Cyber Security for the Smart Grid: Issues and Possibilities

Valentin Tudor, PhD Student, Department of Computer Science and Engineering, Chalmers University of Technology, SE–412 96 Gothenburg, Sweden
tudor@student.chalmers.se, tudor.d.valentin@gmail.com

Abstract:

The traditional electrical grid is transitioning into the smart grid, where devices are equipped with sensors, processing units and two-way communication to simplify the process of monitoring and managing the grid. As such, the smart grid will bring many possibilities through new types of functions but there are also open issues to be solved before the new system is robust and reliable. One challenge is the cross-disciplinary nature of the smart grid where expertise in both Electrical Engineering (EE) and Information and Communication Technology (ICT) is needed.
To illustrate, we make a cross-domain study to investigate how problems in the ICT domain (new functions coupled with security weaknesses) can influence the EE domain (the power quality) as the following example shows.
In the center are the smart meters in a small neighbourhood. The smart meters are replacing the traditional electrical utility meters, offering new functionalities such as remote reading, automatic error reporting, and the possibility for remote shutoff. Although the communication between the smart meter and the control center is presumed to be secure, previous studies have shown that there may be methods to circumvent the security measures in place. A perpetrator could thus gain confidential information about customers behaviour (energy consumption patterns, periods when there is no one at the residence, information about appliances connected to the grid) or even cause a disruption of the energy delivery service by exploiting the remote shutoff function. Concentrating on the remote shutoff function, we simulated the effects on the grid in a small neighbourhood, assuming that a potential perpetrator manages to take control of the smart meters and can issue the remote shutoff command. Thus, the attack in itself comes from the ICT domain, through the new communication and processing possibilities in each meter, while the effects are seen in the EE domain through the variation in power quality.
In this particular example, we emphasize how the need for security but also other areas in the ICT domain plays a major role in the smart grid, such as distributed computing. The smart grid amasses massive volumes of distributed data, which, in the scenario above, could possibly be used to mitigate the effects of the attack by collecting and processing this data in an effective manner. Data collected in the smart grid is sensitive (it can divulge confidential information about the behavior of the dwellers – already mentioned above) so in parallel we investigate ways to anonymize parts of it (like smart meters serial numbers or IDs) so it can be used for research purposes without tracing back to the original smart meter that produced it.

Acknowledgement: Part of the work has been done in collaboration with Mihai Costache, Magnus Almgren, Marina Papatriantafilou and Christopher Saunders, see Costache, Mihai; Tudor, Valentin; Almgren, Magnus; Papatriantafilou, Marina; Saunders, Christopher: *Remote control of smart meters: friend or foe?*. European Conference on Computer Network Defense (EC2ND 2011), pp. 49-56.