A Game-Theoretic Approach to Modeling Attacks and Defenses of Smart Grids at Three Levels

December 28, 2016

Abstract

As optimization, user capabilities, and data-taking abilities are incorporated into next-generation power grids, or smart grids, they face cyber threats. The traditional electrical grid could only be damaged by physical attacks; however the smart grid can suffer remote/cyber attacks, which have not been studied extensively in the literature. The electrical grid forms the backbone of the modern society and its security has significant implications in military settings. This paper applies game theory to model three-levels (power plants, transmission, and distribution networks) of defenses and attacks in smart grid network security. We characterize both the attacker and the defender (who interact at three network levels: distribution, transmission, and power plants) best responses and equilibrium strategies. We find that the defender's best response is not only a function of direct attacks but also of the spread from connected networks. Sensitivity analyses of the equilibrium strategies show that when success probability of an attack against power plants reaches a threshold, the defender increases defending efforts for power plants. In contrast, the attack effort at all levels is not affected by this probability. This paper provides some novel insights to modeling and analyzing the emerging threats to the growing smart grid networks.

Keywords: Smart grid, game theory, cyber-physical security, decision analysis

INTRODUCTION

Economically and efficiently producing electricity is an issue of global concern. As societies become increasingly reliant on modern technologies, concerns about having enough energy become more prevalent (Garrity, 2008). A smart electric grid is designed for this purpose for optimal power and resource distribution with increased automation, real-time data-taking capabilities, integrated new smart technologies and appliances, enhanced electricity storage, and peak saving technologies (Wei, 2010; Bidram and Davoudi, 2012; Sorebo and Echols, 2012).

However, the integration of cyber components and "smart" technologies also significantly increases the vulnerably to remote/cyber attacks. Particularly, interconnecting among different layers in a large network enables globe control over individual electricity consumers instead of isolated control and presents advantages such as improved coordination of electricity usage with risk of serious potential cascading damage effects. The United States Department of Defense is among the biggest energy consumers in the world and the single largest energy consumer in the U.S. (Reitenbach, 2012). Modern terrorist groups such as ISIS and al Qaeda seem capable of launching a main cyber attack against the West (Paganini, 2014), which could have devastating impacts on the military. Therefore, cyber-security issue has be extensively studied to support the development of smart grids (Carin et al., 2008; Gu, 2008; Yan et al., 2012; Wang and Lu, 2013). In 2009, evidence was found that foreign spies had already hacked into parts of the United States power grid and scouted out much of its structure; no direct damage was caused but the stolen information could be the difference between success and failure of a large-scale cyber-attack (Gorman, 2009). Metke and Ekl (2010) provide a review of security technologies developed for smart grids. Defense strategies for smart grids are likely to be different than those for traditional grids. There has been a lot of valuable research devoted to analyzing security of traditional electric grid against intelligent and delicate attacks (Salmeron et al., 2004, 2009). Many papers consider physical attacks where some segments of electricity flow could be interdicted by the attacker with the goal of identifying the optimal or semi-optimal defense strategies (e.g., Bier at al., 2007). In order

to provide insights into the interactions in defending smart grids, this paper models the complex strategic interactions of a defender and an attacker within the context of the smart grid with game theory. To illustrate the game-theoretic model, we simulate optimal attack and defense strategies on three separate levels: power plants, transmission, and distribution networks. In opposition to these parties will be the major threats to the smart grid including smart thieves/stalkers, hackers, and cyber warfare.

The strategic model designed and solved will offer quantitative insights for protecting and designing the smart grid to be resilient against cyber threats. Zahedi (2011) provides a systems model to show the interconnected nature, the topography and benefits of the smart grid, but does not address the inherent risks. Chen et al. (2011) construct nested sets of petri nets to model large-scale simultaneous attacks against smart grid in order to avoid the impracticability of creating a large petri net at once and to allow distributed knowledge of cyber-physical attacks. Petri nets show an advantage over traditional attack trees in handling simultaneous attacks. However, they also state that this method requires currently unavailable data, which could be obtained from experts generating many different low-level petri nets and combining them to create a high-level petri net. Salve et al. (2015) provide a comprehensive review to examine current research in issues of cyber security in smart grids.

Game theory has been widely used in capturing the strategic interactions between the attacker and the defender on critical infrastructure protection (Bier et al., 2007; Zhuang and Bier, 2007; Dighe et al., 2009; Golalikhani and Zhuang, 2011; Hausken and Zhuang, 2011; Zhuang and Bier, 2011; Levitin and Hausken, 2012; Shan and Zhuang, 2013a, b; Shan and Zhuang, 2014a,b). Salmeron et al. (2004) evaluate vulnerability of electrical grids by studying bilevel mathematical models and algorithms. Later on, Salmeron et al. (2009) use Benders decomposition to solve this bilevel optimization problem to identify the optimal interdiction plan. Tas and Bier (2014, 2015) focus on vulnerability of power grid to cascading failures when facing an intelligent attacker. To increase the efficiency in identifying good interdiction plans, Bier et al. (2007) proposes a simple and efficient method based on greedy algorithm. Yuan et al. (2014) propose a Column-and-Constraint

Generation algorithm to efficiently solve a defender-attacker-defender model. Roy et al. (2010) discuss the different variations of games including static and dynamic games and how to apply them in modeling network security. Our research is an implementation of the concepts in Roy et al. (2010) by using game theory to model the cyber network of smart grids. Game theory offers a practical way to model the strategic interactions between attacker and defender of smart grids with available data and potentially bridge the gap between theory and practice on smart grid defenses. On cyber networks, Gu et al. (2008) offer an interesting model for defending a sensor network, which provides critical information about its environment such as positions of hostile targets, against a search-based attack. This model offers up an interesting defense strategy of sacrificing nodes to detect a hidden attacker, allowing the defender to take actions against them. Bursztein et al. (2007) construct a game to test a networks resilience against both attacks and internal faults. They suggest the construction of a model that describes dependencies, responses, and time.

Multiple levels of attacks and defenses have been studied (Levitin, 2003; Haphuriwat and Bier, 2011; Levitin and Hausken, 2012; Hausken, 2013 & 2014; Levitin et al., 2013 & 2014). Cox (2009) and Levitin et al. (2012) investigate attacks and survival of networks. Cascading failures on the network with interdependent components have been examined by Lakdawalla and Zanjani (2002), Kunreuther and Heal (2003), and Hausken (2006).

NETWORK TOPOLOGY

The smart grid is a large network with many different interconnected components: Figure 1 shows a schematic diagram by highlighting its essential form (Flick and Morehouse, 2011). Power is generated by power plants and transmitted and distributed to the consumers' households. Advanced Metering Infrastructure (AMI) is the key network structure underlying a smart grid, and has smart meters and other smart devices as its main components (Sorebo 2012). The main function of AMI is to record real-time power usage that is transmitted back to the utility companies (Sorebo 2012). Using this

information the utility companies can monitor and control power generation and transmission according to real-time need. We acknowledge that network topology might not be necessarily an adequate way to characterize the vulnerability and/or performance of an electricity network. However, network topology provides a great visualization tool to understand the interconnected nature of electricity networks. Besides, electricity flow, especially of a smart grid, would be too complicated to model and yield valuable insights. The simple topology adopted here represents a first attempt in modeling cyber security of complicated smart grid networks.

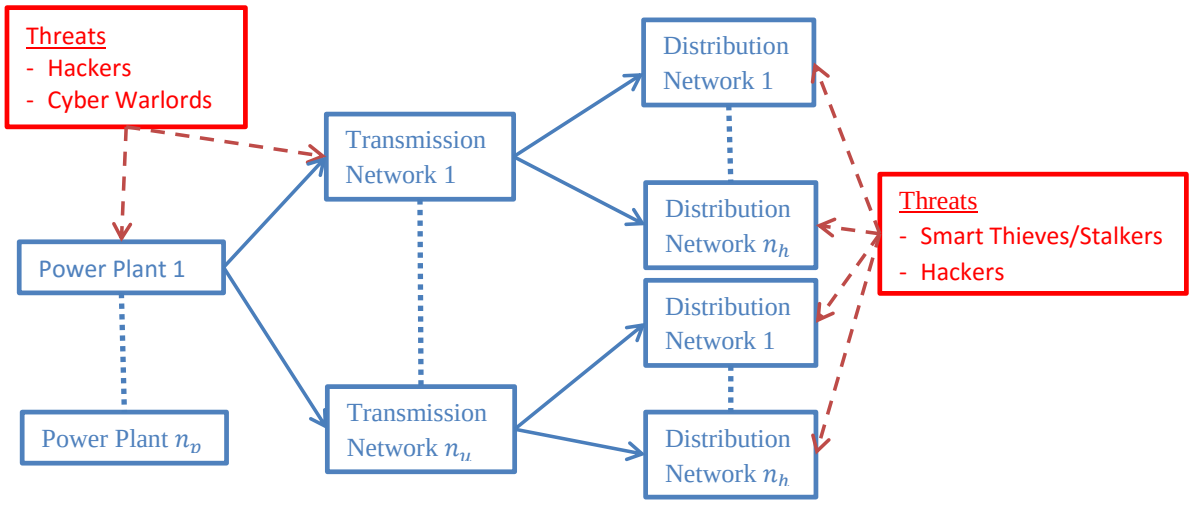

Figure 1: Networks schematic highlighting threats to power plants, transmissions, and distribution networks.

Threats and Attacks Types

With the incorporation of new technologies into the smart grid, new cyber threats must be addressed to have a secure grid, such as from smart thieves or stalkers. With AMI large amounts of personal information such as real-time power usage will be collected. This information if obtained by a smart thief or stalker could be used to map out a potential victim's entire life allowing the thief or stalker to better plan out potential crimes.

Malicious motives for attacking the grid are diverse but fit into two main categories: personal gain and political activism, known as hacktivism (Krapp 2005). Hackers attacking the grid for personal gains will use the addition of malware to the grid software in

attempts to gain money, power, or vengeance. For example, by introducing ransomware (a specific type of malware that holds systems hostage for a ransom), a hacker could hold a consumer's electricity hostage until they were paid off (Sorebo 2012). These attacks can be very subtle with an example being the RansomSMS-AH, which blocks Internet access until the victim sends a text message to a premium rate SMS phone number generating revenue for the hacker. A similar attack to the electronic database at Hollywood Presbysterian Medical Center blocks access of healthcare providers to patient data (Dobuzinskis 2005). They can also be unsubtle and as simple as a note demanding pay-off for the reinstatement of power. By attacking the smart grid, activists affect a massive amount of people and would draw a large amount of public attention to their cause. For this reason the smart grid makes a very appealing target to activist groups. Non-malicious attacks against the grid normally come from hackers trying to prove their skills to themselves and the larger hacking community.

Crippling a nation's infrastructure will greatly hinder its ability to operate in a war scenario. As a result the smart grid will make a likely target for foreign enemies trying to remotely damage the country. This has already occurred in some Middle East countries with stuxnet and flame both significantly damaging Iranian nuclear infrastructure (Faranz and Sonne, 2012). With the development of the smart grid, the avenues of attack and potential for spread greatly increase.

NOTATIONS, ASSUMPTIONS, AND MODEL

Notations

For simplicity, this paper assumes that there is one attacker, or threat, and that the intent of the attacker is to inflict the maximal damage at minimal costs, while the defender intents to maximize protection at minimal costs. The variables, functions, and parameters used throughout the paper are listed in Table 1.

As illustrated in Figure 1, we focus on three types of networks (power plant, transmission, and distribution) in the smart grid and each network consists of different nodes.

Table 1: Notations that are used in this paper

Variable or Parameter	Interpretation
Decision Variables	
$a_p = 0, 1, ..., n_p$	number of nodes in network of type p attacked
$a_u = 0, 1, ..., n_u$	number of nodes in network of type u attacked
$a_h = 0, 1, ..., n_h$	number of nodes in network of type h attacked
$d_p = 0, 1, ..., n_p$	number of nodes in network of type p defended
$d_u = 0, 1, ..., n_u$	number of nodes in network of type u defended
$d_h = 0, 1, ..., n_h$	number of nodes in network of type h defended
Function Definition	
$P_k(a_k, d_k)$	Probability of network of type k operating
$I_{a_k > d_k}$	Indicator function of the event that attacks are more intense than defense of network of type k
U_D	Defender's utility function
U_A	Attacker's utility function
System Parameter	
$k \in \{p, u, h\}$	Network type
p	A power plant, parent Network
u	A transmission, child Network
h	A distribution, grandchild Network
n_k	Number of nodes in network of type k
m_k	Minimal number of operating nodes required for functioning of network of type k
s_k	Number of successful attacks against nodes in network of type k
p_k	Success probability of attacking each node within a network of type k
V_k	Defender loss from breakdown of a network of type k
v_k	Attacker gain from breakdown of a network of type k
g_{kj}	Probability that damage caused to network of type k is spread to network of type j. If $k = p$, $j = u$; if $k = u$, $j = h$
C_k	Unit cost (per node) to defend nodes in network of type k
c_k	Unit cost (per node) to attack nodes in network of type k

In particular, we assume that there are n_k nodes at each of the three layers of networks, where $k = p$ (power plant), u (transmission) or h (distribution). In order to specify the unique relationships between networks characterized by the one-direction effect, we refer to the network of power plants as a parent network to the network of transmissions, which itself is a parent network to the distribution network (grandchild). That is, electricity was generated/distributed by a parent network to its child network. As a result, the shutdown of a parent network will most likely affect the electricity supply to its child network. Due to the limitation of current technologies in electricity distribution, selling electricity back from a child network to a parent network is not widely spread in practice and thus breakdown of a distribution network is not expected to affect its parent network too much. Conversely, the distribution network is named as a child network to the network of transmissions, which in turn is a child network to the network of power plants.

Table 1 lists the decision variables of the attacker and the defender. We assume that each node/component of a network is a potential target to attack or defend. Note that as a first step toward understanding the defense of a smart grid, we assume that the attacker's decision is not on where to attack but instead on the efforts to invest, which translates to how many nodes to attack. Similarly, the defender decides on how much efforts to devote to defense. Table 1 contains four functions studied in the paper: 1) probability of network of type k operating is denoted by $P_k(a_k, d_k)$, which is a key to both the attacker's and the defender's objective functions. Basically, the attacker minimizes the operating probabilities of each network weighted by their valuations while the defender maximizes those probabilities; 2) indicator function of the event that the attacks are more intense than defense of network of type k is represented by $I_{a_k > d_k}$, whose main function is to determine whether or not the attacks on a parent network is sufficiently intense to affect its child network; and 3) utility functions of the defender and the attacker are denoted by U_D and U_A. Note that the cascading failure studied here is different from cascading effects considered for traditional electricity grid (e.g., Tas and Bier, 2014). In Tas and Bier (2014), cascading failures are due to power flow interdiction

affecting the downstream power flow. In contrast, we are considering that some critical nodes of a parent network under cyber-attacks without adequate defense affects other critical nodes of the child network. It could be due to communication failures or other mechanisms than power flow interdiction.

Finally, system parameters are listed in Table 1: network type is denoted by k, which could be p (power plants), u (transmissions), or h (a distribution network). We have n_k as the number of nodes in network k and m_k as the minimal number of operating nodes in network k in order for that network to function. Number of successfully attacked nodes in network k is labeled as s_k while p_k represents the success probability of an individual attack on a node. Defender's loss (attacker's gain) from breakdown of network k is denoted by V_k (v_k). We have g_{kj} as the probability that damage to network k is spread to its child network j, which only occurs if attacks are more intense than defenses. Unit cost to defend (attack) nodes in network k is C_k (c_k). Note that when a network breaks down, its main functionality in supplying critical loads is impaired even though there might be electricity flow in parts of the network. As a first step toward addressing this critical issue, we are only focusing on complete or 100% failures instead of partial failures.

Modeling Concepts and Assumptions

The defender's objective is to maximize the probabilities of each network functioning weighted by their corresponding consequences of breakdown to the defender within its budget limit since a breakdown of a network of power plants is probably more catastrophic than that of a distribution network, which impacts much less individuals. On the other hand, the attacker intents to maximize the breakdown probability of each network, which is weighted by the attacker's valuation of the breakdown, without formidable cost. There are n_k nodes at each of the three layers of networks, where $k \in \{p,u,h\}$ and the defense (attack) efforts are between 0 and n_k. We construct the model based on the following assumptions: first, attacks on the parent network with intensity higher than defenses will negatively affect its child network (e.g., intense attacks on transmission network are

likely to affect the distribution network). Second, attacks on the child network will not affect its parent network (e.g., attacks on utilities are not expected to much affect power generation). The first two model constructs characterize the one-directional relationship of the connections between parent and child networks. This is consistent with the observation that in most of the cases, failures in transmission lines cause power outages to all the downstream circuits. Third, attacks and defenses are focused on each node (not its connections). Due to redundancy in the grid, attacks on the connections are expected to cause much less damage than attacks on the nodes. Fourth, the attacker's decision is on how much attack efforts to devote to each network in each network but not on which nodes to attack. The probability of a network functioning normally as a function of attack and defense efforts are explained in details later in the paper. Note the defender's efforts are not physical protection of critical nodes but efforts in updating cyber-security policies, training security personnel and so on. On the other hand, the attacker's efforts are less known but might involve providing resources for cyber-attacks, opportunity costs of hacking attempts against targeted network and so on. Fifth, the probability of breakdown is a function of both attack and defense efforts and independent between different nodes of the same network.

We assume that a minimal of $d_k - a_k \geq m_k + 1$ components is required for network k to function. That is, a node operates normally if the defender invests more than the sum of the attacker efforts and a maintained level specific to that network. Note that every node in this study is assumed to be a critical node. Defense effort can be perceived as including maintenance effort and an insufficient amount could cause the network to fail without attacks. To relax the first assumption, we assume that if attacks were more intense than the defense at a parent network, with a certain probability the functioning of the child network would also be affected. For example, we assume that if a network of power plants is affected, with probability g_{pu}, the network of transmissions would also fail. Note that this spread effect is one directional and only from parent networks to child networks. As a first step toward solving this emerging and novel problem, the tenth assumption is that both the defender and the attacker have complete information about the structure of the

game, such as target valuations, costs, and the success probability of attacking each node. Moreover, we also assume that to both the defender and attacker power plants have a higher value to the defender than transmissions and distribution networks and that utility companies have a higher value than distribution networks. This is represented for the defender and the attacker respectively as follows,

$$V_p > V_u > V_h \text{ and } v_p > v_u > v_h \tag{1}$$

From the defender's perspective, securing the smart grid is the ultimate goal since its normal operations can bring so many societal and economic benefits. To increase security is arguably equivalent to decreasing the probability of breakdown of its component networks. The probability of a network functioning normally as a function of attack and defense efforts are explained in details later in the paper. Briefly, both the defender and the attacker are assumed to be able to influence the probability of network breakdown (i.e., the network malfunctions and could not deliver sufficient electricity to critical loads). The defender's objective is to maximize the probabilities of each network functioning weighted by their corresponding consequences of breakdown to the defender. The defender's objective function values is also penalized by the defense cost. Basically, the defender is trading off between security benefits and defense costs. In contrast, while the true objective of the attacker are usually unknown to the defender and could deviate from the assumed one, we adopt a reasonable assumption that the attacker intents to maximize the breakdown probability of each network, which is weighted by the attacker's valuation of the breakdown, with formidable cost. We formulate the optimization problem as unconstrained; however, the unit costs of defending (attacking) would prevent unlimited defense (attack) efforts. Therefore, at optimality, we expect the defender (attacker) to balance between defending (attacking) to increase functioning (breakdown) probability of each network and defense (attack) costs.

Objective Functions

To operationalize the objective of defending the smart grid, the defender's objective function is as follows:

$$U_d(a_p, a_u, a_h; d_p, d_u, d_h) =$$

$$\max_{d_p, d_u, d_h} \quad \underbrace{P_p V_p + P_u V_u + P_h V_h}_{\text{[Defender gain for network operation]}} \quad - \underbrace{I_{a_p > d_p} g_{pu} V_u - I_{a_u > du} g_{uh} V_h}_{\text{[Spread of network failure]}} - \underbrace{C_p d_p - C_u d_u - C_h d_h}_{\text{[Defense cost]}} \tag{2}$$

where $d_p = 0, ..., n_p, d_u = 0, ..., n_u, d_h = 0, ..., n_h$.

The defender's objective is to maximize the operating probability of three different networks of the grid, while minimizing the spread of damages weighted by its valuation of each network and cost of defense by deciding upon amount of defense units to be deployed among the three types of networks. In particular, the defender's objective function contains P_p, P_u, P_h as the probability that networks of power plants, transmissions and distribution functions normally, which are weighted by their importance to the defender (or the smart grid). We use V_p, V_u, and V_h to represent the importance of the three types of network. Moreover, we assume that there could be spread of attack impacts from parent network to child network. Specifically, if the attack is more intense than defense as the network of power plants (i.e., $I_{a_p > d_p} = 1$), operation of its child network (transmissions) will be negatively impacted with probability g_{pu}, which is again weighted by the importance of network of transmissions V_u. Similarly, if the attack is more intense than defense at the network of transmissions (i.e., $I_{a_u > d_u} = 1$), operation of its child network (distribution) will be negatively impacted with probability g_{uh} as weighted by the importance of distribution network V_h. Finally, if the defender invests d_p, d_u, d_h on the three networks, the total cost is the sum of their unit cost multiplied by their efforts ($C_p d_p + C_u d_u + C_h d_h$), which the defender tries to minimize.

The attacker's objective function is as follows:

$$U_a(a_p, a_u, a_h; d_p, d_u, d_h) =$$

$$\max_{a_p, a_u, a_h} \underbrace{(1-P_p)v_p + (1-P_u)v_u + (1-P_h)v_h}_{\text{[Attacker gain from network failure]}} + \underbrace{I_{a_p > d_p} g_{pu} v_u + I_{a_u > d_u} g_{uh} v_h}_{\text{[Spread of network failure]}} - \underbrace{c_p a_p - c_u a_u - c_h a_h)}_{\text{[Attack cost]}} \tag{3}$$

where $\quad a_p = 0, ..., n_p, a_u = 0, ..., n_u, a_h = 0, ..., n_h.$

The attacker's objective is to maximize the breakdown probability of three different networks of the grid and the spread of damages weighted by its valuation of each network, while minimizing cost of attacks by deciding upon amount of attack units to be applied against the three types of networks. In particular, the breakdown probabilities of the three networks are represented by $(1-P_p)$, $(1-P_u)$, and $(1-P_h)$, which are weighted by their relative significance to the attacker (v_p, v_u, and v_h). The attacker also intents to have a significant spread from attacks on a parent network to operation of its child network, which could happen if the attacks are more intense than the defense for a given network (i.e., $I_{a_p > d_p} = I_{a_u > d_u} = 1$). Therefore, the attacker also wants to maximize the spread probabilities (g_{pu} and g_{uh}) weighted by their valuations to the attacker (v_u and v_h). Finally, the attacker's objective also contains cost, which is the sum of attack costs on each of the three networks ($C_p d_p + C_u d_u + C_h d_h$).

GAME-THEORETIC MODEL FORMULATION

We first study the probability of a network of type k functioning under attacks. The attacker decides upon how many nodes of each network type to attack (a_k, where $k = p, u,$ and h), while the defender decides upon how many nodes of each network type to defend (d_k, where $k = p, u,$ and h). The probability of each network operating is modeled based upon a binomial random variable, which is the number of successful attacks. That is, the probability describes a binomial distribution, where the probability of success is the probability of a successful attack on a node of network k (p_k). In particular, we have

$$P_k(a_k, d_k) = P_k(s_k \geq m_k + 1 | d_k, a_k) = \begin{cases} 0 & \text{if } 0 \leq d_k \leq m_k \\ \sum_{s_k=0}^{d_k - m_k + 1} \binom{a_k}{s_k} {p_k}^{s_k} (1-p_k)^{a_k - s_k} & \text{if } m_k \leq d_k < a_k + m_k \\ 1 & \text{if } d_k \geq a_k + m_k \end{cases} \tag{4}$$

In other words, Equation (4) states that the probability of network k functioning equals the probability that the number of successful attacks is greater than the minimum number of operating nodes required for the functioning of network k (m_k) given certain defense and attack efforts. Implicitly, we assume that defense efforts will cancel the same amount of attack efforts. We choose binomial distributions to model the probability of network operating because binomial distributions are distributions of the number of successes in a sequence of Bernoulli trials. Since the normal operation of each network can be reasonably perceived as equivalent to the normal operation of at least the minimal number of critical nodes required for maintenance. The operation of each node is stochastically determined by the success probability of an attack and can be considered as independent bernoulli trials.

The right-hand-side of Equation (5) lists the three possible values for that probability: if defense efforts are less than or equal to m_k, the network will break down since no sufficient maintainance/defense efforts have been invested; if defense efforts are greater than the attack efforts (a_k) plus m_k, the network will function normally since sufficient defense efforts are in place and cancel the amount of attack efforts; and if defense efforts are in between, the outcome of the attacks in terms of breaking down the network follows a binomial distribution. For example, the minimal required number of critical nodes for the network of transmission, which has six nodes, are two and the attacker attacks three nodes of this network. If the defense on this network is more than five nodes, the network will operate normally since the defense efforts is more than the sum of both attack efforts and maintenance requirement. If the defense on this network is between two and five nodes, the network might normally operate with a probability of the cumulative sums of probability that no node will fail, probability that one node will fail, probability that two nodes will fail and probability that three nodes will fail and can be obtained by assuming the number of successful attacks (or equivalently, number of failed nodes) follows a binomial distribution with parameter equaling the probability of a successful against a single node. Finally, if the defense is less than two nodes, this network will fail even without attacks. In other words, defense efforts can be also be perceived as maintenance efforts and must meet the minimal requirement for the network to operate.

We also study a sequential game where the defender moves first. We first define the best responses of both players.

Definition 1 Attacker's strategy $(\hat{a}_p, \hat{a}_u, \hat{a}_h)$ is a best response to defender's strategy (d_p, d_u, d_h)

if and only if

$$\hat{a}_p, \hat{a}_u, \hat{a}_h = \underset{a_p, a_u, a_h}{\operatorname{argmax}} U_a(a_p, a_u, a_h; d_p, d_u, d_h)$$

Definition 2 *Similarly, defender's strategy* $(\hat{d}_p, \hat{d}_u, \hat{d}_h)$ *is a best response to attacker's strategy* (a_p, a_u, a_h) *if and only if*

$$\hat{d}_p, \hat{d}_u, \hat{d}_h = \underset{d_p, d_u, d_h}{\operatorname{argmax}} U_d(a_p, a_u, a_h; d_p, d_u, d_h)$$

Then we define a Subgame perfect Nash equilibrium.

Definition 3 *A pair of defender's and attacker's strategies* $(d_p^*, d_u^*, d_h^*;\ \hat{a}_p, \hat{a}_u, \hat{a}_h)$ *is called a subgame perfect Nash equilibrium if and only if*

$$\hat{a}_p, \hat{a}_u, \hat{a}_h = \underset{a_p, a_u, a_h}{\operatorname{argmax}} U_a(a_p, a_u, a_h; d_p^*, d_u^*, d_h^*)$$

$$d_p^*, d_u^*, d_h^* = \underset{d_p, d_u, d_h}{\operatorname{argmax}} U_d(\hat{a}_p, \hat{a}_u, \hat{a}_h; d_p^*, d_u^*, d_h^*)$$

NUMERICAL ILLUSTRATIONS

In the following subsections, we study the attacker's best response assuming that he can choose $a_k = \{0, 1, \ldots, n_k\}$, where $k = p$, u, or h in response to defender's decision ($d_k = \{0, 1, \ldots, n_k\}$, where $k = p$, u, or h). In addition, we study the defender's best response assuming she can choose $d_k = \{0, 1, \ldots, n_k\}$, where $k = p, u$, or h in response to the attacker's decision ($a_k = \{0, 1, \ldots, n_k\}$, where $k = p$, u, or h). Finally, we illustrates equilibrium strategies of both the attacker and the defender within the context of a sequential game where the defender moves first by deciding on resource allocations and also conduct sensitivity analysis to examine the effects of key parameters on equilibriums.

For the numerical illustrations, we used the baseline parameter values listed in Table 2 to solve the attacker's and defender's best response functions.

Attacker's Best Response

Figures 2(a)-(c) show the attacker's best responses at the network fronts of power plants, transmissions, and distributions, respectively. First, Figure 2(a) shows that the attacker's best

Table 2: Baseline Parameter Values in Illustrations

Parameter	Value	Parameter	Value	Parameter	Value
p_p	.1	V_h	2	g_{uh}	.5
p_u	.3	C_p	.4	v_p	5
p_h	.5	C_u	.3	v_u	3
n_p	5	c_h	.2	v_h	1
n_u	6	c_p	.5	m_p	2
n_h	10	c_u	.3	m_u	2
V_p	5	c_h	.1	m_h	3
V_u	4	g_{up}	.5		

response for attacking a power plant does not depend on the defense at the network of transmissions. This result is mainly related to the assumption that the spread of damage is one directional (e.g., only from parent to child network but not the converse). However, since the attacker makes decisions at all three levels, many different other factors might also play a role. Second, Figures 2(b)-(c) show that the best-response function of the attacker completely depends on the defense of the intended target network of the attack. This implies that the spread of damage from parent networks does not affect the attacker choice. We speculate that the selection of particular values of system parameters might contribute to the observed pattern within the context of decision-making at all three levels. Later in the paper, we conduct extensive sensitivity analyses of the parameters to explore this possibility. Figure 2 appears to imply that it is in the best interest of the attacker to directly attack their intended target and not to rely on spread to damage the connected network.

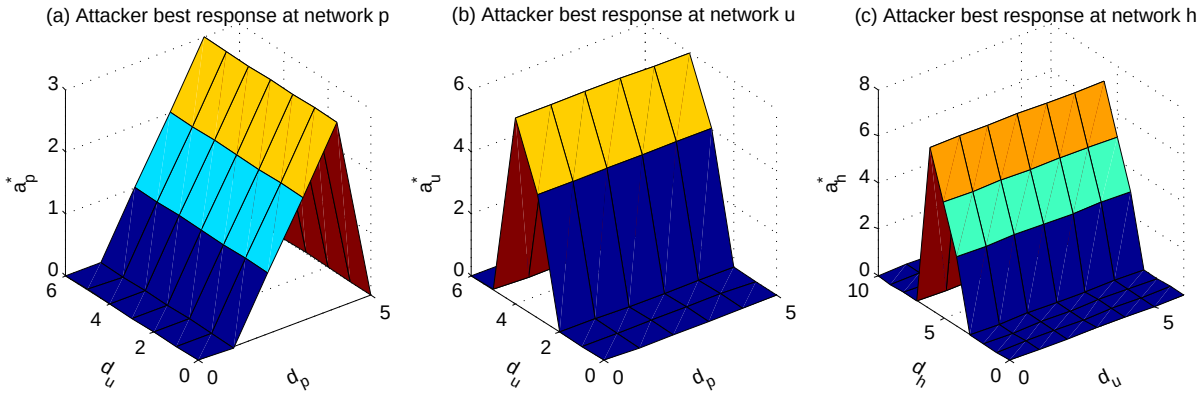

Figure 2: Attacker's best responses at power plants, transmissions, and distribution networks.

Defender's Best Response

Figures 3(a)-(c) show the defender's best response at the network fronts of power plants, transmissions, and distributions, respectively. We observe that the defender's best response does depend on spread unlike the attacker. This is evident from the interdependent relationships illustrated in the power plant and utility company diagrams and missing from the distribution network as shown in Figures 3(a)-(c), respectively. With the chosen set of baseline parameter values, the risk of spread poses a large threat to the whole system of three networks and might play a major role in determining defender's best responses. Therefore, the defender is interested in limiting the spread of attacks on parent networks as much as possible and thus must defend on all levels with a focus on parent networks. The distribution network graph shows

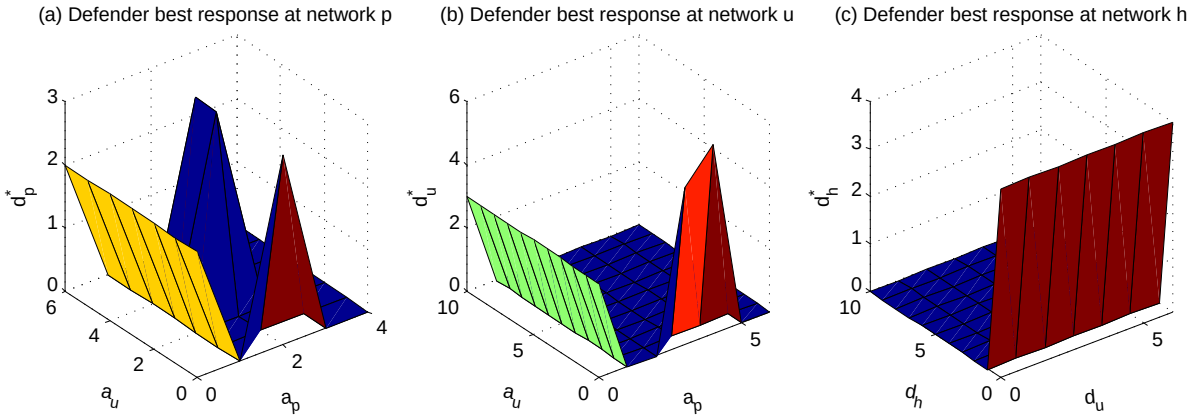

Figure 3: Defender's best responses at power plants, transmissions, and distribution networks.

some intriguing results. It appears that it is in the best interest of the defender to only run a maintenance level of defense at the distribution network. Since our model only considers one directional spread of damage, attacks on a single distribution network might cause negligible amount of damage to the smart grid. Therefore, it is in the best interest of the defender to concentrate resources on transmissions and power plants, where the potential for greater damage is much higher.

Sensitivity Analysis of Equilibrium Strategies

We also study a sequential game where the defender moves first. Figure 4(a) shows the sensitivity analysis with respect to p_p for the attacker and defender equilibrium strategies and utilities. When the probability of a successful attack against network p is low, the utility for the defender

is high and the utility of the attacker is low. They remain the same until p_p= 0.5 where the defender's utility begins to decrease and the attacker's utility increases. The defender's equilibrium strategy of defending network p (d_p^*) remains 0 until p_p=0.5, where d_p^* increases to 5. In contrast, the attacker's equilibrium strategy of attacking each of the three networks (a_p^*, a_u^*, and a_h^*) remains the same regardless of the value of p_p. Note the defender's equilibrium strategy of defending network p decreases as p_p goes from 0.9 to 1. This suggests that the defender is trading off between defense effectiveness and defense cost since if the attack is known to be successful, the defender will save on the defense cost.

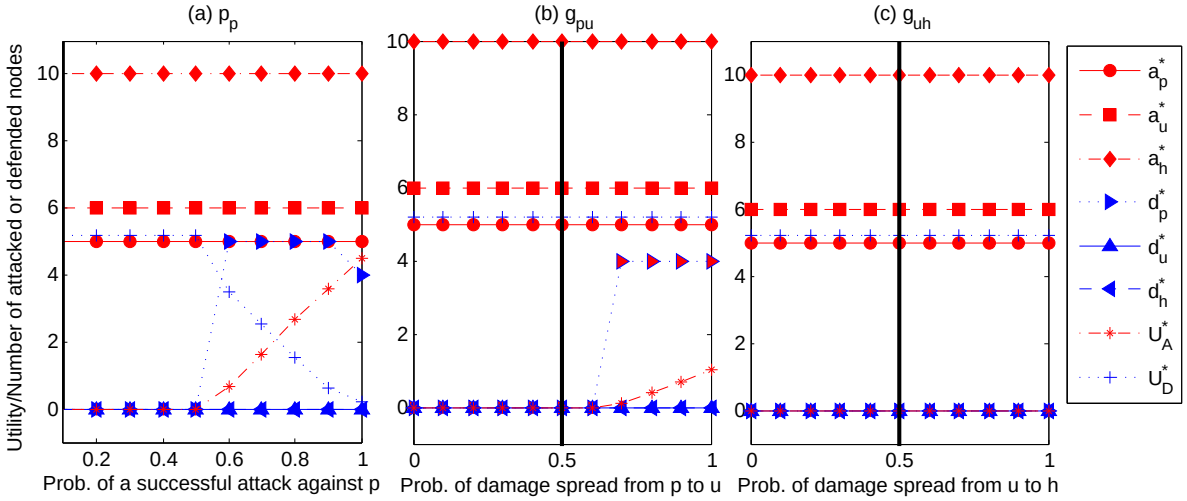

Figure 4: Sensitivity analysis with regard to p_p, g_{pu}, and g_{uh}.

Figures 4(b) and (c) show the sensitivity analysis for g_{pu} and g_{uh}, respectively. Figure 4(b) shows that the attacker and defender efforts are static until the probability of spread reaches 0.6. At this point, the utility of the attacker slightly increases and the defender utility remains the same. Moreover, we see that the defender does not defend any nodes until the probability reaches this threshold value. This pattern is not observed in Figure 4(c) where we see that the utility of both the defender and the attacker remains the same for the whole range between 0 and 1. These results imply that the value of spread to the defender is very low. In this case, the defender gives up defense if the probability of a successful attack against network p is low (e.g., $p_p < 0.6$) and resumes defense efforts when that probability is alarmingly large (e.g., $p_p \geq 0.6$).

CONCLUSION AND FUTURE RESEARCH DIRECTIONS

In this paper, we formulate a game-theoretic model to study the strategic interactions between a defender and an attacker at the three network fronts of power plants, transmissions and distributions within the context of smart grid. We find that the attacker's best responses at all three network types are not affected by the interdependent relationships between the networks. On the other hand, the defender's best responses at networks of power plants and transmissions are not only a function of the number of nodes attacked at that particular level of network, but also the attack strategy at its parent or child network (above the transmission network level) due to the interdependent relationships between the networks.

Sensitivity analysis for equilibrium strategies in a sequential game, where the defender moves first, with respect to the success probability of an attack against a node in the network of power plants shows that until the probability increases to a critical point, the utilities for both the defender and attacker remain the same. The defender does not defend the network of power plants until the probability reaches the critical value. In contrast, the attacker always attacks any one node of the three networks. Furthermore, the defender's equilibrium utility decreases while the attacker's equilibrium utility increases. This suggests that the attacker's equilibrium strategy does not take into account the spread of damage across networks if attack costs are sufficiently low to allow attacking every nodes.

In the attacker's best response functions, we see that the spread does not affect the attacker's decision-making process. In the defender's best response, we find that on the distribution level, the defender should not invest more than a maintenance level of resources, as it is not worthwhile to protect against attacks. This would suggest some future refinement of the modeling approach since in a real-world scenario, transmissions would be expected to protect their consumer base from attacks. If there was no defense support at distributions, consumers would become easy victims for smart thieves and stalkers, as a result no consumer concerned about privacy would accept the smart grid.

There is a number of interesting future research directions. One is to consider continuous levels of attack and defense, which would generate an alternative and more complex optimization problem for both the defender and the attacker. Another is to allow decentralized defense so

that the defender for power plant network and transmissions and the defender for distributions are separate decision-makers. Instead of a topological model, we could also study a flow-based model for smart grids and compare the two models. In addition, instead of 100% blackout of all loads served by a network, we could also consider partial failure of networks. For simplicity, we assume that defense efforts are always effective in countering the attack efforts, which would be relaxed in the future. In addition, we would also consider the criticality of different nodes to their corresponding networks. A small number of nodes are considered for the numerical illustration, we could expand the scale of the model to better reflect the real-world network.

Acknowledgment

This work was funded by the Mathematics of Complex, Distributed, Interconnected Systems Program, Office of Advanced Computing Research, U.S. Department of Energy, and was performed in part at Oak Ridge National Laboratory managed by UT-Battelle, LLC for U.S. Department of Energy under Contract No. DE-AC05-00OR22725. This research was also partially supported by the United States Department of Homeland Security through the National Center for Risk and Economic Analysis of Terrorism Events (CREATE) under award number 2010-ST-061-RE0001, and U.S. National Science Foundation (NSF) under award number 1200899. However, any opinions, findings, and conclusions or recommendations in this document are those of the authors and do not necessarily reflect views of the sponsors.

References

Bidram, A., and Davoudi, A. 2012. Hierarchical Structure of Microgrids Control System, *IEEE Transactions on Smart Grid*, Vol 3, No 4, 1963-1976.

Bier, V., Olivero, S., and Samuelson, L. 2007. Choosing What to Protect: Strategic Defensive Allocation Against an Unknown Attacker, *Journal of Public Economic Theory*, Vol 9, No 4: 563-587.

Bier, V. M., Gratz, E. R., Haphuriwat, N. J., Magua, W., and Wierzbicki, K. R. 2007. Methodology for Identifying Near-Optimal Interdiction Strategies For a Power Transmission System, *Reliability Engineering & System Safety*, Vol 92, No 9, 1155-1161.

Bursztein, E., and Goubault-Larrecq, J. 2007. A Logical Framework for Evaluating Network Resilience aainst Faults and Attacks, *Lecture Notes in Computer Science*, Vol 4846, 212-227.

Carin, L., Cybenko, G., and Hughes, J. 2008. Cybersecurity Strategies: The Queries Methodology, *Computer*, Vol 41, No 8, 20-26.

Chen, T. M. 2011. Petri Net Modeling of Cyber-Physical Attacks on Smart Grid, *IEEE Transactions on Smart Grid*, Vol 2, No 4, 741-749.

Cox, L. A. 2009. Making telecommunications networks resilient against terrorist attacks (Chapter 8). Game Theoretic Risk Analysis of Security Threats, (eds. Bier, V M, Azaiez, M N), Springer: New York, pp. 175-198.

Dighe, N., Zhuang, J., and Bier, V. M. 2009. Secrecy in Defensive Allocations as a Strategy for Achieving More Cost-effective Attacker Deterrence, *International Journal of Performability Engineering,* Special issue on System Survivability and Defense against External Impacts, Vol 5, No 1, 31-43.

Dobuzinskis, A. 2016. Cyber Attack Snarls Los Angeles Hospital's Patient Database. http://www.reuters.com/article/us-california-hospital-cyberattack-idUSKCN0VQ01X Accessed in December, 2016.

Faranz, F., and Sonne, P. 2012. Sophisticated Virus Infects Computers in Iran, Mideast, *The Wall Street Jounral*. http://online.wsj.com/article/SB10001424052702303395604577434582318857536.html (27 June 2012). Accessed in December 2016.

Flick, T., and Morehouse, J. 2011. *Securing the Smart Grid: Next Generation Power Grid Security.* Amsterdam: Syngress.

Garrity, T. F. 2008. Getting Smart. *IEEE Power Energy Magazine*, Vol 6, No 2, 38-45.

Golalikhani, M. and Zhuang, J. 2011. Modeling Arbitrary Layers of Continuous Level Defenses in Facing with a Strategic Attacker. *Risk Analysis*, Vol 31, No 4, 533-547.

Gorman, S. 2009. Electricity Grid in U.S. Penetrated by Spies. *The Wall Street Journal*. http://online.wsj.com/article/SB123914805204099085.html, accessed December, 2016.

Gu, W. 2008. Defending Against Node-targeted Attacks in Wireless Networks. PhD Dissertation, The Ohio State University, Columbus.

Haphuriwat, N. and Bier, V. M. 2011. Trade-offs Between Target Hardening and Overarching Protection. *European Journal of Operational Research* Vol 213, No 1, 320-328.

Hausken, K. 2006. Income, Interdependence, and Substitution Effects Affecting Incentives for Security Investment, *Journal of Accounting and Public Policy* Vol 25, No 6, 629-665.

Hausken, K. 2013. Combined Series and Parallel Systems Subject to Individual Versus Overarching Defense and Attack. *Asia-Pacific Journal of Operational Research* Vol 30, No 2, 1250056 (33 pages).

Hausken, K. 2014. Individual vs Overarching Protection and Attack of Assets, *Central European Journal of Operations Research* Vol 22, No 1, 89-112.

Hausken, K., and Zhuang, J. 2011. Governments' and Terrorists' Defense and Attack in a T-period Game. *Decision Analysis*, Vol 8, No 1, 46-70.

He, F., Zhuang, J., and Rao, N. 2012. Game-theoretic Analysis of Attack and Defense in Cyber-physical Network Infrastructure, in *Proceedings of the 2012 Industrial and Systems Engineering Research Conference*, Orlando, FL.

Krapp, P. 2005. Terror and Play, or What was Hacktivism? Grey Room. MIT Press. accessed in December 2016.

Kunreuther, H., and Heal, G. 2003. Interdependent Security. *The Journal of Risk and Uncertainty*, Vol 26, No 2/3, 231-249.

Lakdawalla, D.,and Zanjani, G. 2002. Insurance, Self-protection, and the Economics of Terrorism. Ms., RAND and NBER, Federal Reserve Bank of New York.

Levitin, G. 2003. Optimal Multilevel Protection in Series Parallel Systems. *Reliability Engineering & System Safety* Vol 81, No 1, 93-102.

Levitin, G., and Hausken, K. 2012. Individual Versus Overarching Protection against Strategic Attacks. *Journal of the Operational Research Society*, Vol 63, No 7, 969-981.

Levitin, G., Hausken, K., and Dai, Y. 2013. Individual vs. Overarching Protection for Minimizing the Expected Damage Caused by an Attack, *Reliability Engineering & System Safety*, Vol 119, 117-125.

Levitin, G., Hausken, K., and Dai, Y. 2014. Optimal Defense with Variable Number of Overarching and Individual Protections, *Reliability Engineering & System Safety*, Vol123, 81-90.

Levitin, G., Hausken, K., Taboada, H. A., and Coit, D. A. 2012. Data Survivability vs. Security in Information Systems, *Reliability Engineering & System Safety*, Vol 100, 19-27.

Metke, A., and Ekl, R. 2010. Security Technology for Smart Grid Networks," *IEEE Transactions on Smart Grid*, Vol 1, No 1, 99-107.

Paganini, P. 2014. Extremists Groups of ISIS and Al Qaeda are Rampiing up Efforts to Launch Major Cyber Attacks on Western Critical Infrastructure to Set up Digital Caliphate. Security Affair, September 14. http://securityaffairs.co/wordpress/28300/cyber-crime/isis-cyber-caliphate.html Accessed in December 2016.

Reitenbach, G. 2012 The U.S. Military Gets Smart Grid, Power, http://www.powermag.com/the-u-s-military-gets-smart-grid/ Accessed in December 2016.

Roy, S., Ellis, C., Shiva, S., Dasgupta, D., Shandilya, V., and Wu, Q. 2010. A Survey of Game Theory as Applied to Network Security, in *Proceedings of 43rd Hawaii International Conference on System Sciences (HICSS)*, Honolulu, HI.

Salmeron, J., Wood, K., and Baldick, R. 2004. Analysis of Electric Grid Security under Terrorist Threat, *IEEE Transactions on Power Systems*, Vol 19, No 2, 905-912.

Salmeron, J., Wood, K., and Baldick, R. 2009. Worst-Case Interdiction Analysis of Large-Scale Electric Power Grids, *IEEE Transactions on Power Systems*, Vol 24, No 1, 96-104.

Salve, S. A., Sarode, S. S., and Sarode, P. S. 2015. Review of Cyber Security Issues and Attacks for Smart Grid Computing, *VidyaCare Journal of Engineering Research* Vol 1, No 1, 27-29.

Shan, X., and Zhuang, J. 2013a. Cost of Equity in Homeland Security Resource Allocation in the Face of a Strategic Attacker. *Risk Analysis,* Vol 33, No 6, 1083-1099.

Shan, X., and Zhuang, J. 2013b. Hybrid Defensive Resource Allocations in the Face of Partially Strategic Attackers in a Sequential Defender-attaacker Game. *European Journal of Operational Research,* Vol 228, No 1, 262-272.

Shan, X., and Zhuang, J. 2014a. Modeling Credible Retaliation in the Smuggling of Nuclear Weapons Using Partial Inspection-A Three-stage Game. *Decision Analysis*, Vol 11, No 1, 43-62.

Shan, X., and Zhuang, J. 2014b. Subidizing to Disrupt a Terrorist Supply Chain - A four-players game. *Journal of the Operational Research Society,* Vol 65, No 7, 1108-1119.

Sorebo, G. and Echols, M. 2012. *Smart Grid Security: An End-to-end View of Security in the New Electrical Grid.* Boca Raton, FL: CRC.

Tas, S., and Bier, V. M. 2014. Addressing Vulnerability to Cascading Failure against Intelligent Adversaries in Power Networks. *Energy Systems*, 1-12.

Tas, S., and Bier, V. M. 2015. Electric Power Vulnerability Models: From Protection to Resilience (Chapter 9), Breakthroughs in Decision Science and Risk Analysis (Wiley Essentials in Operations Research and Management Science), (ed. Cox L A) Wiley, New York, NY.

Wang, W., and Lu, Z. 2013. Cyber Security in the Smart Grid: Survey and Challenges. *Computer Networks* Vol 57, No 5, 1344-1371.

Wei, C. 2010. A Conceptual Framework for Smart Grid. in *Proc. of Power and Energy Engineering Conference*, Chengdu, China, March 28-31, pp. 1-4.

Yan, Y., Qian, Y., Sharif, H., and Tipper, D. 2012. A Survey on Cyber Security for Smart Grid Communications. IEEE Communications Surveys & Tutorials, Vol 14, No 4, 998-1010.

Yuan, W., Zhao, L., and Zeng, B. 2014. Optimal Power Grid Protection through a Defender-attacker-defender Model. *Reliability Engineering & System Safety*, Vol 121, 83-89.

Zahedi, A. 2011. Developing a System Model for Future Smart Grid, in *Proc. of 2011 IEEE PES Innovative Smart Grid Technologies Conference, ISGT Asia*, Perth, November 13-16, pp. 1-5.

Zhuang, J., and Bier, V. M. 2007. Balancing Terrorism and Natural Disasters - Defensive Strategy with Endogenous Attack Effort. *Operations Research*, Vol 55, No 5, 31-43.

Zhuang, J., and Bier, V. M. 2011. Secrecy and Deception at Equilibrium, with Applications to Anti-terrorism Resource Allocation. *Defence and Peace Economics*, Vol 22, No 1, 43-61.