Cybersecurity for Critical Infrastructures: Attack and Defense Modeling

Chee-Wooi Ten, *Student Member, IEEE*, Govindarasu Manimaran, *Senior Member, IEEE*, and Chen-Ching Liu, *Fellow, IEEE*

***Abstract*—Disruption of electric power operations can be catastrophic on national security and the economy. Due to the complexity of widely dispersed assets and the interdependences among computer, communication, and power infrastructures, the requirement to meet security and quality compliance on operations is a challenging issue. In recent years, the North American Electric Reliability Corporation (NERC) established a cybersecurity standard that requires utilities' compliance on cybersecurity of control systems. This standard identifies several cyber-related vulnerabilities that exist in control systems and recommends several remedial actions (e.g., best practices). In this paper, a comprehensive survey on cybersecurity of critical infrastructures is reported. A supervisory control and data acquisition security framework with the following four major components is proposed: 1) *real-time monitoring*; 2) *anomaly detection*; 3) *impact analysis*; and 4) *mitigation strategies*. In addition, an attack-tree-based methodology for impact analysis is developed. The attack-tree formulation based on power system control networks is used to evaluate *system*-, *scenario*-, and *leaf*-level vulnerabilities by identifying the system's adversary objectives. The leaf vulnerability is fundamental to the methodology that involves port auditing or password strength evaluation. The measure of vulnerabilities in the power system control framework is determined based on existing cybersecurity conditions, and then, the vulnerability indices are evaluated.**

***Index Terms*—Attack tree, cybersecurity, defense systems, power system control, security vulnerability.**

I. Introduction

CRITICAL infrastructures are complex physical and cyber-based systems that form the lifeline of a modern society, and their reliable and secure operation is of paramount importance to national security and economic vitality. In most sense, the cyber system forms the backbone of a nation's critical infrastructures, which means that a major security incident on cyber systems could have significant impacts on the reliable and safe operations of the physical systems that rely on it. The recent findings, as documented in government reports [1]–[7], indicate the growing threat of physical and cyber-based attacks in numbers and sophistication on electric grids and other critical infrastructure systems. The focus of this paper is the cybersecurity of an electric power infrastructure. The three modes of malicious attacks on power infrastructure are as follows: 1) attack upon the system; 2) attack by the system; and 3) attack through the system [8].

Physical security of the power infrastructure has been recognized by the power community as an important issue. One example precaution was to prevent vandalism on unmanned substations [9]. Due to the growing concern over the potential sabotage, the focus of physical security has been broadened to incorporate critical substations that may result in cascading effects, leading to a wide-area blackout [10]. The application of sensors to monitor the structural health of transmission lines is also an important way to reduce the power system vulnerability [11]. Electronic security is as important as physical security due to the potential impact that can be made through operations of critical cyberassets. Electronic security here refers to the security of critical cyberassets of the power infrastructure. It includes the supervisory control and data acquisition (SCADA) systems that are widely used in the industry for monitoring and control of the power grid. These systems include computer and communication devices installed in power plants, substations, energy control centers, company headquarters, regional operating offices, and large load sites. Cybersecurity of critical infrastructures systems encompasses three major control systems. SCADA systems are the central nerve system of a wide-area control network that constantly gathers the latest status from remote units [1]. A process control system (PCS) is implemented with a closed-loop control for an ongoing task. A distributed control system (DCS) is the complex combinations of SCADA and PCS. Fundamental materials about SCADA are further detailed in [3], [12], and [13]. A variety of communication systems are deployed on the power grid for the purpose of monitoring and control. The analog and status data acquired by SCADA are utilized by an energy management system (EMS) in the control center to perform a wide range of system functions, including real-time control. The communication system for wide-area protection and control of a power system can be weakened due to component failures or communication delays [14]. Failure of an important communication channel in the operational environment could result in an inability to control or operate important facilities, leading to possible power outages. Other than the communication between the control center and substations that has long been established, the inter-control center communication through the Internet serves as the data exchange mechanism between interconnected networks [15]. Analyzing the events at the interfaces between power and

Manuscript received July 2, 2008. Date of publication June 3, 2010; date of current version June 16, 2010. This work was supported by the Electric Power Research Center, Iowa State University. The authors would also like to acknowledge partial support by the Science Foundation Ireland (SFI) and U.S. National Science Foundation (NSF). This paper was recommended by M. Ulieru.

C.-W. Ten and C.-C. Liu are with the School of Electrical, Electronic and Mechanical Engineering, University College Dublin, National University of Ireland, Belfield, Dublin 4, Ireland (e-mail: cheewooi.ten@ucd.ie; liu@ucd.ie).

G. Manimaran is with the Department of Electrical and Computer Engineering, Iowa State University, Ames, IA 50010 USA (e-mail: gmani@iastate.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSMCA.2010.2048028

telecommunication systems is an important way to understand their dependences [16]. The use of standard protocols on critical systems leads to a source of vulnerability [17].

Due to technological changes over the last decade, protocols have been refined to become more flexible in their interoperability and maintainability, specifically in an open architecture with high-speed communications [12], [18]. The evolution of SCADA systems has also raised concerns about cyber-related vulnerabilities [2], [13]. In addition, interdependences among computers, communication, and power infrastructures have increased the risks due to complexity of the integrated infrastructures [19]. Although the complex infrastructure provides great capabilities for operation, control, business, and analysis, it also increases security risks due to cyber-related vulnerabilities. Technological advances can help to reduce the deficiencies of current power and communication systems [20]. However, technological complexity can also lead to security breaches that are prone to electronic intrusions. A successful intrusion into the control networks can lead to undesirable switching operations executed by attackers, resulting in widespread power outages. Another potential scenarios are intrusion into one or more substations and alteration of the protective relay settings, which could result in undesirable tripping of circuit breakers. The vulnerabilities of a power system include three main components, i.e., computer, communication, and power system [21]–[24]. Attacks can be targeted at specific systems, subsystems, and multiple locations simultaneously from a remote location. Entities in the control center, substation automation system (SAS) [25], [26], distribution management system, Independent System Operator (ISO), and power plant process control system [27]–[31] are interlinked. Interdependence plays an essential role in vulnerability assessment. An enhanced authentication process on the critical cyberassets, such as access to certain control functions, should be validated through the biometric features of an individual [32].

Security awareness for emerging technologies is critical to prevent cyberattacks. Information security in an open system architecture, with respect to potential threats and goals (in terms of confidentiality, integrity, availability, and accountability), is a challenging task [33]. ISO/IEC 17779 recommends a list of important controls on the information security management system [34]. A virtual enterprise is one way to promote a collaborative group of managing existing network enterprises by coordinating, controlling, and communicating remotely to the networks with different roles and user types [35]. Governments have responded by increasing national readiness as the connectivity of control networks increases [4]. Vulnerability assessment for process control systems has been recognized as an important task that has an impact on power system operation [36], [37]. The International Electrotechnical Commission Technical Council (IEC TC 57), i.e., power system management and associated information exchange, has advanced the standard communication protocol security in IEC62351 with stronger encryption and authentication mechanisms [38]. Such mechanisms allow verification and evaluation of potential threats. Aside from the deficiencies of the communication architecture on availability, scalability, and quality of service in real time, a new approach has been envisioned for strengthening power grid in terms of security, efficiency, and reliability [39], [40].

The observation of computer intruder activities by the U.S. Computer Emergency Readiness Team (US-CERT) has been undertaken since the late 1980s. The sophistication of attack trends has advanced from automated to highly firewall-permeable and distributed fashions [41]. Increasingly sophisticated tools help to penetrate existing network connections [42]. Reference [7] identifies the latest cybersecurity technologies for protection. The findings in a 2004 report from the Government Accountability Office (GAO) [3] highlight the extensive plans of sabotage to disrupt the U.S. power grid. A survey conducted by electric utilities indicates the growing concern over the attacks on power grid through communication security breaches. Intrusion into the control networks remains the highest concern based on the survey [43]. Recent computer crime and security surveys from the Computer Security Institute (CSI) indicate that the system penetration by outsiders may cause high financial losses [44]. Specifically, it is the third highest financial loss among other attack types based on the 2007 survey. Due to the fast-growing intrusion attempts through cyberspace, the analysis of direct and indirect cybervulnerabilities and cyberthreats is important. The analysis identifies the possible consequences and measures to prevent them from attacks [45]. Awareness programs about exploited vulnerabilities are set up to improve the control system security [46]. Initiatives addressing the critical infrastructures have been established by US-CERT, i.e., national SCADA test beds [47], [48]. Traditional IT solutions may not be well positioned to control systems in which CERT and national test beds are set up for strengthening the defense for the domain-specific purpose [49]. The initial intention of the American Gas Association 12 Task Group is to establish the protection guidelines for gas SCADA systems [50]. The guidelines have been applied to water and electricity SCADA systems due to technical and operational similarities. The compliance set by North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection has established permanent policies for utilities in the U.S. that are helpful for the reduction of risks from a compromise of critical cyberassets [51], [52]. A comparison between compliance standards of power entity and other similar SCADA systems has been reported in [6] and [53]. Research on information security has stressed on modeling dependability [54] and risk assessment framework [55], [56]. A new paradigm for classification of the security level using declustering in database is introduced [57]. Correlation is also a technique to identify intrusion into a network [58]. A game approach to modeling of response strategies for attackers and administrators is used as a technique to enhance network security [59].

II. SCADA Security Framework

A strategic roadmap framework has been developed to address the security issue in a proactive manner [1], [60], [61]. To assess the information security of control systems, it is useful to quantify the resiliency of a power grid in terms of threats and the impact that they can make. Interdependence modeling with computer and communication infrastructures is useful for determination of the system bottleneck [62], [63]. Security system engineering deals with adversary models that describe attack objectives and relevant impact/mission based on hypotheses [64]. The key is to identify the system properties.

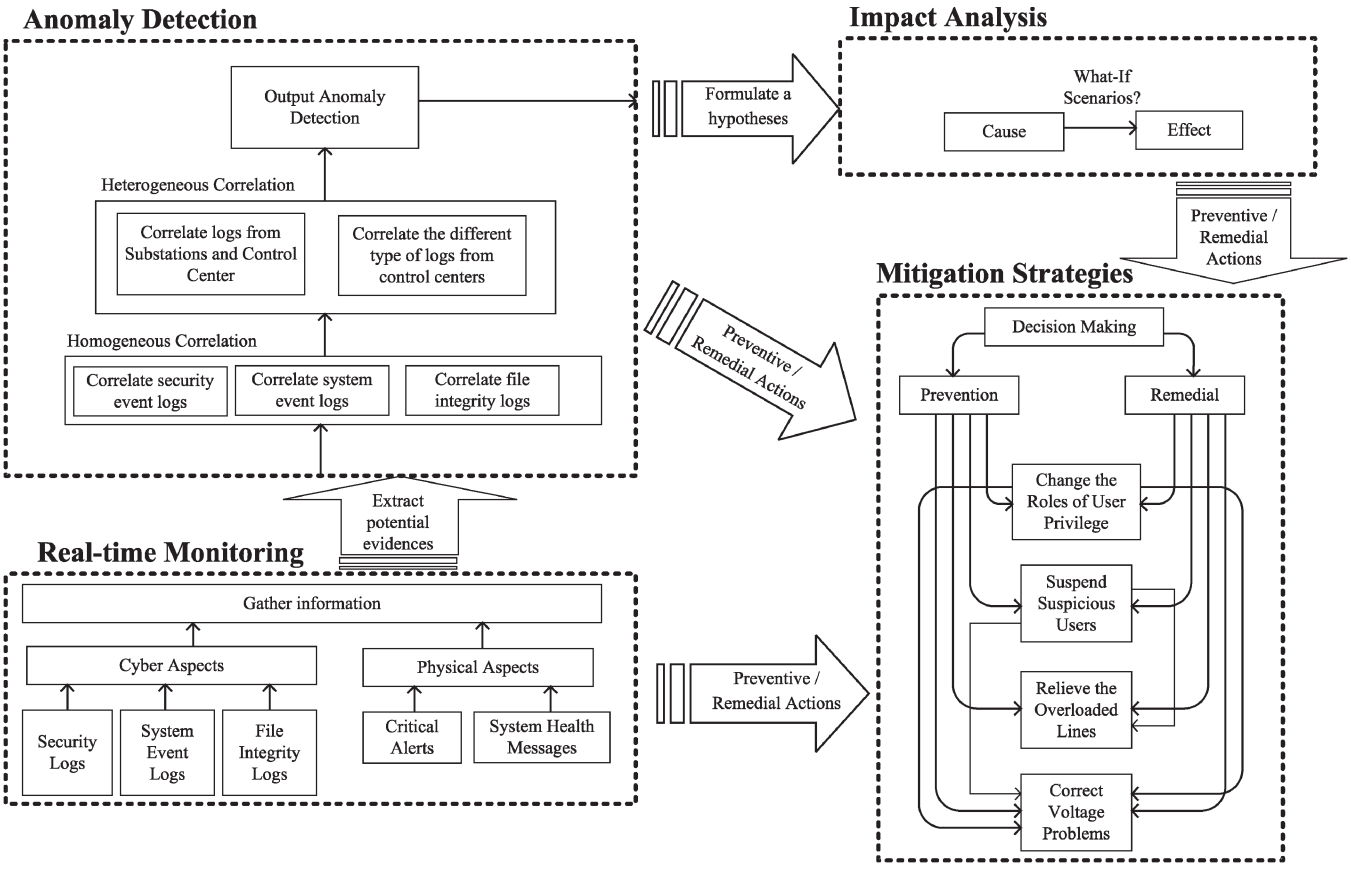

Fig. 1. Proposed SCADA Security Framework: RAIM Framework.

Understanding of the mission impact facilitates analytical evaluation of the interdependences among infrastructures that can hinder the effectiveness of attack modeling [65]. Analysis of the economic impact helps to identify the appropriate measures that mitigate risks at pivotal network nodes [66], [67].

Fig. 1 shows the proposed security SCADA framework, which encompasses four key components: 1) *real-time monitoring*; 2) *anomaly detection*; 3) *impact analysis*; and 4) *mitigation strategies* (RAIM). Each of the key components will be elaborated next.

A. Real-Time Monitoring

A variety of information networks are interconnected to the electric power grid for the purposes of sensing, monitoring, and control [68], [69]. These information networks are closely associated with the SCADA system. The environment of a SCADA system involves a control center, intelligent electronic devices (IEDs) at substations, distributed sensors that measure electrical and other quantities on the network, and a variety of communication links between the control center and substations. These communication links are wireline circuits, microwave channels, or power-line carrier channels. As mentioned, the data acquired through the SCADA system are utilized in the EMS for a wide range of system operation and real-time control functions.

Denial-of-service (DoS) attacks are among the most detrimental, which affect computer and communication performance through resource exhaustion in terms of compute cycles, buffers, and communication bandwidth [69]. A typical resource exhaustion attack, such as a packet flooding attack, involves compromised machines sending a large number of spurious packets to a target server(s) and/or network, which is the potential victim. In addition, there have been large-scale worm propagation activities in recent years that consume a significant amount of compute and network resources, causing disruptions to information infrastructure systems. DoS attacks have evolved to distributed forms [70]. Building a norm profile is essential to detect various flooding attacks by identifying the changes from normal activities. Information and communication infrastructures that are integral parts of the electric power system are not exempt from this potential trend and the consequences. In fact, these issues are more pronounced in critical infrastructure systems due to the legacy nature of the information/communication technologies used therein and the catastrophic nature of the consequences. For example, a DoS attack on power infrastructure elements such as the substation, control center, or the communication network can have a serious effect on the SCADA system and the associated critical functions. These functions include state estimation, alarm processing, and preventive or emergency controls. Resource-exhaustion-based DoS attacks could come in the following forms in an electric power grid environment.

1) They slow down or bring down the control center network, causing degradation in its real-time control performance.
2) They slow down or bring down SASs, causing degradation in real-time sensing and actuation performance.

3) Congest the forward and/or backward communication paths, causing the communication latencies to exceed the limit that can be tolerated for real-time SCADA operation.

Resource-exhaustion-based DoS attacks can be launched even if control centers and substations are fully secured by the latest security technologies and secure versions of SCADA protocols. Examples of secure versions are Modbus and Inter-Control Center Communication Protocols (ICCP) [15].

B. Anomaly Detection

Anomaly detection is based on event correlation techniques to systematically establish the relationship between statistical data sets from various sources. This is an approach to extract and analyze the audit data from power instruments and cyber-related logs to distinguish if a threat is credible [41]. Event correlations can be categorized as follows: 1) *temporal*; 2) *spatial*; or 3) *hybrid*. These combinations introduce a different perspective of threats that may capture local or global abnormality [71], [72].

Sources in SASs that can be correlated in the substation-level (local) and control center (global) networks include the following : 1) relay setting of IEDs [73], [74]; 2) user credentials and application logs; 3) traffic logs, such as volume within local and global networks; and 4) status of running applications. An adaptive anomaly detection strategy to deal with the incomplete data is essential, particularly to identify intentional deception or data errors [75]. Threats such as actual intrusions, intrusion attempts, or DoS shall be inferred through correlation analysis. The correlations that may be applied to the power infrastructure are as follows.

1) *Temporal correlation*: This is a data extraction from a local environment that can be learning- or rule-based by training the instrumental devices to detect the malicious modification in relay settings. There has been a work by Su *et al.* [74] that introduces the intelligence to detect if the relay settings can be altered by amplifying the measurements from voltage or current transformers. However, such an implementation has only considered limited perspectives of abnormality, which can be refined through correlations among other local sources. Extension of the hypotheses is possible.
2) *Spatial correlation*: This involves properties for the analysis of events occurring in multiple substations, in control centers, or at substations and control centers. This is to ensure a higher security level when a system is under sophisticated attacks that may lead to significant economic losses and equipment damage.
3) *Hybrid correlation*: The hybrid approach combines both temporal and spatial correlations to determine and compare the likelihood of the attacks' severity. This can refine the correlation hypothesis, depending on the credibility of the current conditions from the various sources.

To perform anomaly detection and associated impact analysis, the various system logs of the SCADA network need to be periodically monitored and correlated. The system logs include the following:

1) *Communication systems*: Status of the communication server to all IEDs, such as communication link failure (temporary or permanent), or degradation of the expected throughput. An idle connection that has been made over the allowed time frame should also be reported. Detection of DoS by determining the maximum number of connections allowed by considering the number of simultaneous connections or at a different time frame. An irregular frequency and volume of usage on a specific application should be included.
2) *Computer systems*: Alarms of intrusion attempts with respect to the attempt frequency to each system. The number of reset, shutdown, or stopping (dead heartbeat) system applications or controllers, including timestamps on all relevant events. The system should alert a computer permanent failure.

The system logs for vulnerability assessment can be obtained either from real SCADA environments or from a SCADA testbed platform that emulates various SCADA functions.

C. Impact Analysis

Impact analysis is the task to analyze the intrusion behaviors and evaluate the consequences of a cyberattacks on the SCADA system [76]–[79]. The proposed method is used to assess the vulnerability of computer networks and power systems, possibly the potential loss of load in a power system as a result of a cyberattacks. A compromised cybersecurity of a SCADA system can cause serious damage to a power system if the attack is able to launch disruptive switching actions leading to a loss of load or equipment damage. This is particularly troublesome if the attack can penetrate the control center network that is connected to substations under the SCADA system. An integrated risk modeling approach that captures both power control system vulnerabilities and the resulting impacts on the real-time operation of the power system was proposed in [80]. The methodology has the following four key steps.

1) *Cybernet*: Network that incorporates combinations of intrusion scenarios into the SCADA system. The cybernet captures the system configuration, authentication, firewall model, and login/password model. The transition rates of the cybernet are obtained by statistical analysis of system logs. The steady-state analysis of cybernet provides the intrusion probability for each scenario.
2) *Power flow simulation*: The steady-state behavior of a power system under a cyberattacks can be studied using intrusion models and power flow simulations. This evaluation of a power system under cyberattacks can be performed by isolating the compromised subsystems. Failure to obtain a power flow solution is an indication of a major impact that may lead to a power system collapse. The impact of isolating a substation in the overall system is measured by an impact factor corresponding to the substation.

3) *Vulnerability index calculation*: The scenario vulnerability index is computed as the product of steady-state intrusion probability for the scenario (obtained through cybernet analysis) and the impact factor of the component (obtained through power flow simulation). The maximum among the scenario vulnerability indices is used as the system vulnerability index.
4) *Security improvements*: Improve the cybersecurity of the SCADA system based on vulnerability assessment results with the available technologies. This improvement can produce different probabilities that will be used in the quantitative analysis.

D. Mitigation Strategies

The output of the event correlation and hypothesis formation shows the risks. The likely scenarios will undergo an impact analysis to study the severity of risks. If the associated risk is high in terms of the loss of load [80], equipment damages (costly devices such as generators and transformers), or other forms of economic losses, then suitable control actions will be initiated to prevent/mitigate the risks. The nature of the prevention/mitigation techniques depends on the following nature of risk: 1) *intrusion attempts*; 2) *intruded scenario*; or 3) *ongoing DoS attack* [68]. In case of an intrusion attempt, suitable security improvements need to be made at the most vulnerable components of the system that are associated with the identified vulnerability scenario. The most vulnerable components of a scenario can be identified through tracing the path (sequence of events) in risk modeling. Implementation of the proposed framework can be evaluated through test-bed studies to quantify cyber-based vulnerabilities and associated risks in power systems and to also evaluate the effectiveness of risk mitigation under realistic and sophisticated attack scenarios [81]–[83]. A recovery strategy helps to mitigate the cyberattacks with self-healing mechanisms [61].

III. Attack-Tree Modeling

The contribution of this paper is a new algorithm for evaluation of cybersecurity incorporating both password policies and port auditing. The algorithm has been implemented as a software prototype. A case study of the proposed algorithm is simulated and reported in Section V. As shown in the previous section, impact analysis is a way to evaluate the consequences of an attack. Attack trees are simplified methodologies for impact analysis of a computer network system by identifying the adversary objectives. The exploitability index introduced in [63] has associated a system profile with hypotheses. The risk assessment methodology is based on the relevance and priority with a list of hypothesized failures, which is formulated in accordance with the given weight to the probable consequence events. The proposed methods in this paper provide a similar framework to identify system dependences of SCADA systems without including the outage costs.

An attack tree is a graph that connects more than one attack leaf from each node [84]–[88]. An attack tree may consist of a multilevel hierarchy in a predecessor–successor structure that captures the possible ways to achieve subgoals. The top node of an attack tree is the ultimate goal with combinations of subgoals. Each attack leaf may include one or more defense nodes that are direct successors of the attack leaf. Defense nodes provide countermeasures. An attack leaf can be an element of different intrusion scenarios, depending on the node connectivity associated with it. The predecessors of each attack leaf are nodes that are attributed with logic operators "AND" or "OR." Each predecessor node is specific for the given leaf node. Fig. 2 shows attack trees with "AND" and "OR" configurations. All leaves leading to an "AND" box will have to be penetrated in order to move up the attack tree, i.e., a subsystem has been penetrated. On the other hand, in Fig. 2(b), if one of the attack leaves is penetrated, it is sufficient to move up the attack tree.

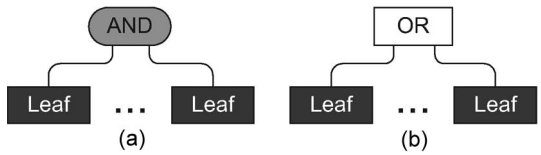

Fig. 2. Attack leaves with "AND" and "OR." (a) Attack leaf with logic operator "AND." (b) An attack leaf with logic operator "OR."

TABLE I
RULES FOR CONDITIONS 1, 2, AND 3

Condition 1	The system is free of intrusion attempt that is concluded from the electronic evidences in the system.
Condition 2	At least one or more countermeasures are implemented to protect an attack leaf.
Condition 3	At least one or more password policies are enforced corresponding to each attack leaf.

A. Introduction to the Methodology

A cybersecurity vulnerability index is a measure of the likelihood that an attack tree or attack leaf will be compromised by hackers. Each attack leaf may have weaknesses that are prone to attacks. The vulnerability index ranges from 0 to 1, from the most invulnerable (0 value) to the most vulnerable (1 value). There are separate vulnerability indices for each attack leaf and each intrusion scenario. There is also an overall system vulnerability index. All indices range from 0 to 1.

A vulnerability index is determined based on the following factors: 1) evidence of attempted intrusions; 2) existing countermeasures and improved countermeasures; and 3) password policy enforcement. The vulnerability index is evaluated with the hypothesis listed in Table I. Three conditions are defined in Table I. Condition 1 states that there is no evidence to suggest that there are intrusion attempts for the system. Condition 1 is not met when there are credible pieces of evidence of malicious attempts based on electronic data. Condition 2 is met when there are one or more countermeasures implemented for an attack leaf. Any technology that is applied to defend the attack leaf would satisfy condition 2. An example is a web server installed with a firewall that monitors the access to prevent malicious intrusions through online traffic. Password implementation for each attack leaf is considered for assessment. Poor password practices result in unauthorized access. A system can face the risks of unauthorized access, even though it may be password protected. Conditions 2 and 3 may influence condition 1.

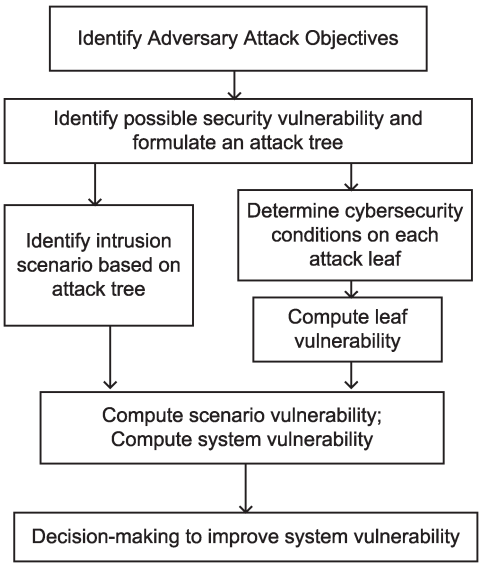

Fig. 3. Procedure to evaluate vulnerability indices.

IV. Vulnerability Assessment of Cybersecurity

The procedure to evaluate vulnerability indices is shown in Fig. 3. As shown in the figure, the procedure starts with an analysis of the attack objectives. Then, the attack tree and countermeasures are established. The system vulnerability index is obtained by evaluating the scenario vulnerability and the leaf vulnerability for the selected scenarios and the corresponding attack leaves. This section describes the procedure to evaluate the vulnerability indices: 1) cybersecurity conditions and 2) evaluation of vulnerability indices.

A. Cybersecurity Conditions

This section evaluates the cybersecurity conditions (χ), which is a preliminary evaluation before the specific vulnerability indices related to leaves and scenarios are calculated. The cybersecurity condition assessment is based on technological countermeasures and enforcement of the password policy.

The cybersecurity condition is measured by a number χ, which assumes the value of 0.33, 0.67, or 1. A low value indicates that the system condition is invulnerable, while the value 1 indicates that the system is vulnerable.

1) $\chi = 0.33$: If [(Condition 1) AND (Condition 2) AND (Condition 3)], then $= 0.33 \rightarrow$ All conditions in Table I are satisfied. Advanced countermeasures are deployed, and comprehensive password policies are enforced. There is no evidence that the system is subject to malicious attempts.
2) $\chi = 0.67$: If $\langle$ [(Condition 1) AND (Condition 2)] OR [(Condition 1) AND (Condition 3)] OR [(Condition 2) AND (Condition 3)] $\rangle$, then $= 0.67 \rightarrow$ Any two of the conditions in Table I are satisfied.
3) $\chi = 1.00$: If ([(Condition 1) OR (Condition 2) OR (Condition 3)] OR (None of the conditions)], then $= 1.00 \rightarrow$ Only one or none of the conditions is met.

For instance, implementation of the new technological countermeasures can reduce the likelihood of intrusions. Applying boundary protection in a firewall with a set of rules can also reduce access from anonymous users. This would reduce attempted intrusions and enhance system security. Detection of a potential intrusion attempt but without reinforcing at least one password policy results in $\chi = 0.67$, i.e., true for conditions 1 and 3 but not for condition 2. The other example is that condition 3, with stronger password policies, would also protect the system from being compromised (in this case, it would be $\chi = 0.33$ as only condition 1 is true). However, this does not change the number of attempts.

B. Evaluation of Vulnerability Indices

This section is concerned with the cybersecurity vulnerability of an attack tree. There are four steps to assess the security vulnerability: 1) identifying the intrusion scenarios; 2) evaluating vulnerability indices for the system, intrusion scenarios, and attack leaves; 3) port auditing; and 4) password strength evaluation.

1) Identifying the Intrusion Scenarios From the Attack Tree: First, the intrusion scenarios from the attack tree are identified. Then, the possible intrusion scenarios are enumerated. Each of the intrusion scenarios is the combination of attack leaves that are formed with "AND" or "OR" attributes configured in the attack tree. The leaf vulnerability index $v(G_k)$ of each attack leaf is evaluated once all the intrusion scenarios are determined. The scenario vulnerability is the product of the corresponding attack leaf vulnerabilities.

2) Evaluating Vulnerability Indices: There are three security vulnerability indices: 1) system vulnerability; 2) scenario vulnerability; and 3) leaf vulnerability. The system vulnerability (V_S) is the vulnerability of an attack tree determined from the scenario vulnerability, as shown in (1). K is the total number of intrusion scenarios. A vector of scenario vulnerabilities is given in (2), where $I = \{i_1, i_2, \ldots, i_K\}$ is a set of intrusion scenarios. The index V_S is the maximum value over the scenario vulnerability set. Each intrusion scenario is a possibility that leads to successful penetration of the system. The vulnerability of a scenario is the product of leaf vulnerabilities, where each scenario vulnerability is formed with a different subset of S. Scenario vulnerability indices are given in (2), where $s_1, s_2, \ldots, s_k \in S$ and $S = \{1, 2, \ldots, n\}$

$$V_s = \max\left(\mathbf{V}(I)\right) \tag{1}$$

$$\mathbf{V}(I) = \begin{pmatrix} V(i_1) & V(i_2) & \cdots & V(i_K) \end{pmatrix}^{\top} = \begin{pmatrix} V(i_1) = \prod_{j \in s_1} v(G_j) \\ V(i_2) = \prod_{j \in s_2} v(G_j) \\ \vdots \\ V(i_K) = \prod_{j \in s_K} v(G_j) \end{pmatrix}. \tag{2}$$

A leaf vulnerability is evaluated by incorporating the strengths of the implemented countermeasures, such as auditing the ports v_α and password combination v_β in a computer. The cybersecurity condition χ must be identified first. The basis for evaluation is to predetermine the leaf vulnerability condition with respect to the evidence of attempted intrusions, technological countermeasures, and password policy enforcement, which was discussed in Section IV-A. Password policies and port auditing on computer systems are important elements of the

proposed analytical method. In this model, both elements are combined for assessment of the leaf vulnerability

$$v(G) = \chi \cdot \max\langle v_\alpha, v_\beta \rangle. \tag{3}$$

The leaf vulnerability index is the maximum value between port and password vulnerability.

3) Port Auditing: Port auditing ensures that a computer system is free from malicious threats that can lead to a system compromise. This includes local security checks, root access, remote file access, default account, Trojan horse, worm, or possible backdoor. In the vulnerability test, the vulnerability of the port is categorized into four levels, i.e., *high*, *medium*, *low*, and *relevant*. The high risk level indicates that the system can be in damage, particularly if it can be used to breach the integrity of the system, or possibly resulting in a DoS attack that brings down the system. The medium risk level has inappropriate data or files in the system, which may be used for a subsequent attack in the system. The low risk level is typically not severe and can only serve as a conjunction to other vulnerability risk that may lead to a security breach. The relevant level is not classified as risky, but for informational purposes, the system administrator should determine if there are malicious indications. The weighted sum of port risk factor is defined as

$$c = \sum_{i \in I} n_i \cdot \omega_i. \tag{4}$$

Classification of risk factor is weighted in accordance with the level of severity ω_i, where each level carries a certain weight of risk factor to the number of findings n_i. The port vulnerability v_α can be normalized by σ, which is obtained from a set of c

$$v_\alpha = \frac{c}{\sigma} \tag{5}$$

where σ denotes the historical worst case among all audits. The weighting factors $\omega_1, \omega_2, \ldots, \omega_4$ for each defined level are assigned to 1, 0.75, 0.5, and 0.25, respectively.

4) Password Strength Evaluation: Password strength is determined by the total combination of character types and its length. The strength of password vulnerability can be measured as

$$s_\beta = \mathcal{C}^L \tag{6}$$

where $\mathcal{C}$ is the combination of character types and L is the length of a password. The strongest password strength deters or prolongs the cracking process. Neither brute-force trials nor social engineering techniques can break through in a short period. For instance, a numeric combination of ten can be improved with additional 52 alphabetical combinations (capital and small letters). This would strengthen the password to prevent the dictionary way of password cracking. In addition, password policies can be enforced with minimum length, password age,

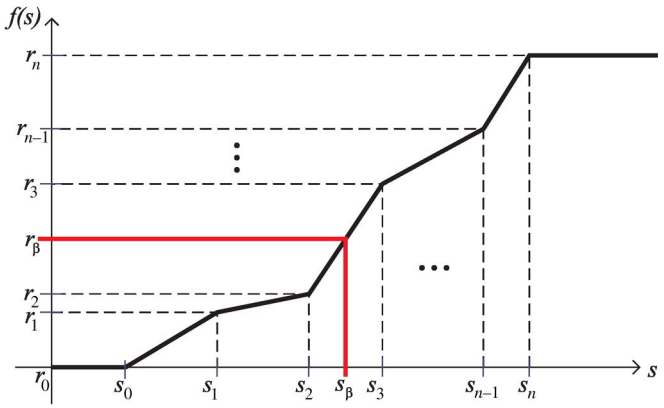

Fig. 4. Piecewise between the defined s_i and s_{i-1}.

and password combination. The password vulnerability v_β is defined as

$$v_\beta = \max\langle 1 - r_\beta \rangle \tag{7}$$

where r_β is the mapping of s_β between 0 and 1 representing the set of total accounts on a computer system. Since the mapping of r_β depends on risk classification, a piecewise linear function for the range of each classification is derived. Supposing that a linear function is defined in (8), where a denotes the slope of a piece and b denotes the interception at the y-axis

$$r_\beta = a \cdot s_\beta + b. \tag{8}$$

s_β is the combination of password that maps to the strength of password defined at the y-axis (shown in Fig. 4). The symbol r_β is the mapping point of s_β. The slope of every piece of linear function can be determined as

$$a = \frac{r_i - r_{i-1}}{s_i - s_{i-1}}. \tag{9}$$

The interception of the point b is generalized as follows:

$$r_i = \frac{r_i - r_{i-1}}{s_i - s_{i-1}} s_i + b \Rightarrow b = \frac{r_{i-1} \cdot s_i - r_i \cdot s_{i-1}}{s_i - s_{i-1}}. \tag{10}$$

In general, it can be expressed in (11), shown at the bottom of the page.

5) Evaluating Security Improvements: Security improvement can be achieved by a replacement or additional countermeasures. The improvement for an attack leaf and intrusion scenario can be measured with the implementation of defense nodes denoted as $v'(G)$ and $V'(i)$, respectively, for the leaf and scenario vulnerability after an improvement is implemented. The degree of improvement for a leaf vulnerability is given by $|(v'(G) - v(G)/v(G)) \times 100\%|$ and similarly for the scenario improvement.

$$r_\beta = \begin{cases} 0, & \text{if } s_\beta < s_0 \\ \left(\frac{r_i - r_{i-1}}{s_i - s_{i-1}}\right) s_\beta + \frac{r_{i-1} \cdot s_i - r_i \cdot s_{i-1}}{s_i - s_{i-1}}, & \text{if } s_{i-1} \le s_\beta < s_i, \\ 1, & \text{if } s_\beta \ge s_n, \end{cases} \quad \begin{array}{l} \text{where } r_{i+1} > r_i, \quad r_0 = 0, \quad i = 1, 2, \ldots, n-1 \\ s_j > s_{j-1}, \qquad j = 1, 2, \ldots, n \end{array} \tag{11}$$

V. Case Study: Intrusion Modeling Using an Attack Tree

The methodology proposed in the previous section is applied to the study cases in this section. The purpose is to identify the access points of power system control networks and evaluate the network vulnerability. The objective of the proposed attack tree is focused on the ports and passwords of the computer systems on the control networks, e.g., substation or process control networks with virtual private network connection. The case study is to ensure the following.

1) All of the computer ports are evaluated (to ensure that there is no worm, Trojan horse, or spyware).
2) The strength of password is high with a good combination of character types to prevent intrusions.
3) System vulnerability is within the reasonable range relative to each scenario vulnerability.

The case study is based on the computer networks set up at Iowa State University. A total of 43 computer systems organized in five subnets, emulating subnets of electric power control networks, are evaluated based on the proposed methodology.

Although all networks are protected by firewalls, they are distinctive in roles, technologies, and architecture.

1) *Primary control center*: This is a wide-area control that consists of real-time communication servers, EMS application servers, and relational databases. These servers are highly redundant systems with additional servers as slave mode; failover in case of unforeseen failures.
2) *Backup control center*: It has identical settings, configurations, and system architecture as the primary control center that serves as "site-backup" mode for disastrous coordination in case of a primary center failure. It periodically updates the latest databases of the primary control center through ICCP servers for real-time data exchange, including real-time and historical power system information.
3) *Substation*: An Ethernet-based peer-to-peer communication within the substation, linking the instrumental devices, e.g., IP-based IEDs, to the substation computer. The main role of substation control is within the substation. The computer in the substation also serves as a server that sends real-time data to other networks and receives control commands from the control center.
4) *Power plant*: The power plant is deployed with high redundancy for data reliability purposes within the network. The power plant network involves complex process control and monitoring functions. It is a high-speed and large capacity network that acquires real-time data from physical devices, e.g., boiler or gas turbine.
5) *Web-based SCADA*: It is a portal page of user interfaces that manages the municipal (smaller) control network, in which data reliability and backup are maintained by third-party vendors. It is a client–server technology that provides same role as a control center.

The evaluation is performed from a server outside the campus' network to determine the vulnerability of the machines and how effective the boundary protection is. Since each computer has been exhaustively scanned through the ports, i.e., 65 535 combinations and specific vulnerability tests, the time required for each machine ranges from 5 to 9 h. The setup of the studies includes different platforms to ensure that local security checks are covered in the test. Tests for DoS are also included in the evaluation. Table II shows the risk vulnerability assessment on 43 computer systems distributed in the control network. This evaluation shows the number of findings that is grouped in each category, i.e., *high*, *medium*, *low*, and *relevant*, with more than 10 000 vulnerabilities scanned. For instance, potential high and medium risk levels associated to each backdoor and DoS shown in the table are detected in 1.1.5.3. It appears that the backdoor can be accessed through ports 5800 and 5900. The detection of DoS can crash a service by sending a single long text line that crashes a software module. Lower risk factors include traceroute from a scanning server and other unknown services that are detected as nonmalicious. By going through similar evaluations on each computer system, the worst case index $\sigma = 5.75$ is obtained. Aside from backdoors that pose the threat of a computer network system, accessing the control network with administrative privilege passwords is one way that can access the SCADA system. To harden intrusion attempts,

TABLE II
Risk Vulnerability Evaluation and Number of Passwords on Computer Network Systems

Network	IP Addr.	High	Med.	Low	Others	# Pwrd.
Primary Control Center	1.1.1.1	0	0	1	1	10
	1.1.1.2	0	0	1	1	6
	1.1.1.3	0	0	0	1	9
	1.1.1.4	0	0	1	1	6
	1.1.1.5	0	0	1	1	9
	1.1.1.6	0	0	0	1	8
	1.1.1.7	0	0	0	1	9
	1.1.1.8	0	0	0	1	7
	1.1.1.9	0	0	0	1	8
	1.1.1.10	0	0	0	1	7
	1.1.1.11	0	0	0	1	5
	1.1.1.12	0	0	1	1	6
Backup Control Center	1.1.4.1	0	1	2	3	9
	1.1.4.2	1	1	3	3	6
	1.1.4.3	0	1	2	3	8
	1.1.4.4	1	1	4	4	9
	1.1.4.5	0	1	3	3	2
	1.1.4.6	1	1	4	4	8
	1.1.4.7	2	1	4	4	7
	1.1.4.8	1	1	4	4	7
	1.1.4.9	0	1	2	3	9
Substation	1.1.3.1	0	0	1	1	8
	1.1.3.2	0	0	3	4	9
	1.1.3.3	0	2	5	6	9
	1.1.3.4	1	1	4	7	6
Power Plant	1.1.5.1	0	1	1	3	5
	1.1.5.2	2	2	3	3	6
	1.1.5.3	2	2	3	3	5
	1.1.5.4	2	2	3	3	6
	1.1.5.5	1	2	3	3	3
	1.1.5.6	1	1	3	4	8
	1.1.5.7	1	1	4	4	8
	1.1.5.8	0	1	3	3	8
	1.1.5.9	0	1	3	3	6
	1.1.5.10	1	1	4	4	9
	1.1.5.11	0	1	3	3	7
	1.1.5.12	1	1	4	4	4
	1.1.5.13	1	1	4	4	7
Web-Based SCADA	1.1.2.1	0	0	3	4	8
	1.1.2.2	0	0	3	4	9
	1.1.2.3	0	0	3	4	10
	1.1.2.4	0	0	3	4	7
	1.1.2.5	0	0	3	4	8

TABLE III
PASSWORD COMBINATION AND ITS VULNERABILITY OF IP 1.1.1.1

Password	$\mathcal{C}^L$	$1-r_\beta$
sdfsd#$%s23	8.751×10^{19}	.5312
9sfdvciij2	3.656×10^{15}	.75
987y9rge	2.821×10^{17}	.9993
IUUJuert53	2.935×10^{25}	.5
456$	2.313×10^{6}	1

a set of administrative passwords are randomly generated for the case study for evaluation of their password strengths. This also incorporates the existence of factory default password and insufficient security improvement [52]. The last column of Table II shows the number of passwords associated with each computer system generated. Equation (12) shows the piecewise functions to determine r_β, where the increment of r_i is 0.25 for each level. The strength of password that is "difficult to crack" (s_i) has been given as 1000, 1×10^{15}, 1×10^{20}, 1×10^{35}, and 1×10^{50}. Table III shows a set of passwords that can be used to access IP 1.1.1.1. It tabulates the combination of each password and its vulnerability level for each password. Equation (7) is used to determine v_β which is 1. Comparison with v_α is necessary to determine the maximum value. This maximum value will be multiplied with the precondition of cybersecurity to determine $v(G)$

$$r_\beta=\begin{cases}0, & \text{if } s_\beta<1000\\ 2.5\times10^{-16}s_\beta, & \text{if } 1000\le s_\beta<1\times10^{15}\\ 2.5\times10^{-21}s_\beta+0.25, & \text{if } 1\times10^{15}\le s_\beta<1\times10^{20}\\ 2.5\times10^{-36}s_\beta+0.5, & \text{if } 1\times10^{20}\le s_\beta<1\times10^{35}\\ 2.5\times10^{-51}s_\beta+0.75, & \text{if } 1\ 10^{35}\le s_\beta<1\times10^{50}\\ 1, & \text{if } s_\beta\ge1\times10^{50}.\end{cases} \tag{12}$$

An attack tree shown in Fig. 5 demonstrates the network relationship between a power plant, a substation, a web-based SCADA, and the primary and backup control centers. The formulation of the attack tree is based upon the abstraction of the power control networks that is monitored through control systems. These combinations may result in an intrusion into the control center. To derive the scenario combination, groups of attack leaves are arranged as follows:

$$\begin{aligned}&\text{Group 1}: (G_{13}\times G_{14}\times\cdots\times G_{17})\\ &\text{Group 2}: \begin{pmatrix}G_{22}\times G_{23}\times\cdots\times G_{26}\\ G_{27}\times G_{28}\\ G_{29}\times G_{30}\end{pmatrix}\\ &\text{Group 3}: (\text{Group 2}\times\text{Group 4}\times\text{Group 5}\\ &\qquad\times G_1\times\cdots\times G_{10})\\ &\text{Group 4}: \begin{pmatrix}G_{31}\times G_{32}\\ G_{33}\times G_{34}\times\cdots\times G_{36}\\ G_{37}\times G_{38}\\ G_{39}\end{pmatrix}\\ &\text{Group 5}: \begin{pmatrix}G_{40}\times G_{41}\\ G_{42}\times G_{43}\end{pmatrix}.\end{aligned}$$

Each group represents the computer systems of a subnetwork from a power plant, substation networks, and a web-based SCADA system. Group 1 represents the disruption of the web-based SCADA system, where security breaches in a web server may be exploited by intruders. Groups 2 and 3 represent a disruption of the backup control center and real-time services in the primary control center. The importance of a backup control center is to continue functions of the primary control center under extreme circumstances. Communication, relational database, and real-time application services in control centers are critical elements. Groups 4 and 5 represent a disruption of power plant operations and substation automation. Security breaches in these groups may also result in penetration into the control center. Each intrusion scenario is derived from attack leaves, where $G_1, G_2, \ldots, G_{43}$ are attack leaves. Intrusion scenarios are expressed as follows:

$$\begin{aligned}&\prod_{i=13,14,\ldots,17} G_i\to i_1\\ &\prod_{i=1,2,\ldots,12,22,23,\ldots,26,31,32} G_i\to i_2\\ &\prod_{i=1,2,\ldots,12,22,23,\ldots,26,33,34,\ldots,36} G_i\to i_3\\ &\prod_{i=1,2,\ldots,12,22,23,\ldots,26,37,38} G_i\to i_4\\ &\prod_{i=1,2,\ldots,12,22,23,\ldots,26,39} G_i\to i_5\\ &\prod_{i=1,2,\ldots,12,27,28,26,31,32} G_i\to i_6\\ &\prod_{i=1,2,\ldots,12,27,28,26,33,34,\ldots,36} G_i\to i_7\\ &\prod_{i=1,2,\ldots,12,27,28,26,37,38} G_i\to i_8\\ &\prod_{i=1,2,\ldots,12,27,28,26,39} G_i\to i_9\\ &\prod_{i=1,2,\ldots,12,29,30,31,32} G_i\to i_{10}\\ &\prod_{i=1,2,\ldots,12,29,30,33,34,\ldots,36} G_i\to i_{11}\\ &\prod_{i=1,2,\ldots,12,29,30,37,38} G_i\to i_{12}\\ &\prod_{i=1,2,\ldots,12,29,30,39} G_i\to i_{13}\\ &\prod_{i=1,2,\ldots,12,22,23,\ldots,26,40,41} G_i\to i_{14}\\ &\prod_{i=1,2,\ldots,12,22,23,\ldots,26,42,43} G_i\to i_{15}\\ &\prod_{i=1,2,\ldots,12,27,28,40,41} G_i\to i_{16}\\ &\prod_{i=1,2,\ldots,12,27,28,42,43} G_i\to i_{17}\\ &\prod_{i=1,2,\ldots,12,29,30,40,41} G_i\to i_{18}\\ &\prod_{i=1,2,\ldots,12,29,30,42,43} G_i\to i_{19}.\end{aligned} \tag{13}$$

The preconditions of cybersecurity (χ) for all systems are determined with 1.00, except for IPs 1.1.1.4, 1.1.1.8, 1.1.2.3, 1.1.4.2, 1.1.4.9, and 1.1.5.6 that are determined with 0.67.

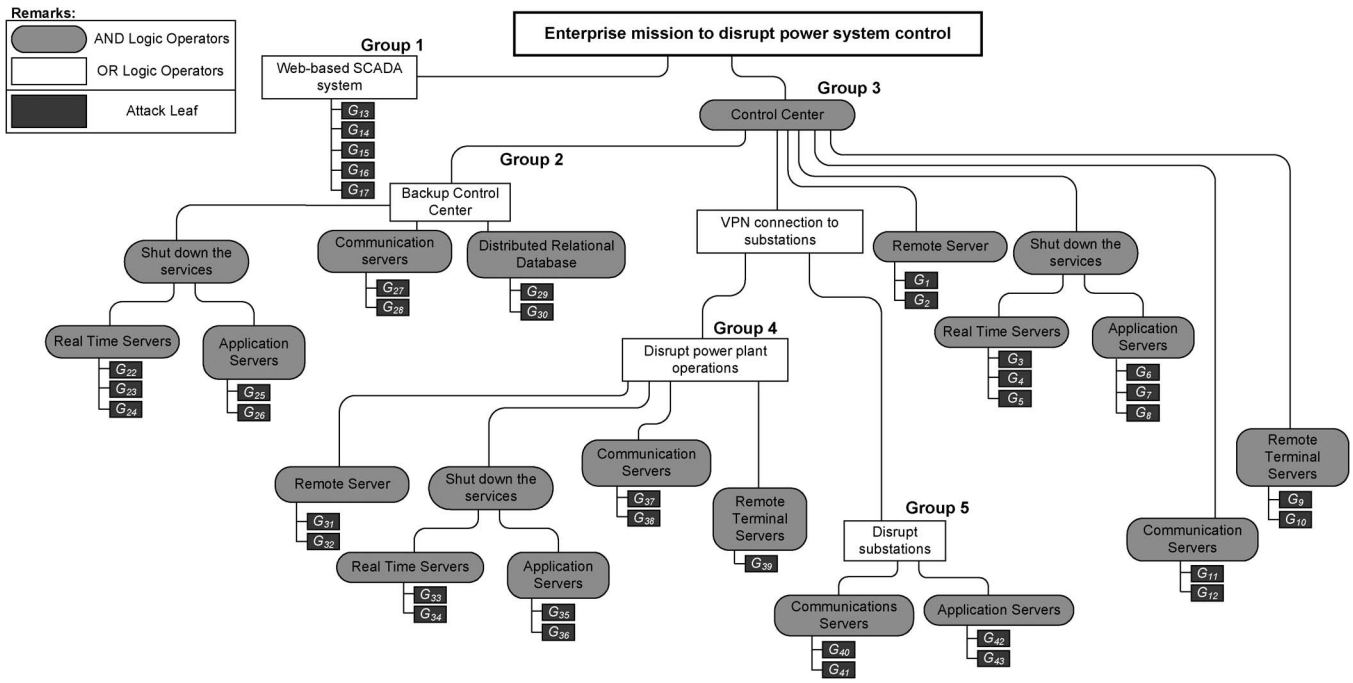

Fig. 5. Attack Tree of the Power System Control Framework.

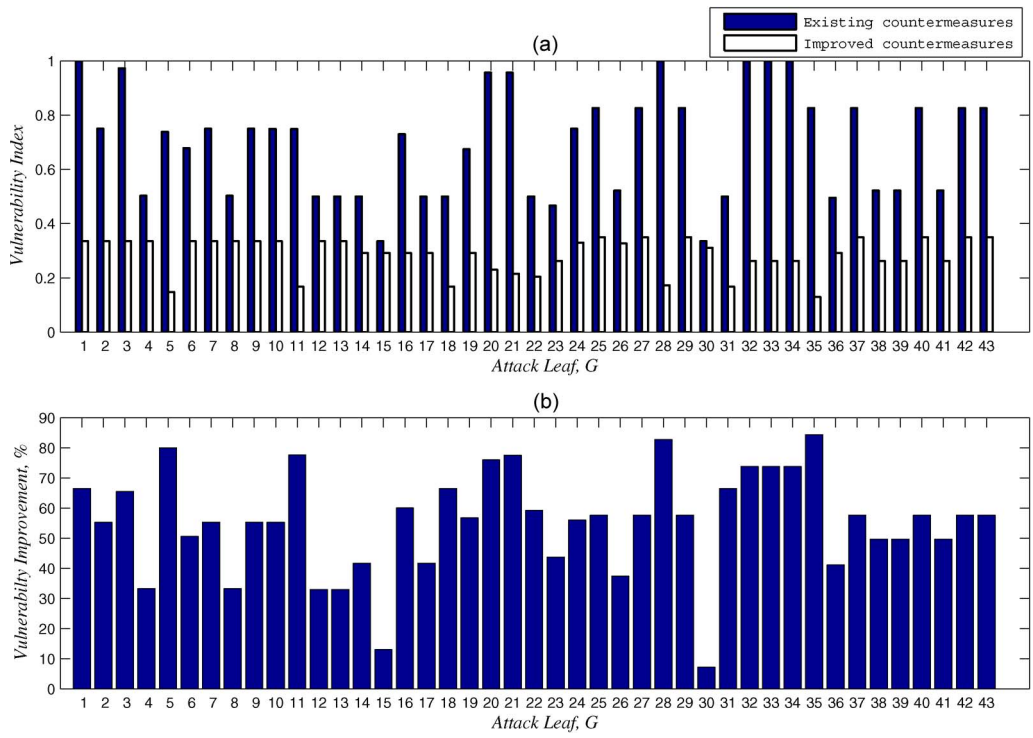

Fig. 6. Leaf vulnerability with implemented and improved countermeasures. (a) Leaf vulnerability. (b) Vulnerability improvement for each attack leaf.

$v(G)$ and $v'(G)$ are computed in accordance with the configuration of the attack tree. The leaf vulnerability and its improvement are shown in Fig. 6(a) and (b). Since the password combination in the set reveals a weakness, a password policy with at least eight characters and four different character types has been enforced for security improvement. This has resulted in improvement of preconditions to 0.67 or, even better, 0.33. The factory default passwords have been replaced with stronger passwords, and the findings on high and medium categories of risk factor for each system have been removed. Overall, this has also lowered all of the leaf vulnerabilities shown in Fig. 6(b). Among which, $v(G_{30})$ has been improved the most with 84.37%. Improvement in all cases has been archived at the level of at least 50%. Also, eliminating the factory default password and guest account reduced the leaf vulnerability. In the next step, $V(I)$ and $V'(I)$ are evaluated using (2). Each

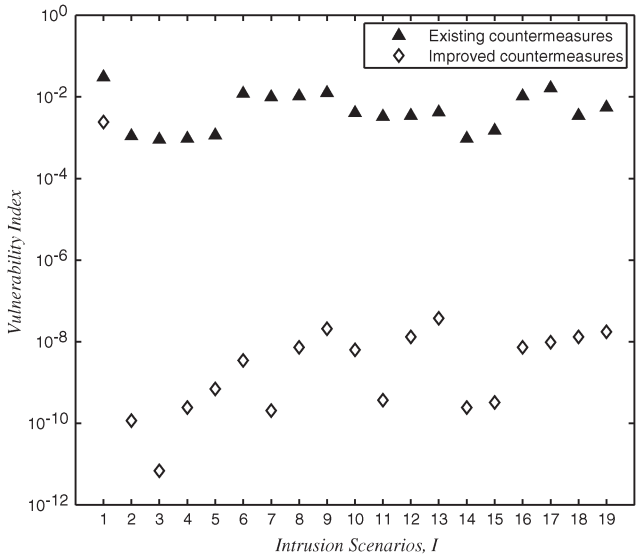

Fig. 7. Scenario vulnerability with implemented and improved countermeasures.

intrusion scenario is the product of attack leaves. The scenario vulnerability is shown in Fig. 7. Note that a logarithmic scale is used to highlight the difference between $V(I)$ and $V'(I)$. The improvement of i_1 is 92.11%. The remaining values are close to 100%. The system vulnerability has been improved from 0.0306 to 0.0024.

VI. Conclusion and Future Work

Cybersecurity for critical infrastructures is an emerging area that requires extensive new research. The comprehensive literature survey reported in this paper has identified the lack of research in some areas. New research needs to be done in each of the components of the RAIM framework, such as the following: 1) SCADA-system-specific real-time correlation and intrusion detection algorithms; 2) online risk monitoring and mitigation algorithms capturing both cyber system vulnerabilities and the resulting consequences; 3) advanced modeling techniques that capture the dynamic nature of the attacker behavior, as well as the system behavior; and 4) advanced modeling that accounts for impacts such as load loss, loss due to equipment damage, and economic loss. Vulnerability assessment can be performed periodically, and the validation of the proposed framework can be conducted through test-bed development. For instance, the components include instrumenting logs (both power equipment logs and computer system logs), real-time monitoring of logs, event correlations and hypothesis formation, what-if impact analysis, and proactive/mitigation countermeasures to restore a power system. The proposed methodology using attack trees provides a simplified way to hypothetically evaluate the system vulnerability level. This paper can be further extended by considering the reduction of system vulnerability within a budgetary limit. Efficient delivery of information from substations or control centers may be needed to help power system dispatchers identify critical messages quickly. Various techniques for visualization of the system health, in terms of vulnerability level and other critical information, are desirable.

References

[1] J. Eisenhauer, P. Donnelly, M. Ellis, and M. O'Brien. (2006, Jan.). *Roadmap to Secure Control Systems in the Energy Sector*. [Online]. Available: http://www.controlsystemsroadmap.net/pdfs/roadmap.pdf

[2] Supervisory Control and Data Acquisition (SCADA) Systems, Nat. Commun. Syst., Arlington, VA, Oct. 2004. [Online]. Available: http://www.ncs.gov/library/tech_bulletins/2004/tib_04-1.pdf

[3] Critical infrastructure protection report, Government Accountability Office, Washington, DC, May 2005. [Online]. Available: http://www.gao.gov/new.items/d05434.pdf

[4] Challenges and Efforts to Secure Control Systems, Government Accountability Office, Washington, DC, Mar. 2004. [Online]. Available: http://www.gao.gov/new.items/d04354.pdf

[5] M. R. Permann and K. Rohde, *Cyber Assessment Methods for SCADA Security*, Research Triangle Park, NC: Instrum. Soc. Amer. [Online]. Available: http://www.oe.energy.gov/DocumentsandMedia/Cyber_Assessment_Methods_for_SCADA_Security_Mays_ISA_Paper.pdf

[6] R. E. Carlson, J. E. Dagle, S. A. Shamsuddin, and R. P. Evans, *A Summary of Control System Security Standards Activities in the Energy Sector*, DC: U.S. Dept. Energy, Office Electricity Delivery Energy Reliab., Nat. SCADA Test Bed (NSTB), Oct. 2005. [Online]. Available: http://www.oe.energy.gov/DocumentsandMedia/Control_System_Security_Standards_Activities.pdf

[7] *Information Security: Technologies to Secure Federal Systems*, Mar. 2004, Report to Congressional Requesters, GAO-04-467. [Online]. Available: http://www.gao.gov/new.items/d04467.pdf

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

[9] J. D. McDonald, *Power Substations Engineering*, 2nd ed. Boca Raton, FL: CRC Press, May 30, 2007.

[10] J. Salmeron, K. Wood, and R. Baldick, "Analysis of electric grid security under terrorist threat," *IEEE Trans. Power Syst.*, vol. 19, no. 2, pp. 905–912, May 2004.

[11] R. A. Leon, V. Vittal, and G. Manimaran, "Application of sensor network for secure electric energy infrastructure," *IEEE Trans. Power Del.*, vol. 22, no. 2, pp. 1021–1028, Apr. 2007.

[12] A. G. Bruce and R. Lee, "A framework for the specification of SCADA data links," *IEEE Trans. Power Syst.*, vol. 9, no. 1, pp. 560–564, Feb. 1994.

[13] R. L. Krutz, *Securing SCADA Systems*, 1st ed. Hoboken, NJ: Wiley, Nov. 28, 2005.

[14] Q. Liu, J.-N. Hwang, and C.-C. Liu, "Communication infrastructure for wide area protection of power systems," in *Proc. Power Syst. Commun. Infrastructures Future*, Beijing, China, Sep. 2002.

[15] C.-L. Su, C.-N. Lu, and T.-Y. Hsiao, "Simulation study of Internet based inter control center data exchange for complete network modeling," *IEEE Trans. Power Syst.*, vol. 17, no. 4, pp. 1177–1183, Nov. 2002.

[16] K. Schneider, C.-C. Liu, and J.-P. Paul, "Assessment of interactions between power and telecommunications infrastructures," *IEEE Trans. Power Syst.*, vol. 21, no. 3, pp. 1123–1130, Aug. 2006.

[17] T. Mander, F. Nabhani, L. Wang, and R. Cheung, "Data object based security for DNP3 over TCP/IP for increased utility commercial aspects security," in *Proc. IEEE Power Eng. Soc. Gen. Meeting*, Jun. 24–28, 2007, pp. 1–8.

[18] M. Adamiak and W. Premerlani, "The role of utility communications in a deregulated environment," in *Proc. 32nd HICSS*, 1999, vol. Track3, p. 3026.

[19] M. Amin and B. F. Wollenberg, "Toward a smart grid: Power delivery for the 21st century," *IEEE Power Energy Mag.*, vol. 3, no. 5, pp. 34–41, Sep./Oct. 2005.

[20] F. F. Wu, K. Moslehi, and A. Bose, "Power system control centers: Past, present, and future," *Proc. IEEE*, vol. 93, no. 11, pp. 1890–1908, Nov. 2005.

[21] *Vulnerability Assessment Methodology for Electric Power Infrastructure*, U.S. Dept. Energy, Office Energy Assurance, Washington DC, Sep. 30, 2002.

[22] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems using attack trees," in *Proc. IEEE Power Eng. Soc. Gen. Meeting*, Tampa, FL, Jun. 24–28, 2007, pp. 1–8.

[23] T. D. Nelson, "Mitigations for security vulnerabilities found in control system networks," in *Proc. 16th Annu. Joint ISA POWID/EPRI Controls Instrum. Conf.*, 2006, pp. 1–12.

[24] C.-W. Ten, G. Manimaran, and C.-C. Liu, "Cybersecurity for electric power control and automation systems," in *Proc. eNetworks Cyberengineering Workshop, IEEE-SMC*, Montreal, QC, Canada, Oct. 7–10, 2007, pp. 29–34.

[25] M. Naedele, D. Dzung, and M. Stanimirov, "Network security for substation automation systems," in *SAFECOMP*, U. Voges, Ed. Berlin, Germany: Springer-Verlag, 2001, pp. 25–34.

[26] T. S. Sidhu and Y. Yin, "Modeling and simulation for performance evaluation of IEC61850-based substation communication systems," *IEEE Trans. Power Del.*, vol. 22, no. 3, pp. 1482–1489, Jul. 2007.

[27] P. Baybutt, "Cybersecurity risk analysis for process control systems using rings of protection analysis (ROPA)," *Process Safety Progr.*, vol. 23, no. 4, pp. 284–290, Dec. 2004, PrimaTech Tech. Rep.

[28] N. Ye, J. Giordano, and J. Feldman, "A process control approach to cyber attack detection," *Commun. ACM*, vol. 44, no. 8, pp. 76–82, Aug. 2001.

[29] J.-W. Park and J.-M. Lee, "Transmission modeling and simulation for Internet-based control," in *Proc. IEEE 27th IECON*, Nov. 2001, pp. 165–169.

[30] A. Miller, "Trends in process control systems security," *IEEE Secur. Privacy*, vol. 3, no. 5, pp. 57–60, Sep. 2005.

[31] C. DeMarco and Y. Braden, "Threats to electric power grid security through hacking of networked generation control," in *Proc. 3rd CRIS*, Alexandria, VA, Sep. 2006.

[32] X. Wu, D. Zhang, and K. Wang, "Palm line extraction and matching for personal authentication," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 36, no. 5, pp. 978–987, Sep. 2006.

[33] S. A. Klein and J. N. Menendez, "Information security considerations in open system architectures," *IEEE Trans. Power Syst.*, vol. 8, no. 1, pp. 224–230, Feb. 1993.

[34] G. N. Ericsson and A. Torkilseng, "Management of information security for an electric power utility—On security domains and use of ISO/IEC17799 standard," *IEEE Trans. Power Del.*, vol. 20, no. 2, pp. 683–690, Apr. 2005.

[35] T.-Y. Chen, Y.-M. Chen, and C.-B. Wang, "A formal virtual enterprise access control model," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 38, no. 4, pp. 832–851, Jul. 2008.

[36] T. Brown, "Security in SCADA systems: How to handle the growing menace to process automation," *IEE Comput. Control Eng.*, vol. 16, no. 3, pp. 42–47, Jun. 2005.

[37] F. Sheldon, S. Batsell, S. Prowell, and M. Langston, "Assessment and remediation of vulnerabilities in the SCADA and process control systems of utilities," Internet Security Systems (white paper), 2005.

[38] F. Cleveland, "IEC TC57 security standards for power system's information infrastructure—Beyond simple encryption," in *Proc. IEEE Power Eng. Soc. Gen. Meeting*, Tampa, FL, Jun. 24–28, 2007, pp. 1079–1087.

[39] Z. Xie, G. Manimaran, V. Vittal, A. G. Phadke, and V. Centeno, "An information architecture for future power system and its reliability analysis," *IEEE Trans. Power Syst.*, vol. 17, no. 3, pp. 857–863, Aug. 2002.

[40] C. H. Hauser, D. E. Bakken, and A. Bose, "A failure to communicate," *IEEE Power Energy Mag.*, vol. 3, no. 2, pp. 47–55, Mar./Apr. 2005.

[41] *Attack trends*, Carnegie Mellon Comput. Emergency Response Team/Center Coordination (CERT/CC), Pittsburgh, PA, 2002. [Online]. Available: http://www.cert.org/archive/pdf/attack_trends.pdf

[42] S. McClure, J. Scambray, and G. Kurtz, *Hacking Exposed: Network Security Secrets and Solutions*, 4th ed. New York: McGraw-Hill, 2003.

[43] M. Amin, "North America's electricity infrastructure: Are we ready for more perfect storms?" *IEEE Secur. Privacy*, vol. 1, no. 5, pp. 19–25, Sep./Oct. 2003.

[44] R. Richardson, "2007 CSI computer crime and security survey," in *Proc. 12th Annu. Comput. Crime Security Survey*, 2007, pp. 1–28.

[45] E. Goetz, "Cybersecurity of the electric power industry," in *Report of Investigative Research for Infrastructure Assurance (IRIA)*. Hanover, NH: Inst. Security Technol. Studies, Dartmouth College, Dec. 2002.

[46] F. Sheldon, S. Batsell, S. Prowell, and M. Langston, *Control Systems Cybersecurity Awareness*. Washington DC: U.S. Comput. Emergency Readiness Team (CERT), Jul. 25, 2005, pp. 1–10.

[47] J. Tang, R. Hovsapian, M. Sloderbeck, J. Langston, R. Meeker, P. McLaren, D. Becker, B. Richardson, M. Baca, J. Trent, Z. Hartley, R. Parks, and S. Smith, "The CAPS-SNL power system security test bed," in *Proc. 3rd CRIS*, Alexandria, VA, Sep. 2006.

[48] G. Dondossola, F. Garrone, J. Szanto, and G. Fiorenza, "Emerging information technology scenarios for the control and management of the distribution grid," in *Proc. 19th Int. Conf. Exhib. Elect. Distrib.*, Vienna, Austria, Mar. 21–24, 2007.

[49] J. M. Weiss, "Control systems cybersecurity–maintaining the reliability of the critical infrastructure," Testimony of Joseph M. Weiss Control Systems Cybersecurity Expert before the House Government Reform Committee's Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census U.S. House of Representatives, Mar. 30, 2004.

[50] F. Sheldon, S. Batsell, S. Prowell, and M. Langston, *Cryptographic Protection of SCADA Communications—Part 1: Background, Policies and Test Plan*. Washington, DC: American Gas Assoc., Sep. 7, 2005.

[51] NERC Tech. Rep. Cybersecurity Standards. [Online]. Available: http://www.nerc.com/filez/standards/Cyber-Security-Permanent.html

[52] *User Manual for the Workshop*, North Amer. Electric Rel. Council (NERC), Minneapolis, MN, Sep. 2006. Cybersecurity Standards Workshop

[53] A. Torkilseng and G. Ericsson, "Some guidelines for developing a framework for managing cybersecurity for an electric power utility," ELECTRA Report—JWG D2/B3/C2.01, Oct. 2006.

[54] D. M. Nicol, W. H. Sanders, and K. S. Trivedi, "Model-based evaluation from dependability to security," *IEEE Trans. Dependable Secure Comput.*, vol. 1, no. 1, pp. 48–65, Jan. 2004.

[55] W. L. McGill and B. M. Ayyub, "The meaning of vulnerability in the context of critical infrastructure protection," in *Critical Infrastructure Protection: Elements of Risk*. Arlington, VA: School of Laws, George Mason Univ., Dec. 2007.

[56] J. Depoy, J. Phelan, P. Sholander, B. Smith, G. Varnado, and G. Wyss, "Risk assessment for physical and cyber-attacks on critical infrastructures," in *Proc. IEEE MILCOM*, Oct. 17–20, 2005, vol. 3, pp. 1961–1969.

[57] S. Kumar, "Classification and detection of computer intrusions," Ph.D. dissertation, Dept. Comput. Sci., Purdue Univ., West Lafayette, IN, Aug. 1995.

[58] Y. Xie, "A spatiotemporal event correlation approach to computer security," Ph.D. dissertation, School Comput. Sci., Carnegie Mellon Univ., Pittsburgh, PA, Aug. 2005, (CMU-CS-05-175).

[59] K. Lye and J. Wing, "Game strategies in network security," in *Proc. Workshop Foundations Comput. Secur.*, Copenhagen, Denmark, 2002, pp. 1–2.

[60] F. Sheldon, T. Potok, A. Krings, and P. Oman, "Critical energy infrastructure survivability, inherent limitations, obstacles, and mitigation strategies," *Int. J. Power Energy Syst.*, no. 2, pp. 86–92, 2004.

[61] F. Sheldon, S. Batsell, S. Prowell, and M. A. Langston, "Position statement: Methodology to support dependable survivable cyber-secure infrastructure," in *Proc. 38th Hawaii Int. Conf. Syst. Sci.*, 2005, vol. 9, pp. 1–10.

[62] G. Dondossola, G. Deconinck, F. D. Giandomenico, S. Donatelli, M. Kaaniche, and P. Verissimo, "Critical utility infrastructural resilience," in *Proc. Complex Netw. Infrastructure Protection*, Rome, Italy, Mar. 28–29, 2006.

[63] G. Dondossola, O. Lamquet, and A. Torkilseng, "Key issues and related methodologies in the security risk analysis and evaluation of electric power control systems," in *Proc. CIGRÉ Session, Study Committee D2 Inf., Telecommun. Telecontrol Syst. Elect. Power Ind.*, Paris, France, Sep. 2006.

[64] S. Evans, D. Heinbuch, E. Kyle, J. Piorkowski, and J. Wallner, "Risk-based systems security engineering: Stopping attacks with intention," *IEEE Secur. Privacy*, vol. 2, no. 6, pp. 59–62, Nov./Dec. 2004.

[65] 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.

[66] S. E. Schechter, "Toward econometric models of the security risk from remote attack," *IEEE Secur. Privacy*, vol. 3, no. 1, pp. 40–44, Jan. 2005.

[67] S. Bistarelli, F. Fioravanti, and P. Peretti, "Defense trees for economic evaluation of security investments," in *Proc. ARES*, 2006, pp. 416–423.

[68] M. Long, C.-H. Wu, and J. Y. Hung, "Denial of service attacks on network-based control system: Impact and mitigation," *IEEE Trans. Ind. Inf.*, vol. 1, no. 2, pp. 85–96, May 2005.

[69] X. Luo, R. Chang, and E. Chan, "Performance analysis of TCP/AQM under denial-of-service attacks," in *Proc. 13th IEEE Int. Symp. Modeling, Anal., Simul. Comput. Telecommun. Syst.*, Sep. 27–29, 2005, pp. 97–104.

[70] D. S. Yeung, S. Jin, and X. Wang, "Covariance-matrix modeling and detecting various flooding attacks," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 37, no. 2, pp. 157–169, Mar. 2007.

[71] J. Bigham, D. A. O. Gamez, X. Jin, J. Rodaway, C. Phillips, and L. Titkov, "Safeguarding electricity cyber-infrastructures against the worm threat," in *Proc. 2nd CRIS*, Grenoble, France, Oct. 25–27, 2004.

[72] S. Nadjm-Tehrani, S. Burschka, K. Burbeck, and T. Chyssler, "Safeguarding information infrastructures: Alarm reduction and anomaly detection," in *Proc. 2nd CRIS*, Grenoble, France, Oct. 25–27, 2004.

[73] Y. Zhang, M. Ilic, and O. Tonguz, "Application of support vector machine classification to enhanced protection relay logic in electric power grids," in *Proc. LESCOPE*, Montreal, QC, Canada, Oct. 10–12, 2007, pp. 31–38.

[74] S. Su, W.-L. Chan, K.-K. Li, X. Duan, and X. Zeng, "Context information-based cybersecurity defense of protection system," *IEEE Trans. Power Del.*, vol. 22, no. 3, pp. 1477–1481, Jul. 2007.

[75] G. A. Wang, H. Chen, J. J. Xu, and H. Atabakhsh, "Automatically detecting criminal identity deception: An adaptive detection algorithm," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 36, no. 5, pp. 988–999, Sep. 2006.
[76] E. Jonsson and T. Olovsson, "A quantitative model of the security intrusion process based on attacker behavior," *IEEE Trans. Softw. Eng.*, vol. 23, no. 4, pp. 235–245, Apr. 1997.
[77] N. Ye, Y. Zhang, and C. M. Borror, "Robustness of the markov-chain model for cyber-attack detection," *IEEE Trans. Rel.*, vol. 53, no. 1, pp. 116–123, Mar. 2004.
[78] L. Lavalle, C. Balducelli, and G. Vicoli, "A CBR-based algorithm to monitor and information intensive critical infrastructure," in *Proc. 2nd CRIS*, Grenoble, France, Oct. 25–27, 2004.
[79] N. Ye, Q. Chen, and C. M. Borror, "EWMA forecast of normal system activity for computer intrusion detection," *IEEE Trans. Rel.*, vol. 53, no. 4, pp. 557–566, Dec. 2004.
[80] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," *IEEE Trans. Power Syst.*, vol. 23, no. 4, pp. 1836–1846, Nov. 2008.
[81] G. Dondossola, J. Szanto, M. Masera, and I. N. Fovino, "Evaluation of the effects of intentional threats to power substation control systems," in *Proc. CNIP*, Rome, Italy, 2006.
[82] C. M. Davis, J. E. Tate, H. Okhravl, C. Grier, T. J. Overbye, and D. Nicol, "SCADA cybersecurity test bed development," in *Proc. NAPS*, Sep. 2006, pp. 483–488.
[83] G. Dondossola, F. Garrone, J. Szanto, and F. Gennaro, "A laboratory test bed for the evaluation of cyber-attacks to interacting ICT infrastructures of power grid operators," in *Proc. CIRED Seminar: SmartGrid Distrib.*, Frankfurt, Germany, Jun. 2008, p. 54.
[84] B. Schneier, "Attack trees: Modeling security threats," *Dobb's J.*, vol. 24, no. 12, pp. 21–29, Dec. 1999.
[85] A. Moore, R. Ellison, and R. Linger, Attack modeling for information security and survivability, Carnegie Mellon Univ., Pittsburgh, PA, CMU/SEI-2001-TN-001. [Online]. Available: http://citeseer.ist.psu.edu/moore01attack.html
[86] G. Conti, M. Ahamad, and J. Stasko, "Attacking information visualization system usability overloading and deceiving the human," in *Proc. ACM Symp. Usable Privacy Security*, Pittsburgh, PA, Jun. 2005, vol. 93, pp. 89–100.
[87] C. Fung, Y. L. Chen, X. Wang, J. Lee, R. Tarquini, M. Anderson, and R. Linger, "Survivability analysis of distributed systems using attack tree methodology," in *Proc. IEEE MILCOM*, Oct. 17–20, 2005, vol. 1, pp. 583–589.
[88] G. C. Dalton, R. F. Mills, J. M. Colombi, and R. A. Raines, "Analyzing attack trees using generalized stochastic Petri nets," in *Proc. IEEE Inf. Assurance Workshop*, Jun. 2006, pp. 116–123.

Chee-Wooi Ten (S'00) received the B.S. and M.S. degrees in electrical engineering from Iowa State University, Ames, in 1999 and 2001, respectively. He is currently working toward the Ph.D. degree in the School of Electrical, Electronic, and Mechanical Engineering, University College Dublin, National University of Ireland, Dublin, Ireland.

He was a Summer Intern with the MidAmerican Energy Control Center in 2000. He was also an Application Engineer with Siemens Energy Management and Information System, Singapore, from 2002 to 2005. His research interests include interdependence modeling for power infrastructure.

Govindarasu Manimaran (M'99–SM'10) received the Ph.D. degree in computer science and engineering from the Indian Institute of Technology, Madras, India, in 1998.

He is currently an Associate Professor with the Department of Electrical and Computer Engineering, Iowa State University (ISU). His research expertise is in the areas of resource management in real-time systems and networks, overlay networks, network security, and their applications to critical infrastructures such as the electric grid. He has published over 100 peer-reviewed research publications. He is the coauthor of the book entitled *Resource Management in Real-Time Systems and Networks* (MIT Press, 2001).

Dr. Manimaran received the Young Engineering Research Faculty Award at ISU in 2003. He has given tutorials on Internet infrastructure security in conferences, such as the IEEE Infocom 2004 and IEEE ComSoc Tutorials Now (2004), and served as Workshop Cochair, Symposium Cochair, and Session Chair on many occasions.

Chen-Ching Liu (F'94) received the Ph.D. degree from the University of California, Berkeley.

He is currently a Professor of power systems with the School of Electrical, Electrionic and Mechanical Engineering, University College Dublin, National University of Ireland, Dublin, Ireland. He was the Palmer Chair Professor of Electrical and Computer Engineering with Iowa State University. During 1983–2005, he was a Professor of electrical engineering with the University of Washington, Seattle, where he also served as the Associate Dean of Engineering from 2000 to 2005.

Dr. Liu received the IEEE Third Millennium Medal in 2000 and the IEEE Power Engineering Society Outstanding Power Engineering Educator Award in 2004. He was the Chair of the Technical Committee on Power System Analysis, Computing, and Economics of the IEEE Power Engineering Society.