Impediments to Survivability of the Electric Power Grid and Some Collaborative EE-CS Research Issues to Solve Them

David Bakken, Anjan Bose, Curtis Dyreson, Sudipto Bhowmik,

Ioanna Dionysiou, Harald Gjermundrod, Lin Xu

School of Electrical Engineering and Computer Science
Washington State University
Pullman, Washington 99164-2752 USA
{bakken,bose,cdyreson,sbhowmik,idionysi,kgjermun,lxu2}@eecs.wsu.edu

1 Introduction

The electric power industry by its very nature must have its supply and demand in very close balance at all times. Supply (generation) needs to be matched accurately and in real-time to demand, otherwise unbalance can result in partial or complete breakdown of the grid [1].

Recent deregulation is allowing many more participants in the power grid. Unfortunately, its status dissemination network was designed for the handful of regulated monopolies of the day, and by engineers who were not experts in computer networking or distributed systems. The monopoly in generating, transmitting and managing power that was present at design time is therefore reflected in the present hardwired control infrastructure of the power grid (see Figure 1). As this is changed to accommodate the new diversity and scale of participants in the power grid, accessing and delivering its real-time and historical data to interested parties must be done reliably and fast without jeopardizing the grid itself.

The power grid also was designed to handle a limited number, type, and geographic proximity of failures. Because of this, failures at one of many points within the grid have the potential to severely degrade the communication necessary for its control. Further, electric power is at risk not only because of the possibility of unintentional failures, but also due to another form of threat, deliberate cyber attacks. Indeed, Paula Scalingi, director of the DOE's Critical Infrastructure Protection Office, noted in [2]:

> The terrorists in the September 11 event had the patience to plan (and) the foresight and the understanding of the infrastructure that could be used to simultaneously or sequentially disrupt the infrastructure electronically and that could cause a major regional failure in this country. There's no question that that's doable…. Communications were one of the first things to go.

Numerous others have noted similar concerns, both before and after September 11, and some have even demonstrated these vulnerabilities beyond reasonable doubt.

We believe that many of these impediments to the survivability of the power grid can be removed with concerted research involving genuine collaboration between researchers and engineers in both electric power and distributed computing systems (including networking, fault tolerance, and computer security). In this position paper we outline four key areas for such collaborative research, and overview research we are conducting in this area, in the hope of stimulating more such research and its transition to the power grid.

2 Open Research Issues

In order to build a more survivable electric power infrastructure, it is essential that research be performed in the following four synergistic areas, which we overview in turn below:

1. Quantifying the effect of degraded communications on grid stability
2. Developing new ways to exploit new technologies in computer networking and distributed systems to provide better control of the grid, both in normal operations and with degraded communications due to failures or attacks

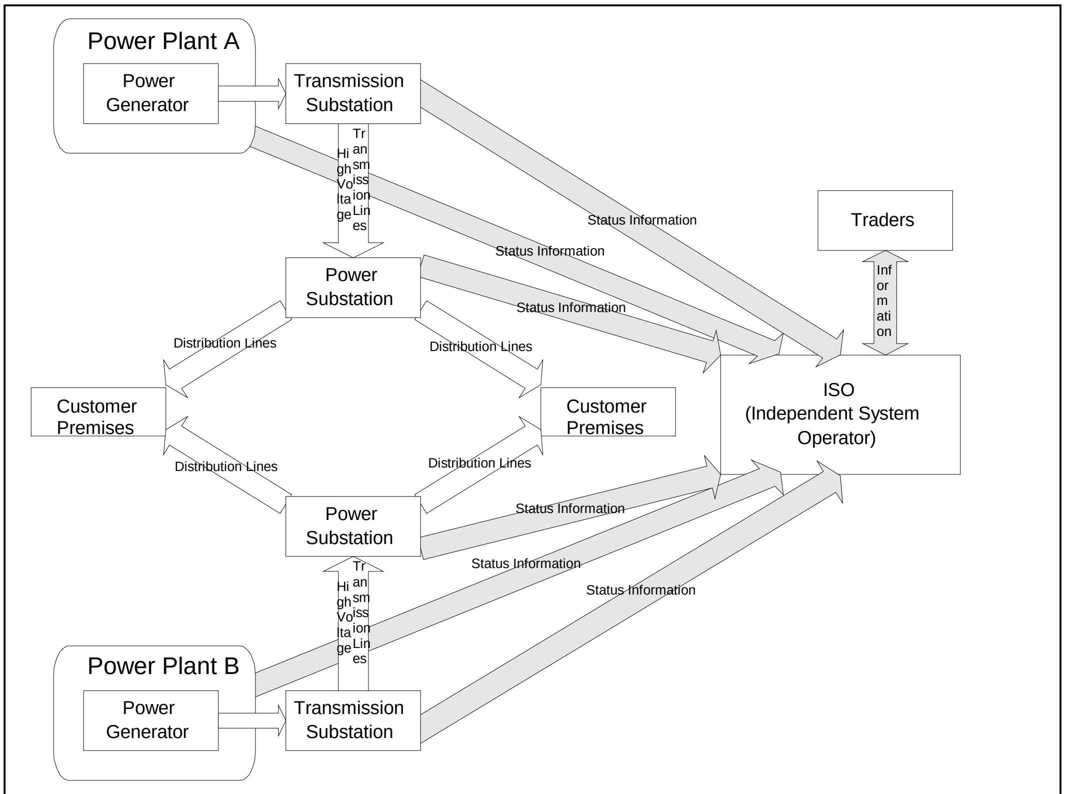

Figure 1: Power Grid Information Infrastructure Example

3. Devising new ways to disseminate status information to a much wider set of parties and in a more survivable manner
4. Devising new ways to organize, classify, query, and use existing status information

Effective research in these areas requires close collaboration between power system researchers and distributed computing. Sadly, genuine collaboration is rare at universities, because the former are typically in electrical engineering departments while the latter are usually in computer science departments. Effective means of fostering such genuine collaboration are thus also required.

2.1 Effect of Degraded Grid Communications

As the process of deregulation in the power industry is implemented, increased dependence on an improved communication infrastructure will be felt for effective operations. The role of data communication in the power system industry will increase and a thorough research of all its implication is becoming mandatory. Current research in this aspect is still at its infancy, as the data communication infrastructure was (barely) adequate to meet all needs in the centralized system (if few or no failures occurred). Much more research is needed to quantify the effects of the effect of degraded communications on the survivability and stability of the power grid, because this is a major prerequisite to enable the designing of an improved grid communications infrastructure.

2.2 New Communications Technologies and Grid Control

The power grid's control algorithms are based on status information delivered with very old networking and distributed systems technologies used in very simplistic ways. Advances in recent years offer the very tangible hope to provide better control of the grid exploiting these technologies. However, to do so new control algorithms and broad theoretical underpinnings must be devised.

The new technologies offer hope of improvements in two situations: normal operations and when communications degrade due to attacks or failures. In normal operations, better status information (more timely, more reliable, more quantity, etc) can help the grid operate in the normal steady-state case where there are presently no anomalies in either the power grid or its communication infrastructure.

Given that communications may be degraded in the presence of unintentional failures or deliberate attacks, it is only prudent to devise new ways of controlling the power grid in the face of higher delays and missing status updates to the control centers. This is essential to meet the grid security and reliability standards. Ways to achieve this with increased communication technology needs to be studied. Market economic factors also have to be taken into account while performing this, as eventually that is the pertinent factor in all transactions in an open market. Very little research has been done in this area as of now.

2.3 Status Dissemination

Increased competition and open access to all key players begets a way to disseminate all the relevant information to the participating players, rethink current control scheme, allow ways to join and leave participating groups etc. NERC (North American Electric Reliability Council) and FERC(Federal Energy Regulatory Comission) have set reliability parameters which can only be met with a substantial improvement in the current communication.

Further, with the rapid growth of the microprocessor-based secondary equipments (such as protective relays, digital fault recorders, etc.), there are more and more communication-enabled devices exists in the power system, especially in the substations. This kind of intelligent electronic device (IED) usually makes much more status data available [3]. However, since different IEDs' vendors might have incompatible communication protocol, and most IEDs only allows direct connection to the personal computer for configuration or diagnostics proposes, their potential to provide useful status information is greatly limited by the current configuration. Thus each IED is turning to an isolated data island. The EPRI is trying to standardize the communication protocols, and UCA (Utility Communication Architecture) is under development. The working status of the UCA can be found in [4].

Additionally, as mentioned earlier, the power grid's hardwired and inflexible infrastructure does not allow decentralization of any information flow other than to the ISOs, which manage exclusively the power distribution grid for specific regions. Recent advances and regulatory reformations in the electric power industry start promoting competition by allowing independent power producers and transmission companies to enter this monopolistic industry. The new services that are emerging require status information dissemination to a wider set of parties, something that is currently unavailable due to the present grid communications infrastructure. What is needed is a status service that will circulate information to legitimate parties. Further, we believe that this infrastructure needs to handle a much greater degree of heterogeneity (diversity) in the kinds of devices, producers of status information, consumers of status information, usage patterns of status information, etc. We believe that a category of software called middleware [5] is especially well suited for supporting the required heterogeneities.

2.4 Utilizing and Classifying Available Status Data

Delivering status data to interested parties is a challenging problem because the data must be integrated from a *heterogeneous* pool of sources. By heterogeneous we mean that the sources of data can have different *meta-data* for the same kinds of data. Meta-data is the schema, naming conventions, and measurement units for the data. Decentralization tends to increase meta-data heterogeneity. But if meta-data can be integrated then consumers of the data can utilize the entire pool of data through a single, homogenous portal. Further, more support for recording anomalies based on complicated temporal relationships between varied status items is necessary, because they can be early warning indicators of anomalous conditions. However, support for such temporal analysis is rudimentary or nonexistent today. Finally, support for querying status data that is current, as well as recent and historical data, is necessary for forensic and legal (liability) reasons.

3 Ongoing Research at WSU

WSU electrical engineers and computer scientists in the School of Electrical Engineering and Computer Science have started working on the above areas in close collaboration. We outline ongoing research and recent results in these areas.

The need for increased communication infrastructure in a distributed scenario was demonstrated in [6]. It broadly quantified the requirements and the effects of communication delays in the traditional Automatic Generation Control scheme. The work also established that there are new data security requirements to ensure effective control of generation to meet the load demand as well as safeguard privacy of electric generation company data.

New control schemes to counter the effects of the delays introduced by the communication network are proposed in [7]. The primary aim is to find a robust controller that can ensure good performance despite indeterminate delays and other problems in the communication network. Using linear matrix inequalities, control gains were found that yielded far better response than traditional control settings. Further, adequate response could be guaranteed for even very large delays. The control approach requires further development for large scale systems.

We are currently designing and developing a middleware framework, GridStat, to deliver status information for the power grid in a fashion conducive to its survivability. GridStat has a publish-subscribe architecture that optimizes performance and resource usage based on the semantics of the particular status items being delivered. It supports a CORBA-compliant API for ease of integration into multiple programming languages. It provides multiple quality of service (QoS) properties: fault tolerance, realtime performance, and network security (confidentiality, integrity, non-repudiation). The degree of each QoS property can be tailored for the particular status item by publishers, subscribers, and hierarchical QoS managers (operated for example by a power company or an ISO).

Finally, we are creating a prototype system to integrate power grid data published using the Extensible Markup Language (XML). Our strategy is to create a homogenous portal by "wrapping" each data source with conversion programs to map from site-specific meta-data to a common, shared DTD and set of units. Since the data is read-only, the opposite conversion is not needed. Furthermore, approximate conversions suffice since XML is quite capable of describing irregular data (data that only loosely conforms to a schema, or has local exceptions). We anticipate that wrappers will often produce irregular data. To provide better service for consumers, we are also developing a query language called ApproXPath [8] that handles irregular data by supporting inexact (as well as exact) searches. We are also beginning work on temporal queries over status information, as well as flexible and adaptable schemes for its hierarchical aggregation.

4 Acknowledgements

This work was funded in part by the US Dept. of Commerce, National Institute of Standards and Technology Grant #60NANB1D0016 (Critical Infrastructure Protection program).

References

[1] Mountford, John and Ricardo Austria, "Keeping the lights on", *IEEE Spectrum*, June 1999, p. 34-39.

[2] "Utah's Black Ice: Cyber-attack scenario", http://www.cnn.com/2001/TECH/ptech/10/21/black.ice.idg/

[3] Dougls Proudfoot, Dave Taylor, "How to Turn a Substation into a Database Server," IEEE Computer Applications in Power, April 1999, pp 29-35

[4] Mark Adamiak, William Premerlani, "Data Communications in a Deregulated Environment," IEEE Computer Application in Power, July 1999, pp 36-39

[5] Bakken, David, "Middleware", Chapter in *Encyclopedia of Distributed Computing*, J. Urban and P. Dasgupta, eds., Kluwer Academic Publishers, 2002, to appear. See http://www.eecs.wsu.edu/~bakken/middleware.pdf.

[6] Bhowmik, Sudipto, "Security and Communications Requirements in Power Systems", MS Thesis, School of Electrical Engineering and Computer Science, Washington State University, August 2000.

[7] Yu, Xiaofeng and Tomsovic, Kevin, "Application of Linear Matrix Inequalities for Load Frequency Control with Communication Delays," submitted to *IEEE Transactions on Power Systems*.

[8] Xu, Lin. ApproXPath: An Approximate Tree Matcher for XML. Masters' of Science Thesis, Washington State University. May, 2002.