Towards modelling the impact of cyber attacks on a smart grid

D. Kundur*, X. Feng, S. Mashayekh, S. Liu, T. Zourntos and K.L. Butler-Purry

Department of Electrical and Computer Engineering,
Texas A&M Univesity,
College Station, Texas 77843-3128, USA
Fax: 979-862-8684
E-mail: deepa@ece.tamu.edu
*Corresponding author

Abstract: This paper provides an introduction to cyber attack impact analysis in the smart grid and highlights existing research in the field. We present an impact analysis framework where we focus on the model synthesis stage where both cyber and physical grid entity relationships are modelled 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.

Keywords: smart grid cyber security; cyber attack impact analysis; graph-based dynamical systems; smart grid model synthesis.

Reference to this paper should be made as follows: Kundur, D., Feng, X., Mashayekh, S., Liu, S., Zourntos, T. and Butler-Purry, K.L. (2011) 'Towards modelling the impact of cyber attacks on a smart grid', *Int. J. Security and Networks*, Vol.

Biographical notes: Deepa Kundur received her BASc, MASc and PhD Degrees all in Electrical and Computer Engineering at the University of Toronto in 1993, 1995 and 1999, respectively. She is currently is an Associate Professor in Electrical and Computer Engineering at Texas A&M University. Her research interests include cyber security of the smart grid, security and privacy of sensor systems and information forensics.

Xianyong Feng is a PhD student in Electrical and Computer Engineering at Texas A&M University. His research interests include load management for integrated power systems, multi-agent system, and cyber-physical energy systems.

Salman Mashayekh is a PhD student in Electrical and Computer Engineering at Texas A&M University. His focus is on power management systems, and physical security and cyber security of power systems.

Shan Liu is a PhD student in Electrical and Computer Engineering at Texas A&M University. Her research includes cyber security of the electric smart grid, security of social networks.

Takis Zourntos received his BASc, MASc and PhD Degrees all in Electrical Engineering at the University of Toronto in 1993, 1996 and 2003, respectively. He is currently a Research Professor in Computer Science and Engineering at Texas A&M University. His research interests include lightweight autonomous robotics and application of nonlinear control theory.

Karen L. Butler-Purry received her BSEE from Souther University in 1985, MSEE from the University of Texas at Austin in 1987 and PhD from Howard University in 1994. She is currently Professor of Electrical and Computer Engineering and Executive Associate Vice President for Graduate Studies at Texas A&M University. Her research interests are in the areas of computer and intelligent systems application to power distribution systems, distribution automation and management, fault diagnosis, estimation of remaining life of transformers, intelligent reconfiguration, and system modelling and simulation for hybrid vehicles.

Copyright © 2011 Inderscience Enterprises Ltd.

1 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 (Amin, 2005, 2008; Boyer and McBride, 2009; McDaniel and Smith, 2009).

Recently, smart grid researchers and standards bodies have developed technological requirements and solutions for protecting cyber infrastructure (Watts, 2003; Committee, 2007; Pietre-Cambacedes et al., 2007, 2008; Endoh, 2008; Falk, 2008; McDonald, 2008; Ericsoon, 2009). However, grid protection remains daunting to asset owners because of resources limitations (Madani and Witham, 2008; Mertz, 2008). 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 (Dagle, 2001; Depoy et al., 2005; Jiaxi et al., 2006). 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 Figure 1 that has been influenced by the needs of electric power utilities.

The contributions of this paper are two-fold:

- Due to the emerging nature of the field of smart grid cyber security, we provide a necessary introduction to motivations and fundamental research and development questions in this active area. We focus on the topic of cyber attack impact analysis.

- We then introduce a graph-theoretic dynamical systems approach for modelling the interactions between the cyber and the electricity networks focusing on the model synthesis stage.

Section 2 introduces and motivates the problem of smart grid cyber security. Sections 3 and 4 introduce the proposed impact analysis framework based on a graph-theoretic dynamical systems approach for modelling the cyber-physical interactions. We demonstrate how model synthesis can be applied to two test systems. Empirical results and discussion are found in Sections 5 and 6 followed by conclusions in Section 7.

2 Smart grid cyber security

2.1 Overview

A *smart grid* is defined as

> "the integration of real-time monitoring, advanced sensing, and communications, utilising 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 centres and advanced metering infrastructure. Such cyber infrastructure increases communications connectivity, automation and control, and employs standardised information technologies (that often have documented vulnerabilities). Coupled with increased motivations for attack (that stem, in part, from privatisation of the energy industry), cyber security of a smart grid represents a timely engineering problem.

Table 1 summarises statistics of recent media reported cases of disruptions to electric power delivery around the world. As can be seen, from the report cases, a majority are due to malicious cyber attack.

Securing a smart grid is also important for protecting the public from terrorism, vandalistic hackers, disgruntled insiders of the electric power industry and cascading failures from the loss of other critical infrastructures. The associated attacks on availability can result in damaging instability such as blackouts and brownouts. Moreover protecting a smart grid makes business sense. Protection of cyber devices is needed to establish compliance to cyber security requirements to be able to compete in the electricity marketplace. Security also represents a means to reduce or divert technical liability and assure revenue by discouraging competitor component cloning.

Preliminary studies and mechanisms for cyber protection focus on data flow between the IEDs and control centres 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

Figure 1 Stages of proposed impact analysis approach (see online version for colours)

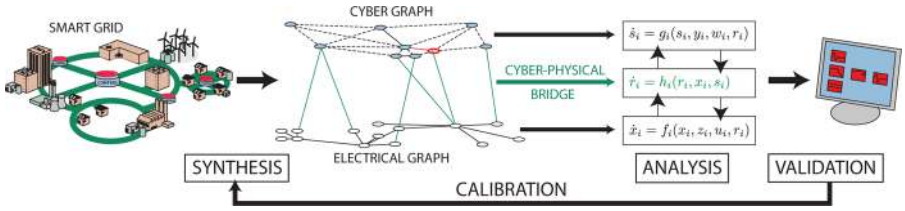


Table 1 Summary statistics of recently reported cases of disruptions to power delivery in recent media

Attribute	*Percentage* (%)	*Attribute*	*Percentage* (%)
Malicious attack	71.4	Operator error	28.6
Resolved within 48 h	76.4	Resolved after 48 h	23.6
Affected $> 100,000$ People	71.4	Affected $< 100,000$	26.6
Solved internally	50.0	Solved externally (gov't intervention)	50.0

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 prioritise mitigation. Specifically, fundamental research and development questions arise: What attack scenarios are plausible to achieve a significant electric supply interruption? 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 (Amin, 2005). 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.

2.2 *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 (Dagle, 2001). Almost a decade ago, they set forth a vulnerability assessment process for energy infrastructure providers that included a series of analysis stages including

- the characterisation of information threats by financially-motivated individuals/organisations, 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
- *impact analysis* of unauthorised access to cyber infrastructure on physical system operations.

Risk characterisation is to be conducted based on the tasks above (and others outlined in Dagle (2001)). Risk of a given failure F is 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 (Liu et al., 2009; Dondossola et al., 2009).

Simply, risk is defined as follows:

$$R(F) = L(F) \times I(F) \tag{1}$$

where $R(F)$, $L(F)$ and $I(F)$ represent the risk, likelihood and impact of a given failure F due to a cyber attack. The likelihood $L(F)$ can further be broken down into the product of the likliehood of threats and vulnerabilities to give a three-dimensional method of evaluating risk.

$$R(F) = L(F) \times I(F) = T(F) \times V(F) \times I(F) \tag{2}$$

where $T(F)$ and $V(F)$ denote the likelihood of threats and vulnerabilities associated with F. It is well known that there is currently a lack of historical data to sufficiently estimate any of the above quantities necessitating the development of appropriate analysis tools focused for emerging power systems. It may be possible to estimate $L(F)$, $T(F)$ or $V(F)$ using conventional analysis methodologies for systems security, but the impact $I(F)$ is difficult to assess given the complex system interdependencies that characterise a smart grid and the evolving nature of modern power systems.

In this paper we consider the problem of *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 (Stamp et al., 2009). Furthermore, based on this information sophisticated dependencies between the cyber and physical systems can be identified also shedding light on behaviours 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 flavours. These techniques can be classified into a number of groups. *Static approaches* (Conte de Leon et al., 2002) consider the topological information about the smart grid in order to study vulnerabilities often using graph-theoretic means. *Empirical approaches* (Dudenhoeffer et al., 2007; Rozel et al., 2008; HadjSaid et al., 2009; Stamp et al., 2009) harness research and development of realistic communications and power systems simulators. These two forms of simulators are combined such that an attack is applied in the communication simulator that transfers data to the power systems simulator which makes decisions based on this possibly corrupt information. Typical traditional power system reliability metrics are used to assess impact of the cyber attacks. In *cyber-physical leakage approaches* (Tan, 2007; Tang and McMillin, 2008; McMillin, 2009) confidentiality of the cyber network is studied by identifying how voltage and current measurements of the physical power system can be analysed for any clues about cyber protocol activity. *Mechanistic techniques* (Sheng et al., 2007; Edwards et al., 2007; Mander et al., 2007; Xiao et al., 2007) involve cyber protocols, algorithms and architectures that account for the physical power system. *Testbed systems research* addresses the exploration of practical vulnerabilities through SCADA testbed development and construction (Davis et al., 2006; Giani et al., 2008; Dondossola et al., 2009). Finally, research on attacks on control systems (Cárdenas et al., 2008a, 2008b, 2008c) focus on how data corruption of denial of information access can affect the control of the power grid.

Our work builds on this body of research by focusing 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 modelling 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 components.

3 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 (Conte de Leon et al., 2002; Dudenhoeffer et al., 2006, 2007; Dawson et al., 2006; McQueen et al., 2006; Xiao et al., 2007; Eberle and Holder, 2009; Ekstedt and Sommestad, 2009; HadjSaid et al., 2009; Hadeli et al., 2009). However, as cited in Ekstedt and Sommestad (2009), 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 modelling system physics. We assert that modelling the electrical grid is a vital component to an effective impact analysis framework.

One approach to physically modelling complex engineering interactions employs dynamical systems. A dynamical system is a mathematical formalisation 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:

$$\dot{\boldsymbol{x}} = \boldsymbol{f}(\boldsymbol{x}, \boldsymbol{u}) \tag{3}$$

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 (Feng et al., 2010).

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 optimisation functions (Amin, 2005), and a graph-based

dynamical systems formulation can naturally portray such separation as well.

Last, a primary effect of including cyber attacks in traditional reliability analysis is that it increases the size of the system under study by several orders of magnitude (Stamp et al., 2009). Our proposed mathematical formulation has the potential to keep studies tractable because our granularity of detail can be tuned and the use of dynamics can enable sophisticated behaviours without a corresponding increase in complexity.

4 Graph-based dynamical systems model synthesis

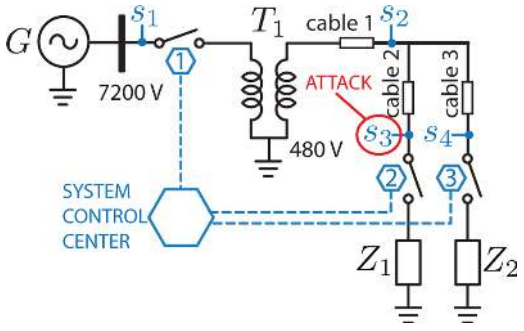
An overview of our impact analysis approach, which is currently a work-in-progress, is shown in Figure 1. The three stages of model synthesis, system analysis and system validation are present. In addition, the output of the validation stage is used to *recalibrate* our synthesis approach.

In our model synthesis stage, which is the focus of the remainder of this paper, we use dynamical systems for the systematic modelling 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 modelling a smart grid system using graph-based dynamical system approach. To elucidate our approach, we focus on two case studies.

4.1 Single generator system

First, we present an 'elementary' example of Figure 2 that represents a potential system overload and instability situation. Then we focus on a microgrid test example modified from the IEEE 13 node distribution test system.

Figure 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 centre (see online version for colours)



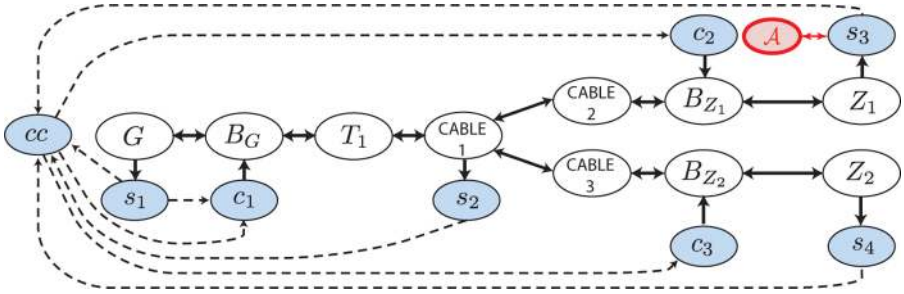
In the initial single generator system, G represents a conventional generator (such as nuclear, coal and natural gas) that serves two loads denoted Z_1 and Z_2. The transformer T_1 steps down the voltage and is connected to Cable 1. Cables 2 and 3 are connected to loads as shown. The hexagon symbols represent cyber infrastructure. The system control centre 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 centre), the control centre 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 centre 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 centre 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.

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 modelling 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 centres, 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 Figure 2; in Figure 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 centre, sensor and actuator. Directed links 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 behaviour using dynamical equations. For simplicity, communication links are modelled 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

Figure 3 Electrical and cyber graphs for system of Figure 2. Nodes are comprised of a generator G, circuit breakers B_i, cables, a transformer T and loads Z_i of the electrical network and a control centre cc, sensors s_i and actuator controls c_i of the cyber network. The cyber graph is distinguished with shaded nodes and dashed edges. Attack $\mathcal{A}$ targets the sensor s_3 (see online version for colours)



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 Figure 3 based on functionally or to balance subsystem order to aid in analysis. We leave agent-based analysis for future work.

4.2 13 node distribution test system

The second system we consider is based on the IEEE 13 node test feeder system (http://ewh.ieee.org/soc/pes/dsacom/testfeeders/index.html), but has been modified in two significant ways. First, three Distributed Energy Resources (DERs) have been added at Nodes 634, 646, 680. Second, a switch has been added after node 650 in order to enable the overall distribution system to operate in islanding mode. In the study of this system, the switch is assumed to always be open. Therefore, the three DERs in the system are responsible to supply as much of the system load as possible. The overall system is shown in Figure 4.

DER1 represents a 150 kW wind power generation unit that is connected to Node 634 through a power electronic interface. DER2 and DER3 are 2000 kW and 500 kW small synchronous generators, respectively that are directly connected to Nodes 680 and 646. Thus, the total generation capacity is 2650 kW. The loads in this system add up to 3466 kW and thus must be selectively prioritised if the system is operating in islanding mode. Table 2 shows the priority levels for each of the nine loads.

The load serving logic is designed such that if the generation capacity is not sufficient to supply a load, but a smaller lower priority load can be supplied with the available capacity, the control centre will bring the smaller lower priority load in. Thus, in normal operation (when no attack is present) the control centre supplies loads 1–5 and loads 6–9 are disconnected in islanding mode. By taking into consideration approximately 30 kW of system loss, the generation margin in this situation is about 40 kW.

The cyber infrastructure encompasses the sensors, $s_1, s_2, \ldots, s_{12}$ that collect measurements from various system points, communication infrastructure, 12 breaker

Table 2 Priority levels of system loads. Please note that percentages do not add up to 100% exactly due to rounding

Priority	*Node*	*Load power* (kW)	% *System load*
1	671	1155	33.3
2	675	843	24.3
3	632-671	200	5.77
4	692	170	4.92
5	611	170	4.92
6	646	230	6.6
7	645	170	4.9
8	634	400	11.5
9	652	128	3.7

actuator controls denoted with numbered hexagons and the control centre as shown in Figure 4. The sensor measurements can include active and reactive power, voltage and current phasors and on/off statuses of the switches. The control centre acts as the overall system *brain* to connect or disconnect the loads to and from the grid based on their priorities and available generation capacity. The control centre commands are sent to the switch actuators through communication links.

As in the previous test case, we model each DER, switch, load, capacity bank and cable as nodes in the electrical graph. Each sensor, breaker actuator and control centre are modelled as distinct nodes of the cyber grid. The overall electrical and cyber graphs are shown in Figure 5. A 'composite' cable node is used to represent the five physical cables connected to Nodes 632–671 of the test system. This has the effect of simplifying the graph while leading to the need for higher dimensional dynamical system equations at this node.

5 Results

A graph-theoretic formulation of distributed control is well-suited to this smart-grid representation because of the common mathematical treatment of cyber and physical components using graphs. It also enables the use of recent contributions to the field of *dynamical systems on graphs* within the multi-agent control systems

Figure 4 Single line diagram of the modified IEEE 13 node distribution test system (see online version for colours)

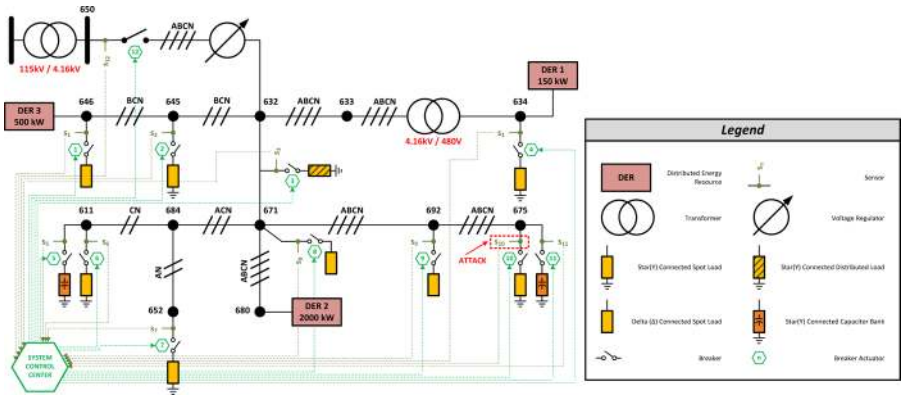
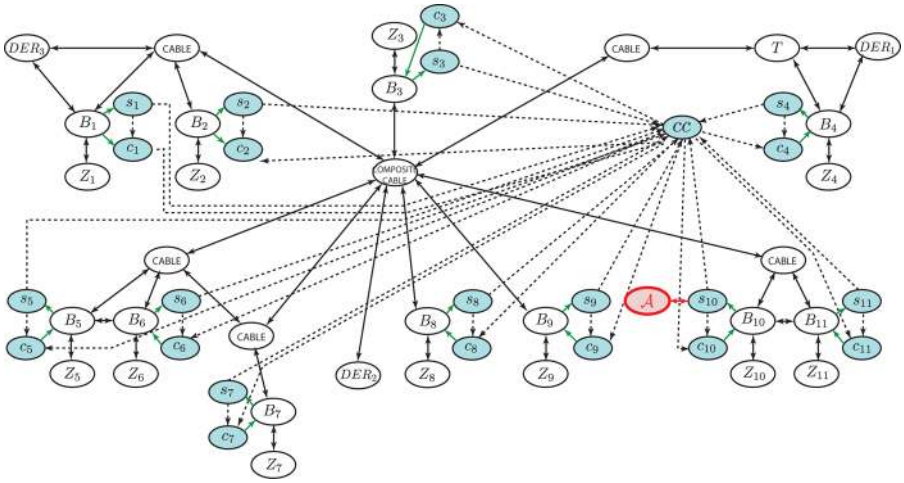


Figure 5 Electrical and cyber graphs for system of Figure 4 in islanding mode. Nodes are comprised of DERs, circuit breakers B_i, cables, a transformer T and loads/capacitor banks Z_i of the electrical network and a control centre cc, sensors s_i and actuator controls c_i of the cyber network. The 'composite cable' graph node represents the five physical cables connected to Nodes 632 and 671 of the IEEE 13 node distribution test system. Edges represent state dependencies for dynamical modelling. The cyber graph is distinguished with shaded nodes and dashed edges. Attack $\mathcal{A}$ targets the sensor s_{10} (see online version for colours)



community (Jadbabaie et al., 2003). Here, we present results pertaining to the graph and dynamical systems modelling of cause-effect relationships of a cyber attack on a test system.

5.1 Case study: single generator system

We first implement the graph-based dynamical system model of Figure 3, which models the system of Figure 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 Figure 6. 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 centre. An ideal transformer with conversion factor 15 is assumed. Both of these types of components represent trivial dynamical systems since they can be modelled 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 modelled 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 centre 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.

Figure 6 Dynamical system model for generator

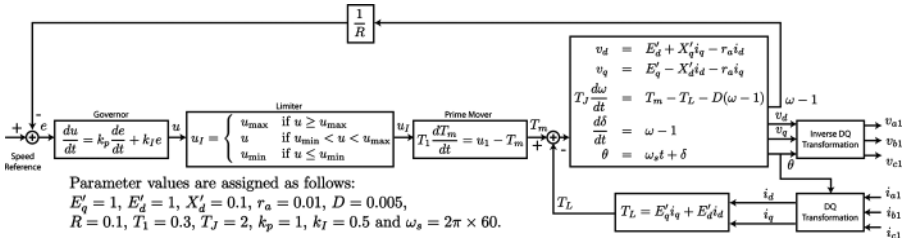
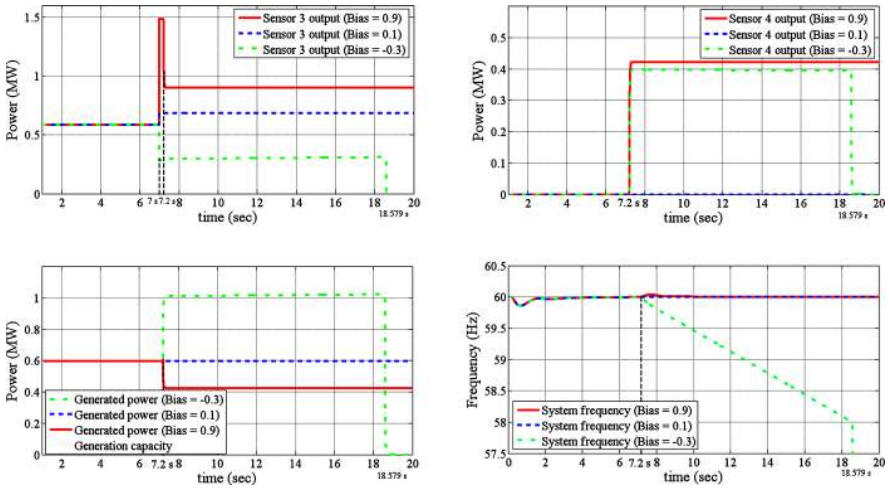


Figure 7 (a) [top-left] Output of s_3; (b) [top-right] output of s_4; (c) [bottom-left] total power generation and (d) [bottom-right] generator frequency (see online version for colours)



The graph-based dynamical system model of Figure 3 was simulated in MATLAB/Simulink using the fourth-order Runge-Kutta method with a step size of 0.001 seconds and simulation duration of 20 s. 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 Figure 2 s_3 is biased through cyber tampering. Thus, we can model the sensor output as:

$$s_3(t) = \mathcal{B}(t) + P_3(t) \tag{4}$$

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 modelling 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 centre will choose to shed Load 2 in favour 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 s) as it is the smaller rated load. In this study a cyber attack is applied at 7 s on s_3 by adding a bias $\mathcal{B}(t)$ such that it may effect load management by the control centre. A load management delay of 0.2 s is assumed.

Figure 7(a) shows the output of s_3. From 0 s to 7 s, Load 1 is being served thus, it is reading 0.6 MW as expected. At 7 s, the sensor is tampered and three different bias values of $\mathcal{B}(t) = 0.9, 0.1, -0.3$ are considered. Figure 7(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 Figure 7(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 Figure 7(d), this has the effect of decreasing generator frequency. At 18.579 s, 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.

5.2 Case study: 13 node distribution test system

The 13 node distribution test system is modelled in PSCAD® which is a transient power system simulation software. In this simulation, three DERs are integrated

into the system to supply power to the isolated power system. When more than one generator supplies power to a system, one larger synchronous generator should be set to isochronous mode to maintain the system frequency of 60 Hz. DER 1 consists of a wind turbine, a synchronous generator, and a power electronic interface. A PQ mode controller is implemented to keep the injected active power and reactive power at desired values. It is also assumed that the wind speed is 15 m/s, and the active and reactive power set points are 150 kW and 120 kVAr, respectively. DERs 2 and 3 are modelled as gas turbine generators with governor and exciter and the inertia constants (H) for these two generators are 1.03 s and 1 s, respectively. For DER 2, an isochronous governor model is used. Hence, the power output of this unit is regulated based on the load changes to maintain the system frequency at 60 Hz. In contrast, DER 3 works in droop mode and the power set point is 500 kW. The synchronous generator model in PSCAD is a very complex nonlinear dynamical system with more than 10 orders, which can help obtain more realistic simulation results. The threshold for the generator under-frequency relay is set to 58.8 Hz (2% mismatch from the normal value). Obviously, when the system frequency drops under 58.8 Hz, the generator will be tripped out.

For system cables, the PI model with non-symmetric self and mutual impedances is used. The transformer between nodes 633 and 634 with a conversion factor 8.67 is modelled with the PSCAD® non-ideal Y-Y transformer model including leakage reactance, which can be modelled using ordinary differential equations. All the loads in the system are constant loads (constant impedance loads, constant current loads, or constant power loads), which can be modelled using differential equations. Moreover, the constant impedance loads can be modelled using RL or RC circuits directly. Breakers are assumed to be ideal and controlled by a control signal from the control centre. As mentioned before, the control centre employs all of the sensor readings $(S_i, i = 1, 2, \ldots, 12)$ to decide to connect or disconnect system loads based on load priorities and available generation capacity. Then the control centre decision is sent to the actuators through the communication links. Note that the focus of this work is on the load management functionality of the control centre which is only one of many responsibilities of the control centre. It is also worth mentioning that as this work tries to show the effect of cyber attacks on the microgrid; thus, the microgrid is assumed to be in islanding mode, because it is more susceptible and fragile during islanding operation. The step size of the PSCAD simulation is 50 microseconds.

We consider three attack scenarios in which the sensor s_{10} at node 675 is compromised by adding a bias $\mathcal{B}(t) = -400, 150, 70$ kW to the measured active power. The attack occurs at $t = 0.5$ s. Thus after $t = 0.5$ s, the attack is modelled as:

$$s_{10}(t) = \mathcal{B}(t) + P_{10}(t) \tag{5}$$

where $\mathcal{B}(t) = -400, 150, 70$ and P_{10} represents the actual active power at Node 675.

Figure 8 considers the first case in which $\mathcal{B}(t) = -400$ and the attacker reduces the power measurement at s_{10} from 850 kW to 450 kW (Figure 8(a)) making the total measured system load decrease from 2575 kW to 2175 kW. This is shown in Figure 8(b). At this time the generation margin increases to 440 kW and with a processing delay of 0.5 s, the control centre decides to bring the next two higher priority loads in (i.e., Loads 6 and 7). By brining the loads at Nodes 645 and 646 in, the total connected load exceeds the total generation capacity by approximately 360 kW. Figure 8(c) shows how DER 2 and DER 3 are overloaded after $t = 1$ second. As a result, the frequency of the overloaded synchronous generators DER 2 and DER 3 starts to drop (Figure 8(d)). Finally, 0.83 s after the cyber attack, the frequencies of these two generators fall below 58.8 Hz and at this time, the under-frequency relays trip DER 2 and DER 3. As a consequence, the control centre disconnects all the loads and the remaining small DER (wind unit) and the system experiences a blackout.

The second and third cases corresponding to $\mathcal{B}(t) = 150, 70$, respectively, are presented in Figure 9. In the second case, a bias value of +150 kW is added to s_{10}. This corrupted sensor value initiates the control centre to disconnect the lowest priority served loads (this corresponds to the 170 kW load at node 611) at $t = 1$ s, as the generators seem to be overloaded by approximately 110 kW.

In the third case, a lower positive bias of +70 kW is considered. As in the previous case, to prevent generator overloading, the control centre disconnects the lowest priority served load (this corresponds to the 170 kW load at node 611) which results in an available generation capacity of approximately 140 kW. This capacity is sufficient to supply the 128 kW load connected to node 652. Therefore at $t = 1$ s, control centre disconnects the load at node 611 and connects the load at node 652. The effect of biased measurement on sensor s_{10} and on the total measured load, variations in power outputs of the DERs, and variations in DER frequencies for both cases are shown in Figure 9(a) and (d), respectively. Note that although the system does not experience a blackout in the second and third scenarios, these attacks result in unnecessary load shedding and serving a wrong load, respectively. Thus an incorrect prioritisation of the loads results.

6 Discussion

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

The complexity of processing is dependent on graph size (i.e., number of nodes), graph connectivity (related

Figure 8 (a) [top-left] Output of P_{10} and s_{10}; (b) [top-right] total system load; (c) [bottom-left] power generation of DERs and (d) [bottom-right] frequencies of DER2 and DER3 (see online version for colours)

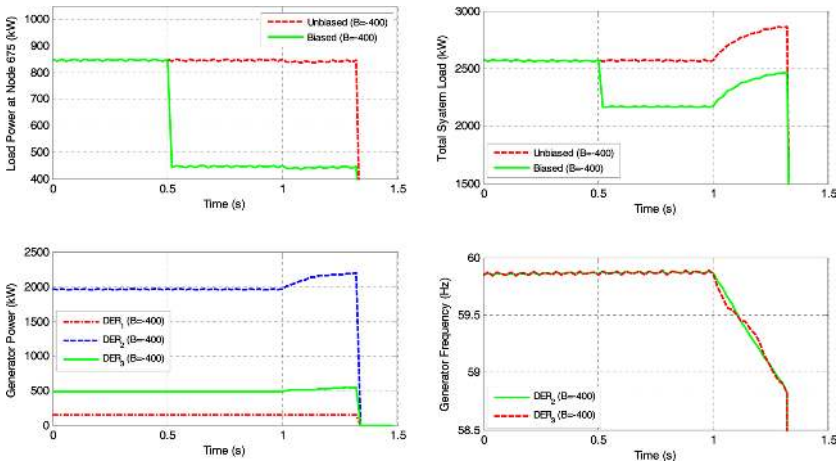
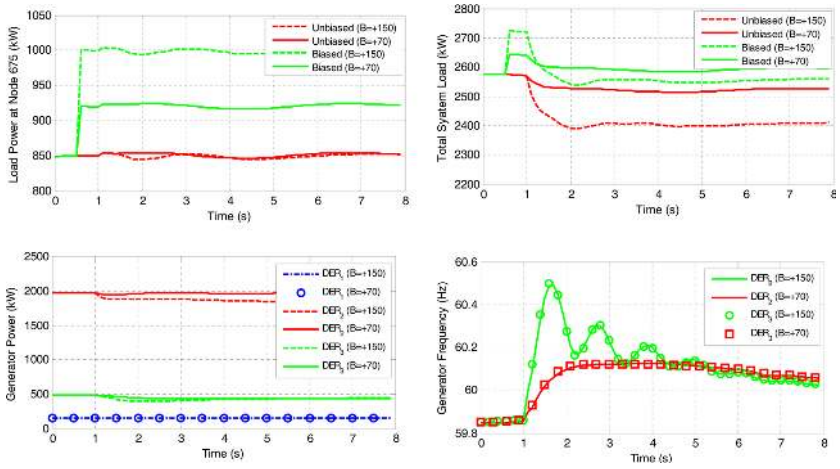


Figure 9 (a) [top-left] Output of P_{10} and s_{10}; (b) [top-right] total system load; (c) [bottom-left] power generation of DERs and (d) [bottom-right] frequencies of DER2 and DER3 (see online version for colours)



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' whereby each agent (instead of node) is modelled using dynamical system equations. Appropriate grouping of agents would allow necessary system behaviours to be characterised while approximating others that are not as salient to impact analysis. This method of grouping with effective modelling of dynamics is currently the focus of future work.

7 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 modelled within one framework allowing a single, but potentially powerful analysis approach. Thus, cause-effect relations for cyber-attacks are better managed for comprehensive impact modelling and analysis. The paradigm has attractive features particularly for realistic systems, where incorporating high-order behavioural models are necessary to assess dynamics, performance, stability and emergent properties. Results for two test systems are presented to show its potential to model cyber attack effects. 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.

Acknowledgements

Funding for this research was provided by the Norman Hackerman Advanced Research Program Project Number 000512-0111-2009 and by the US National Science Foundation under grant ECCS-1028246.

References

Amin, S.M. (2005) 'Energy infrastructure defense systems', *Proceedings of the IEEE*, Vol. 93, No. 5, pp.861–875.

Amin, S.M. (2008) 'For the good of the grid', *IEEE Power and Energy Magazine*, Vol. 6, No. 6, pp.48–59.

Boyer, W.F. and McBride, S.A. (2009) *Study of Security Attributes of Smart Grid Systems – Current Cyber Security Issues*, Report No. INL/EXT-09-15500, Iadaho National Laboratory, Idaho Falls, Idaho, USA.

Cárdenas, A.A., Amin, S. and Sastry, S. (2008a) 'Research challenges for the security of control systems', *Proc. 3rd USENIX Conference on Hot Topics in Security*, Berkeley, California, USA, p.6.

Cárdenas, A.A., Amin, S. and Sastry, S. (2008b) 'Secure control: towards survivable cyber-physical systems', *Proc. 28th International Conference on Distributed Computing Systems Workshops*, Beijing, China, pp.495–500.

Cárdenas, A.A., Roosta, T., Taban, G. and Sastry, S. (2008c) 'Cyber security basic defenses and attack trends', in Franceschetti, G. and Grossi, M. (Eds.): *Homeland Security Technology Challenges*, Artech House, Chapter 4, pp.73–101.

Committee, S. (2007) *IEEE Standard for Substation Intelligent Electronic Devices (IEDs)*, Standard IEEE Std 1686-2007, IEEE Power Enginering Society.

Conte de Leon, D., Alves-Foss, J., Krings, A. and Oman, P. (2002) 'Modeling complex control systems to identify remotely accessible devices vulnerable to cyber attack', *Proc. First Workshop on Scientific Aspects of Cyber Terrorism*, Washington DC.

Dagle, J. (2001) 'Vulnerability assessment activities', *Proc. Power Engineering Society Winter Meeting*, Vol. 1, Columbus, Ohio, pp.108–113.

Davis, C.M., Tate, J.E., Okhravi, H., Grier, C., Overbye, T.J. and Nicol, D. (2006) 'SCADA cyber security testbed development', *Proc. 38th North American Power Symposium*, Carbondale, IL, USA, pp.483–488.

Dawson, R., Boyd, C., Dawson, E. and Manuel Gonzàlez Nieto, J. (2006) 'SKMA – a key management architecture for SCADA systems', *Proc. Fourth Australasian Workshops on Grid Computing and E-Research*, Vol. 54, pp.183–192.

Depoy, J., Phelan, J., Sholander, P., Smith, B., Varnado, G.B. and Wyss, G. (2005) 'Risk assessment for physical and cyber attacks on critical infrastructures', *Proc. IEEE Military Communications Conference*, Vol. 3, Atlantic City, NJ , pp.1961–1969.

Dondossola, G., Garrone, F. and Szanto, J. (2009) 'Supporting cyber risk assessment of power control systems with experimental data', *Proc. IEEE Power Systems Conference and Exposition*, Seattle, Washington, USA, pp.1–3.

Dudenhoeffer, D.D., Permann, M.R. and Manic, M. (2006) 'CIMS: a framework for infrastructure interdependency modeling and analysis', *Proc. 38th Winter Simulation Conference*, Monterey, California, pp.478–485.

Dudenhoeffer, D.D., Permann, M.R., Woolsey, S., Timpany, R., Miller, C., McDermott, A. and Manic, M. (2007) 'Interdependency modeling and emergency response', *Proc. 2007 Summer Computer Simulation Conference*, San Diego, California, pp.1230–1237.

Eberle, W. and Holder, L. (2009) 'Insider threat detection using graph-based approaches', *Proc. Cybersecurity Applications and Technology Conference for Homeland Security*, Washington DC, pp.237–241.

Edwards, D., Srivastava, S.K., Cartes, D.A., Simmons, S. and Wilde, N. (2007) 'Implementation and validation of a mult-level security model architecture', *Proc. International Conference on Intelligent Systems Applications to Power Systems*, Toki Messe, Niigata, Japan, pp.1–4.

Ekstedt, M. and Sommestad, T. (2009) 'Enterprise architecture models for cyber security analysis', *Proc. IEEE Power Systems Conference and Exposition*, Seattle, Washington, USA, pp.1–6.

Endoh, H. (2008) 'Analyzing aspects of cyber security standards for M&CS', *Proc. SICE Annual Conference*, Tokyo, Japan, pp.1478–1481.

Ericsoon, G.N. (2009) '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.

Falk, H. (2008) 'Securing IEC 61850', *Proc. IEEE Power and Energy Society General Meeting – Conversion and Delivery of Electrical Energy in the 21st Century*, Pittsburgh, Pennsylvania, USA, pp.1–3.

Feng, X., Zourntos, T. and Butler-Purry, K.L. (2010) 'Dynamic load management for NG IPS ships', *Proc. IEEE Power Engineering Society General Meeting*, Minneapolis, Minnesota.

Giani, A., Karsai, G., Roosta, T., Shah, A., Sinopoli, B. and Wiley, J. (2008) 'A testbed for secure and robust SCADA systems', *SIGBED Review*, Vol. 5, No. 2, Article No. 4.

Hadeli, H., Schierholz, R., Braendle, M. and Tuduce, C. (2009) 'Generating configuration for missing traffic detector and security measures in industrial control systems based on the system description files', *Proc. IEEE Conference on Technologies for Homeland Security*, Waltham, Massachusetts, USA, pp.503–510.

HadjSaid, N., Tranchita, C., Rozel, B., Viziteu, M. and Caire, R. (2009) 'Modeling cyber and physical interdependencies – application in ICT and power grids', *Proc. IEEE Power Systems Conference and Exposition*, Seattle, Washington, USA, pp.1–6.

Jadbabaie, A., Lin, J. and Morse, A. S. (2003) 'Coordination of groups of mobile autonomous agents using nearest neighbor rules', *Automatic Control, IEEE Transactions on*, Vol. 48, No. 6, pp.988–1001.

Jiaxi, Y., Anjia, M. and Zhizhong, G. (2006) 'Vulnerability assessment of cyber security in power industry', *Proc. IEEE Power Systems Conference and Exposition*, Atlanta, Georgia, pp.2200–2205.

Liu, C-C., Ten, C-W. and Govindarasu, M. (2009) 'Cybersecurity of SCADA systems: Vulnerability assessment and mitigation', *Proc. IEEE Power Systems Conference and Exposition*, Seattle, Washington, USA, pp.1–3.

Madani, V. and Witham, T. (2008) 'Strategies for protection and control standardization and integrated data management applications', *Proc. IEEE/PES Transmission and Distribution Conference and Exposition*, Chicago, Illinois, USA, pp.1–6.

Mander, T., Nabhani, F., Wang, L. and Cheung, R. (2007) 'Integrated network security protocol layer for open-access power distribution systems', *Proc. IEEE Power Engineering Society General Meeting*, Tampa, Florida, USA, pp.1–8.

McDaniel, P. and Smith, S.W. (2009) 'Security and privacy challenges in the smart grid', *IEEE Security and Privacy*, Vol. 7, No. 3, pp.75–77.

McDonald, R. (2008) 'New considerations for security compliance, reliability and business continuity', *Proc. IEEE Rural Electric Power Conference*, Charleston, South Carolina, pp.B1–B1–7.

McMillin, B. (2009) 'Complexities of information security in cyber-physical power systems', *Proc. IEEE Power Systems Conference and Exposition*, Phoenix, Arizona, pp.1–2.

McQueen, M.A., Boyer, W.F., Flynn, M.A. and Beitel, G.A. (2006) 'Quantitative cyber risk reduction estimation methodology for small SCADA control system', *Proc. 39th Annual Hawaii International Conference on Systems Sciences*, Kauai, Hawaii, USA, Vol. 9, pp.226–236.

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

Pietre-Cambacedes, L., Chalhoub, C. and Cleveland, F. (2007) *IEC TC57 WG15 – Cyber Security Standards for the Power Systems*, Report No. D2-02-C02, CIGRÉ Study Committee D2: Information Systems and Telecommunications.

Piètre-Cambacédès, L., Kropp, T., Weiss, J. and Pellizzonni, R. (2008) 'Cybersecurity standards for the electric power industry – a "survival kit"', *Proc. CIGRÉ Paris Session*, Paper D2–213.

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

Sheng, S., Chan, W.L., Li, K.K., Xianzhong, D. and Xiangjun, Z. (2007) 'Context information-based cyber security defense of protection system', *IEEE Transactions on Power Delivery*, Vol. 22, No. 3, pp.1477–1481.

Stamp, J., McIntyre, A. and Ricardson, B. (2009) 'Reliability impacts from cyber attack on electric power systems', *Proc. IEEE Power Systems Conference and Exposition*, Seattle, Washington, USA, pp.1–8.

Tang, H. and McMillin, B. (2008) 'Security property violation in CPS through timing', *Proc. 28th International Conference on Distributed Computing Systems Workshops*, Beijing, China, pp.519–524.

Tan, H. (2007) *Security Analysis of a Cyber-Physical System*, Master's Thesis, University of Missouri-Rolla, Rolla, Missouri, USA.

Watts, D. (2003) 'Security and vulnerability in electric power systems', *Proc. 35th North American Power Symposium*, Rolla, Missouri, pp.559–566.

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