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