Journal of Telecommunications System & Management

Tan, J Telecommun Syst Manage 2014, 3:1
DOI: 10.4172/2167-0919.1000e110

Editorial Open Access

Cyber Security Research in Smart Grid

Song Tan*

Georgia State University, GA, USA

Background

Power grid is the most fundamental and complicated artificial system in human society. With the help of the emerging information technology, the legacy power grid is evolved along the journey to Smart Grid, which leverages the cyber infrastructure within power system for sensing, control, computation and communication, in order to achieve self healing, resilience, sustainability and efficiency. However, the beauty of the Smart Grid innovation comes with its danger: the integration and dependence on cyber infrastructure would greatly increase the risks of cyber attacks, which becomes a key concern with increasing urgency for research community.

Smart Grid

A smart grid is an electrical grid that uses information and communications technology to gather and act on information, such as information about the behaviors of suppliers and consumers, in an automated fashion to improve the efficiency, reliability, economics, and sustainability of the production and distribution of electricity. It is characterized by the two-way communications of data and control signal, large scale penetrations of renewable energy, and the complex interactions of distribution systems with distributed generators, energy markets, and customer behaviors. The implementation of smart grid requires solving a lot of challenging research issues, such as demand response, dynamic pricing, renewable resource integration, security control, sensing and automation.

Cyber Security in Smart Grid

The Smart Grid vision is being realized through the implementation of cyber infrastructure overlaying the legacy power network. The cyber infrastructure enables the collection and analysis of data from millions of distributed end-points such as smart meters, sensors, automated control devices. The functions of SCADA system, substation networking, phasor measurement units, cloud-based load aggregation and demand response services, all rely on a secure and robust cyber infrastructure, which are critical to all aspects of Smart Grid. The cyber vulnerabilities increase the risks of cyber attacks within Smart Grid. It might allows the attackers to intrude the communication network, acquire access to critical control routines, and even manipulate the meter measurements, load conditions and system parameters to destabilize the power system in unpredictable ways. The cyber security for Smart Grid should explore the methodologies to reduce the risk of threats, increase the ability to detect and identify system anomalous behaviour and intrusions in proactive way, and respond and initiate countermeasure quickly to mitigate the effects and restore the system operations rapidly. The nature of threats and vulnerabilities are constantly changing, so application of best current practices for cyber security is necessary but not sufficient – ongoing research and development of new cyber security technologies and methods is essential.

Cyber Security Research in Theory: Attacking Strategies and Countermeasures

Now let's talk about the specific research problems with respect to cyber attacks in Smart Grid. On one hand, since the cyber infrastructure of Smart Grid will not be designed from scratch, but needs to reuse the existing available technologies, the traditional network security research problems would still exist and be valuable within Smart Grid scenario. The attacks against communication protocols, encryptions and decryptions, key distribution and authentication mechanisms are the cornerstones in this category. On the other hand, a newly proposed category of cyber attacks, data integrity attacks, draws more attention to the research community. This category of attack explores and exposes the vulnerability of the bad data detection techniques in the state estimation process within power system. State estimation is a key system monitoring process to get the best estimates of unknown system state variables based on the measurement data. By strategically manipulating the data from analog measurement meters and digital controllers, the attackers from this category could perturb the power system state freely, while without being detected by the existing bad data detection techniques. Such an attack could result in a significant effect on the physical environment and the real time electrical market.

The countermeasures for the first kinds of attacks are usually based on the anomaly detection. Machine learning, data mining or optimization problems are formulated. For the data integrity attack, meter placement is the popular direction. By arranging the meter in specific ways and securing the critical measurement devices, the system observability is kept intact and become more resilient. Distributed robust state estimator is also a potential research direction worth exploring since bad data would be unavoidable when the volumes of data become quite large.

Cyber Security Research in Practice: Experiment Platform

Another important aspect of Smart Grid cyber security research is the experiment platform to demonstrate, validate and verify the proposed ideas of cyber security, either for education purpose or research purposes. Due to the system complexity, typically the high cohesion of communication and power system, and the reliability and integrity requirements of power grid, demonstrating and validating cyber attacking strategies and countermeasure of Smart Grid are not easy jobs, which bring lots of research challenges.

The existing works to solve the problem are generally focused on two categories: hardware platforms and software simulation platforms. The hardware platform approach achieves high fidelity by employing dedicated devices as part of the test beds. For example, remote terminal unit and Ethernet switch can be integrated within the test beds, to achieve the hardware-in-the-loop testing. However, the problems with the hardware platforms are that since the dedicated hardware are the integral parts of the test beds, they cannot be easily accessed

***Corresponding author:** Song Tan, Georgia State University, GA, USA, Tel: 4043741915; E-mail: stan@cs.gsu.edu; songtancs@gmail.com

Received February 25, 2014; **Accepted** February 25, 2014; **Published** March 02, 2014

Citation: Tan S (2014) Cyber Security Research in Smart Grid. J Telecommun Syst Manage 3: e110. doi:10.4172/2167-0919.1000e110

and used by the public research community and difficult to be scaled when the test case becomes quite large. Software simulation platforms, on the other hand, achieve better availability, usability and scalability. They usually combine multiple simulation tools, typically a network simulator and an electric power grid simulator, and a middleware is used to exchange messages periodically and synchronize all the simulators. However, since simulation typically abstracts the operating system, communication protocols and power dynamics into various mathematical simulation models, it can only duplicate the behavior and structure of the system, but not the execution environment of critical control programs.

Conclusion

The cyber security is a key concern for the Smart Grid innovation. From theory perspective, the attacking strategies and countermeasures are worth further exploring. From practice perspective, the experiment platform for validating the ideas is also important. I believe both of them are the valuable research directions for the research community.