Cyber-Physical Systems Security for the Smart Grid

Alvaro A. Cárdenas
Fujitsu Laboratories of America
Email: alvaro.cardenas-mora@us.fujitsu.com

Ricardo Moreno
Universidad de los Andes, Colombia
Email: r-moreno@uniandes.edu.co

I. Introduction

The integration of Information Technology (IT) systems (computations and communications–the cyber world) with sensor and actuation data (the physical world), can introduce new, and fundamentally different approaches to security research in the growing field of Cyber-Physical Systems (CPS), when compared to other purely-cyber systems. In our earlier work [4, 2, 1, 3], we have shown that because of the automation and real-time requirements of many control actions, traditional security mechanisms are not enough for protecting CPS, and we require *resilient control and estimation* algorithms for true CPS defense-in-depth.In this abstract we outline how attacks and resilient mechanisms can affect and defend power grid operations.

II. Energy Management Systems

To characterize the CPS security of the power grid, we need to understand how IT is used in the control centers of the power grid to collect sensor data, estimate the state of the power grid, and issue control commands and pricing signals to the market.

One of the most important components in a control center is the Energy Management System (EMS). The EMS is responsible for many operational tasks. It includes the Network Topology Processor (NTP), state estimation, the market process that delivers Locational Marginal Pricing (LMP), and control actions for transmission automation, such as remote tap adjustment for transformers.

The role of NTP, and state estimation is to collect data from sensors in the field, and give an accurate view (topology and electricity flows). If the data collected is incorrect, operators will get an erroneous view of the system and all management functions of the control center will be affected, (including market computations and control actions). This is the reason why a lot of recent work has focused on deception attacks (also known as false-data injection), where a compromised sensor sends malicious data back to the EMS).

In this abstract we survey recent work on CPS security for power systems and present the work in a unified view by showing how all previous attacks are part of the EMS. We find some limitations with previous work and discuss open problems and new research challenges of parts of the EMS that have not been considered in previous work.

A. State Estimation

The state estimation problem in power systems originates from the need of power engineers to estimate the phase angles $x \in \mathbb{R}^n$ from the measured power flow $z \in \mathbb{R}^m$ in the transmission grid. It is known that the measured

power flow $z = h(x) + e$ is a nonlinear noisy measurement of the state of the system x and an unknown quantity e called the measurement error. To estimate x from this set of equations engineers make usually two simplifications: (1) e is assumed to be a Gaussian noise vector with zero mean and covariance matrix W, and (2) the equation is approximated by the linear equation

$$z = Hx + e$$

(where H is a matrix). Estimating x from these equations is achieved by computing the Minimum Mean Square Error (MMSE) estimate:

$$\hat{x} = (H^T W H)^{-1} H^T W z.$$

Because a typical transmission line system is composed of thousands of sensors (i.e., z is a vector of thousands of scalars) and not all sensors are reliable, power engineers have devised a set of tests to detect bad measurements. The tests are based on the following test:

$$||z - H\hat{x}|| > \tau \tag{1}$$

that is, if the measurement and the estimated measurement are greater than a threshold, then the test decides that there are some faulty sensors in the transmission line. If the test has a value lower or equal to τ then the test concludes that all measurements are correct.

Liu et.al. [8] introduced attacks against the integrity of state estimation algorithms in the power grid by showing that there are attacks where a compromised sensor can send a false measurement reading and yet the bad data detection test will not detect this attack. In particular, they show how by selecting an attack signal $z_a = z + a$, where $a = Hc$ (for any vector c) creates a successful attack. Then they analyzed how attackers can craft these attacks when they have different resources (limited access to meters or limited ability to compromise meters) and different objectives (random attacks or specific errors in the estimate). While attacks in larger systems are difficult to create (in an IEEE 3000 bus system the attacker needs to compromise more than 900 meters) and may have limited negative effects (the injected error might not be too large), the fact that attackers can manipulate the view of one of our critical infrastructures is a worrisome fact.

Some follow up work has discussed extensions on how to better protect the power grid to these attacks.

Some preliminary results in this area of research include the work of Dán and Sandberg [5], who consider a defender that can secure individual measurements by, for example, replacing an existing meter to a meter with better security mechanisms such as tamper resistance or hardware security support. Their goal is to protect the system under a limited budged and to that end they formulate the problem as identifying the best k measurements to protect (they assume the attacker cannot compromise these sensors) in order to minimize the impact of attacks. The mathematical problem they consider is a combinatorial optimization, so this problem is intractable for large systems. The main contribution of this work is to exploit the structure of the power system matrices to make the optimization problem efficient. Kosut et.al. [7] also extend the basic false data injection attack to consider attackers trying to maximize the error introduced in the estimate, and defenders with a new detection algorithm that attempts to detect false data injection attacks. Their new detection algorithm performs better than the traditional bad data detection algorithms (since these algorithms were designed for detecting faults, not network attacks). Their detection algorithm is based on the generalized likelihood ration test, which is not a tractable problem to solve.

B. Network Topology Processor

Each breaker in the transmission system has a sensor reporting if it is open or closed. This information is sent to the NTP to construct the topological model of the system. This topological model is used for the state estimation of the system. If the topology is wrong, the state estimation algorithm will also produce erroneous results.

As far as we know, no previous work has studied the false-data injection problem against the NTP.

C. Electricity Markets

The goal of the electricity market process in the control center is to deliver LMPs. LMPs are computed at each load and at each generation point when the transmission system is congested (which is the default state) to determine how much will utilities pay the system operator (per Megawatt), and how much will the system operator pay the generation points. LMPs are traditionally computed every 5 to 10 minutes, but there is recent work (e.g., New York power system) for computing LMPs in real-time.

Quantifying the cost of security incidents is one of the most difficult problems in computer security because it is hard to quantify the value of information. However, by analyzing attacks against the electricity market, we can quantify the effects of these attacks by leveraging the economic metrics used to measure the efficiency of the system.

As we mentioned before, if the state estimation is incorrect, all management functions of the control center are affected, including the market operations. Xie et.al. [15] studied how false data injection attacks can be used to defraud deregulated electricity markets by modifying LMPs. They consider the case where attackers can manipulate prices while being undetected by the system operator.

In all other attacks considered in this paper, the attacker can be implicitly assumed to be a malicious entity that tries to destabilize the system or reduce the social welfare. on the other hand, the work of Xie et.al., considers a *selfish attacker* instead of a *malicious attacker*. This change in the motivation of the attacker makes it difficult to understand which party will have the long-term motivation to launch these type of attacks. Utilities, generators, and system operators are large, highly regulated companies who have higher incentives to remain in business than to launch an attack that can put their company in jeopardy (in case it is discovered).

So far, all attacks presented in this abstract were based on false-data injection attacks against the sensor data used for state estimation. Negrete-Pincetic et.al [11] consider a new type of attacks by studying the integrity of the control signals (as opposed to the integrity of the sensor signals). In particular, they study how malicious control signals sent to circuit breakers (directing them to remove transmission lines from the system) affect the social welfare metric of the market system.

D. Transmission Automation

In addition to the control signals sent to circuit breakers, as considered by Negrete-Pincetic et.al., there are many other control signals that can be falsified by an attacker, in particular, given that the smart grid is introducing the capability of more distributed, automatic control.

The Flexible Alternate Current Transmission System (FACTS) includes many automatic electronic devices such as Static Voltage Compensators (SVC), which similar to capacitor banks, uses reactive power to improve the voltage profile of the system. Similarly, the Thyristor Controlled Series Compensator (TCSC) is

a control devices in series with a transmission line which can be used to modify its impedance to control the current going through these lines. A taxonomy of attacks against FACTS devices was presented by Phillips et.al. [12] and an implementation of some attacks with false status reports and control actions showed unnecessary VAR compensation and unstable operation of the sytem [14]

Other control signal that can be sent remotely include tap adjustments for smart transformers (used to increase or decrease slightly the voltage on each side of a transformer), and the Automatic Generator Control (AGC) signal (which is used to set the voltage of generators). Robust attack policies have been studied for AGC signals [9, 6], and attacks have shown that if you modify the frequency and tie-line flow measurements, the system can be driven to abnormal operating values [13].

III. Defense Mechanisms

In addition to traditional IT security mechanisms for prevention (authentication, encryption, firewalls) and detection (intrusion detection systems, forensics) we need new CPS security mechanisms.

There are several CPS planning and defense mechanisms that can leverage knowledge of the attacks presented in this abstract. The first is *risk assessment*: given a fixed budget, where should I allocate this budget to minimize my potential *physical* damages?

A second mechanism is *bad data detection* mechanisms. These mechanisms should not assume random, independent failures, but consider detection of sophisticated attackers. Interestingly enough, most previous work has focused on attacks and the quantification of these attacks, but very few have proposed novel attack-detection mechanisms [7]. One particular open problem is to propose *bad topology detection* mechanisms.

Replacing sensed data with false data (a deception attack) is a very generic attack that can be extended to any smart grid application (as all of them are based on correct sensor measurements). It is important to develop intrusion detection mechanisms or reputation management systems for smart grid applications where not all received data can be trusted.

The defense third mechanism is to introduce *resiliency* (or survivability) of the system to attacks. A promising direction is to design the topology of the power distribution network to withstand malicious commands to circuit breakers trying to change and disconnect the network [10].

IV. Conclusions

CPS security is a growing field critical for the vision of a survivable power grid that can withstand attacks and reconfigure or adapt to mitigate adverse effects.

Work on fault tolerance and reliability of control systems is not enough, because these mechanisms generally assume independent and uncorrelated failures; however, cyber-attacks will exploit vulnerabilities in a coordinated and correlated fashion. The most basic example is the work of of false-data injection attacks [8], where it is shown that traditional safety and fault-detection mechanisms currently available in the power grid cannot detect incorrect sensor data when a malicious attacker is the source of these errors.

Therefore instead of relying solely on fault-detection algorithms to protect control algorithms in the power grid, we need to develop new attack-detection algorithms focusing on identifying malicious data in sensor and actuation devices in the power grid.

REFERENCES

[1] S. Amin, A. A. Cárdenas, and S. S. Sastry. Safe and secure networked control systems under denial-of-service attacks. In *HSCC '09: Proceedings of the 12th International Conference on Hybrid Systems: Computation and Control*, pages 31–45, Berlin, Heidelberg, 2009. Springer-Verlag.

[2] A. Cardenas, S. Amin, and S. Sastry. Research Challenges for the Security of Control Systems. In *3rd USENIX workshop on Hot Topics in Security (HotSec '08). Associated with the 17th USENIX Security Symposium.*, July 2008.

[3] A. A. Cárdenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, and S. Sastry. Attacks against process control systems: risk assessment, detection, and response. In *ASIACCS '11: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, pages 355–366, New York, NY, USA, 2011. ACM.

[4] A. A. Cardenas, S. Amin, and S. Sastry. Secure control: Towards survivable cyber-physical systems. In *Proceedings of the First International Workshop on Cyber-Physical Systems.*, June 2008.

[5] G. Dán and H. Sandberg. Stealth Attacks and Protection Schemes for State Estimators in Power Systems. In *First IEEE Smart Grid Commnunications Conference (SmartGridComm)*, October 2010.

[6] P. Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson. A robust policy for automatic generation control cyber attack in two area power network. In *Decision and Control (CDC), 2010 49th IEEE Conference on*, pages 5973 –5978, dec. 2010.

[7] O. Kosut, L. Jia, R. Thomas, and L. Tong. Malicious Data Attacks on Smart Grid State Estimation: Attack Strategies and Countermeasures. In *First IEEE Smart Grid Commnunications Conference (SmartGridComm)*, October 2010.

[8] Y. Liu, M. K. Reiter, and P. Ning. False data injection attacks against state estimation in electric power grids. In *CCS '09: Proceedings of the 16th ACM conference on Computer and communications security*, pages 21–32, New York, NY, USA, 2009. ACM.

[9] P. Mohajerin Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson. Cyber attack in a two-area power system: Impact identification using reachability. In *American Control Conference (ACC), 2010*, pages 962 –967, 30 2010-july 2 2010.

[10] R. Moreno and A. Torres. Network Topological Analysis to Assess the Power Smart Grid. In *2012 IEEE Innovative Smart Grid Technologies (ISGT) Conference*, January 2012.

[11] M. Negrete-Pincetic, F. Yoshida, and G. Gross. Towards quantifying the impacts of cyber attacks in the competitive electricity market environment. In *2009 IEEE PowerTech*, June 2009.

[12] L. Phillips, M. Baca, J. Hills, J. Margulies, B. Tejani, B. Richardson, and L. Weiland. Analysis of operations and cyber security policies for a system of cooperating flexible alternating current transmission system, Dec. 2005.

[13] S. Sridhar and G. Manimaran. Data integrity attacks and their impacts on SCADA control system. In *Prc. IEEE Power Energy Soc. General Meeting*, Jul. 2010.

[14] S. Sridhar and G. Manimaran. Data

integrity attack and its impacts on voltage control loop in power grid. In *Prc. IEEE Power Energy Soc. General Meeting*, Jul. 2011.

[15] L. Xie, Y. Mo, and B. Sinopoli. False Data Injection Attacks in Electricity Markets. In *First IEEE Smart Grid Commnunications Conference (SmartGridComm)*, October 2010.