Towards a Framework for Cyber Attack Impact Analysis of the Electric Smart Grid

Deepa Kundur   Xianyong Feng   Shan Liu   Takis Zourntos   Karen L. Butler-Purry
Department of Electrical and Computer Engineering
Texas A&M University
College Station, Texas 77843-3128
Email: {deepa, takis, klbutler}@ece.tamu.edu, xianyongfeng@gmail.com, liu2712@neo.tamu.edu

***Abstract*—This paper presents a framework for cyber attack impact analysis of a smart grid. We focus on the model synthesis stage in which both cyber and physical grid entity relationships are modeled as directed graphs. Each node of the graph has associated state information that is governed by dynamical system equations that model the physics of the interaction (for electrical grid components) or functionality (for cyber grid elements). We illustrate how cause-effect relationships can be conveniently expressed for both analysis and extension to large-scale smart grid systems.**

I. Introduction

The electric smart grid promises increased capacity, reliability and efficiency through the marriage of cyber technology with the existing electricity network. This integration, however, creates a new host of vulnerabilities stemming from cyber intrusion and corruption potentially leading to devastating physical effects. The security of a system is as strong as its weakest link. Thus, the scale and complexity of the smart grid, along with its increased connectivity and automation make the task of cyber protection particularly challenging.

Recently, smart grid researchers and standards bodies have developed technological requirements and solutions for protecting cyber infrastructure [1]–[8]. However, grid protection remains daunting to asset owners because of resources limitations [9], [10]. Important questions arise when identifying priorities for design and protection: Which cyber components, if compromised, can lead to significant power delivery disruption? What grid topologies are inherently robust to classes of cyber attack? Is the information available through advanced cyber infrastructure worth the increased security risk?

Vulnerability analysis for electric power utilities has begun to aid in answering these questions [11]–[13]. However, before such evaluation can have practical significance, it is necessary to quantitatively study the potential severity of physical impacts of cyber attacks. This requires identifying cascading failures within and between the cyber and physical domains. To address this challenge we study the development of a cyber security analysis methodology that accounts for the complex cyber-to-physical interactions.

The research presented in this paper represents a work in progress towards the development of a comprehensive and practical framework for electric smart grid cyber attack impact analysis shown in Fig. 1 that has been influenced by the needs of electric power utilities. Section II introduces and motivates the problem of smart grid cyber security. Fundamental research and development questions of importance to this area are discussed with a focus on the topic of cyber attack impact analysis. Sections III and IV introduce the proposed impact analysis framework based on a graph-theoretic dynamical systems approach for modeling the cyber-physical interactions. We demonstrate how model synthesis can be applied to an example system. Empirical results and discussion are found in Sections V and VI followed by conclusions in Section VII.

II. Smart Grid Cyber Security

A. Overview

A *smart grid* is defined as "the integration of real-time monitoring, advanced sensing, and communications, utilizing analytics and control, enabling the dynamic flow of both energy and information to accommodate existing and new forms of supply, delivery, and use in a secure and reliable electric power system, from generation source to end-user" (definition by North American Electric Reliability Corporation). From a technical perspective there is increased opportunity for cyber attack in a smart grid because of the greater dependence on intelligent electronic devices (IEDs), flexible communications infrastructures, distributed control centers and advanced metering infrastructure. Such cyber infrastructure increases communications connectivity, automation and control, and employs standardized information technologies (that often have documented vulnerabilities). Coupled with increased motivations for attack (that stem, in part, from privatization of the energy industry), cyber security of a smart grid represents a timely engineering problem.

Preliminary studies and mechanisms for cyber protection focus on data flow between the IEDs and control centers and employ traditionally information-centric metrics of performance. However, there is a significant need to quantitatively account for the physical impacts of a cyber attack since the ultimate objective of a smart grid is to provide reliable and secure power delivery. Hence, it is important to understand the influence a given data set has on power delivery capabilities to prioritize mitigation. Specifically, fundamental research and development questions arise: What attack scenarios are plausible to achieve a significant electric supply interruption?

978-1-4244-6511-8/10/$26.00 ©2010 IEEE

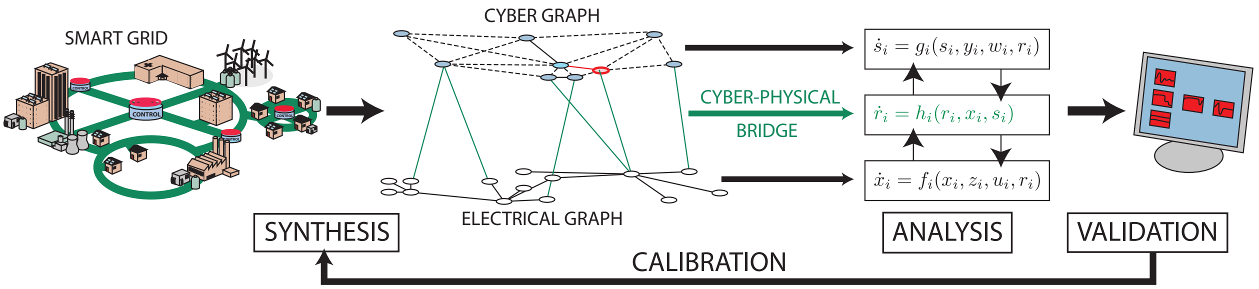

SMART GRID
CONTROL
CYBER GRAPH
ELECTRICAL GRAPH
CYBER-PHYSICAL
BRIDGE
$\dot{s}_i = g_i(s_i, y_i, w_i, r_i)$
$\dot{r}_i = h_i(r_i, x_i, s_i)$
$\dot{x}_i = f_i(x_i, z_i, u_i, r_i)$
SYNTHESIS
ANALYSIS
VALIDATION
CALIBRATION

Fig. 1: Stages of Proposed Impact Analysis Approach.

What realistic impacts can be achieved assuming certain vulnerabilities or successful attacks?

Risk analysis approaches for electric power utilities aim to understand the answers to such questions. However, strategies are as-of-yet ad hoc by nature. Mathematical models of these interactive subnetworks are typically vague or often do not exist [14]. One of the stumbling blocks is the inability to formally measure the impact of a cyber attack on power delivery metrics of importance to the power industry.

B. Cyber Attack Impact Analysis

One of the initial activities on cyber security assessment of power systems was a result of the Department of Energy Infrastructure Assurance Outreach Program [11]. Almost a decade ago, they set forth a vulnerability assessment process for energy infrastructure providers that included a series of analysis stages including

- the characterization of information threats by financially-motivated individuals/organizations, information warfare by other nations, environmental or political terrorists and unstructured adversaries such as hackers,
- cyber network architecture analysis to identify information assurance procedures,
- penetration testing to identify network vulnerabilities exploitable by tools available on the Internet,
- interdependency analysis with other critical infrastructures such as telecommunications and transportation, and
- *impact analysis* of unauthorized access to cyber infrastructure on physical system operations.

Risk characterization is to be conducted based on the tasks above (and others outlined in [11]). Risk of a given failure F is often related to *plausibility* and *severity* of system vulnerabilities, threats, and attack processes causing F as well as the *impact* quantifying the consequence of F on the power service [15]. It is well known that there is currently a lack of historical data to sufficiently estimate the above quantities necessitating the development of appropriate analysis tools focused for emerging power systems.

In this paper we introduce an approach for *cyber attack impact analysis* which involves quantifying the effects of given classes of cyber attack on the physical electrical grid, hence, providing information on the degree of disruption to power delivery that a class of cyber attacks can enable. This information is vital for vulnerability assessment [16]. Furthermore, based on this information sophisticated dependencies between the cyber and physical systems can be identified also shedding light on behaviors of complex interdependent networks.

Recent research that has focused on the interaction between the cyber and physical aspects of a smart grid to aid in cyber attack impact analysis takes on a variety of flavors [15]–[26]. Our work builds on this body of research by focusing in more detail on mathematically representing grid component interactions to better identify non-cookie-cutter vulnerabilities, the relative physical impact of cyber attacks, and cost-benefit trade-offs for potential countermeasures. Thus we aim to obtain a better compromise among computational complexity, generality and modeling accuracy.

Based on these problem requirements, we propose a paradigm for cyber attack impact analysis that employs a graph-theoretic structure and a dynamical systems framework to model the complex interactions amongst the various system system components.

III. Application of Graphs and Dynamical Systems

A graph is a mathematical structure that represents pairwise relationships between a set of objects. A graph is defined by a collection of *vertices* (also called *nodes*) and a collection of *edges* that connect node pairs. Depending the use of a graph, its edges may or may not have direction leading to directed or undirected classes of graphs, respectively. Graphs provide a convenient and compact way to show relationships and relate dependencies within cyber physical power systems as witnessed by recent papers that employ this tool [18], [23], [25], [27]–[33]. However, as cited in [32], purely graph-based approaches do not sufficiently model the state changes within the physical system. Moreover, they do not effectively account for the unique characteristics of the system at various time-scales nor provide a convenient framework for modeling system physics. We assert that modeling the electrical grid is a vital component to an effective impact analysis framework.

One approach to physically modeling complex engineering interactions employs dynamical systems. A dynamical system is a mathematical formalization used to describe time-evolution of a *state* $\mathbf{x}$, which can represent a vector of physical quantities. In continuous-time the deterministic evolution rule describes future states from current states as follows:

$$\dot{\boldsymbol{x}} = \boldsymbol{f}(\boldsymbol{x}, \boldsymbol{u}) \tag{1}$$

where $\dot{\boldsymbol{x}}$ is the time-derivative of $\boldsymbol{x}$ and $\boldsymbol{u}$ an input vector. Dynamical systems theory is motivated, in part, by ordinary differential equations and is well-suited to representing the complex physical interactions of the power grid [34].

We assert that a graph-based dynamical systems formulation is effective for a smart grid cyber attack impact analysis framework for a variety of reasons. First, smart grid impact analysis necessitates relating the cyber attack to physical consequences in the electricity network. A dynamical systems paradigm provides a flexible framework to model (with varying granularity and severity) the cause-effect relationships between the cyber data and the electrical grid state signals and ultimately relate them to power delivery metrics. Furthermore, secondary effects whereby the consequence of an attack itself influences the continued degree of attack can be represented.

Second, graphs enable a tighter coupling between the cyber and physical domains. For a smart grid, the cyber-to-physical connection is often represented through control signals that actuate change in the power system and the physical-to-cyber connection is typically due to the acquisition of power state sensor readings. These connections can be conveniently expressed as specifically located edges of the graphs. Furthermore, as we will discuss, the graphs induce a dynamical systems description of the overall smart grid, which conveniently expresses complex time-varying interrelationships. This way cascading failures and emergent properties from the highly coupled system can be represented. Mitigation approaches often involve islanding of the grid or partitioning of the core smart grid components from optimization functions [14], and a graph-based dynamical systems formulation can naturally portray such separation as well.

IV. Graph-Based Dynamical Systems Model Synthesis

An overview of our impact analysis approach, which is currently a work-in-progress, is shown in Fig. 1. The three stages of model synthesis, system analysis and system validation are present. In addition, the output of the validation stage is used to *recalibrate* our synthesis approach.

In our model synthesis stage, which is the focus of the remainder of this paper, we use dynamical systems for the systematic modeling of the cyber and electrical grids; this affords the flexibility to tune the granularity of detail. The use of graphs conveniently facilitates incorporating complex dependencies within and between the cyber and electric components. This stage is critical as it determines the relative accuracy of a smart grid impact analyses and dictates the possible analysis tools available to glean insights about vulnerabilities and strategies for system hardening. We have developed a general and systematic approach to modeling a smart grid system using graph-based dynamical system approach.

To elucidate our approach, we focus on the "elementary" example of Fig. 2 that represents a potential system overload and instability situation. In the single generator system, G represents a conventional generator (such as nuclear, coal and natural gas) that serves two loads denoted Z_1 and Z_2. The transformer T_1 steps down the voltage and is connected to Cable 1. Cables 2 and 3 are connected to loads as shown. The hexagon symbols represent cyber infrastructure. The system control center is shown and it communicates control signals to each of the three switches shown. For switch i (denoted with a hexagon with an i in the center), the control center communicates control signal $c_i(t)$ where $c_i(t) = 0$ denotes open switch and $c_i(t) = 1$ denotes close switch at time t. The control center senses information at the output of the generator denoted s_1, and at the outputs of Cables 1, 2, and 3 denoted s_2, s_3 and s_4, respectively. This information is passed to the control center which employs a simple load shedding algorithm to ideally avoid an overload situation if load demand exceeds generation. If the sensed overall load demand exceeds generation, then load management sheds one or both loads to avoid instability by opening their corresponding switches using control signals. If sensed information reveals that neither load can individually be served by G then both are shed. If it appears that only one can be served, then the smaller load is shed assuming the larger load can be served by G; otherwise, the smaller load is served.

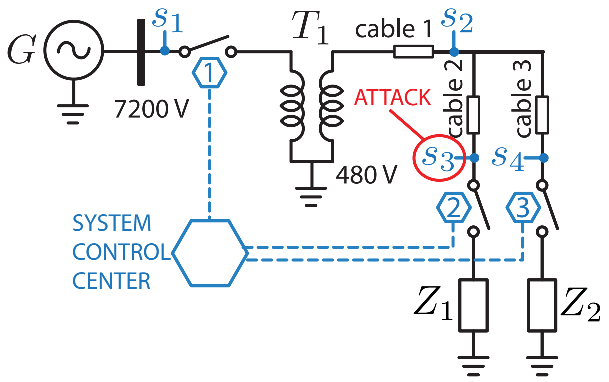


Fig. 2: One Line Diagram of Elementary Power System Example. Cyber attack is applied to tamper with sensor s_3 effecting load management decisions by the control center.

A typical cyber attack can involve fabricating or tampering with the sensor information, so that load management involves incorrect decision-making. In such a situation loads are dropped when it is possible to serve them or loads are not dropped when demand exceeds generation leading to decrease of generator frequency and finally generator trip out.

As a first modeling step, electrical and cyber graphs are formed such that each node represents associated grid elements; in this representation, nodes can be generators, transformers, loads or plug-in hybrids, circuit-breakers (electric), switches and control centers, sensors and breaker actuator controls (cyber). Given this granularity of detail, edges are selected in order to represent state dependencies amongst the various components. As an instructive example, we show the graph corresponding to Fig. 2; in Fig. 3, the electrical and cyber graphs are shown along with edges representing dependencies amongst components within the same network or at the cyber-physical bridge. Thus, there is a node for every generator, transformer, load/plug-in hybrid, circuit breaker, switch, control center, sensor and actuator. Directed links

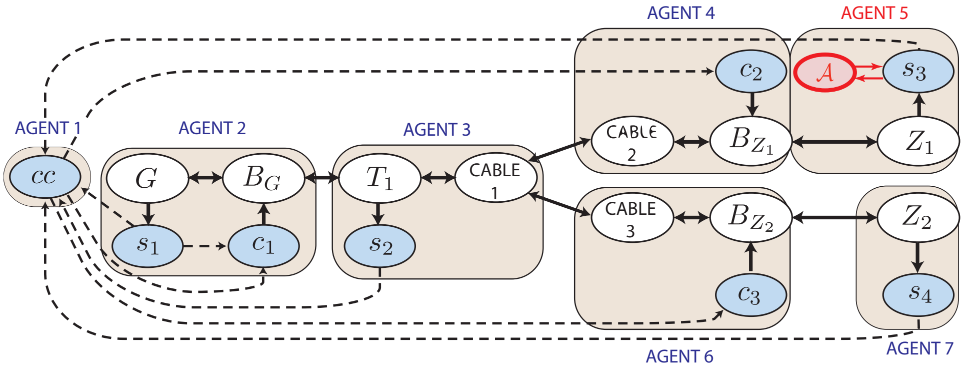


Fig. 3: Electrical and Cyber Graphs for System of Fig. 2. Nodes are comprised of a generators G, circuit breakers B_i, a transformer T and loads/plug-in hybrids Z_i of the electrical network and a control centers cc, sensors s_i and actuator controls c_i of the cyber network. Edges represent state dependencies for dynamical modeling. The cyber graph is distinguished with shaded nodes and dashed edges. Attack $\mathcal{A}$ targets the sensor s_3. Example agent groupings for analysis are also presented.

exist between nodes if there is an energy or information flow dependence. The grid elements are mapped to nodes based on the fact that it is feasible to model their behavior using dynamical equations. For simplicity, communication links are modeled ideally, but this does not have to be the case in general. The cyber attack node $\mathcal{A}$ influences the sensor signal $s_3(t)$ at the output of Cable 2.

Each node has an associated state $\boldsymbol{x}$ (consisting of appropriate system voltages and currents) governed by dynamical system equations that model the physics of the entity (for the case of power system elements) or the functional or computational processing (for the case of cyber elements). The exact expression for $\boldsymbol{f}$ depends on the edges of the associated node. Nodes can be grouped to form *dynamic agents* to represent interactions within a smart grid as highlighted in Fig. 3 based on functionally or to balance subsystem order to aid in analysis. Here, we focus on our preliminary results pertaining to the graph and dynamical systems modeling of cause-effect relationships of a cyber attack.

V. Preliminary Results

We implement the graph-based dynamical system model of Fig. 3, which models the system of Fig. 2. A 12-parameter ordinary differential equation generator model with generator capacity 0.8 MW is employed that incorporates a governor, threshold limiter, and prime mover elements as shown in Fig. 4. The threshold for the generator under-frequency relay is set to 58 Hz; thus, when the system frequency drops under 58 Hz, the generator will be tripped out.

All breakers are assumed to be ideal and controlled by a corresponding control signal $c_i(t)$ from the system control center. An ideal transformer with conversion factor 15 is assumed. Both of these types of components represent trivial dynamical systems since they can be modeled as (time-varying in the case of the switch) amplification systems. All three cables are represented with lumped resistive and inductive models that are easily represented with differential equations and as dynamical systems. Specifically, for Cables 1, 2 and 3, $R = 0.001, 0.001, 0.001\ \Omega$ and $L = 0.000027, 0.000027, 0.000027$ H, respectively. The first load denoted Z_1 is an resistive-inductive load with rating 0.6 MW and 0.8 PF (power factor); it is modeled with $R = 0.2158\ \Omega$ and $L = 0.0004293$ H. The second load denoted Z_2 is a resistive-capacitive load with rating 0.4 MW with 0.8 PF with $R = 0.606\ \Omega$ and $C = 0.0032$ F. The control center employs load management and in our elementary example controls all three switches. The second and third switches before loads Z_1 and Z_2, respectively, allow load shedding at appropriate times to avoid system instability. As previously discussed load shedding occurs only if an individual or the combined load demand exceeds generation. The sensor information s_i, $i = 1, 2, 3, 4$ is employed for this decision-making process. If any of the sensors readings are tampered with through a cyber attack, then there is potential to reach an unwanted outcome.

A. Case Study

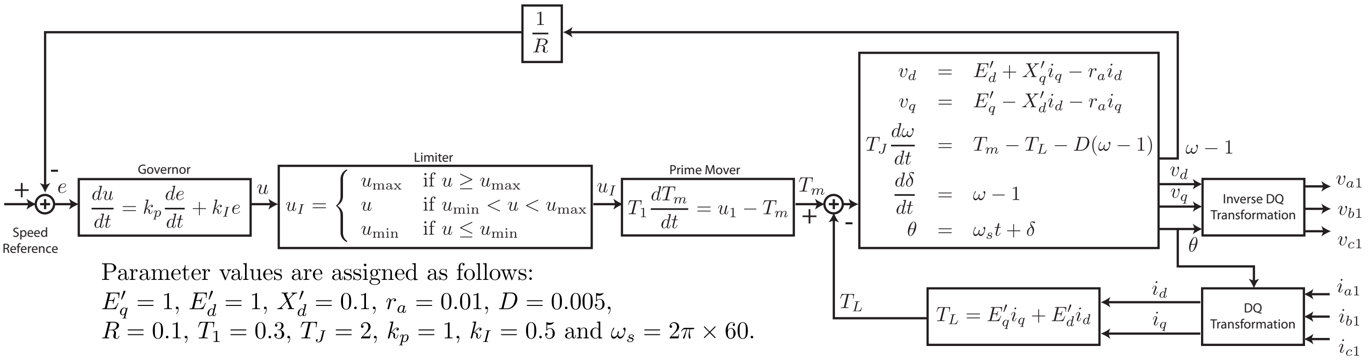
The graph-based dynamical system model of Fig. 3 was simulated in MATLAB/Simulink using the fourth-order Runge-Kutta method with a step size of 0.001seconds and simulation duration of 20 seconds. We present the results of one of our case studies to demonstrate how a cyber attack on sensor reading s_3 will result in a disruption in power delivery. In the system of Fig. 2 s_3 is biased through cyber tampering. Thus, we can model the sensor output as:

$$s_3(t) = \mathcal{B}(t) + P_3(t) \tag{2}$$

where $s_3(t)$ is the tampered sensor reading, $\mathcal{B}(t)$ is an unwanted bias that represents the tampering and $P_3(t)$ is the *true* power at the output of Cable 2 that s_3 is intended to track. Continuous-time modeling is conducted to integrate the cyber-physical graphs, but this can also be modified to discrete-time with some additional overhead at the cyber-physical boundary.

The generator G has capacity of 0.8 MW. Since Loads 1 and 2 have ratings 0.6 MW and 0.4 MW, respectively, it is clear that G cannot simultaneously serve both. The control center will choose to shed Load 2 in favor of Load 1 should they both demand service simultaneously. In the simulations, at 0 seconds Load 1 is assumed to come on and thus Load 2 is shed (if it were one prior to 0 seconds) as it is the smaller rated load. In this study a cyber attack is applied at 7 seconds on s_3 by adding a bias $\mathcal{B}(t)$ such that it may effect load management by the control center. A load management processing delay of 0.2 seconds is assumed.

Fig. 5(a) shows the output of s_3. From 0 to 7 seconds, Load 1 is being served thus, it is reading 0.6 MW as expected. At 7


$\frac{1}{R}$
Governor
$\frac{du}{dt} = k_p\frac{de}{dt} + k_I e$
Limiter
$u_I = \begin{cases} u_{\max} & \text{if } u \geq u_{\max} \\ u & \text{if } u_{\min} < u < u_{\max} \\ u_{\min} & \text{if } u \leq u_{\min} \end{cases}$
Prime Mover
$T_1\frac{dT_m}{dt} = u_1 - T_m$
$v_d = E'_d + X'_q i_q - r_a i_d$
$v_q = E'_q - X'_d i_d - r_a i_q$
$T_J\frac{d\omega}{dt} = T_m - T_L - D(\omega - 1)$
$\frac{d\delta}{dt} = \omega - 1$
$\theta = \omega_s t + \delta$
$\omega - 1$
Inverse DQ Transformation
DQ Transformation
$T_L = E'_q i_q + E'_d i_d$
+
-
e
u
u_I
T_m
T_L
v_d
v_q
θ
i_d
i_q
v_{a1}
v_{b1}
v_{c1}
i_{a1}
i_{b1}
i_{c1}
Speed Reference

Parameter values are assigned as follows:
$E'_q = 1$, $E'_d = 1$, $X'_d = 0.1$, $r_a = 0.01$, $D = 0.005$,
$R = 0.1$, $T_1 = 0.3$, $T_J = 2$, $k_p = 1$, $k_I = 0.5$ and $\omega_s = 2\pi \times 60$.

Fig. 4: Dynamical System Model for Generator.

seconds, the sensor is tampered and three different bias values of $\mathcal{B}(t) = 0.9, 0.1, -0.3$ are considered. Fig. 5(b) presents the output of the sensor at Load 2. As expected, it is not being served. However, for tampered Bias values of $\mathcal{B}(t) = 0.9$ and $\mathcal{B}(t) = -0.3$, Load 2 is served. In the former case, this is because it appears that the second load is being served, and G (with capacity 0.8 MW) cannot serve both, thus, Load 1 is shed (assuming it is the smaller load from the tampered s_3).

In the latter case, of $\mathcal{B}(t) = -0.3$ it appears that both loads can be simultaneously served, so they are both switched on. As seen in Fig. 5(c) this increases the total power generation to be 1 MW, which is the sum of the actual load ratings of 0.6 MW (for Load 1) and 0.4 MW (for Load 2). However, as witnessed in Fig. 5(d), this has the effect of decreasing generator frequency. At 18.579 seconds, the frequency runs below 58 Hz, which instigates the under-frequency relay to trip out the generator creating a system blackout. For a bias $\mathcal{B}(t) = 0.1$, although the sensor reading is incorrect, it does not actuate an incorrect load management decision.

VI. Discussion

It is clear that our graph-based dynamical system model synthesized from Fig. 2 represents expected behaviors. To have potential for realistic cases, it is important to characterize how the approach scales to larger systems.

The complexity of processing is dependent on graph size (i.e., number of nodes), graph connectivity (related to number of links) and the particular dynamics (related to its order) used to model the nodes. Thus, if the same procedure of mapping a smart grid to a graph were used for large studies, such as the IEEE power flow test cases, it is apparent that the size of the graph would grow incredibly. We assert that this may not necessarily increase the complexity of the processing beyond practicality. For instance, the graph-based dynamical systems paradigm allows nodes to be grouped into "agents" as shown in Fig. 3 whereby each agent (instead of node) is modeled using dynamical system equations. Appropriate grouping of agents would allow necessary system behaviors to be characterized while approximating others that are not as salient to impact analysis. This method of grouping with effective modeling of dynamics is currently the focus of future work.

VII. Conclusions

In this paper we have introduced an approach to cyber attack impact analysis applicable to emerging smart grids. The advantage of this graph-theoretic dynamical systems paradigm is that continuous-time electrical, discrete-event cyber and their interface can be modeled within one framework allowing a single, but potentially powerful analysis approach. Future work will involve application of the synthesis methodology to large-scale systems and the use of PSCAD® and Powertech Labs' DSA*Tools*™ to verify our models results.

References

[1] D. Watts, "Security and vulnerability in electric power systems," in *Proc. 35th North American Power Symposium*, Rolla, Missouri, October 2003, pp. 559–566.

[2] S. Committee, "IEEE standard for substation intelligent electronic devices (IEDs)," IEEE Power Enginering Society, Standard IEEE Std 1686-2007, December 5 2007.

[3] L. Pietre-Cambacedes, C. Chalhoub, and F. Cleveland, "IEC TC57 WG15 – Cyber security standards for the power systems," CIGRÉ Study Committee D2: Information Systems and Telecommunications, Tech. Rep. D2-02-C02, 2007.

[4] H. Endoh, "Analyzing aspects of cyber security standards for M&CS," in *Proc. SICE Annual Conference*, Augustt 2008, pp. 1478–1481.

[5] H. Falk, "Securing IEC 61850," in *Proc. IEEE Power and Energy Society General Meeting – Conversion and Delivery of Electrical Energy in the 21st Century*, July 2008, pp. 1–3.

[6] R. McDonald, "New considerations for security compliance, reliability and business continuity," in *Proc. IEEE Rural Electric Power Conference*, April 2008, pp. B1–B1–7.

[7] L. Piètre-Cambacédès, T. Kropp, J. Weiss, and R. Pellizzonni, "Cybersecurity standards for the electric power industry – a "survival kit"," in *Proc. CIGRÉ Paris Session*, 2008, pp. Paper D2–213.

[8] G. N. Ericsoon, "Information security for electric power utilities (EPUs) – CIGRÉ developments on frameworks, risk assessment, and technology," *IEEE Transactions on Power Delivery*, vol. 24, no. 3, pp. 1174–1181, July 2009.

[9] V. Madani and T. Witham, "Strategies for protection and control standardization and integrated data management applications," in *Proc. IEEE/PES Transmission and Distribution Conference and Exposition*, April 2008, pp. 1–6.

[10] M. Mertz, "NERC CIP compliance: We've identified our critical assets, how what?" in *Proc. IEEE Power and Energy Society General Meeting – Conversion and Delivery of Electrical Energy in the 21st Century*, July 2008, pp. 1–2.

[11] J. Dagle, "Vulnerability assessment activities," in *Proc. Power Engineering Society Winter Meeting*, vol. 1, 2001, pp. 108–113.

[12] J. Depoy, J. Phelan, P. Sholander, B. Smith, G. B. Varnado, and G. Wyss, "Risk assessment for physical and cyber attacks on critical infrastructures," in *Proc. IEEE Military Communications Conference*, vol. 3, October 2005, pp. 1961–1969.

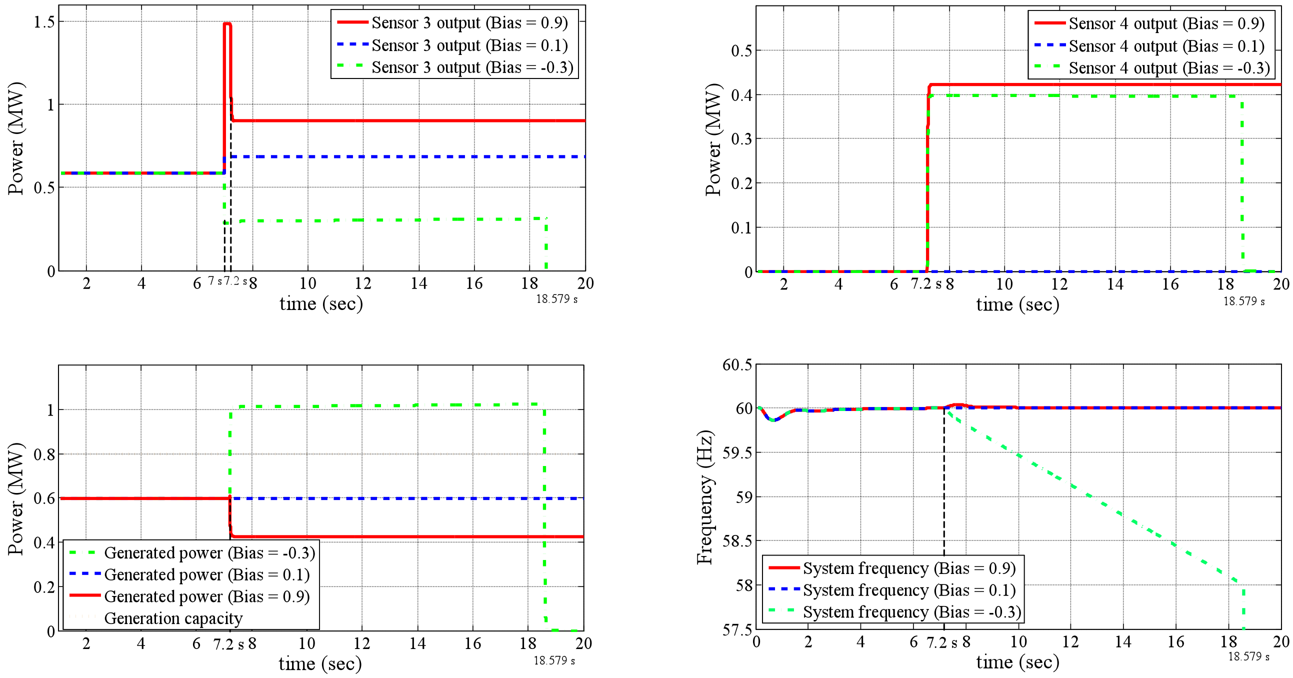


Fig. 5: (a) [top-left] Output of s_3, (b) [top-right] Output of s_4, (c) [bottom-left] Total Power Generation, (d) [bottom-right] Generator Frequency.

[13] Y. Jiaxi, M. Anjia, and G. Zhizhong, "Vulnerability assessment of cyber security in power industry," in *Proc. IEEE Power Systems Conference and Exposition*, October-November 2006, pp. 2200–2205.

[14] M. Amin, "Energy infrastructure defense systems," *Proceedings of the IEEE*, vol. 93, no. 5, pp. 861–875, May 2005.

[15] G. Dondossola, F. Garrone, and J. Szanto, "Supporting cyber risk assessment of power control systems with experimental data," in *Proc. IEEE Power Systems Conference and Exposition*, March 2009, pp. 1–3.

[16] J. Stamp, A. McIntyre, and B. Ricardson, "Reliability impacts from cyber attack on electric power systems," in *Proc. IEEE Power Systems Conference and Exposition*, March 2009, pp. 1–8.

[17] C. M. Davis, J. E. Tate, H. Okhravi, C. Grier, T. J. Overbye, and D. Nicol, "SCADA cyber security testbed development," in *Proc. 38th North American Power Symposium*, September 2006, pp. 483–488.

[18] D. D. Dudenhoeffer, M. R. Permann, S. Woolsey, R. Timpany, C. Miller, A. McDermott, and M. Manic, "Interdependency modeling and emergency response," in *Proc. 2007 Summer Computer Simulation Conference*, July 2007, pp. 1230–1237.

[19] D. Edwards, S. K. Srivastava, D. A. Cartes, S. Simmons, and N. Wilde, "Implementation and validation of a mult-level security model architecture," in *Proc. International Conference on Intelligent Systems Applications to Power Systems*, November 2007, pp. 1–4.

[20] T. Mander, F. Nabhani, L. Wang, and R. Cheung, "Integrated network security protocol layer for open-access power distribution systems," in *Proc. IEEE Power Engineering Society General Meeting*, June 2007, pp. 1–8.

[21] S. Sheng, W. L. Chan, K. K. Li, D. Xianzhong, and Z. Xiangjun, "Context information-based cyber security defense of protection system," *IEEE Transactions on Power Delivery*, vol. 22, no. 3, pp. 1477–1481, July 2007.

[22] B. McMillin, "Complexities of information security in cyber-physical power systems," in *Proc. IEEE Power Systems Conference and Exposition*, March 2009, pp. 1–2.

[23] K. Xiao, N. Chen, S. Ren, L. Shen, X. Sun, K. Kwiat, and M. Macalik, "A workflow-based non-intrusive approach for enhancing the survivability of critical infrastructures in cyber environment," in *Proc. Third International Workshop on Software Engineering for Secure Systems*, May 2007.

[24] B. Rozel, M. Viziteu, R. Caire, N. Hadjsaid, and J.-P. Rognon, "Towards a common model for studying critical infrastructure interdependencies," in *Proc. IEEE Power and Energy Society General Meeting – Conversion and Delivery of Electrical Energy in the 21st Century*, Pittsburgh, Pennsylvania, July 2008, pp. 1–6.

[25] N. HadjSaid, C. Tranchita, B. R. ad M. Viziteu, and R. Caire, "Modeling cyber and physical interdependencies – application in ICT and power grids," in *Proc. IEEE Power Systems Conference and Exposition*, March 2009, pp. 1–6.

[26] C.-C. Liu, C.-W. Ten, and M. Govindarasu, "Cybersecurity of SCADA systems: Vulnerability assessment and mitigation," in *Proc. IEEE Power Systems Conference and Exposition*, March 2009, pp. 1–3.

[27] D. Conte de Leon, J. Alves-Foss, A. Krings, and P. Oman, "Modeling complex control systems to identify remotely accessible devices vulnerable to cyber attack," in *Proc. First Workshop on Scientific Aspects of Cyber Terrorism*, Washington, D.C., November 2002.

[28] D. D. Dudenhoeffer, M. R. Permann, and M. Manic, "CIMS: A framework for infrastructure interdependency modeling and analysis," in *Proc. 38th Winter Simulation Conference*, December 2006, pp. 478–485.

[29] R. Dawson, C. Boyd, E. Dawson, and J. Manuel Gonzàlez Nieto, "SKMA – A key management architecture for SCADA systems," in *Proc. Fourth Australasian Workshops on Grid Computing and E-Research*, vol. 54, January 2006, pp. 183–192.

[30] M. A. McQueen, W. F. Boyer, M. A. Flynn, and G. A. Beitel, "Quantitative cyber risk reduction estimation methodology for small SCADA control system," in *proc. 39th Annual Hawaii International Conference on Systems Sciences*, vol. 9, January 2006, pp. 226–236.

[31] W. Eberle and L. Holder, "Insider threat detection using graph-based approaches," in *Proc. Cybersecurity Applications and Technology Conference for Homeland Security*, 2009, pp. 237–241.

[32] M. Ekstedt and T. Sommestad, "Enterprise architecture models for cyber security analysis," in *Proc. IEEE Power Systems Conference and Exposition*, March 2009, pp. 1–6.

[33] H. Hadeli, R. Schierholz, M. Braendle, and C. Tuduce, "Generating configuration for missing traffic detector and security measures in industrial control systems based on the system description files," in *Proc. IEEE Conference on Technologies for Homeland Security*, May 2009, pp. 503–510.

[34] X. Feng, T. Zourntos, and K. L. Butler-Purry, "Dynamic load management for NG IPS ships," in *Proc. IEEE Power Engineering Society General Meeting*, Minneapolis, Minnesota, July 2010.