Securing the Power Grid with Collaborative Embedded Intelligence

Hairong Qi[1], Leon Tolbert[1], Fangxing (Fran) Li[1], Xiaorui Wang[1], Kevin Tomsovic[1], Fang Z. Peng[2], Peng Ning[3], Massoud Amin[4]

[1]EECS Department, University of Tennessee, Knoxville, TN 37996
[2]ECE Department, Michigan State University
[3]Peng Ning, CS Department, North Carolina State University
[4]Massoud Amin, ECE Department, University of Minnesota

1 Introduction

In a large interconnected power system, security is primarily focused on transient and dynamic stability considerations and intentional attacks are likely to fall within only a few domains of influence upon the grid. Many of the scenarios manifest as equipment failures caused by physical equipment damage/failures, interruption of the communication network, and/or mis-feeding of information. On one hand, the physical interconnection can provide a check on the cyber system should communications be compromised. If system response based on received data is counter to expectations, a device may be able to conclude a security breach. Physical laws govern the power flow in the grid and these cannot be compromised. For example, if control actions such as increasing reactive power output are observed to decrease voltage then the observation is either erroneous or the system has reached such an extreme and unusual state that normal control laws are no longer effective. In this way, control provides feedback for detecting and isolating an attack on the information flow. On the other hand, power systems can also fail through the physical interconnection even if the communication system is secure. For example, a generator, or group of generators, whose controller has been compromised can act in a way to destabilize other units, say by excessive response to minor load fluctuations. Information feedback and collaboration with properly functioning generators units may allow the system to isolate the offending unit and the system to continue to operate. In this way, *both the physical system and the cyber system can act together to help assure system security.*

The power grid is a typical example of cyber-physical systems (CPS) of highly interacting subsystems. Solving these fundamental problems to create a resilient grid has a direct and immediate impact on *this and other critical infrastructure*. To a large extent, security of cyber-physical systems can be modeled as inverse problems where either past states/parameters of the physical system are pursued or a future state is desired based on the steer of present states or parameters. When the inverse problem is ill-posed, regularization methods are usually adopted which would lead to a stable solution under certain constraints. Most existing security solutions only search for constraints in the cyber domain. We argue that an effective solution should be pursued using both cyber constraints and physical constraints of the system. From this point of view, a solution should be based on, first of all, an accurate, just-in-time understanding of the current state of the system, and secondly, local coordination of system components for the incorporation of both physical and cyber constraints.

To achieve better understanding of the system state, higher sensing resolution needs to be implemented at the lower level of the system where direct interactions with the physical system take place. In the meanwhile, intelligence needs to be pushed toward these lower level devices situated at the edge of the system where feasible, allowing local devices to have the capability to make decisions and to react more quickly to contingencies, enabling a more direct reconfiguration of the *physical* makeup of the system, as compared to current (e.g., software-only) approaches. The recent “Smart Grid” initiatives would lay the ground for high-resolution sensing but research on embedded intelligence for faster reaction at the local device level still has a long way to go. On the other hand, to make local intelligence more reliable and to improve the accountability of local decisions, collaboration among neighboring devices is needed in order to assert constraints from geographically-close devices to regulate the decision making process and to handle possible faulty, missing, or incomplete information. In addition, control-theoretic adaptation strategies can be applied for assurance in providing desired dynamic responses to unpredictable system changes and for efficiently maintaining the availability of large distributed systems.

2 Technical Approach

We discuss a proposed structure for a secure reconfigurable system supported by fault-resilient real-time controls to quickly respond to both natural and intentional attacks to the power grid. We expect a resilient reconfigurable power grid to incorporate both *local actuation, supported by devices with embedded intelligence*, and *central system-level adaptation, supported by control-theoretic security solutions*.

2.1 The Threat Model

For convenience, we refer to the entities in a power grid as *system components*. The adversary may certainly launch *external attacks* against the system. Specifically, the adversary may passively intercept the messages exchanged between the system components, actively inject forged messages, or modify messages being transmitted. However, we assume there are communication security mechanisms (e.g., message encryption and authentication) that can handle such threats to a certain extent. Moreover, the adversary may launch Denial of Service (DoS) attacks to disable some system components (e.g., physically destroy a power generator) or the communication between them (e.g., cut the communication line, flood the system with a large number of messages). The adversary may also attempt to delay the communication between system components, aiming at preventing them from meeting certain real-time requirements. However, we assume the adversary cannot disable/delay *all* the system components and communication channels. The adversary may also launch *insider attacks*. Specifically, the adversary may compromise and completely control some system components, and use them to attack the rest of the system. However, we assume the adversary cannot control *all* the system components. The adversary may partially compromise the communication security. For example, the adversary may learn the cryptographic keys shared between some devices and thus can forge malicious messages. However, we assume the adversary can compromise only a portion of the secure communication links.

It should be noted that conventional US power system operations is typically performed with the consideration of N-1 security, where an N-1 contingency means one component (or one set of closely related components) fails. In addition, some regions of the US power system are designed to handle a few critical N-2 or even N-3 contingencies (i.e., simultaneous failures of 2 or 3 components) with the assistance of post-contingency remedial actions. Nevertheless, under the post-9/11 environment, simultaneous coordinated strikes have become a realistic threat, which could lead to N-x operations under emergency. This will put the interconnected power network in greater danger than the power system planners had envisioned.

2.2 Multiple Lines of Defense

The proposed approach studies a systematic solution to fault prevention, detection, and mitigation, providing multiple lines of defense that are specifically tailored for the power grid, with potential generalization to other complex systems. *First of all*, the proposed location-centric hybrid system architecture facilitates the realization of fault prevention, detection, and mitigation at various levels with various degrees of collaboration. *Second*, although there might be different ways to attack the system, the net result is always reflected as voltage, current, and/or frequency changes. Accurately detecting this change (or potential fault) and making quick adjustments at each device level, before it propagates, provide the first line of defense. *Third*, the practice of robust collaboration among neighboring devices and distributed processing schemes at the local level provide the second line of defense in its ability to prevent isolated attacks from propagation and detect and mitigate coordinated attacks. *Fourth*, a control-theoretic adaptation framework at the system level provides the last line of defense, protecting the system from collapse by desired dynamic responses with analytical assurance.

2.3 System Architecture

We first examine the existing power grid infrastructure which basically adopts a centralized control scheme. As shown in Figure 1a, from top to bottom, the control center hosts critical power security analysis modules, such as contingency analysis (CA), based on the input from the state estimation (SE) module, which, in turn, processes raw data sent from RTUs located at various substations. The control center could also issues commands to adjust behaviors of relays and local power electronic devices, including FACTS and DGs that have recently begun to be deployed. Since there is NO direct communication between substations, these devices can only make isolated decisions even though they may be equipped with the communication capability to respond to the control center. Similarly, at the distribution layer, where multiple devices usually reside and could be equipped to respond to say a microgrid energy manager, there is no communication among DGs, let alone DGs across different substations.

Figure 1b illustrates the proposed *location-centric hybrid* architecture, for a reformed power grid. It differs from the existing power grid from four aspects. *First*, both FACTS and DG are embedded with an intelligent controller that makes decisions based on collaborative information from critical peers. *Second*, two levels of collaborations are enabled, one is among DGs within the same area, the other is among FACTS devices across geographically adjacent substations. The location-centric collaboration provides effective mechanisms for preventing isolated attacks and detecting and mitigating coordinated attacks. *Third*, the SE module is not run at the control center. Instead, a distributed execution of SE (DSE) is performed at each substation, only the results from which are integrated at the control center. This way, the time- and resource-consuming SE execution can be distributed to multiple substations and the DSE module could provide feedback to local devices to contain faults locally before it unravels. *Finally*, a control-theoretic adaptation scheme is adopted to help maintain grid stability under attacks, providing another level of protection of the grid.

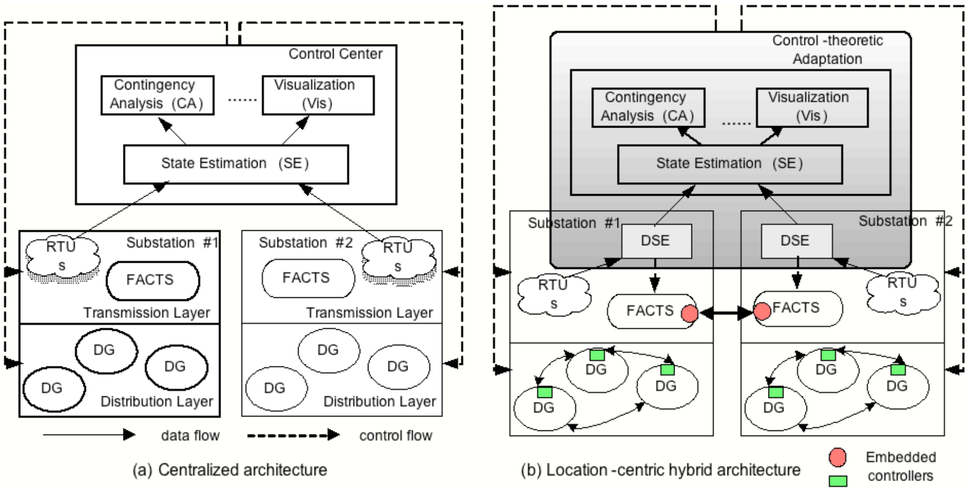

Figure 1. System architecture of the power grid information management – A comparison.

3 Summary

Energy infrastructure is a critical underpinning of modern society where any compromise or sabotage of its secure and reliable operation has an enormous impact on people's daily lives and the national economy. The tragic events of September 11th 2001 have focused new attention on security of infrastructure in the United States. The massive northeastern power blackout of August 2003 and the most recent Florida blackout (February 2008) both highlight the importance of reliable operation of the electric power system. These blackouts have revealed serious defects in both system-level management and device-level designs of the power grid in handling attacks (external or internal, intentional or naturally-occurred, isolated or coordinated). Escalating demands for electricity coupled with an outdated power transmission grid pose a serious threat to the US economy. This threat has significantly increased in recent years because the system is operating closer to its capacity and because terrorist attacks are no longer hypothetical. The proposed research that incorporates constraints from both cyber and physical systems would help secure the grid and prevent potential outages.