Position Statement: Resilient Coordination and Control in Smart Grid Networks

Xenofon Koutsoukos
Institute for Software Integrated Systems (ISIS)
Vanderbilt University
Xenofon.Koutsoukos@Vanderbilt.Edu

The Smart Grid is an emerging distributed Cyber-Physical System (CPS), which should revolutionize the way in which energy is produced, distributed, stored, and consumed. It should provide benefits to all stakeholders. Customers should be able to benefit from the lower energy prices as well as from the capability of Smart Appliances (SA) to adjust dynamically to daily price fluctuations. Providers can benefit because they can buy and resell electricity produced at the customer site. Coordinated energy usage by multiple SA can reduce the energy spikes, thus reducing requirements and related. All this should support sustainable growth of the industry and reduce environmental impact.

In order to accomplish these tasks, beyond the physical grid infrastructure, an extensive logical connection and coordination between all involved components is needed. Coordination can be performed using various networks, both physical and overlay, which also exhibit various levels of dynamic behavior. Smart grid networks are expected to resemble scale-free networks with mesh-like core and tree-like topologies closer to the end customers, e.g., in the Home and Building Area Networks. With exception of the Smart Appliances, which can join and leave the network comparatively often, network topologies evolve slowly in time, and can be considered as static.

The overall system dynamics emerges from the interaction among power networks, communication networks, and information networks. Coordinated network interactions can potentially increase effectiveness and resilience. In the current state of the art, these interactions are not well understood, and system capabilities do not achieve the optimum. The capability for maintaining resilient operation with dynamic reconfiguration across multiple networks based on information of questionable heritage is a major issue. Current research has the potential to address some of these individual issues in isolation. However, managing the complex interactions to optimize resources and to mitigate adversarial actions require a holistic systems view that builds on and exploits of inter-layer optimization.

As part of the NSF CPS Frontier project on Foundations Of Resilient CybEr-physical Systems (FORCES), we investigate methods for resilient coordination and control of electric power distribution and consumption networks. We consider attacks to devices (and interconnected communication links and we are aim at developing a formal integrated taxonomy of attacks, with emphasis on the interdependencies between malicious attacks and random faults. A key problem in attack detection and isolation is to diagnose attacks when the attacker injects false data to sensor-control signals in order to compromise the system performance, and yet evades detection. Our goal is to improve the performance of diagnostic schemes by including models of the underlying physical dynamics. Our approach integrates the theory of robust and distributed control with practical IT security. The inclusion of security and resilience specifications at the design stage permits us to provide quantitative guarantees for time-critical system properties, such as safety, stability, and optimal performance of closed-loop dynamics for a wide-range of scenarios in the face of new and emerging attacks.

Our initial work focuses on resilient distributed protocols in Building Area Networks (BAN), whose network and overlay topologies are trees. As Smart Appliances, which are leaf nodes in these trees, are owned by the end customers as well as exposed to the unrestricted physical access, it is reasonable to assume that they can be rigged. Therefore, protocols resilient to the false information provided by leaf nodes are needed.