Preserving Confidentiality of Power System Information
Position Statement for 2013 National Workshop on Energy Cyber-Physical Systems

Bernard C. Lesieutre (lesieutre@wisc.edu)
University of Wisconsin-Madison

The electric power grid is one of the nation's critical infrastructures and there is considerable concern about its vulnerability to malicious physical and cyber attacks. It constitutes a closely coupled cyber-physical system in which the grid that literately spans the continent is controlled at relatively few discrete locations using dedicated computing facilities that rely on accurate sensing and communication networks. The core computational functions of control centers are to estimate current grid conditions, make adjustments for reliability and for economic optimal use of controllable resources, and to anticipate future disturbance scenarios that may risk blackouts. Event security analyses are run continuously, and optimal economic dispatch programs result in system adjustments on a timescale of every five minutes for some markets. These computational tasks all involve a sophisticated analysis of a large nonlinear model of the electrical network represented by the power flow equations.

There are many aspects of this cyber-physical network that can be examined in terms of vulnerabilities and network security. Much work can and has been done on examining the vulnerabilities to the physical infrastructure, and considerable research has been directed toward understanding cascading outages resulting in blackouts. Our research focuses on the topic of maintaining secure information about the power network that is used in the computing environment that controls the grid. Understandably, the detailed data describing grid topology and components is considered sensitive and can only be shared through a Critical Energy Infrastructure Information (CEII) nondisclosure agreement. This tightly controlled access to power grid information limits advances in power system research and in power system operations. Researchers who work with the data must mask their results in publication, and other researchers cannot openly and independently verify their results. Similarly the care and control of critical information requires security safeguards when using powerful shared computing platforms such as cloud computing.

Our initial research to date has focused on a linear power system representation that is commonly used in optimization problems associated with electricity markets. We have demonstrated that recently developed approaches for masking optimization programs to enable secure use of cloud computing do apply to these power system models. Through a transfer of variables, the structure and form of the model can be masked before sending to the cloud for analysis. In related work, but with a different focus, we have developed a means to transform a power system optimization problem to another different power system optimization problem. The ultimate purpose of this structure-preserving approach is to enable the sharing of like-models among researchers to allow the verification of methods and results. This is achieved by using system models that are provably equivalent to true, critical infrastructure system models through a transformation only known to the transformer. Ideally this will lead to a set of publicly available standard models for use in research.

We are continuing our current work to include nonlinear power system models, and we are expanding to perform the masking of more electricity market data and representation. Specifically we address the need for multi-party optimization that hides specific party economic and network information. This is intended, in part, to enable the joint optimization of microgrids, RTOs, and other participants in an entirely secure market.