f^2) \tag{5.2}$$

We can find the total number of locally tripped lines T_p as:

$$E\big(T_p\big) = \sum_{j=1}^{\frac{N_A}{2}} P(N_A - j) \cdot E\big(T(j)\big) \tag{5.3}$$

(2). Effect of Iterative Area-based Attack

The main idea of area-based attacks is to exploit relay agents to indirectly trip more neighbor lines of compromised relays, in addition to directly tripping the line with the compromised relays. In the best case for an attacker, it attacks each area one by one, and knows the results of the previous attempts on relays and the current system status. So, it can use an iterative area-based attack to select the most important area with the most lines to trip as the next target. So the potential damage of such an attack can be seen as *the upper bound for area-based attacks*. In the basic agent-based protection or the agent-reputation-based protection, a backup relay may be tripped by a trusted reply from a peer agent. The iterative area-based attack will focus on the two primary relays of a selected area, because these relays can be used to trip neighbor relays at both sides of the primary line. Since the attacker knows which area is the most important based on the current system status, if the attempt to a relay in the area is not successful, the attacker will repeatedly attack the relay until the target relay is compromised.

Assume the average degree of the network is $d(avg)$, then the average number of lines in an area is $2 \cdot d(avg) - 1$, with 1 primary line and $2 \cdot (d(avg) - 1)$ neighbor lines. If the two primary relays of an area are compromised, then all backup lines within this area can be tripped by the trip requests from the primary relays, according to the existing protection mechanism. Assume the defense strength of a relay is P_f, because the attacker will keep attacking a relay until the relay is compromised, then on average the attacker needs $\frac{1}{1-P_f}$

units of attack resource to compromise it. In the attack to an area, the attacker needs $\frac{2}{1-P_f}$ units of resource to complete his attack in order to trip all backup lines of the primary line. With a total of N_A resource units, the attacker on average can compromise $N_l = \frac{N_A}{2} \cdot (1-P_f)$ lines in the network. This N_l can be seen as a lower bound of iterative area-based attack (lines tripped by their local protection relays). Based on the attack strategy of iterative area-based attack, we notice that: (i). the attacker can compromise the two primary relays for most of the selected areas; and (ii). many selected areas will have none, or only few lines overlapped with the other areas, since in the selection the attacker already considered how to trip the largest number of lines by avoiding attacking overlapped areas. Thus, we can estimate the expected number of line trips in an iterative area-based attack as:

$$E(iterative) = min\Big(N_l \cdot \big(2 \cdot d(avg) - 1\big), \frac{R}{2}\Big) \tag{5.4}$$

(3). Effect of Direct Cascading-aware Attack

In a direct cascading-aware attack, the maximum total damage is the number of initial line trips plus the number of extra trips as $N_C(max) = n_k + n_m$. To trigger extra damages, all initial lines should be tripped, the probability of triggering a cascading failure is $P(cascading\ trigger) = (1 - P_f^K)^{n_k}$. The expected damage of a cascading failure can be computed as $E_C = E_C(Initial) + E_C(Extra)$. We examine the expected damages in the following.

A cascading-aware attack aims at triggering a cascading failure by tripping a set of initial lines. In the first step, the attacker needs to identify the critical lines to be tripped (e.g., the n_k lines and the exact locations of the critical relays). The overhead of knowing these may be even higher than knowing the topology and area information of the network, which is another issue the attacker has to consider. However, an insider may still have the chance to obtain the knowledge. When cascading failures happen, the damage can be enormous. Knowing n_k and n_m enables the attacker to estimate the cascading damages. In a cascading-aware attack, the attack efficiency $D_U(K)$ (line trips caused by a unit of attack

resource) can be computed as:

$$D_U(K) = \frac{(1 - P_f^K) \cdot n_k + (1 - P_f^K)^{n_k} \cdot n_m}{n_k \cdot K} \tag{5.5}$$

The attacker may adopt a certain value of K to attack a target relay for the highest attack efficiency, based on different factors. When the number of initial line n_k increases, $(1 - P_f^K) \cdot n_k$ will become dominant, as $(1 - P_f^K)^{n_k}$ is relatively small (because a cascading failure is rare). It will be more obvious when P_f is high or K is small. As can be seen from the analysis, when n_k is larger than a certain value, a cascading failure is very difficult to trigger. The expected damage will be determined mainly by the local tripped lines.

5.4 Exploiting Reputation in Relay Protection

5.4.1 Majority-based Confirmation Rule

Based on historical data, more than 70% of major power system disturbances involved relays that caused cascading failures. This is the primary motivation that agent-reputation-based relay protection is developed, which is to further enhance reliability and efficiency of the relay protection system. We have seen that compromising two relays is the minimum requirement under the basic agent-based or basic agent-reputation-based schemes. As a straight-forward improvement, we may expect confirmations from a majority number of neighbor agents. If the majority rule is used, then the attacker needs to compromise more backup relays in a protection area. We may assume for a relay to trip the local line as required by the received trip request, the majority of the received responses should agree with the trip request.

The majority rule in relay trip confirmation is as follows: for an area A_i, the total number of primary and backup relays is N_i. Normally in the basic agent-based protection, for a trip request from a primary relay, the total number of relays needed to confirm is at least $\lfloor \frac{N_i}{2} + 0.5 \rfloor$, including the primary relay issuing the request. If the agent-reputation-based protection is used, considering that not all relays may be always functional correctly,

the system configuration may require the number of confirmations to be majority within the trusted reports received by a relay agent. In a normal situation, the communication network is working correctly, a relay should be able to receive responses from all neighbor relays.

The algorithm of area-based attack under the majority rule is as follows: based on the available attack resources, from the areas that can be attacked by the resources, the attacker selects an area with the most lines to trip. For a selected area A_i, it has totally N_i relays, which includes 2 primary relays and $N_i - 2$ backup relays. The attacker will try to compromise the two primary relays so that he can trip backup lines at both sides; while for backup relays, the attacker needs to compromise $\lfloor \frac{N_i}{2} + 0.5 \rfloor - 2$ backup relays to achieve majority in the selected area. After the attack to one area is completed, the attacker will repeat the above steps and select the next area and its relays.

Under the majority rule, for an area to be completely compromised (e.g., all lines can be tripped), the attacker needs to compromise $\lfloor \frac{N_i}{2} + 0.5 \rfloor$ relays. Assume the attacker has N_A units of resource, then there will be at most $N_l(m) = \frac{N_A}{\lfloor \frac{N_i}{2} + 0.5 \rfloor} \cdot (1 - P_f)$ areas compromised. We use a simple approach to estimate the total number of lines tripped in an iterative area-based attack under the majority confirmation rule as:

$$E_M(iterative) = min\Big(N_l(m) \cdot \big(2 \cdot d(avg) - 1\big), \frac{R}{2}\Big) \tag{5.6}$$

A neighbor line l_n in an area may be tripped by the locally compromised backup relay, or be tripped by the request from a primary relay. Since an iterative area-based attack will avoid attacking overlapped lines, we assume that the attacked areas have almost no overlapped lines.

5.4.2 Reputation-based Cascading-aware Attack

Reputation information is used by relay agents to enhance reliability, make faster and better decisions, and prevent problems caused by occasional relay mechanical errors. The trust value of a peer agent is determined by how it responds to the query of a local agent (e.g.,

periodic data exchange). When a local agent sends out a query, it will then make a decision based on the responses of trusted peer relays. In the normal situation, it is not difficult to make a correct decision as the responses from agents with lower trust values are ignored. However, the agent-reputation-based scheme can be exploited by compromising some critical relays or routers. If a router is compromised, the attacker can modify or drop the response packets sent to a target relay agent. As a result, only the compromised relay agents are "trusted", and will be considered under the majority rule by a target relay agent. Then the attacker can indirectly trip a target relay. This attack method will be especially useful to trick relay agents that are hard to compromise.

When agent-reputation-based protection schemes are enabled, the attacker may trigger a cascading failure in the system with the new attack method. We examine an example in a more detailed way to demonstrate the potential benefit for the attacker. In Fig. 5.2, the goal of the attacker is to trip the critical relay r_i to launch cascading. Instead of directly attacking r_i which may be well protected, the attacker can first identify a line where r_i is a backup relay of this line. Then the attacker can compromise a primary relay r_j of the line, and another relay (e.g., r_k) in this area, assume he knows they have relatively low defense strength. The attacker also compromises the $Router2$ (or $Router1$). Then he can drop the periodic exchanged updates from the uncompromised relay agents. In this way, only the compromised relay agents r_j and r_k have high reputation to be considered as trusted by the targeted agent r_i. The attack will bring the attacker benefit if the expected cost of attacking neighbor devices is much less than attacking a critical one. For instance, if we assume $P_f(r_i) = 0.9$, other relays have defense strength $P_f(r) = 0.5$, $P_f(router) = 0.1$, the resource requirement to compromise a relay or a router is 1, as to the average resources required to trip relay r_i, for direct attack, $E(direct\ attack) = \frac{1}{0.1} = 10$, for agent-reputation-based attack, $E(reputation\ based\ attack) = \frac{2}{0.5} + \frac{1}{0.9} = 6.1$.

From the analysis we can see that the confirmation rules will not affect the direct cascading-aware attack, because this cascading attack directly compromises relays to trip the critical local lines. The effectiveness of cascading attack depends on the defense strength

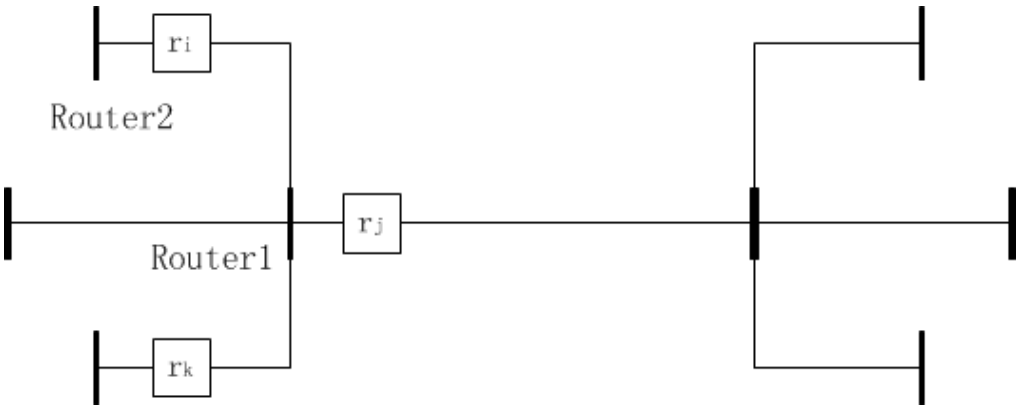


Figure 5.2: Example of Attacks on Relay Protection with Reputation.

of relays, the number of initial lines that the attacker has to trip, and the resources available to the attacker. Under relatively high defense strength (e.g., higher than 0.8) with a considerable size of initial line set, it is rather difficult to trigger cascading failures by directly attacking the critical relays, as the available resources may not be able to support all required line trips. However, by exploiting the potential weakness of agent-reputation-based relay protection, the attacker may obtain a chance to better conduct the cascading-aware attack in the system. In this way, the attacker may not only have better probability to trigger a cascading failure, but also use less resources in an attack. In the following, we will analyze the effect of agent-reputation-based cascading-aware attack.

Assumptions. For simplicity, we have the following assumptions for agent-reputation-based cascading attack:

(1). The relays on the initial lines $\{n_k\}$ have higher defense strength, while the relays on its neighbor lines and the routers in the network have relatively low defense strength.

(2). All initial lines are in different protection areas with no overlaps.

(3). The topology of communication network is the same as the power system. Each node contains one router. When a router is compromised, a relay on a line connected to this router may not be compromised.

Assme the attacker knows the set of initial line $\{n_k\}$, and all these lines are located in different areas that do not overlap. Instead of attacking their relays directly, for each

targeted relay r_i of an initial cascading line $l_i \in \{n_k\}$, the attacker identifies a neighbor line l_j, that r_i is a backup relay of l_j. The attacker attacks the two primary relays of l_j, $r_p(j,1)$ and $r_p(j,2)$ (as information from primary relays may be considered more accurate than from backup relays), and attacks the node (router) RT_i that r_i is directly connected to. Each selected device will be assigned certain amount of attack resources.When the attemps to these neighbor devices succeed, one primary relay can issue a trip request to r_i and the other primary relay will confirm the request. As router RT_i is compromised, the normal periodic updates from other innocent neighbor relays to r_i are dropped, which results in low trust of those neighbor relays.

In this attack, whether a cascading failure can be triggered relies on whether the n_k initial lines can be tripped. To trip a target line under the agent-reputation-based protection scheme, the attacker needs to compromise two relays (e.g., primary relays) and one router. Assume the defense strength of the primary relays is $P_f(r)$, and the defense strength of the router is $P_f(n)$, the attacker use K_r units of resource to attack a relay and K_n units to attack a router. Then, we can find the probability that the targeted relay r_i is tripped, $P_R(r_i)$, as:

$$P_R(r_i) = \left(1 - P_f(r)^{(K_r)}\right)^2 \cdot \left(1 - P_f(n)^{(K_n)}\right) \tag{5.7}$$

The probability of triggering cascading P_T is:

$$P_{T,R} = \prod_{r_i \in \{n_k\}} P_R(r_i) \tag{5.8}$$

The cascading-aware attack on the agent-reputation-based protection is suitable for the situation where critical relays have high defense strength, while the other relays and nodes have relatively lower defense. Under this attack, if the neighbor devices of a critical relay are compromised, a line in the set of initial lines $\{n_k\}$ can be indirectly tripped. We count the total number of line trips in this set and the set of extra tripped lines $\{n_m\}$. The total

expected number of line trips under this attack $E_{C,R}$ is computed as:

$$E_{C,R} = \sum_{l_i \in \{n_k\}} P(l_i \ trip) + P_T \cdot n_m \tag{5.9}$$

5.5 Performance Evaluation

We set up a simulation network and evaluate the attack strategies under various conditions to show the effects of different attacks and also give us better understanding on how to design countermeasures to defend the relay protection in general.

Small World Network. We adopt the small-world model [87, 88, 89] to generate the generic network topologies for our evaluation. It has been shown that many power grids [90, 91] (such as the western US electrical power grid) are small world networks. To construct a small world network, the following steps can be used. Starting with a ring of n vertices, each connected to its k nearest neighbors by undirected edges. A vertex v is selected, and then the edge that connects v to the nearest neighbor is selected. With probability p_r, the edge is reconnected to a vertex chosen randomly over the entire ring, except for the duplicated edges; otherwise the edge is left unchanged. Each vertex will be considered until one lap completed. Next, start from v again, the edge connects to the second nearest neighbor will be selected and rewired as before. The process continues circulating around the ring and proceeding outward to more distant neighbors after each lap, until each edge in the original lattice has been considered once. There are $n \cdot \frac{k}{2}$ edges in the network, and the rewire process stops after $\frac{k}{2}$ laps. It is suggested that for intermediate values of p_r, the graph is a more typical small-world network.

Simulation Setup. The python igraph [92] module is used to generate the small world network. The topology is represented as a graph $G = (dim,\ size,\ nei,\ p_r)$. Four parameters are given to create a network, where dim is the dimension of the initial lattice which can be 1 for simplicity, and $size$ is the number of node in each dimension. A node will connect to neighbors at nei hops away, and p_r is the probability of rewiring: 0 means no rewiring that the initial lattice is regular, and 1 means all initial edges will be rewired. It is suggested that

an average degree of 4 may provide good balance between modularity, performance, and thrift for future power grid [90]. For each simulation, we achieve results from ten randomly generated networks, and compute the averaged value.

5.5.1 Numerical Evaluation of Attack Strategies

We first evaluate the effect of random attack to local lines given certain amount of resources. We compare the results of estimation and simulation in the test. Assume the amount of attack resource $N_A < R$, where R is the number of relays in the network. The setup network parameters are: network of $dim = 1$, $nei = 2$, with size of 60 nodes and 120 lines (240 relays), which means an average node degree of 4. The selection of the parameters is based on a practical system with 60 buses, 110 lines, and average degree of 3.67 [91]. The rewiring probability is set to $p_r = 0.1$, as mentioned in [87, 88, 89, 93, 94] that an intermediate value of p_r (e.g., 0.01 to 0.1) will result in a more typical small world network. The defense strength of relays is set at different levels (e.g., 0.2, 0.5, and 0.8) to test the effects. In the Fig. 5.3, the curves of estimation and simulation almost match. Thus the effect of local attack can be accurately estimated by the attacker as a base case.

Random attack focuses on trip of local lines. Area-based attack amplifies damages by tripping more neighbor lines of the selected targets. As an upper bound, the iterative area-based attack may provide the most benefit for an attacker. We compare the results of estimation and simulation for iterative area-based attack. The network parameters used are the same as in the random attack test. The result is shown in Fig. 5.4a. The difference between estimation and simulation is demonstrated in Fig. 5.4b.

From the result in Fig. 5.4b, we observe that for $P_f = 0.2$, after attack resource is larger than 32 units (e.g., the attacker can attack about 12% of the relays in the system if each is assigned 1 unit of resource), the absolute value of percentage of difference between estimation and simulation $\left|\frac{(simulation\ -\ analysis)}{analysis}\right|$ will be smaller than 10%. The similar trend is also observed for the curve of $P_f = 0.5$ and the curve of $P_f = 0.8$ (when amount of resource larger than 48 and 96 units respectively). From the analysis, the attacker with N_A

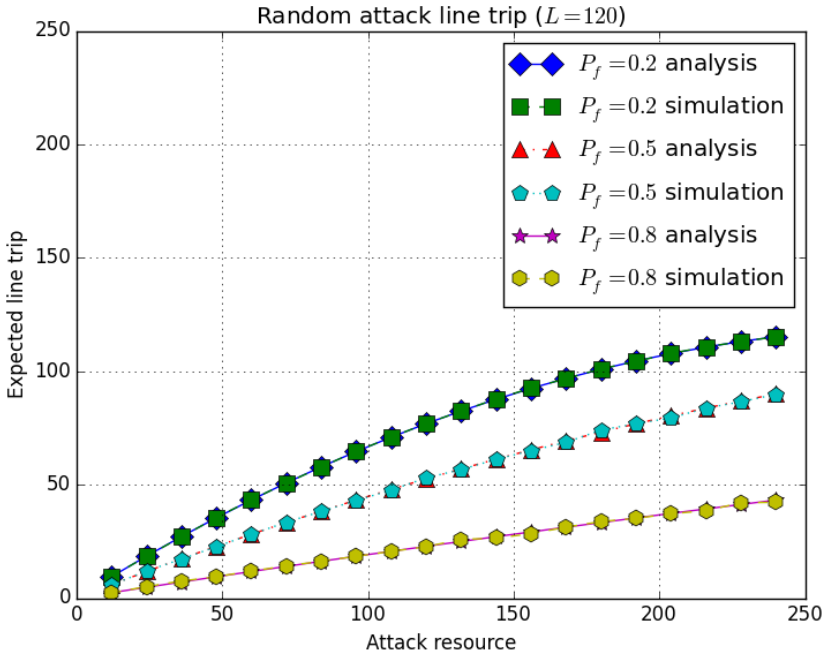
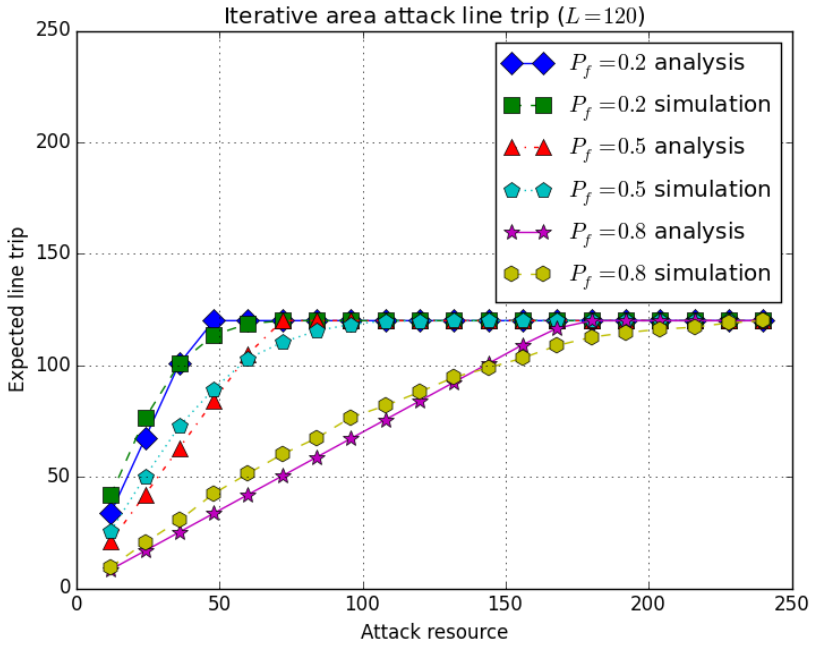


Figure 5.3: Effect of Random Attacks on Local Lines.

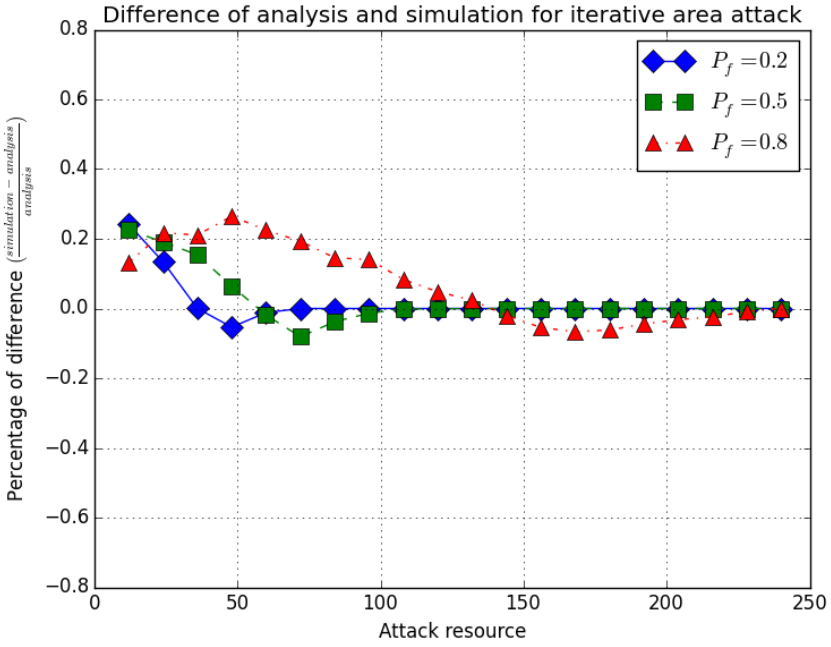
units of resource can compromise $N_r = N_A \cdot (1 - P_f)$ relays in the iterative area-based attack. If we divide N_r by the total number of relays in the system, we get 10.7%, 10% and 9% respectively. Also for iterative area-based attack, the attacker will compromise two primary relays for a target line. Thus on average, when the attacker is able to compromise 10% of the lines/areas, the estimation of the attack result can be more accurate (with difference less than 10%). Compare the result of area-based attack with the result of random attack, we observe that the attack efficiency is dramatically increased at relatively small amount of attack resources.

We also test the effect cascading-aware attack. The probability of triggering cascading failures in a network is analyzed with different parameters of attack number K, defense strength P_f, and size of initial line set n_k. The results are shown in Fig. 5.5. We also examine the attack efficiency in Fig. 5.6, where we change n_m, and set $n_k = 0.05L$. Our observations are as following:

(1). The defense strength P_f has large effect on cascading result, as shown in Fig. 5.5a



(a) Expected Line Trip



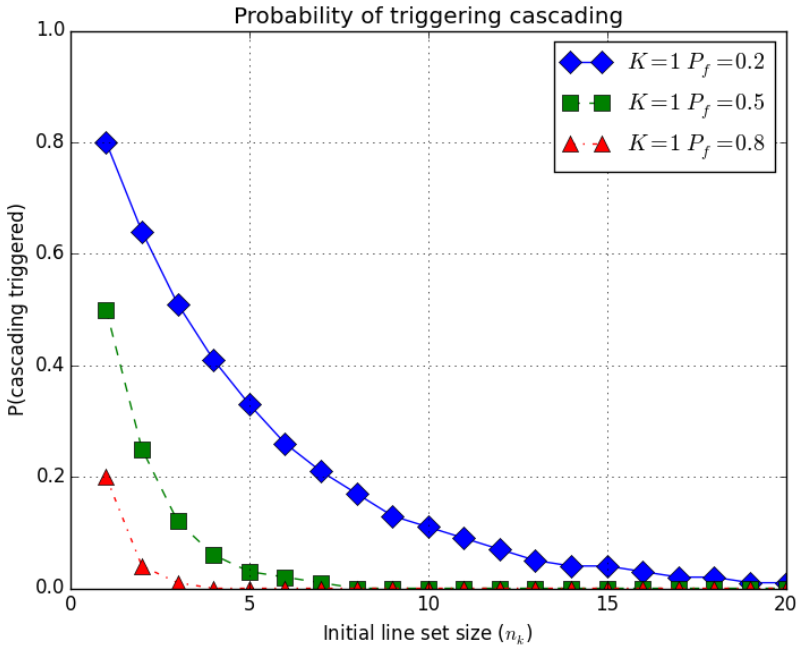
(b) Difference Between Analysis and Simulation

Figure 5.4: Evaluation of Effect of Iterative Area-based Attacks.

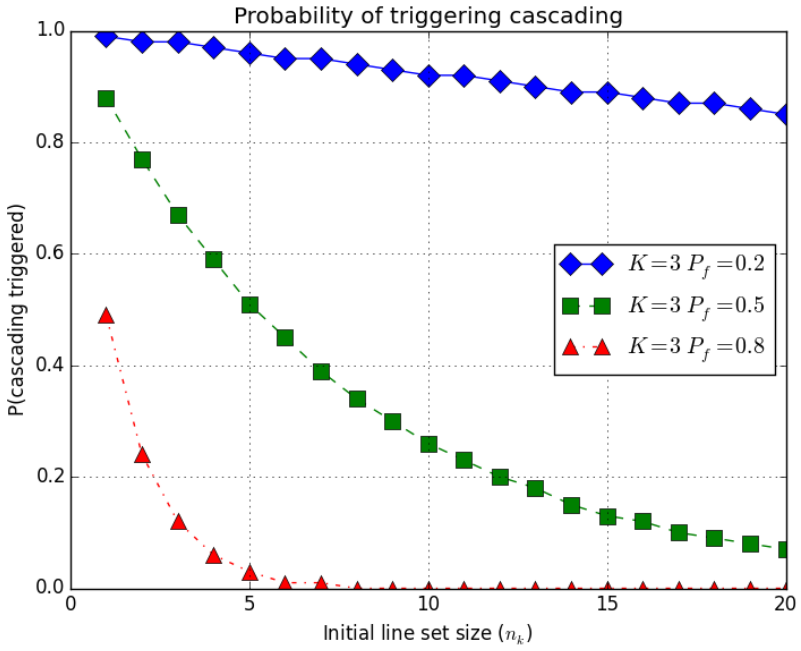
through Fig. 5.5d. As we can see, when system defense is relatively high (e.g., $P_f = 0.8$), as we increase the value of K, the probability of triggering cascading still decreases dramatically. As a comparison, at the situation when P_f is relatively small, increasing K slightly can significantly increase the potential cascading-aware attack damage.

(2). Larger initial line set size n_k also increase the difficulty of cascading-aware attack, because it is more difficult to trip all required initial lines with certain amount of resources, even the critical relays have moderate or low defense strength. In the real world, this may correspond to the situation where the system is relatively large and load is moderate, or the system is designed robustly so that it is not that easy to trigger cascading failure even certain proportion of the system components are out of work.

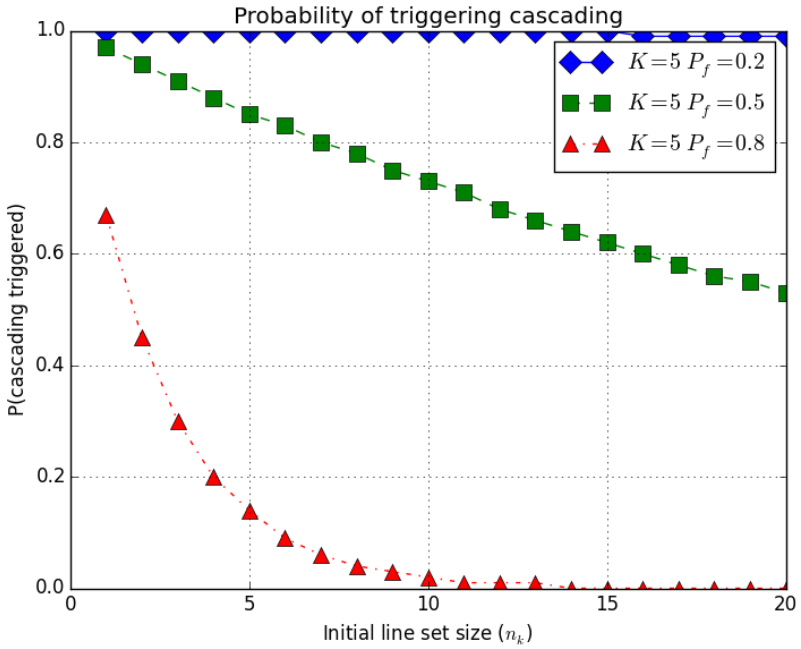
(3). Given certain amount of attack resources, the attacker may determine how to conduct the cascading-aware attack (e.g., amount of resources assigned to a single relay). As shown in Fig. 5.6, for different system conditions, if the attacker knows some critical parameters (e.g., the size of potential extra line trip and relay defense), he can estimate the result of his attack, such as expected number of line trips and attack efficiency. Then the attacker can make decision on how to use his resources for the attack. For example, while more attack resources will lead to higher successful probability, the attacker may assign certain amount of resources to a relay (K) in order to achieve the highest attack efficiency.



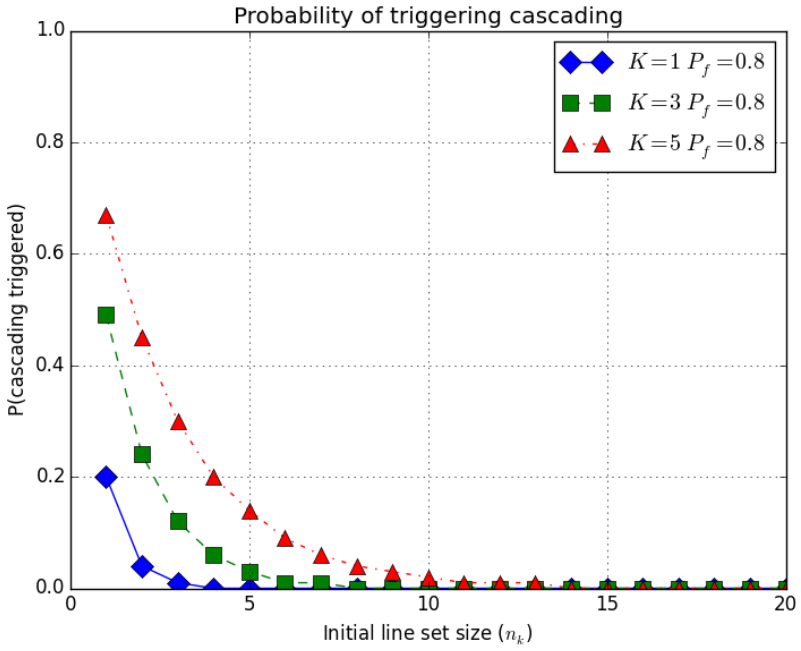
(a) Each Relay Assigned 1 Unit of Resource



(b) Each Relay Assigned 3 Units of Resource

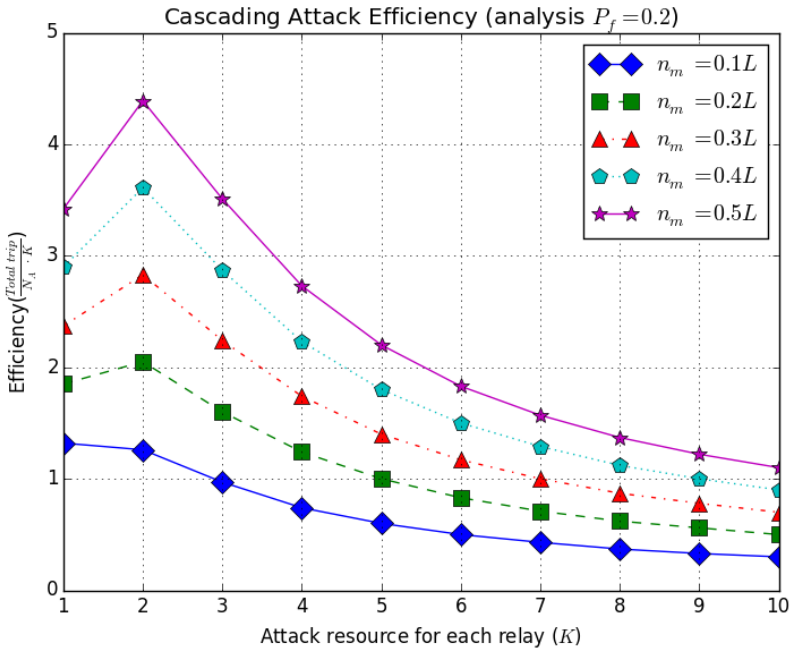


(c) Each Relay Assigned 5 Units of Resource

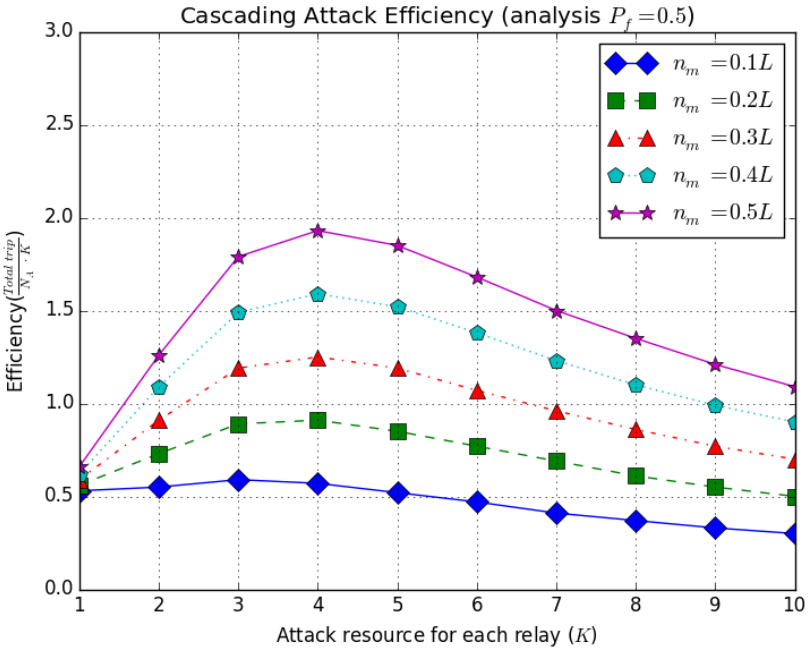


(d) Direct Cascading-aware Attack at High Defense Strength

Figure 5.5: Evaluation of Direct Cascading-aware Attacks.



(a) At Defense Strength $P_f = 0.2$



(b) At Defense Strength $P_f = 0.5$

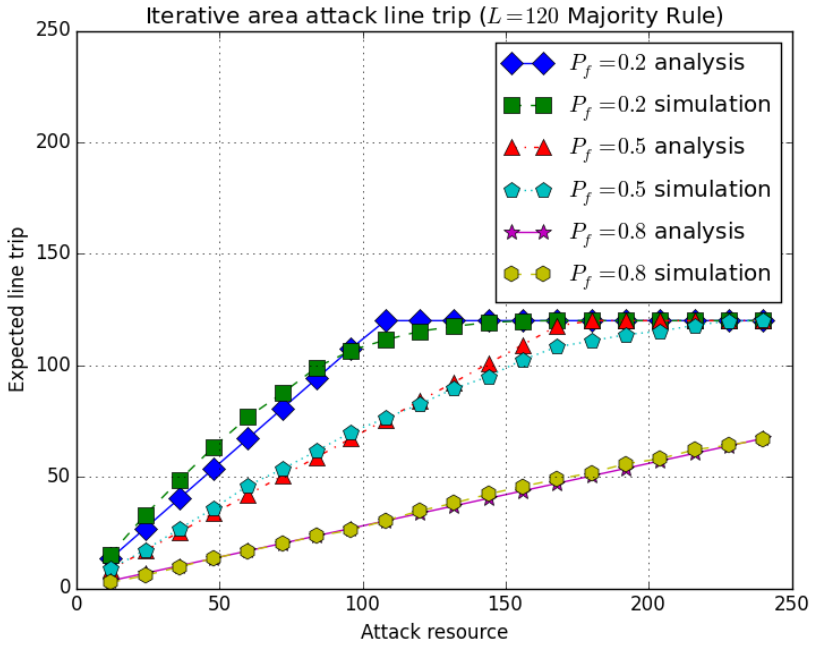
Figure 5.6: Attack Efficiency of Cascading-aware Attacks Under Different Parameters.

5.5.2 Effect of Different Confirmation Rules

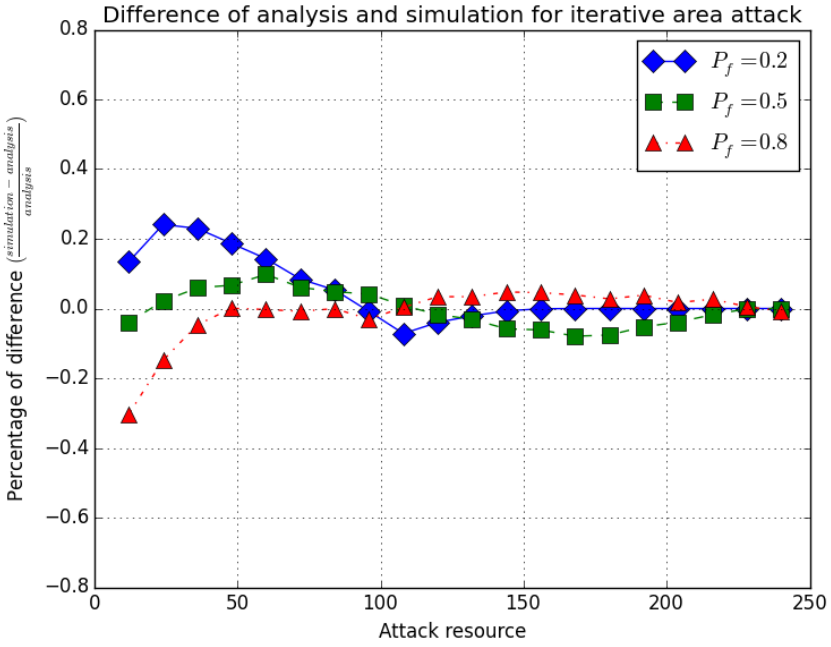
In basic agent-based relay protection and basic agent-reputation-based relay protection, a single confirmation is required if a backup relay receives a trip request from its primary relay. The assumption is that the possibility of multiple hidden failures exposed at the same time is relatively small. By exploiting this protection mechanism, the attacker can compromise the two primary relays of a transmission line, and use area-based attacks to trip the neighbor lines. As a straight-forward improvement, a relay may require the confirmations coming from majority number of neighbor agents in order to trip the line. We will evaluate majority confirmation rule in this section.

We first examine the potential worst case for system protection where the attacker knows that majority confirmation rule is used, and uses iterative area-based attack. To attack the system under majority confirmation rule, the attacker may compromise both primary relays and the corresponding Zone 3 relays in an area. The analysis and simulation results are shown in Fig. 5.7a and Fig. 5.7b, including the expected number of line trips and the difference between analysis and simulation. Similar trend is observed for majority confirmation case compared with basic confirmation case. For different defense strengths of 0.2, 0.5, and 0.8, the difference between estimation and simulation is decreasing as the amount of attack resources goes up. For $P_f = 0.2$, after the attack resource is larger than 70 units, the difference will be smaller than 10%. Under the majority confirmation rule, on average an attack to each area requires 5 relays to achieve majority, in this way the attacker can compromise about 11 areas in the system. Consider there are 120 lines in the system, this ratio is about 9.6%, which is a similar number to the basic confirmation rule. While for the other two curves, their analysis and simulation get closer after 3% of the areas can be compromised. Thus we may consider the estimation to be more accurate if more than 10% of the areas have been compromised, when iterative area-based attack is used under majority confirmation.

When an attacker is planing an attack to the network, he may, or may not know the protection scheme used in system. We test the situation if original relay selection strategy



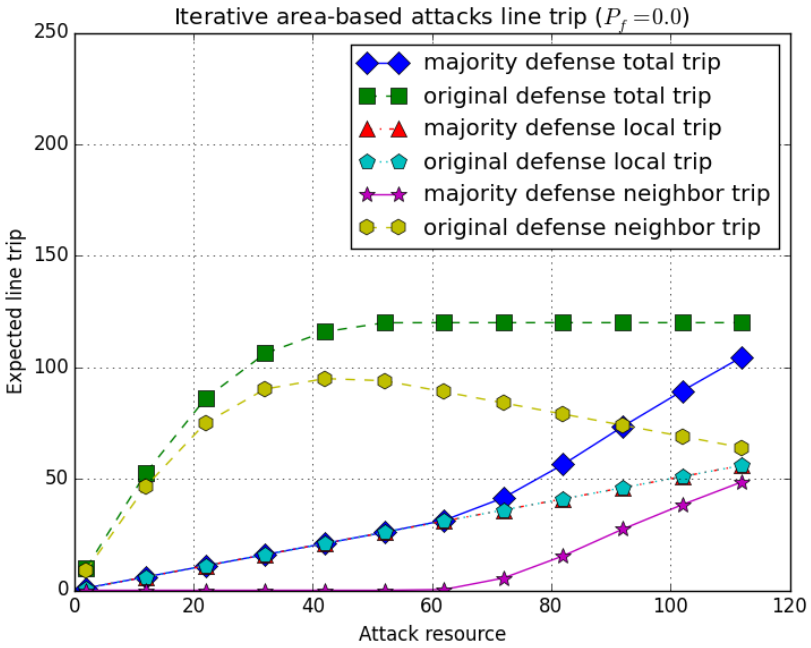
(a) Expected Line Trip



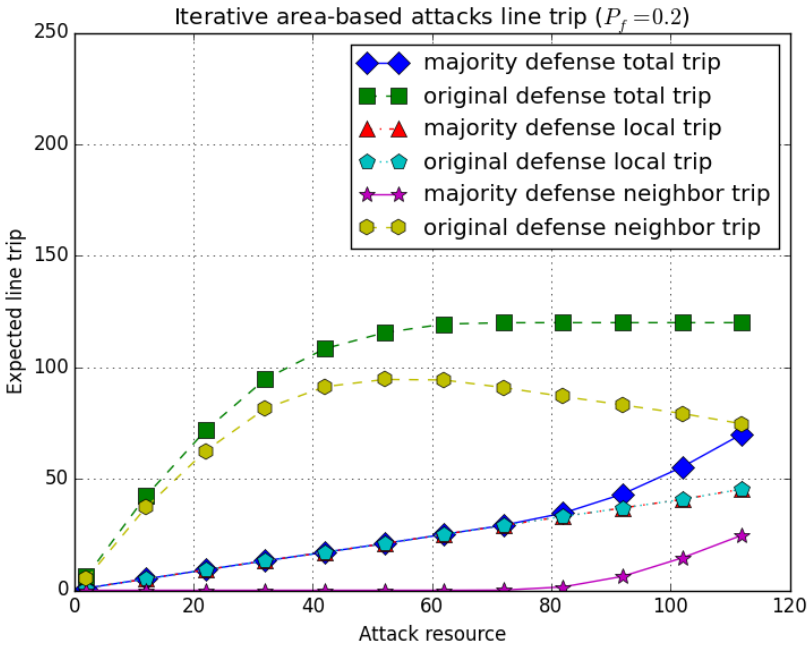
(b) Difference Between Analysis and Simulation

Figure 5.7: Effect of Iterative Area-based Attacks Under Majority Confirmation Rule.

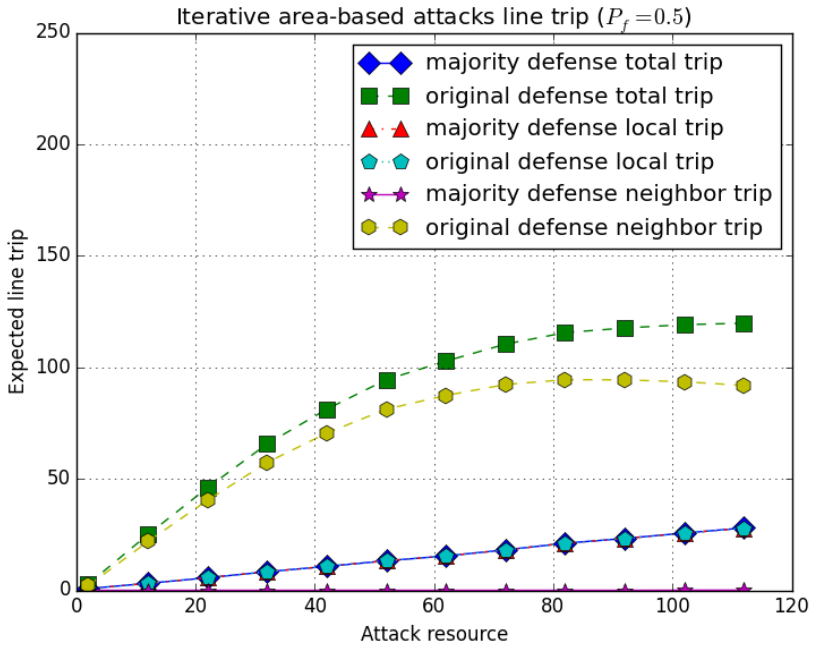
for area-based attack (to attack two primary relays for each selected area) is used, while the system defense actually applies majority-based confirmation rule. We assume that the attacker does not know the defense rule of the system. As a comparison, we also show the effect of using the original area-based relay selection method to target basic confirmation rule. Recall that basic agent-based protection schemes require 1 confirmation from a trusted peer relay. The majority confirmation rule requires that, from all trusted replies, the number of confirmations must be majority. As shown in Fig. 5.8 and Fig. 5.9, generally the number of lines tripped under majority confirmation rule is smaller than the attack result in system where basic confirmation rule is used. When the defense strength of devices is low, the difference is not that significant if the attacker has sufficient attack resources. Because as the amount of resources goes up, more relays are compromised. For a few of the targetted lines, their primary relays and several backup relays may be compromised to achieve the majority, and then their neighbor lines can be tripped indirectly. When the defense strength becomes higher, the original area-based relay selection method can only achieve a much smaller proportion of trips compared with the result at low defense situation. The reason is because relays are more difficult to be compromised, and the majority requirement will be more difficult to achieve for the original area-based relay selection method. As a result, the compromised primary relays can hardly trip their neighbor protection relays (e.g., for the case when $P_f = 0.8$). The tripped lines at the high defense situation are almost contributed by locally compromised relays. For iterative area-based attack, since the selected areas have few overlaps, it is more likely that the compromised relays are not neighbors. Thus starting at moderate defense strength (e.g., $P_f = 0.5$), the effect of iterative area-based attack decreases more significantly. This test demonstrates that majority confirmation rule has improved defense of basic agent-based relay protection and basic agent-reputation-based relay protection to original relay selection in area-based attack strategies. For higher security consideration in the system, relay protection schemes should enable majority-based confirmation rule in trip decision making.



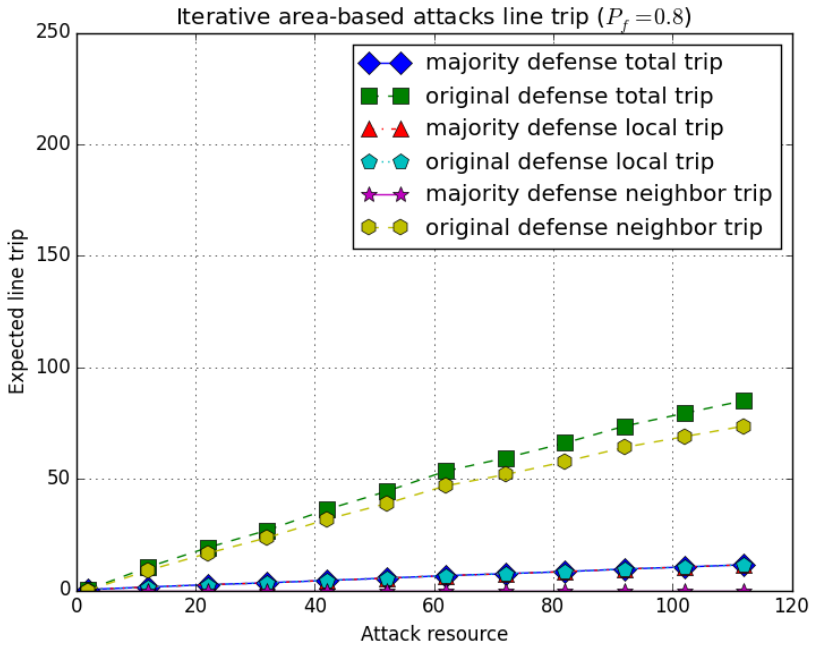
(a) Defense Strength $P_f = 0$



(b) Defense Strength $P_f = 0.2$

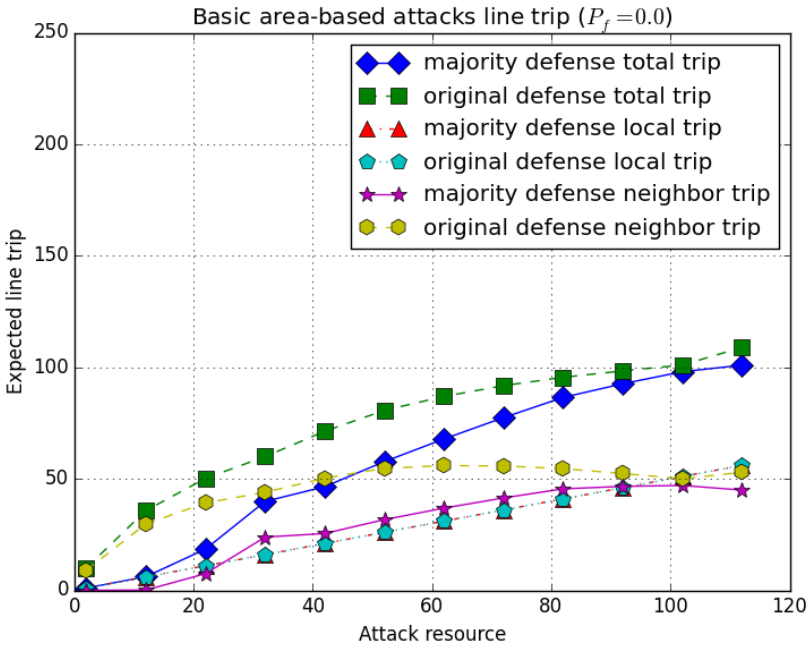


(c) Defense Strength $P_f = 0.5$

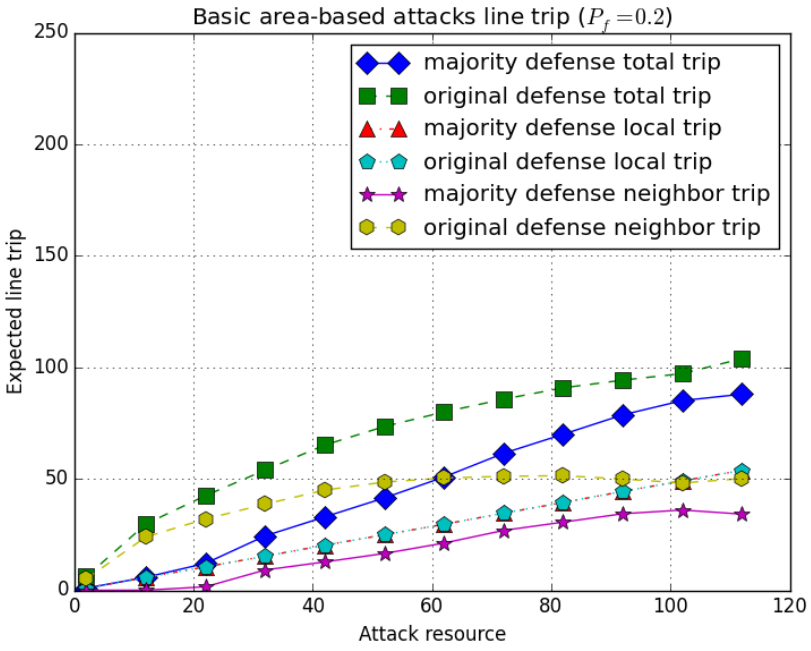


(d) Defense Strength $P_f = 0.8$

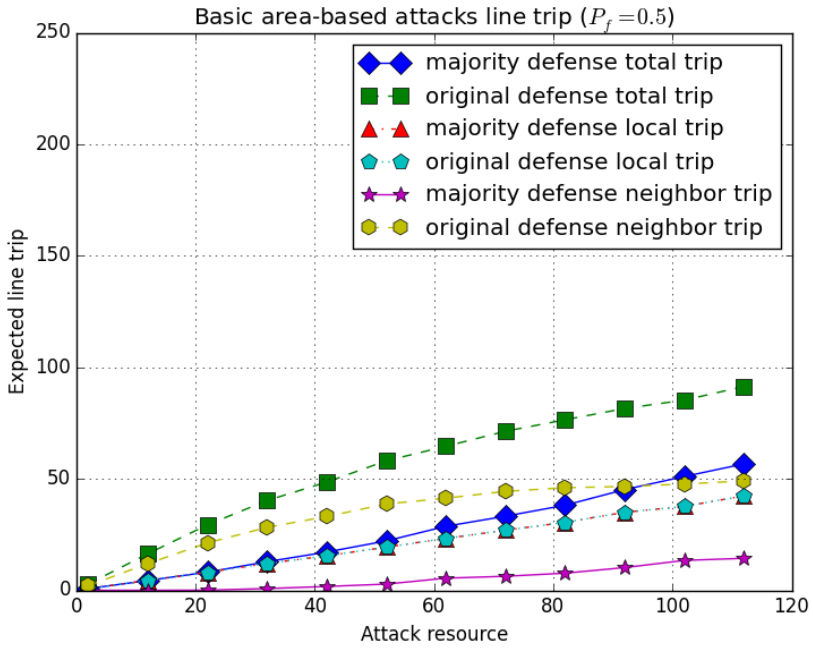
Figure 5.8: Original Relay Selection Under Different Confirmation Rules (Iterative Area-based Attacks).



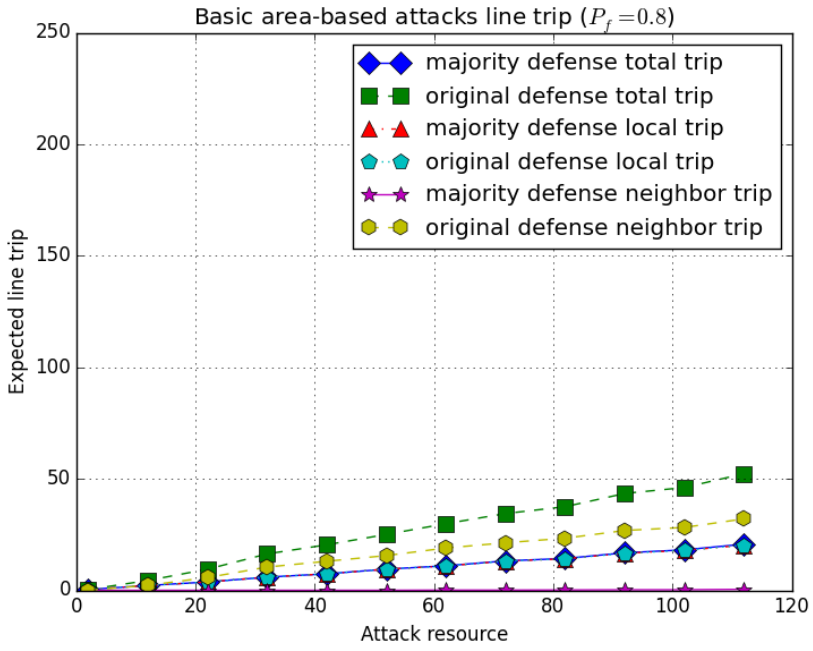
(a) Defense Strength $P_f = 0$



(b) Defense Strength $P_f = 0.2$



(c) Defense Strength $P_f = 0.5$



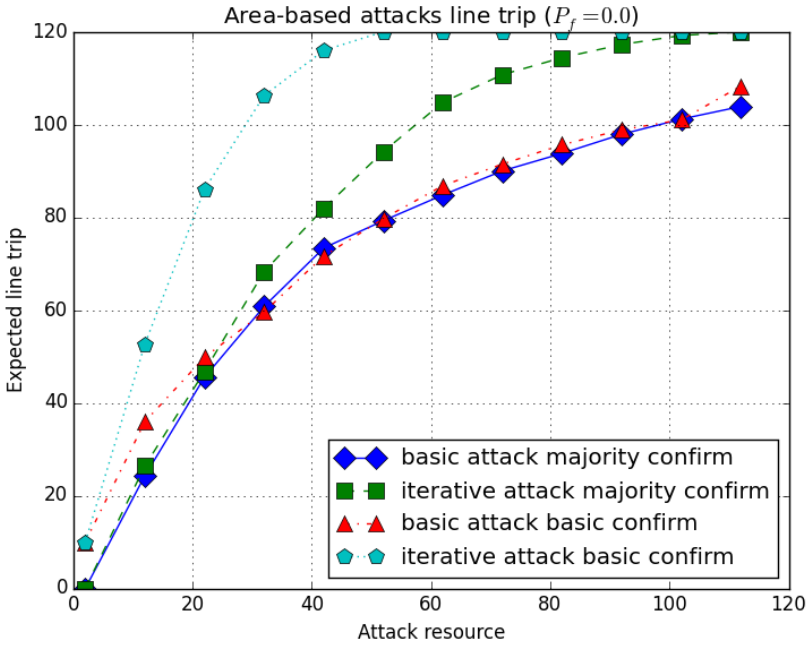
(d) Defense Strength $P_f = 0.8$

Figure 5.9: Original Relay Selection Under Different Confirmation Rules (Basic Area-based Attacks).

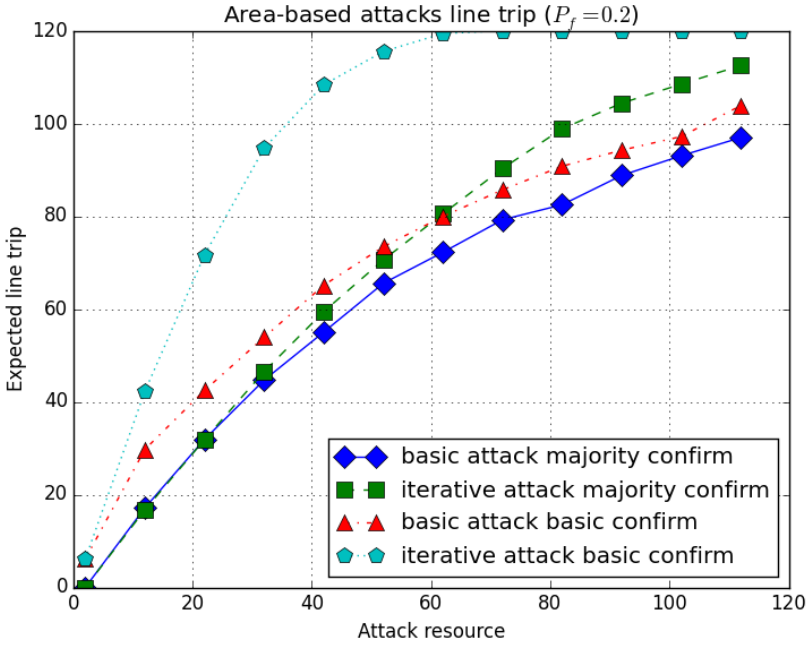
Fig. 5.10a through Fig. 5.10d compare the effects of iterative and basic area-based attacks under different confirmation rules. We test different defense strength levels, including $P_f = 0$, which is the ideal situation to the attacker as all attacks will be successful. As we have seen in previous analysis, iterative area-based attack is the best area-based attack strategy for the attacker if we assume the attacker can know the results of previous attemps. In this test we assume the attacker knows the defense rule used in the system, thus the original area-based relay selection method will be used to attack basic agent-based and basic agent-reputation-based protection schemes, as they require one confirmation. The majority rule-aware area-based attacks will attack systems applying majority-based rule. Under the basic confirmation scheme, if the iterative area-based attack is used, it can achieve much more line trips. The reason is because in each attack the area with the most lines to trip will be selected, and a minimum of two relays are attacked. Thus the attack efficiency of iterative method will be much higher. As for the case under majority rule-based defense, the difference between the two attack methods is up to 20%, which is lower than the difference in the basic confirmation scheme. At the situation of high relay defense strength, for area-based attacks under majority-based rule, the basic and iterative selection methods do not have significant difference. Because when P_f gets large, it will be more difficult to compromise majority number of relays for a selected area in baisc area-based attack. While for iterative area-based attack, the number of compromised areas will be much fewer, as more resources will be used to compromise a single relay.

If the attacker does not have immediate information about previous attack results, or does not have full knowledge of the system, he may use the basic area-based attack method. Under the basic confirmation scheme, the number of line trips in basic area-based attacks will be relatively smaller compared with iterative area-based attacks (e.g., around 60% of the total trip). However, at certain situations the damage may still be significant. For example, at $P_f = 0.2$, with 40 units of resource (e.g., can attack 16% of relays) the attacker trips about 50% of the total lines (although much less than the iterative method). Consider that basic area-based attacks may be conducted within a short period of time, this method

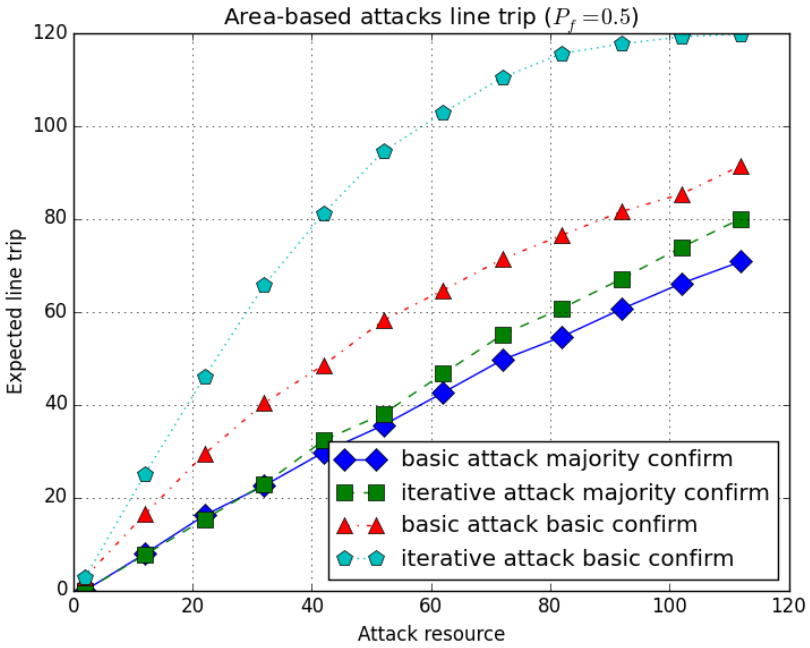
may still be useful for the attacker at relatively low defense situations.



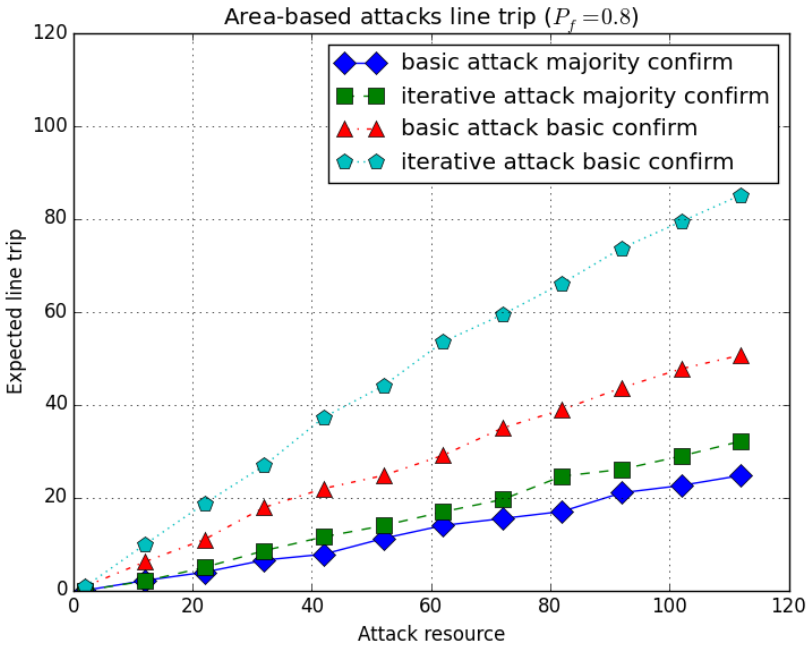
(a) Defense Strength $P_f = 0$



(b) Defense Strength $P_f = 0.2$



(c) Defense Strength $P_f = 0.5$



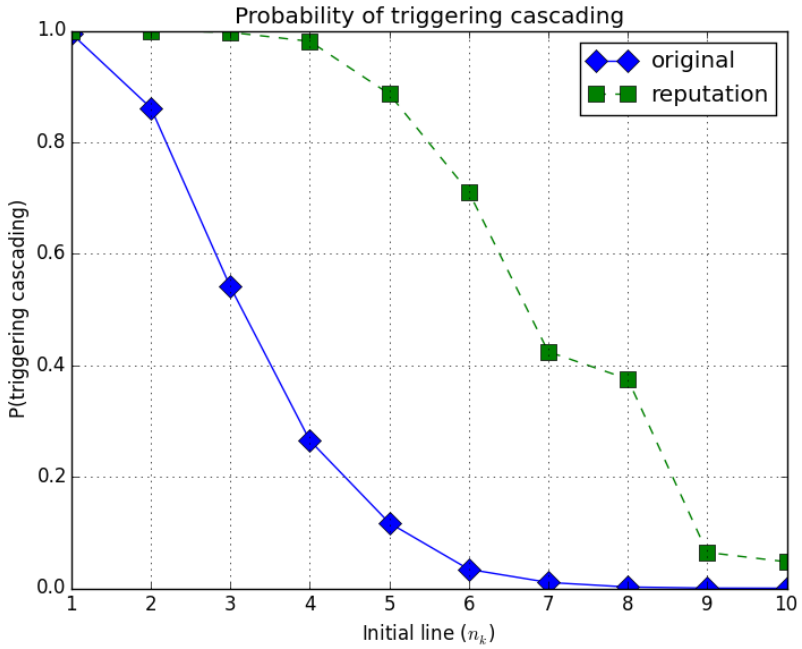
(d) Defense Strength $P_f = 0.8$

Figure 5.10: Comparison of Area-based Attacks Under Different Confirmation Rules.

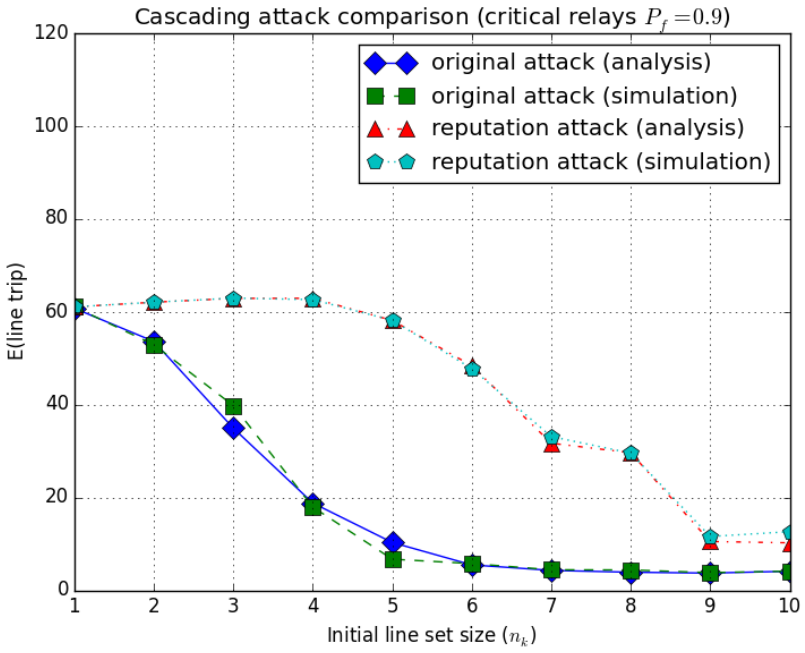
5.5.3 Cascading-aware Attack Exploiting Reputation Schemes

We demonstrate the effect of the cascading attack exploiting agent-reputation-based protection schemes, the results are shown in Fig. 5.11a through Fig. 5.11c. The test network is generated with 120 nodes, $L = 240$ lines, $d(avg) = 4$, $p_r = 0.05$. Assume the relays on the initial lines have high defense strength of 0.9, while other relays and nodes have relatively low defense strength. A total amount of 50 units of resources are used to conduct the cascading-aware attack. Two cascading attack methods are used. For an original direct cascading attack, each relay is assigned $K = \frac{total\ resource}{initial\ size}$ units of attack resources; in a agent-reputation-based cascading attack, each relay is assigned $K_r = \frac{K}{2} - K_n$ units of attack resources where each attacked node is assigned K_n units of resource. We assume in the example that the number of extra cascading line trips $n_m = 0.25L$. In the real world, actual cascading damages may be more serious. According to the evaluation results in [85], when a power system is heavily loaded (e.g., higher than 80%), the ratio of failed components after cascading failure can be higher than 50%, or even approach 100%.

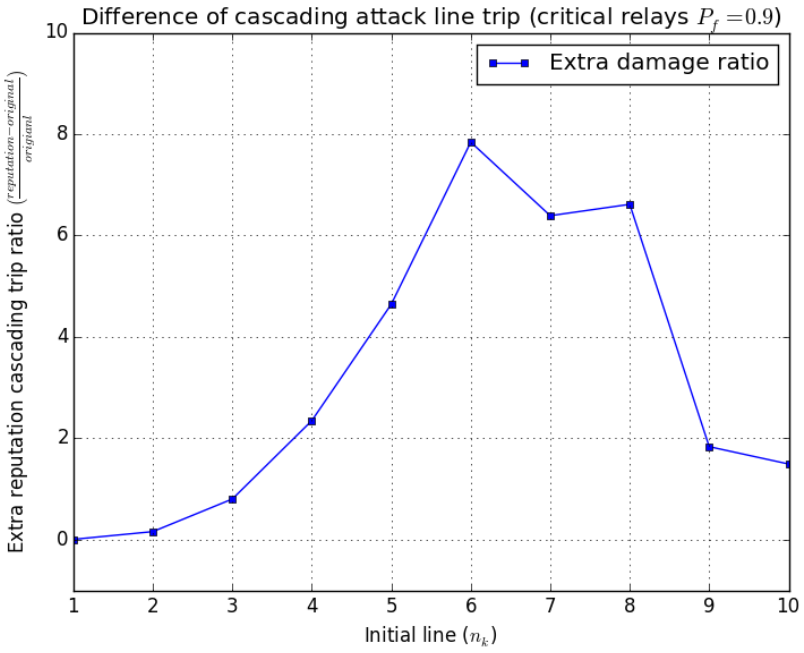
Fig. 5.11a shows the probability of triggering cascading using the two methods. In the test, for a agent-reputation-based cascading attack, we equally divide the attack resources among relays and routers. As we can see, given certain defense parameters, when the initial line set $\{n_k\}$ is relatively small, even the defense strength of the initial lines is high, the original direct cascading-aware attack still has a high probability to trigger cascading failures, because more resources can be used on a relay. When the size of initial line set gets larger, the agent-reputation-based cascading-aware attack becomes more effective since it is more difficult to directly trip all required lines. For example, when the initial line set $n_k = 10$, the probability of agent-reputation-based attack can be 100 times higher than direct attacks. Fig. 5.11b demonstrates analysis of the expected number of tripped lines and the corresponding simulation results. Fig. 5.11c shows the extra line trip ratio of the agent-reputation-based cascading-aware attack from Fig. 5.11b. Denote the expected line trips in the agent-reputation-based cascading-aware attack as E_1, and trips in the direct cascading-aware attack as E_2. The extra trip ratio is computed as $\frac{E_1 - E_2}{E_2}$.



(a) Probability of Triggering Cascading Failure



(b) Expected Line Trip

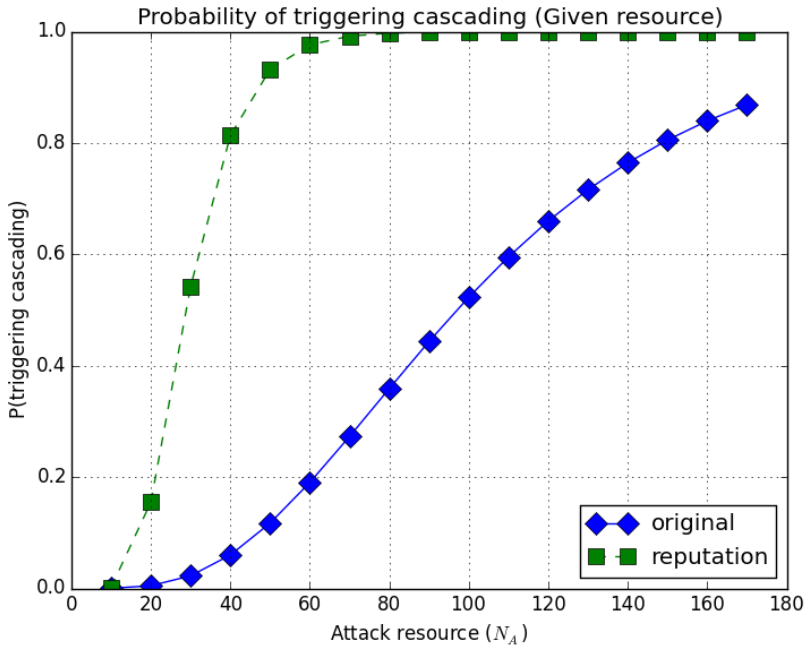


(c) Benefit of Reputation-aware Cascading-aware Attacks over Direct Attacks

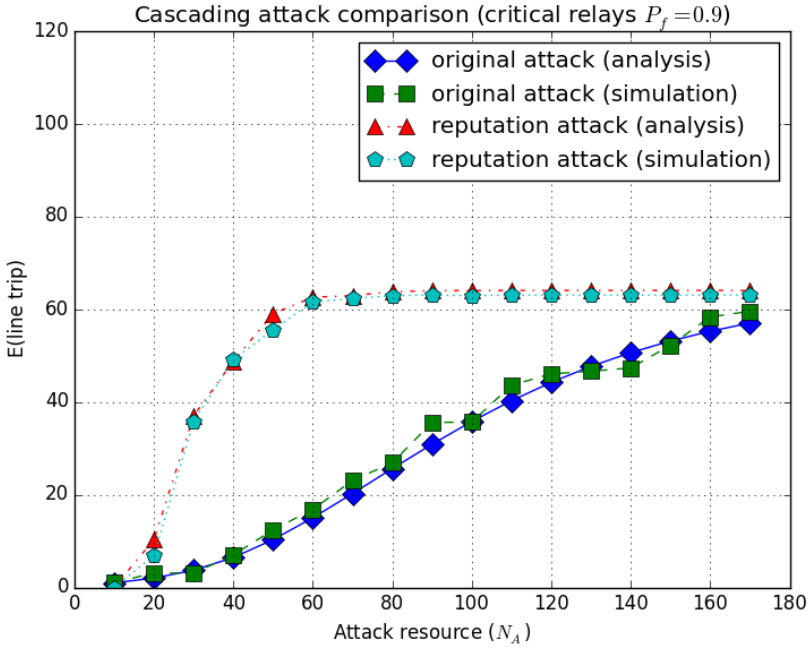
Figure 5.11: Comparison of Cascading-aware Attacks Under Different Sizes of Initial Line Set $\{n_k\}$.

We also test the effect of different amount of attack resources for the two cascading attack methods. The results are shown in Fig. 5.12a through Fig. 5.12c. In this test, we set $n_k = 5$, and keep the other parameters same as in Fig. 5.11. The resources are equally assigned to each selected relay and router. As we can see, at the beginning (e.g., the amount of attack resources is relatively small), when more resources applied, the effect of agent-reputation-based attacks increases much faster than direct attacks. When the amount of resources continues increasing, the cascading triggering probability of the original direct cascading-aware attack will get close to the agent-reputation-based cascading-aware attack method. The analysis and simulation results are shown in Fig. 5.12b. Compare the curves between the two cascading-aware attacks, we can see that, for a given defense strength, the agent-reputation-based cascading attack can achieve the same damage with much less resources (e.g., only take 30% of the resources used by direct attack). The extra line trip

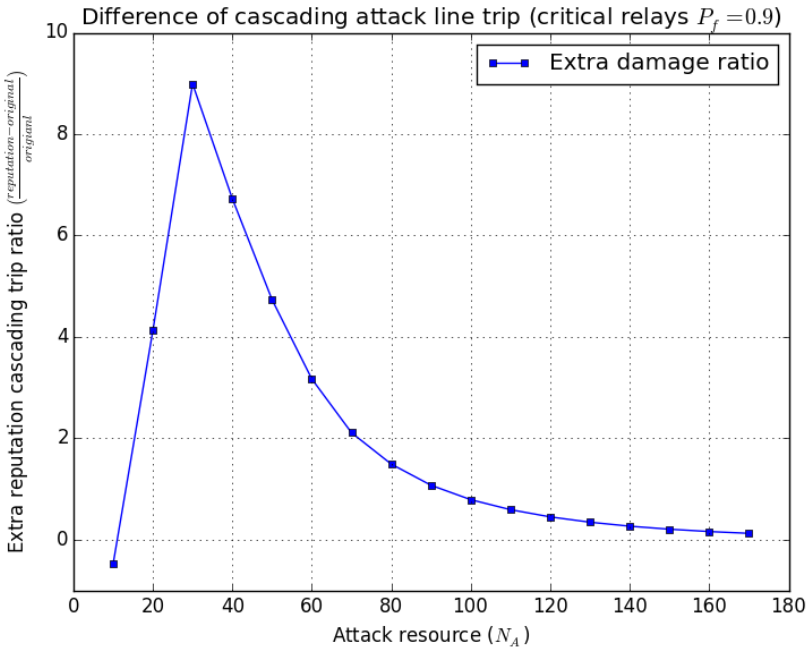
ratio of agent-reputation-based cascading attack is shown in Fig. 5.12c.



(a) Probability of Triggering Cascading Failure



(b) Expected Line Trip

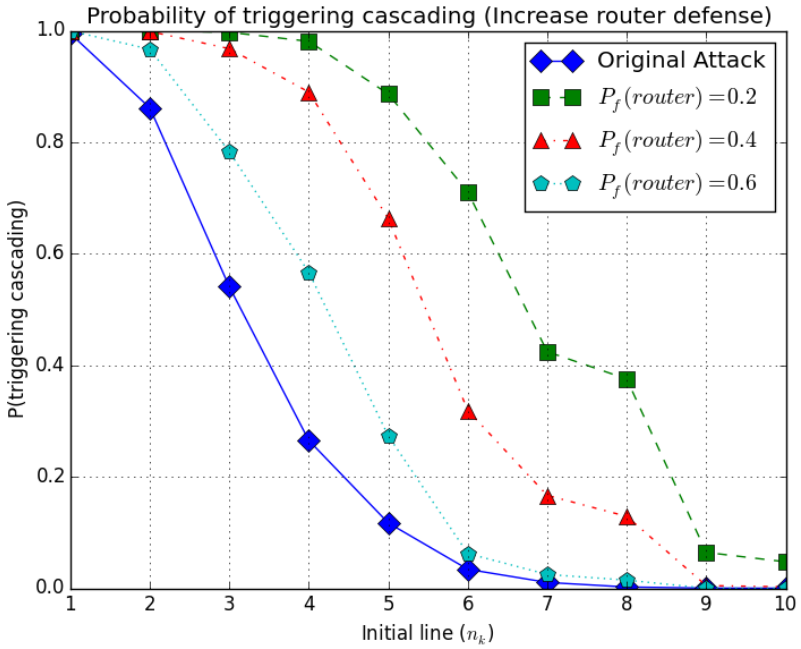


(c) Benefit of Reputation-based Cascading-aware Attacks over Direct Attacks

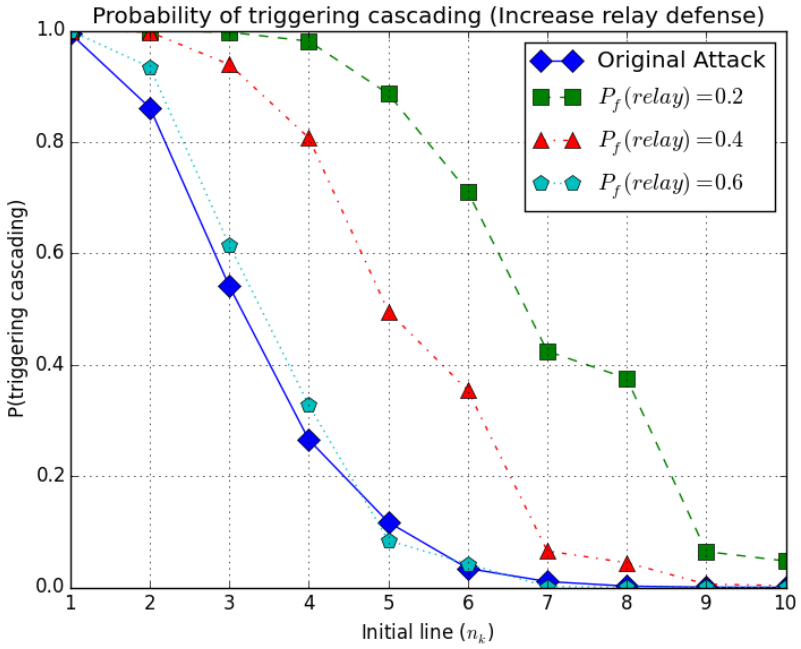
Figure 5.12: Comparison of Cascading-aware Attacks Under Different Attack Resources.

From the evaluation we can see that only increasing the defense strength of critical relays is not sufficient to protect the system due to the potential indirect attacks. A straight forward improvement is to increase the defense strength of the directly connected routers and the neighbor relays, so that indirect attacks will not be as easy as in the previous examples. The network and attack parameters are same as in Fig. 5.11. We first increase the defense of routers by 100% and 200%. The results are shown in Fig. 5.13a. As the size of initial line set becomes larger, the defense is significantly improved (e.g., can be more than 500 times better than low defense). Fig. 5.13b shows the results of increasing neighbor relay defense, which also dramatically decrease the cascading probability. For certain amount of attack resources there is limited improvement when n_k is relatively small because the attacker can still assign sufficient resources to trip the lines; when there are more initial lines, the resources for neighbor devices of each target relay will become less, thus increasing the difficulty of cascading attack. Fig. 5.13c shows the results of increasing both routers' and relays' defense. The effect is better than purely enhancing routers or

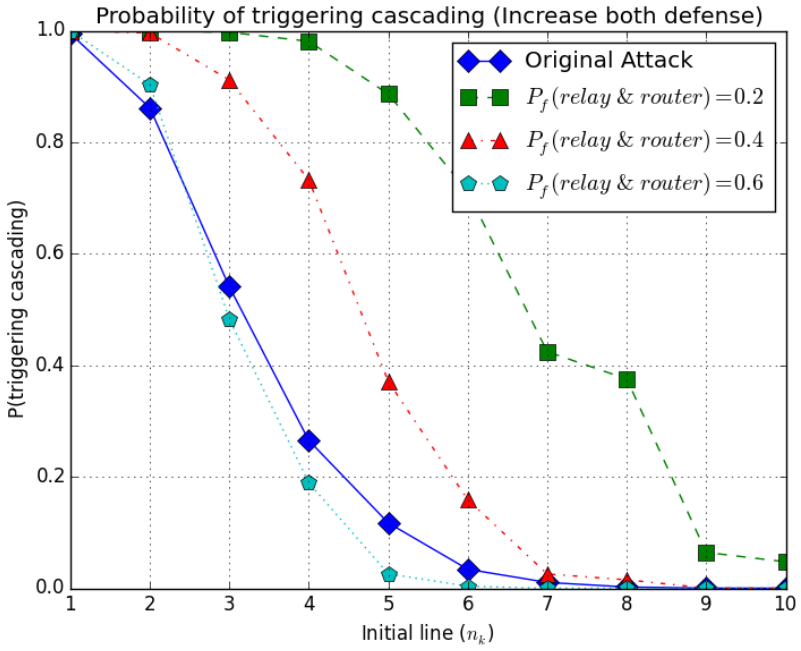
relays, that the probability of cascading failures under agent-reputation-based attacks can decrease even faster than direct attacks.



(a) Improve Defense Strength of Routers



(b) Improve Defense Strength of Relays



(c) Improve Defense Strength of Both Routers and Relays

Figure 5.13: Improve Defense Strength of Network Devices.

In addition, we observe two issues that are also important to mitigate potential cascading damages. The first is to prevent the attacker from knowing or estimating important data, like the current system state, the defense strength, or the potential critical lines. If the attacker manages to learn the information, then the system can only rely on its defense strength to prevent cascading failures. If the attacker happened to "guess" the critical lines, but does not have knowledge about the detailed defense strength, then it will be another problem for him to determine how to select attack method. For different defense parameters, an attack method may be not always superior than another, and at some situations it may perform worse. If the attacker does not select the proper attack method, on one hand he may not conduct the attack successfully, on the other hand, the abnormal conditions may be noticed after certain amount of time. Second, the system should avoid running at heavy load, because the number of initial lines can be small at heavy load. The attacker can use his limited attack resources on the initial lines (if obtaining critical information). A

device may have relatively high defense strength, however, with more resources targeting the device, the attacker can still increase his chance to trigger a cascading failure.

The key component of the agent-reputation-based cascading attack is that the attacker can indirectly trip a critical line from its neighbor relays. In that situation, a critical relay is seen as a backup relay for another line. We argue that protection system should restrict/disable sending of trip requests to the critical relays at the current system state (e.g., lines belonging to $\{n_k\}$), especially when the system load is heavy. As the system is approaching a risky condition, triggering cascading failures will be relatively easier than in the light load situation, and the extra cascading damages can also be enormous, which may result in unstable system state. The goal of trip requests from primary relays is to speed up the react of Zone 3 relays (e.g., to isolate faults faster) when primary relays do not work, or inform Zone 3 relays to trip if they do not behave correctly. When primary relays do not work, if there is a real fault in the primary line, the backup relays should be able to detect the fault, and send queries to its neighbors. If a backup relay does not respond to a remote fault, it means both the primary relay and backup relay encounter faults. This probability can be much smaller than the successful attack probability of malicious attacks.

If a primary relay cannot issue trip requests to its backup relays, then the trip of a critical line $line_i$ will have two cases: (1) the primary relays of $line_i$ are compromised, and (2) the primary relays of $line_i$ are experiencing device malfunctions (e.g., hidden failures). As we have introduced, the agent-based protection is designed to deal with the hidden failure problem. In order for a critical relay to trip, it should receive at least one confirmation from its neighbors. Depending on different protection schemes, we need different numbers of replies. For example, the basic agent-based protection scheme requires one trusted reply, while more strict schemes may require trusted replies from a majority number of neighbors. If an attacker successfully compromises certain neighbor relays, then he can send false confirmations. Denote the probability of hidden failure exposed in a relay as P_{HF}, assume the basic agent-based protection scheme is used as this is the best condition for an attacker,

then the probability of triggering cascading failures can be computed as:

$$P(triggering\ cascaidng) = \left(1 - (1 - P_{HF})^2\right)^{n_k} \cdot \left(1 - P_f^K\right)^{n_k} \tag{5.10}$$

Due to the improved reliability of devices, the failure of a device itself is relatively low (e.g., 10^{-5}), while the probability of exposed hidden failures can be much higher (e.g., 10^{-3}) [95]. We compute the probability of triggering a cascading failure due to false confirmations, and compare with the agent-reputation-based cascading-aware attack. We assume routers and relays have relatively high defense strength (e.g., 0.8), and the number of lines in the initial cascading line set is set to different values in the test. The results are shown in Table. 5.2. We observe that, without primary trip requests, the probability of triggering cascading failures due to hidden failures is much smaller than the results due to deliberate cyber attacks. Thus it is reasonable to consider disabling trip requests to critical relays.

Table 5.2: Comparison of Triggering Cascading without/with Primary Trip Requests.

	$n_k = 1$	$n_k = 2$	$n_k = 3$	$n_k = 4$	$n_k = 5$
Enable request	0.928	0.332	0.028	0.001	2.12×10^{-5}
Disable request	1.99×10^{-3}	3.98×10^{-6}	7.98×10^{-9}	1.59×10^{-11}	3.17×10^{-14}

5.6 Conclusion

In summary, we investigated three potential attack strategies to P2P relay protection schemes. We analyzed and evaluated the effects of random attack, area-based attack, and cascading-aware attack. We also investigated majority confirmation rule in relay protection, and evaluated the effect of area-based attack under majority rule. In addition, we examined agent-reputation-based relay protection. We demonstrated its potential weakness in cascading attacks, and provided several suggestions to mitigate the potential damages.

CHAPTER 6
SYNCHRONIZED ROUTING FRAMEWORK FOR PREDICTABLE REAL-TIME DELIVERY

As the electric power grid uses control and protection schemes to prevent the system from reaching extreme conditions which cause instability or system collapse, the situational awareness of system state is critical, which depends on the fast and accurate delivery of measurements and control decisions. In smart grid, many monitoring and control applications will be deployed across widely geographically separated areas. However, current over-provision based QoS methods cannot effectively provide performance assurance across large areas, and in resource-limited environments like wireless networks, the over-provision is expensive and hard to ensure. Based on these observations, we propose to explore the high accuracy time synchronization available in smart grid. The high resolution and expected wide deployment of these technologies provide us an opportunity to build a communication architecture that is scalable, adaptive, and cost-effective in the smart grid. In this chapter, we exploit the synchronized time as a global reference to help achieve the cooperation among routers, and propose a framework to fulfill the requirement of real-time delivery. We also propose a synchronized multihop scheduling (SMS) to dynamically adjust the service priority of packets arriving at a router [13].

6.1 Background

The large blackouts happened in the traditional power grid lead to the emphasis of higher precision monitoring and control for smart grid. In addition, efficiency is also an important factor to be considered. Adding redundancy and providing enough margin for the power system load enhance the reliability. On the other hand, operating the grid at lower levels than its limits, introduces inefficiency because the transmission system is not fully used. One critical technology involves sensor data that are timestamped at the microsecond level and then delivered in real-time to give a coherent picture of a system for operators. As a result, in smart grid the promising WAMS system is going to replace the old SCADA

system, which is usually deployed in the most critical substations.

To meet these challenges, the communication network of smart grid should be able to provide the required QoS to different types of real-time data. The application requirements vary in SG, and among the most critical ones are measurement and protection data, which usually have to be delivered in tens of milliseconds. The end-to-end delay of a packet consists of three parts: propagation, transmission, and queueing delay. While propagation and transmission delays are usually static and have limited impacts, many researches focus on reducing queueing delays for different classes of traffic through scheduling.

Packet scheduling has been extensively investigated and many ideas have been proposed in the past. First-in-first-out (FIFO) with over-provision does not work well for real-time traffic with strict requirements, especially when across large areas. Per-hop scheduling schemes such as Weighted Fair Queuing (WFQ) [66, 67], Earliest Deadline First (EDF) [68, 69], are not scalable and is difficult to deploy across multiple domains. Core-Jitter Virtual Clock (CJVC) [9] addresses the scalability issue in a domain by eliminating per-flow states at core routers, but it is still difficult to deploy over multiple domains.

Collaborative scheduling schemes such as FIFO+ [70] and CEDF [71], and CMS [72, 73] look into multi-hop scheduling to further exploit sharing among multiple routers. However, they mostly utilize upstream information at a hop, without exploring the dynamics in downstream paths.

6.2 Synchronization Technology

In the characterizing of network performance, one-way delay (OWD) is a straightforward metric for a packet and has received quite a lot of attention. Estimating OWD between the sender and the receiver is fairly easy if the time is synchronized between the sender and the receiver. As a result, the delay can simply be calculated as the difference of the receiver's time-stamp and the sender's time-stamp (stored in the packet header). Currently there are mainly three time synchronization technologies:

- Network Time Protocol (NTP)
- Global Positioning System (GPS)
- IEEE 1588 Protocol (PTP)

NTP is not suitable for real-time traffic due to its relatively low accuracy, e.g., it is estimated that the resolution of NTP on public networks is between 10 and $50ms$. GPS has high accuracy, normally in the order of microseconds. GPS usually requires special equipment such as a receiver and an antenna (compensating the weak signal inside buildings), and may be a little costly than the other two technologies. However, in the smart grid, as a variety of devices and applications requiring high timing precision will be deployed, the overall cost is still acceptable.

The IEEE 1588 was designed to provide accurate timing in distributed systems, for example, enabling precise clock synchronization in measurement and control systems. Today many emerging products supporting this technology are being developed in local networks. The main use of PTP is for a group of relatively stable components, such as local area networks supporting multicast communications (including but not limited to Ethernet). The pure software implementation of PTP on standard components provides precision in the range of 10 to $100\mu s$; while the maximum accuracy in the range of $100ns$ can be achieved with the help of calibrated atomic clocks. For areas where the deployment of GPS is not cost-effective, PTP is a good alternative.

6.3 Proposed Synchronized Architecture

In this section, we first present the proposed synchronized framework, and then analyze its effectiveness for the scheduling scheme. It is extremely challenging to support predictable real-time delivery in a large scale while considering scalability, incremental deployment, cost effectiveness, and adaptivity. We will utilize synchronized time to address the challenge.

Motivation. One main challenge in providing real-time delivery on the current Internet is that we do not have effective cooperative mechanisms among distributed routers,

especially across domains. In reservation-based solutions, each router on a flow path is assigned with a per-hop delay bound during a flow set-up phase. Such static allocations can be easily achieved in a single domain but lack scalability. Moreover, it limits exploiting resource sharing among routers across paths and domains to further improve performance. While core-stateless approaches emphasize inter-router collaboration in a single domain, the current Internet lacks inter-domain cooperation. One domain cannot enforce its policy on other domains, and service polices at each domain may be frequently changed for their own purposes, e.g., load balancing. Therefore, we need a novel mechanism to ease this inter-domain constraint. The proposed framework focuses on this issue, and provides better delivery predictability by exploiting better resource sharing across routers and domains.

Key Idea. We utilize synchronized time as a global reference to assist inter-router and inter-domain cooperation in a distributedly cooperative fashion. First, each router runs a *downstream-delay estimation mechanism* that finds the expected delay from itself to known real-time destination routers. Second, when a real-time packet arrives at the router, a *path-aware collaborative service mechanism* determines the *urgency* of the packet, based on its upstream elapsed delay, its estimated downstream delay, and its delay requirement. The urgency is then used by the router to determine the service priority of a packet. When every router forwards the packet in this way, it will arrive at its destination on time with a high probability, given that the path is not congested with real-time traffic. We can ensure this condition with a simple admission control as discussed in the following.

Basic Assumptions. We first consider a single domain deployment. Our basic assumptions are: (a) Routers collaborate with each other to estimate delays to real-time destinations. (b) A simple admission control is performed at a source router. With a delay estimation mechanism, a source router knows the expected delay to a destination router, D^m. When a source starts a flow to the destination router with a delay requirement smaller than D^m, it will be rejected. (c) No per-flow bandwidth reservation is required on routers. (Static or dynamic per-class reservations can be used for important flows if necessary.) (d) We do not consider selfish routers, which is out of the scope of this paper. (e) For easy

illustration, we divide traffic into two classes at a router: *real-time* and *non-real-time*. We always give real-time traffic higher priority. Note that the estimated delays are only for real-time traffic. (f) Assume that a path from a real-time source to its destination is not heavily congested, e.g., the Internet2 infrastructure is seldom congested. We will investigate intelligent adaptation schemes to ensure this condition. In the meantime, the proposed framework is expected to deal with short-term congestions. The proposed routing scheme can also take advantage of multiple paths for the same flow.

Basic Mechanisms. Since we do not reserve resource for a flow at a router, the question for a router is how to determine the expected service delay at this hop for a packet. We utilize the synchronized time to assist the router: the router first estimates its urgency, and then determines its local target service priority based on the urgency. Two key mechanisms support these operations:

(i) *Downstream-delay estimation mechanism* in a single domain and across multiple domains. We present and discuss the ideas for this mechanism as follows. First, in a single domain, routers exchange measurements with neighbors, either via proactively probing or passively piggybacking. Based on the exchanges, a router builds a complete delay graph of the domain, and then derives a *delay estimation table* that includes various delay metrics to a destination router, e.g., the minimum delay, the average delay and variance. Table 6.1 shows an example of the delay table at router R0, which is used by the collaborative scheduling mechanism to conduct predictable forwarding. We focus on the delays between routers, and assume the first/last hop delay between a host and its router is small and negligible.

Second, for across multiple domains, probing individually is impractical. We will design a *distributed measurement framework* motivated by the research on Internet delay properties. It shows that the delays between domains are multi-level clusters. We will further explore the similar idea as the Internet Atlas [96] to develop a structural delay measurement framework to utilize the known common Internet properties. Assume we have a set of vantage points that constantly generate light measurement traffic among themselves, in order to cover common path segments in the Internet core. These segments are usually shared

on the paths between many sources and destinations. For each domain, it will first locate itself on the Atlas and then utilizes the common measurements on the Atlas to estimate delays to destination domains.

For a real-time flow whose initial path shown in Fig. 6.1, the measured average delay at hop i is d_i with a variance v_i, and the measured minimum delay is d_i^m. In Table. 6.1, we then have the minimum expected delay to destination k as $D_i^m = \sum d_j^m, i \leq j \leq k$; the estimated delay to destination k as $D_i = F(d_i, v_i, \ldots, d_k, v_k)$, and the variance of estimated delay to destination k as $V_i = F_v(d_i, v_i, \ldots, d_k, v_k)$, where $F()$ and $F_v()$ are the functions of downstream delays, loads, and their variances. Also shown in Fig. 6.1, when multiple paths exist for a flow, the proposed scheme can select a proper path based on the expected performance of downstream paths.

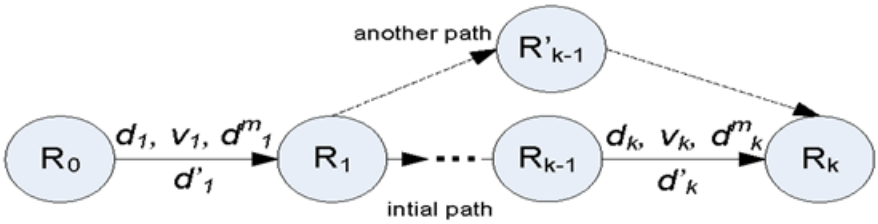


Figure 6.1: Paths from R_0 to R_k.

Table 6.1: Delay Estimation Table at Router R_0.

R_0	Minimum Delay	Average delay	Delay Variance	$\cdots$
R_1	D_1^m	D_1	V_1	$\cdots$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
R_k	D_k^m	D_k	V_k	$\cdots$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$

(ii) A *path-aware collaborative service mechanism* at a router forwards a packet with regard to its end-to-end (e2e) requirement. We summarize the notations in Table. 6.2. Assume that a packet k from flow i, denoted as p_i^k, of a real-time flow carries its birth-time t_0, its end-to-end delay requirement D_0, and its predictability requirement P_0, which means

Table 6.2: Notations Used for Performance Analysis.

Term	Definition
p_i^k	Packet k from flow i
$d_u(p_i^k)$	Upstream delay of p_i^k
$t_{ar}(p_i^k)$	Arrival time of p_i^k at a hop
$t_0(p_i^k)$	The birth time of p_i^k by the source
$d_d(p_i^k)$	Estimated doweam delay of p_i^k
$d_t(p_i^k)$	Target delay of p_i^k at time t
$S(t, p_i^k)$	Slack time of p_i^k at time t
$Q(t, p_i^k)$	Expected queueing delay of p_i^k at time t
P_0	Delay violation requirement

the probability that the packet arrives at its destination with a delay longer than D_0 will be at most P_0 or lower.

When packet p_i^k arrives at router i, its *upstream elapsed delay* up to the router is $d_u(p_i^k) = t_{ar}(p_i^k) - t_0(p_i^k)$, where $t_{ar}(p_i^k)$ is the packet arrival time and $t_0(p_i^k)$ is its birth time t_0. It is easily obtained due to the synchronized time.

At the time of arrival, the *estimated downstream delay* from the current hop to the destination of the packet, denoted as $d_d(t_{ar}, p_i^k)$, is given, e.g., from the delay table. We can then figure out the *target delay* of the packet at time t as $d_t(t, p_i^k) = D_0 - (t - t_0(p_i^k)) - d_d(t, p_i^k)$, which is the maximum delay that the packet is expected to spend at this hop. Here, t can be any time instant while this packet is still at this hop. Based on this target delay, the router's current load, and the resource competition from other real time packets at the router, the packet is given a priority to maximize its probability to reach its destination on time. It is then inserted in a service queue sorted by priority.

Note that once a packet is inserted into the service queue, the router will not reschedule it. Normally, we want to ensure the actual service delay of a packet is smaller than its target time. When each router on the path forwards the packet strictly in this way, it will likely arrive at the destination on time within the given delay requirement.

However, due to resource competition of other real-time packets, the router may not be able to meet the requirement of packet p_i^k, because we do not reserve resource for a flow. A more urgent packet q can be inserted ahead of p_i^k. Then its expected service delay is increased. With a certain probability $P\big(d_t(t, p_i^k) \leq d'(p_i^k)\big)$, we may have the actual delay $d'(p_i^k)$ exceeds its target delay $d_t(t, p_i^k)$. In this case, downstream routers of p_i^k automatically increase its urgency and help it catch up. When these routers have sufficient resource, p_i^k will still reach its destination on time; otherwise, it will be late. To find packets that can cede their resource to a late packet, we define the *slack time* of a packet at time t to represent the maximum extra delay that the packet can spend at a hop, $S(t, p_i^k) = d_t(t, p_i^k) - Q(t, p_i^k)$, where $Q(t, p_i^k)$ is the expected queueing delay of packet p_i^k due to other packets.

Three Basic Scheduling Schemes. To implement the proposed path-ware scheduling idea, we first introduce a scheduling method (**M1**) which simply uses the target delay of a packet $d_t(t, p_i^k)$ as its path-aware priority and serve packets in the increasing order of their target times. We first discuss this method and then define two improvement methods (**M2** and **M3**).

In **M1**, the scheduling process is as follows. When packet p_i^k arrives at a router, we need to decide where to insert it in the routing queue. First, we compute its target time as $t + d_t(t, p_i^k)$, and then compare its target time with packets in the queue to find where to insert. The conditions for packet p_i^k to be inserted before packet p_j^m are $d_t(t, p_i^k) < d_t(t, p_j^m)$ and $S(t, p_j^m) > L/C$, where L is the packet size and C is the link capacity. For ease of discussion, we assume all packets have the same size. The first condition means p_i^k has a smaller target time than p_j^m; the second condition ensures that the service of p_j^m is not damaged if we insert p_i^k in front of p_j^m. If both conditions are met, we consume L/C unit of capacity provided by p_j^m. Furthermore, we continue to compare p_i^k with other packets until we find packet p_l^n of another flow n, $d_t(t, p_i^k) > d_t(t, p_l^n)$ or $S(p_l^n) < L/C$. We then insert p_i^k after p_l^n.

The reason that we use a combination of target time and slack time to determine if a packet can be inserted ahead of another is as follows. After packet p_i^k is enqueued, other

packets with higher priority may be inserted in front of it. In this case, we consider p_i^k as a *catch-up capacity provider* to other packets. However, we need to carefully examine how many packets can use this capacity, because p_i^k might not fulfill its own requirement if there are many such packets.

Now we improve the above method based on known downstream patterns, e.g., the observed delay distribution. Assume the downstream path delay for p_i^k has a normal distribution with parameters (μ, σ), where μ and σ are the mean and standard deviation value of the downstream delay. In **M1**, once a packet p_i^k cannot be moved forward in the queue because of $S(p_l^n) < L/C$, we have $S(t, p_(i, k)) = d_t(t, p_i^k) - Q(t, p_i^k) < 0$, where $Q(t, p_i^k)$ is its queueing delay. This means $D_0 - (t - t_s(p_i^k)) - Q(t, p_i^k) < d_d(t, p_i^k)$, i.e., this packet is expected not to be delivered within its requirement. However, it may still have a chance to arrive on time if it is sped up in its downstream.

To figure out this chance, we define the available time for the packet to traverse the downstream path as $d_A = D_0 - (t - t_0(p_i^k)) - Q(t, p_i^k)$. If we can ensure that at each downstream hop $P(d_D > d_A) \leq P_0$, where P_0 is the packet's violation probability requirement, the path requirement can still be ensured. Since we have the delay distribution to each destination path, we can check whether the above condition is satisfied. If it is, we do nothing at the current hop; if not, we further adjust of the packet's priority and move it ahead other packets in the queue. We name this second method **M2**.

To determine the benefit of such adjustment, we carefully examine whether the overall gain is increased or not, because such adjustment means that another packet is slow down. For two packets p_i^k and p_j^m, when

$$\int_{d_A^i}^{d_A^i + L/C} f_i(t)dt > \int_{d_A^j - L/C}^{d_A^j} f_j(t)dt$$

where $f_i(t)$ and $f_j(t)$ are the measured delay distribution of flow i and flow j to the destination from the current hop, moving p_i^k ahead p_j^m will increase the overall system gain.

We also consider another improvement method over **M2**, named **M3**. In **M2**, we use

the long-term downstream distribution. By applying such distribution, we assume that the downstream delay at the next measurement cycle could be any value satisfying the distribution (μ, σ). However, as the measurement cycle is relative small, the delay change is more closely related to the current measurement (μ', σ'), i.e., the delay seldom has a large change in a small cycle. The probability that the next delay is near the current measurement is higher than a measurement far away. Therefore, we use a local distribution to characterize the delay changes in a small scale. Here we use a simple autoregressive model of $AR(1)$ to represent the delay evolution.

In the *Gaussian first-order autoregressive process*, or $AR(1)$ process, the current value is based on the immediately preceding value. It can be written as:

$$z_t = (1 - \varphi)\theta + \varphi z_{t-1} + \sigma\varepsilon_t$$

where φ, θ, and σ are fixed scalars, and ε is the standard normal variable. With $|\varphi| < 1$, AR(1) has the conditional distribution of $z_t \sim N((1-\varphi)\theta+\varphi z_{t-1}, \sigma^2)$, and the unconditional distribution of $z_t \sim N(\theta, \frac{\sigma^2}{1-\varphi^2})$

The assumption in **M3** is that the next measured value $d_d(t+1)$ has a higher probability to be close to the current $d_d(t)$, in which $d_d(t+1) = (1-a) \cdot b + a \cdot d_d(t) + \Delta$, where $\Delta \sim N(0, \sigma)$, which means the change between the current and the next value is normally distributed; a is an index between $(0, 1)$ showing the dependency of the current and the next value, and b is a fixed scalar. Then we have, conditional mean $E[d_d(t+1)|d_d(t)] = (1-a) \cdot b + a \cdot d_d(t)$, conditional standard deviation $Std[d_d(t+1)|d_d(t)] = \sigma$. That is, $[d_d(t+1)|d_d(t)] \sim N((1-a) \cdot b + a \cdot d_d(t), \sigma)$. When we properly select a, b, and σ, we can decide the local distribution of delay.

6.4 Performance Evaluation

In this section, we first identify the advantage of the proposed schemes using numerical evaluation, and then compare them with existing methods via simulation.

6.4.1 Numerical Comparison of SMS and CMS

We show the advantage of SMS in a simplified numerical comparison, assume ideal situation. We target a single flow i at a single router in the evaluation. We assume that packets of flow i will arrive at the first hop router in a domain, which enables SMS or CMS. The flow has path requirement as $D_0 = 60ms$. We assume the flow already has certain upstream delay, with delay value d_U to be $20ms$ at 80% of time, and the remaining 20% period has a value with a uniform distribution of $[30, 40)ms$. Assume the service time of a packet at the router is $L/C = 4ms$. The total path delay of a packet is $d_U + d_D + d_R$ where d_R is the total delay of the packet at the router. Flow i still has two hops to the destination. We let both CMS and SMS perform adjustment as they can at a hop (e.g., to decrease the packet delay at the router) within their adjustment range ($min(d_R) = 4ms$). We measure their cost to show the overhead they may introduce (e.g., how much time is compensated to speed up packets from flow i). We assume there is another reference flow k at the router. This flow starts at this router, its delay requirement is 60ms, and it has three hops to destination. We assume flow k is "ideal" that it has unlimited ability to "help" the other flows at the router; in addition, it has a downstream delay of exactly 40ms. For the CMS, the adjustment index η is between 40% to 80% of δ to test different adjustment ranges. Notice that at the first hop the packet priority under CMS will be within a range of $[\delta - \eta,\ \delta + \eta]$, while SMS does not have a range limit for the priority. Assume $d_R(i)$ has a relationship to the constant waiting time of the reference flow k ($T_w(k)$) as $\frac{priority(i)}{priority(k)} = \frac{d_R(i)}{T_w(k)}$. Under SMS and CMS, different methods will be used to compute the flow priority.

SMS can better utilize downstream available resource. In the test, we set flow i downstream delay $d_D = 18ms$ for 20% of time so it may compensate some upstream delay variances. We make the period of time when downstream delay drops to overlap with the period when upstream delay increases, as in Fig. 6.2. The percentage of overlapped area, x%, varies from 0 to 100% as shown in Fig. 6.3e. For SMS, within the area of upstream variance and downstream variance overlap, the violation probability of the flow i is $P(d_U > 38ms) = 0.2$; beyond that area, the violation probability is $P(d_U > 36ms) = 0.4$. Thus under SMS, the

total violation probability for an overlap of $x\%$ is $P(v) = 0.2 \cdot x \cdot 0.4 + 0.2 \cdot (1-x) \cdot 0.2$. Although both violation probabilities of SMS and CMS drop as downstream delay decreases, SMS has a much smaller violation probability than CMS.

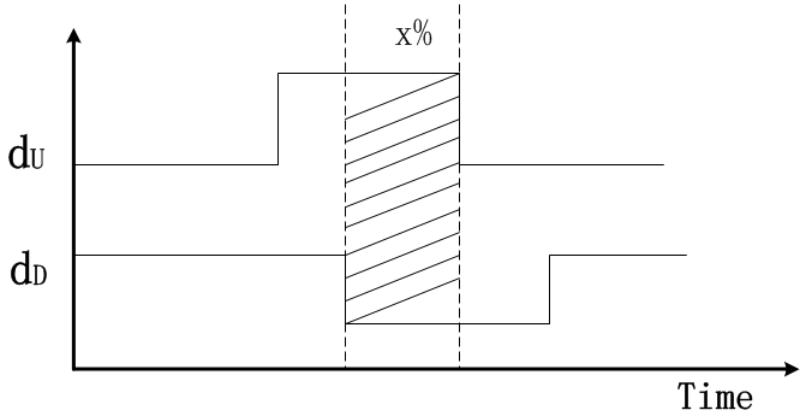
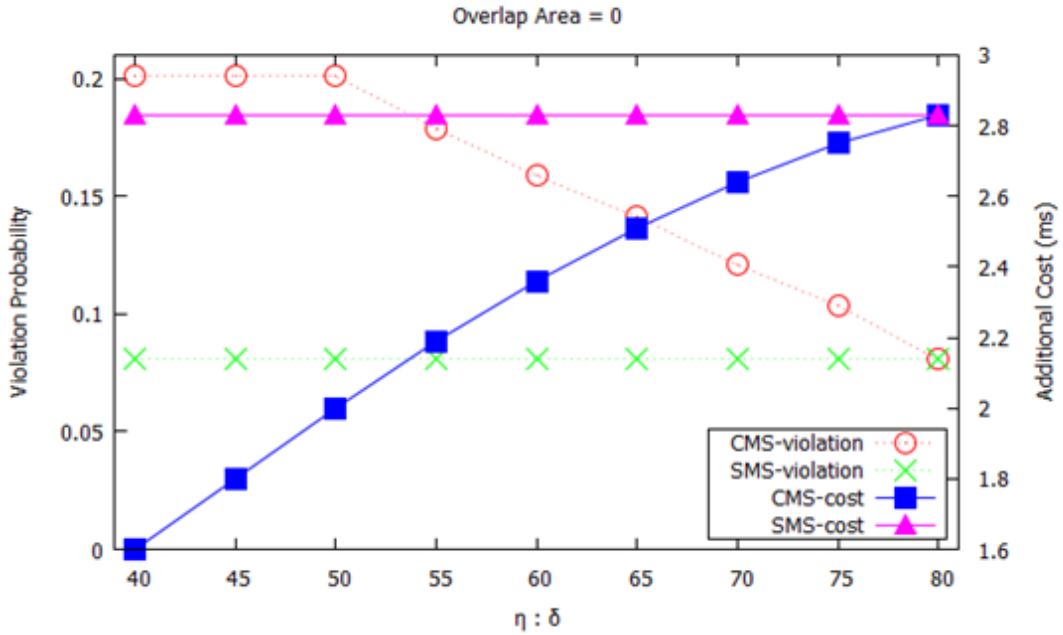
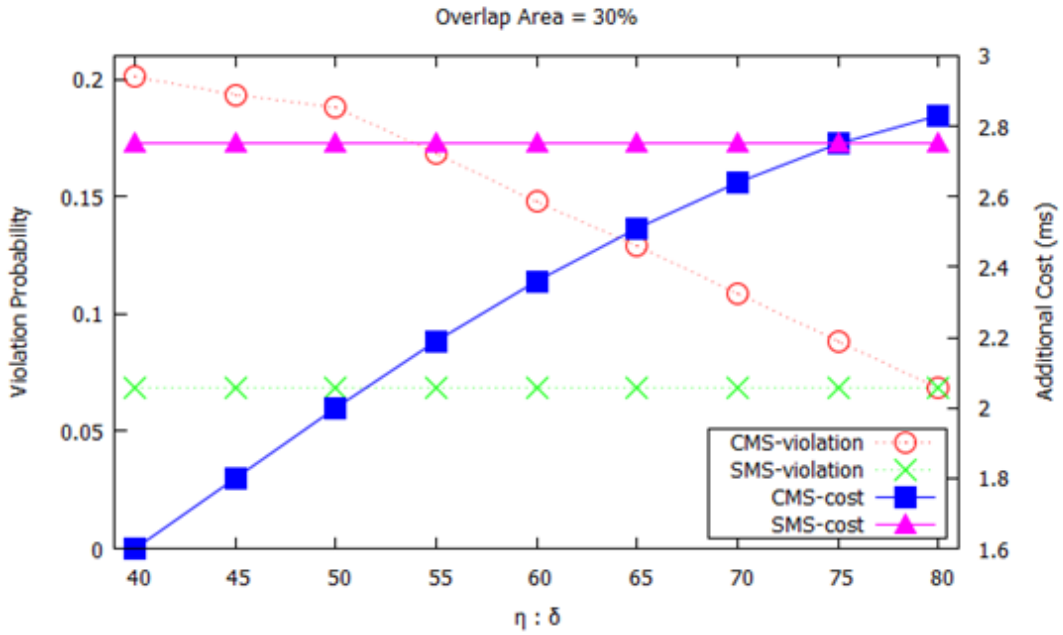


Figure 6.2: Downstream and Upstream Delay Overlap Area.

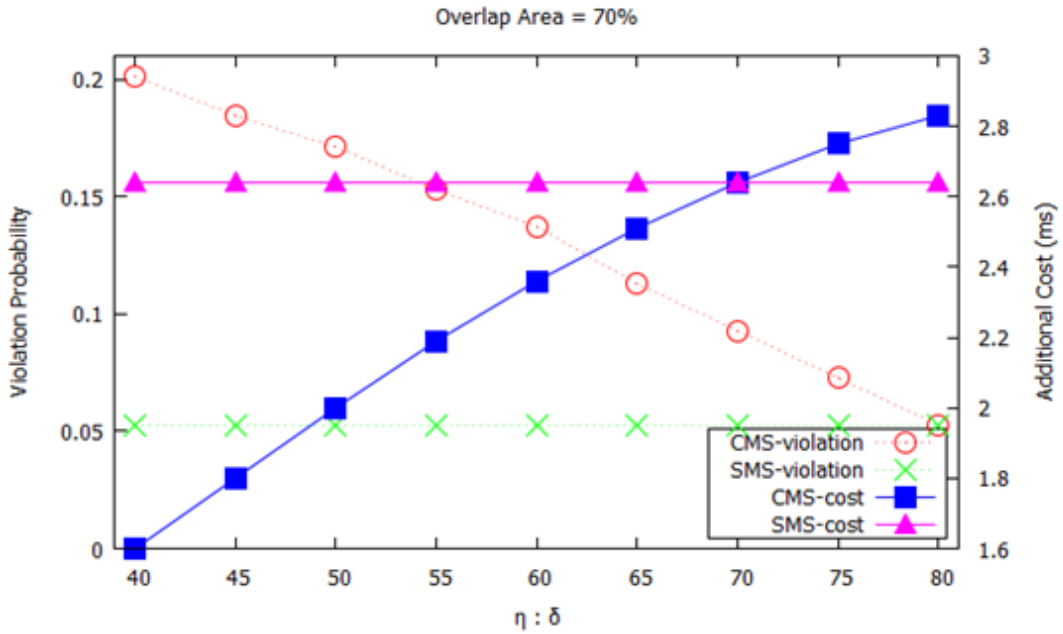
Another observation from Fig. 6.3e is that, under SMS, the average cost of a packet decreases as the overlap area broadens. The reason is that with compensation by the downstream, some packets do not need to be scheduled so aggressively at their current hop and they can still fulfill the requirement. As we can see from Fig 6.3a to Fig. 6.3d, if the adjustment index η_i gets larger, the performance of CMS also becomes better and may reach the same level of SMS. However, for all ranges of overlap area, the cost of CMS does not change; and in order to reach the same violation ratio as SMS, CMS needs to pay more additional cost. In addition, with the increase of the overlap area, this cost difference between CMS and SMS also becomes larger. The reason is that CMS does not consider the information of downstream path. If upstream becomes a little congested, and downstream is not that busy, flows under CMS will have a higher service priority. For example, with some delay drops at downstream, CMS will still aggressively serve the packets at their current hop; while for SMS, for example, if the upstream delay increases by $5ms$ and downstream delay drops $2ms$, then we only need to compensate the remaining $3ms$.



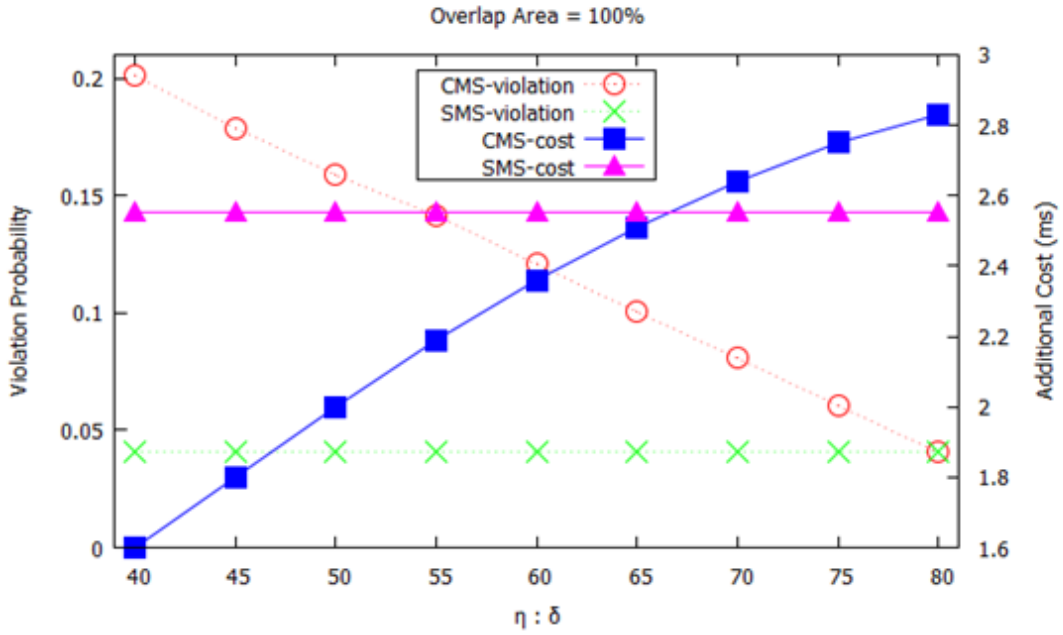
(a) Overlap Area = 0



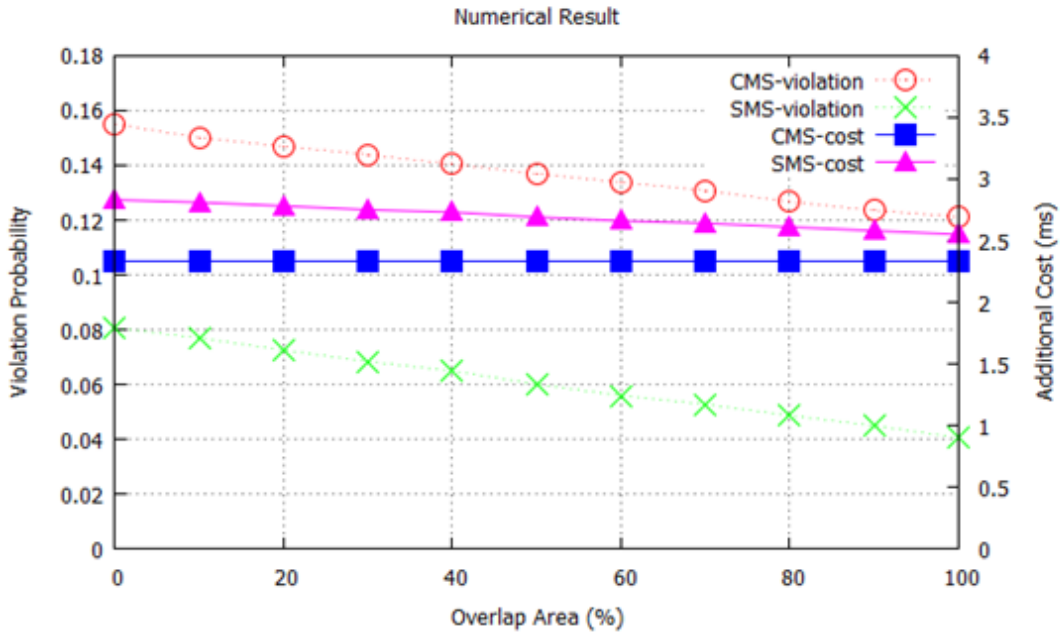
(b) Overlap Area = 30%



(c) Overlap Area = 70%



(d) Overlap Area = 100%



(e) Overall Evaluation

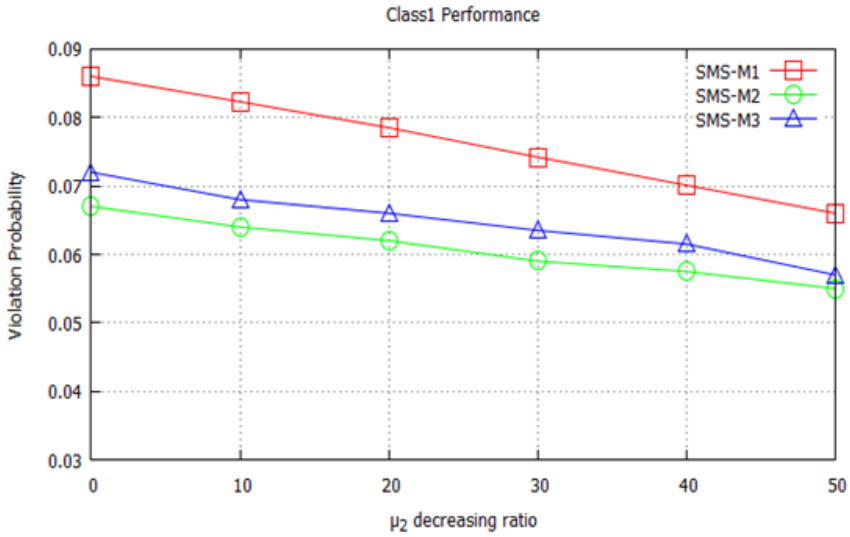
Figure 6.3: Comparison of SMS and CMS.

6.4.2 Simulation Evaluation of Three SMS Schemes

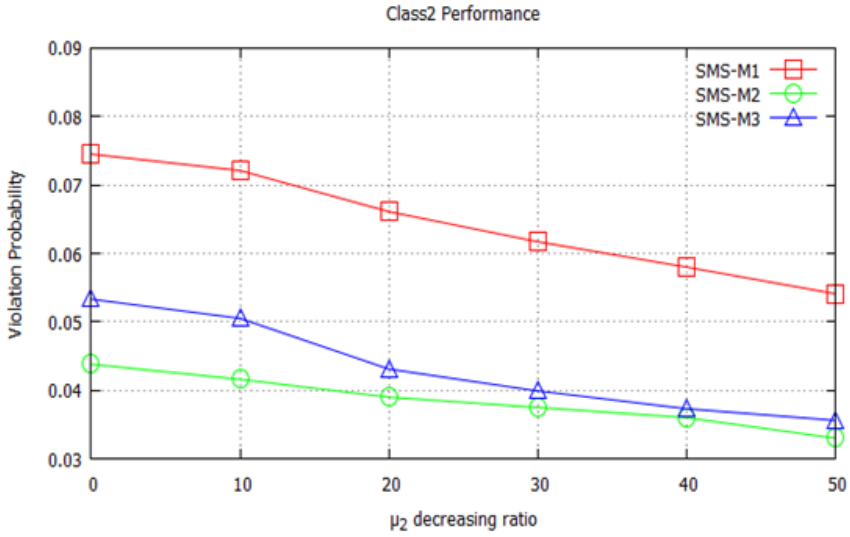
We also examine the performance of SMS under different settings using simulations. To illustrate the basic performance, we focus on scheduling on a single hop, assume we have the downstream delay as a normal distribution (μ, σ). Moreover, we generate the downstream delay following the $AR(1)$ model described in the previous section, such that the delays seen by two adjacent packets are correlated and change in a normally distributed manner. For simplicity, we first examine the effect of downstream delay and set upstream delay to be constant, 0. Assume there are two classes of flows: class1 and class2; each class contains 4 flows and all with a path requirement $D_0 = 80ms$. First we examines the effect of the difference between two downstream paths. We set $\mu_1 = 40ms$, $\mu_2 = 30ms$, $\sigma_1 = \sigma_2 = 12ms$. The flows are generated as exponential on-off sources with a peak rate $r_b = 0.2Mbps$ in an on-period, and 0 bps in an off-period, and $t_{on} = t_{off} = 120ms$. We decrease μ_2 by 10% each time to see the effect.

We can see from Fig. 6.4a through Fig. 6.4c when the difference between μ_1 and μ_2

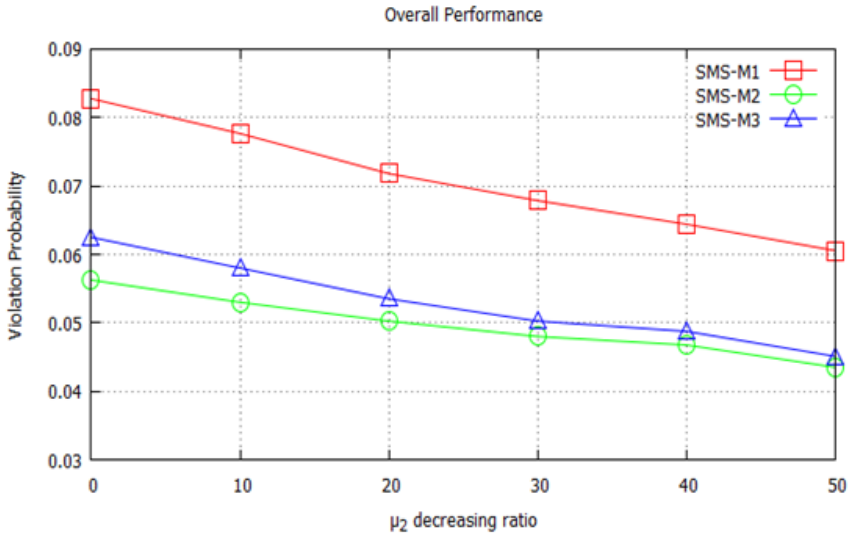
gets larger, all three methods have better performance with less packets violating their requirements, among which, class2 flows have a smaller violation ratio than class1 flows. M2 and M3 are better than M1 due to their additional adjustment of packets according to the known delay distribution. M2 has the lowest violation ratio.



(a) Class-1 Performance Under Different μ_2



(b) Class-2 Performance Under Different μ_2



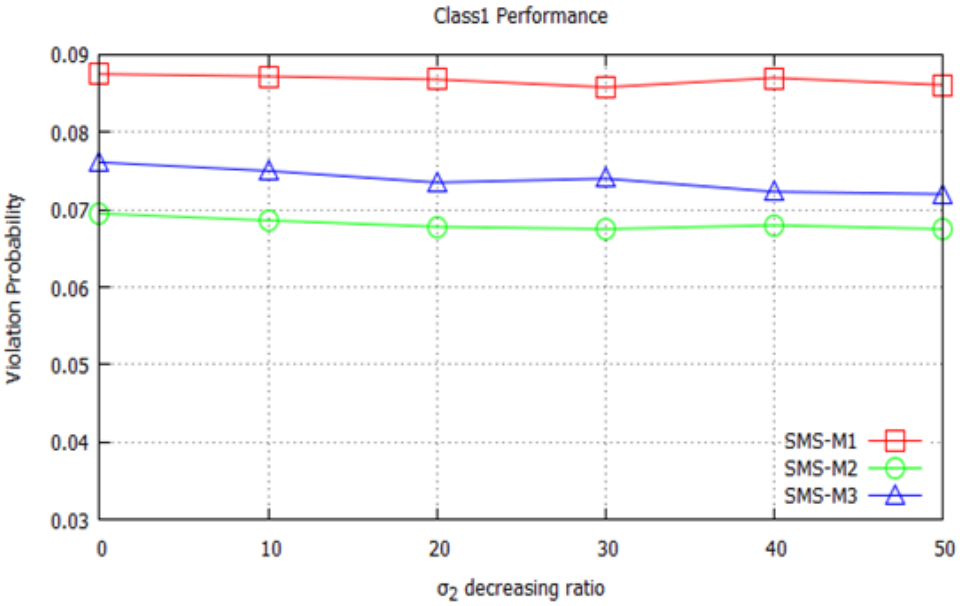
(c) Overall Performance Under Different μ_2

Figure 6.4: Effect of Delay Mean on SMS Performance.

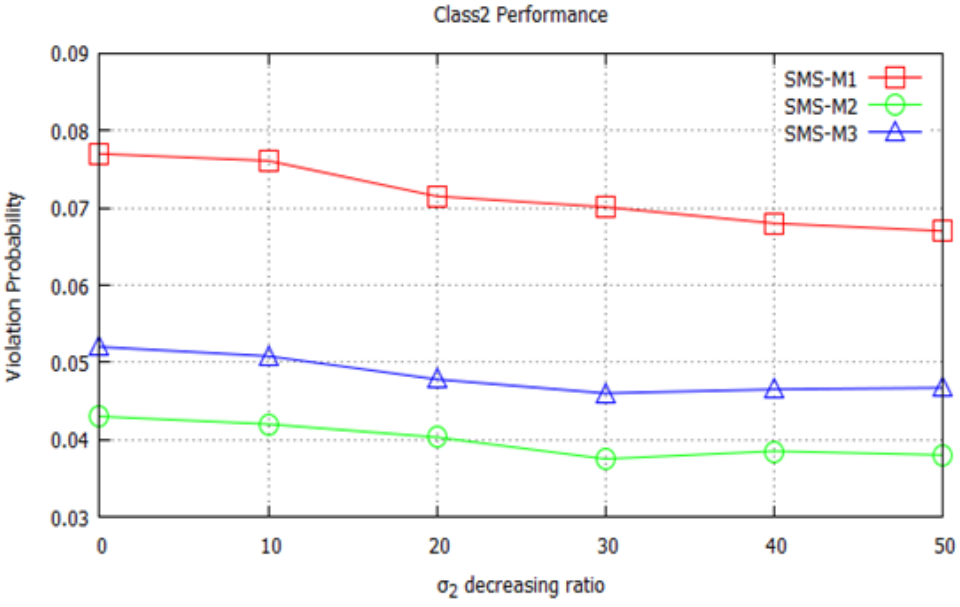
Another parameter of downstream delay is variance. We also test the effect of changing downstream variance and compare the result with the effect of changing mean value. Here we set the parameters as the above case but this time we keep $\mu_1 = 40ms$, $\mu_2 = 30ms$, We decrease σ_2 by 10% each time from the original $12ms$.

As shown from Fig. 6.5a through Fig. 6.5c, when changing the downstream variance, both classes' violation ratios only decrease a little; M2 and M3 still have better performance than M1; M2 also has some advantage over M3. Comparing the above two simulations, we can see that as $\Delta\mu$ becomes larger, it brings two benefits to the traffic: (1) it directly decreases the urgent degree of the target flows, leaving it more opportunities to fulfill the requirements; (2) the decrease of urgent level of class2 traffic also enables it to wait a little more extra time on the hop, thus indirectly contribute some resource to be utilized by others, such as class1 flows here. As a result, all traffic would benefit from this change. On the other hand, the decrease of variance of one path does not improve the performance of class2 traffic by a same factor as the mean. We can see that the performance of class1 changes little, which means class1 hardly benefits from class2's delay variance change. This

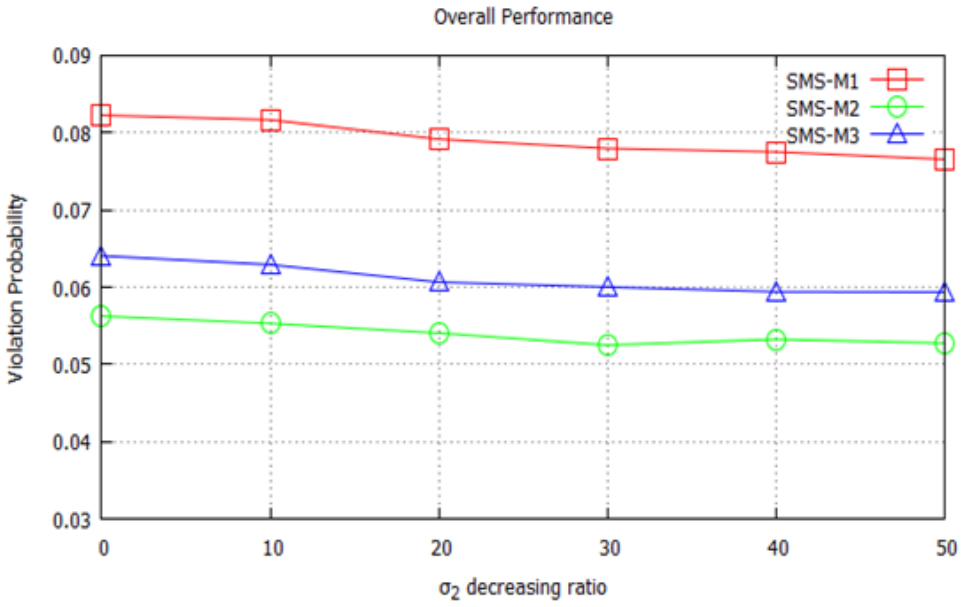
may indicate that we should focus more on the difference of mean value.



(a) Class-1 Performance Under Different σ_2



(b) Class-2 Performance Under Different σ_2



(c) Overall Performance Under Different σ_2

Figure 6.5: Effect of Delay Variance on SMS Performance.

6.4.3 Compare Among Different Scheduling Mechanisms

In this section we compare the performance of different scheduling mechanisms under different settings on a single hop. Particularly we are interested in comparing SMS and CMS because they both focus on coordination. We are interested how SMS can help us.

The simulation environment setting is shown in Fig. 6.6.

To compare with CMS, we assume the simulated hop is the second hop $R2$ as shown in Fig. 6.6. We have two sources S1 and S2 generating traffic. The flow1 and flow2 are competing on $R2$, and the two flows have separated downstream paths from $R3$. We denote them as class1 and class2 traffic, respectively. The flows are generated as exponential on-off sources with a peak rate $r_b = 0.2Mbps$ in an on-period, and 0 bps in an off-period, and $t_{on} = t_{off} = 120ms$. The total requirement is $D_0 = 80$ms. For CMS, let the local deadline to be $\delta_1 = \delta_2 = D_0/4 = 20ms$, the local adjustment to be $\eta_1 = \eta_2 = \delta_1 * 20\%$. Since CMS does not use downstream information, we set both downstream to be $\mu = 0.4 \cdot D_0$, $\sigma = 0.1 \cdot D_0$. For class1 to be adjusted most in CMS, we set the upstream delay of the two

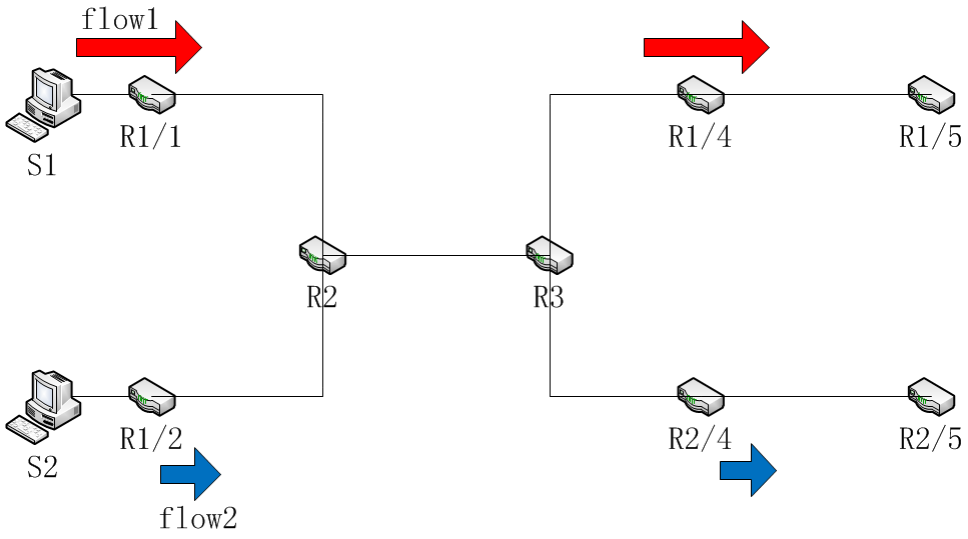


Figure 6.6: Simulation Topology.

classes to be $d_{u,1}(p_1^k) = \delta_1 + \eta_1 = 24ms$ and $d_{u,2}(p_2^k) = \delta_2 - \eta_2 = 16ms$. The average load changes from 60% to 80%. The on and off periods are both $120ms$.

The goal of this setting is to give CMS the opportunity that its largest local adjustment capability can be utilized so that "delayed" packets has the biggest chance to catch up at the local hop under CMS. The test for SMS also follows the same settings as CMS. In other words, this is a case that favors CMS adjustment.

From Fig. 6.7 we can see that at the single hop, when CMS can achieve the largest "help" between two sets of flows, SMS is also able to achieve the similar performance with M1 or a little better (with M2 and M3) for the traffic. This test demonstrates that when CMS is given the "best" condition, at a single hop SMS's performance is still better than CMS. This coincides with our numerical results. In this test case, since the downstream delays of the two classes are the same, we limit the advantage of SMS. If the potential capacity difference between different flows is larger, SMS can achieve even better performance than CMS.

CMS only uses the upstream delay for scheduling and each flow's service priority is dependent on the priority at the previous hop. Thus, at a hop this priority does not have

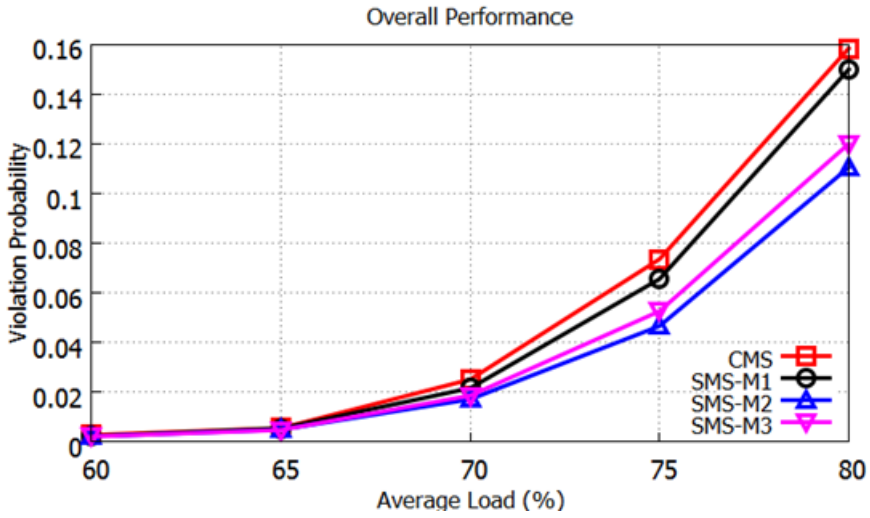


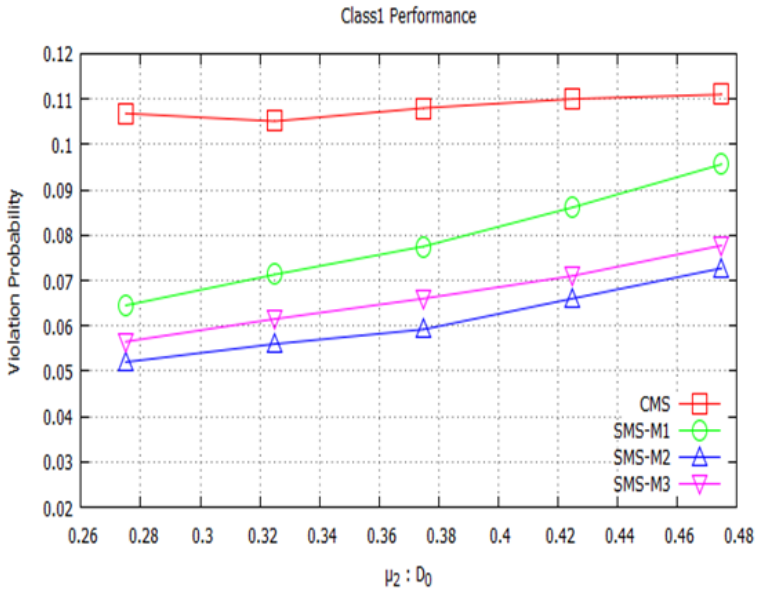
Figure 6.7: Comparison of CMS and SMS when the Setting Favors CMS.

relation to other flows. What if the downstream delay is beyond the original estimation, e.g., with large fluctuation or become large for a certain period? Our next simulation examines such situations.

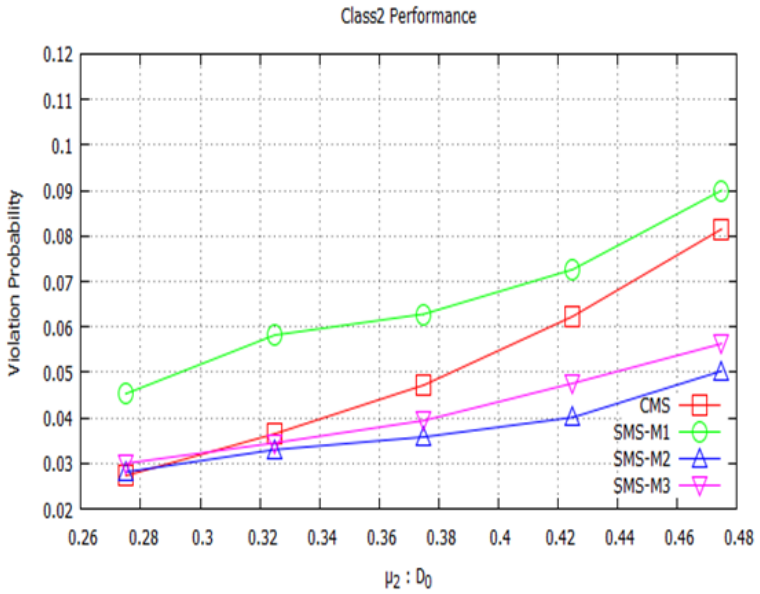
We set the parameters as: upstream delay $d_{u,1} = d_{u,2} = 16ms$, $\mu_1 = 42ms$, μ_2 changes from $22ms$ to $38ms$ and downstream delay variance $\sigma = 8ms$; CMS has the same parameters as the previous case. We also set the requirement $P_0 = 0.1$ for all flows. The flows are generated by exponential on-off sources with peak rate $r_b = 0.1875Mbps$, the average load is 75%. The on and off periods are both $120ms$.

As we can see from Fig. 6.8a to Fig. 6.8c, for CMS, since it does not care the downstream information, both classes would be assigned the same priority at this hop. In fact, at this case, class1 should have been given a higher priority to meet its requirement. As a result, in CMS, more class1 flows experience relatively high delay at the hop and the violation ratio exceeds its requirement; class2 still maintains a good performance since its priority does not change. Compared with CMS, under SMS, class1 has much better performance when using M1, class2s violation ratio increases a little when using M2 and M3. This ratio even decrease due to their additional adjustment (compared with M1). By adjusting the service priority of the two classes, now class2 can wait a little longer time at the hop, letting class1

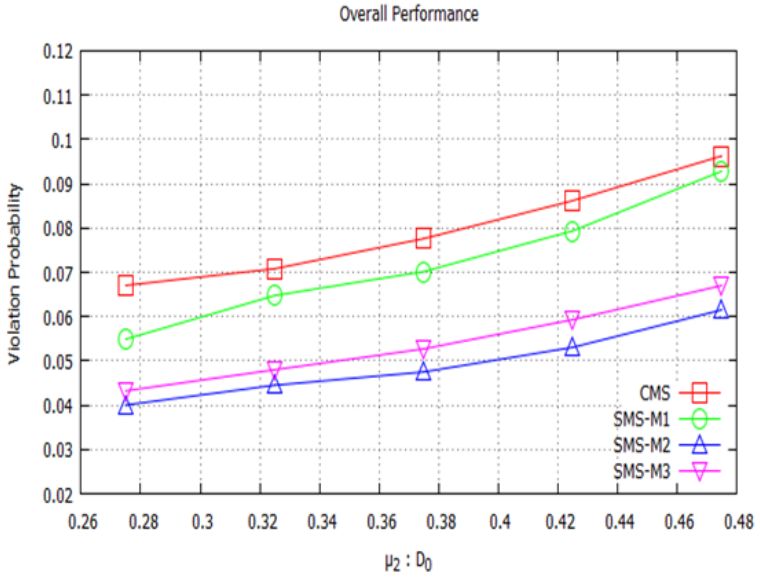
to be served first, thus behaving like a capacity provider. The reason is that by considering both upstream and downstream delays, the router has an overall view of the path condition so that it can make a more accurate decision in resource sharing.



(a) Class-1 Performance Under Different μ_2



(b) Class-2 Performance Under Different μ_2



(c) Overall Performance Under Different μ_2

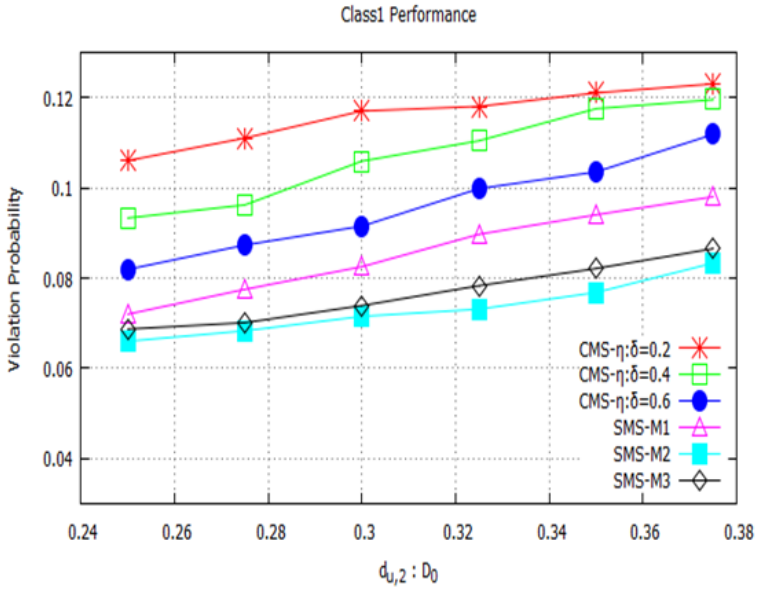
Figure 6.8: Comparison of SMS and CMS Under Different Downstream Delays.

Besides the benefit in using downstream delay, SMS also enables potential larger adjustment range than CMS. Recall that CMS has a local adjustment term η and this term determines the adjustment ability at a hop. We now show the simulated result that if the upstream delay is beyond the adjustment scope.

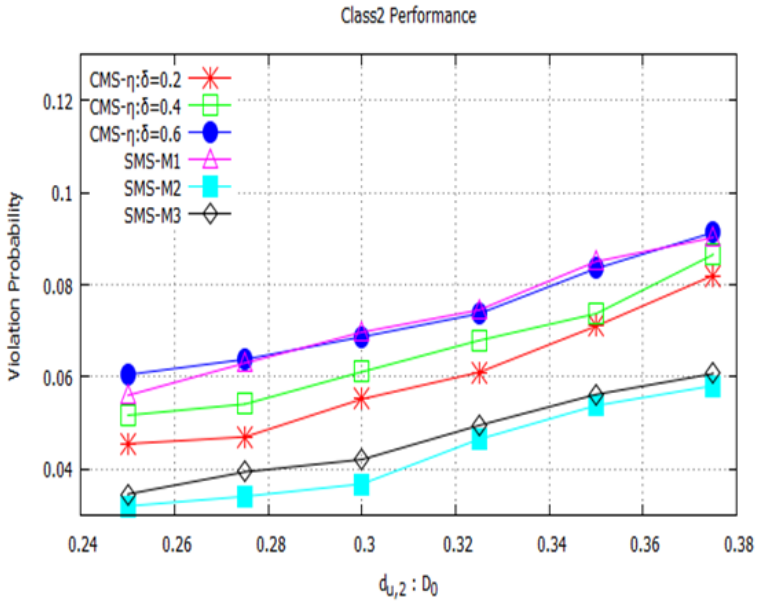
We set the parameters as following: for CMS, local priority increment $\delta_1 = \delta_2 = 20ms$, the local adjustment term $\eta_1 = \eta_2$; the values of η change from $0.2 \cdot \delta_1$ to $0.6 \cdot \delta_1$; for upstream delay $d_{u,1} = 36ms$, $d_{u,2}$ changes from $20ms$ to $30ms$; for downstream delay, mean value $\mu_1 = 26ms$, $\mu_2 = 26ms$, variance $\sigma = 4ms$. The traffic load is 75% as the previous case and the requirement is still $P_0 = 0.1$. We use the identical downstream delay to compare CMS with SMS without taking advantage of downstream information.

When upstream delay is beyond the adjustment capability of the hop, class1 flows cannot get enough service priority (Fig. 6.9a) under CMS to fulfill its requirement. Although class2 flows have good performance under CMS (Fig. 6.9b), this does not help improve the performance of class1 due to the limitation in the assignment of service priority for CMS. As shown in the figures, if we increase the value of η, the adjustment item for CMS,

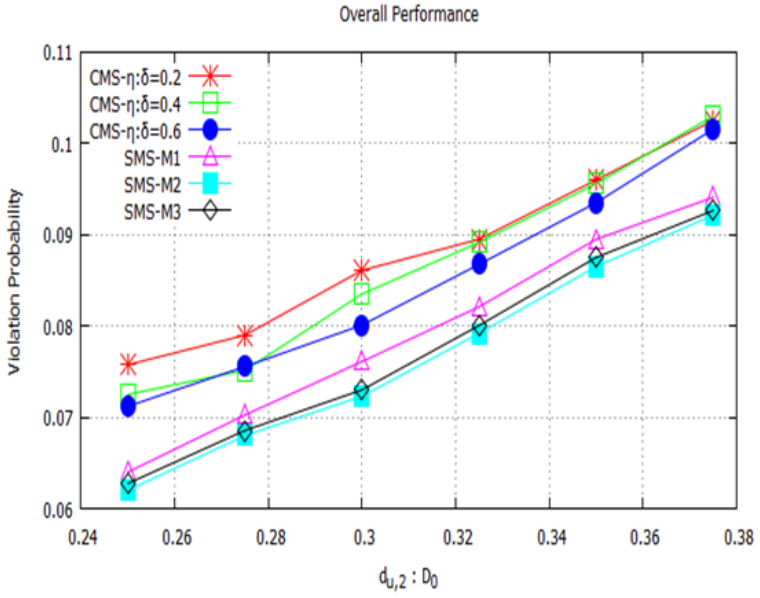
then class1 flows may utilize more resource and will be able to fulfill the requirement, as the distance between two upstream delays start to decrease. As a consequence, class2 is delayed a little but still within its required violation probability. However, as we can see, when $\eta = 0.6 \cdot \delta$, the violation probability of class1 in CMS is still 10% higher than SMS-M1 while the performance of class 2 under CMS is already a little worse than that of SMS-M1. This coincides with our numerical evaluation that CMS needs more cost than SMS in order to fulfill the requirement, since it only relies on upstream path information to make decision. M2 and M3 still have better performance than the others because of their additional adjustments. Another issue we notice from the above two simulations is that, in addition to fulfilling the requirements of different flows, SMS also provides a better overall performance for the traffic (Fig. 6.8c and Fig. 6.9c). The larger the difference among different paths' delay to be (including both upstream and downstream delays), the more advantages SMS will have over CMS.



(a) Class-1 Performance Under Different $d_{u,2}$



(b) Class-2 Performance Under Different $d_{u,2}$

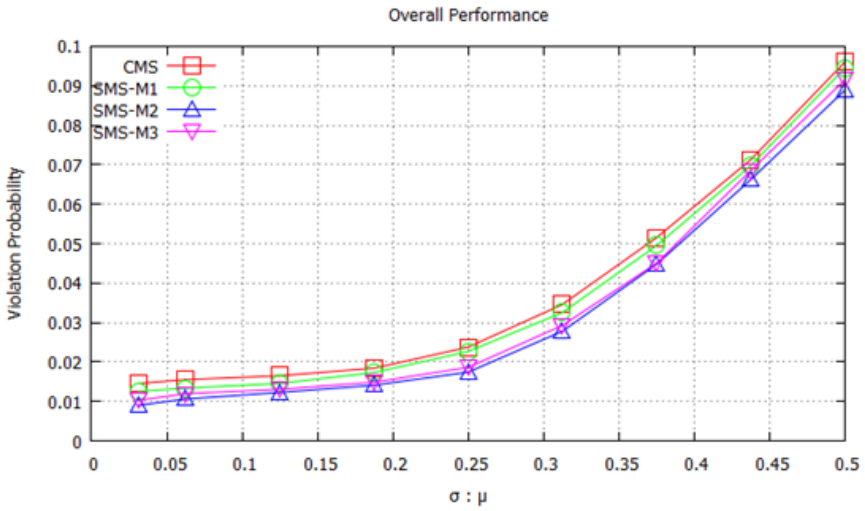


(c) Overall Performance Under Different $d_{u,2}$

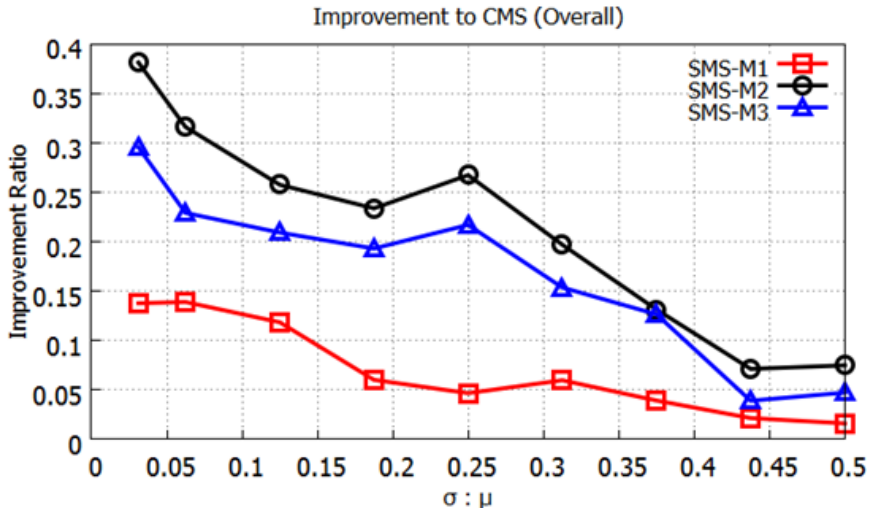
Figure 6.9: Comparison of SMS and CMS Under Different Upstream Delays.

We have demonstrated that, despite the relatively accurate upstream delay, SMS also relies on downstream information for more benefit. Now let us examine the effect of the

accuracy of downstream information. In this simulation, we change the downstream variance of the flows from 1ms to 16ms. The downstream delay parameters are $\mu_1 = \mu_2 = 0.6 \cdot D_0 = 32ms$. We still use the parameters that favor CMS. Thus we set the local adjustment to be $\eta_1 = \eta_2 = \delta_1 \cdot 20\% = 4ms$, the upstream delay of the two classes are $d_{u,1}(p_{1,k}) = \delta_1 + \eta_1 = 24ms$ and $d_{u,2}(p_{2,k}) = \delta_2 - \eta_2 = 16ms$. $\delta_1 = \delta_2 = D_0/4 = 20ms$. The average load is 70%.



(a) Overall Performance Under Different Variance



(b) Overall Improvement Under Different Variance

Figure 6.10: Comparison of SMS and CMS Under Different Downstream Delay Variance.

From Fig. 6.10a, the result looks similar to the previous simulation where we set the

simulation parameters to favor CMS. The absolute difference between SMS and CMS curves are not obvious. As the downstream delay variance gets larger, more packets will violate their requirement. Now we look at how much improvement we have over CMS when the variance changes. Fig. 6.10b shows the ratio of $1 - P_{SMS}(v)/P_{CMS}(v)$, which is the benefit we gain.

The result shows that when the variance increases, the advantage of SMS over CMS varies. The largest benefit appears when the variance is small and decreases as the variance increases. This indicates that when the delay fluctuation is not that high (for example, the delay values of different flows do not cross each other and the priority of flows is obvious over each other), SMS can bring more overall benefit, since the collected delay information can accurately reflect how busy the path is.

6.5 Conclusion

In summary, we proposed a synchronized routing framework in this chapter. We used the synchronized time as the global reference and designed a path-aware collaborative service mechanism. We also proposed three scheduling methods using the synchronized time and knowledge of downstream path delay distribution. We compare our proposed method (SMS) with the existing scheduling scheme CMS. The evaluation shows SMS has a larger adjustment range for packet priority to achieve better coordination of routers.

CHAPTER 7
CONCLUSION AND FUTURE WORK

In this dissertation, we investigated three problems related to smart grid protection, including resource management for agent-based relay protection schemes, effects of cyber attacks on agent-based relay protection schemes, and a synchronized routing framework for real-time data delivery.

First, we proposed a static resource reservation scheme for the MA-based protection, and improved its reliability by using backup paths in the system. We further improved network resource utilization by considering the fact that a single hidden failure is the most common error for relay protection. In addition, with the concrete knowledge of power systems, we can identify the priority of power transmission lines, and select different backup paths based on their priorities. We proposed a power-aware backup scheme to enable us to use less network resources to fulfill the system reliability requirement. We also investigated P2P-based protection. We proposed the primary and backup resource management schemes for the P2P mode. Our evaluation shows that the proposed schemes greatly improve the reliability of the power system while utilizing network resources more effectively.

Second, we investigated potential cyber attacks on P2P agent-based relay protection schemes. We analyzed and evaluated three attack strategies of random attacks, iterative area-based attacks, and cascading-aware attacks to relay agents. We achieve better understanding of how these attacks can reduce the effectiveness of relay protection system. We also investigated the majority rule-based confirmation in relay protection, and observe that it can improve system security compared with the basic confirmation rule. In addition, we also proposed a reputation-based cascading-aware attack, by exploiting weakness of the original reputation-based protection. The evaluation results show that reputation-based attacks can potentially increase the probability of triggering cascading failures compared with direct cascading attacks. Our results also suggest that by disabling trip requests to critical relay agents, we can significantly lower the probability of cascading failures caused

by deliberate cyber attacks.

Third, we proposed a synchronized routing framework. We utilize a synchronized time as the global reference to design routing and scheduling methods. By using accurate upstream delays, and assuming we can obtain downstream delays with the measurement framework, we can dynamically determine service priority for a packet at a router to speed up or slow down its service. Our evaluation shows that we can achieve better overall performance among different flows without explicit reservations for each flow. The proposed scheduling scheme also achieves better coordination among routers by utilizing both upstream and downstream delay information of a packet.

We identify our future research in the following aspects:

(1). Although the P2P-based agent protection uses less network resources than the MA-based protection, the MA-based scheme has the advantage that it knows the state of every line and substation in the system. As the control action on a line may affect other lines, and then affect the reliability of the entire system, a hybrid scheme combining advantages of both MA and P2P protection will be an interesting issue in our future research.

(2). One of the issues in our future research to power grid security is to consider power system properties. As in our current research we primarily focus on the network perspective. Meanwhile, communication delays are critical for both the attacker and system operator, which is closely related to the communication network. By investigating potential attack and defense strategies from time domain, we can better understand the limitations of existing attack and defense strategies, and this can help us design improved defense schemes for future smart grid.

(3). The synchronized framework relies on the estimated downstream delay to adjust the priority of packets. The higher accuracy the downstream delay estimation can achieve, the more effective the scheduling will be. By improving the estimation accuracy, we will be able to improve the delivery of critical data, and also will improve power system reliability. Therefore, the related issues in delay measurement will be investigated in our future research.

BIBLIOGRAPHY

[1] H. Lin. *Communication Infrastructure for the Smart Grid: Co-Simulation Based Study on Techniques to Improve the Power Transmission System Functions with Efficient Data Networks*. PhD thesis, Virginia Polytechnic Institute and State University, Sep. 2012.

[2] S. Garlapati, H. Lin, S. Sambamoorthy, S. K. Shukla, and J. S. Thorp. Agent based supervision of zone 3 relays to prevent hidden failure based tripping. In *Smart Grid Communications, 2010 First IEEE International Conference on*, pages 256–261. IEEE, 2010.

[3] S. Ward, J. O'Brien, B. Beresh, G. Benmouyal, D. Holstein, J. T. Tengdin, K. Fodero, M. Simon, M. Carden, M. V. Yalla, T. Tibbals, V. Skendzic, S. Mix, R. Young, T. Sidhu, S. Klein, J. Weiss, A. Apostolov, D. P. Bui, S. Sciacca, C. Preuss, and S. Hodder. Cyber security issues for protective relays; c1 working group members of power system relaying committee. In *Power Engineering Society General Meeting, 2007. IEEE*, pages 1–8. IEEE, 2007.

[4] X. R. Wang, K. M. Hopkinson, J. S. Thorp, R. Giovanini, K. Birman, and D. Coury. Developing an agent-based backup protection system for transmission networks. In *First International Conference on Power Systems and Communication Systems Infrastructures for the Future*, pages 23–27, 2002.

[5] J. F. Borowski, K. M. Hopkinson, J. W. Humphries, and B. J. Borghetti. Reputation-based trust for a cooperative agent-based backup protection scheme. *IEEE Transactions on Smart Grid*, 2(2):287–301, 2011.

[6] J. E. Fadul, K. M. Hopkinson, C. A. Sheffield, J. Moore, and T. R. Andel. Trust management and security in the future communication-based "smart" electric power grid. In *System Sciences (HICSS), 2011 44th Hawaii International Conference on*, pages 1–10. IEEE, 2011.

[7] J. E. Fadul, K. M. Hopkinson, T. R. Andel, and C. A. Sheffield. A trust-management toolkit for smart-grid protection systems. *IEEE Transactions on Power Delivery*, 29(4):1768–1779, 2014.

[8] W. Zhao, D. Olshefski, and H. G. Schulzrinne. Internet quality of service: An overview. *Columbia University, New York, New York, Technical Report CUCS-003-00*, 2000.

[9] I. Stoica and H. Zhang. Providing guaranteed services without per flow management. In *Proceedings of the 1999 ACM SIGCOMM Conference*, pages 81–94. ACM, 1999.

[10] J. Zhang and Y. Dong. Preventing false trips of zone 3 protection relays in smart grid. *TSINGHUA SCIENCE AND TECHNOLOGY*, 20(2):142–154, 2015.

[11] J. Zhang and Y. Dong. Reliable remote relay protection in smart grid. *ZTE Communications*, 13(3):21–32, 2015.

[12] J. Zhang and Y. Dong. Power-aware communication management for reliable remote relay protection in smart grid. In *Power Systems Conference (PSC), 2016 Clemson University*, pages 1–6. IEEE, 2016.

[13] J. Zhang and Y. Dong. Utilizing path dynamics for delay assurance in synchronized multihop scheduling. In *Computer Communication and Networks (ICCCN), 2014 23rd International Conference on*, pages 1–6. IEEE, 2014.

[14] J. Zhang and Y. Dong. Cyber attacks on remote relays in smart grid. To appear on IEEE Conference on Communications and Network Security, 2017.

[15] J. D. Glover, M. S. Sarma, and T. J. Overbye. *Power System Analysis and Design*, chapter Introduction. CENGAGE Learning, Stamford, USA, 2012.

[16] H. Farhangi. The path of the smart grid. *IEEE Power and Energy Magazine, Vol.8 , Issue.1*, 2010.

[17] X. Fang, S. Misra, G. Xue, and D. Yang. Smart grid - the new and improved power grid: A survey. *IEEE Communications Surveys and Tutorials*, 2011.

[18] E. Ancillotti, R. Bruno, and M. Conti. The role of communication systems in smart grids: Architectures, technical solutions and research challenges. *Computer Communications*, 36(17):1665–1697, 2013.

[19] A. Bose. Smart transmission grid applications and their supporting infrastructure. *IEEE Transactions on Smart Grid*, 1(1):11–19, 2010.

[20] National Institute of Standards and Technology. Smart grid: A beginner's guide. http://www.nist.gov/smartgrid/beginnersguide.cfm, 2012.

[21] Department of Energy. Smart grid: An introduction. http://energy.gov/oe/downloads/smart-grid-introduction-0, 2008.

[22] U.S.-Canada Power System Outage Task Force. Final report on the august 14, 2003 blackout in the united states and canada: Causes and recommendations, 2004.

[23] D. E. Bakken, A. Bose, C. H. Hauser, D. E. Whitehead, and G. C. Zweigle. Smart generation and transmission with coherent, real-time data. *Proceedings of IEEE*, 99(6):928–951, 2011.

[24] D. E. Bakken, C. H. Hauser, H. Gjermundrød, and A. Bose. Towards more flexible and robust data delivery for monitoring and control of the electric power grid. *School Elect. Eng. Comput. Sci., Washington State University, Tech. Rep. EECS-GS-009*, 2007.

[25] J. Ivanovski and V. Maden. Pmu traffic scenarios and network conditions in ip-based wide area communication. *ICT Analysis and Development, Department of Industrial Information and Control Systems, School of Electrical Engineering, KTH-Royal Institute of Technology*, 2009.

[26] B. Johanson and W. Knowle. Traffic modeling and evaluation of qos schemes in wide area monitoring system. Master's thesis, KTH-Royal Institute of Technology, 2013.

[27] V. C. Güngör, D. Sahin, T. Kocak, S. Ergüt, C. Buccella, C. Cecati, and G. P. Hancke. Smart grid technologies: communication technologies and standards. *IEEE transactions on Industrial informatics*, 7(4):529–539, 2011.

[28] N. Cherukuri and K. Nahrstedt. Cooperative congestion control in power grid communication networks. In *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on*, pages 587–592. IEEE, 2011.

[29] M. Ivanov and R. Dimova. Pmu traffic evaluation in wide area monitoring and control systems. Компютърни науки и комуникации, 3(1):3–11, 2014.

[30] S. F. Abelsen, E. S. Viddal, K. H. Gjermundrød, D. E. Bakken, and C. H. Hauser. Adaptive information flow mechanisms and management for power grid contingencies. Technical report, Technical Report EECS-GS-012, School of Electrical Engineering and Computer Science, Washington State University, 2007.

[31] K. H. Gjermundrød. *Flexible QoS-managed status dissemination middleware framework for the electric power grid*. PhD thesis, Washington State University, Aug. 2006.

[32] R. Bobba, E. Heine, H. Khurana, and T. Yardley. Exploring a tiered architecture for naspinet. In *Innovative Smart Grid Technologies (ISGT), 2010*, pages 1–8. IEEE, 2010.

[33] R. Hasan, R. Bobba, and H. Khurana. Analyzing naspinet data flows. In *Power Systems Conference and Exposition, 2009. PSCE'09. IEEE/PES*, pages 1–6. IEEE, 2009.

[34] S. H. Horowitz and A. G. Phadke. Third zone revisiteds. *IEEE Transactions on Power Delivery, Vol. 21, No.1*, Jan. 2006.

[35] NERC. Rationale for the use of local and remote (zone 3) protective relaying backup systems. http://www.nerc.com/docs/pc/spctf/Zone3Final.pdf, 2005.

[36] J. Chen, J. S. Thorp, and I. Dobson. Cascading dynamics and mitigation assessment in power system disturbances via a hidden failure model. *International Journal of Electrical Power & Energy Systems*, 27(4):318–326, 2005.

[37] D. Novosel, M. Begovic, and V. Madan. Shedding light on blackouts. *IEEE Power and Energy Magazine*, Jan. 2004.

[38] J. S. Thorp, A. G. Phadke, S. H. Horowitz, and S. Tamronglak. Anatomy of power system disturbances: Importance sampling. *International Journal of Electrical Power and Energy Systems, Vol. 20, No. 2*, pages 147–152, Feb. 1998.

[39] D. C. E. de la Garza. Hidden failures in protection systems and its impact on power system wide-area disturbances. Master's thesis, Virginia Polytechnic Institute and State University, Apr. 2000.

[40] H. Wang and J. S. Thorp. Optimal locations for protection system enhancement: A simulation of cascading outages. *IEEE Transactions on Power Delivery, vol. 16, no. 4*, Oct 2001.

[41] J. S. Thorp and A. G. Phadke. Protecting power systems in the post restructuring era. *Computer Applications in Power, IEEE*, 12(1):33–37, 1999.

[42] M. A. Haj-ahmed and M. S. Illindala. Intelligent coordinated adaptive distance relaying. *Electric Power Systems Research*, 110:163–171, 2014.

[43] V. Centeno, J. Thorp, and A. Phadke. Advanced protection system using wide area measurements. http://www.uc-ciee.org/~ucciee68/images/downloadable_content/electric_grid/APWA_Final_Report.pdf, 2010.

[44] P. K. Nayak, A. K. Pradhan, and P. Bajpai. Wide-area measurement-based backup protection for power network with series compensation. *IEEE Transactions on Power Delivery*, 29(4):1970–1977, 2014.

[45] P. T. Manditereza and R. Bansal. Renewable distributed generation: The hidden challenges–a review from the protection perspective. *Renewable and Sustainable Energy Reviews*, 58:1457–1465, 2016.

[46] P. Pan, G. Swallow, and A. Atlas. Fast reroute extensions to rsvp-te for lsp tunnels. Technical report, 2005.

[47] M. Gjoka, V. Ram, and X. Yang. Evaluation of ip fast reroute proposals. In *Communication Systems Software and Middleware (COMSWARE), 2007 2nd International Conference on*, pages 1–8. IEEE, 2007.

[48] MPLS Traffic Engineering (TE)–Fast Reroute (FRR) Link and Node Protection. http://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/gslnh29.html, 2004.

[49] D. Katz and D. Ward. Bidirectional forwarding detection (BFD). 2010.

[50] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke. Smart-grid security issues. *IEEE Security & Privacy*, 8(1), 2010.

[51] NERC. Cyber attack task force final report. http://www.nerc.com/docs/cip/catf/12-CATF_Final_Report_BOT_clean_Mar_26_2012-Board%20Accepted%200521.pdf, 2012.

[52] X. Li, X. Liang, R. Lu, X. Shen, X. Lin, and H. Zhu. Securing smart grid: cyber attacks, countermeasures, and challenges. *IEEE Communications Magazine*, 50(8), 2012.

[53] W. Wang and Z. Lu. Cyber security in the smart grid: Survey and challenges. *Computer Networks*, 57(5):1344–1371, 2013.

[54] A. Anwar and A. N. Mahmood. Cyber security of smart grid infrastructure. *arXiv preprint arXiv:1401.3936*, 2014.

[55] Y. Yan, Y. Qian, H. Sharif, and D. Tipper. A survey on cyber security for smart grid communications. *IEEE Communications Surveys and tutorials*, 14(4):998–1010, 2012.

[56] A. R. Metke and R. L. Ekl. Security technology for smart grid networks. *IEEE Transactions on Smart Grid*, 1(1):99–107, 2010.

[57] M. S. Rahman, M. A. Mahmud, A. M. Oo, and H. R. Pota. Multi-agent approach for enhancing security of protection schemes in cyber-physical energy systems. *IEEE Transactions on Industrial Informatics*, 2016.

[58] Y. Zhang. *Mitigating future blackouts via smart relays: a machine learning approach.* PhD thesis, Carnegie Mellon University Pittsburgh, PA, Jul. 2010.

[59] C. M. Shipman, K. M. Hopkinson, and J. Lopez. Con-resistant trust for improved reliability in a smart-grid special protection system. *IEEE Transactions on Power Delivery*, 30(1):455–462, 2015.

[60] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina. The eigentrust algorithm for reputation management in p2p networks. In *Proceedings of the 12th international conference on World Wide Web*, pages 640–651. ACM, 2003.

[61] P. Hines, K. Balasubramaniam, and E. C. Sanchez. Cascading failures in power grids. *IEEE Potentials*, 28(5), 2009.

[62] M. Vaiman, K. Bell, Y. Chen, B. Chowdhury, I. Dobson, P. Hines, M. Papic, S. Miller, and P. Zhang. Risk assessment of cascading outages: Methodologies and challenges. *IEEE Transactions on Power Systems*, 27(2):631, 2012.

[63] N. Bhatt, S. Sarawgi, R. O'Keefe, P. Duggan, M. Koenig, M. Leschuk, S. Lee, K. Sun, V. Kolluri, S. Mandal, M. Peterson, D. Brotzman, S. Hedden, E. Litvinov, S. Maslennikov, X. Luo, E. Uzunovic, B. Fardanesh, L. Hopkins, A. Mander, K. Carman, M. Vaiman, and M. Povolotskiy. Assessing vulnerability to cascading outages. In *Power Systems Conference and Exposition, 2009. PSCE'09. IEEE/PES*, pages 1–9. IEEE, 2009.

[64] Z. Liu, Z. Chen, H. Sun, and Y. Hu. Multiagent system-based wide-area protection and control scheme against cascading events. *IEEE Transactions on Power Delivery*, 30(4):1651–1662, 2015.

[65] S. Park. Cyberattacks on Utah's secure government networks up dramatically. http://www.deseretnews.com/article/865573798/Cyberattacks-on-Utahs-secure-government-networks-up-dramatically.html?pg=all, 2013.

[66] T. Y. Tsai, Chung Y. L, and Z. Tsai. Introduction to packet scheduling algorithms for communication networks. *Communications and Networking*, pages p263–271, 2010.

[67] A. K. Parekh and R. G. Gallager. A generalized processor sharing approach to flow control in integrated services networks: the single-node case. *IEEE/ACM Transactions on Networking (TON)*, 1(3):344–357, 1993.

[68] D. Ferrari and D. C. Verma. A scheme for real-time channel establishment in wide-area networks. *Selected Areas in Communications, IEEE Journal on*, 8(3):368–379, 1990.

[69] J. Liebeherr, D. E. Wrege, and D. Ferrari. Exact admission control for networks with a bounded delay service. *IEEE/ACM Transactions on Networking (TON)*, 4(6):885–901, 1996.

[70] D. D. Clark, S. Shenker, and L. Zhang. Supporting real-time applications in an integrated services packet network: Architecture and mechanism. In *ACM SIGCOMM Computer Communication Review*, volume 22, pages 14–26. ACM, 1992.

[71] M. Andrews. Probabilistic end-to-end delay bounds for earliest deadline first scheduling. In *INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, volume 2, pages 603–612. IEEE, 2000.

[72] C. Li and E. W. Knightly. Coordinated multihop scheduling: a framework for end-to-end services. *IEEE/ACM Transactions on Networking (TON)*, 10(6):776–789, 2002.

[73] C. Li and E. W. Knightly. Schedulability criterion and performance analysis of coordinated schedulers. *IEEE/ACM Transactions on Networking (TON)*, 13(2):276–287, 2005.

[74] W. Wang, Y. Xu, and M. Khanna. Survey paper: A survey on the communication architectures in smart grid. *Comput. Netw.*, 55(15):3604–3629, October 2011.

[75] J. Gao, Y. Xiao, J. Liu, W. Liang, and C. L. P. Chen. A survey of communication/networking in smart grids. *Future Generation Computer Systems*, 28(2):391–404, 2012.

[76] OMRON. Solid state relays technical information. http://media.digikey.com/pdf/Other%20Related%20Documents/Omron%20Other%20Doc/SSR%20Design%20Considerations.pdf.

[77] Working Group I19 IEEE PSRC. Redundancy considerations for protective relaying systems. http://www.pes-psrc.org/Reports/Redundancy_Considerations_for_Protective_Relaying_Systems_WG%20I19.pdf, 2010.

[78] C. Hertzog. Reliability and the smart grid. http://www.smartgridlibrary.com/2010/08/02/reliability-and-the-smart-grid/.

[79] G. Castañón, G. Campuzano, and O. Tonguz. High reliability and availability in radio over fiber networks. *Journal of Optical Networking*, 7(6):603–616, 2008.

[80] PowerWorld Corporation. Powerworld homepage. http://www.powerworld.com/.

[81] A. Agatep. Voltage stability analysis using simulated synchrophasor measurements. Master's thesis, California Polytechnic State University, San Luis Obispo, May. 2013.

[82] I. Musirin and T. A. Rahman. On-line voltage stability based contingency ranking using fast voltage stability index (FVSI). In *Transmission and Distribution Conference and Exhibition 2002: Asia Pacific. IEEE/PES*, volume 2, pages 1118–1123. IEEE, 2002.

[83] S&C Electric Company. Designing a smart grid communication system to achieve 99.999% link availability. http://www.sandc.com/edocs_pdfs/edoc_075041.pdf.

[84] H. Ren and I. Dobson. Using transmission line outage data to estimate cascading failure propagation in an electric power system. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 55(9):927–931, 2008.

[85] I. Dobson, B. A. Carreras, and D. E. Newman. A loading-dependent model of probabilistic cascading failure. *Probability in the Engineering and Informational Sciences*, 19(01):15–32, 2005.

[86] A. Bernstein, D. Bienstock, D. Hay, M. Uzunoglu, and G. Zussman. Power grid vulnerability to geographically correlated failuresanalysis and control implications. In *INFOCOM, 2014 Proceedings IEEE*, pages 2634–2642. IEEE, 2014.

[87] D. J. Watts and S. H. Strogatz. Collective dynamics of small-worldnetworks. *nature*, 393(6684):440–442, 1998.

[88] X. F. Wang and G. Chen. Complex networks: small-world, scale-free and beyond. *IEEE circuits and systems magazine*, 3(1):6–20, 2003.

[89] Q. K. Telesford, K. E. Joyce, S. Hayasaka, J. H. Burdette, and P. J. Laurienti. The ubiquity of small-world networks. *Brain connectivity*, 1(5):367–375, 2011.

[90] G. A. Pagani and M. Aiello. Power grid complex network evolutions for the smart grid. *Physica A: Statistical Mechanics and its Applications*, 396:248–266, 2014.

[91] G. A. Pagani and M. Aiello. The power grid as a complex network: a survey. *Physica A: Statistical Mechanics and its Applications*, 392(11):2688–2700, 2013.

[92] Python igraph. http://igraph.org/python/.

[93] Small world networks. http://mathinsight.org/small_world_network.

[94] Social and technological network analysis: Small world and weak ties. https://www.cl.cam.ac.uk/teaching/1213/L109/stna-lecture2.pdf.

[95] Q. Qiu. *Risk assessment of power system catastrophic failures and hidden failure monitoring & control system.* PhD thesis, Virginia Polytechnic Institute and State University, Dec. 2003.

[96] R. Durairajan, S. Ghosh, X. Tang, P. Barford, and B. Eriksson. Internet atlas: a geographic database of the internet. In *Proceedings of the 5th ACM workshop on HotPlanet*, pages 15–20. ACM, 2013.