Strategic Power Infrastructure Defense

HAO LI, MEMBER, IEEE, GARY W. ROSENWALD, MEMBER, IEEE, JUHWAN JUNG, MEMBER, IEEE, AND CHEN-CHING LIU, FELLOW, IEEE

Invited Paper

This paper provides a comprehensive state-of-the-art overview on power infrastructure defense systems. A review of the literature on the subjects of critical infrastructures, threats to the power grids, defense system concepts, and the special protection systems is reported. The proposed Strategic Power Infrastructure Defense (SPID) system methodology is a real-time, wide-area, adaptive protection and control system involving the power, communication, and computer infrastructures. The SPID system performs the failure analysis, vulnerability assessment, and adaptive control actions to avoid catastrophic power outages. This paper also includes a new concept for bargaining by multiagents to identify the decision options to reduce the system vulnerability. The concept of a flexible configuration of the wide-area grid is substantiated with an area-partitioning algorithm. A 179-bus system is used to illustrate the area partitioning method that is intended to minimize the total amount of load shedding.

Keywords*—*Critical infrastructures, defense systems, intelligent systems, multiagent technology, power infrastructure security.

I. INTRODUCTION

Critical infrastructures include the electric power grids, telecommunications, public transportation, natural gas and oil, water supply systems, banking, finance, and other fundamental structures and services that are vital for the well being of our society, the economy, and national security. A painful lesson learned from the tragic events of 11 September 2001 is that the security and robustness of the critical infrastructures cannot be taken for granted. In particular, the electric power infrastructure is the most critical infrastructure upon which other infrastructures depend. The security, vulnerability, interdependency, protection, and emergency response are highly important research subjects for the critical infrastructures.

In recent decades, the electric power industry has become more and more automated, interconnected, and computerized. While interconnection and advanced technologies lead to greater efficiency and reliability, they also bring new sources of vulnerability through the increasing complexity and external threats. Threats to the power infrastructure include natural disasters, human errors, power system component failures, information and communication system failures, gaming in the electricity markets, intrusion, and sabotage. Among these threats, sabotage is probably more difficult to handle due to its secretive and hostile characteristics. Sabotage can cause great damage to power grid facilities, including nuclear power stations or major transmission facilities. Sabotage can also involve communication, computer and information system damage, and cyberattacks that can severely undermine the reliability of the electricity supply. Clearly sabotage is intended to cause maximum damage and disruption to the society. Due to these threats, it is critical to develop defense plans and technologies for the electric power and related infrastructures.

Defense plans for the power infrastructure should include the strategies and procedures to defend the grids against the various threats. A basic defense system for the power grid may involve load shedding in the event of a major system disturbance. More sophisticated defense systems are wide-area, real-time protection and control systems with full sensing, communication and information capabilities. The Strategic Power Infrastructure Defense (SPID) systems refer to such advanced system concepts that involve real-time sensing and communication, failure analysis, vulnerability assessment, and self-healing control features. Although the wide-area defense systems are still in development, well-developed special protection systems and schemes are available for integration into the defense plans.

Manuscript received October 16, 2003; revised January 4, 2004. This work was supported in part by the National Science Foundation under Grants ECS-0217701 and ECS-0424022 on transmission reliability and economics. The SPID research was supported by the U.S. Department of Defense and the Electric Power Research Institute. The APT Center at the University of Washington is supported by AREVA T&D, the Bonneville Power Administration, CESI, LS Industrial Systems, PJM Interconnection, and RTE.

H. Li and G. W. Rosenwald are with AREVA T&D Inc., Bellevue, WA 98004 USA (e-mail: hao.li@areva-td.com; gary.rosenwald@areva-td.com).

J. Jung is with LS Industrial Systems, Seoul, Korea (e-mail: jhjung@lsis.biz).

C.-C. Liu is with the Department of Electrical Engineering, University of Washington, Seattle, WA 98195 USA (e-mail: liu@engr.washington.edu).

Digital Object Identifier 10.1109/JPROC.2005.847260

The purpose of this paper is to provide a comprehensive overview of the power infrastructure defense systems and to report new research results for the defense systems. Section I includes a summary of the state of the art in critical infrastructures, threats to the power infrastructure, and the relevant defense system technologies and special protection systems. In Section II, the SPID system technology is described with the multiagent, distributed intelligence systems serving as the foundation technology for the implementation of an SPID system. Two new research results are reported in this paper. In Section III, a proposed multiagent bargaining algorithm allows the agents to work as a team synergistically in order to reduce the system vulnerability. Section IV provides a power system reconfiguration algorithm that allows the grids to be partitioned into self-sufficient subsystems in such a way that the overall system vulnerability will be reduced. A simulation example based on a variation of the western interconnection of the United States is used to illustrate the proposed reconfiguration algorithm. Finally, the areas for future research and development are given in Section V.

A. Critical Infrastructures

The research needs and requirements related to the critical infrastructure protection have been widely discussed by government organizations and the public and private sectors [1]–[17]. However, the amount of literature that reports concrete research results in this area is small. A taxonomy of tools for defining research requirements necessary to develop the next generation of tools for the critical infrastructure was developed [1]. Reference [1] provides an overview of tools necessary to conduct an in-depth analysis and characterization of threats, vulnerabilities, and interdependencies of critical infrastructure subsystems and their interaction with one another. A number of tools have been discussed with an emphasis on modeling, simulation, and testing. In addition to tools, a number of system-level research suggestions were provided, including development of system architecture, data flow models, national level resources, and a national test bed. As mentioned in [1], an infrastructure is a coupled system of various types of subsystems. Information technology revolution has made critical infrastructures highly interconnected and mutually dependent. Intrusions and disruptions in one infrastructure might provoke unexpected failures to others. How to handle interdependencies becomes an important problem. As an initial step, [2] proposed the taxonomy to facilitate infrastructure interdependencies research. The taxonomy frame described six aspects of infrastructure interdependencies: types of interdependencies, infrastructure environment, coupling and response behavior, infrastructure characteristics, types of failures, and state of operations. Reference [3] presented a simple conceptual infrastructure layer model to compare different infrastructures and outlined the challenges for infrastructure systems research and design.

The issues for research and development of power industry are addressed in [4]–[6]. The power infrastructure is operated closely with the information and communication infrastructures. The operation, protection and control of the power grid rely on a large number of computers in the control centers (e.g., energy management systems (EMS), supervisory control and data acquisition (SCADA) systems) and substations (e.g., digital relays). Power system communication for control centers is traditionally based on microwaves; however, it is increasingly dependent on optical fibers. The Internet is being used for electricity market functions. More critical operations in the power industry now use the Internet as a communications highway. This creates special problems because the Internet is an open system by design and hence is prone to malicious intervention [7]–[9]. The author of [10] believes that the growing reliance of the electric power industry on information technologies introduces a new class of cyber-vulnerability. For example, dependency on Internet is exemplified by the open-access-same-time information system (OASIS), which is used to post information on power transfer capabilities and can greatly influence power system management and trading [10]. The paper [11] analyzes the risks arising from the interdependencies between the global information infrastructure and other critical infrastructures including electric power infrastructure. After illustrating the energy infrastructure's (as well as other infrastructures') dependency on technologies, the author of [12] claims that technologies available for attacking infrastructure systems have become much easier to obtain and use, while technologies for defending infrastructure systems and preventing damage have not kept the pace with the capability for destroying such systems. As a result, considerable research needs are indicated in [12]. These research needs include computer protection and component-level and system-level issues. For example, the system-level issues include vulnerability assessment methodologies, risk management decision support, incident response planning, and information sharing. Finally, the author of [12] points out that technology can help prevent infrastructure damage and can assist in recovering from damage, but technology cannot prevent sabotage. Since sabotage cannot be eliminated, the task is to minimize the risks. The paper [13] discusses the concepts and perspectives for developing methodology for infrastructure vulnerability studies. The main focus is on the vulnerability of the power distribution and the digital communications that are utilized in the control system of the electricity network and how modern digital control systems might facilitate the recovery of damaged power systems. The authors of [13] stress the research need on technical crisis management, based on experiences from case studies of the large power failures in New Zealand and Canada in 1998. The report [14] provides a high-level overview of the vulnerability assessment methodology being developed and applied to the electric power infrastructure by the Office of Energy Assurance (OEA), Department of Energy (DOE). The methodology has been successfully applied as part of OEA's Vulnerability Assessment Program to help energy-sector organizations identify and understand the threats to their infrastructures and physical and cyber-vulnerabilities of their infrastructures. The effort of [15] is on creating a bridge between vulnerability assessment, risk estimation and representation, and the use of IT tools.

As a timely response to the 11 September 2001's tragic events, the Electric Power Research Institute (EPRI) is developing a program: the Infrastructure Security Initiative, which is a "three-phase effort to pinpoint vulnerabilities in the electric power infrastructure, to develop strategies to strengthen and protect them, and to outline plans for rapid recovery from terrorist attacks should they occur [7]." The North American Electric Reliability Council (NERC) has developed several critical infrastructure protection programs: Critical Infrastructure Protection Working Group; Indications, Analysis, and Warnings Program; Electricity Sector Information Sharing and Analysis Center; Critical Infrastructure Protection Planning; and Partnership for Critical Infrastructure Security [16]. These programs can provide the National Infrastructure Protection Center (NIPC) with information necessary for NIPC to provide the electric industry with timely, accurate, and actionable alerts and warnings of imminent or emerging physical or cyberattacks. Reference [17] concludes that there are numerous opportunities to increase the security of the nation's energy system and many solutions exist in already available technologies. For example, increasing energy efficiency and utilizing distributed generation will help reduce the energy system vulnerability to terrorist attacks and provide the nation with secure and reliable energy service.

B. Threats to Power Infrastructure

The historic blackouts and power failures, such as the U.S. northeast blackout of 1965 [18], [19], the New York City power failure in July 1977 [20], the 2 July 1996 cascading outage of the western North American power system [21], [22], the power system outage that occurred on the U.S. western interconnection on 10 August 1996 [22]–[24], and the major blackout that occurred in the eastern U.S. in August 2003 [25], serve as a powerful reminder that the power infrastructure in the U.S. is severely underprepared for catastrophic events. The various potential sources of power system vulnerability are discussed in [26].

C. Defense Systems

It is important to develop a real-time defense strategy that helps minimize the potential impact of the threats to power infrastructure. An overview of the Brazilian defense plan against extreme contingencies is presented in [27]. The concept of security zones and network security matrix has been developed. A programmable logic controller (PLC)-based special protection system was designed to create controllable zones. In France, a coordinated defense plan to prevent large regions of the country from blackouts and to accelerate restoration is presented in [28]. The principles of the defense plan and the architecture of the defense system are discussed in detail in [28]. Hydro-Québec has established a defense plan to deal with extreme contingencies and reduce the frequency and extent of major or total power failures [29].

In our previous work sponsored by the Department of Defense and EPRI, the conceptual design of the SPID system has been developed. The SPID system is aimed at prevention of the wide-area grid outages against cascaded events caused by a series of problems including short circuits and equipment failures [30]. The communication issues including information transmission network design and data exchange architecture design for the SPID system are addressed in [31]. The authors of [32] suggest a new algorithm for the communication system in a power system wide-area protection scheme such as the SPID system. The communication infrastructure is expected to provide high-speed, low-delay, reliable, robust data transmission for dissemination and exchange of the critical control signals and other data. The design of a self-healing strategy of the SPID system after large disturbances is reported in [33].

D. Special Protection Systems and Schemes

As part of the Hydro-Québec's defense plan [29], a new generation of programmable load shedding systems (PLSSs) has been developed [34]. These PLSSs perform power system frequency and voltage monitoring tasks. They can be programmed on-site or remotely to offer customized solution to power system protection. By use of special protection systems with special load and generation rejection schemes at Ontario Hydro's largest generation complex, transmission constraints caused by regulatory delay have been reduced [35]. Reference [36] reports on a joint IEEE–CIGRE survey to determine the experience with special protection schemes. The purpose of the report is to help develop methods of reliability analysis for special protection schemes.

A method by performing voltage phase angle measurements to detect loss of synchronism for the French defense plan is introduced in [37]. A statistical analysis of the impact on security of on-load tap changers (OLTCs) automatic blocking devices in the French power system is presented in [38]. As a protection scheme, these OLTC automatic blocking devices were installed to prevent voltage collapses.

A technique to catalog and analyze the possible hidden failures in the protection systems of a power network is presented in [39]. This technique would help reduce the likelihood of protection system hidden failures contributing to wide-area disturbances [39]. Study results by using special protection systems and various fast-acting devices to improve the stability performance and to maximize power transfer capability of the Western Electricity Coordinating Council (WECC) systems are provided in [40]. In [41], the importance of developing a systematic and comprehensive reliability framework for special protection systems is discussed, and several reliability assessment methods are described. A generic procedure for risk-based assessment of special protection systems is proposed in [42]. From an operations point of view, the paper [43] discusses the impact of special protection systems on the system operator, operational problems associated with special protection systems documentation, problems due to rapid proliferation of special protection systems, and concerns about the reliability of special protection systems. Other special protection schemes include defense measures proposed in [44] to deal with the sabotage or tampering in nuclear power plants, and the various techniques documented in [45] to rapidly

and efficiently restore transmission line services after an emergency.

II. Multiagent System Technologies and Their Application to the SPID System

A. Multiagent System Technologies

Intelligent systems are emerging technologies to deal with large and complex systems. For decades, engineers have developed various intelligent systems such as knowledge-based systems, neural networks, fuzzy logic, and other qualitative reasoning techniques [46] to solve challenging problems in power engineering. One important application of intelligent systems is to monitor, analyze, and control power grids. Most conventional intelligent control systems are centralized and supervised in a top-down fashion. As the size of power systems increases and the competitive power industry evolves, these conventional intelligent systems might not be able to appropriately respond to the changes and uncertainty of the power infrastructure.

Distributed artificial intelligence (DAI) is receiving considerable attention due to its abilities to tackle uncertainties of the systems. In DAI systems, control tasks are assigned to various modules. Each module is designed to handle well-defined and limited tasks, so the overall computation can be carried out in parallel within a short time. The global goals are achieved through the integration of different views and problem-solving techniques in various modules. The DAI framework can achieve effective controls for uncertain systems while maintenance is much simplified relative to conventional centralized structures. The multiagent system (MAS) technology is a major research area in DAI. An MAS structure consists of a number of agents coupled with networks and a protocol for interactions among the agents. Each agent performs its own tasks as an autonomous entity, while the global goal is achieved by interactions among agents. An important feature is that each agent has the ability to perceive the environment, communicate with other agents and take actions to affect the environment based on its knowledge and the results of communications [47]. It is natural that MAS becomes a promising design method to construct a complex control system with a "decentralized" fashion.

Due to restructuring of the power industry, the operation and control of power systems may not be centralized. As a result, MAS technology is a promising tool for power system problems. The research effort of [48] is to produce an MAS infrastructure for distributed rational decision making in power systems. A multiagent approach to the development and implementation of systems to assist engineers with disturbance diagnosis is proposed in [49]. A new EMS architecture based on the agent technology is proposed in [50] in order to deal with continuously evolving goals and requirements in power systems. The authors describe how the openness of a control system can be achieved through the MAS technology. The structure of MAS for power system restoration is proposed in [51] and [52]. In [51], the blackboard method, which is a global memory shared by agents, is proposed for the agent communication and coordination purposes. Since the agents in the system are independent of each other and their decision-making processes to achieve goals are asynchronous, the authors propose an asynchronous MAS architecture, "A-team." The MAS technique has been applied to power markets to support new market activities [53]. The developed MAS simulator, where agents represent market entities such as generators, consumers, traders, and market operators, can probe the effects of market rules and conditions by simulating the participants' strategic behavior.

B. The SPID System

To prevent or reduce catastrophic failures and cascading sequences of events caused by various sources of vulnerability, the proposed defense system, which is referred to as the SPID system, is to provide a wide-area, intelligent, adaptive protection and control system that empowers future power grids by providing critical and extensive information in real time, assessing system vulnerability quickly, and performing timely self-healing and adaptive reconfiguration actions based on system-wide vulnerability analysis. The recent blackout scenarios (i.e., 10 August 1996 in the western U.S. and 14 August 2003 in the eastern U.S.) show that the current philosophies and technologies allow only local, narrowly focused control actions based on measurements at the substation or line level. Thus, the SPID system aims at implementing mathematical and computational techniques that are able to meet the four objectives as follows.

1) Failure Analysis: The power system is monitored and analyzed to detect hidden failures in protective devices and control schemes based on a system-wide assessment. This analysis first examines possible hidden failures on a protection device that is unable to perform its designed and expected actions under abnormal power system conditions. Based on the hidden failure information, the analysis identifies the region of vulnerability that is a physical region in the power grid such that a hidden failure of the protection device will trigger cascading events of other components (i.e., lines, transformers, and generators) or hidden failures on other protective devices within the region. Thus, the region of vulnerability can be represented as follows [39]:

$$V_R = \{C_1, C_2, \ldots C_n\} \tag{II.1}$$

where C is a component or protective device. Each component can be represented as

$$C_i = f(H_{Pf}, S_{Pf}, S_{Ci}), \quad i = 1 \text{ to } n \tag{II.2}$$

where H_{Pf} is the type of hidden failure of the protection device P_f, S_{Pf} and S_{Ci} are the settings/ parameters of the protection device and the component respectively, and f is the function which represents the protection coordination logic between the protection device and the component. In other words, the function f identifies if the hidden failure of the protection device P_f leads to the failure of the component C_i based on the protection coordination schemes.

2) Vulnerability Assessment: The power system is assessed with possible sources of vulnerability such as human

errors, natural calamities, failures in protection, or inadequate information. This analysis assesses under the current system status how vulnerable the power grid is. Since the purpose of the SPID system is to minimize catastrophic power outages with respect to the Failure Analysis, the vulnerability assessment should reflect the extent that loads may be lost. Therefore, the SPID system uses the anticipated loss of load, $\sum MW$, with respect to a sequence of events/ failures as a vulnerability index. If the system can be stabilized after $\sum MW$ of load shedding, the index represents how vulnerable the current power grid is. Here it is assumed that the available options and control actions are taken before load shedding takes place.

3) Adaptive Self-Healing Strategy: This strategy is to achieve autonomous, adaptive, preventive, and corrective remedial control actions by providing adaptive and intelligent protection. Current technologies on power system reconfiguration and protection are not designed to change or adjust parameters and strategies in order to adapt to changing system conditions (i.e., vulnerable conditions). The self-healing strategy figures out the optimal sequence of control actions that can minimize the vulnerability index. In order to meet the requirements above, the temporal difference (TD) method is used as follows [54]:

$$V_{n+1} = V_n + a(R_n - V_n) \tag{II.3}$$

where V is the vulnerability index, n is the index of the current step, R_n is the cumulative actual reward value (i.e., the vulnerability index after a control action is taken at each step) received from the power system, and a ($0 \leq a \leq 1$) is a constant step-size parameter which is called the adaptive factor. Using the method above, the SPID system is able to adaptively find the optimal sequence of control actions that minimize the power system vulnerability.

4) Information and Sensing: Current information and sensing technologies in power systems are narrowly focused. Only part of the online information is transferred to the control center from remote terminal units through dedicated communication links. Therefore, SPID also includes a robust and fast communication network to monitor and control a power system in a wide area. Since communication plays an important role in the SPID system, the vulnerability of the communication network has to be assessed. Specifically, a critical control signal should arrive at a destination (e.g., a protection device or circuit breaker) in time. However, if the communication network is congested due to severe communication traffic during the sequence of events/failures, the communication network becomes vulnerable, which eventually leads to the power system's vulnerability. The communication system's vulnerability index, therefore, can be defined as follows [32]:

$$V_{\text{comm}} = \frac{\text{Congested Link Count}}{\text{Total Link Count}}. \tag{II.4}$$

The function is a measure of the effect of higher priority data throughput. It is assumed that a link is congested if the throughput of the higher priority data exceeds two-thirds of the capacity.

The objectives in the SPID system require a large number of software and hardware tools (or subsystems) to work together. Each entity (i.e., software of hardware) involved in the SPID system has only a local view of the entire scope while the entire system should react in such a way that all entities are closely coordinated. The structure of the SPID system, therefore, is designed based on MAS technologies to provide self-healing control actions and fast assessment of a power system. The MAS for the SPID system consists of two types of agents.

1) Cognitive agent: An agent that has a knowledge base available, all the data, and know-how to achieve its task(s) and to deal with interactions with other agents/ environments. This type of agent has goals and explicit plans allowing the agent to intelligently achieve its goal(s).
2) Reactive agent: An agent that works in a stimulus-response manner. Thus, each reactive agent in the SPID system does not necessarily have to be "intelligent." The goals of a reactive agent are implicitly represented by the rules/logic that are programmed in advance so it might be costly to encode/maintain the numerous rules for the SPID system. However, the advantage of the reactive agents is their ability to react fast.

Based on the two types of agents above, the MAS for the SPID system consists of three hierarchical layers as illustrated in Fig. 1. The cognitive agents are located in the highest layer, the *deliberative layer*. The agents in the lowest layer, the *reactive layer*, are reactive agents that are located in every local subsystem and perform preprogrammed self-healing control actions requiring an immediate response. The middle layer, the *coordination layer*, consists of agents that have heuristic knowledge to identify which events from the reactive layer are urgent, important, or resource consuming. If the events exceed a predefined threshold value, the agents in the middle layer will deliver the events to the deliberative layer. The middle layer also continuously examines any change between the power system models of deliberative and reactive layer. If there is any mismatch between two power system models (i.e., power system status changed), then the coordination layer updates the power system model of the deliberative layer so that the agents in the deliberative layer can always respond to the current power system status. However, it is possible that the control actions/decisions from the deliberative layer can be outdated so the coordination layer should verify the control actions/decisions with the current power system status. The SPID multiagent system is able to perform immediate response against a fault/disturbance by the agents in the reactive layer, but these narrowly focused responses can often be inadequate from the system-wide perspectives. Therefore, the agents in the deliberative layer can revise these locally limited responses of the reactive layer and inhibit the responses (if needed) from the system-wide point of view. The subsumption architecture, which uses hierarchically coordinated agents' layers, is used to coordinate

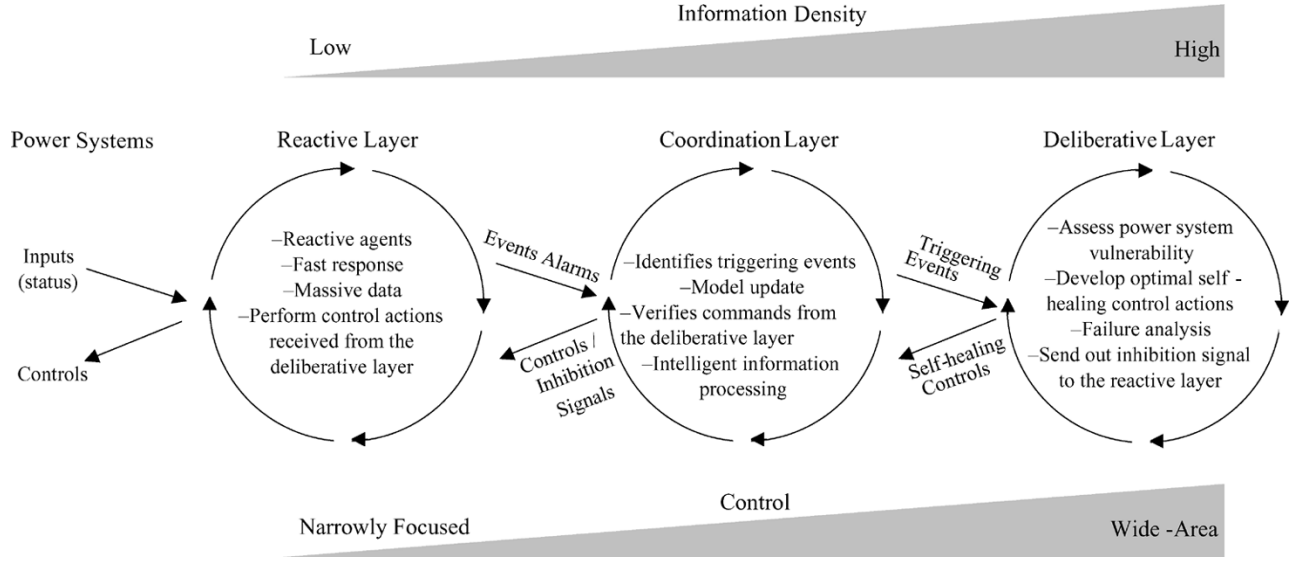

Fig. 1. Hybrid multiagent system architecture for the SPID system.

the local (from reactive layer) and system-wide (from deliberative layer) control actions.

III. Aumann–Maschler Bargaining Sets for Infrastructure Security Analysis

The formation of decisions in a multiagent system can be analyzed by modeling the negotiated decisions as a coalition between agents. The Aumann–Maschler (A–M) version of bargaining sets [55] is used to analyze the distribution of benefits in the potential coalition structures that may be formed between the agents (e.g., the level of physical security that can be reached for different sets of agent decisions). The outcome of the bargaining analysis is the determination of stable distributions of the benefits arising from a coalition so that one member of the coalition will not leave to find a more beneficial coalition. In the framework of multiagent SPID systems, distributed agents may be used to respond quickly to events and system conditions to determine actions needed to conform with specified security assessments. An analytical framework is developed for a multiagent SPID system that has the following attributes.

1) Vulnerability is measured by loss of load and is determined outside the negotiation analysis for the various events and system conditions.
2) Agents are initially assigned a portion of the vulnerability responsibility.
3) Agents can meet their vulnerability obligation by taking other actions that reduce local measures of vulnerability or ultimately by shedding load.
4) Actions taken by an agent impact local measures of vulnerability for that agent and/or other agents.
5) Vulnerability obligation can be transferred between agents.
6) Only bilateral coalitions between agents to take mutually agreeable actions that impact vulnerability are described.

The concept of A–M bargaining sets in bilateral coalitions requires the consideration of external agents that act as threats for each of the agents in the coalition. The distribution of the benefits is considered stable if any threat to leave the current coalition and form one with an external third agent has a counterthreat where the second agent and external third agent can exclude the objecting agent in a new coalition where both the second and third agent are better off. The A–M bargaining set analysis determines the point for which the benefit received by the third party (the threat) is the same in both of the bilateral coalitions that may be threatened by the original two bargaining parties.

A. Predicting Multiagent SPID Outcomes With A–M Bargaining Sets

Combining the calculation of A–M bargaining sets with local vulnerability analysis results in a method for calculating potential outcomes of decisions made to enhance the physical security of the power system by distributed multiagent systems where each agent is attempting to best enhance its local security. The benefit in reduced local vulnerability produced by one agent's actions or the combined action of agents in potential coalitions is determined using local vulnerability analysis. These benefits can then be used in the calculation of the A–M bargaining sets for different coalitions in the multiagent negotiation process.

The benefits created by a potential coalition are a critical factor in the formation of the coalition. The benefit ν used in determining A–M bargaining sets is the sum of the benefit, i.e., reduced local vulnerability, realized by the parties in the coalition

$$\nu = \sum_{a \in \text{coalition}} \nu_a. \tag{III.1}$$

Using this definition of coalition benefits, A–M bargaining sets can be applied to a three agent system composed of two agents (A and B) and any third agent (T) that may be used

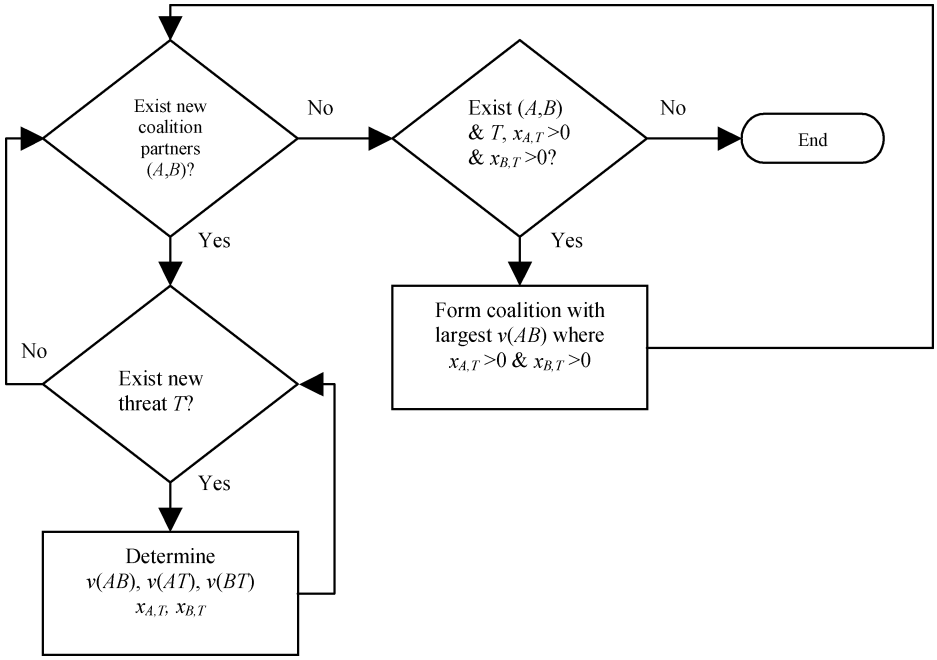

Fig. 2. Calculating expected agent activity.

as a threat for a proposed coalition between A and B. For this three-agent system, the agent A can choose to form a coalition (i.e., a set of actions and/or exchange for vulnerability responsibility) with agent B, to form no coalition with any agent, or to pursue other opportunities with another agent (T). Each agent has a similar set of choices. If the benefit between two agents were negative, they would be better off not forming the coalition and should choose not to form the coalition. The option of forming no coalition ensures that agents will not be worse off than they would be alone.

The sum of the benefit of coalition γ is denoted as $v(\gamma)$, and the allocation of benefit to agent A is denoted as x_A, etc. The two-agent coalitions include $\{AB\}$ in which agents A and B form an agreement and coalitions $\{AT\}$ and $\{BT\}$ in which the company and competitor form a coalition with the threat agent T.

The A–M condition for stability in such a three-agent problem is that the maximal offers from A and B to the third agent T (in an attempt to form $\{AT\}$ and $\{BT\}$, respectively) be of equal value, i.e., $x_T = v(AT) - x_A = v(BT) - x_B$. This equation represents the bargaining position of each of the agents. Combining this with the equation $v(AB) = x_A + x_B$ indicating that the benefit of the current coalition will be divided among the coalition members, the stable A–M bargaining set for the $\{AB\}$ coalition is

$$x_A = \frac{v(AB) + v(AT) - v(BT)}{2} \qquad \text{(III.2)}$$

$$x_B = \frac{v(AB) + v(BT) - v(AT)}{2} \qquad \text{(III.3)}$$

$$x_T = \frac{v(AT) + v(BT) - v(AB)}{2}. \qquad \text{(III.4)}$$

If x_A or x_B is less than zero, the AB coalition will not be formed, since the agent with a negative benefit would choose not to join the coalition. If x_T is less than zero, the threat described above is not credible, since the threat agent cannot be forced to join a coalition. When $x_T < 0$, the agent T can still be used as a threat, but the resulting bargaining set solution is a range of values. When $x_T < 0$, A is able to threaten to form a coalition with T in which $x_T = 0$ or $x_A = v(AT)$. In this case, $x_B = v(AB) - x_A = v(AB) - v(AT)$. But when $x_T < 0$, B is also able to threaten with a coalition in which $x_B = v(BT)$ and $x_T = 0$. Then $x_B = v(AB) - v(BT)$. The bargaining set for this case is a range of benefit distributions between these limits. When a single predicted outcome is needed, the middle of the range is used as an expected value if no other information is known about the coalition negotiation process. These expected benefits may be incorporated in the coalition analysis of each agent as it considers which coalitions to accept.

B. Procedure for Calculating Expected Agent Activity

The method for determining A–M bargaining sets is performed for proposed coalitions of agents. In selecting the coalitions that yield the most benefit for the agents, the bargaining set analysis predicts the results of agent behavior.

Assuming: 1) sequential coalition decisions; 2) local vulnerability dependency on previous decisions; and 3) greedy selection of coalitions providing the most benefit, a procedure for calculating the potential benefit of interconnected decision making is described in Fig. 2. For each potential set of coalition partners (A, B), the A–M bargaining set for each of the potential threat agents T is determined. Once the bargaining sets are determined, if there is a viable coalition and threat combination, the greedy selection is employed and the most beneficial coalition is formed.

Following this decision, the process is repeated and the benefits and bargaining sets are recalculated for potential new coalitions. The process terminates when there are no

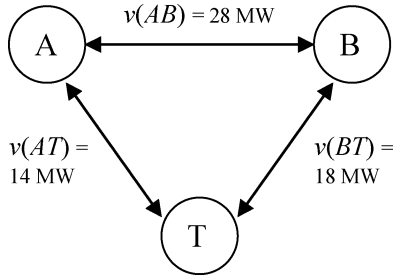

Fig. 3. Potential coalition benefits.

beneficial coalitions to be formed. The result at the end of the process is an estimated result of the negotiation process between the multiagent systems.

C. Example A–M Bargaining Set Analysis

A three-agent system is used in this section to demonstrate the calculation of A–M bargaining sets, the core calculation in the procedure to calculate expected activities of multiple agents in a SPID framework. The calculation of the distribution of benefits described in this example would be repeated many times in estimating agent negotiation. In this example, the coalition between agents A and B is investigated with each using the threat of agent T to establish its relative bargaining position.

First, the benefit generated by the various coalitions is determined. In this example, the benefit is the reduction of load shedding vulnerability measured in megawatts. (Positive megawatts indicates a reduction in vulnerability.) Fig. 3 summarizes the benefits of the potential coalitions.

Applying the A–M bargaining set (III.2)–(III.4), the following estimates are made for the division of benefits between coalitions:

$$x_A = \frac{v(AB)+v(AT)-v(BT)}{2} = \frac{28+14-18}{2} = 12 \text{ MW}$$
$$x_B = \frac{v(AB)+v(BT)-v(AT)}{2} = \frac{28+18-14}{2} = 16 \text{ MW}$$
$$x_T = \frac{v(AT)+v(BT)-v(AB)}{2} = \frac{14+18-28}{2} = 2 \text{ MW}.$$

This division of benefits is stable in that if agent A were to try to achieve more than the 12-MW reduction in vulnerability by forming a coalition with T, agent A would have to offer T less than 2 MW in reduction. Agent B could counter the (A,T) coalition threat by offering T the same benefit in a (B,T) coalition in which B has a lower vulnerability than in the (A,B) coalition.

The proposed A–M bargaining set method is an important technique to facilitate distributed decision making by the agents through bargaining. To allow faster response by multiple agents, load shedding options are formed by agents with local and system vulnerability considerations.

IV. Flexible Grid Configuration by Partitioning to Enhance Power Infrastructure Security

Power systems become more vulnerable as they are operated closer to their limits. The potential sources of vulnerability to power infrastructure can be classified as internal and external sources. Internal sources include power system component failures, protection and control system failures, information system and communication network failures, and inadequate security assessment. External sources are natural calamities, human errors in operations, gaming in electricity markets, and sabotage [30]. Both kinds of sources may lead to catastrophic events and cascading outages. In addition to resolving the local and regional levels power disturbances and outages, the industry must begin to evaluate the possibility of the larger, more systemic, impacts of sabotage activities [7]. To minimize the potential damage caused by such radical events, the power infrastructure must be more intelligent and flexible, allowing coordinated operation and control measures to absorb the shock and minimize the impact. Therefore, new research problems need to be formulated. Once the damage is translated into its effects on the power grid components or subsystems, much of the existing techniques for power system analysis will be applicable.

Among different defense schemes, power network reconfiguration, controlled islanding, and load shedding have shown potential abilities to help power systems survive catastrophic events. By comparing with natural island formation, the advantages of forced island formation for partial system preservation and system recovery have been shown in [56]. The islands formed by controls would be more stable and less prone to disintegration than those formed naturally. Moreover, system restoration will be less complex and the overall restoration time can be reduced if the islanding scheme is well designed and operated [56]. Various islanding schemes used for captive power plants in India are introduced in [57]. Without these islanding schemes, the severe disturbance of the power grid may result in significant losses in production, damage to process equipment, and even loss of life [57]. The successful operation of an islanding protection scheme prevented the customers of the metropolitan area in Tokyo from a blackout in 1999, in which an airplane crashed and damaged a 275-kV transmission tie line [58].

The new vulnerabilities require fundamental rethinking to protect the power infrastructure from events that will cause severe impact on the society. Revolutionary concepts and technologies are urgently needed to modernize our power infrastructures. Due to the limitation of investments in upgraded existing transmission lines and other equipment, the development of "smart grid" technologies becomes more and more important. The above research results and industry operation experience [56]–[58] demonstrate that the flexible network configuration scheme can play a significant role in the defense systems against catastrophic events.

"Flexible Grid Configuration by Partitioning" is a "smart grid" technology that can be used in SPID. This technology is developed to enhance power infrastructure robustness to minimize the impact of catastrophic events. There are two promising applications for this technology:

1) partitioning power grids based on the vulnerability considerations;
2) flexible grid configuration to enhance the wide-area grid shock absorption capability.

At present, there is no systematic method for partitioning the power grids based on the vulnerability considerations. Indeed, traditional islanding occurs when the system is experiencing an emergency operating condition such as a voltage collapse. The flexible grid configuration by partitioning based on the vulnerability analysis is a new approach to planning and operation of the power grids. This approach can be used to minimize the damage or impact caused by potential catastrophic events. While risk to power infrastructure generally cannot be eliminated, enhancing protection from known or potential threats can help reduce it. For example, when the power grid is on a high-level alert, preventive actions should be taken to limit the extent of possible damage. The SPID system will construct a flexible grid configuration by partitioning to best use the available resources. In the approach, the power system is separated into self-sufficient subnetworks at a reduced capacity taking into account important aspects of restoration. Assuming a stable grid of subnetworks is established, a self-healing strategy could be used to gradually bring the power system back to its normal state when the risk level is lowered. Note that there is no power system technical problem when the security alert status is high; therefore, the flexible configuration may be maintained for an extended period until the security alert status is lowered. Partitioning the grids is an innovative idea; over the last decades the grids are usually operated as a wide-area grid with various interconnections. In the scenario of a heightened security alert that may threaten the power grids, partitioning the wide-area grids into self-sufficient subnetworks will reduce the vulnerability of the power infrastructure.

Flexible grid configuration can also be used to deal with the cascading events that may lead to catastrophic outages. The methodology of flexible grid configuration to enhance the wide-area grid shock absorption capability is detailed below.

A. Properties of Laplacian Matrix of a Graph

The definition of Laplacian Matrix $Q(G)$ of a graph G is given in [59].

Given an undirected edge-weighted graph $G = (V, E)$, where V and E are respectively the set of vertices and the set of edges of the graph, the edge-weight a_{uv} is assigned for each pair of vertices $(u, v) \in V$, the matrix $A = [a_{uv}]$, is called the adjacency matrix of the graph. Let $d(v)$ denote the degree of $v \in V$, and let D be the diagonal degree matrix indexed by V with $d_{vv} = d(v)$; the matrix $Q(G) = D - A$ is called the Laplacian Matrix of graph G.

The basic spectral properties of Laplacian Matrix $Q(G)$ are given in [59] and [60]: Let G be a weighted graph with all weights nonnegative; then:

1) $Q(G)$ has only real eigenvalues;
2) $Q(G)$ is positive semidefinite;
3) its smallest eigenvalue is $\lambda_1 = 0$, with a corresponding eigenvector with identical elements;
4) the multiplicity of zero as an eigenvalue of $Q(G)$ is equal to the number of components (connected subgraphs) of G;
5) let $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$ be the eigenvalues of $Q(G)$ in increasing order and repeated according to their multiplicity.

B. Area-Partitioning Algorithm

To implement the concept of flexible grid configurations, the determination of the subnetworks, i.e., the points of separation, for a given operating condition is critical. For convenience, these subnetworks will be referred to as areas. That is, the wide-area grid is operated as a collection of self-sufficient areas that are electrically isolated from one another. Note that these areas do not necessarily correspond to a specific power company.

A set of criteria for the determination of the physical boundary of each area has been developed in this research. For example, the inherent structural characteristics of the system should be considered in identifying the areas. An important consideration is the generation load imbalance in each area. The reduction of generation load imbalance in each area reduces the amount of load shedding to be performed. It also makes it easier for each area to match the generation and load within the prescribed frequency limit and is beneficial during restoration.

The developed area-partitioning algorithm is based on graph spectral partitioning techniques. The objective is to develop a spectral k-way partitioning algorithm, which uses the global information available in the eigenvectors and divides the power network into k disjoint areas simultaneously with the consideration of least generation load imbalance in each area. The following theorem that sets up a connection between graph spectra and "minimum ratio cuts" is proved in [61].

Theorem: The sum of the smallest k eigenvalues of Laplacian Matrix Q of a weighted graph G is a lower bound on $\sum_{h=1}^{k}(E_h/|P_h|)$ for any k-way partition of G

$$\sum_{i=1}^{k} \lambda_i \leq \min_{P \in \Pi} \sum_{h=1}^{k} \frac{E_h}{|P_h|} \tag{IV.1}$$

where $P = \{P_1, P_2, \ldots P_k\}$ is a k-way partition of the nodes of graph G, Π is the set of all k-way partitions of graph G, and E_h is the total weight of the edges in G having exactly one endpoint in P_h [61].

An advanced spectral k-way partitioning approach that involves finding the k smallest eigenvalue/eigenvector pairs is presented in [61]. These k eigenvectors are believed to provide an embedding of the graph's n vertices into a k-dimensional subspace. The cosine of the angle between the vertices in the k-dimensional embedding is used to form partitions.

Based on the graph-theoretic techniques discussed in [61]–[63], an efficient heuristic area-partitioning algorithm to separate a power system network into k areas simultaneously (k-way partitioning) with the consideration of minimizing the generation load imbalance in each area is developed. First, the power system network is modeled as a

weighted graph, whose edge weights are assigned according to the absolute values of real power flow of corresponding transmission lines. Then the Laplacian matrix of this graph is calculated. The corresponding eigenvectors of the smallest k eigenvalues of the Laplacian matrix provide an embedding of the graph's n vertices into a k-dimensional subspace. Thus, the partition matrix can be constructed from the vector consisting of the k eigenvectors. This partition matrix provides a measure of how close the n vertices are from each other. K seeds (vertices) are selected by keeping distances as far as possible from one another based on the information of the partition matrix. These k seeds are served as the k centers of the k areas. Finally, the remaining n-k vertices are assigned to the k areas according to the distances between the n-k vertices and the k centers. Some details of the algorithm are given as follows.

Step 1: *Convert the power network to an edge-weighted graph G.*

- Compute the power flow of the power system network.
- Convert the power system network into a graph G.
- Each bus of the power network is a vertex of the graph G.
- Each transmission line of the one-line power system diagram is an edge of graph G.
- The weight of each edge of graph G is assigned according to the absolute value of real power flow of the corresponding transmission line.

Step 2: *Compute the Laplacian matrix Q and its eigenvalues and corresponding eigenvectors.*

- Compute the Laplacian matrix Q of graph G.
- Compute adjacency matrix A and diagonal degree matrix D of graph G.
- The Laplacian matrix $Q = D - A$.
- Compute the k smallest eigenvalues $\lambda_1, \lambda_2, \ldots \lambda_k$ of Laplacian matrix Q.
- Compute the k eigenvectors $x_1, x_2, \ldots, x_k$, the real eigenvectors associated with $\lambda_1, \lambda_2, \ldots \lambda_k$.

Step 3: *Construct the partition vector from the first k eigenvectors of Laplacian matrix Q* [61].

- Approximate the ratioed assignment matrix by the first k eigenvectors $X = [x_1, \ldots, x_k]$.
- **The partition matrix** $\widehat{P}$ is recovered from a projector (XX^T) formed by the eigenvectors after normalization:
- $\widehat{P} = N(X)XX^TN(X)$, where $N(X)$ is a diagonal matrix with $n_{ii} = 1/\sqrt{\sum_{h=1}^{k} x_{ih}'^2}$ (n_{ii} is the reciprocal of the norm of row i of X).
- $\widehat{P}_{ij} = x_i'^T x_j'/(\|x_i'\|\|x_j'\|)$ is the cosine of the angle between the two row vectors i and j of X (or the column vectors of $X^T = [x_1', \ldots, x_k']$). These directional cosines provide a measure of how close the vertices are from each other.

Step 4: *Select k vertices to serve as the k seeds of the k partitioned areas.*

- Choose a vertex as the first seed.
- Let the vector "Seeds" store the k centers of the k partitioned areas.
- Let Seeds $= \{S_1\}$ to store the first seed as the first center.
- While $|\text{Seeds}| < k$ do as follows:
- Find a new vertex v, which satisfies $\{\max\cos(v, S_i)\}$ is minimized, i.e., the new seed is selected in such a way that the new center should be as far as possible from all the previous selected centers. The values of $\cos(v, S_i)$ are available in the Partition Matrix $\widehat{P}$.
- Store the new seed into the vector, Seeds = {Seeds} $\cup$ $\{v\}$.
- After all the k seeds are selected, the vector becomes Seeds $= \{S_1, S_2 \ldots S_K\}$, where S_i is the center of area i ($i = 1, 2, \ldots, k$).

Step 5: *Classify the remaining n–k vertices into the k areas and obtain the k partitions.*

- For $i = 1$ to $(n\text{-}k)$ do
- Find the index j, which s.t. $\cos(S_j, v_i)$ is maximized, $1 \le j \le k$. That is finding the seed S_j which has the shortest distance to the vertex v_i among all k seeds.
- Let $P = \{A_1, A_2, \ldots A_K\}$ is the area set, then area $A_j = A_j \cup \{v_i\}$.

Now the k-way partitions to separate a power system network into k areas with the consideration of minimizing the generation load imbalance in each area are obtained.

C. Flexible Grid Configuration to Enhance Wide-Area Grid Shock Absorption Capability

Many power system blackouts result from cascading events. A cascading event refers to a series of tripping initiated by one or several components failure in the power system. The initial component(s) failure could be caused by

sabotage, overcurrent, or voltage dropping. Here the initial component(s) failure is designated as "shock" to the power infrastructure. If no effective control actions are taken to absorb the shock, the initial triggering event might propagate along the wide-area grid and become a cascading event.

If a power network is passively broken into several islands, for instance, m islands, that means m eigenvalues of the Laplacian Matrix $Q(G)$ of the network become zero. It is a good idea to find the better partition points to actively separate the network into m areas, i.e., actively make m eigenvalues of the Laplacian Matrix $Q(G)$ equal to zero. The developed area-partitioning algorithm above can make use of information of the m smallest eigenvalues and their corresponding eigenvectors to partition the network into specified m areas with the consideration of least load-generation imbalance in each area. Furthermore, an optimal number K^* of areas can be determined when actively partitioning the system. The optimal K^* partition means the losses of load will be the smallest among all acceptable partitions.

The following simulation procedure is used to illustrate how flexible grid configuration can absorb the shock before the initial triggering event propagates along the wide-area grid. Assume the power flows of a base case satisfy the system operation constraints, i.e., the system is originally operating in a normal state. After a shock, the faulted transmission line or equipment will be tripped. A series of tripping might be started due to the violations of line flow constraints after the initial fault clearing action. If the area-partitioning algorithm combined with an optimal load-shedding program is applied this time, the wide-area grid will survive from the shock without losing most of load.

Step 1: *Compute the power flows based on the new network configuration after the initial tripping.*

Step 2: *Use area-partitioning algorithm to separate the system into K areas instead of tripping the lines on violation. This will prevent the initial component(s) failure from becoming a cascading event.*

- $K = 1, 2, \ldots, K^{\max}$, where $K^{\max}$ is a (specified) largest acceptable number of areas that a system can be separated into.
- Select the initially faulted bus (i.e., the bus connected by the tripped transmission line(s)) as the first seed for the area-partitioning algorithm.
- According to the information provided by the partition matrix P, find other $K - 1$ seeds and classify all the nodes into the K areas. The K seeds should keep distances from one another as far as possible, while the center of each area should be the closest seed to the nodes within its area.

Step 3: *In each of the K areas, use the optimal load-shedding program to minimize the amount of load shedding subject to the system constraints.*

- After the system is separated into K areas, it is necessary to redispatch the power and shed some load to satisfy the system constraints within each area.
- This problem can be converted to an optimization problem. For each area, the optimization is to minimize the amount of load shedding subject to the system constraints, such as the power balance of the area, the generator limits, and the line flow limits within the area.

Step 4: *For $K = 1, 2, \ldots, K^{\max}$ different scenarios, find the optimal K^* that gives the smallest loss of load. The system should be separated into K^* areas to absorb the shock.*

D. A Simulation Example

The normal configuration of the 179-bus system that resembles the WECC grid is a wide-area grid as shown in Fig. 4. The system is operating in a normal state, where all the flows satisfy system operation constraints. The system has a total generation of 61 410.33 MW and 12 325.57 MVar. It has a total load of 60 785.41 MW and 15 351.25 MVar.

Suppose there is a severe fault on the transmission line which is connected between (Bus 83–Bus 168) as indicated in Fig. 4. This line is tripped immediately to clear the fault. After the tripping, the flexible grid configuration strategy is used instead of tripping the overlimit transmission lines.

For $K = 1, 2. \ldots, 5$ different scenarios, the optimal K^* equals 2. The system is actively separated into two areas by using the area-partitioning algorithm. The faulted-line connected bus, Bus 83, is selected as the first seed. The following results are obtained from the area-partitioning algorithm:

$$\begin{aligned}
\text{Seeds} &= [\text{Bus } 83,\ \text{Bus } 168] \\
\text{Area One} &: \{\text{Bus } 30 \sim 36, 65 \sim 135, 156 \sim 157, 161 \sim 162, \\
&\qquad 168 \sim 174, 176, 178, 180\} \\
\text{Area Two} &: \{\text{Bus } 2 \sim 29, 37 \sim 64, 136 \sim 155, 158 \sim 160, \\
&\qquad 163 \sim 167, 175, 177, 179\} \\
\text{Cut Set} &= \{(\text{Edge } 156\text{-}155, \text{Edge } 156\text{-}167), \\
&\qquad (\text{Edge } 174\text{-}175, \text{Edge } 176\text{-}177, \text{Edge } 178\text{-}179)\}.
\end{aligned}$$

The Cut Set provides the points of separation. Area One has 92 buses and 117 branches. Area Two has 87 buses and 140 branches. The two areas are shown in Fig. 5.

The power flows of Area One are solved based on its network configuration. All the 35 684.71-MW loads are supplied and no line flow constraints violations are found. The power flows of Area Two are solved based on its network

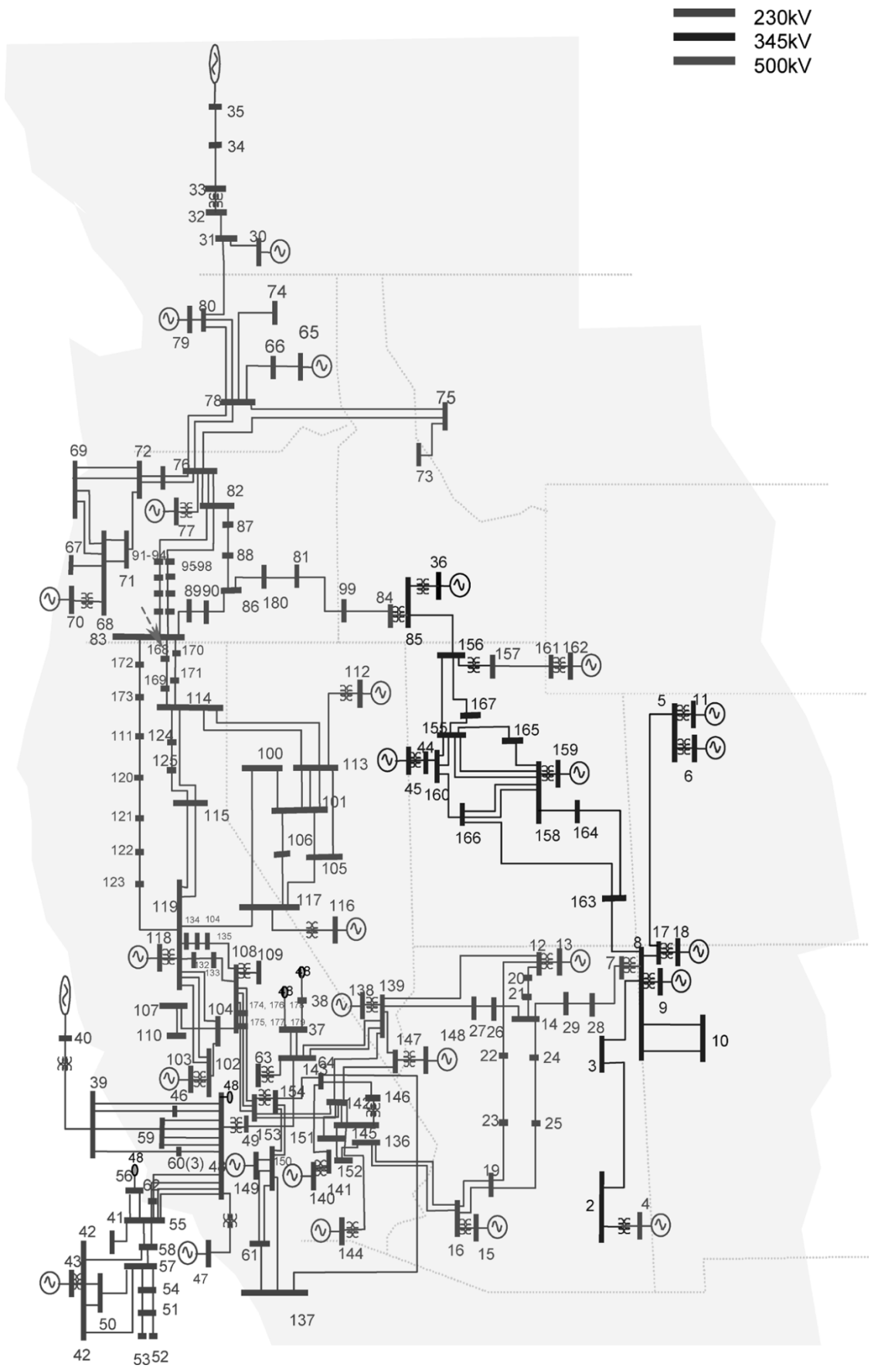

Fig. 4. WECC 179-bus system one-line diagram.

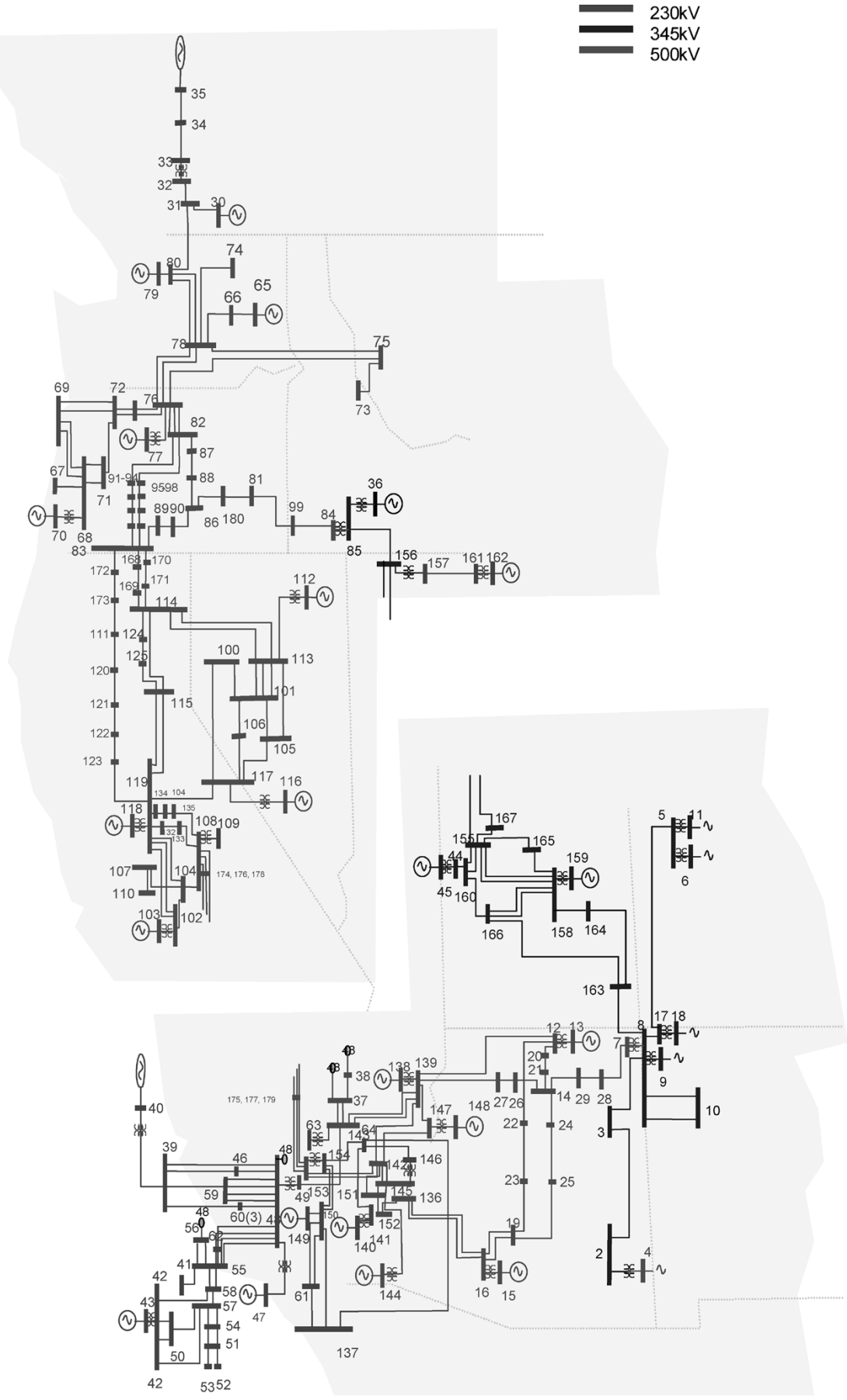

Fig. 5. Separate the WECC 179-bus system into two areas.

Table 1
Load-Shedding Results of Area Two

Bus #	*Original Load (MW)*	*Load Shed (MW)*	*Load Supplied (MW)*
8	*239*	*188*	*51*
16	*793.4*	*64.4*	*729*
154	*1066*	*60*	*1006*

configuration. Seven transmission lines of Area Two are found on limit violation.

The optimal load-shedding program is used to minimize the amount of load shedding subject to the system constraints of Area Two. Table 1 illustrates the load-shedding results.

In total, $188 + 64.4 + 60 = 312.4$ MW of load is shed in order to make Area Two satisfy its system operation constraints. Compared with the system total load of 60 785.41 MW, only $312.4\ \text{MW}/60\,785.41\ \text{MW} \times 100\% = 0.51\%$ of total load will be shed to help the system survive the catastrophic event. Without using the flexible grid configuration strategy, in this scenario, the whole system will collapse and lose most of the load due to continuously tripping the over-limit transmission lines.

The above example shows that flexible grid configuration strategy used in the SPID system can significantly enhance the power infrastructure's shock absorption capability.

V. Areas for Future Research and Development

Defense systems for complex power infrastructures require an extensive amount of research, development and implementation. Based on the state-of-the-art survey of this paper, the field is still in its early stage of maturity. The following high priority issues remain to be addressed:

- online vulnerability indicators for the power infrastructures;
- practical multiagent technologies for implementation of defense systems;
- real-time, wide-area control and protection methods;
- multiagent models and tools that allow coordination among participants in a wide-area grid;
- independencies among power, communication, and computer infrastructures;
- smart grid concepts and technologies;
- shock absorption capabilities for the wide-area power grids;
- impact of disruption on the electricity market;
- technologies for realization of flexible configurations such as voltage and frequency control for subsystems;
- online methods to stop cascading events in an early stage;
- innovative power system restoration methods in the future industry environment.

Acknowledgment

The authors would like to thank the Advanced Power Technologies (APT) Center for their support in the work on flexible reconfiguration and other techniques for power and other critical infrastructures.

References

[1] S. R. Trost, "Tools for 21st century infrastructure protection," presented at the Workshop Protecting and Assuring Critical National Infrastructure: Setting the Research and Policy Agenda, Palo Alto, CA, 1997.

[2] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE Control Syst. Mag.*, vol. 21, no. 6, pp. 11–25, Dec. 2001.

[3] W. A. Thissen and P. M. Herder, "Critical infrastructures: Challenges for systems engineering," in *Proc. 2003 IEEE Int. Conf. Systems, Man and Cybernetics*, vol. 2, pp. 2042–2047.

[4] R. Cerveny and S. Stephenson, "Managing technology of America's infrastructure," in *Proc. Portland Int. Conf. Technology and Innovation Management (PICMET '99)*, vol. 1, pp. 458–459.

[5] M. Amin, "Security challenges for the electricity infrastructure," *Computer*, vol. 35, no. 4, pp. 8–10, Apr. 2002.

[6] ——, "Evolving energy enterprise-"Grand challenges": Possible road ahead and challenges for R&D," in *Proc. IEEE Power Engineering Soc. Summer Meeting*, vol. 3, 2002, pp. 1705–1707.

[7] ——, "Modernizing the national electric power grid," in *Proc. Workshop Modernizing the National Electric Power Grid*, New Orleans, LA, 2002.

[8] T. A. Longstaff, C. Chittister, R. Pethia, and Y. Y. Haimes, "Are we forgetting the risks of information technology?," *Computer*, vol. 33, no. 12, pp. 43–51, Dec. 2000.

[9] J. Kumagai, "The web as weapon [cyberwarfare]," *IEEE Spectr.*, vol. 38, no. 1, pp. 118–121, Jan. 2001.

[10] D. A. Jones and R. L. Skelton, "The next threat to grid reliability—data security," *IEEE Spectr.*, vol. 36, no. 6, pp. 46–48, Jun. 1999.

[11] M. Masera and M. Wilikens, "Interdependencies with the information infrastructure: Dependability and complexity issues," presented at the 5th Int. Conf. Technology, Policy and Innovation, Delft, The Netherlands, 2001.

[12] H. Drucker. A technology battlefield in the 21st century. [Online]. Available: http://www.osti.gov/

[13] Å. Holmgren, S. Molin, and T. Thedéen, "Vulnerability of complex infrastructure," presented at the 5th Int. Conf. Technology, Policy and Innovation, Delft, The Netherlands, 2001.

[14] "Vulnerability assessment methodology—Electric power infrastructure," Office of Energy Assurance, U.S. Dept. Energy, Washington, DC, 2002.

[15] A. V. Gheorghe and D. V. Vamanu, "Indicators for vulnerability assessment and management of critical infrastructures," presented at the 5th Int. Conf. Technology, Policy and Innovation, Delft, The Netherlands, 2001.

[16] L. Leffler, "The NERC program for the electricity sector critical infrastructure protection," in *Proc. IEEE Power Engineering Society Winter Meeting*, vol. 1, 2001, pp. 95–97.

[17] (2001) National energy security: Implications for national energy policy. Environmental and Energy Study Institute. [Online]. Available: http://www.eesi.org/publications/10.04.01nationalsecurity.pdf

[18] G. S. Vassell, "Northeast blackout of 1965," *IEEE Power Eng. Rev.*, vol. 11, no. 1, pp. 4–8, Jan. 1991.

[19] Prevention of power failures (1967, Jul.). [Online]. Available: http://chnm.gmu.edu/blackout/archive/a_1965.html

[20] The Con Edison power failure of July 13 and 14, 1977 (1978, Jun.). [Online]. Available: http://chnm.gmu.edu/blackout/archive/a_1977.html

[21] C. W. Taylor and D. C. Erickson, "Recording and analyzing the July 2 cascading outage [western U.S. power system]," *IEEE Comput. Appl. Power*, vol. 10, no. 1, pp. 26–30, Jan. 1997.

[22] C. W. Taylor, "Improving grid behavior," *IEEE Spectr.*, vol. 36, no. 6, pp. 40–45, Jun. 1999.

[23] D. N. Kosterev, C. W. Taylor, and W. A. Mittelstadt, "Model validation for the August 10, 1996 WSCC system outage," *IEEE Trans. Power Syst.*, vol. 14, no. 3, pp. 967–979, Aug. 1999.

[24] WSCC Operations Comm.. (1996) Western Systems Coordinating Council (WSCC) Disturbance Report for the Power System Outage that Occurred on the Western Interconnection, August 10, 1996. [Online]. Available: ftp://www.nerc.com/pub/sys/all_updl/docs/pubs/AUG10FIN.pdf

[25] "The US blackout timeline," *Power Eng.*, vol. 17, no. 5, pp. 11–11, Oct.-Nov. 2003.

[26] C.-C. Liu, J. Jung, G. T. Heydt, V. Vittal, and A. G. Phadke, "The Strategic Power Infrastructure Defense (SPID) system. A conceptual design," *IEEE Control Syst. Mag.*, vol. 20, no. 4, pp. 40–52, Aug. 2000.
[27] V. X. Filho, L. A. S. Pilotto, N. Martins, A. R. C. Carvalho, and A. Bianco, "Brazilian defense plan against extreme contingencies," in *Proc. IEEE Power Engineering Soc. Summer Meeting*, vol. 2, 2001, pp. 15–19.
[28] O. Faucon and L. Dousset, "Coordinated defense plan protects against transient instabilities," *IEEE Comput. Appl. Power*, vol. 10, no. 3, pp. 22–26, Jul. 1997.
[29] G. Trudel, S. Bernard, and G. Scott, "Hydro-Québec's defence plan against extreme contingencies," *IEEE Trans. Power Syst.*, vol. 14, no. 3, pp. 958–965, Aug. 1999.
[30] J. Jung and C.-C. Liu, "Multi-agent technology for vulnerability assessment and control," in *Proc. 2001 IEEE Summer Meeting*, pp. 1287–1292.
[31] B. Qiu, Y. Liu, and A. G. Phadke, "Communication infrastructure design for Strategic Power Infrastructure Defense (SPID) system," in *Proc. IEEE Power Engineering Soc. Winter Meeting*, vol. 1, 2002, pp. 27–31.
[32] Q. Liu, J.-N. Hwang, and C.-C. Liu, "Communication infrastructure for wide area protection of power systems," in *Power Systems and Communications Infrastructures for the Future* Beijing, China, 2002.
[33] H. You, V. Vittal, and Z. Yang, "Self-healing in power systems: An approach using islanding and rate of frequency decline-based load shedding," *IEEE Transactions on Power Systems*, vol. 18, pp. 174–181, Feb. 2003.
[34] P. Cote, S.-P. Cote, and M. Lacroix, "Programmable load shedding systems Hydro-Quebec's experience," in *Proc. IEEE Power Engineering Soc. Summer Meeting*, vol. 2, 2001, pp. 818–823.
[35] D. R. Cowbourne and P. M. Murphy, "The application of system control centre computer assisted special protection systems in Ontario Hydro," in *Proc. 4th Int. Conf. Developments in Power Protection*, 1989, pp. 156–161.
[36] P. M. Anderson and B. K. LeReverend, "Industry experience with special protection schemes," *IEEE Trans. Power Syst.*, vol. 11, no. 3, pp. 1166–1179, Aug. 1996.
[37] P. Denys, C. Counan, L. Hossenlopp, and C. Holweck, "Measurement of voltage phase for the French future defence plan against losses of synchronism," *IEEE Trans. Power Del.*, vol. 7, no. 1, pp. 62–69, Jan. 1992.
[38] C. Lebrevelec, P. Cholley, J. F. Quenet, and L. Wehenkel, "A statistical analysis of the impact on security of a protection scheme on the French power system," in *Proc. 1998 Int. Conf. Power System Technology (POWERCON '98)*, vol. 2, pp. 1102–1106.
[39] D. C. Elizondo, J. de La Ree, A. G. Phadke, and S. Horowitz, "Hidden failures in protection systems and their impact on wide-area disturbances," in *Proc. IEEE Power Engineering Soc. Winter Meeting*, vol. 2, 2001, pp. 710–714.
[40] J. Hsu, G. DeShazo, and W. Wong, "Use of special protection systems to overcome power congestion in the Western United States," in *Proc. Int. Conf. Power System Technology (POWERCON '02)*, vol. 3, pp. 1339–1343.
[41] J. D. McCalley and W. Fu, "Reliability of special protection systems," *IEEE Trans. Power Syst.*, vol. 14, no. 4, pp. 1400–1406, Nov. 1999.
[42] W. Fu, S. Zhao, J. D. McCalley, V. Vittal, and N. Abi-Samra, "Risk assessment for special protection systems," *IEEE Trans. Power Syst.*, vol. 17, no. 1, pp. 63–72, Feb. 2002.
[43] E. K. Nielsen, M. E. Coultes, D. L. Gold, J. R. Taylor, and P. J. Traynor, "An operations view of special protection systems," *IEEE Trans. Power Syst.*, vol. 3, no. 3, pp. 1078–1083, Aug. 1988.
[44] J. W. Senders, "Tampering in nuclear power plant control rooms: Human factors issues," in *Conf. Rec. 1988 IEEE 4th Conf. Human Factors and Power Plants*, 1988, pp. 454–459.
[45] M. Aristizabal and S. Cortez, "Transmission line restoration techniques in Colombia, South America," in *Proc. 6th Int. Conf. Transmission and Distribution Construction and Live Line Maintenance*, 1993, pp. 293–307.
[46] G. P. Lekkas, N. M. Avouris, and G. K. Papakonstantinou, "Development of distributed problem solving systems for dynamic environments," *IEEE Trans. Syst., Man, Cybern.*, vol. 25, no. 3, pp. 400–414, Mar. 1995.
[47] R. L. Grossman, A. Nerode, A. P. Ravn, and H. Rischel, *Hybrid Systems*. Berlin, Germany: Springer-Verlag, 1993.
[48] V. Vishwanathan, J. McCalley, and V. Honavar, "A multiagent system infrastructure and negotiation framework for electric power systems," presented at the 2001 IEEE Power Tech Conf. , Porto, Portugal.
[49] J. A. Hossack, J. Menal, S. D. J. McArthur, and J. R. McDonald, "A multiagent architecture for protection engineering diagnostic assistance," *IEEE Trans. Power Syst.*, vol. 18, no. 2, pp. 639–647, May 2003.
[50] G. P. Azevedo, B. Feijo, and M. Costa, "Control centers evolve with agent technology," *IEEE Comput. Appl. Power*, vol. 13, no. 3, pp. 48–53, Jul. 2000.
[51] S. Talukdar, V. C. Ramesh, R. Quadrel, and R. Christie, "Multiagent organizations for real-time operations," *Proc. IEEE*, vol. 80, no. 5, pp. 765–778, May 1992.
[52] T. Nagata and H. Sasaki, "A multi-agent approach to power system restoration," *IEEE Trans. Power Syst.*, vol. 17, no. 2, pp. 457–462, May 2002.
[53] I. Praca, C. Ramos, Z. Vale, and M. Cordeiro, "Mascem: A multiagent system that simulates competitive electricity markets," *IEEE Intell. Syst.*, vol. 18, no. 6, pp. 54–60, Nov.-Dec. 2003.
[54] J. Jung, C.-C. Liu, S. L. Tanimoto, and V. Vittal, "Adaptation in load shedding under vulnerable operating conditions," *IEEE Trans. Power Syst.*, vol. 17, no. 4, pp. 1199–1205, Nov. 2002.
[55] P. D. Straffin, *Game Theory and Strategy*. Washington, D.C.: Mathematical Assoc. Amer., 1993.
[56] B. A. Archer and J. B. Davies, "System islanding considerations for improving power system restoration at Manitoba Hydro," in *Proc. IEEE Canadian Conf. Electrical and Computer Engineering (CCECE 2002)*, vol. 1, pp. 60–65.
[57] K. Rajamani and U. K. Hambarde, "Islanding and load shedding schemes for captive power plants," *IEEE Trans. Power Del.*, vol. 14, no. 3, pp. 805–809, Jul. 1999.
[58] S. Agematsu, S. Imai, R. Tsukui, H. Watanabe, T. Nakamura, and T. Matsushima, "Islanding protection system with active and reactive power balancing control for Tokyo metropolitan power system and actual operational experiences," in *Proc. 7th IEE Int. Conf. Developments in Power System Protection*, 2001, pp. 351–354.
[59] B. Mohar *et al.*, "The Laplacian spectrum of graphics," in *Graph Theory, Combinatorics, and Applications*, Y. Alavi *et al.*, Eds. New York: Wiley, 1988, pp. 871–898.
[60] M. Fiedler, "Algebraic connectivity of graphs," *Czechoslovak Math. J.*, vol. 23, no. 98, pp. 298–305, 1973.
[61] P. K. Chan, M. Schlag, and J. Zien, "Spectral K-way ratio-cut partitioning and clustering," *IEEE Trans. Computer-Aided Design Integr. Circuits Syst.*, vol. 13, no. 9, pp. 1088–1096, Sep. 1994.
[62] L. Hagen and A. B. Kahng, "New spectral methods for ratio cut partitioning and clustering," *IEEE Trans. Computer-Aided Design Integr. Circuits Syst.*, vol. 11, no. 9, pp. 1074–1085, Sep. 1992.
[63] T. F. Chan, P. Ciarlet Jr., and W. K. Szeto, "On the optimality of the median cut spectral bisection graph partitioning method," *SIAM J. Comput.*, pp. 943–948, 1997.

Hao Li (Member, IEEE) received the B.S.E.E. and M.S.E.E. degrees from Tsinghua University, Beijing, China, in 1996 and 1999, respectively, and the Ph.D. degree in electrical engineering from the University of Washington, Seattle, in 2004.

During 2002, he worked as a Power Systems Engineer in Technical Operations at the Bonneville Power Administration (BPA). He joined AREVA T&D Inc., Bellevue, WA, in 2004. His research interests include intelligent system applications to power systems and power system economics.

Gary W. Rosenwald (Member, IEEE) received the B.S. and Ph.D. degrees in electrical engineering from the University of Washington, Seattle, in 1992 and 1996, respectively.

He joined AREVA T&D Inc., Bellevue, WA, in 2001. His current research focus is on development and implementation of deregulated electricity market solutions.

Juhwan Jung (Member, IEEE) received the Ph.D. degree from the University of Washington, Seattle, in 2002.

He is currently with LS Industrial Systems, Seoul, Korea. His research interests include power systems and artificial intelligence system applications

Chen-Ching Liu (Fellow, IEEE) received the Ph.D. degree from the University of California, Berkeley, in 1983.

Since 1983, he has been with the University of Washington, Seattle, where he is a Professor of Electrical Engineering and Associate Dean of Engineering.

Dr. Liu received an IEEE Third Millennium Medal in 2000 and the IEEE Power Engineering Society Outstanding Power Engineering Educator Award in 2004. He serves as Chair of the Technical Committee on Power System Analysis, Computing and Economics (PSACE), IEEE Power Engineering Society. He led the Advanced Power Technologies (APT) Consortium, consisting of Arizona State University, Iowa State University, Virginia Tech, and the University of Washington, that completed the conceptual design of the Strategic Power Infrastructure Defense (SPID) system sponsored by the Electric Power Research Institute (EPRI) and the U.S. Department of Defense.