Towards Quantifying the Impacts of Cyber Attacks in the Competitive Electricity Market Environment

Matias Negrete-Pincetic, Felipe Yoshida and George Gross
Department of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign

***Abstract*—We provide in this paper the first steps towards the quantification of the impacts of cyber attacks on the power grid. We present a review of key-issues on cyber security of power systems, and show the main challenges as well as complicating factors. In order to do the quantification, we propose the application of a conceptual four-layer framework that represents the physical, communication/control, market levels of the electricity infrastructure, and a cyber security investment layer. We characterize each layer and discuss the relationship among them. We focus on quantify the impacts that cyber attacks can have on the market layer using the system social welfare as the main metric. We use a small system to illustrate the application of our framework on the evaluation of investment alternatives on cyber security.**

***Index Terms*—Power system economics, cyber security, risk management, national security.**

I. Introduction

THE power grid is the skeleton in which our modern society is sustained. Electricity as a source of energy has become indispensable and interruptions of the service can have tremendous social and economic impacts. For example, the 2003 mega-blackout in the East coast of the United States affected 50 million people and cost an estimate of 6-13 billion dollars. The complexity of the power grid has increased as a result of the restructuring of the industry moving towards a market environment with new players and uncertainty sources, the use of more communication networks, Supervisory Control And Data Acquisition (SCADA) control systems, wireless communications, and the Internet. These have opened new vulnerabilities, the so-called cyber-vulnerabilities [1], [2], [3], [4]. Such cyber-vulnerabilities, which key characteristic is the no necessity of physical interaction with the power grid, can be thought as additions to the well-known physical vulnerabilities. Only using communication networks, from anywhere in the world, such vulnerabilities can be detected and exploited. This non-physical characteristic creates a new scenario for reliability considerations, and, in general, the notions as well as several tools for reliability analysis need to be upgraded or created for the new environment. Size is the critical parameter in usual reliability considerations in the sense that, for example, large generation plants impact more than small ones. However, in this new cyber scenario, connectivity emerges as the single most critical issue [1]. Large isolated plants with no electronic connections have less impact than small electronically connected plants. For this reason, any system electronically connected must be considered in any cyber risk assessment. Key-challenges in this research topic are the characterization of cyber attacks, the quantification of impacts, and the assessment of risks. The complexity of such tasks becomes particularly pronounced due to the large-scale nature of the grid and the interrelationships between the several levels –physical, communications/control and market– that make-up the electricity industry. In this paper, we present the first steps to quantify the economic impacts cyber attacks might have. In order to do the quantification, we propose the application of a conceptual four-layer framework that represents the physical, communication/control, market levels of the electricity infrastructure, and a cyber security investment layer. We characterize each layer and discuss the relationship among them. We focus on quantifying the impacts cyber attacks can have on the market layer using the system social welfare as the main metric. We present some numerical results showing the application of our framework on a small system. This paper contains seven more sections. Section II presents a review of main issues in cyber security. Section III is devoted to cyber attacks. In section IV, we present several examples of cyber security attacks. In section V, we present the proposed framework to quantify the economic impact. Section VI shows numerical results of the application of such framework. Finally, we provide some concluding remarks and further research directions in section VII.

Matias Negrete-Pincetic mnegret2@uiuc.edu, Felipe Yoshida fyoshid2@illinois.edu, and George Gross gross@illinois.edu) are with the Department of Electrical and Computer Engineering at the University of Illinois at Urbana-Champaign.

II. EMS/SCADA criticalness

The electric energy industry, just as any other sort of business, is in search for the maximization of profits using the minimum of available resources as possible. With the introduction of more complex electrical systems, it became impossible for a human being to monitor and control them in real time in order to obtain the best configuration of the system. The Energy Management System (EMS) is the technology that made it possible. With information from specific points of the power grid, this computational system is able to determine the most economic way to operate the grid, maintaining a specified voltage, frequency, and dynamic stability.

In order to gather all the necessary information and deliver the commands, it is necessary to have a network that is capable of collecting and sending data from great distances that might

exceed hundreds of miles. Due to the ability of performing this function with a reduced cost, SCADA systems are used not only in the electric infrastructure, but also in gas, water and telephony systems. It is composed basically of three parts: the Remote Terminal Units (RTU), a master station, and a network connection between them. The RTUs and the master station work logically together in two ways; on one way, the data acquired locally from all the RTUs are aggregated in the master station, which is part of the EMS. On the other end, the master station sends back commands to the RTUs. The transmission channel can diverse: leased lines, Internet, Ethernet, and wireless, among others [2].

The importance of the SCADA system is due to its ability of gathering data and taking the required actions according to the necessity. It can take measurements of thousands of points, such as voltages, frequency, or breaker and relay status. Also, according to the decisions of the EMS, it can take the required actions, such as the opening or closing of breakers or changing a transformer tap. This way, the SCADA system can be used to help the generation, transmission, and distribution systems to maintain the quality and the dynamic stability of the grid.

However, the use of the SCADA introduces a series of vulnerabilities into the power grid. As it becomes more dependent on IT, there is a bigger susceptibility on cyber security attacks. Legacy protocols have little or no attention to security [2]. Moreover, due to the great importance of the power as one of the most critical infrastructures –if not the most important one–, the risk associated of being the target of a cyber attack increases considerably. Even if an attacker is capable of disrupting the grid for some hours, without permanent damage, the losses can be of billions of dollars.

III. Attacks Characterization

There are several types of attack that can be made to the SCADA, most of which are already common by their use in the Internet or in other networks. In this section we will be describing some of them. Each attack will be characterized, its possibility will be analyzed, and its outcome (most likely and worst case) will be studied. At the end, we will classify them in a subjective scale of difficulty and impact.

When protecting the SCADA, just as in any other interconnected information scheme, we need to take in account the three information security components: confidentiality, integrity, and availability [5]. Confidentiality is the ability of only the authorized system to access a determined information; integrity is the quality of the data sent to be exactly the same as the one received; and availability is the capability of a system to be available when needed. Analyzing each type of attack regarding these three characteristics will make it easier to identify the consequences of each attack.

The first attack we will describe is the Denial of Service attack (DoS). Its objective is to make a resource temporarily unavailable through the overloading of the communications of a respective target. In some network protocols, the participants of the connection keep listening to the medium, waiting for their turn to transmit. The way this turn is chosen is variable, but if there is someone misbehaving in the network, that is, always transmitting, it becomes impossible to send a message. For example, in a SCADA network, an attacker could be trying to disrupt the communications between the EMS and the RTUs, sending spurious packets in the network. This way, there will not be any possibility of communication, the EMS will not receive signals, and control messages will not be received also. Availability, thus, is severely compromised. In the worst case, all the communication in the system is disabled, so, if an emergency situation happens when the system is in this state, or an action is required by the system operator, it will not be realized, as it will be impossible to use the communication medium. However, the loss of communication will most likely be local, as it is highly dependent on the topology of the network. For example, a star topology is less vulnerable than a multi-drop one, as there is less medium sharing. In addition, in many cases a dedicated channel is used, like a leased line, which makes this attack senseless. Therefore, we can classify this attack as relatively easy, as only a connection to the network is necessary, and the effect is most likely light, only a temporary lost of connection would happen.

With the popularization of open protocols rather than proprietary ones, it became easier for an attacker to understand what is going on in the transmission, as the knowledge to interpret the message is available to anyone. This fact facilitates the use of another attack, the replay. It consists in "listening" the traffic in the network, identifying a message, and replaying it in an opportune time to repeat a previous action. For example, an interceptor is able to listen to the network, and identify a transmitted message as being the issue of the command "open breaker number 12". Later, in an opportune time, he will be able to retransmit the same message, pretending he is the EMS, and obtain the same result. The opposite direction can also happen, when the transmitted message has its target the EMS instead of an RTU. This way, the attacker could trick the EMS, by sending a bad state and forcing a wrong response. This attack compromises the confidentiality and integrity of the system. It is just possible if there is nonexistent/low encryption in the data transmission, and if the attacker has to be able to access the SCADA network. It is slightly more improbable than the DoS attack, as it also requires that the invader is able to determine what the messages mean, and not only have access to the network. However, the damage that can be caused is higher, as he would have a minimum control over what will happen in the system, which did not happen in the DoS attack. In the worst case, permanent damage can be done if the attacker has knowledge of power systems and if the EMS does not take the required actions in time. Most likely, only temporary blackouts will happen if the attacker is successful, as he would not have power over the EMS control commands.

The man-in-the-middle attack resembles the replay, but is more sophisticated. On it, the attacker acts between two communication points. He tricks the sender, making it believe he is the correct receiver, and/or also the receiver, tricking him that he is the sender. This way all the messages between them can be altered, omitted, or inserted in the system. For example, the attacker acts as a middleman between an RTU and the EMS. He could intercept emergency messages sent

from the RTU, and retransmit it as if the status is OK, or even transmit a warning when the system needs no action. In the other way, it can also modify, ignore, or insert a command sent by the EMS. As the replay attack, it compromises the confidentiality and integrity of the system. It is even more difficult to be made, as the intruder has to be able to trick the sender that he is the receiver, and/or the receiver that he is the sender. Nevertheless, it is even more powerful, as besides having full control over a point (or points), the EMS will not be able to realize what is going on these spots. If the intruder has a good knowledge about power systems, the attack can be devastating, as he would have full control over the points he tricked. Though, many proper conditions are necessary, such as the ability to break the encryption if present, have access to the network, and be able to mislead both sender and receiver of the messages.

Reprogramming the RTUs is also a destructive possibility, but is very unlikely to happen. In this case, the attacker would reprogram as many RTUs as he wants or is able to. He would insert malicious behavior that could be changing its master from the EMS to the attacker, or taking a wrong action at a predetermined time. It would be necessary for the attacker to have knowledge on the programming of the RTUs, and either that the RTUs can be reprogrammed remotely or that the attacker has physical access to the RTUs. Both cases are much unlikely to happen, the first one because it would be a big mistake by the system administrator to allow remote programming without any special precaution like strong password protection, and the second one because it would be easier for the attacker to plant a bomb or damage the equipment if he has access to the building where RTU is. Moreover, in this case, to have a large-scale attack, it would be necessary to reprogram a great number of RTUs, which would require a huge effort, as they are usually distributed through a large area. Though, if the attacker were capable of performing this attack, he would be able to have complete control over the reprogrammed RTUs.

All the described attacks need an access to the SCADA network. Basically, it can be obtained through two ways: either by getting the access from inside the network itself (local), or through another network (remote) [5]. In the former, the intruder would get the connection in one of the RTUs, as having physical access to the EMS or wiretapping the connection would be significantly more difficult. This kind of approach is not likely to happen, as it would require knowledge of the protocol used, and the topology of the network, which would probably limit the size of the attack. In addition, it would require the attacker to be physically close to the connection, which might scare someone who does not wish to be caught. The latter, much more likely to occur, would be through any other network that is connected to the SCADA network, probably the corporate network. In this case, if any of the connected networks is also connected to the Internet, the attack can be initiated from virtually anywhere in the world. Of course, some conditions are required, such as misconfigured firewalls, access to the corporate network, or weak/no passwords (these conditions have already been proven that exist, as we will see in the next section). Moreover, many of the policies implemented are inappropriate to the SCADA networks [1].

In order to have a better characterization of the attacks, we need to be able to compare them directly regarding two parameters; the difficulty of an attack, and the impact it can cause. The difficulty factor is determined by the amount of effort needed to be performed, the probability, the necessary conditions to happen, as well as the knowledge the attacker needs. The impact is directly associated with the social, and economic losses, and it is function of the size and period of the attack. To make this comparison, we present the Impact vs. Difficulty chart, shown in Fig. 1. In this chart, the four types of attack are arranged and classified subjectively according to these two parameters. We can see that there is no attack that is easily feasible, and at the same time, that would cause a huge damage. Thus, a big organized group such as a terrorist organization or a foreign country that wants to severely damage the electric infrastructure, would most likely follow a man-in-the-middle attack rather than the other attacks, while a hacker who wants to call attention would probably go with a DoS attack.

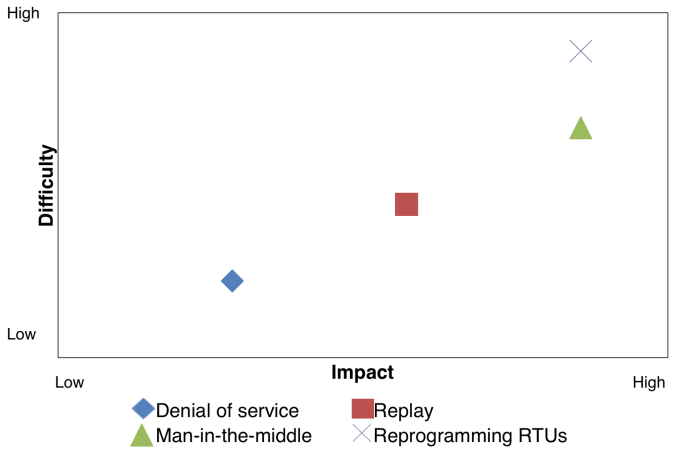

Fig. 1. Impact vs. difficulty chart

IV. Vulnerabilities and Attacks Examples

We present a review of real examples of vulnerabilities and cyber attacks. Those examples illustrate the threats cyber attacks represent, and the necessity to pursue research on the understanding and protection against cyber attacks on the electric infrastructure.

A. Aurora

On March 2007, the Department of Defense launched an experimental cyber attack that caused a generator to self-destruct. The experiment was conducted in the Department of Energy Idaho Lab, where a replica of a power plant control system was hacked, making a generator shake and shut down in smoke. This kind of attack, coordinated in a large scale could damage the electric infrastructure for months [7], [8].

B. Ira-Winkler

The security consultant Ira Winkler and his team were hired by a power company to test the vulnerabilities in their computer system. Using social engineering and corrupting browsers, they were able to hack into the power plant control network in one day, being able to oversee the power production and distribution. Besides having access of the SCADA system, the team was able to download the CIO and CEO records [9], [10].

C. TVA

According to the Government Accountability Office, the Tennessee Valley Authority (TVA) was vulnerable to cyber attacks. Their Power network stretch across 80,000 square miles and provide electricity to more than 8.7 million people. The main vulnerability is related to the connection between the corporate and the power control network, where weaknesses in the corporate side could be used to take control or damage the system in the other side. Also, there was a series of weak configurations, such as bad configured firewalls, lack of effective virus protection and weak passwords [11], [12] and [13].

D. Hatch-power plant

On March 2008, a unit of the Hatch power plant in Georgia had to shut down for 48 hours, after an engineer installed a patch in a computer in the corporate network, which was used to monitor data from the control system. As the computer rebooted, there was no data in system, which was interpreted as a drop in the reactor's cooling water, causing the plant to treat it as a severe failure [14], [15] and [16].

V. Framework

In order to analyze the problem from a better perspective, an analytic framework, which is shown in Fig. (2) was developed. The four-layer structure represents the market, the communication and control, the physical levels, and the "new" cyber security investment of the electricity infrastructure.

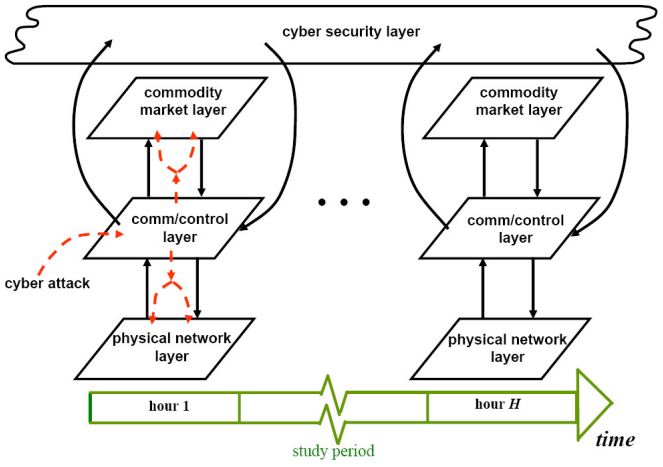

Fig. 2. The conceptual framework.

The lowest one, the physical, is where the distribution, transmission, and generation systems are included. By itself, it does not "see" the electrical system as a whole. It is monitored and controlled by its upper layer, the communications/control layer. This layer is where the EMS and the SCADA system are located, and also, where a cyber attack is more likely to be initiated, as there is the intensive exchange of data in the SCADA network. Besides the connection with the physical layer, the communication/control layer has connections with the upper market layer. The market layer represents all the market mechanism of the industry such as day-ahead, real-time, long-term contract, and financial energy instruments markets.[1] Information generated in this layer impacts directly the operation of the physical layer. The key-point between these three layers is the central role of the communication/control layer. Both, market and physical layers are interconnected through the communication/control layer. For that reason, a cyber-attack, which can be initiated in the communication/control layer, can have tremendous impacts on both layers. The top layer is the cyber security investment layer, which represents several investment alternatives and upgrades to the security on the communication and control layer. In the rest of this section, we make a characterization of each layer, highlighting the key-issues and the information needed to perform the cyber attack impacts quantification.

A. Physical Layer

We consider a system with $N+1$ buses and L lines. We call $\mathcal{N} \triangleq \{0, 1, 2, ..., N\}$ the set of buses, with the slack bus represented by bus 0, and $\mathcal{L} \triangleq \{l_1, l_2, ..., l_L\}$ the set of transmission lines that connect the buses on $\mathcal{N}$. Each element of the set $\mathcal{L}$ has associated an ordered pair (i, j), and we write $l = (i, j)$. We use f_l to represent the line flows. We uses the convention that the direction of the flow on line l is from node i to node j, so that $f_l \geq 0$. The network flows are represented by the vector $\underline{\mathbf{f}} = [f_1, f_2, ..., f_L]^T$. We denote by p_n the net active power injection at node $n \in \mathcal{N}$. The system net power injections are represented by the vector $\underline{\mathbf{p}} = [p_1, p_2, ..., p_N]^T$. The line series admittance of line l is represented by $Y_l = g_l - jb_l$. We define the $L \times L$ diagonal branch susceptance matrix by $\underline{\mathbf{B}}_d = diag\{b_1, b_2, ..., b_l\}$ and by $\underline{\bar{\mathbf{A}}} \triangleq [\underline{\bar{\mathbf{a}}}_0, \underline{\bar{\mathbf{a}}}_1, ..., \underline{\bar{\mathbf{a}}}_L]$ the augmented branch-to-node incidence matrix, in which,[2]

$$\underline{\bar{\mathbf{a}}}_{l(i,j)k} = \delta_{ik} - \delta_{jk} \tag{1}$$

Since we are considering the slack bus entry, $\underline{\bar{\mathbf{a}}}_l \in \mathbb{R}^{N+1}$. In addition, we use a *node-to-node* susceptance matrix defined by $\underline{\mathbf{B}} = \underline{\bar{\mathbf{A}}}^T \underline{\mathbf{B}}_d \underline{\bar{\mathbf{A}}}$. Given the scope of our analysis we adopt a DC power flow model. We assume a lossless power system and the typical DC power flow assumptions [17]. The DC power flow equation is stated as,

$$\underline{\mathbf{p}} = \underline{\mathbf{B}}\theta \tag{2}$$

[1] For simplicity, we focus only on the commodity markets. Hence, we call indistinctively this layer market or commodity market layer.

[2] δ_{ij} represents a kronecker delta. If $i = j$ $\delta_{ij} = 1$ if not $\delta_{ij} = 0$

At this stage, we adopt active power line flow limits,

$$\underline{\mathbf{B}}_d\underline{\mathbf{A}}\theta \leq \underline{\mathbf{f}}^{\max} \tag{3}$$

In which, $\underline{\mathbf{A}}$ represents the reduced incidence matrix, constructed from the augmented incidence matrix $\bar{\underline{\mathbf{A}}}$ by removing the corresponding row/columns associated with the slack bus,

$$\underline{\mathbf{A}} \triangleq [\underline{\mathbf{a}}_1, \underline{\mathbf{a}}_2, ..., \underline{\mathbf{a}}_L] \tag{4}$$

and in this case, $\underline{\mathbf{a}}_l \in \mathbb{R}^N$.

B. Commodity Market Layer

We follow a similar description of the commodity market layer as that in [18]. We use a market structure in which the players submit energy offers to sell to and bids to buy from the ISO. We assume a competitive market, hence offers and bids reflect truthful cost and benefits. Just for simplicity, we assume there are at most one seller and one buyer at each node. In addition, we assume the market is cleared every hour. The bids and offers are represented by differentiable functions $\sigma_n^s(p_n^s)$ and $\nu_n^b(p_n^b)$, respectively. The integral of those functions gives the benefits and cost functions on each node, $B_n^b(p_n^b)$ and $C_n^s(p_n^s)$, respectively. The information about selling and buying of energy at each node is tabulated into the vectors $\underline{\mathbf{p}}^s \triangleq [p_1^s, p_2^s, ..., p_N^s]^T$ and $\underline{\mathbf{p}}^b \triangleq [p_1^b, p_2^b, ..., p_N^b]^T$. The settlement of the market for a particular hour results from the maximization of social welfare, subject to the physical network constraints. The associated optimization problem is,

$$\begin{aligned} \max s(p_0^s, p_0^b, \underline{\mathbf{p}}^s, \underline{\mathbf{p}}^b) &= \sum_{n=0}^{N} \left\{B_n^b(p_n^b) - C_n^s(p_n^s)\right\} \\ s.t. \qquad p_0^s - p_0^b &= \underline{\mathbf{b}}_0^T\underline{\theta} \\ \underline{\mathbf{p}}^s - \underline{\mathbf{p}}^b &= \underline{\mathbf{B}}\underline{\theta} \\ \underline{\mathbf{B}}_d\underline{\mathbf{A}}\underline{\theta} &\leq \underline{\mathbf{f}}^{\max} \end{aligned} \tag{5}$$

C. Communication and Control Layer

The communication/control layer is the responsible for managing the physical layer with information received from the market layer. This work can be done with the EMS and the SCADA, which is composed of the communication network and the RTUs. All the information, such as which generators are scheduled at a given time, what is the current load in the system, and which physical components are available is gathered in the EMS, who is the responsible for the control part of the layer. According to this data, decisions are made regarding what should be done in the physical layer. These decisions are transmitted through the communication network to the place where the action should be taken. As there is an intensive exchange of data in this network, it is the place where a cyber attack is more likely to be initiated. Finally, when the information gets to its destination, the RTUs are responsible to take the physical action, such as opening or closing a breaker. Key-information related with this layer for the framework application is the set of vulnerabilities and potential attacks. It is necessary to have a detailed characterization of the hardware, software and communication protocols to be able to find vulnerabilities and characterize potential cyber attacks.

D. Cyber Security Investment Layer

Given the set of vulnerabilities and potential attacks against the communication and control layer, the cyber security investment layer models the upgrades to the communication and control layer to decrease the possibility of cyber attacks. It is mandatory, for the good representation of this layer, to have a careful characterization the type of investments needed given the set of potential cyber attacks against the communication and control layer. A simple attack could be, for example, the opening of a set of lines producing a topology change. Such topology change can affect the congestion patterns, impacting the clearing of the market, and in a big scale, the whole system operation. In order to avoid the impacts of such attacks, investments on cyber security must be performed. We differentiate the investments in terms of the extent and scope of the cyber security measures. Different extent levels of investment can span from a total-vulnerable system, in which no investment in cyber security has been implemented; mid- or low-vulnerable systems, in which only some areas of the system have cyber security investment; up to finally a fully extent secured system, in which the whole system has implemented cyber security measures. Different scopes of cyber security investment could be, for example, focus on confidentiality, integrity or availability of the system. In order to quantify the impacts of cyber attacks and investments, we evaluate the change on some expected market metrics for several investment options. For every investment alternative, we need to evaluate the total social welfare associated with potential cyber attacks over the period of study,

$$\begin{aligned} \max S = \sum_{h=1}^{H}\sum_{n=0}^{N} &\left\{B_n^{b,h}(p_n^{b,h}) - C_n^{s,h}(p_n^{s,h})\right\} \\ s.t. \qquad p_0^{s,h} - p_0^{b,h} &= \underline{\mathbf{b}}_0^{hT}\underline{\theta}^h, \\ \underline{\mathbf{p}}^{s,h} - \underline{\mathbf{p}}^{b,h} &= \underline{\mathbf{B}}^h\underline{\theta}^h, \qquad h = 1, 2, ..., H \\ \underline{\mathbf{B}}_d^h\underline{\mathbf{A}}^h\underline{\theta}^h &\leq \underline{\mathbf{f}}^{\max}, \end{aligned} \tag{6}$$

In our illustration of the framework, we will use the extent as the parameter to differentiate investments, and the opening of lines as the potential cyber attack. We define as $\mathcal{C} \subseteq \mathcal{L}$ the set of lines associated with a cyber security investment level. For simplicity, we assume that such set of lines cannot be disconnected by remote attacks.[3] In addition, we assume that a line disconnected by a cyber attack will be out-of-service for a couple of hours, hence the matrices $\underline{\mathbf{B}}^h$ and $\underline{\mathbf{A}}^h$ will have to be updated during the study. The topology impacts of cyber attacks to an unsecured set of lines are time invariant. However, the impact on the market outcomes and consequently social welfare will be time variant. A cyber attack at midnight can have a totally different outcome than at noon. In order to capture that, we need to assign probabilities to several attacks, run several realizations of such attacks, and then compute the expected social welfare value. In the next section, using a small 7-bus system, we illustrate the main steps of the proposed framework.

[3] In reality, there is no investment able to guarantee complete invulnerability.

TABLE I
INVESTMENT ALTERNATIVES

alternative	$\mathcal{C}$
a	$\emptyset$
b	$(0,2)$, $(0,1)$, (1,3)
c	$(2,5)$, $(5,6)$, (6,4)
d	$\mathcal{L}$

VI. NUMERICAL SIMULATION STUDIES

We illustrate the framework using a 7-bus system with 5 sellers and 7 buyers shown in Fig. (3). We use the system and the players bids and offers data from [19]. We are going to compare several cyber security investment alternatives. The alternatives of cyber security investments and associated $\mathcal{C}$ are shown in the table I. Alternative a represents no cyber security investment, hence the whole system is vulnerable to cyber attacks. Alternatives b and c implement cyber security measures on some parts of the system, for example, associated with different geographic regions. We illustrate those areas on Fig. (3). Alternative d is an implementation of cyber security measures on the whole system.

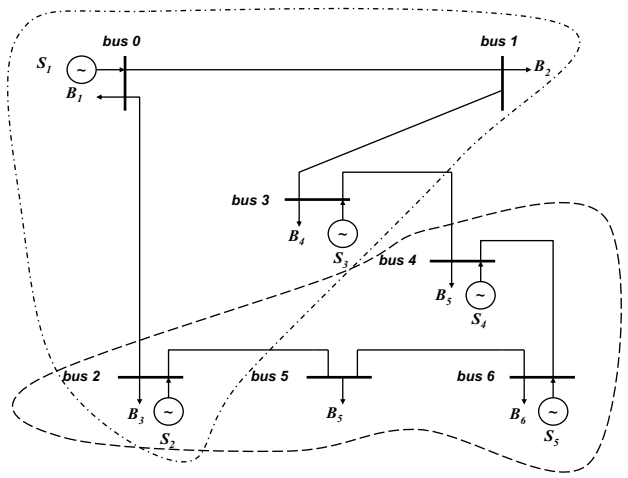

Fig. 3. System topology and two cyber secured areas.

The next step is to characterize the attacks. As we mentioned above, the lines in $\mathcal{C}$ are no subject to the impact of cyber attacks, hence they cannot be disconnected. For each cyber security investment alternative, we construct the possible set of attacked lines from the subset of lines $\mathcal{L} - \mathcal{C}$. Given the possibility of multiple line outages, the total number of possible attacks on the cyber security risk assessment is large. For large systems, similar to the cascading failures problem [20], an exhaustive characterization is infeasible. Hence, one of the challenges of this research area is precisely how to deal with this large-scale characteristic. Results from the cascading failure research such as identification of critical subsets [21] could be explored. However, this is beyond the scope of this paper, here we just focus on picking up a representative subset of attacks and evaluates the market metrics in order to illustrate the framework. Hence, for each cyber security investment alternative, we evaluate the economic impacts of one possible attack. The possible attacks are represented in table II.

TABLE II
CYBER ATTACKS

alternative	outage lines
a	$(0,1)$, $(3,4)$
b	$(4,6)$
c	$(3,4)$
d	$\emptyset$

TABLE III
EXPECTED SOCIAL WELFARE FOR EACH ALTERNATIVE

alternative	expected social welfare ($)
a	1925400
b	1927300
c	1927200
d	1928400

In order to capture season and daytime changes of the cyber attack impacts, we evaluate attacks on fall, winter, spring and summer, and on-peak/off-peak conditions. We assume equal probability for attacks on each season (0.25), and equal probability for attacks on on-peak/off-peak times (0.5). Those figures for the probabilities can certainly be fine-tuned. However, statistical analysis to calculate attacks probabilities are difficult given the lack of information about real cyber attacks. The metric associated with the selected cyber attack, for each cyber security investment alternative k, is the expected social welfare,

$$\mathrm{E}(S^k) = \sum_{i=1}^{4}\sum_{j=1}^{2} \pi_{ij} \max(S^k)_{ij} \tag{7}$$

in which $\max(S^k)_{ij}$ is the solution of problem (6) under the k investment alternative, given that the selected cyber attack happens on season i and time j. π_{ij} are the probabilities associated with each scenario. In our numerical example, for each investment alternative k, $\pi_{ij} = 0.125$.

We use quadratic functions for the benefits and cost functions of problem (6), given by

$$B_n^{b,h}(p_n^{b,h}) = \beta_n^{b,h} p_n^{b,h} - \frac{1}{2}\gamma_n^{b,h}(p_n^{b,h})^2 \tag{8}$$

$$C_n^{s,h}(p_n^{s,h}) = \beta_n^{s,h} p_n^{s,h} + \frac{1}{2}\gamma_n^{s,h}(p_n^{s,h})^2 \tag{9}$$

Our study period will be 96 hours, using 24 hours for each season. In order to capture demand changes associated with each hour and season, we modify the buyer's parameter $\beta_n^{b,h}$. Sellers' bids' parameters are not modified over the study period. We present the results of evaluating (6) and (7) for each cyber attack on table III

We present two representative plots of the expected locational marginal prices (LMP) of the system. In Figs. (4) and (5), we plot the expected system LMP[4] for the summer and winter demand patterns. From all the possible attacks we

[4]We evaluate the system LMP taking the average of the LMP at each bus.

picked up, the double outage of lines $(0, 1)$ and $(3, 4)$ produces the large decrement on the social welfare, and the large increments on the system LMPs. The attacks producing single line outages have very similar results for both social welfare and system LMPs. We should highlight that on the evaluation of cyber attacks, unlike typical reliability considerations, the outage of two lines could have similar probability of the outage of a single line. Hence, given that the impact of the double outage is higher, the risk[5] associated could be also higher.

The aim of this numerical simulation was to illustrate and highlight the main points of the proposed framework using a simple and idealized system. Conceptually, the application of the framework in more realistic system is similar. The main challenge on real systems is the characterization of vulnerabilities and attacks. Given that information, the proposed framework and the same LMPs and social welfare metrics are useful to evaluate cyber attacks and investments. We are currently working on that direction. We will report our findings in forthcoming publications.

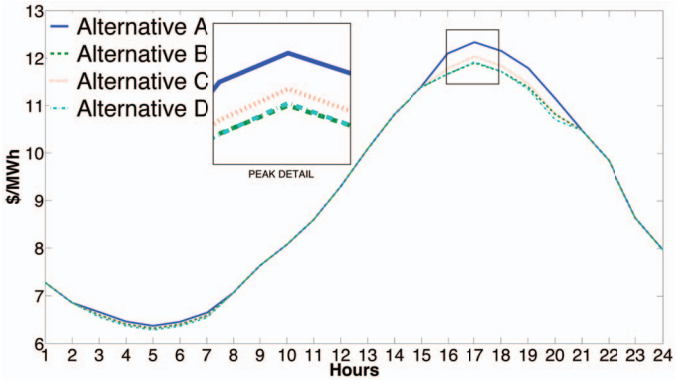

Fig. 4. Expected system LMPs summer attack.

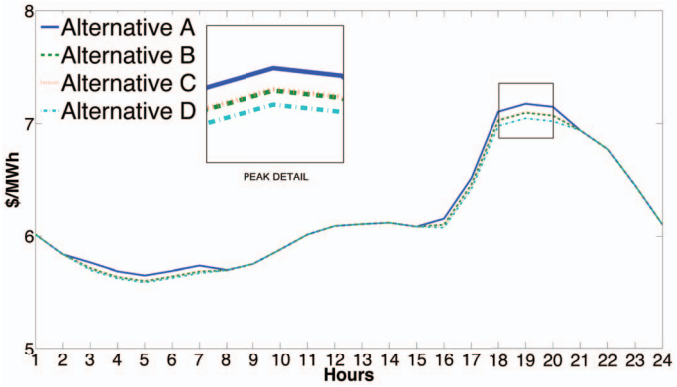

Fig. 5. Expected system LMPs winter attack.

VII. Conclusions

In this paper, we presented the first steps toward the quantification of the impacts of cyber attacks on competitive electricity markets. Also, we presented the main challenges of this research area, described and categorized cyber attacks, and finally, provided examples of vulnerabilities and attacks. Using a conceptual multi-layer framework, we represented the physical, communication and control, market, and the "new" cyber security investment layer of the electricity industry. Moreover, using the social welfare as a metric, we were able to quantify the economic impacts cyber attacks can have. Furthermore, we illustrated the conceptual framework on a 7-bus system for the evaluation of cyber security investment alternatives. Further research must be performed in the direction of a detailed characterization of cyber attacks and their impacts on the physical layer, probabilities associated, and how to deal with the large-scale of scenarios available.

[5]Assuming the standard definition of risk as probability times impact.

Acknowledgments

We thank Alejandro Dominguez-Garcia and Himanshu Khurana for insightful discussions and comments related with this work. Felipe Yoshida's work was supported by the Information Trust Institute Summer Internship, 2008.

References

[1] J. Weiss, "Key Issues for Implementing a Prudent Control System Cyber Security Program," Electric Energy T & D Magazine, March-April 2008.
[2] P. Ralston, J.Graham, J. Hieb, "Cyber security risk assessment for SCADA and DCS networks", ISA Transactions, Volume 46, Issue 4 , October 2007, Pages 583-594.
[3] S. Massoud Amin and B.F. Wollenberg, "Toward a smart grid: power delivery for the 21st century," Power and Energy Magazine, IEEE , vol.3, no.5, pp. 34-41, Sept.-Oct. 2005.
[4] C. Ten, C. Liu, M. Govindarasu, "Vulnerability assessment of cybersecurity for SCADA systems", Power Engineering Society General Meeting, 2007. IEEE, pp.1-8, 24-28 June 2007.
[5] T. Fleury, H. Khurana, V. Welch, "Towards a taxonomy of attacks against energy control systems", Proceedings of the IFIP International Conference on Critical Infrastructure Protection, March 2008.
[6] K. LaCommare, J. Eto, "Cost of power interruptions to electricity consumers in the United States (US)", EnergyVolume 31, Issue 12, , September 2006, Pages 1845-1855.
[7] Forbes, Congress Alarmed At Cyber-Vulnerability Of Power Grid: http://www.forbes.com/2008/05/22/cyberwar-breach-government-tech-security _cx_ag_0521cyber.html
[8] CNN, Sources: Staged cyber attack reveals vulnerability in power grid: http://www.cnn.com/2007/US/09/26/power.at.risk/index.html
[9] Internet Evolution, How to Take Down the Power Grid: http://www.internetevolution.com/author.asp?doc_id=136047&f_src =drnewsalert
[10] Network World, Experts hack power grid in no time: http://www.networkworld.com/news/2008/040908-rsa-hack-power-grid.html
[11] The Washington Post, TVA Power Plants Vulnerable to Cyber Attacks, GAO Finds: http://www.washingtonpost.com/wp-dyn/content/article/2008/05/20/AR2008052002354.html
[12] United States Government Accountability Office, TVA Needs to Address Weaknesses in Control Systems and Networks: http://www.gao.gov/new.items/d08526.pdf
[13] PC World, Lawmakers See Cyber Threats to Electrical Grid: http://www.pcworld.com/businesscenter/article/146153/lawmakers_see _cyber_threats_to_electrical_grid.html
[14] U.S. Nuclear Regulatory Commission, NRC begins special inspection at Hatch nuclear plant to review shutdown: http://www.nrc.gov/reading-rm/doc-collections/news/2006/06-016ii.html
[15] IEEE Spectrum, Software Update Brings Down Nuclear Power Plant: http://blogs.spectrum.ieee.org/riskfactor/2008/06/software _update_brings_down_nu.html
[16] The Washington Post, Cyber Incident Blamed for Nuclear Power Plant Shutdown: http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html
[17] B. Wollenberg, "Power Generation, Operation and Control," Wiley Interscience.

[18] M. Liu, "A Framework for Transmission Congestion Management Analysis," Ph.D.Thesis, Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign, 2005.
[19] P. Caro-Ochoa, "Evaluation of Transmission Congestion Impacts on Electricity Markets," M.S. Thesis, Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign, 2003.
[20] I. Dobson, K.R. Wierzbicki, J. Kim, H. Ren, "Towards quantifying cascading blackout risk," Bulk Power System Dynamics and Control-VII, Charleston SC USA, August 2007.
[21] Q. Chen and J. McCalley, "Identifying High-Risk N-k Contingencies for On-line Security Assessment," IEEE Transactions on Power Systems, Vol. 20, Issue 2, May 2005 pp. 823−834.

Matias Negrete-Pincetic received the B.S. degree in Electrical Engineering and the M.S. degree in Physics from the Pontificia Universidad Catolica de Chile in 2003 and 2005. Currently, he is a Ph.D. candidate at the Department of Electrical and Computer Engineering at the University of Illinois at Urbana-Champaign. His current research activities are in the areas of electricity market design and risk management in power systems

Felipe Yoshida is an exchange student in Prof. Gross' research group. He was an intern of the TCIP project at the University of Illinois during the summer of 2008. Currently, He is finishing his B.S. in Electrical Engineering at the Sao Paulo University at Brazil. His current research interest include cyber security, power system operations, and electricity market design

George Gross is Professor of Electrical and Computer Engineering and Professor, Institute of Government and Public Affairs, at the University of Illinois at Urbana-Champaign. His current research and teaching activities are in the areas of power system analysis, planning, economics and operations and utility regulatory policy and industry restructuring. His undergraduate work was completed at McGill University, and he earned his graduate degrees from the University of California, Berkeley. He was previously employed by Pacific Gas and Electric Company in various technical, policy and management positions