Design and Simulation of Fast Substation Protection in IEC 61850 Environments

Alfonso Valdes, Cui Hang, Prosper Panumpabi,
Nitin Vaidya, Chris Drew
Information Trust Institute
University of Illinois at Urbana-Champaign
Urbana, IL, 61801 USA
{avaldes, hangcui2, panumpa1, nhv, cdrew3}@illinois.edu

Dimitry Ischenko
ABB US Corporate Research Center
Raleigh, NC, 27606 USA
dmitry.ishchenko@us.abb.com

***Abstract*—The IEC 61850 protocol suite provides significant benefits in electrical substation design and enables formal validation of complex device configurations to ensure that design objectives are met. One important benefit is the potential for protective relays to react in a collaborative fashion to an observed fault current. Modern relays are networked cyber-physical devices with embedded systems, capable of sophisticated protection schemes that are not possible on legacy overcurrent relays. However, they may be subject to error or cyber attack. Herein, we introduce the CODEF (Collaborative Defense) project examining distributed substation protection. Under CODEF, we derive algorithms for distributed protection schemes based on distributed agreement. By leveraging Kirchhoff's laws, we establish that certain fast agreement protocols have important equivalences to linear coding and error correction theory. In parallel, we describe a cyber-physical simulation environment in which these algorithms are being validated with respect to the strict time constraints of substation protection.**

Keywords*—IEC 61850, substation protection, protective relays, cyber-physical simulation, distributed agreement, error-correcting codes

I. Introduction

The migration to IEC 61850 [1, 2] for substation communications promises significant benefits in substation configuration, interoperability, and topology definition. Those benefits will directly support migration of legacy electric systems to "smart grids," a strategy now being pursued in many parts of the world. Since 61850 is Ethernet-based, there is concern that it is subject to cyber network attacks. In addition to attacks, there may be malfunctions or outages either in the substation network or in the Intelligent Electronic Devices (IEDs) themselves. For the purposes of this paper, the IEDs of interest are primarily protective relays that sense fault currents, trip breakers, and inform their peers of protective actions taken.

In typical 61850 substation design, the relays are configured with time-response logic so that the breaker closest to a fault trips first (thereby minimizing the extent of the affected service area), and other relays have redundant views of the fault current. If a further relay continues to sense a fault, its logic trips a breaker, but in this case more of the circuit is affected by the outage. This latter case is indicative of a malfunction or compromise of the relay that should have tripped. The collaborative defense algorithm we propose below achieves distributed agreement among the community of relays as to the presence and location of a fault current, and the correctness of a trip response.

We are particularly concerned with attacks wherein an adversary injects syntactically correct but malicious measurements in 61850 GOOSE (Generic Object Oriented Substation Event) or SV (Sampled Value) messages. Our approach also addresses the case of non-malicious error in measurement.

As GOOSE and SV are priority real-time messages, they bypass the TCP/IP stack and interface directly to the Ethernet Link Layer. GOOSE messages, including trip, interlocking, and inter-trip messages, belong to the "fast message" class and should be transmitted within 10 ms, or as little as 3 ms for some messages. SV messages occur at rates dependent on message class, with classes of 1.5 KHz, 4 KHz, and 12 KHz defined. Client-server messages in 61850 go through the TCP/IP stack, and although no explicit timing requirements are specified, rates of hundreds per second should be expected [1].

A key contribution of our work is a novel distributed agreement scheme based on substation topology and the Kirchhoff current and voltage laws (KCL and KVL). In particular, our derivation benefits from a useful equivalence to Hamming error control codes [3], enabling identification of malicious or faulty measurements, even in the presence of noise, within the computational time budget. Connections between coding theory and distributed consensus have been developed in [4] and [5], which partially form the basis for our present work.

II. Electrical System Protection With IEC 61850

In power systems, "protection" refers to detection of potentially dangerous fault currents, and isolation of the affected system components. Failure of the system to respond quickly to a fault can result in widespread outages, damage to expensive equipment, and safety hazards.

This work is sponsored by the Department of Energy under grant DE-OE0000674, under subcontract to ABB Research. The views expressed are those of the authors.

In legacy systems, protection is based on a physical response (a fuse element melts, or an induction disk rotates to open the contact) in response to a fault. Modern systems increasingly use circuit breakers that trip under the control of microprocessor-based relays, which are cyber-physical components with multiple stages of time-response elements to sense overcurrent, over- and under- voltage, and frequency anomalies. These elements are combined to create a trip logic within the relay. In a modern IEC 61850 configuration, relays have the ability to communicate with peers or to a master control at a substation.

IEC 61850 [2] is increasingly being adopted for substation configuration, communications, and implementation of advanced protection and control schemes. Relays are examples of Intelligent Electronic Devices (IEDs), for which the IEC standard specifies self-describing object models. The standard also includes an XML-based Substation Configuration Language (SCL), which is used to configure compliant devices and permits formal analysis to verify correctness of configurations. The standard simplifies substation configuration and communication by replacing point-to-point serial links with a high-speed Ethernet bus and ensures interoperability by using standard, vendor-independent hierarchical object models.

For the purposes of protection, the time-current response of a particular relay can be configured through SCL and stored in the instantiated IED description file (*.IID). The response logic implementing the non-directional overcurrent protection function typically calls for an immediate trip when a current over a threshold magnitude is sensed, and a delayed trip that effectively integrates fault current over time and trips when the integrated current exceeds a second threshold.

In a digital substation environment, voltage and current sensors are connected to merging units (MUs), which digitize and publish voltage and current measurements using the 61850 Sampled Values (SV) message class. The sampling rate for most MUs now implemented is 80 samples/cycle (4.8 kHz at 60 Hz), as specified in IEC 61850-9-2LE. Relays subscribe to the SV streams, perform internal signal processing, and execute control actions as needed. Relays can also report events using the GOOSE message class. GOOSE message payloads are highly configurable by protection engineers and may include circuit breaker status, analog measurements (for example, phasor measurements as calculated internally by DFT), or any internal IED parameter from the SCL file exposed to the corresponding IEC 61850 communications interface. For instance, a relay would typically issue a GOOSE message to notify its peers if it has undertaken a trip action.

The time-current response characteristics of upstream and downstream IEDs are coordinated so that the relay closest to the fault trips first. In that way, the system maintains safe operation while minimizing the extent of the resultant outage. After the relay closest to the fault trips, it signals its peers so that they do not trip needlessly. This signal is known as a *blocking response*.

Relays are aware of currents and voltages at the points they measure directly and through GOOSE messages from peer relays. In typical deployments, relays are placed in such a way that multiple relays measure a given bus or line. Our agreement algorithm exploits this partially redundant view of the system, based on the system topology and the current and voltage laws that describe power flow. There is enough redundancy that the agreement can be considered algebraically similar to an error-correcting code, as we will discuss in Section IV.

The protocol allows for an implementation in which relays send messages through MUs, where a single MU may mediate the communication of a number of relays and interact with other MUs. A relay may subscribe to SVs from its own MU as well as from adjacent MUs, but this may incur a computational burden beyond current hardware capabilities. (Measurements must be processed via computationally costly signal processing transforms.) Alternatively, a relay may subscribe to the SV stream from its associated MU and receive phasor values as GOOSE messages from its neighbors, but this incurs some delay. We will model such delay artifacts as the fidelity of our simulation improves, but at present our algorithm addresses either implementation.

III. Threat Model and Related Work

As the relays are cyber-physical systems, we are concerned about multiple kinds of adversary actions.

- A malicious MU can issue a false SV that indicates a fault current when none is present, potentially leading to a needless trip action by the relay subscribing to the SV stream.
- A malicious MU can mask a fault by issuing a false SV indicating that no fault is present. The system would then operate in a dangerous state until the time-current logic of an upstream relay issues a trip order, but the outage would be more widespread and the damage more severe than if the correct action had been taken.

The latter class of attack is of concern in two scenarios. First, faults may arise out of the attacker's control, in which case the attack causes damage opportunistically. Second, one of these attacks can be launched as part of a blended cyber-physical attack wherein the attacker causes the fault by some physical mechanism while impeding the protection response by means of a cyber compromise.

The above attacks are examples of false data injection attacks into electrical systems, which have been described in [6, 7, 8]. In [6], the authors identify a stealthy injection attack into state estimations algorithms. State estimation uses an iterative approach to estimate state from observable measurements. Measurements are related to state via a Jacobean matrix. The rank of the Jacobean in typical transmission systems is such that injected error vectors in the kernel of the matrix will lead to an incorrect state estimate, but the injected error vector will not be flagged by the commonly used bad data detection algorithms. The authors of [7] extended this result by considering detection and countermeasures consisting of optimally placing a limited number of costly but higher-fidelity, harder-to-compromise measurement units (modern Phasor Measurement Units, or PMUs) so as to achieve a degree of redundancy that greatly increases the attacker's burden. Those two papers considered distribution systems. In [8], the authors considered a radial distribution system in which Conservation Voltage Reduction (CVR) is applied. CVR is an energy-saving technique in which voltage at the head of the feeder is reduced slightly. Depending on the nature of the load, a modest reduction in energy consumption can be achieved with satisfactory performance of electrical equipment. In CVR, measurements must be taken along the feeder, and transformers along the feeder may be required to maintain end-line voltage above the specified limit (typically, 95% of nominal). The challenge in that case is that radial topologies allow for less redundancy, but it was nonetheless observed that the impact of a stealthy attack is modest.

IV. DISTRIBUTED AGREEMENT

In this section, we describe an agreement approach that enables collaborating IEDs to agree on the presence of a fault condition and on whether a protective action (breaker trip) is warranted. The approach detects a limited number of incorrect or malicious measurements in a GOOSE and/or SV as described above. The community of IEDs considers the measurements from their peers, reinforced by the actual measurement each can record, and applies Kirchhoff's laws to determine whether the set of measurements is valid. In the case of invalid measurements, we seek to identify the malfunctioning relays, even in the presence of noise. We consider the simplified ring circuit topology shown in Figure 1 (arrows denote current direction).

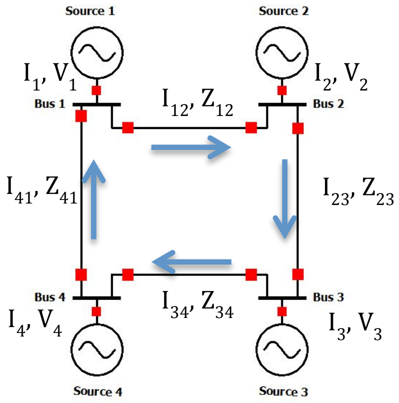

Figure 1. 4-Generator, 4-Bus Circuit Used for Simulation

The current and voltage at node n are denoted by I_n and V_n, respectively, and the current between nodes m and n by I_{mn}. The complex impedance in phasor form between nodes m and n is denoted by Z_{mn}. The corresponding KCL/KVL equations are given by

$$\begin{aligned}
&I_1 + I_{41} - I_{12} = 0\\
&I_2 + I_{12} - I_{23} = 0\\
&I_3 + I_{23} - I_{34} = 0\\
&I_4 + I_{34} - I_{41} = 0\\
&I_{12} - V_1 / Z_{12} + V_2 / Z_{12} = 0\\
&I_{23} - V_2 / Z_{23} + V_3 / Z_{23} = 0\\
&I_{34} - V_3 / Z_{34} + V_4 / Z_{34} = 0\\
&I_{41} - V_4 / Z_{41} + V_1 / Z_{41} = 0
\end{aligned} \tag{1}$$

These can be expressed in matrix form as

$$\begin{pmatrix}
1 & 0 & 0 & 0 & -1 & 0 & 0 & 1 & 0 & 0 & 0 & 0\\
0 & 1 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 1 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 1 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -\frac{1}{Z_{12}} & \frac{1}{Z_{12}} & 0 & 0\\
 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -\frac{1}{Z_{23}} & \frac{1}{Z_{23}} & 0\\
 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -\frac{1}{Z_{34}} & \frac{1}{Z_{34}}\\
 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \frac{1}{Z_{41}} & 0 & 0 & -\frac{1}{Z_{41}}
\end{pmatrix}
\begin{pmatrix} I_1\\ I_2\\ I_3\\ I_4\\ I_{12}\\ I_{23}\\ I_{34}\\ I_{41}\\ V_1\\ V_2\\ V_3\\ V_4 \end{pmatrix}
=
\begin{pmatrix} 0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0 \end{pmatrix} \tag{2}$$

We can rewrite the above succinctly as

$$A \times [I, V]^{\mathrm{T}} = 0 \tag{2'}$$

Let us assume that an adversary can inject a malicious change ΔI into the current vector. In the absence of measurement noise, the result is

$$\begin{aligned}
&A\left[I + \Delta I, V\right]^T = S\\
&\Rightarrow S = A \times [\Delta I, 0]^{\mathrm{T}}
\end{aligned} \tag{3}$$

If the adversary can corrupt one current measurement, then ΔI has one nonzero value f at, say, position j. In that case, S (analogous to a syndrome vector in coding theory) is f times column j of A.

In the presence of measurement noise, a threshold test is applied to determine if the measurements are consistent with KCL. It is assumed that the system is operating normally if $||S|| < \tau$, where the threshold τ is determined based on statistical analysis of historical measurements. If the threshold test fails, the measurement corresponding to the column of A that best aligns with S is identified as faulty. A heuristic is defined based on the normalized dot product of S with the columns of A,

$$Y = S^T A \times DIAG(W) \tag{4}$$

where W are weights proportional to the inverse norm of the columns of A. The weights are static for a particular topology and can be precomputed. The largest element of Y corresponds to the column of A most aligned with S, and therefore identifies the faulty measurement.

A can be transformed to the standard form of a matrix for a linear code through algebraic manipulation to obtain

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{Z_{12}}-\frac{1}{Z_{41}} & \frac{1}{Z_{12}} & 0 & Z_{41} \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{Z_{12}} & -\frac{1}{Z_{12}}-\frac{1}{Z_{23}} & \frac{1}{Z_{23}} & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{Z_{23}} & -\frac{1}{Z_{23}}-\frac{1}{Z_{34}} & \frac{1}{Z_{34}} \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & \frac{1}{Z_{41}} & 0 & \frac{1}{Z_{34}} & -\frac{1}{Z_{34}}-\frac{1}{Z_{41}} \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -\frac{1}{Z_{12}} & \frac{1}{Z_{12}} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -\frac{1}{Z_{23}} & \frac{1}{Z_{23}} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -\frac{1}{Z_{34}} & \frac{1}{Z_{34}} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \frac{1}{Z_{41}} & 0 & 0 & -\frac{1}{Z_{41}} \end{pmatrix} \begin{pmatrix} I_1 \\ I_2 \\ I_3 \\ I_4 \\ I_{12} \\ I_{23} \\ I_{34} \\ I_{41} \\ V_1 \\ V_2 \\ V_3 \\ V_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad (5)$$

The voltage and current measurement vector may be viewed as a linear code, and the transformed matrix A as the corresponding parity check matrix. The parity check matrix has Hamming distance $d = 4$. For t (error correction) and u (error detection), distance $t + u + 1$ ($u \geq t$) is required. With distance 4, the code may be used in one of two ways [3]:

- $t = 0$, $u = 3$ (3-error detection): detect a problem in the presence of up to 3 errors, but without the ability to correct the error.
- $t = 1$, $u = 2$ (correct 1 error, and detect 2 errors): detect a problem in the presence of up to 2 errors, with the ability to correct one.

V. Cyber-Physical Simulation Environment

We are implementing a simulation environment to validate the above algorithms. Our implementation is based on the Real Time Digital Simulator (RTDS) [9], which is widely used in the utility sector and power systems research to simulate grid systems. Within RTDS, we are able to define a topology model and simulate a variety of operational and fault conditions, with inputs and outputs that interface to real power system components. This capability enables high-fidelity, "hardware-in-the-loop" simulation for power systems. For the present work, we are incorporating physical ABB Relion family relays. The simulation environment topology is shown in Figure 2.

RTDS is designed for use by power system engineers to simulate complex power system circuits and potentially signal actual power system equipment, permitting realistic hardware-in-the-loop simulation at time steps as small as 50 μs.

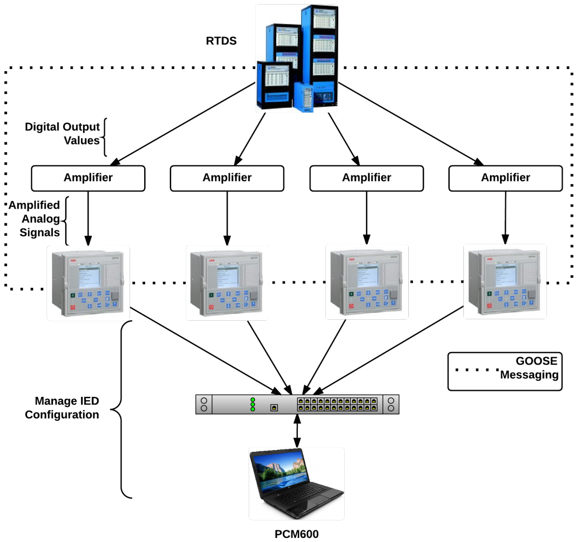

Figure 2. Cyber-Physical Simulation Environment

We are presently able to simulate a variety of fault types (single phase to ground, bi-phase, or three-phase) at any distance between the head of the feeder and the end customer.

We are in the process of implementing a relay-testing configuration, wherein signals are extracted from the RTDS through GTAO cards (capable of providing analog output from a running simulation to external equipment), and then sent through amplifiers to produce currents that the Relion family relays will sense as actual faults. For configurations needing more than four physical devices, we are implementing emulated relays using BeagleBone Black development platforms [10] and the open-source libIEC61850 [11]. The Relion family relays are configured using ABB's PCM600 system, which allows us to manage multiple IEDs as well as export their configuration, via SCL files, to the emulated devices to ensure consistent configuration. The use of low-cost emulated devices will permit additional flexibility of configuration with respect to the number of devices and circuit topology.

VI. Simulation Results

We now present the results of a MATLAB/Simulink [12] simulation using the power system tools. The circuit used was the 4-bus, 4-generator example shown in Figure 1 above. Ground truth voltages and currents were simulated, and then random noise was added to each measurement.

For the circuit in question, we set nominal values for circuit parameters to be typical of voltages, impedances, and angle differences in a nominal 240 kV system. The parameters do not represent any actual system. The bus voltages and angles are given in Table 1.

Table 1. Bus Voltages and Angles

	Voltage (kV)	Angle (deg)	Comment
V_1	228.70	0.119975	Slack bus
V_2	241.825	5.6478	PQ bus
V_3	245.915	7.4258	PQ bus
V_4	241.825	5.6478	PQ bus

Impedances Z_{12}, Z_{23}, Z_{34}, and Z_{41} were set to 1.85 + j 37.67 Ohm. Those parameters were chosen as they correspond to an RTDS model that converges to steady state in 4 iterations.

The simulated noise was Gaussian and zero-mean, with a standard deviation equal to $f\,M$, where M is the nominal value for a voltage or current measurement, and f is a parameter that is on the order of 0.01 to 0.05. At each step, we drew noise values from the respective noise distributions and executed a realization of the circuit behavior. For our runs, we used f = 0.01 for the steady state. In the steady state, we obtained all the required measurements. A faulty voltage measurement was injected at realization 50, and a current fault was injected at step 75.

Figures 3, 4, and 5 show traces of the syndrome vector elements corresponding to voltage and current, as well as the norm of the syndrome vector. These traces were normalized by the element-wise average (excluding the injected fault values) to account for the differences in units between voltage and current.

Figure 3 shows the normalized syndrome vector for the case in which the faulty voltage was injected at step 50. While the spike is largest for the injected voltage (V_2), we notice that there are less pronounced spikes for other voltage measurements. We hypothesize that they are due to other apparent voltage values changing to maintain the KVL condition.

Figure 4 shows the normalized syndrome vector corresponding to current values. In this case, a faulty measurement was injected at step 75. Once again, the faulty measurement was the largest-magnitude spike, but other current measurements spiked as well.

Figure 5 shows a trace of the norm of the syndrome vector. The norm would be used for a threshold test as described in Section IV.

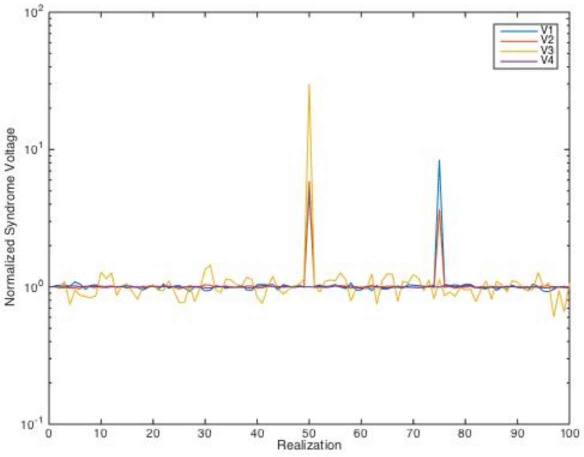

Figure 3. Normalized Syndrome Vector Elements (Voltage)

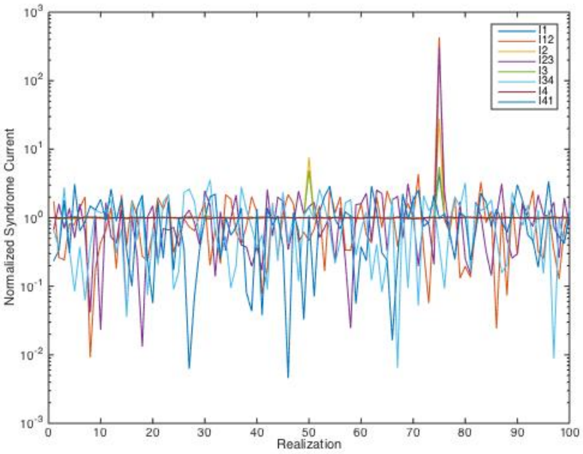

Figure 4. Normalized Syndrome Vector Elements (Current)

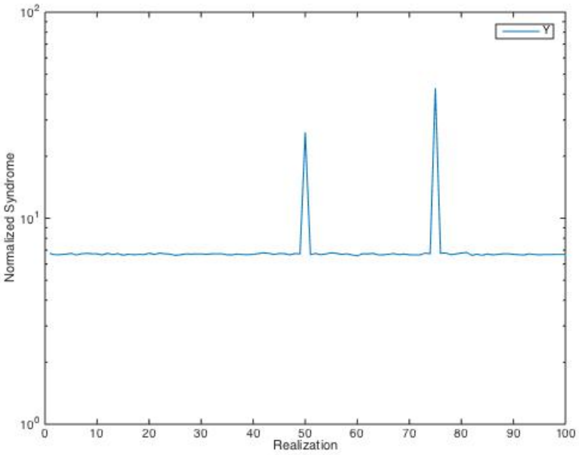

Figure 5. Norm of the Syndrome Vector

The simulations of steady state and faulty measurement may be done over a range of values for f. This provides a sensitivity analysis of the technique's ability to detect faulty measurements as noise is increased. Alternatively, the lower limit of f at which an attack is detectable can be seen as the degree to which an attacker can alter a measurement and remain stealthy.

VII. Summary and Future Work

As smart grids evolve to become increasingly sophisticated cyber-physical systems requiring distributed agreement and coordinated response to adverse events, the potential for damage from cyber attacks becomes a serious concern. The sampling rates and response time constraints are sufficiently challenging that conventional cybersecurity approaches based on cryptographic protocols are infeasible. These systems require fast algorithms to achieve consensus about actual or apparent adverse conditions, such as fault currents.

The typical deployment of protective relays in electric systems permits a degree of redundancy, based on system topology and well-known voltage and current laws. Our research has identified similarities between the matrix equations that describe measurements according to topology and physics, and the matrices used in error-correcting codes. That observation has permitted us to cast the distributed cyber-physical agreement problem using techniques from the coding field. Specifically, identification of faulty measurements and identification of a particular faulty device are possible under typical substation configurations.

Our hypotheses have been demonstrated via a MATLAB simulation, in which we can identify faulty measurements as claimed even in the presence of noise. We are in the process of migrating the simulation to a higher-fidelity real-time simulation environment, using actual relays provided by ABB as "hardware in the loop." The eventual simulation environment will permit assessment of the performance of the approach when considering realistic features of actual devices, system delays, and distributed computation.

References

[1] F. Hohlbaum, M. Braendle, and F. Alvarez, "Cyber security: Practical considerations for implementing IEC 62351," presented at the Inaugural PAC World Conference, Dublin, Ireland, 2010.

[2] IEC 61850, "Communication networks and systems in substations," (all parts), Reference number IEC 61850-SER. [Online]. Available: http://www.iec.ch/smartgrid/standards/. Accessed on: Mar. 11, 2015.

[3] S. Lin and D. J. Costello, *Error Control Coding*, Prentice-Hall, 1983.

[4] R. Friedman, A. Mostefaoui, S. Rajsbaum, and M. Raynal, "Asynchronous agreement and its relation with error-correcting codes," *IEEE Transactions on Computers*, vol. 56, no. 7, pp. 865–875, July 2007.

[5] A. Moustefaoui, S. Rajsbaum, and M. Raynal, "The synchronous condition-based consensus hierarchy," *Proc. 18th Int. Conf. Distributed Computing*, *Lecture Notes in Computer Science*, vol. 3274, Springer, 2004, pp. 1–15.

[6] Y. Liu, P. Ning, and M. Reiter, "False data injection attacks against state estimation in electric power grids," *Proc. 16th ACM Conf. on Computer and Communications Security (CCS '09)*, Chicago, IL, 2009, pp. 21–32.

[7] R. Bobba, K. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. Overbye, "Detecting false data injection attacks on DC state estimation," *Proc. 1st Workshop on Secure Control Systems (SCS)*, Stockholm, Sweden, 2010. [Online]. Available: https://www.truststc.org/conferences/10/CPSWeek/program.htm

[8] A. Teixeira, G. Dán, H. Sandberg, R. Berthier, R. B. Bobba, and A. Valdes, "Security of smart distribution grids: Data integrity attacks on integrated volt/VAR control and countermeasures," *Proc. American Control Conference (ACC)*, Portland, OR, 2014, pp. 4372–4378.

[9] RTDS Technologies. 2015. [Online]. Available: http://www.rtds.com/index/index.html. Accessed on: Jan. 8, 2015.

[10] BeagleBone Black. 2015. [Online]. Available: http://beagleboard.org/black. Accessed on: Mar. 3, 2015.

[11] libIEC61850: Open source library for IEC 61850. 2014. [Online]. Available: http://libiec61850.com/libiec61850/. Accessed on: March 3, 2015.

[12] MATLAB. The MathWorks Inc. [Online]. Available: http://www.mathworks.com/products/matlab/. Accessed on: Jan. 29, 2015