Modeling Cyber-Physical Vulnerability of the Smart Grid With Incomplete Information

Anurag Srivastava, *Senior Member, IEEE*, Thomas Morris, *Senior Member, IEEE*, Timothy Ernster, *Student Member, IEEE*, Ceeman Vellaithurai, *Student Member, IEEE*, Shengyi Pan, *Student Member, IEEE*, and Uttam Adhikari, *Student Member, IEEE*

***Abstract*—This paper addresses the attack modeling using vulnerability of information, communication and electric grid network. Vulnerability of electric grid with incomplete information has been analyzed using graph theory based approach. Vulnerability of information and communication (cyber) network has been modeled utilizing concepts of discovery, access, feasibility, communication speed and detection threat. Common attack vector based on vulnerability of cyber and physical system have been utilized to operate breakers associated with generating resources to model aurora-like event. Real time simulations for modified IEEE 14 bus test case system and graph theory analysis for IEEE 118 bus system have been presented. Test case results show the possible impact on smart grid caused by integrated cyber-physical attack.**

***Index Terms*—Aurora attack, cyber-physical vulnerability, graph theory, information and communication technology for smart grid, RTDS.**

I. Introduction

THE SMART electric grid utilizes enhanced information and communication technology (ICT) coupled with advanced control algorithms to improve efficiency and reliability of system [1], [2]. Enhanced usage of ICT provides a number of advantages, but at the same time generates more cyber intrusion access points [3]. The synergy between heterogeneous physical and cyber components in a smart grid allows easy translation between cyber intrusions to a possible loss/damage of physical electric grid components [3]. Cyber intrusions may divulge confidential information, enable denial of service attacks leading to a loss of visibility and control of the system. Command and measurement injection attacks will lead to harming a system or incorrect control actions.

As part of the smart grid, intelligent electronic devices (IEDs) with embedded communication, intelligence, and information technologies enable local and/or remote sensing and control of substation equipments. IEDs also helps in control and protection mechanism of the electric power grid (EPG). If compromised, IEDs can maliciously remove generators or lines from the EPG.

Generally, EPGs are designed to handle a single contingency (the "N-1" case) without violating system security constraints and still meeting reliability criteria [4]. EPG security analysis ranks most critical physical components at given operating condition for planning and possible preventive control actions. Security analysis requires knowledge of complete EPG network topological characteristics and operations conditions [5]. Commonly studied "N-1" contingencies are the loss of a single line or generator. However, a coordinated cyber-attack can cause multiple generator or line contingencies simultaneously, resulting in a "N-X" contingency. Under such circumstances, power flows, voltages, and system frequency may vary outside tolerable constraints resulting in the conditions necessary for cascading failures leading to a system blackout [6].

It is necessary to understand and model such a possible "planned coordinated cyber-physical attack," so appropriate mitigation strategies can be determined [7]. Many approaches exist to provide vulnerability discovery, risk analysis, and recommended security practices for electric power systems. In [8], authors provide a cyber-security vulnerability analysis and solutions for various measurement and control systems found in EPG. The paper recommends evaluation of risk on the dependency of a system on the cyber infrastructure and discusses the importance of cyber infrastructure security in terms of its impacts on power grid applications. Liu *et al.* [9] describe a vulnerability analysis frame work for coordinated switching attacks against breakers in a power system. The authors in [10] discuss development of a cyber-to-physical bridge to provide an estimation of electric supply events caused by cyber-attacks. The paper further describes a methodology, Reliability Impacts from Cyber Attack (RICA), for measuring the impact of cyber-attacks on power system reliability. For finding physical vulnerabilities, bulk of existing literature are based on assuming complete knowledge of the system operating state, or information needed to carry out an ac or dc power flow [11], [12]. However, in most cases it would not be appropriate to assume a cyber-attacker is in possession of complete power system state information. Therefore, cyber-physical vulnerability assessments of a power system based on incomplete information [13] needs to be studied. In [7], coordinated planned attack with limited information was addressed with focus on exploring the application of graph theory and validating degree, eigenvector, closeness, vertex betweeness, and edge betweeness centrality measures against conventional dc power flow based linear sensitivity factor. In

Manuscript received April 01, 2012; revised September 08, 2012; accepted October 02, 2012. This work was supported in part by the Department of Energy (DoE) Award Number DE-OE0000097 (Trustworthy Cyber Infrastructure for the Power Grid). Paper no. TSG-00178-2012.

A. Srivastava, T. Ernster, and C. Vellaithurai are with the School of Electrical Engineering and Computer Science, Washington State University, Pullman, WA 99164 USA (e-mail: asrivast@eecs.wsu.edu).

T. Morris, S. Pan, and U. Adhikari are with the Department of Electrical and Computer Engineering, Mississippi State University, Mississippi State, MS 39762 USA (e-mail: morris@ece.msstate.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/TSG.2012.2232318

[7], it was determined that the closeness centrality measure tends to correlate well with the power system to a loss in bus injection contingency for the N-1 case.

The focus of this paper is addressing ICT and EPG vulnerabilities with incomplete information and to model an aurora-like event to cause maximum adverse impact to the smart grid. In this paper, aurora refers to a cyber event in which rapid opening and closing of a breaker near a generator causes excessive torque and may lead to physical harm to the generator [14]. The original research contribution of this paper is integration of cyber and physical vulnerability models given incomplete information. Specific contributions are a new cyber vulnerability ranking, a novel graph based N-X generator contingency ranking, an integrated cyber physical vulnerability index, and real time modeling of a coordinated aurora like event to demonstrate a cyber-physical attack. Closeness centrality measure for N-1 generator outage in [7] was further extended to the N-X case in this paper and combined with the new cyber vulnerability index for assessment of integrated cyber-physical vulnerability.

II. Vulnerability of ICT in Smart Grid

Communication networks are an integral part of monitoring and control infrastructure within the smart grid. These communication networks may be penetrated by external or internal attackers to perform 4 classes of attacks; reconnaissance, denial of service (DOS), command injection, and sensor measurement injection [14]. The relays and other intelligent electronic devices (IED) found in a smart grid may be connected to control room computers via dial-up modems, RS-232 [16], or Ethernet with TCP and UDP ports and services.

Communication systems in the smart grid may be penetrated at multiple locations. Control room and substation computers, IED, and communication equipment are typically isolated in an electronic security perimeter (ESP) [17]. The control room ESP connects to substation ESP via fiber optic, microwave, satellite, frame relay, or dial-up modem systems. The interconnections between ESP are considered untrusted and therefore ESP includes firewall to limit communication connections into and out of the ESP. The inter-ESP link may be wireless or may use leased bandwidth from a third party and is therefore at risk of penetration. ESP may also often have connections to corporate enterprise networks and external connections to other utilities or regional control centers via servers placed in demilitarized zones. Servers in demilitarized zones may use one-time password systems to limit access, may use certificates to authenticate attaching computers or users, or may require username and password entry. Penetration may occur through these external connections. The cyber devices in an ESP may be compromised by accidental introduction of malware via Universal Serial Bus (USB) thumb drive attack, virus penetration, or infected software patches. A compromised system within an ESP may establish communication via an ESP's existing network connections to outside attackers. Finally, devices within an ESP may be compromised intentionally by an individual with authorized physical access.

The Stuxnet [18] worm penetrated industrial control systems by first compromising control room computers by exploiting both USB thumb drive and printer server vulnerabilities. A commercial one-time password system vendor recently divulged key material for a commercially available one time password system after a spear phishing attack [19]. Spear phishing attacks may also be directed at utility employees with remote access to control system ESP. Wireless networks in industrial control systems may also be penetration points [20], [21]. Computers in ESP may also be compromised by malware introduced from infected patches or from viruses. Dial-up connections into ESP can be found via war dialing attacks [22]. Port scan attacks may be used to find IED connected to a penetrated Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) network [23].

After penetration, an attacker may perform reconnaissance, denial of service (DOS), command injection, or measurement injection attacks [17]. Reconnaissance attacks are used by a "penetrating attacker" to identify systems for attack before penetration and to learn system model and version details to enable future attacks after penetration. Denial of service attacks attempt to break communication links to stop command and sensor measurement traffic from reaching intended destinations. Command injection attacks send falsified commands to devices. Measurement injection attacks falsify or alter sensor measurements to indirectly cause a human or automated controller to take an incorrect control action.

Utilities perform vulnerability analysis on devices declared as cyber critical assets (CCA) [15]. Discovered vulnerabilities are ranked by severity. Vulnerability ranking systems attempt to measure likelihood of exploitation, complexity of an exploit, potential cost of exploitation, and the availability and cost of defenses against such exploits. The common vulnerability scoring system (CVSS) [24] is commonly used to estimate the risk associated with enterprise and information system cyber security vulnerabilities. Separate vulnerability assessment methodologies have been proposed for critical infrastructure [25].

A. Aurora Attack

A successful aurora attack would first require communication network penetration. This may happen by penetrating a communication link from control room to a generation or transmission relay/IED. After penetration the attacker would inject falsified commands to trip and reclose a relay in a rapid repetitive manner.

All relays have an intentional delay in operation to prevent control action during transients in the power system. These transients may be due to a sudden switching of a load on/off the grid. Relays are expected to protect the system by isolating faulty parts, while also preventing unnecessary tripping of power components due to short period transients. These delays result in a small window where no protection device actuates. This window is typically less than fifteen cycles to launch an aurora attack [14]. The objective of an aurora attack is to intentionally take a generator off the grid and connect it to the grid out of synchronism. This is facilitated by the opening and closing of a circuit breaker or combination of circuit breakers. For preventing out of synchronism connection of a generator to the grid, synchronism check relays are used. In the case of an aurora attack, it is assumed that the function of a synchronism

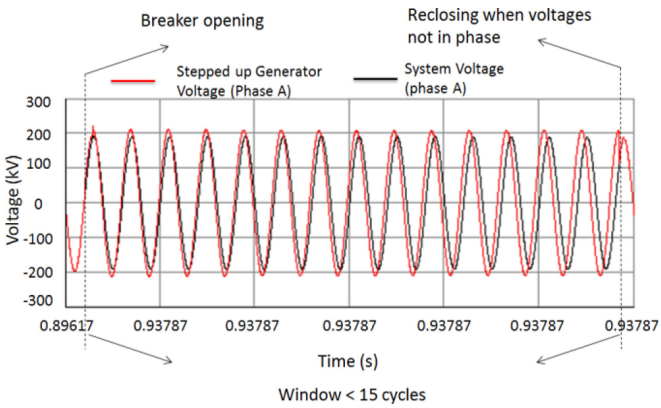

Fig. 1. Breaker opening and out of synchronism reclosing.

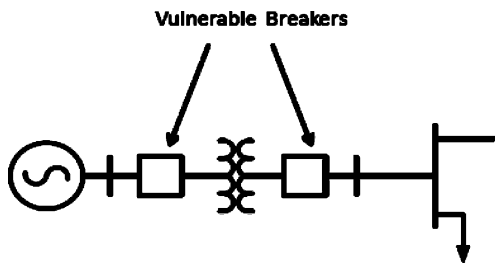

Fig. 2. Aurora attack with local beaker opening.

check element is compromised by hacking the relay. It may also be absent in the case of attack due to operation of remote breaker away from the generator. The breaker opening and out of synchronism reclosing can be seen in Fig. 1.

When the circuit breaker is opened, the generator is isolated from the grid. The mechanical power input to the generator changes slowly due to the governor action being slow. Due to the continued mechanical power input, the generator starts to speed up and the frequency of the generator starts to increase. This leads to frequency difference between the grid and the generator. The angle of separation starts to increase with time. The window for attack is only 15 cycles and hence the circuit breaker is closed before this time window expires [26]. The generator is now pulled into synchronism with "out-of-sync" conditions and this causes large electrical and mechanical transients. These transients may lead to permanent damage to the generators, if opening and closing operation is repeated as demonstrated by the experiment at the Idaho National Laboratory [26]. The aurora attack can be a simple manual physical opening and reclosing of a circuit breaker in a substation or a sophisticated attack, which involves hacking into the communication channel of a substation to alter the settings relays to cause operation of the circuit breakers. There could be two types of possible aurora attack:

1) Scenario 1:-Local Attack: As shown in Fig. 2, a local aurora attack generally involves the operation of the breakers close to the generator within a generation level substation.

2) Scenario 2:-Remote Breaker Attack: Depending on the topology of the system, the attack can be successful by attack on breakers, which would still cause isolation of the generator from the grid like tie line breakers as shown in Fig. 3.

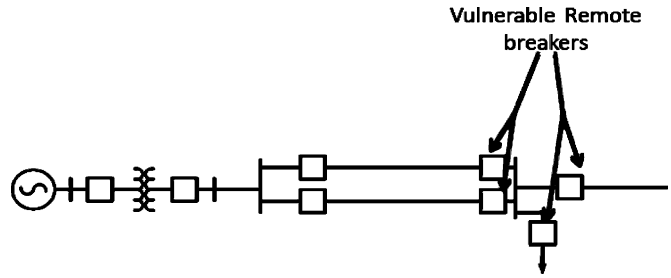

Fig. 3. Aurora attack with remote beaker opening.

B. A New Approach for Cyber Vulnerability Ranking

An attacker who penetrates a utility communication network may find many relays to operate breakers leading to aurora attack. Attacker may develop a scoring system to decide which relay is the most vulnerable for aurora attack. A sample scoring methodology is presented here with potential vulnerability ranking criteria: discovery, finger printing, access, detection threat and, connection speed.

Relay *discovery* includes penetration of the local area network connected to a relay and identification of a relay on the network. For an Ethernet network this requires penetration of the electronic security perimeter. For dialup connection this discovery requires successfully finding a dial up phone number into a substation and then successfully penetrating the secure dial up gateway by providing a valid authentication code. Once connected to the substation local area network (LAN), Ethernet connected relays may be discovered using port scanning tools such as the network mapping program NMAP [27]. Relays connected to a dial-up gateway by serial connection may be discovered by Modicon-Bus (MODBUS) address scanning. Discovery (d_i) is scored with a binary value $(0 = \text{no discovered}, 1 = \text{discovered})$. Access is the ability to access and control the relay. Accessibility (a_i) is scored with a binary value $(0 = \text{not accessible}, 1 = \text{accessible})$. Discovered relays may be finger printed to identify the relay brand and model. Attackers often access vulnerability lists to learn potential weaknesses of a device. The feasibility of an attack against a relay depends upon knowledge of a vulnerability which allows the attacker to assume control of the relay. Feasibility (f_i) is scored with a binary value $(0 = \text{not feasible}, 1 = \text{feasible})$.

Access exceeds connectivity and feasibility in that the relay is discovered, vulnerability is known, and an exploit is available to allow the attacker to assume control of the relay. Detection threat is the risk that an attack will be discovered before successfully damaging the generator. Detection threat is less with a RS-232 or dialup connection since intrusion detection systems for these systems are uncommon [15]. Detection threat increases as network penetration time increases. Therefore, if an attack requires long-term penetration to learn passwords, the detection threat will be higher than a short penetration time. Detection threat is scored with a three values $(0 = \text{no threat}, 1 = \text{low threat}, 2 = \text{high threat})$. Communication connection speed impacts potential aurora attack success. Slower connection speed may limit how fast the trip and reclose commands can be sent. Connection speed is scored with 3 values $(0 = s_i <= 1200, 1 = 2400 > s_i > 19200, 2 = s_i >$

TABLE I
POSSIBLE VULNERABILITY INDEX VALUES

d_i	f_i	a_i	s_i	t_i	v_i	*Description*
1	1	1	2	0	5	High s_i, low t_i, maximum v_i
1	1	1	2	1	4	High s_i, medium t_i, medium-high v_i
1	1	1	1	0	4	Medium s_i, low t_i, medium-high v_i
1	1	1	2	2	3	High s_i, high t_i, medium v_i
1	1	1	0	0	3	Low s_i, low t_i, medium v_i
1	1	1	1	1	3	Medium s_i, medium t_i, medium v_i
1	1	1	1	2	2	Low s_i, medium t_i, medium-low v_i
1	1	1	0	1	2	Low s_i, medium t_i, medium-low v_i
1	1	1	0	2	1	Low s_i, high t_i, low v_i
0	-	-	-	-	0	Not discovered, 0 v_i
-	0	-	-	-	0	Not feasible, 0 v_i
-	-	0	-	-	0	Not accessible, 0 v_i

$19200\ \mathrm{baud}$). Connection speed is not related to network penetration time. An attacker may connect to the network to monitor traffic to perform reconnaissance necessary to execute a successful aurora attack. This reconnaissance period is the network penetration time and as the length of the reconnaissance period increases more artifacts of the penetration are created and therefore detection threat increases. Connection speed refers only to the communication link bandwidth.

$$v_i = d_i{}^* f_i{}^* a_i{}^* (s_i - t_i + 3). \tag{1}$$

Equation (1) gives the vulnerability index (v_i). The vulnerability index has possible values of $\{0 \cdots 5\}$. The minimum vulnerability index value, 0, indicates minimum risk and the maximum value, 5, indicates maximum risk.

Table I shows the possible values for the vulnerability index (v_i). Subtracting detection threat (t_i) from connection speed (s_i) in the vulnerability index product allows detection threat to counter connection speed such that a high-speed connection with high detection threat has a low score while a high-speed connection with low detection threat has the highest possible score. As the connection speed increases the vulnerability increases. As the detection threat increases the vulnerability index decreases. The lowest possible score of 0 is reserved for the cases where the relay is not discovered $(d_i = 0)$, is not accessible $(a_i = 0)$, or an attack is infeasible $(f_{i=0})$. Nonzero values are required for all these parameters for a successful attack. The " $+3$" term in (1) ensures that if a relay is discoverable, accessible, and an attack is feasible the vulnerability index will be non-zero indicating there is always some risk in this situation.

The above developed vulnerability index will be used to rank the cyber vulnerability to attack a relay to cause opening and closing a breaker.

III. VULNERABILITY OF PHYSICAL SMART GRID

To cause a maximum adverse generator outage impact on EPG, it is necessary to find the most critical set of generators. An attacker would mass their resources in damaging these critical set of generators to remove from service. Security analysis contingency ranking schemes identify critical generators or lines based on the severity of impact on the system. Existing research concerning contingency ranking typically relies on knowing the operational state of the power system, such as the voltage magnitude and MW injection at each PV buses, the MW and MVAr injection at all PQ buses, and the topology parameters of branches connecting the system buses. However, bus voltage and power injection are dynamic variables. Yet the system topology tends to remain considerably more static.

It must therefore be considered unlikely that an outside attacker will know the precise operational state of a power system (line MVA flows, bus voltages, generation dispatch, load demand) at the time of an intended coordinated attack. Accordingly, conventional contingency screening algorithms would be difficult to be utilized by attackers in assessing the physical vulnerability of a power system. A more simple power system vulnerability analysis method will need to be employed that selects critical targets for a coordinated cyber-attack based on topology data. Topology based physical vulnerability assessments could be easily performed by attackers with non-confidential publicly available information.

Existing use of topology based electrical distance characteristics in contingency analysis is limited to the concept of concentric relaxation, which establishes a geographical boundary for the impact of a given contingency based on the assumption that the effects of a contingency are principally local [28]. While the use of concentric relaxation assumptions is conventionally utilized to speed up contingency analysis by fixing bus voltages and phase angles outside a certain boundary layer, the concept forms a basis for utilizing topology based studies of a power system for limited information attack scenario planning.

The use of graph theory in performing a limited information topology based contingency analysis is rooted in the power flow equations given by (2) and (3):

$$P_i = \sum_{j=1}^{n} V_i V_j Y_{ij} \cos(\delta_i - \delta_j - \theta_{ij}) \tag{2}$$

$$Q_i = \sum_{j=1}^{n} V_i V_j Y_{ij} \sin(\delta_i - \delta_j - \theta_{ij}) \tag{3}$$

where P_i and Q_i are the active and reactive power injection at bus i, $V_i \delta_i$ is the voltage and phase angle at bus i (or bus j depending on the subscript), and Y_{ij} is the element of the bus admittance matrix defining the admittance between buses i and j[5]. Conventional forms of contingency analysis utilize forms of the power flow equations to assess the impact of loss of a generator or line on the branch flows and bus voltages. In the case of a generator outage, the lost MW injection must be made up by other remaining generators in the power system. Such a redispatch in generation will change the steady state bus voltage and line flow values from the pre-outage state.

Even if an external attacker is not likely to know the voltage and power injection at each bus, the bus admittance matrix terms can be readily estimated based on line and transformer physical characteristics available from public information and intelligent guesses. Knowing that topology plays a role in the calculation of the post-contingency state of a power system after a generator outage, the severity of changes in MW and MVAr injections and voltages must be assessed based on the topology of a given electric grid. Naturally, this cannot be assessed by conventional mathematical derivation. However, by performing statistical tests comparing graph theory based vertex ranking schemes and conventional dc power flow based generation shift factor measures, results can be presented in support of certain graph

theory based ranking techniques in predicting the sensitivity of a power system to loss in generation at specific buses.

A. A Novel Approach of N-X Generator Contingency Ranking With Incomplete Information Using Graph Theory

For purposes of topology analysis, a power system will be modeled as a graph G, where the buses in a power system are treated as a set of vertices V and the branch components as the set of edges E. As it would be improper to treat all transmission lines and transformers in a power system as equal, the edges in a graph model of a power system must be assigned weights to reflect the inherent dissimilarity between branch components. While branch impedances Z consist of both a resistive component R and reactive component X, edge weights are assigned based on the magnitude of X since generally $X \gg R$ for most branches in a power system [29].

Given such a graph model of a power system, the question remains concerning how to use such a model to identify the most critical components in the system. For purposes of determining which generator to target for a cyber-attack, we will utilize concepts of vertex centrality. Vertex centrality measures assign ranking coefficients to vertices in a graph, from which we can deduce that the most important generators are those located on a bus with a highly ranked vertex centrality. While there are numerous vertex centrality measures, evidence is strongest in support of the relationship between closeness centrality in relation to more conventional methods of assessing the impact of generator outages [7]. Formally, closeness centrality for a n bus power system is defined as:

$$C_C(v_i) = \frac{\sum_{j \in V \setminus i} d(i,j)}{n-1}. \tag{4}$$

Here, determination of closeness centrality relies upon the shortest path matrix D_G with entries $d_G(i,j)$ that indicate the shortest path from a bus i to another bus j. Determination of D_G relies on a shortest path algorithm, such as the Floyd-Warshall [30], [31], Dijkstra [32], Bellman-Ford [33], [34], or Johnson's algorithm [35]. One of the issues associated with validating closeness centrality is that, as a topological based vulnerability assessment algorithm, it is subject to inaccuracies under certain actual operating conditions of the power system. When selecting targets based on topology vulnerability, a rough estimation of power generation at a specific bus would be required to ensure attack resources are not wasted removing a small generator from service. The closeness centrality algorithm can be validated against the dc power flow based generation shift factor (GSF). The GSF is defined as:

$$a_{li} = \frac{\Delta f_l}{\Delta P_i}. \tag{5}$$

where Δf_l is the change in MW power flow on line l when a change in MW generation ΔP_i occurs at bus i. The dc power flow based assumptions of neglecting MVAR flows and bus voltage magnitudes only introduces errors in calculated line flows of approximately 5% [5]. In order to assess the overall impact of all line redistributions attributed to a given generator outage, the GSF is utilized to generate a generator shift impact factor (GSIF) a_i defined as:

$$a_i = \sum\nolimits_l |a_{li}|. \tag{6}$$

For all non-swing buses i reflecting the sum of the magnitude of the factors a_{li} attributable to bus i, or the L_1 norm of each column of a_{li}. In one of the previous publication, authors of this paper have shown that there exists a negative correlation between closeness centrality and the GSIF, which together with nonparametric statistical ranking tests provides evidence in support of the closeness centrality measure as a means to reflect the severity of a given generator outage contingency based on limited information [7].

In this paper, we extended the closeness centrality concept to the general case involving N-X generator outages. A subset of vertices $V_{gen} \subseteq V\,(G)$ are defined as the non-swing generator buses of the power system being modeled as a graph G. For some N-X contingency, $k \in \mathbb{R}^X$, we define the set of X verticies reflecting the buses locations of each generator outage as $V_{cont} = \{v_k\} \subseteq V_{gen}$. A new closeness centrality impact measure CI_c can then be introduced reflecting a collective topology assessment of multiple generator outages, defined as:

$$CI_C(k) = \sum\nolimits_{i \in V_{cont}} |C_C(v_i)|. \tag{7}$$

IV. Test Case Studies

To test the developed algorithms for cyber and physical vulnerability, two standard test systems have been used here: IEEE 14 bus system and IEEE 118 bus system [36].

A. IEEE Test Cases

The IEEE 14 bus system is shown in Fig. 4. The IEEE 14 bus system was modified for simulation purposes. The following changes were made as shown in Table II:

i. All synchronous condensers were changed to generators.
ii. Circuit breakers were included after each generator before being connected to the grid.
iii. Generation values at each bus were modified to the values shown in Table I.

The IEEE 118 bus system consists of 186 branches, 64 PQ buses, and 54 voltage controlled buses (19 are MW producing generators and 35 are condensers producing MVARs).

B. Simulation Tools

MATLAB: Since conventional power systems analysis software packages do not include graph theory analysis tools, code was written in MATLAB to implement the graph theory vulnerability analysis algorithms. Using the MATPOWER package of M-files, the generation shift factors were calculated. Additionally, MATLAB code was written to compare the graph theory results with the MATPOWER generated GSF factors [37].

RTDS: The Real Time Digital Simulator (RTDS) [38] is an example of virtual power system simulator designed for continuous real time operation. Models of the simulated power system are defined using a graphical modeling language,

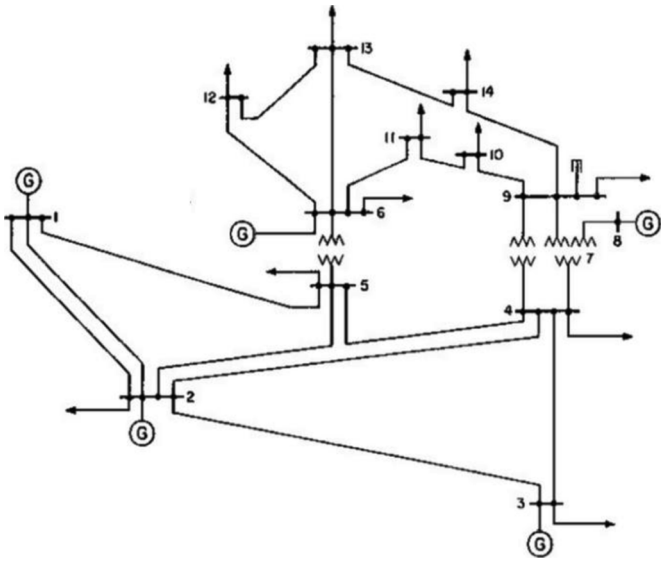

Fig. 4. Modified IEEE 14 bus system.

TABLE II
GENERATION DATA FOR MODIFIED IEEE 14 BUS SYSTEM

Bus Number	MW	Mvar	MVA
1 (G1)	106.6	4.147	150
2 (G2)	37.4	17.37	60
3 (G3)	41.6	2.627	60
6 (G4)	41.6	-3.283	60
8 (G5)	41.6	16.68	60

RSCAD. RTDS can be connected to external devices that allow closed loop testing of real-world physical equipment, like relay [38].

Wireshark: is an Ethernet data logger used to capture, store, and display network packets. Packets are time-stamped and each network layer is shown individually. Wireshark was used to capture and study relay trip and reclose packets [39].

Ettercap: is a man-in-the-middle (MITM) framework which allows attackers to design and execute MITM attacks against network switches [40].

Expect: is a script language used to automate and replicate queries and responses manual command line interfaces. Expect was used to automate sending relay command passwords and trip and reclose commands [40].

Python: is a script language with high levels of abstraction. Python libraries were used to send MODBUS packets containing open and reclose commands [41].

C. Simulation Results

1) Generator Contingency Ranking: Using developed algorithm for generator contingency, set of generators for both the cases were ranked for "N-1," "N-2," and "N-3" contingency for the IEEE 14 and 118 bus system as shown in Tables III–VI. Note that developed algorithm can be easily extended for higher contingencies. From a cyber attacker's perspective, they may not know the exact dispatch of each generator, voltage set points, or the demand at each load. However, we assume that the attacker can determine the topology and branch impedances from publically available maps showing the location and voltage base

TABLE III
N-1 AND N-2 GENERATOR OUTAGE CONTINGENCY RANKING FOR THE MODIFIED IEEE 14 BUS SYSTEM

Rank	N-1 Contingencies			N-2 Contingencies		
	Gen	Bus	C_C	Gens	Buses	CI_C
1	G5	8	1.7857	G3,G5	3,8	3.8205
2	G3	3	2.0348	G2,G5	2,8	4.0261
3	G2	2	2.2404	G4,G5	6,8	4.2454
4	G4	6	2.4597	G2,G3	2,3	4.2752
5	N/A	N/A	N/A	G3,G4	3,6	4.4945
6	N/A	N/A	N/A	G2,G4	2,6	4.7001

TABLE IV
N-3 GENERATOR OUTAGE CONTINGENCY RANKING FOR THE IEEE 14 BUS SYSTEM

Rank	N-3 Contingencies		
	Gen	Bus	CI_C
1	G2,G3,G5	2,3,8	6.0609
2	G3,G4,G5	3,6,8	6.2802
3	G2,G3,G4	2,3,6	6.7349

TABLE V
TOP FIVE N-1 AND N-2 GENERATOR OUTAGE CONTINGENCY RANKING FOR THE IEEE 118 BUS SYSTEM

Rank	N-1 Contingencies			N-2 Contingencies		
	Gen	Bus	C_C	Gens	Buses	CI_C
1	G15	87	1.0875	G15,G19	87,111	2.3415
2	G19	111	1.2540	G15,G16	87,89	2.4728
3	G16	89	1.3853	G16,G19	89,111	2.6393
4	G6	46	1.6680	G6,G15	46,87	2.7555
5	G8	54	1.7041	G8,G15	54,87	2.7916

TABLE VI
TOP FIVE N-3 GENERATOR OUTAGE CONTINGENCY RANKING FOR THE IEEE 118 BUS SYSTEM

Rank	N-3 Contingencies		
	Gen	Bus	CI_C
1	G15,G16,G19	87,89,111	3.7268
2	G15,G16,G18	87,89,103	4.2592
3	G15,G16,G17	87,89,100	4.4130
4	G16,G17,G19	89,100,111	4.5795
5	G5,G6,G15	31,46,87	4.6696

of generators, substations, and transmission lines. For the modified IEEE 14 bus system, there are limited numbers of choice for possible generator attack with 5 generators.

Tables III and IV show the "N-1," "N-2," and "N-3" contingency ranking for modified IEEE 14 bus system. Tables V and VI show top five "N-1," "N-2," and "N-3" contingency rankings for the IEEE 118 bus system. An attacker interested in targeting a subset of the 19 generators based on the physical vulnerability of the system is modeled such that the impact of a coordinated generator attack has the greatest chance of causing a maximal adverse reliability impact. Detailed analyses for IEEE 118 bus system are not shown here due to space limitations.

2) Cyber Vulnerability Ranking: All the relays connected to generator breakers were ranked using the developed cyber vulnerability ranking. Table VII shows an example vulnerability ranking for the 5 generator relays from the modified IEEE 14 bus system. Relays 2, 3, 4 and 5 have been discovered by an attacker and therefore share discovery (d_i) scores of 1. Relay 1 is unknown to the attacker and therefore has a discovery (d_i) score of 0, eliminating it from attack consideration. The attacker has

TABLE VII
VULNERABILITY RANKING FOR THE IEEE 14 BUS SYSTEM

Relay	d_i	f_i	a_i	s_i	t_i	v_i
1	0	-	-	-	-	0
2	1	0	-	-	-	0
3	1	1	1	1	1	3
4	1	1	1	0	1	2
5	1	1	1	2	1	4

finger printed relays 3, 4, and 5 to learn the manufacturer and model number of the relays and has learned of vulnerabilities for each via internet search, hence a feasibility score (f_i) of 1 for each. Relay 2 may have been finger printed but no vulnerability is known and therefore has a feasibility (f_i) score of 0, eliminating it from attack consideration.

For this example a highly capable attacker is assumed. The highly capable attacker will be able to exploit all known vulnerabilities. Relays 3, 4, and 5 have been discovered and are feasible and accessible. Relay 3 is connected to a compromised dial-up modem gateway with baud rate of 1200 bits per second giving a speed score of 0, and a detectability threat score of 0 since the dial-up network is unlikely to include an intrusion detection system (IDS). The low connection speed limits the likelihood of an effective aurora attack; however, the low detection threat results in medium risk. Relay 5 is connected to a 10 megabit per second Ethernet network, which results in a connection speed score of two. Relay 5 is given a detectability threat score of 1 since the Ethernet network may have include an IDS, though the likelihood of IDS in a substation is low. Relay 4 connected to a compromised substation computer with TCP-to-Serial converter with a 9600 bits per second link to the relay. Relay 4 has a speed score of 1 based on the slowest portion of the link and a detection threat score of 1 since connecting to over Ethernet increases detection risk. Based upon the vulnerability ranking function from (1), relay 5 is the most likely to be the source of the aurora attack.

To execute an aurora attack, an attacker must first penetrate a communication interface connected to a generator relay. The communication interface may be dialup modem, RS-232, or a routable connection. For dialup, a war dialing program may be used to find modems which answer in prefixes and area codes which match other phones at a generation facility. RS-232 connections are non-routable. Penetrating a RS-232 connection requires either compromising a master terminal which may be reachable via routable network or compromising the interconnection between the master terminal and the remote device which may use frame-relay or a wireless interconnection. Routable networks may be penetrated at the ESP boundary or by compromising a device within the ESP connected to the same communication network as the generator relay.

Relays often are configured with logic to allow remote trip and reclose commands. The aurora attack requires repeatedly sending trip and reclose commands to the generator relay. Before initiating the aurora attack the attacker may finger print the relay to ensure settings include both trip and reclose logic. If the relay settings do not support remote trip and reclose commands the settings may be changed, if the attacker knows the relay's settings password. Typically the settings password may

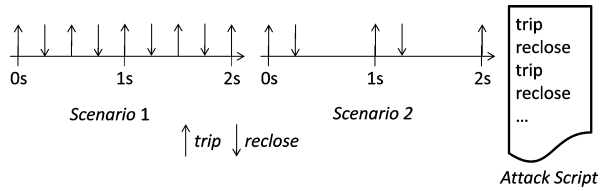

Fig. 5. Attack scenarios.

be learned by eavesdropping on communications between control room and the relay. The settings password is typically transmitted as plaintext and is easy to learn.

After ensuring the relay settings support remote trip and reclose commands a command injection attack is required to rapidly send the relay trip and reclose commands. Relays typically require command password entry before allowing remote command execution. The attacker can learn the relay password by eavesdropping on communications between control room and the relay, if it exists.

Two relays based on vulnerability ranking were attacked in experiments for this study. Relay 3 included a telnet service to allow remote control. Relay 5 included a MODBUS service to allow remote control. In both cases command password are used to authorize commands. In both cases, entry of the command password initiates an escalated privilege session in which the command password is entered once and then any amount of commands may subsequently entered until the escalated privilege session times out.

For Relay 3, an Expect script [39] was used to automate sending trip and reclose commands via command line interface relay using a Telnet session. Fig. 5 diagrams the two attack scenarios. Two scenarios were implemented and testing was done in laboratory experiments. In the first scenario, the trip and reclose commands are separated by 0.25 seconds and then repeated. In the second scenario, the trip command is sent then the reclose command is sent 0.25 seconds later, then the attack script waits 0.75 seconds and repeats.

For Relay 5, MODBUS packets were sent to trip and reclose the breaker. The exact function code and register contents required to trip and reclose the relay were learned via eaves dropping. Wireshark [38] was used to capture MODBUS traffic during a remote trip and reclose scenario. The individual MODBUS packets were then manually extracted from the Wireshark data and used with a Python [40] script to send the trip and reclose packets with the same timings described for scenario 1 and 2 for Relay 3.

3) Integrating Cyber Vulnerability With Physical Vulnerability Ranking: Developed cyber vulnerability can be combined with physical vulnerability in number of different ways. In this work, the simple formula for integrated cyber physical vulnerability ranking (CP) used is:

$$CP = CI_c * \sum_{i=1}^{N} \frac{(6 - v_i)}{N} \quad \text{if } v_i \neq 0$$
$$CP = \frac{N}{A} \quad \text{if } v_i = 0;.$$

Here N is the number of relays/generators in the system. Note that for single generator C_c will be used instead of CI_c. A lower cyber physical vulnerability infers a more vulnerable system.

TABLE VIII
CYBER PHYSICAL VULNERABILITY RANKING FOR N-1 AND N-2 CONTINGENCIES IN IEEE 14 BUS SYSTEM

Rank	N-1 Contingencies			N-2 Contingencies		
	Gen	Bus	CP	Gens	Buses	CP
1	G5	8	3.5714	G3,G5	3,8	9.5512
2	G3	3	6.1044	G4,G5	6,8	12.7362
3	G4	6	9.8388	G3,G4	3,6	15.7307
4	G2	2	13.4424	G2,G5	2,8	N/A
5	N/A	N/A	N/A	G2,G3	2,3	N/A
6	N/A	N/A	N/A	G2,G4	2,6	N/A

TABLE IX
CYBER PHYSICAL VULNERABILITY RANKING FOR N-3 CONTINGENCIES IN IEEE 14 BUS SYSTEM

Rank	N-3 Contingencies		
	Gen	Bus	CP
1	G3,G4,G5	3,6,8	18.8406
2	G2,G3,G5	2,3,8	N/A
3	G2,G3,G4	2,3,6	N/A

This developed integrated index will be used to attack most vulnerable generator with maximum impact on system.

The generator(s) to attack were selected based on the integrated cyber physical vulnerability ranking. Integrated cyber physical vulnerability indices are shown in Tables VIII and IX. If the CP index is N/A, it means that an aurora type cyber-attack is not possible for that combination. For example, in Table VII, it can be seen that the relay at generator 2 is not considered for attack. Hence any combination with generator 2 will not have a CP associated with it. The combination with least CP index is chosen in each contingency for RTDS simulation.

4) Real Time Simulation: The IEEE 14 bus system was modeled in RSCAD and simulated in the RTDS. Five different cases were simulated to represent N-1, N-2, and N-3 contingencies. The results obtained were found to be close to the expected values. System was modified and simulated in RTDS for aurora like event.

5) Case 1: Breaker opened for 0.25 seconds and closed for 0.25 seconds, single generator (G5) attack (scenario 1): The results obtained are shown in Fig. 6. It was observed that there is rapid variation in the electrical torque, current, speed, and power output of the machine. When the machine is connected out of phase with the grid, it experiences a synchronizing torque which tries to pull the machine back into synchronism. The machine experiences very high mechanical stress which will lead to potentially irreversible damage to the machine.

6) Case 2: Breaker opened for 0.25 seconds and closed for 0.75 seconds, single generator (G5) attack (scenario 2): Simulation results are shown in Fig. 7.

7) Case 3: Breaker opened for 0.25 seconds and closed for 0.25 seconds, two generator attack (G3 and G5) (scenario 1): In this case, the attack is coordinated to attack two generators simultaneously. G3 and G5 are selected based on the contingency ranking. This is repeated six times and then the generators are taken out of the system to simulate effect on system due to loss of the generators. It was observed that there is a voltage collapse as the power required cannot be supplied by the slack bus/other generators due to capacity limitations. This leads to a blackout. Simulation results from RTDS are shown in Fig. 8.

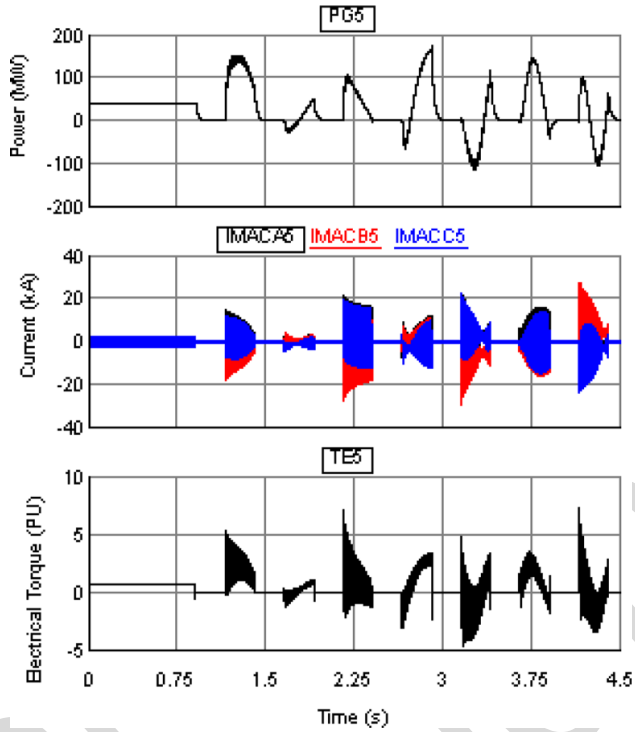

Fig. 6. Power output, current, electrical torque for Case 1 in RTDS.

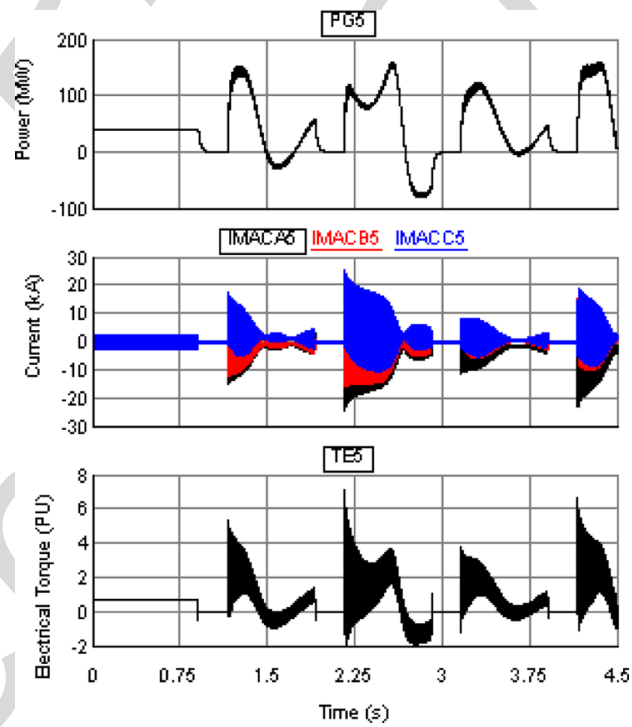

Fig. 7. Power output, current, electrical torque for Case 2 in RTDS.

8) Case 4: Breaker opened for 0.25 seconds and closed for 0.75 seconds, two generator attack (G3 and G5, scenario 2): Simulation results are shown in Fig. 9.

9) Case 5: This case shows the simulation results for an "N-3" contingency, wherein three generators are targeted by the attacker. Note that top ranked cyber-physical vulnerability will be combination of G3, G4, and G5 based on the cyber-vulnerability ranking and generator outage contingency ranking. It was

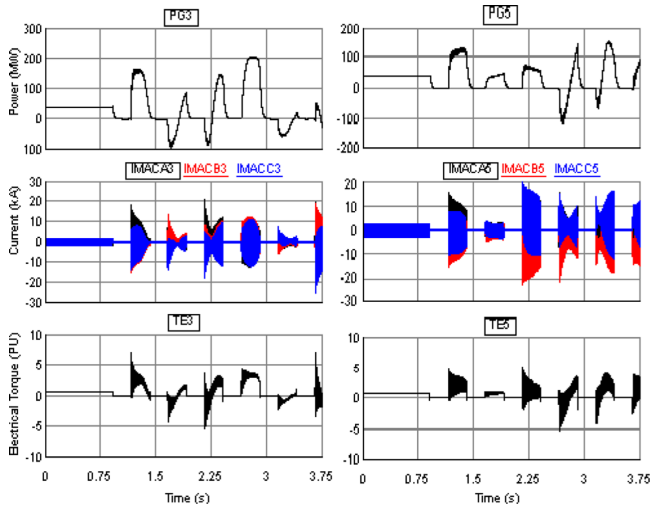

Fig. 8. Power output, current, electrical torque for Case 3 in RTDS.

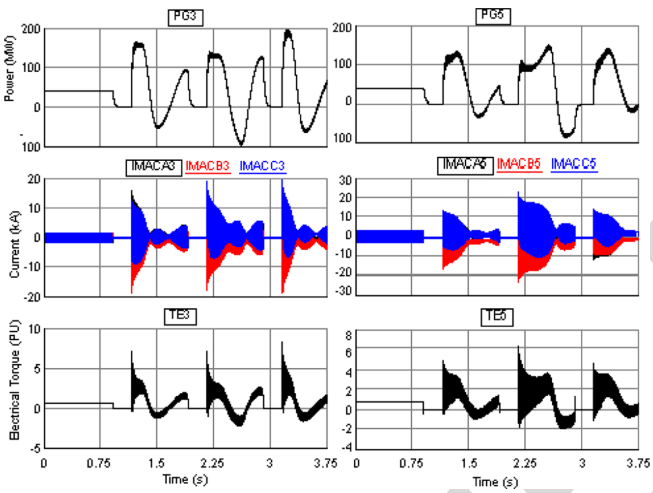

Fig. 9. Power output, current, torque for Case 4 in RTDS.

observed that N-3 contingency would lead to massive load shedding and drop in voltage as shown in Figs. 10 and 11. The basic idea of an aurora attack is to cause damage to the generators in such a way that the other protective equipment do not cause trip. However for a N-3 contingency on the IEEE 14 bus system, it is very likely that other protective equipment will also cause a trip.

These results demonstrate the impact of an aurora kind of attack on the test case considered here. Repeated transients such as the ones seen in the simulation will lead to potential damage to generators. The generators will not be available for restoration operation. This will create problem in restoration of the system after blackout/brownout caused by cyber-attack. Results presented here can be easily extended for IEEE 118 bus system similar to IEEE 14 bus analysis.

V. Conclusions

Integrated cyber physical vulnerability of smart grid with limited information has been presented in this paper. A new cyber vulnerability index based on discovery, feasibility, access, detection threat and connection speed has been developed. New graph theory based, multi contingency physical vulnerability algorithms have been also discussed. Integrated cyber physical

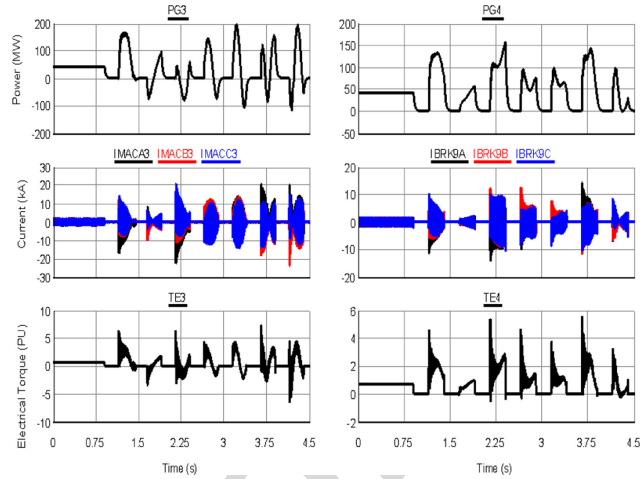

Fig. 10. Power output, current, torque for Case 5 in RTDS (G3 and G4).

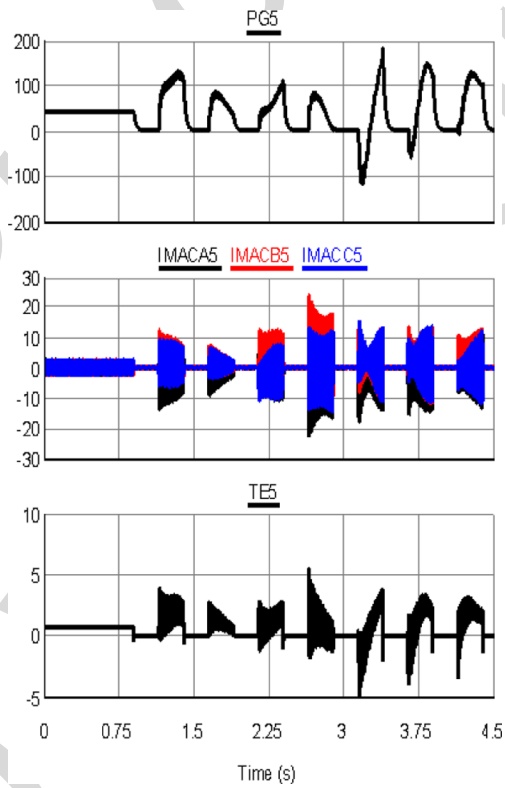

Fig. 11. Power output, current, torque for Case 5 in RTDS (G5).

vulnerability index has been developed and has been utilized for real time modeling to demonstrate impact of aurora attack. Test case results for IEEE 14 and IEEE 118 bus test case show an adverse impact on power grid. Mitigation techniques need to be developed to avoid such coordinated cyber-physical attacks on the smart grid.

References

[1] S. 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.

[2] E. Santacana, G. Rackliffe, L. Tang, and X. Feng, "Getting smart," *IEEE Power Energy Mag.*, vol. 8, no. 2, pp. 41–48, Mar.–Apr. 2010.

[3] T. Morris, A. K. Srivastava, B. Reaves, K. Pavurapu, R. Vaughn, W. McGrew, and Y. Dandass, "Engineering future cyber-physical energy systems: Challenges, research needs, and roadmap," in *Proc. North Amer. Power Symp.*, Oct. 4–6, 2009.

[4] *Reliability Standards for the Bulk Electric Systems of North America*, NERC Standard TOP-002-2, May 2009.
[5] A. J. Wood and B. F. Wollenberg, *Power Generation Operation and Control*, 2 ed. New York, NY, USA: Wiley, 1996, pp. 421–427.
[6] D. Kirschen, "Power system security," *Power Eng. J.*, vol. 16, no. 5, pp. 241–248, Oct. 2002.
[7] T. A. Ernster and A. K. Srivastava, "Power system vulnerability analysis-towards validation of centrality measures," in *Proc. IEEE T&D Conf. Expo.*, Orlando, FL, May 2012.
[8] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.
[9] S. Liu, X. Feng, D. Kundur, T. Zourntos, and K. Butler-Purry, "Switched system models for coordinated cyber-physical attack construction and simulation," in *Proc. IEEE 1st Int. Workshop Smart Grid Model. Simul. (SGMS)*, Oct. 17, 2011, pp. 49–54.
[10] J. Stamp, A. McIntyre, and B. Ricardson, "Reliability impacts from cyber attack on electric power systems," in *Proc. IEEE Power Syst. Conf. Expo.*, Mar. 15–18, 2009, pp. 1–8.
[11] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 382–390, Jun. 2011.
[12] 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.
[13] L. Fu, W. Huang, S. Xiao, Y. Li, and S. Guo, "Vulnerability assessment for power grid based on small-world topological model," in *Proc. Asia-Pacific Power Energy Eng. Conf. (APPEEC)*, Mar. 2010.
[14] M. Zeller, "Myth or reality-does the aurora vulnerability pose a risk to my generator," in *Proc. 37th Annu. Western Protective Relay Conf.*, Spokane, WA, Oct. 2010.
[15] T. Morris, R. Vaughn, and Y. Dandass, "A retrofit network intrusion detection system for MODBUS RTU and ASCII industrial control systems," in *Proc. 45th IEEE Hawaii Int. Conf. Syst. Sci. (HICSS-45)*, Grand Wailea, Maui, Jan. 4–7, 2012.
[16] M. Seyer, *RS-232 Made Easy: Connecting Computers, Printers, Terminals, and Modems*. Upper Saddle River, NJ, USA: Prentice-Hall, 1984.
[17] "Critical infrastructure protection (CIP)," NERC, North American Electric Reliability Corporation [Online]. Available: http://www.nerc.com/page.php?cid=2|20
[18] N. Falliere, L. Murchu, and E. Chien, "BW32.Stuxnet Dossier," Symantec, Tech. Rep., 2010.
[19] B. Parmar, "Protecting against spear-phishing," *Computer Fraud Security*, vol. 2012, no. 1, pp. 8–11, Jan. 2012.
[20] B. Reaves and T. Morris, "Discovery, infiltration, and denial of service in a process control system wireless network," in *Proc. IEEE eCrime Researchers Summit*, Tacoma, WA, Oct. 20–21, 2009.
[21] J. Slay and M. Miller, "Lessons learned from the Maroochy water breach," in *Critical Infrastructure Protection*, ser. IFIP International Federation for Information Processing, E. Goetz and S. Shenoi, Eds. Boston, MA: Springer, 2008, vol. 253, pp. 73–82.
[22] H. Berghel, "Wireless infidelity I: War driving," *Commun. ACM*, vol. 47, no. 9, pp. 21–26, Sep. 2004.
[23] P. Oman, E. Schweitzer, and J. Roberts, *Safeguarding IEDS, Substations, and SCADA Systems Against Electronic Intrusions*. Pullman, WA: Schweitzer Engineering Labs..
[24] P. Mell, K. Scarfone, and S. Romanosky, "Common vulnerability scoring system," *IEEE Security Privacy*, vol. 4, no. 6, pp. 85–89, Dec. 2006.
[25] S. Wang, L. Hong, and X. Chen, "Vulnerability analysis of interdependent infrastructure systems: A methodological framework," *Physica A: Stat. Mech. Its Appl.*, vol. 391, no. 11, pp. 3323–3335, Jun. 2012.
[26] J. Meserve, "Staged cyber-attack reveals vulnerability in power grid," in CNN 2007 [Online]. Available: www.cnn.com/2007/US/09/26/power.at.risk/
[27] G. Lyon, *NMAP Network Scanning Official NMAP Project Guide to Network Discovery and Security Scanning*. Sunnyvale, CA: Insecure Press, 2008.
[28] J. Zaborszky, W. Keh-Wen, and K. Prasad, "Fast contingency evaluation using concentric relaxation," *IEEE Trans. Power App. Syst.*, vol. PAS-99, no. 1, pp. 28–36, Jan. 1980.
[29] Z. Wang, A. Scaglione, and R. J. Thomas, "Electrical centrality measures for electric power grid vulnerability analysis," in *Proc. 29th IEEE Conf. Decision Control*, Dec. 2010, vol. 15, pp. 5792–5797.
[30] R. W. Floyd, "Algorithm 97: Shortest path," *Commun. ACM*, vol. 5, pp. 345–345, Jun. 1962.
[31] S. Warshall, "A theorem on boolean matrices," *J. ACM*, vol. 9, pp. 11–12, Jan. 1962.
[32] E. W. Dijkstra, "A note on two problems in connection with graphs," *Numerishe Matematik*, vol. 1, pp. 269–271, Dec. 1959.
[33] R. Bellman, "On a routing problem," *Quart. Appl. Math.*, vol. 16, pp. 87–90, 1958.
[34] L. R. D. Ford and R. Fulkerson, "Maximal flow through a network," *Can. J. Math.*, vol. 8, pp. 399–404, 1956.
[35] D. B. Johnson, "Efficient algorithms for shortest paths in sparse networks," *J. ACM*, vol. 24, pp. 1–13, 1977.
[36] Power Systems Test Case Archive Univ. Washington, Seattle, WA, USA [Online]. Available: http://www.ee.washington.edu/research/pstca/
[37] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "MATPOWER: Steady-State operations, planning and analysis tools for power systems research and education," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 12–19, Feb. 2011.
[38] P. McLaren, R. Kuffel, and R. Wierckx, "A real time digital simulator for testing relays," *IEEE Trans. Power Syst.*, vol. 7, pp. 207–213, 1992.
[39] A. Orebaugh, G. Ramirez, and J. Beale, *Wireshark & Ethereal Network Protocol Analyzer Toolkit*. Rockland, MA, USA: Syngress, Feb. 2007.
[40] D. Libes, "Expect: Scripts for controlling interactive processes," in *Computing Systems*. Berkeley, CA: Univ. California Press, 1991, vol. 4.
[41] M. Lutz, *Learning Python*, 4th ed. Sebastopol, CA, USA: O'Reilly Media, 2009.

Anurag K. Srivastava (M'00–SM' 09) received the Ph.D. degree from Illinois Institute of Technology (IIT), Chicago, in 2005.

He joined Washington State University, Pullman, as Assistant Professor in August 2010. He worked as an Assistant Research Professor at Mississippi State University from 2005–2010. His research interests include power system operation, control, security, and stability within smart grid and micro grid.

Dr. Srivastava is a Member of the IEEE Power and Energy Society (PES), IET, Sigma Xi, and Eta Kappa Nu. He is chair of the IEEE PES career promotion subcommittee and vice-chair of the IEEE PES student activities subcommittee and is active in several other IEEE PES technical committees.

Thomas Morris (M'00–SM' 08) received the Ph.D. degree from Southern Methodist University, Dallas, TX, in 2008.

He joined Mississippi State University (MSU), Mississippi State, as Assistant Professor in August 2008. His research interests include industrial control system penetration testing and intrusion detection systems.

Timothy A. Ernster (S'08) received the B.S. degree from Gonzaga University, Spokane, WA, in 2006, and is currently pursuing graduate studies at Washington State University, Pullman.

Since 2006 he has worked as an Electrical Engineer for the U.S. Army Corps of Engineers, with notable awards for service in support of the U.S. reconstruction mission in Baghdad, Iraq, during Operation Iraqi Freedom. His interests include power system operation and security.

Ceeman B. Vellaithurai (S'12) received the B.E. degree from Anna University Tiruchirappalli, India, in 2011 and is currently pursuing graduate studies at Washington State University, Pullman.

His research interests include real time modeling and simulation of power system.

Shengyi Pan (S'12) received the B.Eng. degree from Fuzhou Univeritys, China, in 2008 and the M.S. degree from University of Sheffield, U.K., in 2009. He is currently working toward the Ph.D. degree in Mississippi State University, Mississippi State. His research interests include security and intrusion detection for computer network, process control system, and smart grid.

Uttam Adhikari (S'11) received the B.S. degree in electrical engineering from Tribhuvan University, Nepal, in 2005, and is currently pursuing graduate studies at Mississippi State University, Mississippi State.

His research interests include wide area monitoring, control, and cyber security in smart grid.

Modeling Cyber-Physical Vulnerability of the Smart Grid With Incomplete Information

Anurag Srivastava, *Senior Member, IEEE*, Thomas Morris, *Senior Member, IEEE*, Timothy Ernster, *Student Member, IEEE*, Ceeman Vellaithurai, *Student Member, IEEE*, Shengyi Pan, *Student Member, IEEE*, and Uttam Adhikari, *Student Member, IEEE*

***Abstract*—This paper addresses the attack modeling using vulnerability of information, communication and electric grid network. Vulnerability of electric grid with incomplete information has been analyzed using graph theory based approach. Vulnerability of information and communication (cyber) network has been modeled utilizing concepts of discovery, access, feasibility, communication speed and detection threat. Common attack vector based on vulnerability of cyber and physical system have been utilized to operate breakers associated with generating resources to model aurora-like event. Real time simulations for modified IEEE 14 bus test case system and graph theory analysis for IEEE 118 bus system have been presented. Test case results show the possible impact on smart grid caused by integrated cyber-physical attack.**

***Index Terms*—Aurora attack, cyber-physical vulnerability, graph theory, information and communication technology for smart grid, RTDS.**

I. Introduction

THE SMART electric grid utilizes enhanced information and communication technology (ICT) coupled with advanced control algorithms to improve efficiency and reliability of system [1], [2]. Enhanced usage of ICT provides a number of advantages, but at the same time generates more cyber intrusion access points [3]. The synergy between heterogeneous physical and cyber components in a smart grid allows easy translation between cyber intrusions to a possible loss/damage of physical electric grid components [3]. Cyber intrusions may divulge confidential information, enable denial of service attacks leading to a loss of visibility and control of the system. Command and measurement injection attacks will lead to harming a system or incorrect control actions.

As part of the smart grid, intelligent electronic devices (IEDs) with embedded communication, intelligence, and information technologies enable local and/or remote sensing and control of substation equipments. IEDs also helps in control and protection mechanism of the electric power grid (EPG). If compromised, IEDs can maliciously remove generators or lines from the EPG.

Generally, EPGs are designed to handle a single contingency (the "N-1" case) without violating system security constraints and still meeting reliability criteria [4]. EPG security analysis ranks most critical physical components at given operating condition for planning and possible preventive control actions. Security analysis requires knowledge of complete EPG network topological characteristics and operations conditions [5]. Commonly studied "N-1" contingencies are the loss of a single line or generator. However, a coordinated cyber-attack can cause multiple generator or line contingencies simultaneously, resulting in a "N-X" contingency. Under such circumstances, power flows, voltages, and system frequency may vary outside tolerable constraints resulting in the conditions necessary for cascading failures leading to a system blackout [6].

It is necessary to understand and model such a possible "planned coordinated cyber-physical attack," so appropriate mitigation strategies can be determined [7]. Many approaches exist to provide vulnerability discovery, risk analysis, and recommended security practices for electric power systems. In [8], authors provide a cyber-security vulnerability analysis and solutions for various measurement and control systems found in EPG. The paper recommends evaluation of risk on the dependency of a system on the cyber infrastructure and discusses the importance of cyber infrastructure security in terms of its impacts on power grid applications. Liu *et al.* [9] describe a vulnerability analysis frame work for coordinated switching attacks against breakers in a power system. The authors in [10] discuss development of a cyber-to-physical bridge to provide an estimation of electric supply events caused by cyber-attacks. The paper further describes a methodology, Reliability Impacts from Cyber Attack (RICA), for measuring the impact of cyber-attacks on power system reliability. For finding physical vulnerabilities, bulk of existing literature are based on assuming complete knowledge of the system operating state, or information needed to carry out an ac or dc power flow [11], [12]. However, in most cases it would not be appropriate to assume a cyber-attacker is in possession of complete power system state information. Therefore, cyber-physical vulnerability assessments of a power system based on incomplete information [13] needs to be studied. In [7], coordinated planned attack with limited information was addressed with focus on exploring the application of graph theory and validating degree, eigenvector, closeness, vertex betweeness, and edge betweeness centrality measures against conventional dc power flow based linear sensitivity factor. In

Manuscript received April 01, 2012; revised September 08, 2012; accepted October 02, 2012. This work was supported in part by the Department of Energy (DoE) Award Number DE-OE0000097 (Trustworthy Cyber Infrastructure for the Power Grid). Paper no. TSG-00178-2012.

A. Srivastava, T. Ernster, and C. Vellaithurai are with the School of Electrical Engineering and Computer Science, Washington State University, Pullman, WA 99164 USA (e-mail: asrivast@eecs.wsu.edu).

T. Morris, S. Pan, and U. Adhikari are with the Department of Electrical and Computer Engineering, Mississippi State University, Mississippi State, MS 39762 USA (e-mail: morris@ece.msstate.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/TSG.2012.2232318

[7], it was determined that the closeness centrality measure tends to correlate well with the power system to a loss in bus injection contingency for the N-1 case.

The focus of this paper is addressing ICT and EPG vulnerabilities with incomplete information and to model an aurora-like event to cause maximum adverse impact to the smart grid. In this paper, aurora refers to a cyber event in which rapid opening and closing of a breaker near a generator causes excessive torque and may lead to physical harm to the generator [14]. The original research contribution of this paper is integration of cyber and physical vulnerability models given incomplete information. Specific contributions are a new cyber vulnerability ranking, a novel graph based N-X generator contingency ranking, an integrated cyber physical vulnerability index, and real time modeling of a coordinated aurora like event to demonstrate a cyber-physical attack. Closeness centrality measure for N-1 generator outage in [7] was further extended to the N-X case in this paper and combined with the new cyber vulnerability index for assessment of integrated cyber-physical vulnerability.

II. Vulnerability of ICT in Smart Grid

Communication networks are an integral part of monitoring and control infrastructure within the smart grid. These communication networks may be penetrated by external or internal attackers to perform 4 classes of attacks; reconnaissance, denial of service (DOS), command injection, and sensor measurement injection [14]. The relays and other intelligent electronic devices (IED) found in a smart grid may be connected to control room computers via dial-up modems, RS-232 [16], or Ethernet with TCP and UDP ports and services.

Communication systems in the smart grid may be penetrated at multiple locations. Control room and substation computers, IED, and communication equipment are typically isolated in an electronic security perimeter (ESP) [17]. The control room ESP connects to substation ESP via fiber optic, microwave, satellite, frame relay, or dial-up modem systems. The interconnections between ESP are considered untrusted and therefore ESP includes firewall to limit communication connections into and out of the ESP. The inter-ESP link may be wireless or may use leased bandwidth from a third party and is therefore at risk of penetration. ESP may also often have connections to corporate enterprise networks and external connections to other utilities or regional control centers via servers placed in demilitarized zones. Servers in demilitarized zones may use one-time password systems to limit access, may use certificates to authenticate attaching computers or users, or may require username and password entry. Penetration may occur through these external connections. The cyber devices in an ESP may be compromised by accidental introduction of malware via Universal Serial Bus (USB) thumb drive attack, virus penetration, or infected software patches. A compromised system within an ESP may establish communication via an ESP's existing network connections to outside attackers. Finally, devices within an ESP may be compromised intentionally by an individual with authorized physical access.

The Stuxnet [18] worm penetrated industrial control systems by first compromising control room computers by exploiting both USB thumb drive and printer server vulnerabilities. A commercial one-time password system vendor recently divulged key material for a commercially available one time password system after a spear phishing attack [19]. Spear phishing attacks may also be directed at utility employees with remote access to control system ESP. Wireless networks in industrial control systems may also be penetration points [20], [21]. Computers in ESP may also be compromised by malware introduced from infected patches or from viruses. Dial-up connections into ESP can be found via war dialing attacks [22]. Port scan attacks may be used to find IED connected to a penetrated Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) network [23].

After penetration, an attacker may perform reconnaissance, denial of service (DOS), command injection, or measurement injection attacks [17]. Reconnaissance attacks are used by a "penetrating attacker" to identify systems for attack before penetration and to learn system model and version details to enable future attacks after penetration. Denial of service attacks attempt to break communication links to stop command and sensor measurement traffic from reaching intended destinations. Command injection attacks send falsified commands to devices. Measurement injection attacks falsify or alter sensor measurements to indirectly cause a human or automated controller to take an incorrect control action.

Utilities perform vulnerability analysis on devices declared as cyber critical assets (CCA) [15]. Discovered vulnerabilities are ranked by severity. Vulnerability ranking systems attempt to measure likelihood of exploitation, complexity of an exploit, potential cost of exploitation, and the availability and cost of defenses against such exploits. The common vulnerability scoring system (CVSS) [24] is commonly used to estimate the risk associated with enterprise and information system cyber security vulnerabilities. Separate vulnerability assessment methodologies have been proposed for critical infrastructure [25].

A. Aurora Attack

A successful aurora attack would first require communication network penetration. This may happen by penetrating a communication link from control room to a generation or transmission relay/IED. After penetration the attacker would inject falsified commands to trip and reclose a relay in a rapid repetitive manner.

All relays have an intentional delay in operation to prevent control action during transients in the power system. These transients may be due to a sudden switching of a load on/off the grid. Relays are expected to protect the system by isolating faulty parts, while also preventing unnecessary tripping of power components due to short period transients. These delays result in a small window where no protection device actuates. This window is typically less than fifteen cycles to launch an aurora attack [14]. The objective of an aurora attack is to intentionally take a generator off the grid and connect it to the grid out of synchronism. This is facilitated by the opening and closing of a circuit breaker or combination of circuit breakers. For preventing out of synchronism connection of a generator to the grid, synchronism check relays are used. In the case of an aurora attack, it is assumed that the function of a synchronism

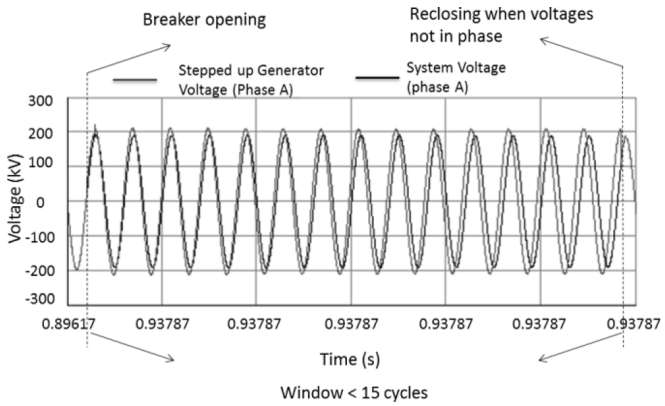

Fig. 1. Breaker opening and out of synchronism reclosing.

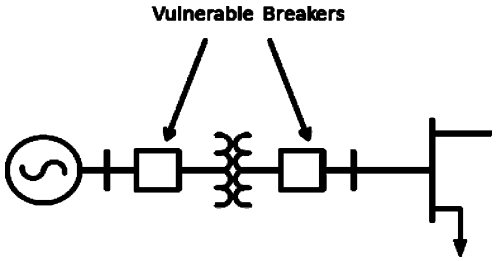

Fig. 2. Aurora attack with local beaker opening.

check element is compromised by hacking the relay. It may also be absent in the case of attack due to operation of remote breaker away from the generator. The breaker opening and out of synchronism reclosing can be seen in Fig. 1.

When the circuit breaker is opened, the generator is isolated from the grid. The mechanical power input to the generator changes slowly due to the governor action being slow. Due to the continued mechanical power input, the generator starts to speed up and the frequency of the generator starts to increase. This leads to frequency difference between the grid and the generator. The angle of separation starts to increase with time. The window for attack is only 15 cycles and hence the circuit breaker is closed before this time window expires [26]. The generator is now pulled into synchronism with "out-of-sync" conditions and this causes large electrical and mechanical transients. These transients may lead to permanent damage to the generators, if opening and closing operation is repeated as demonstrated by the experiment at the Idaho National Laboratory [26]. The aurora attack can be a simple manual physical opening and reclosing of a circuit breaker in a substation or a sophisticated attack, which involves hacking into the communication channel of a substation to alter the settings relays to cause operation of the circuit breakers. There could be two types of possible aurora attack:

1) Scenario 1:-Local Attack: As shown in Fig. 2, a local aurora attack generally involves the operation of the breakers close to the generator within a generation level substation.

2) Scenario 2:-Remote Breaker Attack: Depending on the topology of the system, the attack can be successful by attack on breakers, which would still cause isolation of the generator from the grid like tie line breakers as shown in Fig. 3.

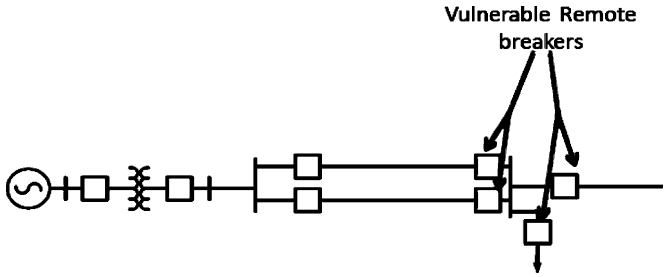

Fig. 3. Aurora attack with remote beaker opening.

B. A New Approach for Cyber Vulnerability Ranking

An attacker who penetrates a utility communication network may find many relays to operate breakers leading to aurora attack. Attacker may develop a scoring system to decide which relay is the most vulnerable for aurora attack. A sample scoring methodology is presented here with potential vulnerability ranking criteria: discovery, finger printing, access, detection threat and, connection speed.

Relay *discovery* includes penetration of the local area network connected to a relay and identification of a relay on the network. For an Ethernet network this requires penetration of the electronic security perimeter. For dialup connection this discovery requires successfully finding a dial up phone number into a substation and then successfully penetrating the secure dial up gateway by providing a valid authentication code. Once connected to the substation local area network (LAN), Ethernet connected relays may be discovered using port scanning tools such as the network mapping program NMAP [27]. Relays connected to a dial-up gateway by serial connection may be discovered by Modicon-Bus (MODBUS) address scanning. Discovery (d_i) is scored with a binary value $(0 = \text{no discovered}, 1 = \text{discovered})$. Access is the ability to access and control the relay. Accessibility (a_i) is scored with a binary value $(0 = \text{not accessible}, 1 = \text{accessible})$. Discovered relays may be finger printed to identify the relay brand and model. Attackers often access vulnerability lists to learn potential weaknesses of a device. The feasibility of an attack against a relay depends upon knowledge of a vulnerability which allows the attacker to assume control of the relay. Feasibility (f_i) is scored with a binary value $(0 = \text{not feasible}, 1 = \text{feasible})$.

Access exceeds connectivity and feasibility in that the relay is discovered, vulnerability is known, and an exploit is available to allow the attacker to assume control of the relay. Detection threat is the risk that an attack will be discovered before successfully damaging the generator. Detection threat is less with a RS-232 or dialup connection since intrusion detection systems for these systems are uncommon [15]. Detection threat increases as network penetration time increases. Therefore, if an attack requires long-term penetration to learn passwords, the detection threat will be higher than a short penetration time. Detection threat is scored with a three values $(0 = \text{no threat}, 1 = \text{low threat}, 2 = \text{high threat})$. Communication connection speed impacts potential aurora attack success. Slower connection speed may limit how fast the trip and reclose commands can be sent. Connection speed is scored with 3 values $(0 = s_i <= 1200, 1 = 2400 > s_i > 19200, 2 = s_i >$

TABLE I
POSSIBLE VULNERABILITY INDEX VALUES

d_i	f_i	a_i	s_i	t_i	v_i	*Description*
1	1	1	2	0	5	High s_i, low t_i, maximum v_i
1	1	1	2	1	4	High s_i, medium t_i, medium-high v_i
1	1	1	1	0	4	Medium s_i, low t_i, medium-high v_i
1	1	1	2	2	3	High s_i, high t_i, medium v_i
1	1	1	0	0	3	Low s_i, low t_i, medium v_i
1	1	1	1	1	3	Medium s_i, medium t_i, medium v_i
1	1	1	1	2	2	Low s_i, medium t_i, medium-low v_i
1	1	1	0	1	2	Low s_i, medium t_i, medium-low v_i
1	1	1	0	2	1	Low s_i, high t_i, low v_i
0	-	-	-	-	0	Not discovered, 0 v_i
-	0	-	-	-	0	Not feasible, 0 v_i
-	-	0	-	-	0	Not accessible, 0 v_i

$19200\ \mathrm{baud}$). Connection speed is not related to network penetration time. An attacker may connect to the network to monitor traffic to perform reconnaissance necessary to execute a successful aurora attack. This reconnaissance period is the network penetration time and as the length of the reconnaissance period increases more artifacts of the penetration are created and therefore detection threat increases. Connection speed refers only to the communication link bandwidth.

$$v_i = d_i{}^* f_i{}^* a_i{}^* (s_i - t_i + 3). \tag{1}$$

Equation (1) gives the vulnerability index (v_i). The vulnerability index has possible values of $\{0 \cdots 5\}$. The minimum vulnerability index value, 0, indicates minimum risk and the maximum value, 5, indicates maximum risk.

Table I shows the possible values for the vulnerability index (v_i). Subtracting detection threat (t_i) from connection speed (s_i) in the vulnerability index product allows detection threat to counter connection speed such that a high-speed connection with high detection threat has a low score while a high-speed connection with low detection threat has the highest possible score. As the connection speed increases the vulnerability increases. As the detection threat increases the vulnerability index decreases. The lowest possible score of 0 is reserved for the cases where the relay is not discovered $(d_i = 0)$, is not accessible $(a_i = 0)$, or an attack is infeasible $(f_{i=0})$. Nonzero values are required for all these parameters for a successful attack. The " $+3$" term in (1) ensures that if a relay is discoverable, accessible, and an attack is feasible the vulnerability index will be non-zero indicating there is always some risk in this situation.

The above developed vulnerability index will be used to rank the cyber vulnerability to attack a relay to cause opening and closing a breaker.

III. VULNERABILITY OF PHYSICAL SMART GRID

To cause a maximum adverse generator outage impact on EPG, it is necessary to find the most critical set of generators. An attacker would mass their resources in damaging these critical set of generators to remove from service. Security analysis contingency ranking schemes identify critical generators or lines based on the severity of impact on the system. Existing research concerning contingency ranking typically relies on knowing the operational state of the power system, such as the voltage magnitude and MW injection at each PV buses, the MW and MVAr injection at all PQ buses, and the topology parameters of branches connecting the system buses. However, bus voltage and power injection are dynamic variables. Yet the system topology tends to remain considerably more static.

It must therefore be considered unlikely that an outside attacker will know the precise operational state of a power system (line MVA flows, bus voltages, generation dispatch, load demand) at the time of an intended coordinated attack. Accordingly, conventional contingency screening algorithms would be difficult to be utilized by attackers in assessing the physical vulnerability of a power system. A more simple power system vulnerability analysis method will need to be employed that selects critical targets for a coordinated cyber-attack based on topology data. Topology based physical vulnerability assessments could be easily performed by attackers with non-confidential publicly available information.

Existing use of topology based electrical distance characteristics in contingency analysis is limited to the concept of concentric relaxation, which establishes a geographical boundary for the impact of a given contingency based on the assumption that the effects of a contingency are principally local [28]. While the use of concentric relaxation assumptions is conventionally utilized to speed up contingency analysis by fixing bus voltages and phase angles outside a certain boundary layer, the concept forms a basis for utilizing topology based studies of a power system for limited information attack scenario planning.

The use of graph theory in performing a limited information topology based contingency analysis is rooted in the power flow equations given by (2) and (3):

$$P_i = \sum\nolimits_{j=1}^{n} V_i V_j Y_{ij} \cos(\delta_i - \delta_j - \theta_{ij}) \tag{2}$$

$$Q_i = \sum\nolimits_{j=1}^{n} V_i V_j Y_{ij} \sin(\delta_i - \delta_j - \theta_{ij}) \tag{3}$$

where P_i and Q_i are the active and reactive power injection at bus i, $V_i \delta_i$ is the voltage and phase angle at bus i (or bus j depending on the subscript), and Y_{ij} is the element of the bus admittance matrix defining the admittance between buses i and j[5]. Conventional forms of contingency analysis utilize forms of the power flow equations to assess the impact of loss of a generator or line on the branch flows and bus voltages. In the case of a generator outage, the lost MW injection must be made up by other remaining generators in the power system. Such a redispatch in generation will change the steady state bus voltage and line flow values from the pre-outage state.

Even if an external attacker is not likely to know the voltage and power injection at each bus, the bus admittance matrix terms can be readily estimated based on line and transformer physical characteristics available from public information and intelligent guesses. Knowing that topology plays a role in the calculation of the post-contingency state of a power system after a generator outage, the severity of changes in MW and MVAr injections and voltages must be assessed based on the topology of a given electric grid. Naturally, this cannot be assessed by conventional mathematical derivation. However, by performing statistical tests comparing graph theory based vertex ranking schemes and conventional dc power flow based generation shift factor measures, results can be presented in support of certain graph

theory based ranking techniques in predicting the sensitivity of a power system to loss in generation at specific buses.

A. A Novel Approach of N-X Generator Contingency Ranking With Incomplete Information Using Graph Theory

For purposes of topology analysis, a power system will be modeled as a graph G, where the buses in a power system are treated as a set of vertices V and the branch components as the set of edges E. As it would be improper to treat all transmission lines and transformers in a power system as equal, the edges in a graph model of a power system must be assigned weights to reflect the inherent dissimilarity between branch components. While branch impedances Z consist of both a resistive component R and reactive component X, edge weights are assigned based on the magnitude of X since generally $X \gg R$ for most branches in a power system [29].

Given such a graph model of a power system, the question remains concerning how to use such a model to identify the most critical components in the system. For purposes of determining which generator to target for a cyber-attack, we will utilize concepts of vertex centrality. Vertex centrality measures assign ranking coefficients to vertices in a graph, from which we can deduce that the most important generators are those located on a bus with a highly ranked vertex centrality. While there are numerous vertex centrality measures, evidence is strongest in support of the relationship between closeness centrality in relation to more conventional methods of assessing the impact of generator outages [7]. Formally, closeness centrality for a n bus power system is defined as:

$$C_C(v_i) = \frac{\sum_{j \in V \setminus i} d(i,j)}{n-1}. \tag{4}$$

Here, determination of closeness centrality relies upon the shortest path matrix D_G with entries $d_G(i,j)$ that indicate the shortest path from a bus i to another bus j. Determination of D_G relies on a shortest path algorithm, such as the Floyd-Warshall [30], [31], Dijkstra [32], Bellman-Ford [33], [34], or Johnson's algorithm [35]. One of the issues associated with validating closeness centrality is that, as a topological based vulnerability assessment algorithm, it is subject to inaccuracies under certain actual operating conditions of the power system. When selecting targets based on topology vulnerability, a rough estimation of power generation at a specific bus would be required to ensure attack resources are not wasted removing a small generator from service. The closeness centrality algorithm can be validated against the dc power flow based generation shift factor (GSF). The GSF is defined as:

$$a_{li} = \frac{\Delta f_l}{\Delta P_i}. \tag{5}$$

where Δf_l is the change in MW power flow on line l when a change in MW generation ΔP_i occurs at bus i. The dc power flow based assumptions of neglecting MVAR flows and bus voltage magnitudes only introduces errors in calculated line flows of approximately 5% [5]. In order to assess the overall impact of all line redistributions attributed to a given generator outage, the GSF is utilized to generate a generator shift impact factor (GSIF) a_i defined as:

$$a_i = \sum\nolimits_l |a_{li}|. \tag{6}$$

For all non-swing buses i reflecting the sum of the magnitude of the factors a_{li} attributable to bus i, or the L_1 norm of each column of a_{li}. In one of the previous publication, authors of this paper have shown that there exists a negative correlation between closeness centrality and the GSIF, which together with nonparametric statistical ranking tests provides evidence in support of the closeness centrality measure as a means to reflect the severity of a given generator outage contingency based on limited information [7].

In this paper, we extended the closeness centrality concept to the general case involving N-X generator outages. A subset of vertices $V_{gen} \subseteq V(G)$ are defined as the non-swing generator buses of the power system being modeled as a graph G. For some N-X contingency, $k \in \mathbb{R}^X$, we define the set of X verticies reflecting the buses locations of each generator outage as $V_{cont} = \{v_k\} \subseteq V_{gen}$. A new closeness centrality impact measure CI_c can then be introduced reflecting a collective topology assessment of multiple generator outages, defined as:

$$CI_C(k) = \sum\nolimits_{i \in V_{cont}} |C_C(v_i)|. \tag{7}$$

IV. Test Case Studies

To test the developed algorithms for cyber and physical vulnerability, two standard test systems have been used here: IEEE 14 bus system and IEEE 118 bus system [36].

A. IEEE Test Cases

The IEEE 14 bus system is shown in Fig. 4. The IEEE 14 bus system was modified for simulation purposes. The following changes were made as shown in Table II:

i. All synchronous condensers were changed to generators.
ii. Circuit breakers were included after each generator before being connected to the grid.
iii. Generation values at each bus were modified to the values shown in Table I.

The IEEE 118 bus system consists of 186 branches, 64 PQ buses, and 54 voltage controlled buses (19 are MW producing generators and 35 are condensers producing MVARs).

B. Simulation Tools

MATLAB: Since conventional power systems analysis software packages do not include graph theory analysis tools, code was written in MATLAB to implement the graph theory vulnerability analysis algorithms. Using the MATPOWER package of M-files, the generation shift factors were calculated. Additionally, MATLAB code was written to compare the graph theory results with the MATPOWER generated GSF factors [37].

RTDS: The Real Time Digital Simulator (RTDS) [38] is an example of virtual power system simulator designed for continuous real time operation. Models of the simulated power system are defined using a graphical modeling language,

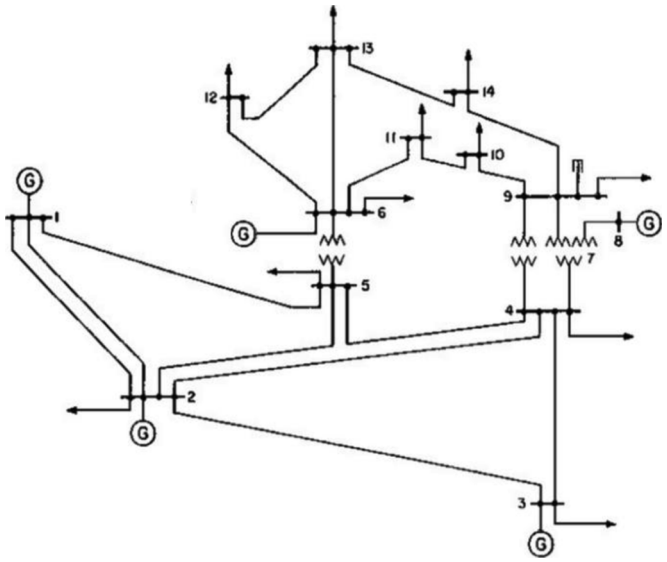

Fig. 4. Modified IEEE 14 bus system.

TABLE II
GENERATION DATA FOR MODIFIED IEEE 14 BUS SYSTEM

Bus Number	MW	Mvar	MVA
1 (G1)	106.6	4.147	150
2 (G2)	37.4	17.37	60
3 (G3)	41.6	2.627	60
6 (G4)	41.6	-3.283	60
8 (G5)	41.6	16.68	60

RSCAD. RTDS can be connected to external devices that allow closed loop testing of real-world physical equipment, like relay [38].

Wireshark: is an Ethernet data logger used to capture, store, and display network packets. Packets are time-stamped and each network layer is shown individually. Wireshark was used to capture and study relay trip and reclose packets [39].

Ettercap: is a man-in-the-middle (MITM) framework which allows attackers to design and execute MITM attacks against network switches [40].

Expect: is a script language used to automate and replicate queries and responses manual command line interfaces. Expect was used to automate sending relay command passwords and trip and reclose commands [40].

Python: is a script language with high levels of abstraction. Python libraries were used to send MODBUS packets containing open and reclose commands [41].

C. Simulation Results

1) Generator Contingency Ranking: Using developed algorithm for generator contingency, set of generators for both the cases were ranked for "N-1," "N-2," and "N-3" contingency for the IEEE 14 and 118 bus system as shown in Tables III–VI. Note that developed algorithm can be easily extended for higher contingencies. From a cyber attacker's perspective, they may not know the exact dispatch of each generator, voltage set points, or the demand at each load. However, we assume that the attacker can determine the topology and branch impedances from publically available maps showing the location and voltage base

TABLE III
N-1 AND N-2 GENERATOR OUTAGE CONTINGENCY RANKING FOR THE MODIFIED IEEE 14 BUS SYSTEM

Rank	N-1 Contingencies			N-2 Contingencies		
	Gen	Bus	C_C	Gens	Buses	CI_C
1	G5	8	1.7857	G3,G5	3,8	3.8205
2	G3	3	2.0348	G2,G5	2,8	4.0261
3	G2	2	2.2404	G4,G5	6,8	4.2454
4	G4	6	2.4597	G2,G3	2,3	4.2752
5	N/A	N/A	N/A	G3,G4	3,6	4.4945
6	N/A	N/A	N/A	G2,G4	2,6	4.7001

TABLE IV
N-3 GENERATOR OUTAGE CONTINGENCY RANKING FOR THE IEEE 14 BUS SYSTEM

Rank	N-3 Contingencies		
	Gen	Bus	CI_C
1	G2,G3,G5	2,3,8	6.0609
2	G3,G4,G5	3,6,8	6.2802
3	G2,G3,G4	2,3,6	6.7349

TABLE V
TOP FIVE N-1 AND N-2 GENERATOR OUTAGE CONTINGENCY RANKING FOR THE IEEE 118 BUS SYSTEM

Rank	N-1 Contingencies			N-2 Contingencies		
	Gen	Bus	C_C	Gens	Buses	CI_C
1	G15	87	1.0875	G15,G19	87,111	2.3415
2	G19	111	1.2540	G15,G16	87,89	2.4728
3	G16	89	1.3853	G16,G19	89,111	2.6393
4	G6	46	1.6680	G6,G15	46,87	2.7555
5	G8	54	1.7041	G8,G15	54,87	2.7916

TABLE VI
TOP FIVE N-3 GENERATOR OUTAGE CONTINGENCY RANKING FOR THE IEEE 118 BUS SYSTEM

Rank	N-3 Contingencies		
	Gen	Bus	CI_C
1	G15,G16,G19	87,89,111	3.7268
2	G15,G16,G18	87,89,103	4.2592
3	G15,G16,G17	87,89,100	4.4130
4	G16,G17,G19	89,100,111	4.5795
5	G5,G6,G15	31,46,87	4.6696

of generators, substations, and transmission lines. For the modified IEEE 14 bus system, there are limited numbers of choice for possible generator attack with 5 generators.

Tables III and IV show the "N-1," "N-2," and "N-3" contingency ranking for modified IEEE 14 bus system. Tables V and VI show top five "N-1," "N-2," and "N-3" contingency rankings for the IEEE 118 bus system. An attacker interested in targeting a subset of the 19 generators based on the physical vulnerability of the system is modeled such that the impact of a coordinated generator attack has the greatest chance of causing a maximal adverse reliability impact. Detailed analyses for IEEE 118 bus system are not shown here due to space limitations.

2) Cyber Vulnerability Ranking: All the relays connected to generator breakers were ranked using the developed cyber vulnerability ranking. Table VII shows an example vulnerability ranking for the 5 generator relays from the modified IEEE 14 bus system. Relays 2, 3, 4 and 5 have been discovered by an attacker and therefore share discovery (d_i) scores of 1. Relay 1 is unknown to the attacker and therefore has a discovery (d_i) score of 0, eliminating it from attack consideration. The attacker has

TABLE VII
VULNERABILITY RANKING FOR THE IEEE 14 BUS SYSTEM

Relay	d_i	f_i	a_i	s_i	t_i	v_i
1	0	-	-	-	-	0
2	1	0	-	-	-	0
3	1	1	1	1	1	3
4	1	1	1	0	1	2
5	1	1	1	2	1	4

finger printed relays 3, 4, and 5 to learn the manufacturer and model number of the relays and has learned of vulnerabilities for each via internet search, hence a feasibility score (f_i) of 1 for each. Relay 2 may have been finger printed but no vulnerability is known and therefore has a feasibility (f_i) score of 0, eliminating it from attack consideration.

For this example a highly capable attacker is assumed. The highly capable attacker will be able to exploit all known vulnerabilities. Relays 3, 4, and 5 have been discovered and are feasible and accessible. Relay 3 is connected to a compromised dial-up modem gateway with baud rate of 1200 bits per second giving a speed score of 0, and a detectability threat score of 0 since the dial-up network is unlikely to include an intrusion detection system (IDS). The low connection speed limits the likelihood of an effective aurora attack; however, the low detection threat results in medium risk. Relay 5 is connected to a 10 megabit per second Ethernet network, which results in a connection speed score of two. Relay 5 is given a detectability threat score of 1 since the Ethernet network may have include an IDS, though the likelihood of IDS in a substation is low. Relay 4 connected to a compromised substation computer with TCP-to-Serial converter with a 9600 bits per second link to the relay. Relay 4 has a speed score of 1 based on the slowest portion of the link and a detection threat score of 1 since connecting to over Ethernet increases detection risk. Based upon the vulnerability ranking function from (1), relay 5 is the most likely to be the source of the aurora attack.

To execute an aurora attack, an attacker must first penetrate a communication interface connected to a generator relay. The communication interface may be dialup modem, RS-232, or a routable connection. For dialup, a war dialing program may be used to find modems which answer in prefixes and area codes which match other phones at a generation facility. RS-232 connections are non-routable. Penetrating a RS-232 connection requires either compromising a master terminal which may be reachable via routable network or compromising the interconnection between the master terminal and the remote device which may use frame-relay or a wireless interconnection. Routable networks may be penetrated at the ESP boundary or by compromising a device within the ESP connected to the same communication network as the generator relay.

Relays often are configured with logic to allow remote trip and reclose commands. The aurora attack requires repeatedly sending trip and reclose commands to the generator relay. Before initiating the aurora attack the attacker may finger print the relay to ensure settings include both trip and reclose logic. If the relay settings do not support remote trip and reclose commands the settings may be changed, if the attacker knows the relay's settings password. Typically the settings password may be learned by eavesdropping on communications between control room and the relay. The settings password is typically transmitted as plaintext and is easy to learn.

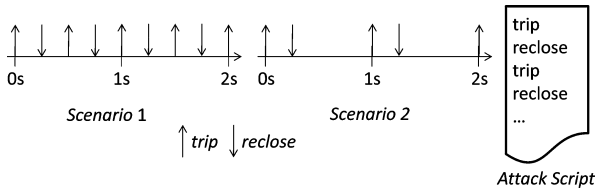

Fig. 5. Attack scenarios.

After ensuring the relay settings support remote trip and reclose commands a command injection attack is required to rapidly send the relay trip and reclose commands. Relays typically require command password entry before allowing remote command execution. The attacker can learn the relay password by eavesdropping on communications between control room and the relay, if it exists.

Two relays based on vulnerability ranking were attacked in experiments for this study. Relay 3 included a telnet service to allow remote control. Relay 5 included a MODBUS service to allow remote control. In both cases command password are used to authorize commands. In both cases, entry of the command password initiates an escalated privilege session in which the command password is entered once and then any amount of commands may subsequently entered until the escalated privilege session times out.

For Relay 3, an Expect script [39] was used to automate sending trip and reclose commands via command line interface relay using a Telnet session. Fig. 5 diagrams the two attack scenarios. Two scenarios were implemented and testing was done in laboratory experiments. In the first scenario, the trip and reclose commands are separated by 0.25 seconds and then repeated. In the second scenario, the trip command is sent then the reclose command is sent 0.25 seconds later, then the attack script waits 0.75 seconds and repeats.

For Relay 5, MODBUS packets were sent to trip and reclose the breaker. The exact function code and register contents required to trip and reclose the relay were learned via eaves dropping. Wireshark [38] was used to capture MODBUS traffic during a remote trip and reclose scenario. The individual MODBUS packets were then manually extracted from the Wireshark data and used with a Python [40] script to send the trip and reclose packets with the same timings described for scenario 1 and 2 for Relay 3.

3) Integrating Cyber Vulnerability With Physical Vulnerability Ranking: Developed cyber vulnerability can be combined with physical vulnerability in number of different ways. In this work, the simple formula for integrated cyber physical vulnerability ranking (CP) used is:

$$CP = CI_c * \sum_{i=1}^{N} \frac{(6 - v_i)}{N} \quad \text{if } v_i \neq 0$$
$$CP = \frac{N}{A} \quad \text{if } v_i = 0;.$$

Here N is the number of relays/generators in the system. Note that for single generator C_c will be used instead of CI_c. A lower cyber physical vulnerability infers a more vulnerable system.

TABLE VIII
CYBER PHYSICAL VULNERABILITY RANKING FOR N-1 AND N-2 CONTINGENCIES IN IEEE 14 BUS SYSTEM

Rank	N-1 Contingencies			N-2 Contingencies		
	Gen	Bus	CP	Gens	Buses	CP
1	G5	8	3.5714	G3,G5	3,8	9.5512
2	G3	3	6.1044	G4,G5	6,8	12.7362
3	G4	6	9.8388	G3,G4	3,6	15.7307
4	G2	2	13.4424	G2,G5	2,8	N/A
5	N/A	N/A	N/A	G2,G3	2,3	N/A
6	N/A	N/A	N/A	G2,G4	2,6	N/A

TABLE IX
CYBER PHYSICAL VULNERABILITY RANKING FOR N-3 CONTINGENCIES IN IEEE 14 BUS SYSTEM

Rank	N-3 Contingencies		
	Gen	Bus	CP
1	G3,G4,G5	3,6,8	18.8406
2	G2,G3,G5	2,3,8	N/A
3	G2,G3,G4	2,3,6	N/A

This developed integrated index will be used to attack most vulnerable generator with maximum impact on system.

The generator(s) to attack were selected based on the integrated cyber physical vulnerability ranking. Integrated cyber physical vulnerability indices are shown in Tables VIII and IX. If the CP index is N/A, it means that an aurora type cyber-attack is not possible for that combination. For example, in Table VII, it can be seen that the relay at generator 2 is not considered for attack. Hence any combination with generator 2 will not have a CP associated with it. The combination with least CP index is chosen in each contingency for RTDS simulation.

4) Real Time Simulation: The IEEE 14 bus system was modeled in RSCAD and simulated in the RTDS. Five different cases were simulated to represent N-1, N-2, and N-3 contingencies. The results obtained were found to be close to the expected values. System was modified and simulated in RTDS for aurora like event.

5) Case 1: Breaker opened for 0.25 seconds and closed for 0.25 seconds, single generator (G5) attack (scenario 1): The results obtained are shown in Fig. 6. It was observed that there is rapid variation in the electrical torque, current, speed, and power output of the machine. When the machine is connected out of phase with the grid, it experiences a synchronizing torque which tries to pull the machine back into synchronism. The machine experiences very high mechanical stress which will lead to potentially irreversible damage to the machine.

6) Case 2: Breaker opened for 0.25 seconds and closed for 0.75 seconds, single generator (G5) attack (scenario 2): Simulation results are shown in Fig. 7.

7) Case 3: Breaker opened for 0.25 seconds and closed for 0.25 seconds, two generator attack (G3 and G5) (scenario 1): In this case, the attack is coordinated to attack two generators simultaneously. G3 and G5 are selected based on the contingency ranking. This is repeated six times and then the generators are taken out of the system to simulate effect on system due to loss of the generators. It was observed that there is a voltage collapse as the power required cannot be supplied by the slack bus/other generators due to capacity limitations. This leads to a blackout. Simulation results from RTDS are shown in Fig. 8.

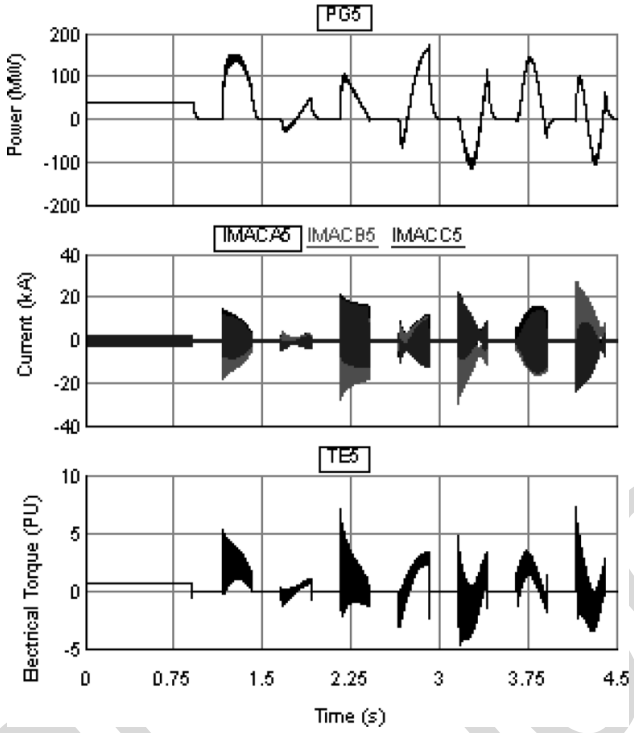

Fig. 6. Power output, current, electrical torque for Case 1 in RTDS.

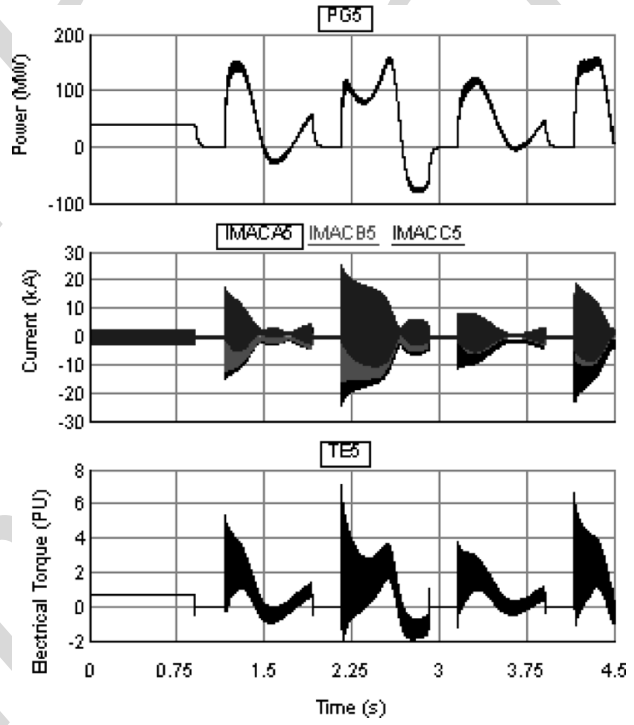

Fig. 7. Power output, current, electrical torque for Case 2 in RTDS.

8) Case 4: Breaker opened for 0.25 seconds and closed for 0.75 seconds, two generator attack (G3 and G5, scenario 2): Simulation results are shown in Fig. 9.

9) Case 5: This case shows the simulation results for an "N-3" contingency, wherein three generators are targeted by the attacker. Note that top ranked cyber-physical vulnerability will be combination of G3, G4, and G5 based on the cyber-vulnerability ranking and generator outage contingency ranking. It was

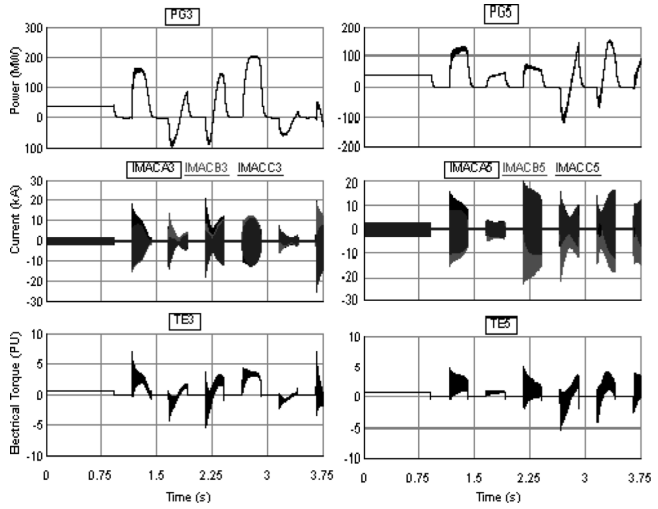

Fig. 8. Power output, current, electrical torque for Case 3 in RTDS.

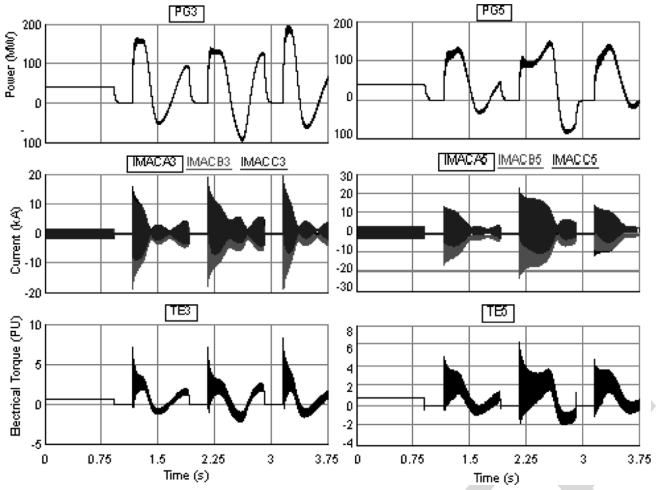

Fig. 9. Power output, current, torque for Case 4 in RTDS.

observed that N-3 contingency would lead to massive load shedding and drop in voltage as shown in Figs. 10 and 11. The basic idea of an aurora attack is to cause damage to the generators in such a way that the other protective equipment do not cause trip. However for a N-3 contingency on the IEEE 14 bus system, it is very likely that other protective equipment will also cause a trip.

These results demonstrate the impact of an aurora kind of attack on the test case considered here. Repeated transients such as the ones seen in the simulation will lead to potential damage to generators. The generators will not be available for restoration operation. This will create problem in restoration of the system after blackout/brownout caused by cyber-attack. Results presented here can be easily extended for IEEE 118 bus system similar to IEEE 14 bus analysis.

V. Conclusions

Integrated cyber physical vulnerability of smart grid with limited information has been presented in this paper. A new cyber vulnerability index based on discovery, feasibility, access, detection threat and connection speed has been developed. New graph theory based, multi contingency physical vulnerability algorithms have been also discussed. Integrated cyber physical

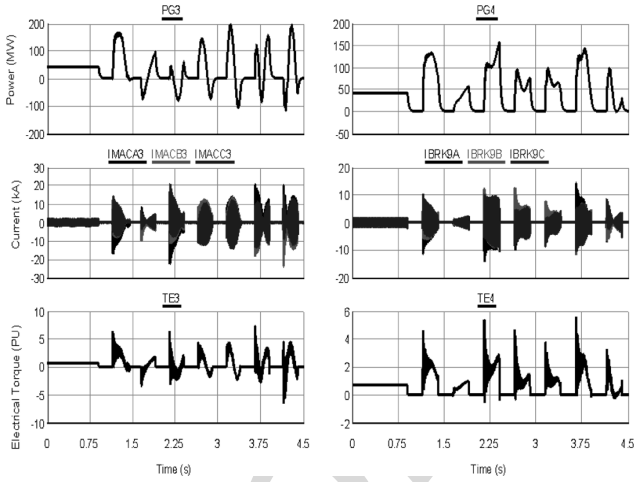

Fig. 10. Power output, current, torque for Case 5 in RTDS (G3 and G4).

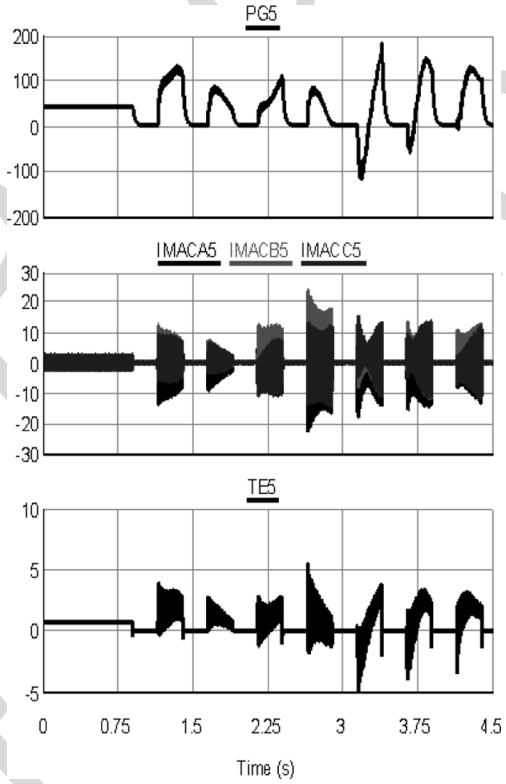

Fig. 11. Power output, current, torque for Case 5 in RTDS (G5).

vulnerability index has been developed and has been utilized for real time modeling to demonstrate impact of aurora attack. Test case results for IEEE 14 and IEEE 118 bus test case show an adverse impact on power grid. Mitigation techniques need to be developed to avoid such coordinated cyber-physical attacks on the smart grid.

References

[1] S. 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.

[2] E. Santacana, G. Rackliffe, L. Tang, and X. Feng, "Getting smart," *IEEE Power Energy Mag.*, vol. 8, no. 2, pp. 41–48, Mar.–Apr. 2010.

[3] T. Morris, A. K. Srivastava, B. Reaves, K. Pavurapu, R. Vaughn, W. McGrew, and Y. Dandass, "Engineering future cyber-physical energy systems: Challenges, research needs, and roadmap," in *Proc. North Amer. Power Symp.*, Oct. 4–6, 2009.

[4] *Reliability Standards for the Bulk Electric Systems of North America*, NERC Standard TOP-002-2, May 2009.
[5] A. J. Wood and B. F. Wollenberg, *Power Generation Operation and Control*, 2 ed. New York, NY, USA: Wiley, 1996, pp. 421–427.
[6] D. Kirschen, "Power system security," *Power Eng. J.*, vol. 16, no. 5, pp. 241–248, Oct. 2002.
[7] T. A. Ernster and A. K. Srivastava, "Power system vulnerability analysis-towards validation of centrality measures," in *Proc. IEEE T&D Conf. Expo.*, Orlando, FL, May 2012.
[8] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.
[9] S. Liu, X. Feng, D. Kundur, T. Zourntos, and K. Butler-Purry, "Switched system models for coordinated cyber-physical attack construction and simulation," in *Proc. IEEE 1st Int. Workshop Smart Grid Model. Simul. (SGMS)*, Oct. 17, 2011, pp. 49–54.
[10] J. Stamp, A. McIntyre, and B. Ricardson, "Reliability impacts from cyber attack on electric power systems," in *Proc. IEEE Power Syst. Conf. Expo.*, Mar. 15–18, 2009, pp. 1–8.
[11] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 382–390, Jun. 2011.
[12] 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.
[13] L. Fu, W. Huang, S. Xiao, Y. Li, and S. Guo, "Vulnerability assessment for power grid based on small-world topological model," in *Proc. Asia-Pacific Power Energy Eng. Conf. (APPEEC)*, Mar. 2010.
[14] M. Zeller, "Myth or reality-does the aurora vulnerability pose a risk to my generator," in *Proc. 37th Annu. Western Protective Relay Conf.*, Spokane, WA, Oct. 2010.
[15] T. Morris, R. Vaughn, and Y. Dandass, "A retrofit network intrusion detection system for MODBUS RTU and ASCII industrial control systems," in *Proc. 45th IEEE Hawaii Int. Conf. Syst. Sci. (HICSS-45)*, Grand Wailea, Maui, Jan. 4–7, 2012.
[16] M. Seyer, *RS-232 Made Easy: Connecting Computers, Printers, Terminals, and Modems*. Upper Saddle River, NJ, USA: Prentice-Hall, 1984.
[17] "Critical infrastructure protection (CIP)," NERC, North American Electric Reliability Corporation [Online]. Available: http://www.nerc.com/page.php?cid=2|20
[18] N. Falliere, L. Murchu, and E. Chien, "BW32.Stuxnet Dossier," Symantec, Tech. Rep., 2010.
[19] B. Parmar, "Protecting against spear-phishing," *Computer Fraud Security*, vol. 2012, no. 1, pp. 8–11, Jan. 2012.
[20] B. Reaves and T. Morris, "Discovery, infiltration, and denial of service in a process control system wireless network," in *Proc. IEEE eCrime Researchers Summit*, Tacoma, WA, Oct. 20–21, 2009.
[21] J. Slay and M. Miller, "Lessons learned from the Maroochy water breach," in *Critical Infrastructure Protection*, ser. IFIP International Federation for Information Processing, E. Goetz and S. Shenoi, Eds. Boston, MA: Springer, 2008, vol. 253, pp. 73–82.
[22] H. Berghel, "Wireless infidelity I: War driving," *Commun. ACM*, vol. 47, no. 9, pp. 21–26, Sep. 2004.
[23] P. Oman, E. Schweitzer, and J. Roberts, *Safeguarding IEDS, Substations, and SCADA Systems Against Electronic Intrusions*. Pullman, WA: Schweitzer Engineering Labs..
[24] P. Mell, K. Scarfone, and S. Romanosky, "Common vulnerability scoring system," *IEEE Security Privacy*, vol. 4, no. 6, pp. 85–89, Dec. 2006.
[25] S. Wang, L. Hong, and X. Chen, "Vulnerability analysis of interdependent infrastructure systems: A methodological framework," *Physica A: Stat. Mech. Its Appl.*, vol. 391, no. 11, pp. 3323–3335, Jun. 2012.
[26] J. Meserve, "Staged cyber-attack reveals vulnerability in power grid," in CNN 2007 [Online]. Available: www.cnn.com/2007/US/09/26/power.at.risk/
[27] G. Lyon, *NMAP Network Scanning Official NMAP Project Guide to Network Discovery and Security Scanning*. Sunnyvale, CA: Insecure Press, 2008.
[28] J. Zaborszky, W. Keh-Wen, and K. Prasad, "Fast contingency evaluation using concentric relaxation," *IEEE Trans. Power App. Syst.*, vol. PAS-99, no. 1, pp. 28–36, Jan. 1980.
[29] Z. Wang, A. Scaglione, and R. J. Thomas, "Electrical centrality measures for electric power grid vulnerability analysis," in *Proc. 29th IEEE Conf. Decision Control*, Dec. 2010, vol. 15, pp. 5792–5797.
[30] R. W. Floyd, "Algorithm 97: Shortest path," *Commun. ACM*, vol. 5, pp. 345–345, Jun. 1962.
[31] S. Warshall, "A theorem on boolean matrices," *J. ACM*, vol. 9, pp. 11–12, Jan. 1962.
[32] E. W. Dijkstra, "A note on two problems in connection with graphs," *Numerishe Matematik*, vol. 1, pp. 269–271, Dec. 1959.
[33] R. Bellman, "On a routing problem," *Quart. Appl. Math.*, vol. 16, pp. 87–90, 1958.
[34] L. R. D. Ford and R. Fulkerson, "Maximal flow through a network," *Can. J. Math.*, vol. 8, pp. 399–404, 1956.
[35] D. B. Johnson, "Efficient algorithms for shortest paths in sparse networks," *J. ACM*, vol. 24, pp. 1–13, 1977.
[36] Power Systems Test Case Archive Univ. Washington, Seattle, WA, USA [Online]. Available: http://www.ee.washington.edu/research/pstca/
[37] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "MATPOWER: Steady-State operations, planning and analysis tools for power systems research and education," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 12–19, Feb. 2011.
[38] P. McLaren, R. Kuffel, and R. Wierckx, "A real time digital simulator for testing relays," *IEEE Trans. Power Syst.*, vol. 7, pp. 207–213, 1992.
[39] A. Orebaugh, G. Ramirez, and J. Beale, *Wireshark & Ethereal Network Protocol Analyzer Toolkit*. Rockland, MA, USA: Syngress, Feb. 2007.
[40] D. Libes, "Expect: Scripts for controlling interactive processes," in *Computing Systems*. Berkeley, CA: Univ. California Press, 1991, vol. 4.
[41] M. Lutz, *Learning Python*, 4th ed. Sebastopol, CA, USA: O'Reilly Media, 2009.

Anurag K. Srivastava (M'00–SM' 09) received the Ph.D. degree from Illinois Institute of Technology (IIT), Chicago, in 2005.

He joined Washington State University, Pullman, as Assistant Professor in August 2010. He worked as an Assistant Research Professor at Mississippi State University from 2005–2010. His research interests include power system operation, control, security, and stability within smart grid and micro grid.

Dr. Srivastava is a Member of the IEEE Power and Energy Society (PES), IET, Sigma Xi, and Eta Kappa Nu. He is chair of the IEEE PES career promotion subcommittee and vice-chair of the IEEE PES student activities subcommittee and is active in several other IEEE PES technical committees.

Thomas Morris (M'00–SM' 08) received the Ph.D. degree from Southern Methodist University, Dallas, TX, in 2008.

He joined Mississippi State University (MSU), Mississippi State, as Assistant Professor in August 2008. His research interests include industrial control system penetration testing and intrusion detection systems.

Timothy A. Ernster (S'08) received the B.S. degree from Gonzaga University, Spokane, WA, in 2006, and is currently pursuing graduate studies at Washington State University, Pullman.

Since 2006 he has worked as an Electrical Engineer for the U.S. Army Corps of Engineers, with notable awards for service in support of the U.S. reconstruction mission in Baghdad, Iraq, during Operation Iraqi Freedom. His interests include power system operation and security.

Ceeman B. Vellaithurai (S'12) received the B.E. degree from Anna University Tiruchirappalli, India, in 2011 and is currently pursuing graduate studies at Washington State University, Pullman.

His research interests include real time modeling and simulation of power system.

Shengyi Pan (S'12) received the B.Eng. degree from Fuzhou Univeritys, China, in 2008 and the M.S. degree from University of Sheffield, U.K., in 2009. He is currently working toward the Ph.D. degree in Mississippi State University, Mississippi State. His research interests include security and intrusion detection for computer network, process control system, and smart grid.

Uttam Adhikari (S'11) received the B.S. degree in electrical engineering from Tribhuvan University, Nepal, in 2005, and is currently pursuing graduate studies at Mississippi State University, Mississippi State.

His research interests include wide area monitoring, control, and cyber security in smart grid.